White Paper

Bitdefender

Old dog with new tricks. A study on the resurfacing of the Glupteba malware

Contents

Summary 3

Infection chain 4

Dropper 4

Backdoor capabilities and techniques 5

Techniques Present From MITRE ATT&CK Matrix 6

Appendix 1 - Monthly detection rate 7

Appendix 2 - Download URLs since August 2019 8

Appendix 3 - Process name frequency by month 9

Appendix 4 - Number of detected payloads launched with fake svchost parent 10

Appendix 5 - Detection distribution by region 11

Author: János Gergő SZÉLES - Senior Software Engineer, Bitdefender

Summary

In the cat and mouse game of cybersecurity, researchers are used to analyzing and prioritizing new malware techniques that emerge in the wild. In this context, malicious actors often launch campaigns based on old malware or old techniques, and they frequently succeed at staying under the radar. That's what happened with Glupteba, a backdoor first spotted in 2014. At the end of 2018, our Advanced Threat Control team observed a considerable wave of detections on a particular process name, ‚***app.exe***', and started actively looking into it. We traced the process to the original Glupteba malware. The increasing number of such detections throughout the year suggests an extensive campaign focused on enterprise customers.

Infection does not take place through the consecrated attack avenues in enterprise, such as spear-phishing or APTs. Instead, the payload arrives on the computer by malvertising or through potentially unwanted applications (PUAs) designed to download it from compromised websites. These domains typically have a human-friendly name rather than a randomly generated one. The tell-tale sign is that they contain the malicious executable files in a specific sub-path ‚/app/', which indicates the attackers generate and register these domains specifically to host the payload.

While the process that runs in the background might have several names, almost all infection cases reference the ‚app.exe' process. That's why we might call the malware AppExe and Glupteba interchangeably in this article.

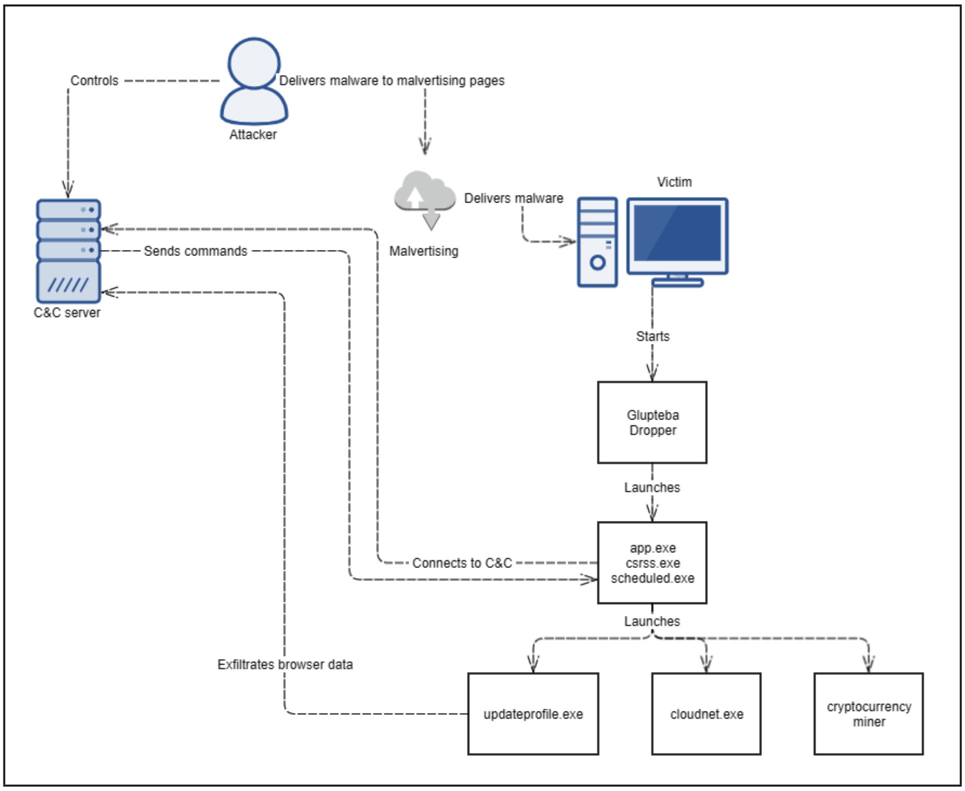
Operation of an already discovered malware comes with advantages and disadvantages. One advantage might be that some infection patterns are no longer trending and may go unnoticed by researchers. The disadvantage is implicit: researchers already know the malware's actions and indicators of compromise. However, attackers use a variety of tricks to keep the malware on the cutting edge of detection evasion. Such techniques include:

- packing, to generate lots of different hashes for the same code and evade static analysis
- specific command line triggers, to prevent execution in an automated sandboxed environment
- living-off-the-land techniques for downloading updates and maintaining persistence
- creating copies of itself with names that resemble critical system processes
- mimicking various process trees to trick an observer into thinking it is a benign process

Even though AppExe installs through malvertising campaigns, its primary purpose is far from just delivering annoying ads. The capabilities of this malware include:

- backdoor with persistence achieved via scheduled tasks and regular updates saved under various process names
- adding the infected machine to a botnet
- data exfiltration
- remote process execution, mostly cryptocurrency mining and browser information theft

Infection chain



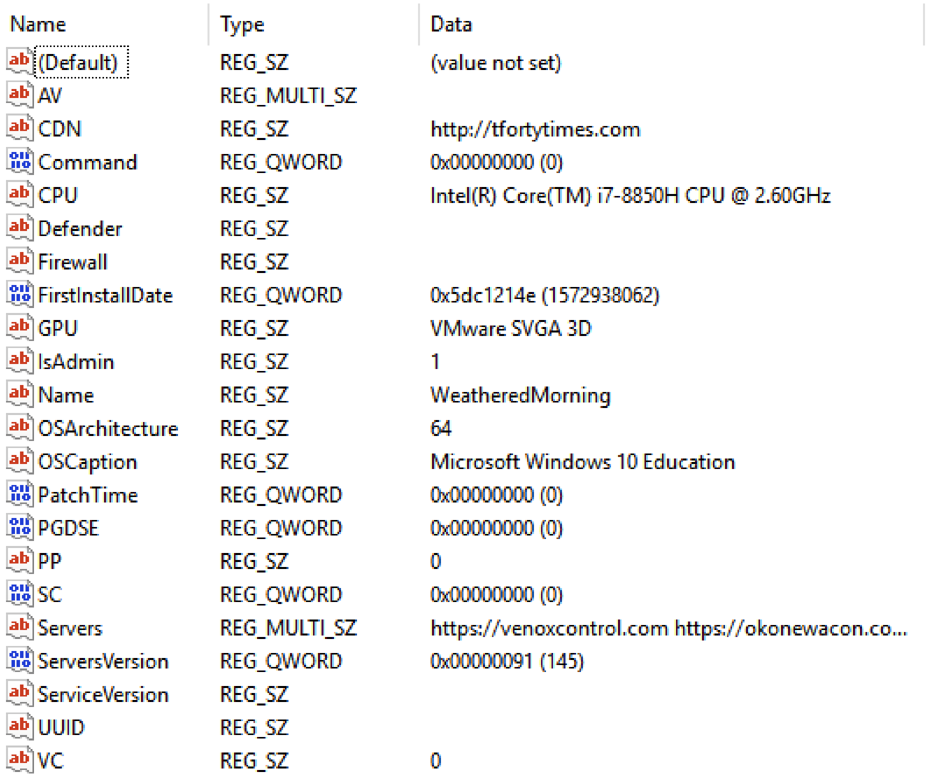
Dropper

The malware arrives on the system via malvertising websites by tricking the user into running an installer bundled with the malicious executable. When launched, the ***app.exe*** process unpacks its code from its file. The malicious binary file has several variations as it uses a custom packer written in Go. Packing with lots of variations helps Glupteba evade static detection and makes it hard to be signed by scan engines. Our malware zoo currently holds more than 6,500 different Glupteba hashes so far.

Our research identified two code patterns present in 50% of the files analyzed (Appendix 7). These patterns vary slightly (inversed "if" conditions, different mathematical operations with the same results) but they are recognizable nonetheless. The other half of the observed binary files have gone through obfuscation and, subsequently, follow no pattern.

