Forensic Challenge

Cas 1 : Intrusion sur un serveur Windows

1. Introduction

1.1 Contexte

Un serveur Windows appartenant à l’entreprise a présenté des comportements suspects, notamment des connexions réseau inhabituelles et des processus inconnus. Une image forensique du système a été réalisée pour analyse approfondie.

1.2 résumé des événements

Entre le 4 et le 9 février 2024, le serveur, accessible à distance via Internet pour permettre le télétravail de l’administrateur, a été compromis suite à une attaque par bruteforce. Les attaquants ont testé des milliers de combinaisons jusqu’à trouver un mot de passe administrateur valide. Une fois l’accès obtenu, ils ont créé un nouveau compte “admin”, installé des outils d’administration et de repérage pour cartographier le réseau, et affaibli l’antivirus intégré afin d’éviter toute détection. Par la suite, ils ont déposé et extrait une archive contenant deux programmes malveillants déguisés en outils Windows, appartenant à la famille Petya (chiffrement des données à des fins d’extorsion). En parallèle, ils ont compressé et exfiltré le dossier partagé des utilisateurs du serveur. Une note de rançon est également apparue. Enfin, les attaquants ont propagé et exécuté automatiquement le programme malveillant sur six ordinateurs du réseau.

2. Analyse technique

2.1 Timeline (UTC+1, Paris)

05/02/2024

- 01:37 — Début du bruteforce RDP (100014 4625): 36.133.110.87 (kali) user : Administrator
- 09:52 — Première session RDP réussie : 195.21.1.97 user : Administrator
- 11:55 — 4624 / LogonType=3 depuis 36.133.110.87
- 18:13 — Dernière session RDP de 195.21.1.97
- 21:58 — Fin du bruteforce de 36.133.110.87
- 23:43 — Début des tentatives depuis 185.229.66.183 (kali) — 4625 user : Administrator
- 23:55 — 4624 / LogonType=3 réussi depuis 185.229.66.183

06/02/2024

- 00:00 — session RDP réussie depuis 185.229.66.183 user : Administrator
- 00:02 — 4720 — Création du compte admin
- 00:28 — Création de C:\Users\admin\Desktop\share.zip
- 00:42 — Installation des dépendances de scan réseau : Nmap, Npcap
- 09:45 — Première session RDP de 195.21.1.97
- 18:12 — Dernière session RDP de 195.21.1.97
- 20:52 — Première apparition de 31.220.85.162 (kali) user : admin
- 22:31 — Suppression des tâches planifiées Windows Defender (*Cleanup*, *Verification*, *Cache Maintenance*)
- 22:49 — Création de la tâche planifiée \Enterpries backup par *BRANCHOFFICE\admin*
- 23:14 — USN/$J — Suppression de share.zip → $RAN75BL.zip

07/02/2024

- 09:45 — Première apparition de 195.21.1.97
- 11:15 — Première apparition de 31.220.85.162 user : admin
- 17:48 — RDP (Type 10) depuis 31.220.85.162
- 18:14 — Dernière apparition de 195.21.1.97

08/02/2024

- 09:45 — Première apparition de 195.21.1.97
- 18:11 — Dernière apparition de 195.21.1.97
- 20:00 — Première apparition de 31.220.85.162
- 23:57 — Dernière apparition de 31.220.85.162

09/02/2024

- 09:45 — Première apparition de 195.21.1.97
- 18:12 — Dernière apparition de 195.21.1.97
- 16:04 — Première apparition de 31.220.85.162
- 22:46 — Exécution de \Enterpries backup
- 23:52 — Dernière apparition de 31.220.85.162

2.2 IP externes

36.133.110.87 : attaquant
185.229.66.183 : attaquant
31.220.85.162 : attaquant
195.21.1.97 : au vu du comportement probablement le véritable admin, a confirmer.

2.3 IOC

important.zip (Users/admin/Desktop/important.zip): archive contenant les fichiers rename.exe et dir.exe
dire.exe (Users/admin/Desktop/dir.exe) : binaire petya « plein format ».
MD5 : af2379cc4d607a45ac44d62135fb7015
SHA-1 : 39b6d40906c7f7f080e6befa93324dddadcbd9fa
rename.exe (Users/admin/Desktop/rename.exe) binaire petya version «dropper ».
MD5 : a92f13f3a1b3b39833d3cc336301b713
SHA-1 : d1c62ac62e68875085b62fa651fb17d4d7313887
RyukReadMe.txt : fichier texte de rançon. (voir annexe)

Anexe

RyukReadMe.txt :

```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest military algorithms RSA4096 and AES-256.

Photorec, RannohDecryptor etc repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files wrote to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions to get teh decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you an additional +0.5BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions on how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
elismarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk
No system is safe
```