SectorM04 Targeting Singapore – An Analysis

threatrecon.nshc.net/2019/03/19/sectorm04-targeting-singapore-custom-malware-analysis/

Overview

On or around June 27, 2018, personal particulars of almost 1.5 million people was exfiltrated from a SingHealth database in Singapore where information on patients was stored. Multiple pieces and types of malware was used in this attack which took place over almost a year [1].

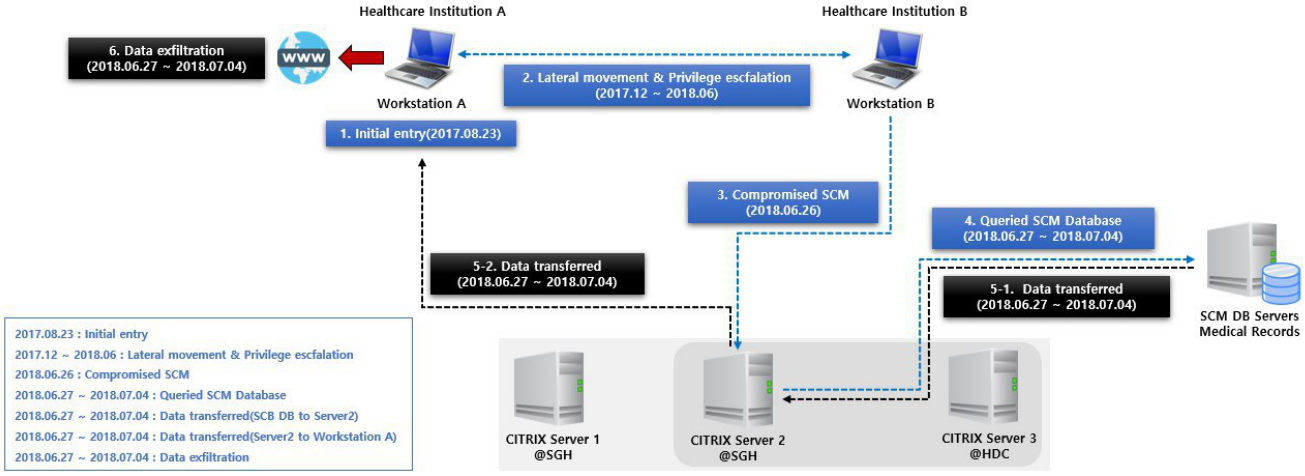

Illustration using details from p.53 of the COI report

On 6th March, Symantec released a blog article [2] linking several pieces of malware and a threat group which we will be tracking as SectorM04 to Singapore's SingHealth breach last year. One such artifact we found an exact match on was the DLL Shellcode Loader which was referred to as Trojan.Vcrodat that is one of the files dropped as something which has characteristics of the PlugX RAT. The PlugX RAT is a RAT which has been used by multiple threat groups, including one which was reported to have interests in the healthcare sector [3].

Decoy (e9b12791e0ab3a952fa09afd29e5a1416abd917edf5c913af7573adf8ccc39b0)

The dropper for that file was in the form of a decoy executable/document and named as "PositionRequirement-SeniorCivilEngineer.doc.exe". Opening this results in the Word document below being opened, and everything will seem normal to the victim.

Position: Senior Civil Engineering Technician

Location: Colombo, Sri Lanka

JOB SUMMARY:

Provide engineering assistance and support in the area of construction plans, specifications, project designs, surveying, material testing, construction inspection, and bridge safety inspection.

Essential Duties and Responsibilities

The following duties are normal for this position. These duties are not to be construed as exclusive or all-inclusive. Other duties may be required and assigned

- Conduct field surveys to gather data for construction plans.
- Design construction plans, specifications and estimates using design software.
- Assist in the preparation of reports, letters and other documents regarding the design or pending construction of highway improvement projects (i.e. study reports, wetland projects).
- Prepare preliminary project designs such as horizontal and vertical alignment, intersection layouts and turn lane areas.
- Provide preliminary and construction staking/surveying for all elements of highway/bridge construction.
- Inspect and document construction activities, quantities, and all material quality needed on projects. Assist with/Conduct compliance tests for soils, aggregates, bituminous, concrete, and other.
- Independently monitor and inspect the progress and construction methods to ensure projects meet specifications as well as local/state/federal guidelines, standards, and laws.

Decoy document that is opened after executing the malware

However, this is actually a trick because the malware uses a ".docx.exe" extension. The actual executable drops other files in the same folder – a legitimate signed executable, a malicious DLL file which abuses the DLL search order [4] from the executable, a compressed shellcode file, a simple batch script (a.bat) to clear its tracks, and a normal Word document. The executable then executes the normal Word document, the batch script, and drops the remaining three files and executes the legitimate signed executable.

a.bat – a simple batch script to hide the tracks of the original EXE

```
:Repeat
del [filepath]\filename.docx.exe
if exist [filepath]\filename.docx.exe goto Repeat
```

If this was the RAT used for the initial infection, then it seems to reinforce the theory that one likely initial infection vector was via spear phishing using a link or an archived file [1]. This is because using an exploit to automatically run this dropper would not make sense as the malware also automatically opens a benign Word document which would arouse suspicion if it opened by itself.

