CYSIV
A FORESCOUT COMPANY

Threat Report: StrongPity Spyware

August 7, 2020

Table of Contents

Table of Figures

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 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).

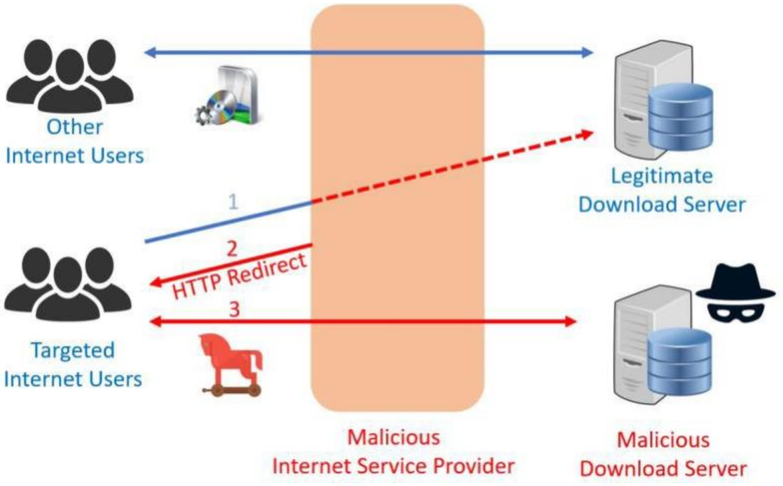
By analyzing different campaigns of Promethium APT, the Cysiv threat research team has identified three main techniques used to distribute StrongPity spyware:

1. Malicious Internet Service Provider (ISP)
2. Domain typosquating
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).

Figure 1 – Malicious ISP Watering Hole Attack



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

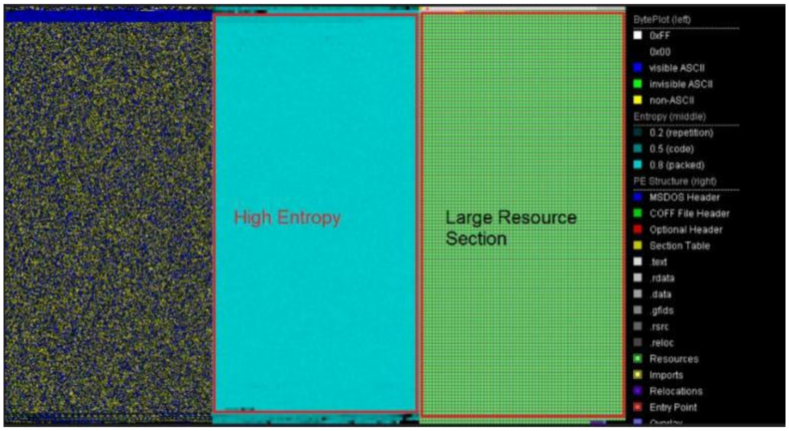
Data Compression, Encryption and Archiving Tools	Internet Tools	Windows Utilities
TrueCrypt WinRAR 7z VPNpro	Internet Donwload Manager Opera Browser Firefox Browser Skype	CCleaner Driver Booster The VLC Media Player Disk Drill DriverPack 5kPlayer Winbox SanDisk WinUtils

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.

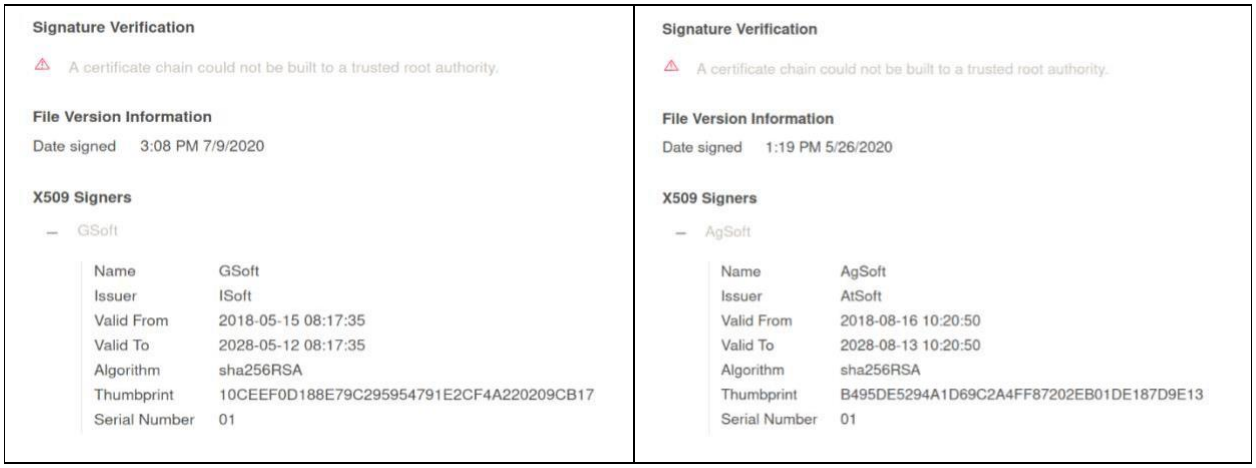
Another common characteristic among all the trojanized installers is their unusually large and high entropy .rsrc section (See Figure 3). All the StrongPity's modules are encrypted and stored in this section.

