SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°6
Août 2019

Forensics

2ème partie: Analyse à froid

EvilGNOME

Le nouveau backdoor Linux

CVSS

Evaluer la gravité des vulnérabilités

Ransomwares

Tendance en 2019

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Urgent11

Des vulnérabilités critiques VxWorks

Des chercheurs en sécurité d'Armis, une entreprise spécialisée dans la sécurité IoT, ont découvert 11 vulnérabilités dans VxWorks. Ce dernier est le système d'exploitation en temps réel (RTOS) le plus utilisé, notamment dans les équipements critiques tels que les appareils industriels, médicaux et d'entreprise.

Ces vulnérabilités, surnommées « URGENT / 11 », affectant IP net (la pile TCP / IP de VxWorks). Elles peuvent permettre l'exécution de code à distance sur les périphériques vulnérables et même de contourner les dispositifs de sécurité périmétrique comme les pare-feu ainsi que les solutions NAT.
Les 11 vulnérabilités trouvées sont composées de 6 vulnérabilités critiques pouvant conduire à l'exécution de code à distance :

• CVE-2019-12255 : Pointeur d'urgence TCP = 0 piste vers le dépassement de précision d'entier (integer underflow).

• CVE-2019-12256 : Débordement de pile dans le code d'analyse des options IP du paquet IPv4.

• CVE-2019-12257 : Débordement du tas (heap overflow) dans l'analyse DHCP Offer/Ack dans ipdhcpc.

• CVE-2019-12260 : État de confusion du pointeur d'urgence TCP causé par une option TCP AO inadéquatement constituée.

• CVE-2019-12261 : État de confusion du pointeur d'urgence TCP durant la connexion() à un hôte distant.

• CVE-2019-12263 : État de confusion du pointeur d'urgence TCP causé par une concurrence critique (race condition).

Et 5 vulnérabilités pouvant mener à un déni de service et des fuites d'informations :

• CVE-2019-12258 : DoS de la connexion TCP par l'entremise d'options TCP inadéquatement constituées.

• CVE-2019-12262 : Traitement des réponses ARP inversées non sollicitées (faille de logique).

• CVE-2019-12264 : Faille de logique dans l'attribution IPv4 par le client DHCP ipdhcpc.

• CVE-2019-12259 : DoS par déréférence NULL dans l'analyse IGMP.

• CVE-2019-12265 : Fuite d'information IGMP par l'entremise de rapports spécifiques d'abonnement IGMPv3.

URGENT / 11 menacent tous les périphériques connectés VxWorks actuellement utilisés. Il existe trois scénarios d'attaque, en fonction de l'emplacement du périphérique sur le réseau et de la position de l'attaquant. Le premier scénario d'attaque concerne tout périphérique VxWorks, directement exposé à Internet, tel que pare-feu, modems, routeurs. Le deuxième scénario d'attaque concerne tout périphérique VxWorks situé dans le réseau interne, qui se connecte à Internet via un pare-feu ou une solution NAT : un attaquant intercepte les connexions TCP créées via Internet en utilisant des techniques comme le MITM. Dans le dernier scénario, un attaquant déjà positionné sur le réseau à la suite d'une attaque antérieure peut envoyer des paquets IP capables de prendre le contrôle total des périphériques VxWorks vulnérables dans le réseau local.

Les vulnérabilités d'URGENT / 11 affectent toutes les versions de VxWorks depuis la version 6.5, à l'exception des versions du produit conçues pour la certification, telles que VxWorks 653 et VxWorks Cert Edition. De nouvelles mises à jour ont été fournies et de plus amples informations sont disponibles dans l'alerte de sécurité Wind River publiée dans le centre de sécurité de la société.

Source
https://armis.com/urgent11/

Analyse forensique d'une machine Windows - 2ème partie

Lors d'un incident de sécurité au sein d'un SI, il est nécessaire de comprendre le mode opératoire de l'attaquant afin de retracer ses actions, mais également de pouvoir collecter assez de preuves pour pouvoir porter plainte (criminalité, intrusion, etc.). L'analyse forensique peut être utilisée dans plusieurs cas comme : l'analyse de malwares, la récupération de preuves en vue d'une plainte, les tests d'intrusion ou la récupération de données.

Nous avons consacré un article dans le numéro précedent de notre magazine à présenter l'analyse à chaud d'une machine Windows. Nous allons nous intéresser dans ce numéro à la deuxième approche de l'analyse forensique qui est l'analyse à froid.

Analyse à froid (dead forensics)

Elle consiste à analyser un système éteint. Dans ce cas l'ensemble des données du système sera copié et analysé ultérieurement C'est l'approche la plus complète mais qui nécessite le plus de temps.

L'analyse à froid consiste à analyser l'ensemble du système et de son contenu:

•Les logiciels installés,
•Les fichiers présents sur le disque,
•Les journaux de logs et d'événements, navigation,
•Les informations confidentielles (fichiers protégés par mot de passe, mots de passe enregistrés) etc…

L'analyse à froid permet d'aller beaucoup plus en profondeur lors d'une analyse car elle permet d'accéder à l'ensemble des données d'un disque.

La méthodologie de cette analyse

L'analyse forensique exige de la méthodologie. Il va s'agir de collecter et de préserver les preuves. Il est donc recommandé de suivre un guide des bonnes pratiques afin de pas altérer les données analysées. Un point essentiel de l'analyse forensique est la documentation et l'horodatage des actions effectuées.

4 étapes sont essentielles pour l'analyse à froid:

1. La collecte des preuves
2. L'examen des preuves
3. L'analyse des preuves
4. Le signalement

Ces étapes nécessitent des outils comme Access FTK Imager, OSForensics, Forensic Toolkit ou encore des outils payants comme Encase.

Collecte des preuves

Cette étape consiste à récupérer les données d'une machine dans le but de les analyser, en évitant toute modification du système et des informations elles-mêmes.

a. Copie du disque

Il faut commencer toujours par effectuer une copie bit par bit du disque. Plusieurs outils comme Helix, Dd, encase permettent de le faire.

Il est important de mentionner qu'après la copie du disque, un hash de l'image doit être réalisé afin de pouvoir vérifier l'intégrité de l'image effectuée et que une copie de sauvegarde est recommandée.

b. Montage de l'image

Une fois la copie réalisée, il va falloir monter celle-ci sur un autre poste afin de pouvoir l'analyser. Pour se faire, il existe les outils suivants : Lmdisk14 (émuler un ou plusieurs lecteurs de disques), FTK imager, Encase.

Il peut être parfois intéressant de convertir une image en machine virtuelle afin de pouvoir la démarrer. Pour cela, il existe le logiciel LiveView qui se charge de cette tâche. Il suffit d'indiquer l'emplacement de l'image et cet outil se charge de la convertir en image Vmware. il suffit ensuite de démarrer l'image convertie avec Vmware.

Analyse du disque

Il s'agit d'analyser le disque afin d'extraire des informations pertinentes : identification du système, récupération des fichiers effacés, analyse des logs, récupération d'informations sensibles, etc.

a. identification du disque

La première étape de l'analyse est de déterminer le système d'exploitation utilisé, ces informations sont disponibles sous "c:\Windows".

b. récupération des fichiers effacés

Quand un document est effacé, seule la référence dans l'index du disque dur est modifiée. Le fichier est toujours là, mais inaccessible. Plusieurs outils sont à disposition pour récupérer les fichiers effacés comme Foremost, Dd_rescue, NTFS undelete, Fatback, Sleuth Kit,...

