SUPPLY CHAIN ATTACKS

THREATS TARGETING SERVICE PROVIDERS AND DESIGN OFFICES

Version 1.0

October 7th 2019

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Table of contents

1 Introduction

This document aims at warning about a cyber threat targeting service providers and design offices. Attackers are compromising these enterprise networks in order to access data and eventually the networks of their clients.
Information provided in this report is based on ANSSI's investigations following incident response activities. At this point, analysis suggests two waves of attacks separated in time and without technical evidence of a link between them. The first wave uses mainly the **PlugX** malware. The second wave relies on legitimate tools and credentials theft.
This document focuses on the second and most recent wave and the intrusion set[1] involved in it. Appendix only focuses on the **PlugX** malware (chapter 6).

2 Attack chain

2.1 Initial access

To gain initial foothold on targeted networks, the attackers exploit vulnerabilities on low-secured services exposed on the Internet, discovered through scanning with tools like **Acunetix**. Other methods may also be used such as phishing emails or usage of leaked credentials.

2.2 Access and persistence

To access the targeted networks after initial compromise, the attackers use legitimate VPN credentials that have probably been stolen on the victim's network.
The attackers may use other methods such as installed RATs (Remote Access Tool) or other backdoors like webshells, as demonstrated during former intrusions using **PlugX** malwares.

2.3 Privilege escalation

In order to acquire higher privileges on victim's machines, the attackers use legitimate tools such as **ProcDump** or **Certmig** (see section 3.2). Administrator accounts with a naming pattern incoherent with the usual patterns used by the victims have been observed on targeted networks (for instance an account named « `aaaa` »).

2.4 Lateral movement

RDP connections with stolen credentials are mainly used by the attackers to move inside the compromised network, as well as **Netscan** commands and **WMIExec** scripts.

2.5 Objectives

The first objective of the attackers seem to be the understanding of the network configuration and its external authenticated connections to clients.
After such information is acquired, the attackers move to the client network in order to gather relevant information. This information can be exfiltrated through the service provider or the client network.

[1] Characteristic tools, tactics, techniques and procedures (TTPs) used by one or several malicious actors accross one or several attack campaigns. It can be seen as an identity card of a threat which should not be confused with an attacker or group of attackers linked to a broader concept involving individuals and physical organisations.

2.6 Operational security

Even if the sophistication of the tools used by the attackers is quite low, they are well organised in the deletion and the deactivation of all activity logs on devices they visit.
Incoming connections of the attackers are anonymized through IP addresses belonging to VPN providers or TOR network.

3 Tools and malwares

3.1 Custom malware

In addition to all legitimate tools described below, the attackers use a custom piece of malware they may have developped.
This custom malware is designed to monitor the web browsers of a victim. This enables the gathering of credentials and session cookies. This malware communicates with a C2 server through HTTP or HTTPS.

3.2 Legitimate tools

The attackers have used the following legitimate tools:

- **ProcDump**: command-line tool used to monitor a running process and dump memory depending on custom criteria. The attackers use this tool to dump the LSASS process to gather WINDOWS credentials hashes;
- **CertMig**: command-line tool used to import and export certificates on a machine. The attackers use this tool to gather credentials used for VPN authentication to the clients' networks;
- **WMIExec.vbs**: tool used to remotely administrate a machine in *VBScript* with functionalities similar to **SysInternals PsExec**;
- **rar.exe**: command-line version of the file compression utility WINRAR. The attackers use this tool to compress, protect and split both exfiltrated data and imported toolset;
- **MimiKatz**: tool used for diverse actions on a WINDOWS system such as injection of libraries, process tampering and credential dumping;
- **Netscan**: tool used to scan IPv4/IPv6 networks and remotely execute PowerShell commands.

4 Detection methods for these attackers

In observed incidents, attackers have mainly used legitimate credentials and tools. IOC-based detection is therefore unefficient in this case.
The following rules do not give a full certainty on the attackers presence on an information system but matching circumstances should be investigated as a potential compromise.

