TLP:WHITE

SUPPLY CHAIN ATTACKS

MENACES SUR LES PRESTATAIRES DE SERVICE ET LES BUREAUX D'ÉTUDES

Version 1.0

07/10/2019

TLP:WHITE

Sommaire

1 Introduction

Ce document vise à alerter d'une menace informatique ciblant les prestataires de service et les bureaux d'études. Des attaquants semblent vouloir prendre position sur les réseaux de prestataires afin de récupérer les données, voire d'accéder aux réseaux, de leurs clients.
Les informations contenues dans ce rapport sont issues des analyses de l'ANSSI suite au traitement d'incidents suivant ce schéma d'attaque. Les premières analyses menées pourraient laisser penser à des attaques en deux phases : elles sont temporellement éloignées et aucun lien technique n'a pour le moment été établi entre les deux. La première phase utilise principalement le code malveillant **PlugX**. La seconde s'appuie essentiellement sur des outils légitimes et le vol d'identifiants de connexion.
Ce document se concentre sur la seconde intrusion et le mode opératoire d'attaque[1] utilisé. Il fournit en annexe des éléments sur le code malveillant **PlugX** (chapitre 6).

2 Chaîne d'attaque

2.1 Compromission initiale

Pour prendre pied pour la première fois sur les réseaux ciblés, l'attaquant exploite des vulnérabilités sur des services exposés sur Internet et peu sécurisés, qu'il découvre en utilisant des outils comme **Acunetix**. D'autres méthodes usuellement employées sont l'utilisation d'identifiants présents dans des bases de données en ligne ou encore l'envoi de courriels piégés.

2.2 Accès et persistance

L'attaquant utilise des comptes VPN légitimes dont les identifiants ont probablement été dérobés pour revenir sur le réseau.
L'attaquant pourrait avoir d'autres moyens d'accès au réseau, que ce soit par des codes malveillants de type *RAT (Remote Access Tool)* ou des portes dérobées tels que des *webshells*, comme démontré lors d'intrusions plus anciennes avec des codes de la famille **PlugX**.

2.3 Élévation de privilèges

Afin d'obtenir plus de droits sur les machines sur lesquelles il se connecte, l'attaquant utilise des outils légitimes tels que **ProcDump** ou **Certmig** (voir section 3.2). L'acteur semble également créer des comptes administrateurs sur certains postes du réseau qui ne correspondent pas aux conventions de nommage habituellement utilisées sur les réseaux ciblés (par exemple un compte nommé « `aaaa` »).

2.4 Latéralisation

L'attaquant utilise principalement des connexions RDP avec des identifiants récupérés, des commandes **Netscan** et des scripts **WMIExec** afin de se propager dans le réseau.

2.5 Objectifs opérationnels

Les premières motivations de l'attaquant semblent être la compréhension du réseau et des interconnexions avec les clients et les modes d'authentification avec les réseaux des clients.

[1] Somme des outils, tactiques, procédures, techniques et caractéristiques mises en œuvre par un ou plusieurs acteurs malveillants dans le cadre d'une ou plusieurs attaques informatiques. Il s'agit de façon imagée de la carte d'identité technique d'un procédé d'attaque. À ne pas confondre avec un groupe d'attaquants qui recouvre une réalité plus large, notamment des individus et une organisation physique

Une fois ces informations obtenues, l'acteur s'étend sur le réseau des clients afin d'agréger les informations qu'il souhaite exfiltrer.
L'attaquant peut ensuite utiliser le réseau du client ou du prestataire pour effectuer l'exfiltration.

2.6 Sécurité opérationnelle

Bien que les outils utilisés par l'attaquant ne soient pas sophistiqués, il fait preuve d'organisation en supprimant ou en désactivant les journaux d'activité sur les machines sur lesquels il rebondit.
L'attaquant anonymise ses connexions vers ses cibles : les adresses IP utilisées pour se connecter au VPN des prestataires sont celles de points de sortie VPN ou du réseau TOR.