Figure 3 – Unusually High Entropy PE Section



Finally, the trojanized installers are usually signed with invalid code signing certificates (Figure 4).

Figure 4 – Examples of StrongPity Invalid Code Certificates



Signature Verification

⚠ A certificate chain could not be built to a trusted root authority.

File Version Information

Date signed 3:08 PM 7/9/2020

X509 Signers

– GSoft

Name	GSoft
Issuer	ISoft
Valid From	2018-05-15 08:17:35
Valid To	2028-05-12 08:17:35
Algorithm	sha256RSA
Thumbprint	10CEEF0D188E79C295954791E2CF4A220209CB17
Serial Number	01

Signature Verification

⚠ A certificate chain could not be built to a trusted root authority.

File Version Information

Date signed 1:19 PM 5/26/2020

X509 Signers

– AgSoft

Name	AgSoft
Issuer	AtSoft
Valid From	2018-08-16 10:20:50
Valid To	2028-08-13 10:20:50
Algorithm	sha256RSA
Thumbprint	B495DE5294A1D69C2A4FF87202EB01DE187D9E13
Serial Number	01

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:

```
powershell.exe Set-MpPreference -ExclusionPath ‘C:\Windows\System32’, ‘C:\Windows\SysWOW64’,
‘C:\Users\admin\AppData\Local\Temp’ -MAPSReporting 0 -DisableBehaviorMonitoring 1 -
SubmitSamplesConsent 2
```

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

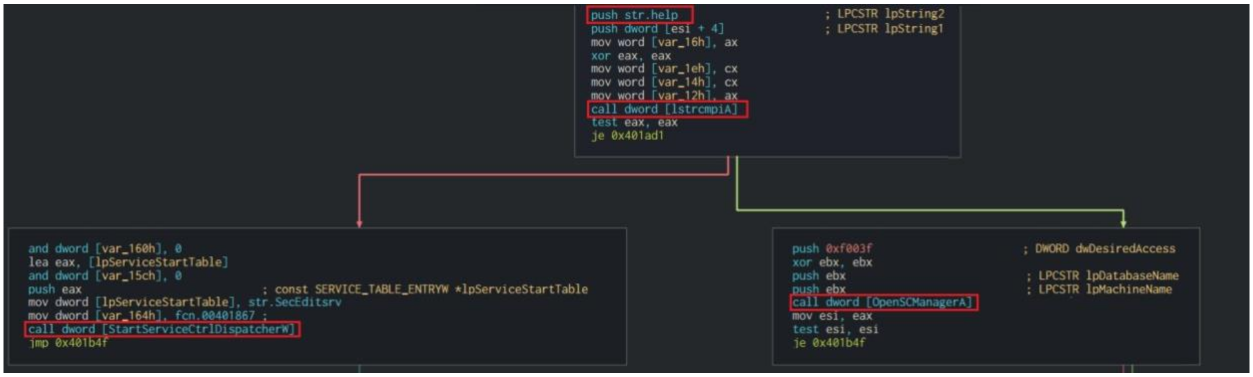
Module	Observed Names
Service Installer Module	nvvscv.exe, netplviz.exe, services.exe, dusntask.exe, wvsvcs32.exe, rmaserv.exe, seceditr.exe.
Data Exfiltration Module	dcomx32.exe, IpOve32.exe, printoi32.exe, ngentask.exe, spoolcl.exe, printque.exe, winprint32.exe, sivsnui.exe, winslui32.exe.
Data Packing Module	evntwn32.xml, wiminit.xml, mssqldbserv.xml, sqlhostserv.xml, wintcsr.exe, spoolsrv32.exe, spools32.exe, winsys.exe, srvolpsm.exe.