Un disque dur ne dispose pas de fonction d'effacement : une fois une donnée écrite, la seule façon de l'effacer est donc d'écrire d'autres données par-dessus les données existantes. Il existe de nombreux outils permettant un effacement sécurisé des données tel que Eraser, Clean Disk Security, Prevent Restore, CCleaner,..

c. analyse de la base de registre

Le Registre est une véritable mine d'informations pour l'administrateur et l'investigateur. Dans de nombreux cas, le logiciel utilisé par un pirate laisse une empreinte dans le Registre, donnant alors à l'investigateur des indices sur l'incident. La base de registre se présente sous forme de différentes « ruches » (fichiers) qui sont stockées dans :

- C:\Windows\System32\Config
- C:\Document and Settings\#utilisateur#\NTUSER.dat
- C:\Windows\repair

En réalité, la base du registre est divisée en deux parties: HKEY_LOCAL_MACHINE et HKEY_USERS, souvent écrites en abrégé : HKLM et HKU

Les trois autres branches principales sont des liens vers des sous répertoires de ces deux clefs.

• HKEY_CLASSES_ROOT: Il s'agit d'un lien vers HKEY_LOCAL_MACHINE\SOFTWARE\Classes et contient des liens entre les applications et les types de fichiers ainsi que des informations sur OLE.

• HKEY_CURRENT_USER: Il s'agit d'un lien vers HKEY_USERS\<SID of User> et contient des informations sur les utilisateurs actuellement connectés (environnement, connexions réseaux, imprimantes etc.)

• HKEY_USERS: Contient des informations sur les profils utilisateurs actuellement chargés, y compris "defaut" qui est le profil utilisateur par défaut.

• HKEY_CURRENT_CONFIG: Il s'agit d'un lien vers HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current et contient des informations sur la configuration courante.

• HKEY_LOCAL_MACHINE: Contient les informations sur la station de travail, le matériel qu'on y trouve, les logiciels installés, et les préférences locales applicables à tout usager se branchant sur cet ordinateur. Ses principales sous-clés sont:
Hardware: principalement pour des informations sur la communication par port série
Network: informations propres au réseau auquel l'usager est branché;
Security: paramètres de sécurité du réseau
Software:certains paramètres logiciels
System: informations quant au lancement du système, à ses périphériques et aux paramètres du système d'exploitation en tant que tel.

• HKEY_USERS Contient les préférences individuelles de chaque usager pour la station de travail en question, chaque usager étant représenté par une sous-clé SID (Security Identification) se retrouvant sous la branche principale

Pour récupérer les sous clés du Hive HKLM, nous allons utiliser la commande reg.exe pour gérer le registre : https://windows.developpez.com/cours/ligne-commande/?page=page_17

• SAM Security Account Manager : base de données des comptes locaux sur windows
reg save HKLM\sam c:\sam
reg save HKLM\security c:\security

• SOFTWARE: contient des paramètres relatifs aux logiciels inclut dans windows
reg save HKLM\software c:\software

• SYSTEM : contient des paramètres matériel ainsi que des informations sur le système, tels que les pilotes ou la mémoire système.
reg save HKLM\system c:\system

• HARDWARE: cette sous clé comprend les informations sur la configuration matérielle, telles qu'elles sont détectées par Windows au démarrage.
reg save HKLM\hardware c:\hardware

Pour analyser une base de registre offline, il existe de nombreux outils gratuits : Autoruns de sysinternals, RegRipper, Rip, RipXP, RegSlack, Mitec Windows Registry.
Dans cet exemple, nous allons analyser le fichier NTUSER.dat avec l'outil RegRipper

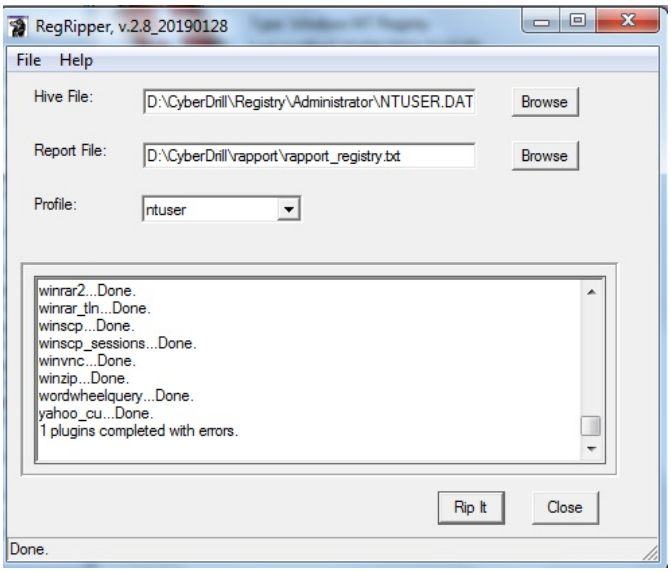


Figure 1: Analyse de la base de registre avec RegRipper

Cette analyse permet de récupérer par exemple tous les fichiers qui ont été exécutés sur la machine

```
MUICache
Software\Microsoft\Windows\ShellNoRoam\MUICache
LastWrite Time Sun Jul 20 20:38:59 2008 (UTC)
      C:\WINDOWS\system32\igfxtray.exe (igfxTray Module)
      C:\WINDOWS\system32\hkcmd.exe (hkcmd Module)
      C:\WINDOWS\system32\igfxpers.exe (persistence Module)
      D:\Program Files\Adobe\Reader 8.0\Reader\Reader_sl.exe
(Adobe Acrobat SpeedLauncher)
      C:\Program Files\Java\jre1.6.0_03\bin\jusched.exe (Java(TM)
Platform SE binary)
      C:\WINDOWS\RTHDCPL.EXE (Realtek HD Audio Control Panel)
      C:\WINDOWS\ALCMTR.EXE (Realtek Azalia Audio - Event Monitor)
      C:\Program Files\Asus\EeePC ACPI\AsTray.exe (Eee PC Tray
Utility)
      C:\Program Files\Asus\EeePC ACPI\AsAcpiSvr.exe (Asus Eee PC
ACPI Service)
      C:\Program Files\Elantech\ETDCtrl.exe (ETD Ware TSR |
Enhancements)
      C:\sysprep\factory.exe (Factory pre-installation utility)
```

Figure 2: Fichiers exécutés sur la machine

Elle peut aussi nous donner plusieurs informations comme la version de windows installée, les points de montage pour savoir si un disque dur chiffré a été monté, les documents recement ouverts, les programmes qui se lancent avec windows, paramètres du proxy

```
MountPoints2
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
LastWrite Time Mon Mar 31 11:38:45 2014 (UTC)

Remote Drives:

Volumes:
Wed Mar 26 00:05:50 2014 (UTC)
  {06b1eac2-b430-11e3-9ad3-f32a1fee9128}
Tue Mar 25 09:53:10 2014 (UTC)
  {1b758ac1-b3fe-11e3-a907-806e6f6e6963}
Tue Mar 25 09:42:19 2014 (UTC)
  {1b758ac0-b3fe-11e3-a907-806e6f6e6963}
  {1b758ac4-b3fe-11e3-a907-806e6f6e6963}

Drives:
Tue Mar 25 15:14:29 2014 (UTC) - E
Tue Mar 25 09:42:16 2014 (UTC) - A,C,D

Unique MAC Addresses:
80:6E:6F:6E:69:63
F3:2A:1F:EE:91:28
```

Figure 3: Exemple de volumes montés sur le poste

La liste des documents récement ouverts peut aussi être consultée, elle se trouve sous NTUSER\Software\Microsoft\Windows\CUrrentVersion\Explorer\RecentDocs

```
RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Thu Apr 10 21:01:28 2014 (UTC)
  1 = Local Disk (C:)
  0 = DB-Test02.csv
  7 = DB-Test01.csv
  5 = W3SVC1
  6 = ex140325.log
  4 = ex140326.log
  3 = MSSQL
  2 = readme.txt
```

