RAPPORT DE CYBERSÉCURITÉ

Par le groupe 4 : Shayan, Florian, Draxan, Matis

Introduction

Ce rapport a pour objectif de répertorier nos analyses et nos remarques concernant le malware, le point central de cette semaine.

Afin de suivre correctement le rapport, notre répertoire GitHub contient les différents fichiers nécessaires pour progresser dans ce document.

Lien GitHub : https://github.com/Mine-Map/CyberSecu

Story 1

Malware testé sur debian et windows. Le fichier zip s'extrait et fait crash debian. Sur Windows 11 et 10, il ouvre rapidement un terminal avec un message affiché, puis ce terminal se réduit.

Story 2

J'ai analysé un fichier suspect en utilisant le site VirusTotal pour vérifier s'il s'agit d'une menace connue. En recherchant le fichier sur VirusTotal, j'ai trouvé que ce fichier est un TROJAN détecté pour la première fois le 13 octobre 2022 à 07:43:41 UTC, : six types différents de hash cryptographiques ont été générés , fournissant ainsi des empreintes numériques complètes et robustes pour l'identification du fichier.

- MD5 (954f7f91688a0d4eb5a60692bd27f1e3)
- SHA-1 (1d9e88ef0ab9003b4dc8f34cf0341105ac3cdb7e)
- SHA-256 (a1af8eeaa7fda7ced591a72c572a12c2298ddb763defaa36ce5b17be1411c2be)
- Vhash (bbce6dc16cd60ec54cd4b49aea8a08f0)
- SSDEEP (196608:CIDGGIZBGavaavmoqB9ohIUuF5LRkBkOa1qBg:sevgBqWLdOaABg)
- TLSH(T12596330SF6FBA9957F13829EAAF6011C50D69541EE45C93DA30801A7E08EFE4F4EC26F)

Story 3

J'ai réalisé une analyse statique du malware en travaillant sur le fichier Env.exe extrait de l'archive ZIP, sans jamais l'exécuter afin d'éviter tout risque. Le fichier est un exécutable Windows de type PE32, développé en C++ avec le framework Qt. L'étude de ses dépendances met en évidence l'utilisation de bibliothèques classiques telles que Qt5Core, Qt5Network, KERNEL32, SHELL32, msvcrt et libstdc++. Cela correspond à une application graphique standard, avec des capacités réseau possibles, mais qui ne peuvent pas être confirmées à ce stade.

L’extraction et l’analyse des chaînes de caractères n’ont révélé aucun élément suspect : aucune URL, adresse IP, chemin système sensible (AppData, Run) ou commande système comme cmd ou PowerShell. La structure interne du binaire (.text, .data, .rdata, .idata, etc.) est conforme à un exécutable Windows classique, sans signe de compression, de chiffrement ou d’obfuscation. Les empreintes cryptographiques du fichier (MD5 et SHA-256) ont été relevées afin de permettre son identification. Aucun mécanisme de persistance, d’injection de code ou d’anti-analyse n’a été identifié lors de cette analyse statique.

Commande :

- **cd ~/malware/US3/Malware**
- **ls**
- Malware.zip VIRUS
- **cd VIRUS**
- **ls**

  Env.exe
  Res.exe
  Qt5Core.dll
  Qt5Gui.dll
  Qt5Network.dll
  Qt5Widgets.dll
  libgcc_s_dw2-1.dll
  libstdc++-6.dll
  libwinpthread-1.dll
- **ls -lh**

  -rw-rw-r-- 1 mat mat 52K 13 août 2022 Env.exe
  -rw-rw-r-- 1 mat mat 116K 23 janv. 10:38 hashes.txt
  -rw-rw-r-- 1 mat mat 118K 13 août 2022 libgcc_s_dw2-1.dll
  -rw-rw-r-- 1 mat mat 1.5M 13 août 2022 libstdc++-6.dll
  -rw-rw-r-- 1 mat mat 78K 13 août 2022 libwinpthread-1.dll
  -rw-rw-r-- 1 mat mat 5.9M 13 août 2022 Qt5Core.dll
  -rw-rw-r-- 1 mat mat 6.0M 13 août 2022 Qt5Gui.dll
  -rw-rw-r-- 1 mat mat 1.8M 13 août 2022 Qt5Network.dll
  -rw-rw-r-- 1 mat mat 6.1M 13 août 2022 Qt5Widgets.dll
  -rw-rw-r-- 1 mat mat 25K 22 août 2022 Res.exe
  -rw-rw-r-- 1 mat mat 12K 23 janv. 10:38 strings.txt

file *

- Env.exe: PE32 executable for MS Windows 4.00 (GUI), Intel i386 (stripped to external PDB), 8 sections
- hashes.txt: ASCII text
- libgcc_s_dw2-1.dll: PE32 executable for MS Windows 4.00 (DLL), Intel i386 (stripped to external PDB), 10 sections
- libstdc++-6.dll: PE32 executable for MS Windows 4.00 (DLL), Intel i386 (stripped to external PDB), 10 sections
- libwinpthread-1.dll: PE32 executable for MS Windows 4.00 (DLL), Intel i386 (stripped to external PDB), 10 sections