AppExe implements persistence by first copying itself to either ***\Windows\rss\***, ***\Windows\temp\*** or \AppData\Local\Temp\ under a name that mimics system processes (csrss.exe, scheduled.exe or the most frequent app.exe, as shown in Appendix 3). Thus, a user might believe the backdoor that runs on the system is benign. Afterwards, the dropper launches ***schtasks.exe*** to schedule the executable to run periodically with the highest privileges, along with another scheduled task that downloads the malware again by using ***certutil.exe***. The most common download URLs are listed in Appendix 2.

When the malware runs for the first time, it collects information about the operating system it runs on, hardware configuration and the current user. It also contacts its C&C server to check availability and version. It then creates a registry key in *HKEY_USERS\<SID>\Software\Microsoft\TestApp* and store all information there.



Name	Type	Data
(Default)	REG_SZ	(value not set)
AV	REG_MULTI_SZ	
CDN	REG_SZ	http://tfortytimes.com
Command	REG_QWORD	0x00000000 (0)
CPU	REG_SZ	Intel(R) Core(TM) i7-8850H CPU @ 2.60GHz
Defender	REG_SZ	
Firewall	REG_SZ	
FirstInstallDate	REG_QWORD	0x5dc1214e (1572938062)
GPU	REG_SZ	VMware SVGA 3D
IsAdmin	REG_SZ	1
Name	REG_SZ	WeatheredMorning
OSArchitecture	REG_SZ	64
OSCaption	REG_SZ	Microsoft Windows 10 Education
PatchTime	REG_QWORD	0x00000000 (0)
PGDSE	REG_QWORD	0x00000000 (0)
PP	REG_SZ	0
SC	REG_QWORD	0x00000000 (0)
Servers	REG_MULTI_SZ	https://venoxcontrol.com https://okonewacon.co...
ServersVersion	REG_QWORD	0x00000091 (145)
ServiceVersion	REG_SZ	
UUID	REG_SZ	
VC	REG_SZ	0

The process first verifies whether it's running under a regular user or an administrator account. If it is less privileged, it performs a UAC bypass by exploiting the registry checks of an auto-elevated Windows binary, ***fodhelper.exe.*** Once the malware obtains administrator privileges, it can ensure that its process runs under the SYSTEM user. It steals a winlogon.exe token to run as Trusted Installer [2], which is a process that runs as SYSTEM. After the privileged process starts, the only remaining step is to contact the C&C server and execute the received commands.

Backdoor capabilities and techniques

Like any other backdoor, Glupteba has a command interpreter and can perform various actions upon the C&C server's demand. The main commands are [1]:

- **update:** download and run the latest version of the malware
- **download:** download a file to the system
- **execute:** run a file from on the system
- **notify:** start sending periodic heartbeats to the server
- **verify-signature:** check the signature of the PE file, to ensure that it is the correct version
- **sc:** take a screenshot
- **upload-file:** exfiltrate a file to the server
- **update-cdn:** update C&C server information

The malware can also steal information from Chrome, Opera and Yandex browsers, including history, cookies and passwords.

Due to the capabilities of the malware, the infected systems get recruited into a botnet. This way, attackers could sell some machines on illicit platforms to perform various tasks. For instance, someone may use a chunk of the botnet to download and execute cryptocurrency miners.