3 Outils utilisés

3.1 Outil spécifique

Outre les outils légitimes décrits plus loin dans le document, l'attaquant semble avoir développé un outil spécifique utilisé durant la seconde phase de l'attaque.
Le code malveillant spécifique permet principalement la supervision du navigateur *web* du poste infecté. Cela permet entre autres à l'attaquant de récupérer les identifiants de connexion ou encore les cookies de session. Le code communique avec son serveur de commande et contrôle en HTTP ou HTTPS.

3.2 Outils légitimes

L'attaquant semble utiliser les outils légitimes suivants :

- **ProcDump** : outil en ligne de commande qui permet de surveiller un processus en cours d'exécution, puis de créer un *dump* de la mémoire en fonction de critères spécifiques. L'attaquant utilise l'outil afin de récupérer les informations du processus LSASS en mémoire afin de récupérer les condensats des identifiants Windows ;
- **CertMig** : outil en ligne de commande qui permet l'import et l'export des certificats de la machine. L'attaquant utilise l'outil afin de récupérer les certificats permettant l'identification sur les VPN des clients du prestataire ;
- **WMIExec.vbs** : outil permettant l'administration de machines à distance en *VBScript* avec des fonctionnalités similaires à **SysInternals PsExec** ;
- **rar.exe** : version en ligne de commande de l'outil de compression de fichier WinRAR. L'attaquant l'utilise pour compresser, protéger et découper en plusieurs morceaux les informations à exfiltrer et les outils qu'il télécharge ;
- **MimiKatz** : outil permettant d'effectuer diverses actions sur un système Windows tel que l'injection de bibliothèques, la manipulation de processus, l'extraction de condensats et de mots de passe notamment ;
- **Netscan** : outil de scans réseaux IPv4/IPv6 permettant également l'exécution de commandes *PowerShell*.

4 Heuristiques de recherche des attaquants

Dans les incidents observés, les attaquants ont essentiellement utilisé des comptes et des outils légitimes. La détection basée sur des IOC usuels s'avère peu efficace dans de telles circonstances.
En revanche, les règles énoncées ci-dessous, bien que ne donnant pas une certitude absolue de compromission, pointent vers des anomalies indicatives de présence des attaquants et devraient faire l'objet d'une levée de doute.

4.1 Connexion VPN

4.1.1 Sources de connexion

Les attaquants utilisent essentiellement des services commerciaux de VPN ainsi que le réseau TOR pour anonymiser leur source de connexion. Dans la plupart des cas, les adresses IP des clients VPN ont des enregistrements associés à des services de VPN commerciaux, relativement populaires et fréquemment rencontrés dans la navigation web (HTTP/HTTPS) et l'envoi de courriel (SMTP/SMTPS).
En revanche, des utilisateurs se connectant à des VPN d'entreprise depuis un nœud de sortie de VPN public sont des anomalies.

Heuristique : rechercher les connexions entrantes dans les journaux d'entrée VPN ou VDI dont la source est un nœud de sortie du tableau suivant. Cette liste n'est pas exhaustive.

Adresses IP				
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 Adresse MAC de l'attaquant

Dans certaines configurations, l'adresse MAC de la machine source d'une connexion est enregistrée dans les journaux du VPN.
Dans la plupart des cas observés lors de la campagne, les attaquants semblent avoir utilisé des machines virtuelles VMware pour se connecter sur l'infrastructure de leur victime.
Si les journaux le permettent, et suivant les pratiques au sein de chaque organisation, les connexions effectuées depuis des interfaces réseau d'adresses MAC attribuées à VMware peuvent être liées à l'attaque.

Heuristique : rechercher des connexions VPN où l'adresse MAC de l'adaptateur réseau du client a un préfixe attribué à VMware.

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

4.1.3 Alternance de comptes utilisateurs différents

L'attaquant a utilisé des comptes légitimes usurpés pour se connecter sur le VPN et les systèmes de la victime. De façon notable, les attaquants ont fait usage de comptes différents pour s'identifier sur le VPN et sur le domaine Windows. Ceci devrait être inhabituel dans la plupart des organisations. Rechercher des utilisateurs s'authentifiant avec des comptes sans rapport sur le VPN et le domaine Windows fait apparaître la plupart des connexions hostiles.

