Rapport d'investigation - Pièce jointe malveillante

1.Analyse Oletools :

*L'analyse du fichier **facture_edf_1.docm** a révélé la présence d'une macro VBA malveillante qui se déclenche à la fermeture du document via la commande AutoClose.*

Éléments identifiés :

- WScript.Shell : Utilisé pour exécuter des commandes système.

- Run : Exécution d'un script PowerShell.

- Chaînes Base64 et Hex : Utilisées pour obfusquer le code.

- PowerShell : Exécution d'un script encodé en Base64 pour dissimuler ses actions.

- Extrait du script PowerShell : CN = "powershell -noP -sta -w 1 -enc SQBmACgAJABQAFMAVg..."

Décodage : *Le script PowerShell tente de contacter un serveur externe, probablement pour télécharger ou exécuter des fichiers malveillants supplémentaires.*

2. Analyse du fichier facture_edf_1.docm sur VirusTotal :

Caractéristiques du fichier :

SHA256 : 1c10ddc82fc2799acd9a3ee2d9ca6f9733efe005866bdaf2a7ab6105f42d61ec

SHA1 : 32748377a75aa7faba3b556fa11bcfd86758fa54

MD5 : 4ecfb5cec0dc5455f038c5539e2949de

Détection : 41/67 moteurs antivirus identifient ce fichier comme malveillant (Trojan, Downloader, Script PowerShell).

Comportement malveillant :

- Obfuscation des macros : Cache les véritables intentions du fichier.

- Exécution de PowerShell : Téléchargement d'un fichier depuis une URL malveillante.

- Évasion des systèmes de sécurité : Désactivation de protections comme l'AMSI (Antimalware Scan Interface).

Indicateurs de compromission (IOCs) :

IP malveillante : 107.189.8.58

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

User-Agent : Mozilla/5.0

3. Analyse IP 107.189.8.58 sur VirusTotal :

Informations générales sur l'IP :

Adresse IP : 107.189.8.58

ASN : 53667 (PONYNET)

Pays : Luxembourg

Région : Europe

Plage IP : 107.189.8.0/22

Détection globale : 8/94 fournisseurs de sécurité signalent cette IP comme malveillante.

Dernière analyse : 10 jours avant cette investigation.

Détail des détections malveillantes :

Moteurs ayant marqué l'IP comme malveillante :

alphaMountain.ai, ArcSight Threat Intelligence, BitDefender, CRDF, CyRadar, G-Data, Lionic, Sophos.

Rôle de cette IP : Le fichier malveillant utilise une commande PowerShell pour contacter cette IP, probablement afin de télécharger un fichier supplémentaire ou exécuter des actions malveillantes. Elle fait partie de l'infrastructure d'attaque.

Domaines résolus :

Domaines malveillants : bad3.yourironcore.com (5/94 détections), www.jieav.club (1/94 détections).

Autres domaines : hosted-by.meow.surf, control.meowcatto.com, www.uuanime.com, uuanime.com.

Fichiers communiquant avec cette IP :

- Fichier facture_edf_1.docm (41/67 détections).

- Fichier Android malveillant (détection 10/64).

Fichiers référents : Certains fichiers mentionnent cette IP dans des bases de données de botnets, scanners et zombies :

- botnets_zombies_scanner_spam_ips.txt
- awstats102023.1-nationcountry.com.txt

Résumé des conclusions :

Risque élevé : L'IP est identifiée comme malveillante par plusieurs moteurs de sécurité et est liée à des fichiers malveillants, notamment facture_edf_1.docm.

Infrastructure malveillante : Cette IP fait partie d'une infrastructure utilisée pour des activités malveillantes (ex. : téléchargement de charges supplémentaires via PowerShell).

Focus nécessaire : Cette IP doit être prioritaire dans l'investigation en raison de son rôle dans l'infection.

4. Analyse Elastic Connexion réseau suspecte entre 192.168.1.100 et 107.189.8.58 :

Résultats de l'analyse :

Date et Heure : 27 février 2023 @ 17:58:31

Action :

RolandBlanc a établi une connexion réseau suspecte via PowerShell vers l'IP 107.189.8.58, un serveur externe identifié comme malveillant sur VirusTotal.

Cette connexion pourrait indiquer une communication avec un serveur de commande et contrôle (C2), souvent utilisé dans les attaques pour exfiltrer des données ou exécuter des commandes à distance.

Détails techniques :

- Processus exécuté : powershell.exe
- Emplacement du fichier : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- PID du processus : 15,206
- IP source : 192.168.1.100
- Port source : 55,154
- IP de destination : 107.189.8.58
- Port de destination : 8,088
- Protocole : HTTP sur TCP (IPv4)
- Direction du réseau : Outbound (sortant)

Utilisateur impliqué :

Nom d'utilisateur : RolandBlanc

Domaine utilisateur : AzureAD

Source machine : DESKTOP-UUNV01D

Système d'exploitation : Windows 10 Pro (version 10.0)

Recommandations :

- Bloquer les Iocs

- Surveiller de près les actions futures de cet utilisateur.

- Analyser les processus liés à PowerShell pour détecter d'éventuelles modifications réseau ou de nouvelles connexions suspectes.

- Isoler la machine DESKTOP-UUNV01D pour éviter la propagation potentielle de la menace et effectuer une analyse approfondie des fichiers exécutés.

- Sensibiliser les utilisateurs aux risques des pièces jointes malveillantes et aux bonnes pratiques concernant l'utilisation de macros dans les documents.

- Mettre à jour toutes les signatures antivirus et EDR avec les nouveaux indicateurs de compromission pour renforcer la détection.

Liste d'IOCS et actifs impactés :

Actifs impactés :

Machine : DESKTOP-UUNV01D

Utilisateur : RolandBlanc

IP source : 192.168.1.100

IOCs (Indicateurs de compromission) :

Fichier malveillant : facture_edf_1.docm

IP malveillante : 107.189.8.58

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

User-Agent malveillant : Mozilla/5.0

Hash du fichier malveillant (facture_edf_1.docm) :

SHA256 : 1c10ddc82fc2799acd9a3ee2d9ca6f9733efe005866bdaf2a7ab6105f42d61ec