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.

Figure 6 – Service Installer Options



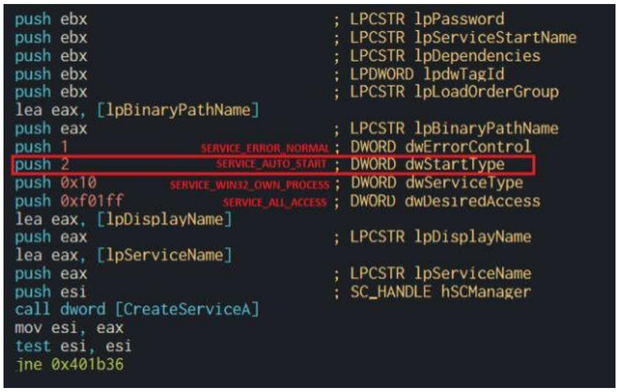
```
push str.help                        ; LPCSTR lpString2
push dword [esi + 4]                 ; LPCSTR lpString1
mov word [var_16h], ax
xor eax, eax
mov word [var_1eh], cx
mov word [var_14h], cx
mov word [var_12h], ax
call dword [lstrcmpiA]
test eax, eax
je 0x401ad1
```

```
and dword [var_160h], 0
lea eax, [lpServiceStartTable]
and dword [var_15ch], 0
push eax                         ; const SERVICE_TABLE_ENTRYW *lpServiceStartTable
mov dword [lpServiceStartTable], str.SecEditsrv
mov dword [var_164h], fcn.00401867 ;
call dword [StartServiceCtrlDispatcherW]
jmp 0x401b4f
```

```
push 0xf003f                     ; DWORD dwDesiredAccess
xor ebx, ebx
push ebx                         ; LPCSTR lpDatabaseName
push ebx                         ; LPCSTR lpMachineName
call dword [OpenSCManagerA]
mov esi, eax
test esi, esi
je 0x401b4f
```

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.

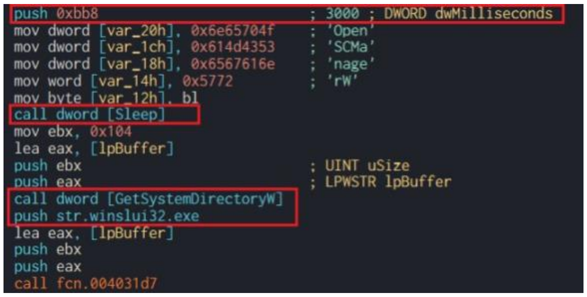
Figure 7 – Service Registration



```
push ebx                                       ; LPCSTR lpPassword
push ebx                                       ; LPCSTR lpServiceStartName
push ebx                                       ; LPCSTR lpDependencies
push ebx                                       ; LPDWORD lpdwTagId
push ebx                                       ; LPCSTR lpLoadOrderGroup
lea eax, [lpBinaryPathName]
push eax                                       ; LPCSTR lpBinaryPathName
push 1                   SERVICE_ERROR_NORMAL  ; DWORD dwErrorControl
push 2                     SERVICE_AUTO_START  ; DWORD dwStartType
push 0x10          SERVICE_WIN32_OWN_PROCESS   ; DWORD dwServiceType
push 0xf01ff                SERVICE_ALL_ACCESS ; DWORD dwDesiredAccess
lea eax, [lpDisplayName]
push eax                                       ; LPCSTR lpDisplayName
lea eax, [lpServiceName]
push eax                                       ; LPCSTR lpServiceName
push esi                                       ; SC_HANDLE hSCManager
call dword [CreateServiceA]
mov esi, eax
test esi, esi
jne 0x401b36
```

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.