Heuristique : rechercher parmi les adresses IP assignées sur le VPN celles effectuant des authentifications sur le domaine Windows avec une identité différente de celle utilisée sur le VPN.

4.2 Informations système

4.2.1 Usage de répertoires inhabituels

L'attaquant a principalement utilisé deux types de répertoires pour stocker ses outils et archives.
La première catégorie recouvre des répertoires nommés pour ressembler à des installations d'antivirus comme :

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

L'attaquant a aussi utilisé des répertoires existant sur la plupart des installations de Microsoft Windows, mais dans lesquels aucun exécutable et aucune archive RAR ne devrait se trouver, comme notamment :

- `\ProgramData`
- `c:\windows\AppPatch`
- `c:\PerfLogs` et ses sous-répertoires.

Dans tous les cas, la présence de fichiers directement sous ces répertoires est une anomalie qui devrait être investiguée.

Heuristique : rechercher des fichiers executables ou des archives (Zip ou RAR) créés dans les répertoires : `\ProgramData\ESETOEM`, `\ProgramData\McAfeeOEM`, `\ProgramData` ou `c:\PerfLogs`.

4.2.2 Positionnement de redirection réseau

L'attaquant a fait usage du pare-feu Windows pour mettre en place des transferts de port réseau (*Port Forwarding*) de son point d'entrée vers la cible finale.
Pour ce faire, la commande `netsh` est utilisée comme suit:

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

Cette commande configure une redirection du trafic réseau à destination du port TCP/443 local d'une station compromise vers la cible XXX.XXX.XXX.XXX sur le port TCP/443.
Quand cette commande est exécutée, elle crée et positionne une clé de base de Registre.
De façon remarquable, quand cette configuration est ultérieurement désactivée, le contenu de la clé est effacé, mais la clé n'est pas détruite.
Ce type de configuration est rare en environnement Windows. Rechercher les machines sur lesquelles cette clé est positionnée est un moyen de recherche de compromission fiable.

Heuristique : rechercher la clé de base de Registre `HKLM\SYSTEM\ControlSet{0,n}\services\PortProxy\v4tov4` sur les machines Windows.

5 Recommandations

5.1 Pour les prestataires

Dans le but d'éviter au maximum ce type d'incidents, l'ANSSI recommande les bonnes pratiques suivantes pour les prestataires de services et bureaux d'études :

- Administrer de manière sécurisé les systèmes d'informations (Guide de l'ANSSI : Administration sécurisée des systèmes d'information – v.2) ;
- Mettre en place une capacité de supervision de la sécurité ;
- Réaliser un inventaire des interconnexions avec les clients et en assurer la supervision ;
- Mettre en place un cloisonnement entre les différents clients.

5.2 Pour les clients

Dans le but d'éviter au maximum ce type d'incidents, l'ANSSI recommande les bonnes pratiques suivantes pour les clients :

- Administrer de manière sécurisé les systèmes d'informations (Guide de l'ANSSI : Administration sécurisée des systèmes d'information – v.2) ;
- Mettre en place une capacité de supervision de la sécurité ;
- Réaliser un inventaire des interconnexions avec ses prestataires et en assurer la supervision ;
- Appliquer le principe du moindre privilège pour les accès octroyés aux prestataires (comptes, interconnexions, approbations).

6 Annexes : PlugX

Le code malveillant **PlugX** n'a été vu que lors de la première phase de l'attaque. Pour rappel l'ANSSI n'est pas en mesure à ce stade d'identifier un lien entre les deux phases.

6.1 Description

PlugX est une famille de codes malveillants connue aussi sous les noms **KorPlug**, **SOGU**, **Scontroller**, etc. La principale fonction de ce code est de permettre le contrôle de l'hôte infecté à distance. Les artefacts systèmes retrouvés permettent de dire que le mode opératoire utilise la technique de *DLL sideloading* pour charger le code malveillant dans la mémoire de l'hôte.

6.2 Règle SNORT

Les règles SNORT suivantes permettent de détecter les communications de la version 2 de **PlugX** (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 - 07/10/2019

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