- Qt5Core.dll: PE32 executable for MS Windows 4.00 (DLL), Intel i386 (stripped to external PDB), 11 sections
- Qt5Gui.dll: PE32 executable for MS Windows 4.00 (DLL), Intel i386 (stripped to external PDB), 11 sections
- Qt5Network.dll: PE32 executable for MS Windows 4.00 (DLL), Intel i386 (stripped to external PDB), 11 sections
- Qt5Widgets.dll: PE32 executable for MS Windows 4.00 (DLL), Intel i386 (stripped to external PDB), 11 sections
- Res.exe: PE32 executable for MS Windows 4.00 (console), Intel i386 (stripped to external PDB), 8 sections strings.txt: assembler source, ASCII text

file Env.exe

- Env.exe: PE32 executable for MS Windows 4.00 (GUI), Intel i386 (stripped to external PDB), 8 sections

- **ls -lh Env.exe**
- rw-rw-r-- 1 mat mat 52K 13 août 2022 Env.exe

- **md5sum Env.exe > hashes.txt**
- **sha256sum Env.exe >> hashes.txt**
- **cat hashes.txt**
- abbc02a7e5ff7b884700eac7087cf743 Env.exe
- e09ec2098363a129de143fdaf73ad6e2e61266fba3f638a25214af3a8bc8f2f2 Env.exe

- **strings Env.exe > strings.txt**
- **grep -i -E "http|https|ftp|AppData|Users|Run|cmd|powershell" strings.txt**
- !This program cannot be run in DOS mode.
- Mingw-w64 runtime failure:
- _ZN7QString8truncateEi
- -acmdln

- **objdump -p Env.exe | grep DLL**
- vma: Hint Temps Avant DLL Premier
- DLL Name: Qt5Core.dll
- DLL Name: Qt5Network.dll
- DLL Name: libgcc_s_dw2-1.dll
- DLL Name: KERNEL32.dll
- DLL Name: msvcrt.dll
- DLL Name: SHELL32.dll
- DLL Name: libstdc++-6.dll

- **objdump -h Env.exe**

Sections:

- Idx Name Size VMA LMA File off Algn
- 0 .text 00006dd8 00401000 00401000 00000400 2**4
  CONTENTS, ALLOC, LOAD, READONLY, CODE, DATA
- 1 .data 00000070 00408000 00408000 00007200 2**2

CONTENTS, ALLOC, LOAD, DATA
- 2 .rdata 000017f4 00409000 00409000 00007400 2**5
  CONTENTS, ALLOC, LOAD, READONLY, DATA
- 3 .eh_fram 000010ac 0040b000 0040b000 00008c00 2**2
  CONTENTS, ALLOC, LOAD, READONLY, DATA
- 4 .bss 00000444 0040d000 0040d000 00000000 2**6
  ALLOC
- 5 .idata 00002c20 0040e000 0040e000 00009e00 2**2
  CONTENTS, ALLOC, LOAD, DATA
- 6 .CRT 00000034 00411000 00411000 0000cc00 2**2
  CONTENTS, ALLOC, LOAD, DATA
- 7 .tls 00000020 00412000 00412000 0000cd00 2**2
  CONTENTS, ALLOC, LOAD, DATA

- **ls**
  Env.exe
  Res.exe
  Qt5Core.dll
  Qt5Gui.dll
  Qt5Network.dll
  Qt5Widgets.dll
  libgcc_s_dw2-1.dll
  libstdc++-6.dll
  libwinpthread-1.dll
  hashes.txt
  strings.txt

Story 4

Un RAT qui reposent sur le framework Qt été installé et à crée un dossier C:\WindSyst\ qui ressemble au dossier System32 avec deux exécutables (Env.exe, Res.exe), des DLLs Qt5 et dépendances C++, ainsi qu'un keylogger dans log.txt enregistrant les frappes utilisateur. Grâce au logiciel Wireshark on peut identifier une connexion Command & Control vers 23.58.193.189:443 pour exécuter des commandes distantes et surveiller l'utilisateur en temps réel.

Story 5

L’analyse dynamique a mis en évidence une compromission critique de la machine par un malware de type RAT (Remote Access Trojan) basé sur le framework Qt. Le malware établit une communication chiffrée sortante vers un serveur de commande et contrôle distant (23.58.193.189:443), confirmant une prise de contrôle à distance. Les échanges réseau, bien que brièvement établis, montrent un comportement furtif avec fermeture volontaire de la connexion (TCP RST).