PlugX Trinity

Those remaining three files are actually the three files in what other researchers have dubbed the PlugX Trinity [5] – a legitimate signed executable, a loader DLL, and a shellcode file.

In this example, while the legitimate signed executable was a file named adobe.exe it was actually an application from ESET. However, the attacker uses DLL side loading, and this “adobe.exe” file tries to load MSVCR110.dll which is a legitimate system DLL. But because of the way the DLL search order works, the system tries to find MSVCR110.dll from the directory from which the application loaded first, thus loading the attacker’s version of MSVCR110.dll.

MSVCR110.dll is a tiny dll made up of exported functions which the real MSVCR110.dll should have. These external functions simply jump to the MSVCR90.dll when called, except for the “__crtGetShowWindowMode” function which calls the malicious function. The malicious function will proceed to read the MSVCR110.dat shellcode file into memory and decompress the buffer using RtlDecompressBuffer under the COMPRESSION_FORMAT_LZNT1 scheme, a method seen since early days of the PlugX RAT [6], and further unpack the shellcode. Throughout the unpacking process, it makes use of its Process Environment Block (PEB) to parse the PEB_LDR_DATA structure for getting addresses of functions and libraries it wants to use.

When starting, this malware uses the Global mutex named “eeclnt”. It will run another copy of itself with the arguments “258”, and this copy will run %windir%\system32\msiexec.exe as it disables WOW64 redirection.

The created msiexec.exe will be started with the flags 0x434 which among other things starts the process in a suspended mode and command line arguments “259”, then performs process injection so that the malware is running as msiexec.exe.

Persistence

In order to persist on a system, the malware makes use of %APPDATA%\Windows folder, setting the folder attributes to HIDDEN | SYSTEM and moving MSVCR110.dll, MSVCR110.dat, and eeclnt.exe (renamed from adobe.exe) there. It stores this new location of the shellcode file (MSVCR110.dat) in an environment variable “%UI00%” and the location of the DLL file (MSVCR110.dll) in an environment variable “%UI01%”.
There are two persistence mechanisms it makes use of:

1. Service with service name and display name set to “WanServer”, which starts %APPDATA%\Windows\eeclnt.exe with the command line arguments “260”. The service description used is “Network for this computer. If this service is stopped, these functions will be unavailable.”, which is a generic sounding but unique description for this malicious service.
2. If the service failed to be created, most likely due to insufficient privileges, then the malware would make use of the standard run registry key located at HKCU\Software\Microsoft\Windows\CurrentVersion\Run with key “eeclnt” and value %APPDATA%\Windows\eeclnt.exe with the command line arguments “260”.

Command Line	Description
NULL	Re-run with arguments “258” and continue
“258” / “260”	Run %windir%\system32\msiexec.exe with arguments “259” or “261” respectively in suspended mode and inject itself into it
“259”	Create persistence via service / run registry key and run itself as “eeclnt.exe” with arguments “260”
“261”	Run normally, including C2 communications.

C2 Beacon

The malware beacons using a legitimate HTTPS POST on port 443 to “/login.asp?id=%d” where %d is the victim identifier using the user-agent “User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.0)” via WinINet.dll’s HttpSendRequestA. If the configuration uses a different port, then the request is done via HTTP.

Hooking

The malware manually sets inline hooks on SspiCli.dll’s AcquireCredentialsHandleA function if running on Windows 10. AcquireCredentialsHandleA is actually a function normally called from secur32.dll, which then forwards the API call to SspiCli.dll. Before performing the actual function, the inline hook will use the process token from explorer.exe and perform ImpersonateLoggedOnUser() with that token, which is a trick we are seeing for the first time and seems to be for UAC bypass.
The malware also manually sets inline hooks on WSs2_32.dll’s closesocket and shutdown functions. Before performing the closesocket function, the inline hook will perform “setsockopt(socket, SOL_SOCKET, SO_DONTLINGER, 0, 4)” and on shutdown, the inline hook will simply return from the function instead.

Information Collected

The malware mainly collects the following information from the system automatically:

- Major, minor, and build OS versions
- NetBIOS Name
- MAC Address
- Logged on user name

Other PlugX Capabilities

Similar to previous PlugX variants [7], this version zeroes out its entire PE header (without that false “XV” header), together with other certain other PE sections we presume the attacker did not want others to see.
Finally, besides this technical analysis, it is important to remember that PlugX in general has reverse shell capabilities and typically has additional modules which might be either decrypted or downloaded as shellcode [8].

Summary

While we cannot be sure of the SectorM04’s motives, healthcare data is information that has a lot of potential for intelligence gathering with the most obvious being used for blackmail. They have shown their willingness, ability, and patience to compromise their targets, of which Singapore appears to be one of the bigger ones. As is the case for many nation state threat actor groups, it is important to remember that cyber is only one part of an intelligence operation.

ATT&CK Matrix

Initial Access
Spearphishing Attachment
Valid Accounts

Execution
Command-Line Interface
PowerShell
Regsvr32
Rundll32
Scripting
User Execution

Persistence
AppInit DLLs
DLL Search Order Hijacking
Office Application Startup
Valid Accounts

Privilege Escalation
AppInit DLLs
DLL Search Order Hijacking
Exploitation for Privilege Escalation
Valid Accounts

Defense Evasion
DLL Side-Loading
Indicator Removal from Tools
Indicator Removal on Host
Process Hollowing
Regsvr32

Rundll32
Scripting
Valid Accounts

Credential Access
Credential Dumping
Credentials in Files

Lateral Movement
Pass the Ticket
Remote Desktop Protocol
Remote File Copy

Collection
Data Staged

Command and Control
Remote File Copy

Exfiltration
Exfiltration over Command and Control Channel

Indicators of Compromise (IoCs)

PlugX Trinity Hashes (SHA-256)

PlugX RAT Full Dropper
e9b12791e0ab3a952fa09afd29e5a1416abd917edf5c913af7573adf8ccc39b0

PlugX Trinity – Legitimate signed executables
fafb6ffd3ffcf414b702354f62a5216351af4566ed61ece7784846a6938bb8d9
36d76999e9090c99fae2388cd3476134464807fc597f67c60eebc76e32339683

PlugX Trinity – Malicious DLLs which are used to abuse search order
CACEA09B3A5839B0A158F49B4EFEC2A698DB8688F57A92CBA61F287A1619833E
ED3CD71EACA603A00E4C0804DC34D84DC38C6C1E1C1F43AF0568FB162C44C995
3B86CF2DEB6524D556AB0109B39A31AEDE3D0ACE423C94FD72DEFD6AB592A3AB
D784A12FEC628860433C28CAA353BB52923F39D072437393629039FA4B2EC8AD
6e874ac92c7061300b402dc616a1095fa7d13c8a18c8a3ea5b30ffa832a7372c

PlugX Trinity – Shellcode files
2201C3AC955148A078D366DC1E9F552FCA4A872756D3B6DA93494CDE8D5DECD5
5664334F2DE563B9F8978B7E33AED4526F96D6D9751F1204D7FBBF659C4F0F7B

Other Hashes (SHA-256)

Another RAT Used

b2b2e900aa2e96ff44610032063012aa0435a47a5b416c384bd6e4e58a048ac9
c83651940e90fd315f29fa878e96b9e1f624c840c09c187b376cffdd4c7dcd79
6a633b83987dc01ec30d07b56e8a8b632dcb8ad40602e7036648cd70cdfb9fde
9c2a0f30d49b70a9e81461c91e26ede52b9b65da4d44b7f81299914497203f29
552cc8f42953ece5f69cd8c75dd9af3c059d10327ac6b75e4922f01572d4b7b7

Others

9d9a6337c486738edf4e5d1790c023ba172ce9b039df1b7b9720ed4c4c9ade90
93c9310f3984d96f53f226f5177918c4ca78b2070d5843f08d2cf351e8c239d5
dda22de8ad7d807cdac8c269b7e3b35a3021dcbff722b3d333f2a12d45d9908d
f562e9270098851dc716e3f17dbacc7f9e2f98f03ec5f1242b341baf1f7d544c
a196dfe4ef7d422aadf1709b12511ae82cb96aad030422b00a9c91fb60a12f17

Network information

Domains

api[.]edu-us[.]tk
api[.]officeonlinetool[.]com
news[.]singmicrosoft[.]ga
api[.]micsoftoffice[.]ga

IP Addresses

195[.]20[.]45[.]94
64[.]20[.]227[.]134
50[.]63[.]202[.]51
192[.]71[.]247[.]131
158[.]255[.]4[.]177

References

[1] https://www.mci.gov.sg/coireport
[2] https://www.symantec.com/blogs/threat-intelligence/whitefly-espionage-singapore
[3] https://www.kaspersky.com/about/press-releases/2018_chinese-speaking-apt-actor-caught-spying-on-pharmaceutical-organizations
[4] https://docs.microsoft.com/en-us/windows/desktop/dlls/dynamic-link-library-search-order#standard-search-order-for-desktop-applications
[5] https://citizenlab.ca/2012/09/human-rights-groups-targeted-by-plugx-rat/
[6] https://sophosnews.files.wordpress.com/2013/07/sophosszappanosplugxrevisitedintroducingsmoaler-rev1.pdf
[7] https://unit42.paloaltonetworks.com/unit42-paranoid-plugx/
[8] https://www.fortinet.com/blog/threat-research/deep-analysis-of-new-poison-ivy-plugx-variant-part-ii.html