4.1 VPN connections

4.1.1 Source of connection

The attackers mainly rely on commercial VPN services as well as the TOR network to anonymize their incoming connections.
In most cases, IP addresses of VPN clients have Whois records linked to popular commercial VPN services used for web navigation (HTTP/HTTPS) and emails (SMTP/SMTPS).

However, users connecting to a company VPN through a commercial VPN exit node or a TOR node is an anomaly.

Detection rule: look for incoming connections in VPN or VDI logs with a source which is an exit node in the following table. This list is not comprehensive.

IP addresses				
45.41.134.0/24	45.41.136.0/24	45.41.144.0/24	45.41.145.0/24	45.41.147.0/24
45.41.180.0/24	45.56.136.0/24	45.56.140.0/24	45.56.141.0/24	45.56.142.0/24
45.56.143.0/24	45.56.146.0/24	45.56.148.0/24	45.56.149.0/24	45.56.150.0/24
45.56.151.0/24	45.56.152.0/24	45.56.153.0/24	45.56.154.0/24	45.56.155.0/24
45.56.156.0/24	45.56.157.0/24	45.56.158.0/24	45.56.183.0/24	46.244.28.0/24
64.64.108.0/24	64.64.123.0/24	85.203.23.0/24	104.143.84.0/24	104.143.92.0/24
104.143.95.0/24	104.194.203.0/24	104.194.218.0/24	104.194.220.0/24	104.238.45.0/24
104.238.51.0/24	104.238.58.0/24	104.238.59.0/24	104.238.62.0/24	104.37.30.0/24
104.37.31.0/24	157.97.121.0/24	173.239.195.0/24	173.239.197.0/24	173.239.198.0/24
173.239.199.0/24	173.239.207.0/24	173.244.55.0/24	185.198.240.0/24	191.101.252.0/24

4.1.2 MAC address of the attackers

In some cases, the MAC address of the source machine is recorded in VPN logs.
In most cases observed during these attack campaigns, the attackers have used VMware virtual machines to connect to their victims.
If this information is logged and depending on the usages of VMware inside a company, incoming connections with VMware MAC addresses may be linked to an attack.

Detection rule: look for VPN connections with a client network interface MAC address starting with a VMware attributed prefix.

Prefix
00:0c:29
00:50:56
00:1C:14
00:05:69

4.1.3 Incoherent user accounts

The attackers are using legitimate credentials to connect to the victim's VPN endpoint and computers. Interestingly, they are using different accounts for the VPN authentication and for the Windows domain authentication. This is an anomaly for most companies. Looking for users using a different account for the domain authentication compared to the one used for the VPN authentication has uncovered most of the hostile connections.

Detection rule: among IP addresses assigned to the VPN which are authenticating on the Windows domain, look for a different identity than the one used on the VPN.

4.2 System indicators

4.2.1 Uncommon folders

The attackers have mainly used two types of folders to save tools and archives.
The first category contains folders named as antivirus software installation folders such as:

- `\ProgramData\ESETOEM`
- `\ProgramData\McAfeeOEM`

The second category contains folders existing for most Microsoft Windows installations but which should not contain any executables or RAR archives such as:

- \ProgramData
- c:\windows\AppPatch
- c:\PerfLogs and subfolders.

Generally speaking, having these types of files in these folders is an anomaly and should be investigated.

Detection rule: look for executables or archives (Zip, RAR) created in folders \ProgramData\ESETOEM, \ProgramData\McAfeeOEM, \ProgramData or c:\PerfLogs.

Setup of network port forwardings

The attackers have used the Windows firewall to set up port forwarding between their entry point and their final victim.
To do so, the netsh command has been used as follows:

```
netsh interface portproxy add v4tov4 listenport=443 connectaddress=XXX.XXX.XXX.XXX connectport=443
```

This command will set up a forward on port TCP/443 from the compromised workstation to the target XXX.XXX.XXX.XXX on port TCP/443.
When this command is executed, it will create and set a registry key.
Interestingly, when the configuration is later disabled, the key content is erased, but the key is not deleted.
This kind of configuration is rare in Windows environments. Looking for machines where this key is positioned has been a reliable indicator of compromise.