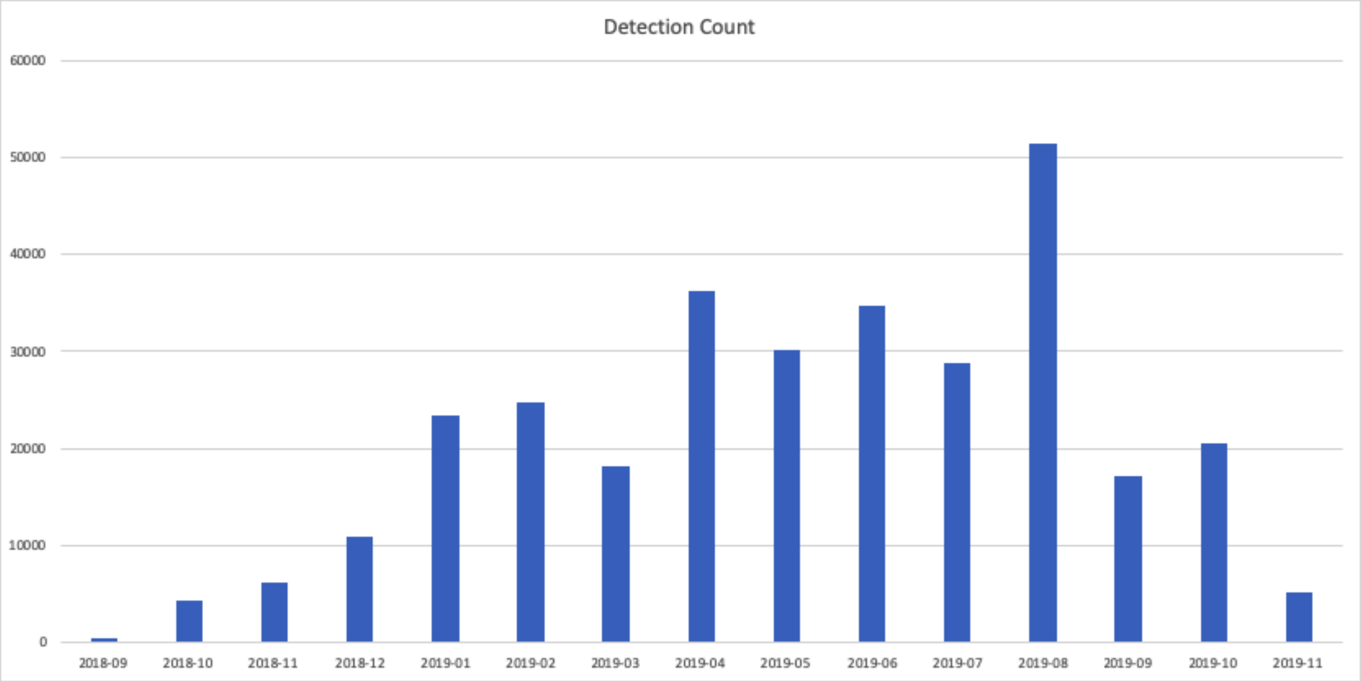
Based on our telemetry, we observed that, in the past few months, Glupteba has been mainly used to execute the browser stealer process, ***updateprofile-<random number>.exe***.

The way AppExe runs the payload processes is also deceptive for the user, as the malware changes the payload's parent process to ***svchost.exe*** instead of itself. This technique is growing in popularity, as shown in Appendix 4.

Techniques Present From MITRE ATT&CK Matrix

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Command and Control	Exfiltration	Impact
Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Access Token Manipulation	Credentials in Files	Security Software Discovery	Data from Local System	Commonly Used Port	Data Encrypted	Resource Hijacking
Scheduled Task	Scheduled Task	Bypass User Account Control	Bypass User Account Control		System Information Discovery	Screen Capture	Standard Application Layer Protocol	Exfiltration Over Command and Control Channel	
		Scheduled Task	Deobfuscate/Decode Files or Information		System Owner/User Discovery				
			Disabling Security Tools		System Time Discovery				
			File Deletion						
			File and Directory Permissions Modification						
			Software Packing						

Appendix 1 - Monthly detection rate

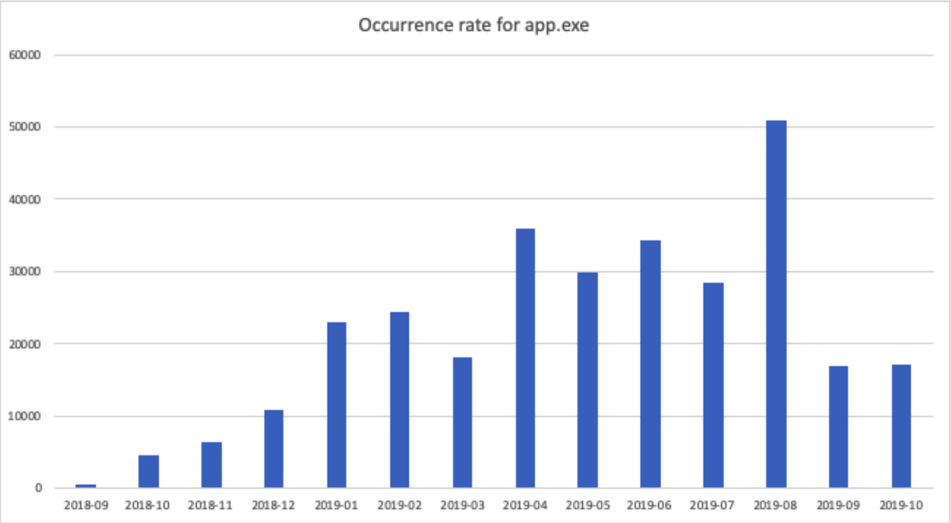


Appendix 2 - Download URLs since August 2019

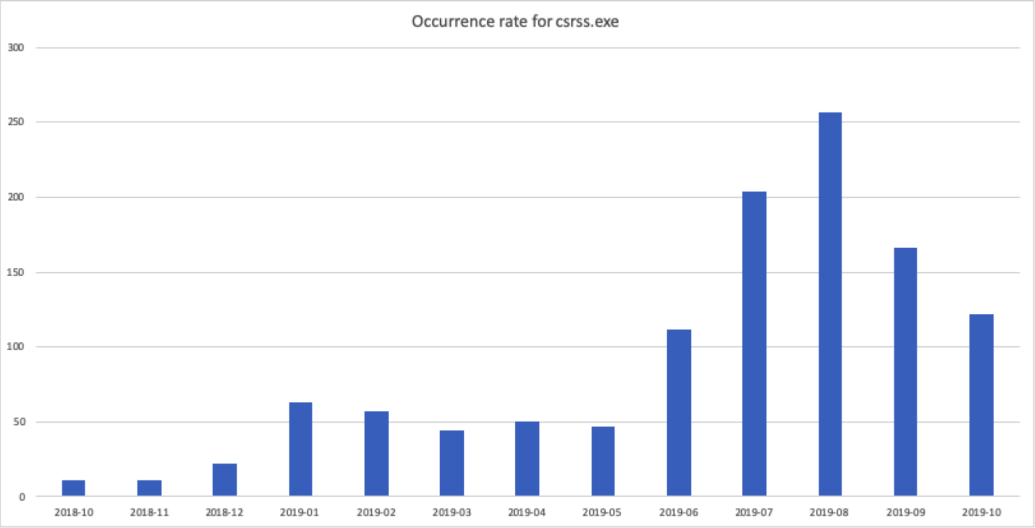
Count	URL
299	hxxp://bigtext.club/app/app.exe
283	hxxp://newscommer.com/app/app.exe
64	hxxp://tfortytimes.com/app/app.exe
40	hxxp://gamedemo.xyz/app/app.exe
37	hxxp://nevernews.club/app/app.exe
29	hxxp://foxmusic.xyz/app/app.exe
27	hxxp://skolkovotop.info/app/app.exe
19	hxxp://beguest.xyz/app/app.exe
10	hxxp://fstyline.xyz/app/app.exe
6	hxxp://roundworld.club/app/app.exe
6	hxxp://andreysharanov.info/app/app.exe
5	hxxp://headbuild.info/app/app.exe
4	hxxp://dp.fastandcoolest.com/app/3/app.exe
4	hxxp://krokas.info/app/app.exe
3	hxxp://monopeets.com/app/app.exe
3	hxxp://seamonkey.club/app/app.exe
2	hxxp://seasondjmusic.com/app/app.exe
2	hxxp://dp.fastandcoolest.com/app/4/app.exe
2	hxxp://cfpoweredcdn.com/app/app.exe
2	hxxp://tfortytimes.com/app/app.exe
2	hxxp://proactor.xyz/app/app.exe
2	hxxp://singlemusic.club/app/app.exe
2	hxxp://jeopath.club/app/app.exe
1	hxxp://speedandmusic.com/app/app.exe
1	hxxp://nadequalif.club/app/app.exe