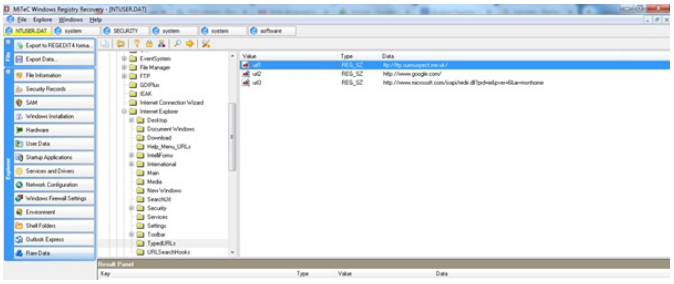
Figure 4: Liste des documents récement ouverts

La liste des adresses tapées dans Internet Explorer est aussi accessible

```
TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Thu Apr 10 21:04:30 2014 (UTC)
  url1 -> ftp://ftp.suesuspect.me.uk/
  url2 -> http://www.google.com/
  url3 -> http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
----------------------------------------
```

Figure 5: La liste des adresses tapées dans Internet Explorer

Nous pouvons récupérer la même liste avec L'outil MiTec Windows Registry Recovery



d. analyse des fichiers Log / évènements

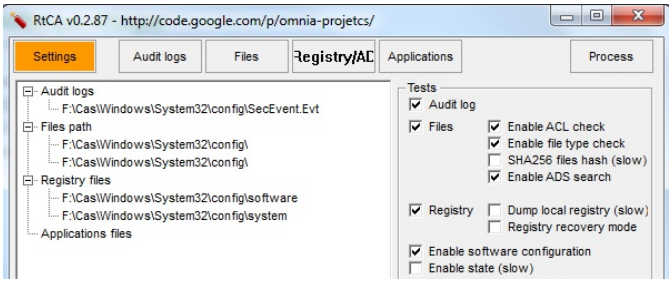
Tout comme la base de registre, les journaux d'enregistrement peuvent être une source d'informations très riches. Ceux-ci localisés dans le répertoire « Windows\System32\Config », sont activés par défaut sur la plupart des systèmes Windows (application, sécurité, system).

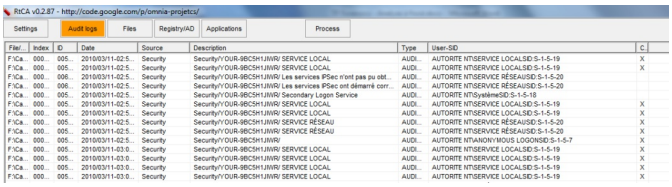
En analysant ces fichiers, on peut trouver rapidement un évènement répétitif (tentatives multiples de login par exemple qui peut traduire une tentative d'intrusion ou un malware par exemple) qui peut donner des pistes.

Concernant l'analyse des fichiers logs, événements, il existe :

- Log Parser(outil qui permet un accès universel aux fichiers journaux)
- Evtrpt.pl (script perl permettant d'établir des statistiques)
- RtCA (outil d'aide aux analyses)

Avec l'outil RtCA, on peut analyser de manière simple et détaillée un fichier log.





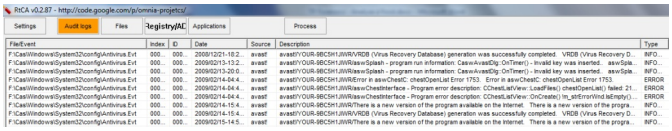


Figure 6: Analyse de fichier log avec l'outil rtCA

e. analyse des traces de connexion Internet

Il peut être judicieux d'analyser les navigations web effectuées à partir du poste. Pour cela, il existe de nombreux utilitaires :

- ProDiscover
- NetAnalysis
- Web Historian
- IEHistoryView, etc

En général ces outils analysent le fichier « index.dat » présents dans « document and settings\#user#\Cookies »

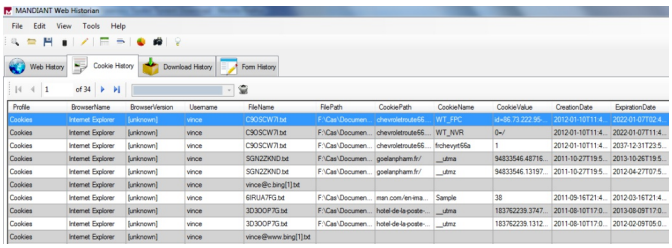


Figure 7: Exemple d'analyse web avec Web Historian

f. recherche de fichiers

Il peut être parfois fastidieux d'effectuer des recherches de fichiers sur un disque dur, de par la multitude des fichiers existants. Il existe des outils conçus pour cette tâche. Parmi eux, nous pouvons citer :

- Access Forensic Toolkit
- OSForensics
- Scalpel
- Sleuth Kit

Par exemple avec l'outil Forensic Toolkit, nous pouvons facilement créer un index des fichiers, ce qui permet d'avoir un tri selon le type de fichier et leur extension.

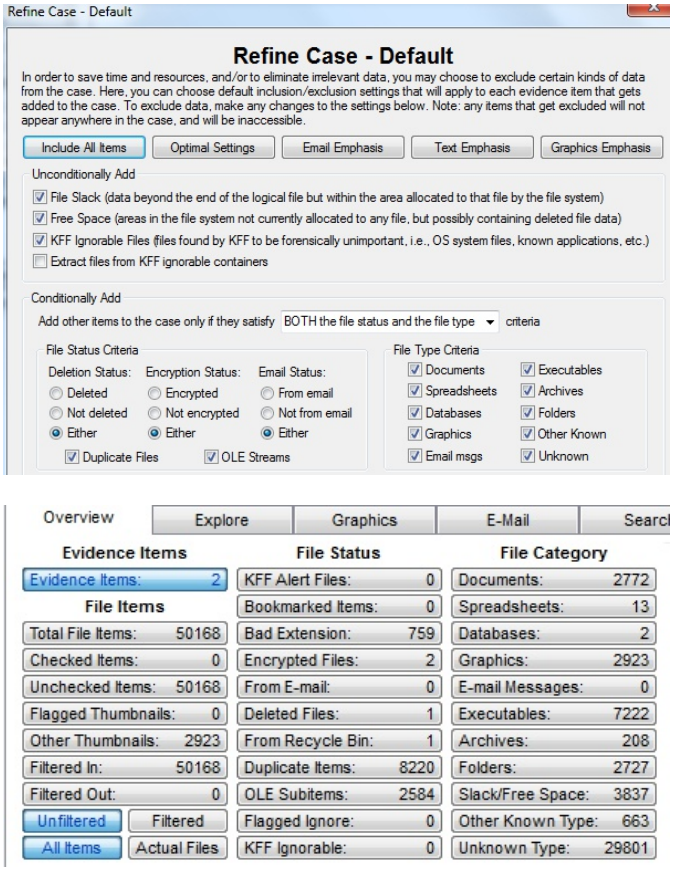


Figure 8: Création d'un index avec Forensic Toolkit

g. récupération d'informations sensibles

La récupération d'informations sensibles est une partie des plus intéressantes de l'analyse forensique, en effet, nous pouvons récupérer les comptes utilisateurs de la machine et les mots de passe associés, les mots de passe enregistrés dans les navigateurs ou encore utilisés pour des logiciels tiers.

