Forensic Challenge

23/09/2025

Abdalla Hamd-Mohamed, Olivier Baudry

Cas 1 : Intrusion sur un serveur Windows

Sommaire

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 5 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 tenté de propager et exécuter automatiquement le programme malveillant sur six ordinateurs du réseau mais cette action a échouée.

2. Analyse

2.1 sources

Image E01 du Windows serveur dont ont été extrait :

Journaux Windows :

Security.evtx
System.evtx
PowerShell/Operational.evtx
RemoteConnectionManager/Operational.evtx
TaskScheduler/Operational.evtx

Registre :

ruche SYSTEM
SECURITY
SOFWARE

NTFS :

$MFT
$J

2.2 Outils utilisés

Autopsy /FTK imager pour l'analyse de l'image forensique en lecture seule.
Observateur d'événements pour l'analyse des journaux Windows.
Events-Ripper pour le parsing et l'analyse des journaux Windows.
MFTECmd pour l'analyse du registre.

2.3 IOC

important.zip (Users/admin/Desktop/important.zip): archive contenant les fichiers rename.exe et dir.exe

dir.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)

Logs de scans Nmap (Users/admin/Desktop/map)

202402062109 Intense scan on 10.44.24.1_24.xml

202402071016 Intense scan on 10.44.24.1_24.xml

share.zip ($Recycle.bin → $RAN75BL.zip) : archive contenant la copie du répertoire share

nmap-7.93-setup.exe (Users/admin/Download/nmap-7.93-setup.exe)

Enterpries backup : tâche Windows exécutant PsExec à la date du 9/02/2024

PsExec.exe - accept-eula \\Desktop-001,Desktop-002,Desktop-003, Desktop-004,Desktop-005,Desktop-006 -c -d -u admin -p letmein -realtime C: \Users\admin\Desktop\rename.exe

→ Objectif : pousser puis exécuter rename.exe à distance via les partages ADMIN$ des postes.

IP externes identifiées:

36.133.110.87 : malveillante

185.229.66.183 : malveillante

31.220.85.162 : malveillante

195.21.1.97 : au vu du comportement : le véritable admin, a confirmer.

2.4 Synthèse

L’intrusion se caractérise par une compromission RDP avérée consécutive à une campagne de force brute (100 014 événements 4625).
Les tentatives proviennent principalement de 36.133.110.87, complétées par 31.220.85.162 et 185.229.66.183 ; des ouvertures de session 4624, d’abord en NLA puis en RDP, confirment l’obtention d’identifiants valides.

Dans la foulée, l’attaquant crée un compte local « admin » (4720), ouvre des sessions dotées de privilèges spéciaux (4672) et procède à une élévation par appartenance de groupe dans l’AD (4728, ajout à un groupe global), établissant un contrôle durable.

Un paquetage « share.zip » est préparé sur le bureau du compte « admin » puis déplacé en Corbeille, ce qui suggère un exfiltration des dossiers partagés utilisateurs.
Parallèlement, des événements liés à Windows Defender (notamment 5007 et 7036/7040) témoignent d’actions de configuration/service sur WinDefend durant la fenêtre d’attaque.

La reconnaissance interne est objectivée par un scan Nmap du segment 10.44.24.0/24 qui dresse l’inventaire de cinq hôtes Windows (DESKTOP-001 à -005) exposant SMB et RDP ; cette cartographie alimente une tentative de mouvement latéral via une tâche planifiée « \Enterpries backup » qui lance PsExec avec les identifiants « admin/letmein » vers Desktop-001..006.

Les journaux Task Scheduler montrent le déclenchement effectif de la tâche et la création du processus PsExec, mais l’action échoue à l’authentification (ResultCode 0x8007052E : « Logon failure »).

En synthèse, le corpus atteste un enchaînement « Valid Accounts → Privilege Escalation → Defense Evasion → Discovery → Lateral Movement (tenté) », corespond à une attaque de type ransomware la dernière étape ayant été empêchée par l’échec d’authentification.

3. Recommandations

3.1 Mesures immédiates

Isolement réseau du serveur et des postes visés
Blocage des IP externes identifiées
Désactiver le compte admin créé et réinitialiser tous les comptes Administrateur
Supprimer les tâches suspectes
Conservations des artefacts pour preuve

3.2 Renforcement

Sécurisation RDP (NLA, MFA, audits)
Renforcement des défenses (EDR, durcissement Defender)
Gestion des comptes (LAPS)
Sauvegardes immuables

3.3 Surveillance continue

Détection des événements suspects (7045, 7036, tâches planifiées, PsExec)
Corrélation des journaux RDP (Schannel, 4624/1149)

4. Conclusion

L’analyse converge vers attaque de type ransomware par une compromission initiale via RDP exposé et attaqué en brute-force depuis Internet, suivie de connexions réussies et de la création d’un compte local admin puis d’élévations de privilèges.

L’attaquant a ensuite outillé le serveur, modifié Defender, et mené une reconnaissance réseau en vue d’une propagation latérale via PsExec orchestrée par une tâche planifiée.

Cette tentative a échoué à l’authentification, ce qui a probablement empêché l’exécution à distance des binaires et la phase de chiffrement.

En l’état, l’impact confirmé est limité au serveur (ouverture de sessions privilégiées, création de compte, exfiltration de données via share.zip).
La propagation vers les postes n’a pas abouti et le chiffrement n’a pas été observé.

Les éléments collectés (EVTX, $MFT/$J, tâches, navigateur, etc.) constituent des preuves suffisantes pour documenter la chaîne d’intrusion et alimenter la défense (blocage des IP, détection sur IOC).

La priorité est désormais de pérenniser le durcissement (RDP uniquement via VPN, MFA, désactivation des comptes et services non indispensables) et de renforcer la supervision.

Annexe

Timeline (UTC+1, Paris)

05/02/2024

- 01:37 — Début du bruteforce RDP (100014 4625): 36.133.110.87 (kali) cible : 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 de la vague 36.133.110.87
- 23:43 — Début des tentatives depuis 185.229.66.183 (kali) — 4625 cible : 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 par Administrator
- 00:24:35 — 4728 : ajout de CN=A Admin,… au groupe global “A Admin” → élévation de privilèges.
- 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
- 21:09 — Arrivée et extraction de Important.zip contenant dir.exe et rename.exe sur le bureau d’admin.
- 22:09 — Scan intense de Nmap (échec)
- 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 — StreamChange sur PsExec.exe / PsExec64.exe
- 23:14 — 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
- 11:16 — Scan intense de Nmap
  → Hôtes up : 10.44.24.1 → DESKTOP-001, .6 → DESKTOP-002, .7 → DESKTOP-003, .8
  → DESKTOP-004, .9 → DESKTOP-005. → Ports principaux : 135/139/445 (SMB), 3389 (RDP).
- 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 la tâche \Enterpries backup
- 22:46 — échec de l’action (ResultCode=0x8007052E → Logon failure: unknown user name or bad password).

- 23:52 — Dernière apparition de 31.220.85.162

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
```