Appendix 3 - Process name frequency by month

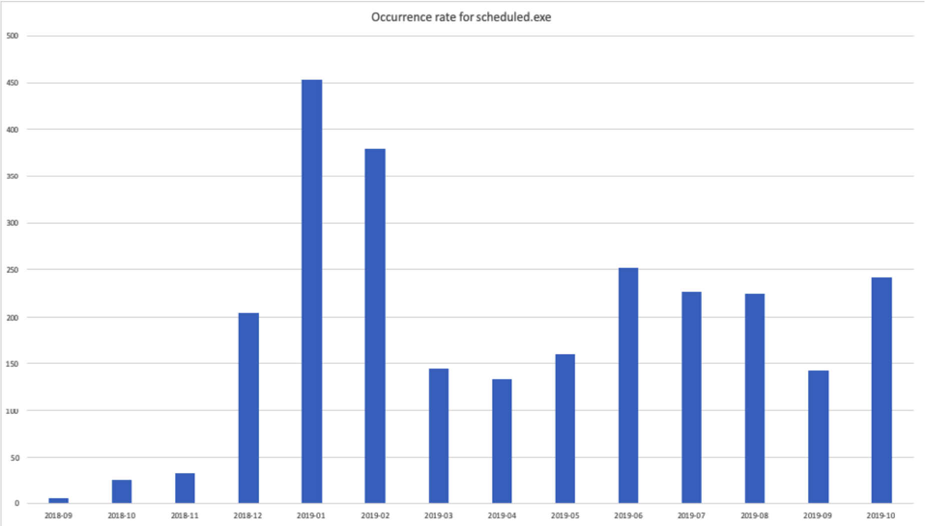
app.exe



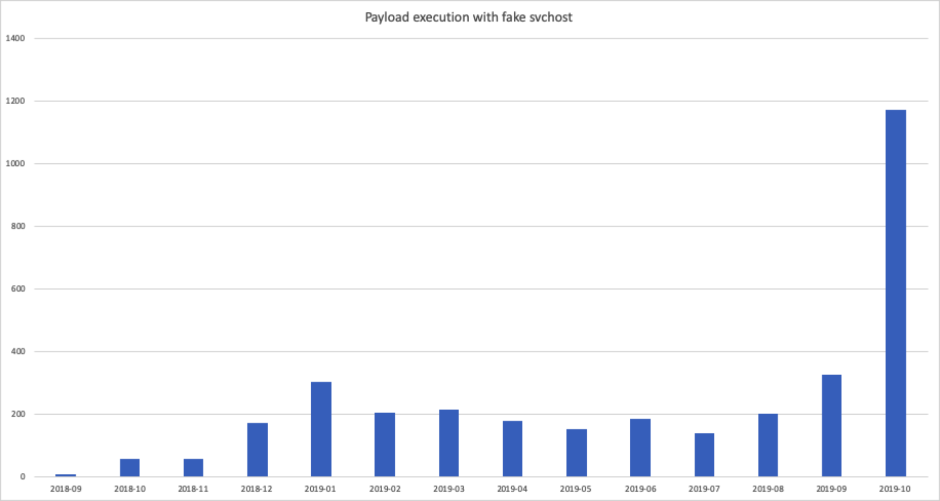
csrss.exe



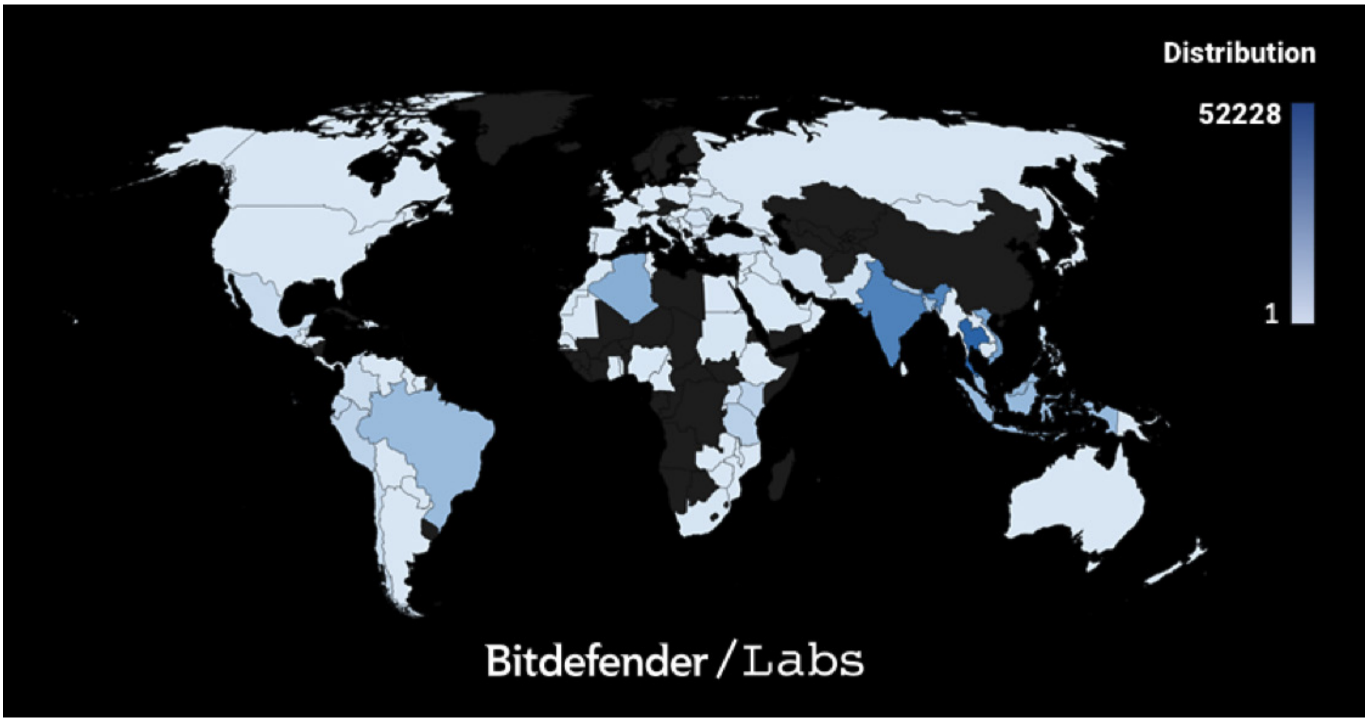
scheduled.exe



Appendix 4 - Number of detected payloads launched with fake svchost parent



Appendix 5 - Detection distribution by region



Country	Count
Thailand	52228
India	38884
Vietnam	26596
Algeria	21365
Malaysia	18095
Indonesia	17133
Brazil	16265
Bangladesh	12935
Nepal	12363
Tanzania	7981
Kenya	7506
Peru	6916
Ecuador	6623
Philippines	5856
Republic of Moldova	4998
Mexico	4550
Chile	4466
Uganda	3802
Colombia	3696
Pakistan	2398
Iran	2209
Turkey	1722
Romania	1643
Sri Lanka	1332
Brunei	965
Palestine	836
Democratic Republic of Timor-Leste	794
Rwanda	766
South Africa	645
Ukraine	622
Morocco	585
Cambodia	543
United Arab Emirates	531
Sudan	518
Laos	421
Russia	421
Egypt	312
Georgia	304
Dominican Republic	287
Tunisia	262
Nigeria	201

Iraq	197
Saudi Arabia	194
Montenegro	162
Papua New Guinea	149
Senegal	129
Argentina	76
Albania	70
Zambia	51
Myanmar	51
Serbia	50
Mauritius	48
United States	47
Ethiopia	45
Italy	43
Bolivia	40