Figure 8 – Executing Data Exfiltration Module

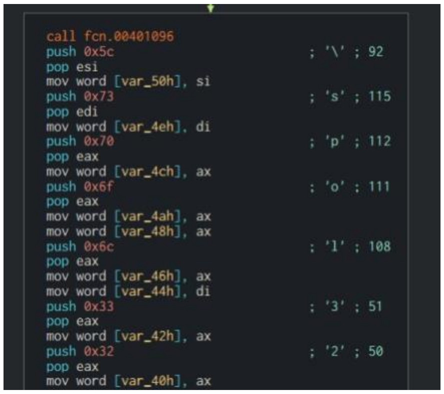


```
push 0xbb8                              ; 3000 ; DWORD dwMilliseconds
mov dword [var_20h], 0x6e65704f         ; 'Open'
mov dword [var_1ch], 0x614d4353         ; 'SCMa'
mov dword [var_18h], 0x6567616e         ; 'nage'
mov word [var_14h], 0x5772              ; 'rW'
mov byte [var_12h], bl
call dword [Sleep]
mov ebx, 0x104
lea eax, [lpBuffer]
push ebx                                ; UINT uSize
push eax                                ; LPWSTR lpBuffer
call dword [GetSystemDirectoryW]
push str.winslui32.exe
lea eax, [lpBuffer]
push ebx
push eax
call fcn.004031d7
```

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.

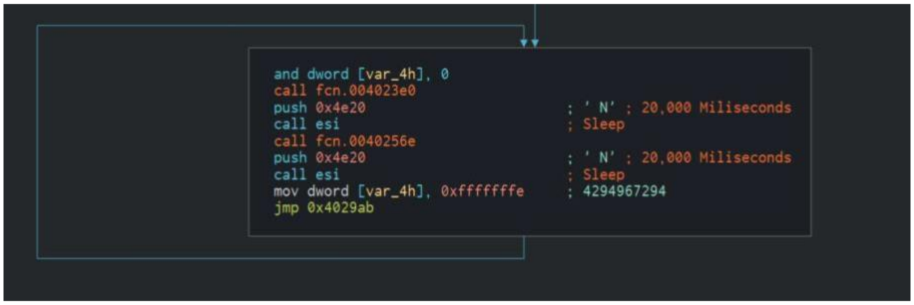
Figure 9 – Data Stealer Module's Name in Stack String



```
call fcn.00401096
push 0x5c                               ; '\' ; 92
pop esi
mov word [var_50h], si
push 0x73                               ; 's' ; 115
pop edi
mov word [var_4eh], di
push 0x70                               ; 'p' ; 112
pop eax
mov word [var_4ch], ax
push 0x6f                               ; 'o' ; 111
pop eax
mov word [var_4ah], ax
mov word [var_48h], ax
push 0x6c                               ; 'l' ; 108
pop eax
mov word [var_46h], ax
mov word [var_44h], di
push 0x33                               ; '3' ; 51
pop eax
mov word [var_42h], ax
push 0x32                               ; '2' ; 50
pop eax
mov word [var_40h], ax
```

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.

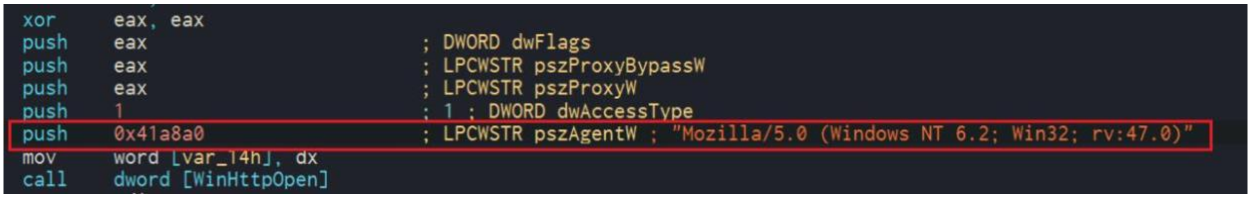
Figure 10 – C2 Exfiltration Infinite Loop



```
and dword [var_4h], 0
call fcn.004023e0
push 0x4e20                       ; ' N' : 20,000 Miliseconds
call esi                          ; Sleep
call fcn.0040256e
push 0x4e20                       ; ' N' : 20,000 Miliseconds
call esi                          ; Sleep
mov dword [var_4h], 0xfffffffe    ; 4294967294
jmp 0x4029ab
```

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.