Detection rule: look for the registry key HKLM\SYSTEM\ControlSet{0,n}\services\PortProxy\v4tov4 on Windows machines.

5 Recommendations

5.1 For service providers

In order to prevent as much as possible these incidents, ANSSI recommends the following best practices to service providers and design offices:

- Use secure administration methods on IT systems (ANSSI's recommendations to secure administration of IT systems);
- Set up a security monitoring capability;
- Make a list of connections with clients and monitor them;
- Segregate clients between them.

5.2 For clients

In order to prevent as much as possible these incidents, ANSSI recommends the following best practices to clients of service providers:

- Use secure administration methods on IT systems (ANSSI's recommendations to secure administration of IT systems);
- Set up a security monitoring capability;
- Make a list of connections with service providers and monitor them;
- Apply a least privilege model to accesses given to external entities (accounts, connections, trust relashionships).

6 Appendix: PlugX

PlugX malware has only been observed during the first wave of attack. As a reminder, ANSSI is not able to link this phase with the second one for now.

6.1 Description

PlugX is a malware family also known as **KorPlug**, **SOGU**, **Scontroller**, etc. The main function of this malware is to take control of a remote host. System artefacts observed show that the *DLL sideloading* method is used to load the malware in the host memory.

6.2 SNORT rules

The following SNORT rules detect communications linked to **PlugX** version 2 (source : `https://www.us-cert.gov/ncas/alerts/TA17-117A`):

```
alert tcp any any -> any any (msg:"Non-Std TCP Client Traffic contains 'HX1|3a|' 'HX2|3a|' 'HX3|3a|' 'HX4|3a|' (PLUGX
     Variant)"; sid:XX; rev:1; flow:established,to_server; content:"Accept|3a 20 2a 2f 2a|"; nocase; content:"HX1|3a|"
     ; distance:0; within:6; fast_pattern; content:"HX2|3a|"; nocase; distance:0; content:"HX3|3a|"; nocase; distance
     :0; content:"HX4|3a|"; nocase; distance:0; classtype:nonstd-tcp; priority:X;)

alert tcp any any -> any any (msg:"Non-Std TCP Client Traffic contains 'X-Session|3a|''X-Status|3a|''X-Size|3a|''X-Sn
     |3a|'(PLUGX)"; sid:XX; rev:1; flow:established,to_server; content:"X-Session|3a|"; nocase; fast_pattern; content:
     "X-Status|3a|"; nocase; distance:0; content:"X-Size|3a|"; nocase; distance:0; content:"X-Sn|3a|"; nocase;
     distance:0; classtype:nonstd-tcp; priority:X;)

alert tcp any any -> any any (msg:"Non-Std TCP Client Traffic contains 'MJ1X|3a|' 'MJ2X|3a|' 'MJ3X|3a|' 'MJ4X|3a|' (
     PLUGX Variant)"; sid:XX; rev:1; flow:established,to_server; content:"MJ1X|3a|"; nocase; fast_pattern; content:"
     MJ2X|3a|"; nocase; distance:0; content:"MJ3X|3a|"; nocase; distance:0; content:"MJ4X|3a|"; nocase; distance:0;
     classtype:nonstd-tcp; priority:X;)

alert tcp any any -> any any (msg:"Non-Std TCP Client Traffic contains 'Cookies|3a|' 'Sym1|2e|' '|2c|Sym2|2e|' '|2c|
     Sym3|2e|' '|2c|Sym4|2e|' (Chches Variant)"; sid:XX; rev:1; flow:established,to_server; content:"Cookies|3a|";
     nocase; content:"Sym1|2e|0|3a|"; nocase; distance:0; fast_pattern; content:"|2c|Sym2|2e|"; nocase; distance:0;
     content:"|2c|Sym3|2e|"; nocase; distance:0; content:"|2c|Sym4|2e|"; nocase; distance:0; classtype:nonstd-tcp;
     priority:X;)
```

Version 1.0 - October 7th 2019

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN