Threat Report: StrongPity Spyware
August 7, 2020
Table of Contents

1 EXECUTIVE SUMMARY ............................................................................................................. 3

2 ANALYSIS .................................................................................................................................. 5
  2.1 Overview ................................................................................................................................. 5
  2.2 Attack Vectors .......................................................................................................................... 5
    2.2.1 Malicious Internet Service Providers ............................................................................... 5
    2.2.2 Domain Typosquatting ..................................................................................................... 6
    2.2.3 Software Downloading Websites ..................................................................................... 6
  2.3 Trojanized Installers ................................................................................................................ 7
    2.3.1 Targeted Software .............................................................................................................. 7
    2.3.2 Common Characteristics .................................................................................................... 7
    2.3.3 Antivirus Evasion Techniques ......................................................................................... 8
  2.4 StrongPity Modules .................................................................................................................. 9
    2.4.1 List of Main modules ........................................................................................................... 9
    2.4.2 Service installer Module ................................................................................................... 9
    2.4.3 Data Exfiltration Module .................................................................................................. 11
    2.4.4 Data Packing Module ....................................................................................................... 13
  2.5 C2 Infrastructure .................................................................................................................... 13

3 REFERENCES .............................................................................................................................. 15

Table of Figures

Figure 1 – Malicious ISP Watering Hole Attack ............................................................................. 6
Figure 2 – Targeted Software ......................................................................................................... 7
Figure 3 – Unusually High Entropy PE Section ............................................................................ 8
Figure 4 – Examples of StrongPity Invalid Code Certificates .......................................................... 8
Figure 5 – StrongPity’s Main Modules ............................................................................................ 9
Figure 6 – Service Installer Options ............................................................................................... 10
Figure 7 – Service Registration ..................................................................................................... 10
Figure 8 – Executing Data Exfiltration Module .......................................................................... 11
Figure 9 – Data Stealer Module’s Name in Stack String ................................................................. 11
Figure 10 – C2 Exfiltration Infinite Loop ..................................................................................... 12
Figure 11 – Hardcoded User-agent String .................................................................................... 12
Figure 12 – HTTP Request for Data Exfiltration ......................................................................... 13
Figure 13 – Command and Control Domains .............................................................................. 14
Figure 14 – Common Command and Control URL Path ............................................................... 14

© Cysiv Inc, 2020. All rights reserved.
1 EXECUTIVE SUMMARY

Promethium is an Advanced Persistence Threat (APT) that has been active since 2012. However, technical reports about their operations were not published until 2016. Since then, many cyber campaigns related to espionage have been attributed to the group due to the tools and techniques being used.

Promethium’s main weapon is StrongPity spyware, which is usually used in targeted attacks. StrongPitty is distributed through spear phishing and watering hole attacks. However, the latter technique is the main attack vector. StrongPity can easily gain administrator privileges because the victim will give full permission to run the (trojanized) installer. This is a huge advantage of this type of attack, since the malware will not have to perform privilege escalation.

By analyzing different campaigns of Promethium APT, the Cysiv threat research team has identified three main techniques used to distribute StrongPity spyware:

1. Malicious Internet Service Provider (ISP)
2. Domain typosquating
3. Software downloading websites

StrongPity was used to target individuals in Turkey, Italy, Belgium, Western Europe, and was then expanded to other countries including France, Canada, Colombia, Russia, India, and Vietnam. In order to target a wider variety of victims, Promethium APT has trojanized many different software installers with StrongPity. The targeted software can be divided into three main categories:

1. Data compression, encryption and archiving tools
2. Internet tools
3. Windows utilities

Some trojanized installers with StrongPity will check for common anti-virus software before dropping the malicious modules. If an anti-virus process is detected, it will not drop any malicious files. The installers can also execute a Powershell command to add the directories used by StrongPity (including %TEMP%, %Windir%/System32, and %Windir%/SysWOW64) to the Windows Defender exclusions list and prevent sample submission.

Despite using different files names for different modules of StrongPity spyware in different campaigns, the Cysiv threat research team has been able to summarize the main modules of the spyware, which includes a service installer module, a data exfiltration module and a data packing module.