Germany	39
Paraguay	34
Syria	32
Togo	28
France	28
Greece	26
Hong Kong	26
Mozambique	25
Ghana	24
Panama	20
Cameroon	19
Belize	19
Honduras	19
Singapore	18
Hungary	17
Canada	16
Kuwait	14
Malawi	12
United Kingdom	12
Mongolia	9
South Korea	9
Malta	8
Guyana	8
Hashemite Kingdom of Jordan	8
Spain	7
Costa Rica	6
Croatia	6
Zimbabwe	6
Australia	5
Qatar	5
New Zealand	5
Venezuela	4
Azerbaijan	4
Oman	3
Latvia	3
Taiwan	3
Bosnia and Herzegovina	3
Poland	3
Suriname	3
Mauritania	2
Bulgaria	2
Maldives	2
Guatemala	2
Slovenia	2
Trinidad and Tobago	2
Belarus	2
El Salvador	1
Haiti	1
Portugal	1
Seychelles	1
Netherlands	1
Japan	1

References:

[1] https://blog.trendmicro.com/trendlabs-security-intelligence/glupteba-campaign-hits-network-routers-and-updates-cc-servers-with-data-from-bitcoin-transactions/

[2] https://github.com/nfedera/run-as-trustedinstaller/blob/master/run-as-trustedinstaller/main.cpp

An extensive list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. More information about the program is available at https://www.bitdefender.com/oem/advanced-threat-intelligence.html.

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/.