Rapport d'investigation – Comportement suspect sur le poste de travail

Contexte :

Un employé de la division recrutement a signalé des activités anormales sur son poste de travail, notamment l'activation de la caméra et l'apparition d'invites de commande. Un fichier PCAP a été analysé pour identifier les connexions sortantes suspectes.

L'objectif est de comprendre la menace et d'identifier les actifs compromis.

1. Extraction des connexions sortantes via Wireshark:

L'analyse du fichier PCAP a révélé plusieurs connexions sortantes suspectes, identifiées comme suit :

192.168.1.35 → 101.43.190.181 (Shenzhen Tencent Computer Systems, Chine)

192.168.1.100 → 107.189.8.58 (Luxembourg, PONYNET)

192.168.1.100 → 209.197.3.8 (StackPath LLC, USA)

2. Analyse de la réputation des adresses IP via VirusTotal

101.43.190.181 : Liée à des fichiers malveillants détectés, notamment DS.exe et wda.exe. Utilisée pour des activités malveillantes.

107.189.8.58 : Associée au BumbleBee botnet, avec plusieurs alertes pour des activités malveillantes comme des attaques de type DoS et bruteforce.

209.197.3.8 : Associée à StackPath LLC (légitime), mais liée à des fichiers fortement détectés comme svrwsc.exe et retro.exe, indiquant un possible compromis de services.

3. Investigation sur Elastic pour identifier les processus suspects :

L'utilisation d'Elastic a permis d'identifier les processus à l'origine des connexions suspectes :

Processus suspect : powershell.exe

Poste : DESKTOP-O6CSQRA

Utilisateur : PrinceGbedjinou

Connexion : 192.168.1.35 → 101.43.190.181 via PowerShell, avec port de destination 8088.

Processus suspect : powershell.exe

Poste : DESKTOP-UUNV01D

Utilisateur : RolandBlanc

Connexion : 192.168.1.100 → 107.189.8.58, communication suspecte par PowerShell avec l'IP malveillante, port utilisé : 8088.

(En lien avec l'alerte 1 : "Pièce jointe malveillante")

Actifs impactés :

Machine : DESKTOP-O6CSQRA

Machine : DESKTOP-UUNV01D

Utilisateur : PrinceGbedjinou

Utilisateur : RolandBlanc

IP source : 192.168.1.35

IP source : 192.168.1.100

IOCs (Indicateurs de compromission) :

IP malveillante : 101.43.190.181

IP malveillante : 107.189.8.58

IP potentiellement compromise : 209.197.3.8

Fichier malveillant : facture_edf_1.docm

Hash de mshta.exe : 7762a4766bc394b4cb2d658144b207183ff23b3139181cd74e615db63e6e57d6

URL malveillante : http://107.189.8.58:8088/admin/get.php

Recommandations :

Bloquer IPs :

101.43.190.181 (Chine)

107.189.8.58 (Luxembourg)

Surveillance de l'IP 209.197.3.8 (USA)

URL :

http://107.189.8.58:8088/admin/get.php

Mise en liste noire du fichier malveillant :

- facture_edf_1.docm

Bloquer hash :

- Hash de mshta.exe : 7762a4766bc394b4cb2d658144b207183ff23b3139181cd74e615db63e6e57d6

Isolation des machines impactées :

- DESKTOP-O6CSQRA
- DESKTOP-UUNV01D

Analyse des processus PowerShell pour détecter toute activité malveillante.

Gestion des comptes compromis :

Suppression des comptes utilisateurs créés non autorisés.

Réduction des privilèges administratifs sur les machines impactées.

Renforcement des politiques de sécurité :

Restreindre et surveiller l'usage de PowerShell.

Limiter l'utilisation de netsh.exe et renforcer les contrôles réseau.

Surveillance continue :

Surveillance active des machines impactées pour détecter toute activité suspecte.

Vérification des fichiers liés aux IPs suspectes pour s'assurer qu'ils ne sont plus actifs.

Malwares similaires :

Dans le cadre de l’investigation, plusieurs malwares similaires à celui utilisé par l’attaquant ont été identifiés. Ces malwares partagent des caractéristiques communes,

notamment l’utilisation de Remote Access Trojans (RATs) pour prendre le contrôle à distance des machines compromises.

Voici une liste des malwares similaires trouvés lors de la recherche :

budha.exe : Un fichier malveillant utilisé dans des attaques à distance pour exécuter des commandes sur des machines compromises.

Il est souvent lié à des activités de contrôle à distance.

svrwsc.exe : Un autre malware utilisé pour des activités similaires, notamment l’exfiltration de données et le contrôle à distance des postes de travail via des commandes malveillantes.

Ces malwares sont utilisés pour compromettre des systèmes en exploitant des vulnérabilités et en prenant le contrôle total des machines à des fins malveillantes,

comme c'est le cas avec les actions observées dans ce rapport.

Conclusion : Ces deux malwares partagent des similitudes avec les activités observées dans l'attaque sur les postes DESKTOP-O6CSQRA et DESKTOP-UUNV01D, notamment l'exécution

de PowerShell et l'établissement de connexions vers des IP malveillantes.