The StrongPity samples analyzed by the Cysiv threat research team connect to more than 50 domains. These domains are registered and used at different times. However, the pattern of domain names the group like to use is apparent.

Protection Provided by Cysiv:
© Cysiv Inc, 2020. All rights reserved.
Cysiv SOC-as-a-Service provides protection from a broad range of threats, including StrongPity spyware:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Threat hunting helps to identify suspicious activity and digital footprints that are indicative of an intrusion.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on endpoints, for users, and that can be monitored as part of the Cysiv service, will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that may already be deployed (or can be deployed by Cysiv) on servers and workloads, and that can be monitored as part of the Cysiv service, uses a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless malware. Additionally, it will monitor events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that may already be deployed (or can be deployed by Cysiv) and that can be monitored as part of the Cysiv service will detect malicious attachments and URLs, and are able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they're not being downloaded in the physical endpoint.
2 ANALYSIS

2.1 Overview

Promethium is an Advanced Persistence Threat (APT) that has been active since 2012. However, technical reports about their operations were not published until 2016. Since then, many cyber campaigns related to espionage have been attributed to the group because of the tools and techniques being used.

Promethium’s main weapon is StrongPity spyware, which is bundled into legitimate software installers. Over time, the group has added many different software and countries into their target list. However, the main modules of StrongPity spyware remain almost unchanged. This proves that StrongPity’s simple design is still working effectively despite the deployment of basic security controls and practices.

2.2 Attack Vectors

StrongPity spyware is usually used in targeted attacks and is distributed through spear phishing and watering hole attacks. However, the latter technique is the main attack vector. StrongPity can easily gain administrator privileges because the victim will give full permission to run the (trojanized) installer. This is a huge advantage of this type of attack, since the malware will not have to perform privilege escalation.

StrongPity has been used to target individuals in Turkey, Italy, Belgian, Western Europe, and has since been expanded to other countries such as France, Canada, Colombia, Russia, India, and Vietnam. In order to target a wider group of victims, Promethium APT has trojanized many different software installers with StrongPity (See section 2.3.1).

By analyzing different campaigns of Promethium APT, the Cysiv threat research team has identified three main techniques used to distribute StrongPity spyware:

1. Malicious Internet Service Provider (ISP)
2. Domain typosquatting
3. Software downloading websites

2.2.1 MALICIOUS INTERNET SERVICE PROVIDERS

Deploying a watering hole attack at an Internet Service Provider (ISP) level is one of the most stealthy way to target Internet users. In this case, the targeted individuals will be unknowingly redirected to a malicious download server by the malicious ISP when they try to download certain software (See Figure 1).
At the ISP level, any unencrypted traffic can be tampered. Therefore, redirection is possible when the website uses a non-HTTPS connection for downloads or supports HTTPS but does not restrict to HTTPS only.

### 2.2.2 DOMAIN TYPOSQUATING

Domain typosquatting has also been used to distribute StrongPity spyware. The attacker(s) simply register for a domain that looks similar to the legitimate the domain, which tricks the user into accessing the malicious domain instead of the benign one.

As an example, Promethium APT set up a domain name to target WinRAR users. More specifically, it registered the domain name `ralrab[.]com` to mimic the legitimate WinRAR distribution site `rarlab[.]com`.

### 2.2.3 SOFTWARE DOWNLOADING WEBSITES

Software aggregation and sharing sites are also a great target for watering hole attacks. In 2016, the group targeted the TrueCrypt application on the downloading website `tamin-dir[.]com` to redirect users to their malicious downloading website:

- `hxxp://www.true-crypt[.]com/download/TrueCrypt-Setup-7.1a.exe`
- `hxxp://true-crypt[.]com/files/TrueCrypt-7.2.exe`

This technique still works since many Internet users do not follow security practices when downloading the installing software.
2.3 Trojanized Installers

Most of the trojanized installers with StrongPity spyware have unusually high entropy and are signed with invalid digital certificates. When executed, the installers will start the installation of the benign software, but then will drop StrongPity’s three main components and steal data in the background. This section identifies the common characteristics of the trojanized installers.

2.3.1 TARGETED SOFTWARE

As mentioned, Promethium APT has trojanized many different software installers with StrongPity to expand its victims over time. Figure 2 is a non-exhaustive list of the software that has been targeted by Promethium APT.

![Figure 2 – Targeted Software]

<table>
<thead>
<tr>
<th>Data Compression, Encryption and Archiving Tools</th>
<th>Internet Tools</th>
<th>Windows Utilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>TrueCrypt</td>
<td>Internet Download Manager</td>
<td>CCleaner</td>
</tr>
<tr>
<td>WinRAR</td>
<td>Opera Browser</td>
<td>Driver Booster</td>
</tr>
<tr>
<td>7z</td>
<td>Firefox Browser</td>
<td>The VLC Media Player</td>
</tr>
<tr>
<td>VPNpro</td>
<td>Skype</td>
<td>Disk Drill</td>
</tr>
</tbody>
</table>

2.3.2 COMMON CHARACTERISTICS

All of the trojanized installers (and StrongPity modules) observed match the signature of a Microsoft Linker (14.0, Visual Studio 2015 14.0). This common characteristic among all modules over a couple of few years suggests that either only Promethium APT has access to the source code of StrongPity spyware or the group has developed a StrongPity builder for different targeted software.

Another common characteristic among all the trojanized installers is their unusually large and high entropy .rsrc section (See Figure 3). All the StrongPity’s modules are encrypted and stored in this section.
Finally, the trojanized installers are usually signed with invalid code signing certificates (Figure 4).

![Figure 4 – Examples of StrongPity Invalid Code Certificates](image)

Invalid certificates have been observed being reused for different trojanized installers that are built at almost the same time. The certificates are usually signed with the name of software companies but cannot be verified.

### 2.3.3 ANTI-VIRUS EVATION TECHNIQUES

Some StrongPity trojanized installers will check for common anti-virus software before dropping the malicious modules. If the anti-virus process is detected, it will not drop any malicious files. The installers can also execute a Powershell command to add the directories used by StrongPity (including %TEMP%, %Windir%/System32, and %Windir%/SysWOW64) to the Windows Defender exclusions list and prevent sample submission:

© Cysiv Inc, 2020. All rights reserved.
2.4 StrongPity Modules

2.4.1 LIST OF MAIN MODULES

Despite different files names being used for different modules of StrongPity spyware in different campaigns, Cysiv Threat Research team is able to summary three main modules of the spyware, which includes a service installer module, a data exfiltration module and a data packing module. The list of modules is shown in Figure 5.

Figure 5 – StrongPity’s Main Modules

<table>
<thead>
<tr>
<th>Module</th>
<th>Observed Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Installer Module</td>
<td>nvvscv.exe, netplviz.exe, services.exe, dusntask.exe, wvsvcs32.exe, rmaserv.exe, seceditr.exe.</td>
</tr>
<tr>
<td>Data Exfiltration Module</td>
<td>dcomx32.exe, IpOve32.exe, printoi32.exe, ngentask.exe, spoolcl.exe, printque.exe, winprint32.exe, sivsnui.exe, winslui32.exe.</td>
</tr>
<tr>
<td>Data Packing Module</td>
<td>evntwn32.xml, wiminit.xml, mssqlbserv.xml, sqlhostserv.xml, wintcsr.exe, spoolsrv32.exe, spools32.exe, winsys.exe, srvolpsm.exe.</td>
</tr>
</tbody>
</table>

The three modules will be dropped (in %TEMP%, %Windir%/System32, and %Windir%/SysWOW64) at the same time as dropping the benign installer, and only the service installer module will be started after the benign installer has started. The service installer will register to run as a service and start the data exfiltration module. The data exfiltration module will then start the data packing module and exfiltrate the packed data to its command and control server.

2.4.2 SERVICE INSTALLER MODULE

When executed with the option ‘help’, the service installer module will register itself to run as a service. The command line option comparison is shown in Figure 6.
As shown in Figure 7, the service will be registered to run in an independent process, with all access, and be started automatically by the service control manager during system start-up. This will ensure the module has all the access it needs to achieve its malicious goals.