Sur le plan système, le malware crée un dossier camouflé C:\WindSyst\ contenant des exécutables malveillants (Env.exe, Res.exe), des bibliothèques Qt et C++ embarquées, ainsi

qu’un fichier de journalisation. Ce fichier confirme la présence d’un keylogger actif, entraînant une compromission totale des données saisies par l’utilisateur. Le malware assure sa persistance au démarrage, lui permettant de se relancer automatiquement après chaque redémarrage. Bien que détecté par Windows Defender, le virus pourrait être modifier pour ne plus lettre.

L’impact est critique : la confidentialité, l’intégrité et la fiabilité du système sont compromises. La machine ne peut plus être considérée comme sûre.

La mesure de mitigation recommandée est une réinstallation complète du système après formatage, suivie d’une mise à jour intégrale. Tous les identifiants utilisés sur la machine doivent être changés. À titre complémentaire, le blocage des indicateurs de compromission, le renforcement de la sécurité système et la surveillance accrue du trafic réseau sont nécessaires pour prévenir toute récidive.

Story 6

Acquisition de la RAM :

- **Avec WinPMEM :**

Une fois les commandes exécutées, un fichier ram_dump.raw sera créé. Ce fichier sera exploitable avec Volatility.

- **Avec DumpIt :**

Une fois l'exécutable exécuté, un fichier .dmp (contenant le nom du PC comme CYBERSECURITE-20260122-082535, CYBERSECURITE = nom du PC) sera créé. Ce fichier sera exploitable avec Volatility.

Analyses Mémoire :

Ces analyses ont été effectuées grâce à Volatility avec le dump RAM récupéré avec DumpIt.

- **Processus actifs :**

L'investigation des processus en cours à l'aide du plugin windows.pslist a aidé à détecter le processus Res.exe, qui est associé à l'un des exécutables que le logiciel malveillant a implantés sur la machine.

Ce processus fonctionne dans un environnement utilisateur et est lié à des processus de console (conhost.exe, WindowsTerminal.exe), ce qui correspond au comportement constaté lors de l'exécution du trojan (fenêtre terminal qui enregistre les frappes clavier, keylogger). Aucune autre procédure suspecte, portant un nom atypique ou lancée depuis une localisation inhabituelle, n'a été détectée.

- **Processus terminés/cachés :**

L'examen effectué avec l'outil windows.psscan révèle la présence du processus Res.exe dans la mémoire, sans signaler de tentative de camouflage ou de furtivité.On n'a observé aucun

processus caché, orphelin ou incohérent, ce qui indique que le malware fonctionne comme un processus utilisateur standard, sans dispositif de dissimulation sophistiqué en mémoire vive.

- **Connexions réseau :**

L'analyse des liaisons réseau grâce au plugin windows.netscan, au moment de l'acquisition mémoire, n'a détecté aucune connexion réseau active. Bien que le logiciel malveillant intègre des bibliothèques réseau, notamment par l'intermédiaire du framework Qt (Qt5Network.dll), aucune communication continue ou tentative d'exfiltration n'a été détectée en mémoire lors de la sauvegarde.

Conclusion :

L'analyse de la mémoire vive a révélé la présence d'un logiciel malveillant identifié comme étant Res.exe, en cours d'exécution au moment de la collecte et lié à une exécution en mode console, ce qui est compatible avec un comportement typique de keylogger. Il n'a été découvert aucune indication de tentative de dissimulation, de persistance ou de communication externe au sein de la RAM.

Ces éléments indiquent que le malware est un simple Trojan (cheval de Troie), qui opère uniquement quand il est exécuté et repose principalement sur des objets sauvegardés sur le disque dur. Cela souligne l'importance du moment choisi lors d'une acquisition mémoire forensique.

Story 7

L'image disque bit-à-bit a été acquise via FTK Imager au format EnCase (E01) avec compression niveau 9 en un seul segment, capturant l'intégralité du disque dur de la machine. Le conteneur EnCase/E01 encapsule la copie secteur par secteur, des métadonnées d'acquisition et des sommes d'intégrité pour vérifier l'absence d'altération. L'analyse forensique complète du dump révèle une compromission de la machine.

Infrastructure de persistance détectée : dossier camouflé `C:\WindSyst\` contenant deux exécutables (Env.exe, Res.exe), quatre DLL Qt5 (Core, Gui, Network, Widgets), trois dépendances C++ (libgcc_s_dw2-1.dll, libstdc++-6.dll, libwinpthread-1.dll), et un fichier log.txt (396 bytes). Tous les fichiers portent la marque Internet Zone, indiquant leur extraction depuis l'archive ZIP téléchargée.

Extraction complète de la structure malveillante depuis l'archive : dossier `/Malware-main/Malware-main/Malware/VIRUS/` contenant les mêmes dépendances C++ et bibliothèques Qt5, confirmant le chaînage d'exécution du malware (déballage de l'archive suivi de l'exécution de Res.exe et Env.exe).

Analyse de l'artefact réseau : communication TCP établie vers 23.58.193.189:443 (HTTPS/TLS) indiquant contact avec serveur C&C, suivi d'un TCP Reset/ACK attestant fermeture intentionnelle après transmission de commandes. Log.txt contient les traces d'un keylogger enregistrant les frappes utilisateur (cmd.exe, PowerShell, énumérations système).

Story 8

Scénario d'attaque (théorique) :

Lors de l’exécution du malware, le keylogger est déclenché. Les fichiers du trojan sont alors copiés dans le dossier C:\WindSyst\, comprenant notamment Res.exe, Env.exe, des bibliothèques Qt5, des dépendances C++ ainsi que le fichier log.txt.

Une fois les fichiers copiés, Res.exe est exécuté et apparaît comme un processus actif en mémoire (RAM). Côté interface, le terminal ouvert par Res.exe est réduit dans la barre des tâches. Le terminal récupère les saisies au clavier, tandis que le fichier log.txt conserve ces saisies et se met à jour à chaque fois qu’une touche est pressée, les données étant stockées sur le disque et non dans la RAM.

À l’exécution du malware, une communication réseau ponctuelle est effectuée vers l’adresse 23.58.193.189 sur le port 443 (HTTPS), permettant l’envoi de données et la réception de commandes.

Enfin, après redémarrage du système, le malware se relance automatiquement.

Correspondances RAM et disque :

Dans la mémoire vive, le fichier Res.exe est repéré comme étant un processus actif et ce fichier se trouve dans le disque et n'est jamais supprimé. Les consoles ouvertes par le trojan pour lancer le keylogger sont visibles dans la RAM et les saisies sont stockées en brut dans le disque dans log.txt.

L'analyse des connexions réseau via le dump de la RAM n'a pas permis de détecter de liaison avec un quelconque réseau, mais une communication TCP a été repérée dans l'artéfact réseau du disque.

Persistance :

D'après nos analyses, le processus Res.exe est relancé automatiquement, relançant ainsi le keylogger. Le malware persiste donc sur le système, même après un reboot, bien que le mécanisme exact n'ait pas été identifié.

Story 9

L’analyse de la clé de registre USBSTOR dans le hive SYSTEM a permis d’identifier une clé USB SanDisk Cruzer Blade précédemment connectée au système.
Le numéro de série unique (USB Serial/UID) du périphérique est : 4C530000281008116284&0.

Cet identifiant peut être utilisé pour relier le périphérique à un utilisateur ou à un événement de fuite de données.

Récupération des données:

- git clone https://github.com/Waelmeg/Dump_memoire.git
- cd Dump_memoire

Extraction de l’archive mémoire :

- unzip dump.zip
- cd dump

- **Vérification :**
  ls -lh

Analyse du registre avec hivexsh :

- hivexsh SYSTEM

Navigation vers les périphériques USB :

- cd ControlSet001
- cd Enum
- cd USBSTOR
- ls

Accès au périphérique USB identifié :

- cd Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00
- ls

Extraction du numéro de série (UID) :

- cd 4C530000281008116284&0

Story 10

Utilisation de Registry Explorer pour windows. L'analyse du hive SYSTEM a permis d'identifier un périphérique de stockage USB dont l'identifiant matériel unique (UID) est associé aux propriétés temporelles suivantes :

- Première insertion du périphérique (First Install Date – valeur 0064) : 03 février 2020 à 12:12:32
- Dernière connexion du périphérique (Last Arrival Date – valeur 0065) : 03 février 2020 à 12:12:32
- Dernière éjection du périphérique (Last Removal Date – valeur 0066) : 03 février 2020 à 12:44:21
- Dernière mise à jour de l'installation du périphérique (Last Install Date / Update – valeur 0067) : 03 février 2020 à 12:45:00

La concordance entre la date de première insertion et celle de dernière connexion indique que ce périphérique USB n'a été connecté qu'une seule fois au système analysé.

La période d'utilisation du périphérique s'étend donc du 03/02/2020 à 12:12:32 jusqu'à son retrait à 12:44:21, soit une durée d'environ 32 minutes.

Toute action réalisée à l'aide de ce périphérique USB, y compris l'introduction de fichiers ou de programmes malveillants, a nécessairement eu lieu durant cette période.