Extraction de comptes utilisateur de la machine

La base de données du gestionnaire des comptes de sécurité (SAM, Security Accounts Manager) de Microsoft Windows stocke des copies hachées des mots de passe des utilisateurs. Cette base de données est chiffrée avec une clé système stockée localement. Pour conserver la base de données SAM sécurisée, Windows requiert que les hachages des mots de passe soient chiffrés. Windows empêche l'utilisation de hachages de mots de passe stockés non chiffrés.

il existe de nombreux outils comme pwdump ou cain pour extraire les compte utilisateur. Cain propose des méthodes pour casser le mot de passe chiffrés. Un simple clic droit sur le compte permet de choisir sa méthode.

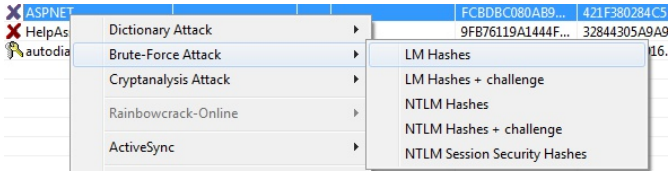


Figure 9: Crack des mots de passe à l'aide de l'outil cain

Extraction des mots de passe des navigateurs

Il est possible de scanner une machine afin d'y récupérer les mots de passe des différents navigateurs. Plusieurs outils sont disponibles à cet effet, comme l'outil PasswordFox qui permet d'extraire les mots de passe Firefox localement ou situé sur un disque externe.

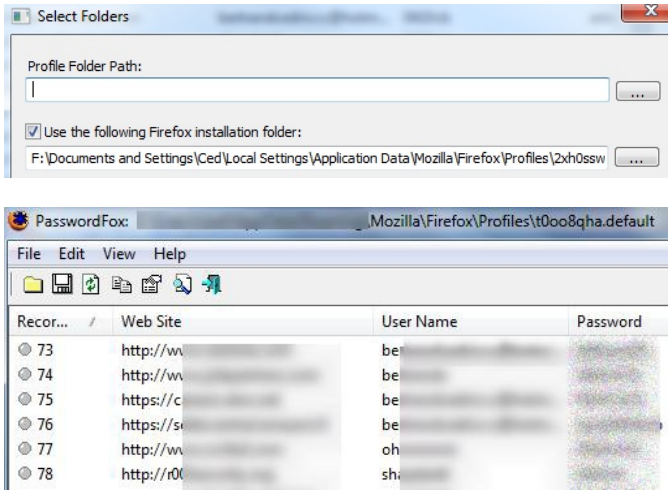


Figure 10: Récupération des mots de passe stockés par Firefox

Extraction des secrets LSA

LSA pour Local Security Autority est un espace de stockage des informations tel que les mots de passe utilisés pour démarrer certains services. Pour extraire les mots de passe LSA, on peut utiliser l'outil LSASecretsView de Nirsoft. Cet outil permet aussi de retrouver les mots de passe d'une machine externe.

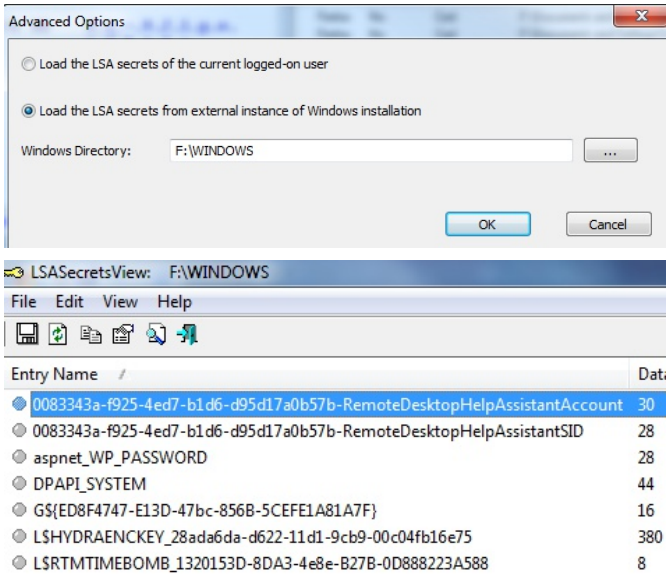


Figure 11: Extraction des secrets LSA

Recherche de fichiers protégés

On appelle par « fichier protégé », les fichiers qui nécessitent un mot de passe (exemple : fichier zip protégé par un mot de passe). Pour rechercher ce type de fichiers sur un poste, nous pouvons par exemple utiliser l'outil « Password Recovery Toolkit Forensic». C'est un outil offrant de nombreuses fonctions dont le déchiffrement de conteneurs truecrypt, la récupération de mots de passe, le crackage de fichiers protégés, etc. Une fois qu'un fichier protégé a été trouvé, il est aussi possible de chercher le mot de passe.

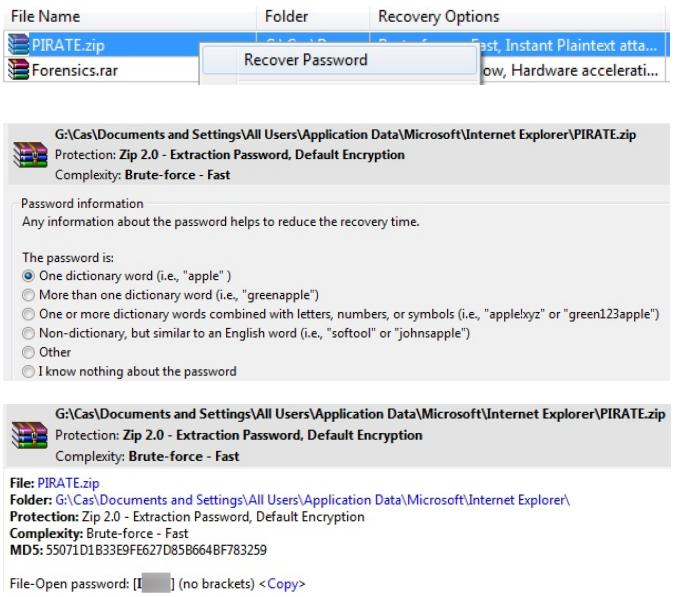


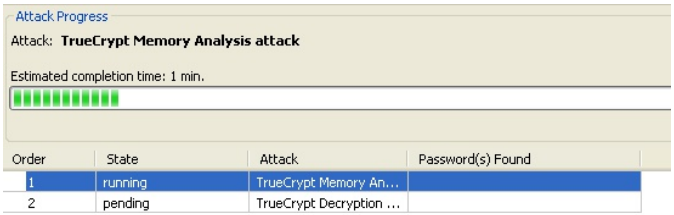
Figure 12: Crack du mot de passe d'un fichier protégé

Déchifrement de containers TrueCrypt

Une option intéressante de "Password Recovery Toolkit Forensic" est la possibilité de lancer une attaque pour trouver les mots de passe de containers truecrypt. TrueCrypt est un outil permettant de créer des disques durs virtuels chiffrés.

Une fois l'emplacement du container TrueCrypt indiqué, une attaque de recherche de mots de passe est lancée. Par contre la vitesse de calcul est tellement basse que sans indication du mot de passe, il est illusoire d'espérer le trouver.

Néanmoins une option de l'outil est de permettre de rechercher la trace de clé de chiffrement aes dans la mémoire vive, ce qui permet le déchiffrement rapide d'un container TrueCrypt.