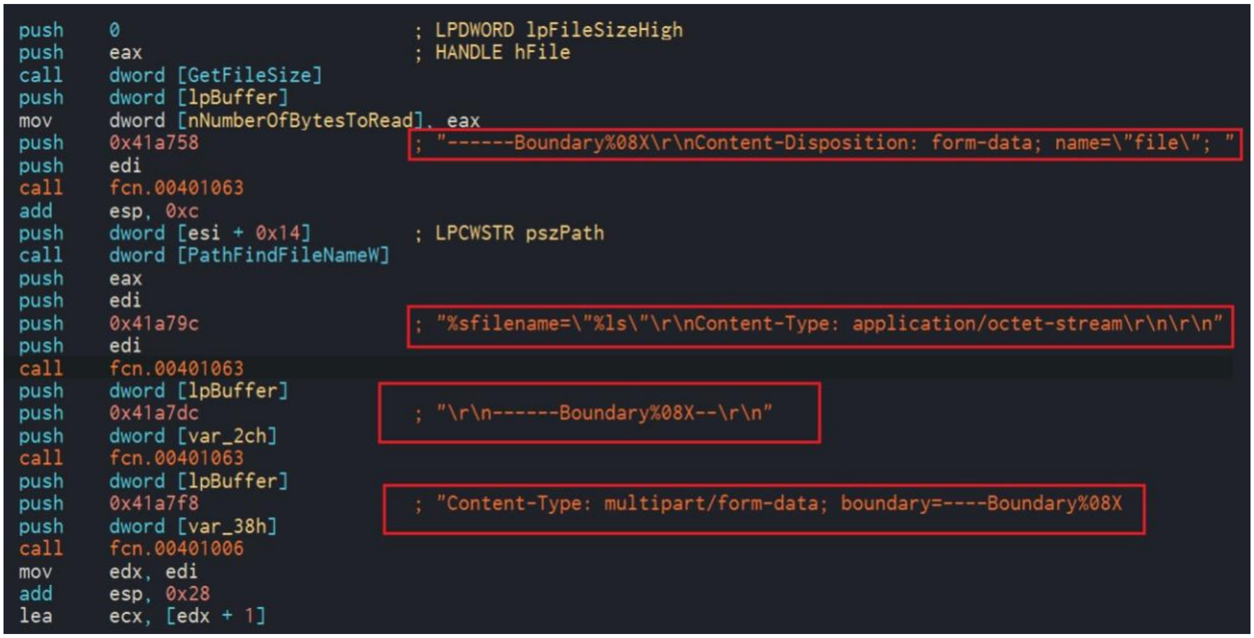
Figure 11 – Hardcoded User-agent String



```
xor     eax, eax
push    eax                         ; DWORD dwFlags
push    eax                         ; LPCWSTR pszProxyBypassW
push    eax                         ; LPCWSTR pszProxyW
push    1                           ; 1 ; DWORD dwAccessType
push    0x41a8a0                    ; LPCWSTR pszAgentW ; "Mozilla/5.0 (Windows NT 6.2; Win32; rv:47.0)"
mov     word [var_14h], dx
call    dword [WinHttpOpen]
```

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



```
push    0                          ; LPDWORD lpFileSizeHigh
push    eax                        ; HANDLE hFile
call    dword [GetFileSize]
push    dword [lpBuffer]
mov     dword [nNumberOfBytesToRead], eax
push    0x41a758                   ; "------Boundary%08X\r\nContent-Disposition: form-data; name=\"file\"; "
push    edi
call    fcn.00401063
add     esp, 0xc
push    dword [esi + 0x14]         ; LPCWSTR pszPath
call    dword [PathFindFileNameW]
push    eax
push    edi
push    0x41a79c                   ; "%sfilename=\"%ls\"\r\nContent-Type: application/octet-stream\r\n\r\n"
push    edi
call    fcn.00401063
push    dword [lpBuffer]
push    0x41a7dc                   ; "\r\n------Boundary%08X--\r\n"
push    dword [var_2ch]
call    fcn.00401063
push    dword [lpBuffer]
push    0x41a7f8                   ; "Content-Type: multipart/form-data; boundary=----Boundary%08X
push    dword [var_38h]
call    fcn.00401006
mov     edx, edi
add     esp, 0x28
lea     ecx, [edx + 1]
```

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 straight forward. 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 group 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 time. However, we can see the pattern of domain names that the group like to use.