When executed as a service, the module will start the data exfiltration module as shown in Figure 8 (i.e. C:\Windows\system32\winslui32.exe in this case). A small delay is also added before starting the new process to reduce the possibility of being noticed.
2.4.3 DATA EXFILTRATION MODULE

As noted earlier, the data exfiltration module will start the data packing module to collect data on the victim’s machine. The path to the data packing module is built at run time on the stack as shown in Figure 9. In this case, the path is %Temp%\ACB-D11C-335AAF\spools32.exe.

After the preparation steps, it will enter an infinite loop to find the packed data (prepared by the data packing module), and transfer them to the C2 server (Figure 10). A long sleep of 20 seconds is also added between the exfiltration steps to avoid consuming unusually high Internet bandwidth.
Inside the infinite loop, the module will build an HTTP header to communicate with the server. It starts by creating a WinHTTP-session with a hardcoded user-agent string as shown in Figure 11.

Figure 11 – Hardcoded User-agent String

The rest of the HTTP request is built as shown in Figure 12, which include the file name in the Content-Disposition header.
Figure 12 – HTTP Request for Data Exfiltration

The data will be transferred to the C2 server in the form of an HTTP POST request’s payload.

2.4.4 DATA PACKING MODULE

The data packing module is straightforward. It will search for files with the targeted extensions (such as .ppt, .pptx, .xls, .xlsx, .txt, .doc, .docx, .pdf, and .rtf). It will then compress the files into a temporary ZIP file and create .sft files for exfiltration. Note that this module is only started by the exfiltration module.

2.5 C2 Infrastructure

Promethium APT uses different domains for different campaigns for timespan. This can be a way to isolate different groups of victim’s data or to avoid detection (Old domains being backlisted).

The StrongPity samples analyzed by Cysiv Threat Research team connects to more than 50 domains as shown in Figure 13. These domains are registered and used at different times. However, we can see the pattern of domain names that the group like to use.

© Cysiv Inc, 2020. All rights reserved.
When communicating with their server, different StrongPity spyware variants will contact hardcoded URL paths. Therefore, there are not many URL paths used on the server side. The list of common command and control URL path of StrongPity spyware is shown in Figure 14. Note that this list is not exhaustive.

### Figure 14 – Command and Control Domains

<table>
<thead>
<tr>
<th>StrongPity’s Command and Control Domains</th>
<th>Common Command and Control URL Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>apn-state-upd2.com</td>
<td>/parse_ini_file.php</td>
</tr>
<tr>
<td>app-mx3-delivery.com</td>
<td>/ini.php</td>
</tr>
<tr>
<td>app-system2-update.com</td>
<td>/phpinfo.php</td>
</tr>
<tr>
<td>apt5-secure3-state.com</td>
<td>/s3s3sxxhxTuDSrkBQb88wE99Q.php</td>
</tr>
<tr>
<td>awe232-service-app.com</td>
<td>/kU2QLsNB6TzexJv5vGdunVXT.php</td>
</tr>
<tr>
<td>cdn2-state-upd.com</td>
<td>/p55C3xhxTuD5rkBQbB8wE99Q.php</td>
</tr>
<tr>
<td>cdn2-svr-state.com</td>
<td>/p5Pss34GvX21px0bz25vLqU.php</td>
</tr>
<tr>
<td>cdn2-system3-secrv.com</td>
<td>/p5pss34gvx21px0bz25vlu.php</td>
</tr>
<tr>
<td>dangerposedbyhaving.com</td>
<td>/goN9Z2In7mYQmN92dzX11CQL.php</td>
</tr>
<tr>
<td>dwn-balance.net</td>
<td></td>
</tr>
<tr>
<td>file3-netwk-system.com</td>
<td></td>
</tr>
<tr>
<td>fileservingpro.com</td>
<td></td>
</tr>
<tr>
<td>forwardyourenetwork.com</td>
<td></td>
</tr>
</tbody>
</table>
3 REFERENCES

Note: A comma-separated values (.csv) file of more IOCs is available at

cy4iv.com/forescout

© Cysiv Inc, 2020. All rights reserved.