Volume image file: secret_truecrypt
Folder: C:\Documents and Settings\Ced\Mes documents\
Physical memory image file: memdump_xp.mem
Folder: C:\Documents and Settings\Ced\Mes documents\Capture\
Protection: TrueCrypt Volume - Open Password, TrueCrypt AES Encryption
Complexity: Instant Unprotection

Unprotected file: secret_truecrypt-decrypted

```
C:\Tools_hpvc>strings secret_truecrypt-decrypted

Strings v2.42
Copyright (C) 1999-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

CRIME
PACK 3
CRIMEP^10
```

Récupération du mot de passe VNC

Si le logiciel VNC est installé sur le poste analysé, il est possible d'extraire la clé de registre correspondante et de retrouver le mot de passe. Pour cela, nous pouvons utiliser l'outil vncpwdump.

```
C:\Documents and Settings\Ced\Mes documents\vncpwdump-win32-1_0_6>vncpwdump -r C
:\\tmp\\NTUSER.dat

VNCPwdump v.1.0.6 by patrik@cqure.net
-----------------------------------

Password: password
```

Figure 13: Récupération du mot de passe VNC

Sources

https://repo.zenk-security.com/Forensic/Acquisition%20de%20preuves%20et%20analyse%20a%20froid%20d%20un%20systeme%20sous%20Windows.pdf

https://repo.zenk-security.com/Forensic/Acquisition%20de%20preuves%20et%20analyse%20a%20froid%20d%20un%20systeme%20sous%20Windows.pdf

https://www.hackersrepublic.org/forensic-corner/registre-windows-explications

EvilGnome : Nouveau Backdoor qui espionne les utilisateurs de Linux !

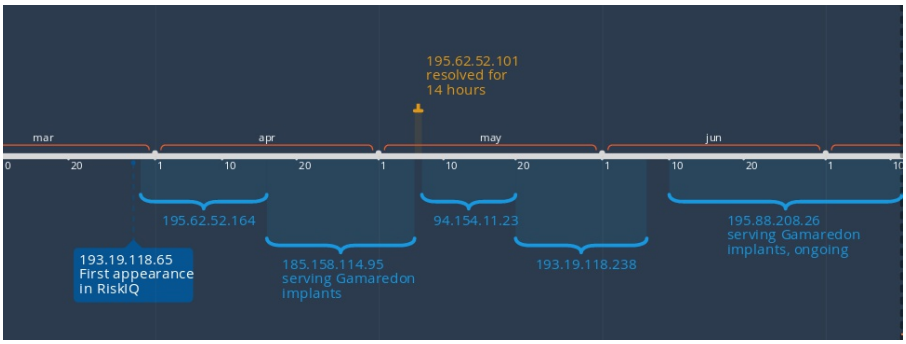
EvilGnome est un logiciel espion, il est conçu pour espionner les utilisateurs des systèmes Linux. Les fonctionnalités de EvilGnome incluent des captures d'écran de bureau, le vol de fichiers et de capturer un enregistrement audio depuis le microphone de l'utilisateur.

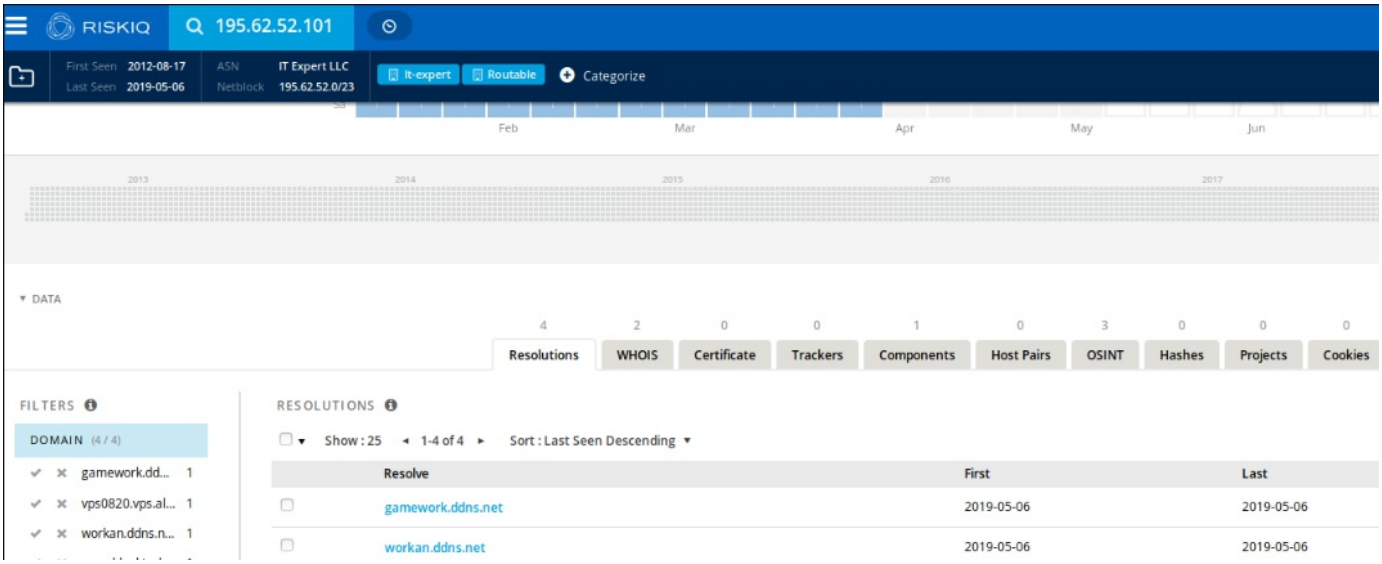
Le spyware « EvilGnome » cible la communauté relativement petite qui utilise le système d'exploitation Linux sur leur ordinateur portable par rapport à la majorité qui utilisent des systèmes d'exploitation Microsoft.

Analyse de SPYWARE
Hébergement
Les opérateurs du spayware EvilGnome utilisent un fournisseur d'hébergement utilisé depuis des années par le groupe Gamaredon (groupe russe, actif depuis 2013 et a ciblé des personnes susceptibles d'être impliquées dans le gouvernement ukrainien, infecte les victimes à l'aide de pièces jointes malveillantes transmises via des techniques de phishing.)

L'adresse IP de EvilGnome 195.62.52.101 a été résolue aux domaines gamework.ddns.net et workan.ddns.net, associés au groupe Gamaredon.

Historique du domaine gamework.ddns.net
Les résultats montrent qu'EvilGnome utilise une adresse IP contrôlée par le groupe Gamaredon il y a deux mois





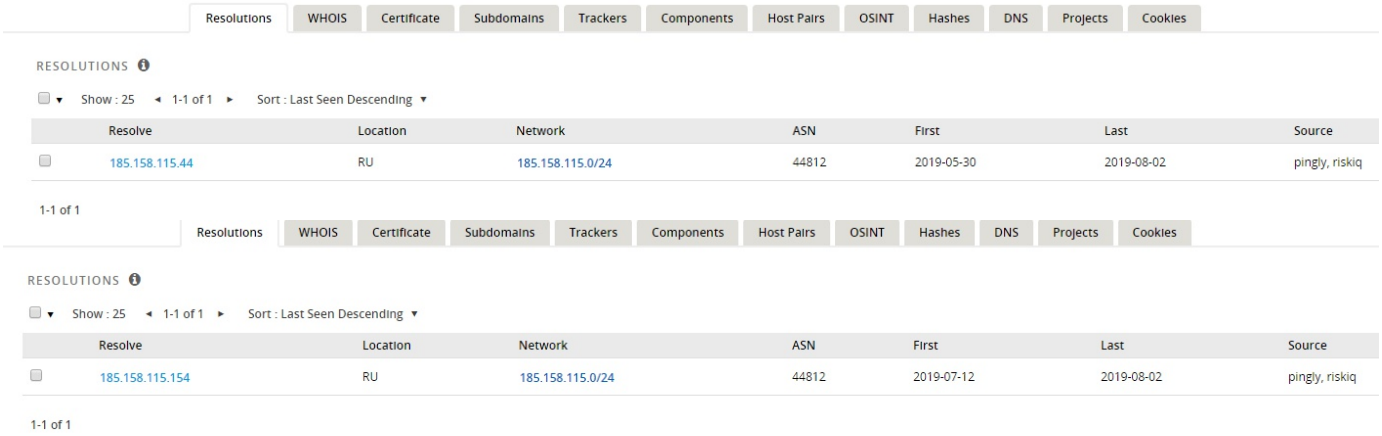
Infrastructure EvilGnome
Une enquête faite par INTEZER montre que le spyware EvilGnome utilise le port 3436 pour se connecter aux serveurs de commande et contrôle (C2) via SSH.

```
;; ANSWER SECTION:
rnbo-ua.ddns.net.       3       IN      A       85.143.219.52

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Jul 14 14:22:55 IDT 2019
;; MSG SIZE  rcvd: 61

paul@p:~$ nc 85.143.219.52 3436
SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6
^C
paul@p:~$ nc 195.62.52.101 3436
SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u6
```

INTEZER se charge à la recherche de cette empreinte réseau chez le fournisseur d'hôte d'EvilGnome et a identifié deux serveurs supplémentaires avec des noms de domaine similaires au modèle de nommage des domaines Gamaredon (utilisation de .space TTLD et de ddns):

- 185.158.115.44 => kotl.space
- 185.158.115.154 => clsass.ddns.net

Résultat de recherche sur RISKIQ:



Analyse technique
EvilGnome est un véritable logiciel espion qui se fait passer pour une extension GNOME.

Ce spyware est livré sous la forme d'un script shell d'archive self-extractable créé avec « makeself », un petit script shell qui génère une archive .tar compressé. Il persiste sur le système cible à l'aide de crontab, un outil similaire au planificateur de tâches de Windows, et envoie les données volées à un serveur distant contrôlé par un attaquant.

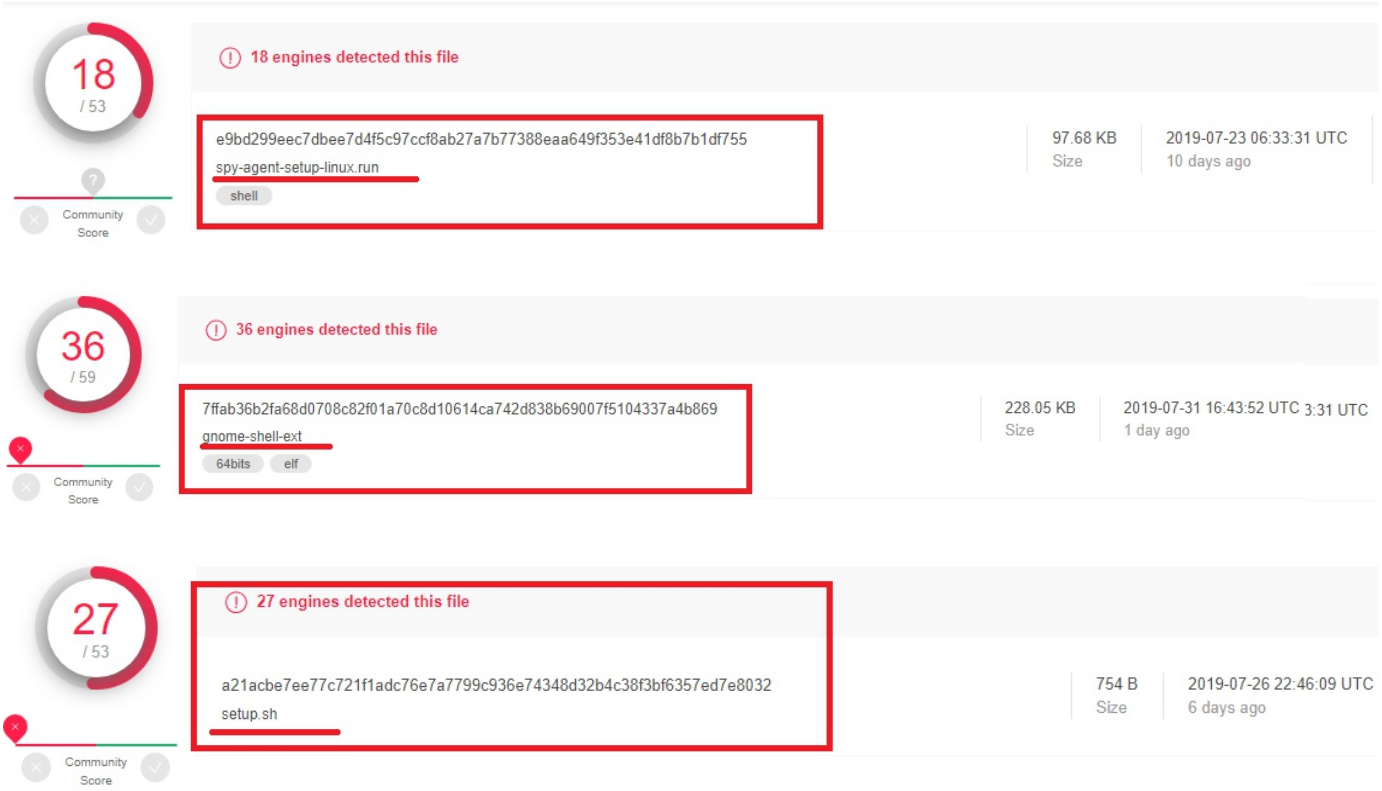
```
paul@u:~$ ./spy-agent-setup-linux.run --list
Target directory: spy-agent
drwxr-xr-x shurik/shurik     0 2019-07-04 02:51 ./
-rwxr-xr-x shurik/shurik 233528 2019-07-04 02:51 ./gnome-shell-ext
-rwxr-xr-x shurik/shurik    754 2019-07-04 02:25 ./setup.sh
-rw-r--r-- shurik/shurik     56 2019-07-04 02:51 ./rtp.dat
-rwxr-xr-x shurik/shurik    244 2019-07-04 02:25 ./gnome-shell-ext.sh
```

Le script installe le logiciel malveillant dans ~/.cache/gnome-software/gnome-shell-extensions/ pour le déguiser en une extension du shell Gnome. De plus, pour gagner en persistance, gnome-shell-ext.sh est enregistré pour s'exécuter à chaque fois dans crontab.

L'archive contient quatre fichiers:

1. gnome-shell-ext - l'exécutable de l'agent espion
2. setup.sh - le script d'installation exécuté par makeelf après décompression
3. rtp.dat - fichier de configuration pour gnome-shell-ext
4. gnome-shell-ext.sh - vérifie si gnome-shell-ext est déjà en cours d'exécution sinon, l'exécute

```
paul@u:~$ ./spy-agent-setup-linux.run --info
Identification: setup files...
Target directory: spy-agent
Uncompressed size: 248 KB
Compression: gzip
Date of packaging: Thu Jul 4 12:51:00 MSK 2019
Built with Makeself version 2.3.0 on
Build command was: /usr/bin/makeself \
    "--notemp" \
    "/media/data/work/Rostov/spy/spy-source/spy-agent/../../spy-build/Linux/spy-agent" \
    "/media/data/work/Rostov/spy/spy-source/spy-agent/../../spy-binary/Linux/spy-agent-setup-linux.run" \
    "setup files..." \
    "./setup.sh"
Script run after extraction:
    ./setup.sh
directory spy-agent is permanent
```



Modules EvilGnome

L'agent d'espionnage du spyware EvilGnome contient cinq modules malveillants appelés "Shooters", comme expliqué ci-dessous :

• ShooterSound - ce module utilise PulseAudio pour capturer l'audio du microphone de l'utilisateur et télécharger les données sur le serveur de commande et contrôle de l'opérateur.

• ShooterImage - ce module utilise la bibliothèque open source Cairo pour capturer des captures d'écran et les télécharger sur le serveur C&C. Cela se fait en ouvrant une connexion au serveur d'affichage XOrg, qui est le backend du bureau Gnome.

• ShooterFile - ce module utilise une liste de filtres pour analyser le système de fichiers des nouveaux fichiers créés et les télécharger sur le serveur C&C.

• ShooterPing - le module reçoit de nouvelles commandes du serveur C&C, telles que télécharger et exécuter de nouveaux fichiers, définir de nouveaux filtres pour l'analyse des fichiers, télécharger et définir une nouvelle configuration d'exécution

• ShooterKey - ce module est non implémenté et inutilisé, ce qui est probablement un module de keylogging inachevé.

Comment détecter les logiciels malveillants EvilGnome?

Pour vérifier si votre système Linux est infecté par le logiciel espion EvilGnome, vous pouvez rechercher l'exécutable "gnome-shell-ext" dans le répertoire "~/.cache/gnome-software/gnome-shell-extensions".

IOCs

SHA-256

• a21acbe7ee77c721f1adc76e7a7799c936e74348d32b4c38f3bf6357ed7e8032
• 82b69954410c83315dfe769eed4b6cfc7d11f0f62e26ff546542e35dcd7106b7
• 7ffab36b2fa68d0708c82f01a70c8d10614ca742d838b69007f5104337a4b869

IP

• 195.62.52.101
• 185.158.115.44
• 185.158.115.154

Domaines

• clsass.ddns.net
• gamework.ddns.net
• kotl.space
• workan.ddns.net

RECOMMENDATIONS

• Assurez-vous que le logiciel antivirus et les fichiers associés sont à jour,

• Vérifier la légitimité de toutes les pièces jointes non sollicitées - supprimé sans ouvrir si vous ne pouvez pas valider,

• Rechercher les signes existants des IoCs indiqués dans votre environnement,

• Bloquez tous les IoCs basés sur les URL et IP au niveau du pare-feu, des IDS, des passerelles Web, des routeurs ou autres périphériques basés sur un périmètre.

Sources

https://www.intezer.com/blog-evilgnome-rare-malware-spying-on-linux-desktop-users/

Tendance des Ransomwares en 2019

L'attaque par ransomware est considérée comme l'une des plus grandes menaces de logiciels malveillants dans le monde, en effet les entreprises ne cessent de payer des millions de dollars afin de dévérouiller leurs fichiers cryptés.

ERIS ransomware

Le ransomware ERIS a été découvert en mai 2019. Les attaquants utilisent le kit d'exploitation RIG pour distribuer le ransomware. Le chercheur sur le kit d'exploitation, nao_sec, a découvert qu'il était distribué par le biais d'une campagne de publicité malveillante utilisant le kit d'exploitation RIG.

Le kit d'exploitation RIG recherche des vulnérabilités sur quelques ordinateurs, exploite une vulnérabilité de Shockwave (SWF) dans le navigateur de la victime et installe le ransomware à l'insu de l'utilisateur.

Lors de la compromission de la machine, le ransomware chiffre les fichiers et les ajoute avec l'extension .ERIS. Chaque fichier crypté contient un marqueur de fichier _FLAG_ENCRYPTED_ à la fin du fichier comme preuve qu'il a été crypté. En plus, le ransomware laisse une note de rançon nommée @ LISEZ MOI POUR RÉCUPÉRER DES FICHIERS @ .txt, qui demande à l'utilisateur victime de contacter Limaooo@cock.li pour obtenir des instructions de paiement. Malheureusement, il n'existe actuellement aucun moyen de déchiffrer gratuitement les fichiers cryptés par ERIS.

Source :
https://medium.com/cyber-journal/-newly-discovered-eris-ransomware-leverages-rig-exploit-kit-for-propagation-c87ce38c32c9

Sodin ransomware

Sodinokibi (également connu sous le nom de Sodinokibi et Revil) est un ransomware qui a été repérée à la fin du mois de mai 2019, lorsque plusieurs machines en Allemagne étaient infectées par des documents malveillants contenant de macros.

Sodinokibi est similaire à GandCrab dans la conception. Il utilise des techniques anti-débogages et d'obfuscation, utilise les algorithmes SHA3-256 et AES-256 en mode CFB pour chiffrer les fichiers, remplace l'arrière-plan du bureau de la machine par une image bleu foncé et crée un fichier de note de rançon. En plus, il supprime les « shadow copies », ce qui complique encore la récupération des données. Il désactive aussi la fonction de réparation de démarrage de Windows et peut modifier les entrées de registre ou même les fonctionnalités de sécurité. C'est pour cela que plusieurs experts en sécurité doutent que ce ransomware a été créé par les mêmes développeurs qui ont introduit le ransomware GandCrab.

Sodinokibi utilise diverses méthodes d'infection. Ils exploitent plusieurs vulnérabilités telles que la vulnérabilité WebLogic, RDP brute-force, la vulnérabilité CVE-2019-3396 ainsi que la vulnérabilité CVE-2018-8453.

Source :
https://www.sangfor.com/source/blog-network-security/1249.html

Loocipher ransomware

Loocipher est un nouveau ransomware qui a été découvert récemment. Il était propagé à l'aide d'un fichier contenant une macro simple et sans obfuscation.Une fois exécuté, il lance le cryptage de tous les fichiers de la victime, à l'exception des dossiers système pour permettre à l'utilisateur de se connecter à son PC pour terminer le paiement de rançon.

Selon FortiGuard Labs, leur analystes ont trouvé plusieurs codes de chiffrement dans le corps du logiciel malveillant, tels que DES, AES et ECC / ECDSA (cryptographie à courbe elliptique ou algorithme de signature numérique à courbe elliptique).Mais en le testant, seul le mode AES-128 ECB a été utilisé pour chiffrer les fichiers. Ils pensent que ces codes de cryptage sont là pour une utilisation future.

Lors de l'infection, Loocipher crée un fichier avec le nom d'origine du fichier en cours de chiffrement, puis ajoute une extension .lcphr au nom. Ce nouveau fichier contient le contenu du fichier original mais chiffré avec l'algorithme AES-128 ECB à l'aide de la clé aléatoire générée de 16 octets, en laissant le fichier d'origine sous la forme d'un fichier de 0 octet.

Loocipher crée aussi une note de rançon qui contient un montant de rançon (300 €/330 USD), une adresse bitcoin pour envoyer le paiement et des instructions pour effectuer un paiement. En plus, une fenêtre Loocipher Decryptor sera affichée. Ce programme permet de récupérer vos fichiers si un paiement a été effectué.

Enfin, le ransomware envoie la clé de cryptage à un serveur C2 (commande et contrôle) ou on stocke les clés dans une base de données. Comme AES est un algorithme à clé symétrique, la récupération de la clé permet de restaurer tous les fichiers cryptés. La clé sera envoyée à C2 via HTTP sous forme de paramètre GET («k =»), mais elle est évidemment obscurcie. Les chercheurs Fortinet indiquent que la récupération de la clé se fait soit avec l'interception du trafic réseau soit avec la mémoire de processus en cours d'exécution.