Figure 13 – Command and Control Domains

StrongPity’s Command and Control Domains
apn-state-upd2.com
app-mx3-delivery.com
app-system2-update.com
apt5-secure3-state.com
awe232-service-app.com
cdn2-state-upd.com
cdn2-svr-state.com
cdn2-system3-secrv.com
dangerposedbyhaving.com
dwn-balance.net
file3-netwk-system.com
fileservingpro.com
forwardyournetwork.com
hostoperationsystems.com
hybirdcloudreportingsoftware.com
inhousesoftwaredevelopment.com
mailtransfersagents.com
mentiononecommon.com
ms21-app3-upload.com
ms2-cdn4-east-upd.com
ms6-upload-serv3.com
ms-sys-security.com
mx1-upd-systm.com
mx3-rewc-state.com
network-msx-system33.com
oem-sec4-mx32.com
safecopydisk.com
secretinformations.com
secure-upd21-app2.com
selectednewfile.com
service-net2-file.com
srv5-upd51-mx3-sec22.com
srv6-service-cdmcom
srv-cdn3-system.com
state-awe3-apt.com
svr-sec2-system.com
sys4-upload2-srv.com
syse-update-app4.com
system2-access-sec43.com
system2-cdn5-mx8.com
system6-mxe-ups3.com
system-upload-srv.com
upd2-app-state.com
upd32-secure-serv4.com
upd3-srv-system-app.com
upd56-state3-cdn7-mx8.com
upd8-sys2-apt.com
update5-sec3-system.com
upd-cdn6-state.com
upd-ms3-app-state.com
upd-ncx4-server.com
upd-network-ms2.com
upd-secure-srv1.com
updt-servc-app2.com

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 – Common Command and Control URL Path

StrongPity’s Common Command and Control URL Path
/parse_ini_file.php
/ini.php
/phpinfo.php
/s3s3sxhxTuDSrkBQb88wE99Q.php
/kU2QLsNB6TzexJv5vGdunVXT.php
/p55C3xhxTuD5rkBQbB8wE99Q.php
/p5Pss34GvX21pxO0bz25vLqU.php
/p5pss34gvx21pxo0bz25vlqu.php
/goN9Z2In7mYQmN92dzX11CQL.php

3 REFERENCES

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

```
02d68d2a9b62d1fd79c80e7c01182d18966a8fccc07d997b0f4c3ef71e87910f
05be705bfc38c5daff3e1050d3b1424127f3eb555e185cf0bc93cc4a36fe306f
0713eb6b1f49b3dab0f6000a005f9376bf5b91480d2fe69f77df97fe66c89c7d
0db11972e8b3be2a954bb017a4a9d01758167badce14f5b919db8d2eed16b5eb
0ee93b67b482a029a98d9b8c089d37320c047b99bb59087ccbadc05a1396b384
11849a6fcb76267676532422db4e9bf4f5c8c525fea0d950f844736bedb8b53e
12e670dc36ac50e86a58f759fa4a5de25e574227a19e1942aaa788c82540a910
13ace63b9e6524cdc0932767bde4a296d83f05d2e5679876dffb75a1a0ffc00b
158e4057f3d2751cf110c5924f289e5b45348f037b3931b9695d3ba045026b4e
17adbb68c3410d3f1c4c19b1808149e74148839f1c082c3011bff86ddb71acb4
1af0958f8590b626bedfcd1972cd3ea49d9576db86f1e768e5520f9615d01a19
211aae5346741680cb921d73e2833368cd0f0cc36e15b16115599554dcb2386d
2311cf291d0b759df354b050107f153aec8b707321978783efa493e934e5270d
24e8f4917bb3cf7d6fd91fc1c95e978ea75a0e6da9033911e48b0fda94be62af
2a7898573bd8be121eda249e7521efd2d599354d51fabae7edafef9d60dae8b1
2b62a469fa9737dabc52840a741a7d71c86c74bd6909c30cb481e2d66e0df75e
2c84f3d64d4d5dd1bb45aca5c411d64a12fd615d60fed9912349d84dc4063faa
2ed06fc1d1f9447fa7473ef6177eb2112e8f200765ea7aa0e6b63a87a0bbe4ee
2ee74ceaa5964cf223aefb3cf4e0c25ea96c7d4bc0eba48439716e763d2f3837
3099f3fd6a1463c4176daae7d76c4d1754993ff5aff74847eeb020f18f5bc8b4
333a2f4347ecfdb3ab988e152ca59cc510a4b2ec480f545d4b4c1f2fa8cc0ebd
35f03cb2dbc71b0450a8eeea0f379e22e2371cc78f956a8d98fa75a576ab5638
39cf2459a85f9b8bcc81233964e05dec3f5ec9e8de74329f995c6a0cc8a8db36
3cb36e3c96b10b1265d6b34f1c7f8a64fb7826dbb1a49a38ddfadfc86defb91f
3e58d7efc5e03bd06f227041e5c73f4ecfa5e35ca8419a9ff8b8571eafd34e48
3feb6ecbc3b5f4ef64cf974fc117e58ac750188c483c488dd5b5970263bfdb0e
418203a531ceb1f08a21b354bc0d3bf8f157c76b521495c29639d7bffa416b38
4282ac2c4b38f2fa79b3f77f9af80053befb69634f8e93d9e1941a600ae08857
444fb297df499527c757ff16cb15211ebaca3054c143f6df6a7cb8a0d69b04ec
49bb248813eb4eaadadde62146fece2012b7ca3378fa9759aeda8f960a4bd8e4
4e4ba22dd01939ce4556bbdceedd1db548740b8484e29bbd63f44faaddd83697
5190c4fbddb2bfd08ce4a11714ec54dcaf57978f6193720c5b2c7127ef2c5f1f
53d85d8c4ee63eca18604bc5db5f1ad732c789c18c03e1ef5462a1364aba1da1
55b0bc3b61ee76561ffaa1323fd20a9522e786bfa5eadbba621582ad529ff9e1
582e4c8e421bdd44693b7b4af86a97b282909399f166d1cb8241c237ba93ee60
58787795d74588a8d4ab6db2eccd296ddebb9b9b645465f46f44f7e88be09169
5cb8f86e03a544531d972e132c81d6785b66dd1b15b6c35a0a04fd83a8bed695
61f8dc6d618572a86bd0b646d16186bb6b0fff970947a7df754add4f65ec8625
644a69d58817a308865782fab967288cfd1cc0dae8aa34f465ee9b30068f8331
64a448ee194fe58c8c212faa4fbe737f8088ef387cc4551a0f1d86e9d4bdab02
6684c2348d205962d41977b2db6263733809b635cdc039447373c34e04d6bc20
68e23ca117e410b70a77d015154d5ec94735dd57a691507089ac18258bb1424a
69c1c79f4c8c962449e949de1b0ce30eab0e0c112045bdd98596848aa33f7256
6b0a28fe1954ae41e17ffd6b83a2ac7112cc98b64ba6b2a05448d200b42bb2dc
6d4af9f7e14e1ae7f871cd0bcdd87927cde8d236fd9d37e76554729abe3e31e4
70f92d1fedd5412ad3aee7f98cad25487af8407e407003701b240235a9b1fb6f
738cef8c1b3d7d0b583e931855509068cba3ab40f5527a4f4dbef4eb0b547b80
783b3c61a4069f0325f3560ab9664ff5fb381f37b08a3d4eb4866ba6bc194135
7a32367033d635ee882b06d98534fc8609b30fdbd7fc1de700493875fbb3089f
7c195b85528b3ed75672fbcea0d32a2f45d541cf8c71e855b03d6266a8facdc0
80ad6598f6e0b7c2b7258cbb69aa782dbcac308ca3d9d451b9bb5290b943a58f
835a545fe93bfa75931079ef36169bfc56906f74b9b9862848ff79534b33f416
84942df440c892c1e63aff41d9fe4694ea4b8a9102c62faf07c4510671abef13
89cb2564137e7816bf3b6a2022263f70301fe7b7f5a0f76073fbd0757fe3cf43
8e3993583cd2506ccbac4b247949ddee7d6971432576a0f9c485f9f0942054ae
904d237729d99a5eacc6b9721ed6d4914f303131cc855ead12b21b0b9c8d3332
92ff23ab81cc20c4916441547745f336cf612c21a049cdcbb01f11d83a40979e
9ce65cced9949cef6b69f86542533e653b91ce7d43cb6b51e8ae402b6dadf651
a1ce1b78cc1a9d6092b086f2d0796cde519033ec0935d9cecdea86b6cda87882
a34e636625cd9468c2802a1a3d9ba5c2ab611e0f6f5b1b4f17ad0151f63173e4
a5465100546468c8d5c1d59206d68f1b81853788ffe129aba8e96e0ff4e973d4
a6298a1b8c9844764c731327bb1daa7abd50cd85b9f5556e38bd5c88b8184cc4
a97702b25fea7863bff4a1f37b5e5a4733f2772f9e0cb55e73956acaddf53ab1
ac527beb0459f6b0d22673b2a2e6cad3e289df894bb9f28dd0ece34dff64fe5e
ae41ba7b4728a6322660443273d7ea6e50c6f804a7d726d0439fac956c7923e7
b06ab1f3abf8262f32c3deab9d344d241e4203235043fe996cb499ed2fdf17c4
b1446718a8dc2a4d97d0d2758149b80d761740a0bb4b6c758b92e3069802c732
b1916e7de11e87fa45c222d0532955e781f6695ae0ee15775894d3b3aa72ba98
b4548a933d5a59d096d75ad4c6aec1046017a62ca2a1d59edd2d97d760dca1eb
bac8489de573f614d988097e9eae53ffc2eb4e7dcb0e68c349f549a26d2130a8
bd21bf716c3bdff02f1eebae207a1a4e07c5a7f11565b3c3aabff9d925330dcf
c00c6d8052bdc047089b2d4827c3f07d88025263bb47e79fb591dc39eaed275d
c2c020dc44cf10072bc37f2912c970d7e74707ea0fe7612ce989ce2564a0dc4f
c34b9a5d82e10fa6ebfb010a01e42cd288e90c59e4f3984116ecb4f5428fbdf1
c72bf8537fc189b81855666d7f59ad8e24011c735921a15932275757a485e7a4
c790e1916a475fbc18e7f239acf0d9399234cf2160529ba25ab44179674d549a
c94e52455826c63a8800e6a66d72db467e1266f3b06aabbaad14c0d7463ee266
cac5c0da0b4495a1dee326e4259fb8bcdecb162a780d0d215ad33e751ebbff34
d0ee66f8be0ed721774391365604de70dda4751213a667812e4c4a661f71559d
d2426af686785808b956450388c6be912a2402d074d6c9d5786f49efae66c5d7
d40a3503a960663187a83f560e94563cd11606a610a4b176b0ac065af037f175
d63533bb200525a0a88a68c592c8d4f534fcf83b0acf8ec6be24b7059b0352ae
d8d0c3854c54e2bacb40ead54d94268dda6ea6aef1ac1f78b8d10b990a4441a2
db3398c3c78f52164266cbd06959e00dc556cfbd7599c7a80fbd3fdce02ee46e
dbf3e5bb9b7b5806d831617fbeed088d56fc2f5794a833d24eff96c165ba417b
dd812ba2bc5f441d8a9594443040f8fea7e3f91bdf1dd1968bbbbc7747e0bc68
e2cd8fd988a9a08f4bd73d7343ae54e68ee2a0a4728277792115edc86900e899
e4135bfeda1de00c3834f7782b77fdb2811f5d07fc60f643553426d9e45b664c
e5073d8534fbf2a2a8893197700b93b92d91338a2f18ae4ab1f2065810f33650
e7023aa6b2694a3bb165432b155684d0d917dba94640a607725f95c9a04c44a4
e843af007ac3f58e26d5427e537cdbddf33d118c79dfed831eee1ffcce474569
e964182ccaea84106573bb7b988b321b6721eca4217bd59b2f2807eee9220ce5
ea750383d3af605e5cdf2647b9cd30886aa8a428b3bcf6bc96cc178c9afa78d9
ed2aa3272db6eebedcabbb3c61cb699e6ec5d91b4297b8a6186a03f5b4999a80
eeed4d7c85b28f0f13d0eebf9c8606c7dafc14a068f1cdcb71721022c8529fe0
f19444a540e46bedec32059c8b501f1289b8c1d9ab5d81a0d1c01ad3301ef802
f1d0fa6ab4159344c62f9544411677270a0883b64f857a5eac087d5eb40d4fd4
f92dee20a0e72ee714d1508023a6684a07503712eefe5e83ee380ee01b9f54bb
fa71584f27f5eacca9f3d5644fd06ccebcc14b8394efeaccd38259f8382c26e5
fad11a279c6fe195f8110702f962c5296015344da17919b361f73f7f504063ca
fcfd34f99b0a5f4bb91c0d6eaa9b2fdcc3bf9b3dd594213a389a056828a537c1
ff8b71b7e9b320d272babb15324b7417f182313f71c4af0b9961424a12154b66
```