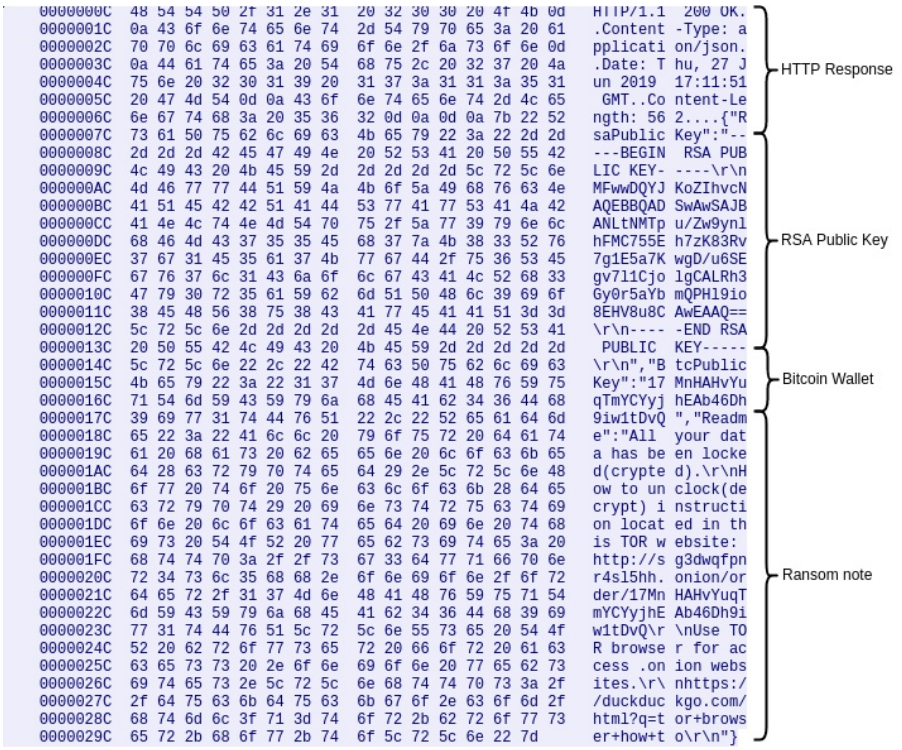
En se basant sur ce qui précède, Cybaze-Yoroi ZLab a publié un outil capable de procéder au déchiffrement de tous les fichiers chiffrés. L'outil nécessite que le processus loocipher soit actif.
L'outil est disponible sur GitHub à l'URL suivante:
https://github.com/ZLab-Cybaze-Yoroi/LooCipher_Decryption_Tool
Quelques jours après, Emsisoft propose également son propre decrypteur contre ce ransomware. Cettte solution nécessite une connexion Internet et l'accès à une paire de fichiers composée d'un fichier crypté et de la version d'origine non cryptée du fichier crypté pour reconstituer les clés de cryptage nécessaires au décryptage du reste de vos données.Cet outil est disponible à l'URL suivante :

https://www.emsisoft.com/decrypter/-loocipher

Source
https://www.fortinet.com/blog/threat-research/loocipher-can-encrypted-files-be-recovered.html
https://blog.yoroi.company/announcement/loocipher-ransomware-decryptor-released-for-free/

QNAPCrypt ransomware
Ces dernières années, plusieurs analystes de la sécurité ont signalé différentes vulnérabilités liées aux produits QNAP NAS. Bien que la société ait essayé de les corriger, elle a eu du mal à éviter le nouveau ransomware appelé «eCh0raix» ou bien « QNAPCrypt ».

Découvert par des chercheurs de deux sociétés de sécurité distinctes, Intezer et Anomali, la nouvelle famille de ransomwares cible les systèmes de stockage de fichiers (serveurs NAS) basés sur Linux via des attaques par force brute, où des informations d'identification SSH faibles seraient exploitées par des pirates pour s'infiltrer dans les réseaux de l'entreprise.
Surnommé "QNAPCrypt" par Intezer et "eCh0raix" par Anomali, le nouveau ransomware est écrit dans le langage de programmation Go.



L'équipe de détection de menaces d'Anomali a été la première à détecter des attaques d'un ransomware sur les machines QNAP NAS. Selon Joakim Kennedy, responsable de la cyber-menace d'Anomali, le ransomware est accompagné d'une note de demande de rançon à la victime, affirmant que leurs données ont été chiffrées. Pour le déchiffrer, les victimes doivent se rendre sur un site Web avec un RPT pour effectuer le paiement en Bitcoins.

Chez Intezer, les analystes ont confirmé que lors de la compromission de la victime, le logiciel malveillant demande au serveur de commande et de contrôle (C & C) une adresse de « bitcoin wallet » et une clé RSA publique avant le cryptage de fichier.

A l'aide de la clé publique RSA, une séquence aléatoire d'octets sera chiffrée. Cette clé cryptée sera encodée en base64 et écrite à la fin du ransom note. Ensuite, le ransomware chiffre les fichiers de la machine infectée à l'aide d'AES CFB avec la clé chiffrée dérivée et ajoute l'extension .encrypted au nom du fichier crypté, en évitant de chiffrer la ransomnote créée.
L'équipe d'Intezer a approfondi sa recherche sur QNAPCrypt et son fonctionnement. Ils ont découvert deux défauts de conception majeurs dans l'infrastructure contre ce ransomware : Premièrement, la liste des « bitcoin wallets » a été créée à l'avance et était statique. Par conséquent, il ne crée pas un nouveau « wallet » pour chaque nouvelle victime en temps réel, mais extrait une adresse de portefeuille d'une liste fixe prédéterminée.

Deuxièmement, une fois que tous les «wallets »sont attribués (ou envoyés), le ransomware ne peut plus poursuivre son opération malveillante sur la machine de la victime.

GandCrab ransomware
Nous avons parlé dans les derniers numéros de notre magazine du fameux ransomware GandCrab.
Depuis mars 2019, ce malware a engendré des variantes distinctes (v1,v2,v3,v4,v4.1,v5,v5.1,v5.2) dont les 8 premières versions sont uniquement déchiffrables. Récemment, Bitdefender a publié un décrypteur gratuit prenant en charge la dernière version v5.2 afin que les victimes puissent restaurer leurs données précieuses.

Le ransomware GandCrab V5.2 cible toutes les versions de Windows, y compris Windows 7, Windows 8.1 et Windows 10.Il crypte les documents personnels de la victime à l'aide de la clé RSA-2048 (algorithme de cryptage AES CBC 256 bits), puis affiche un message proposant de décrypter les données en payant entre 1 200 $ et 2 400 $, soit en Bitcoin soit en DASH. Les instructions sont décrites dans un fichier ID-DECRYPT.txt ou ID-DECRYPT.html, placé sur le bureau de la victime.

GandCrab V5.2 ransomware recherche les fichiers avec certaines extensions de fichier à chiffrer et modifie le nom de chaque fichier crypté au format suivant: [nom du fichier] .XYZLMNO.
Le 17 juin 2019, en collaboration avec Europol, le FBI, NoMoreRansom et Bitdefender, ont publié un outil de décryptage pour les fichiers chiffrés avec les versions 1, 4 et 5 à 5.2 de GandCrab.

Cet outil est disponible sur:
https://www.nomoreransom.org.

RECOMMENDATIONS

• Sauvegarder vos données sensibles sur des disques durs externes et n'oublier pas de les débrancher après la fin de l'opération de sauvegarde ;

• Créer, périodiquement, des points de restauration pour récupérer les fichiers système en cas d'infection; et veiller à les sauvegarder sur un support externe ;

• Vérifier l'authenticité et la fiabilité des expéditeurs avant la lecture de chaque message reçu par e-mail ou sur vos réseaux sociaux (Facebook, Twitter, etc..). En cas de doute, il ne faut ni répondre ni cliquer sur les liens ou les images qu'il contient ;

• Pour les utilisateurs d'Outlook, on vous conseille de désactiver les générateurs d'aperçus de pièces jointes ;

• Vérifier tous les messages portant des pièces jointes du type:

- .js (Javascript),
- .jar (java),
- .bat(Batch),
- .exe (fichier exécutable),
- .cpl (Control Panel),
- .scr (Screen saver),
- .com (COM file),
- .pif (Program Information File),
- .vbs (Visual Basic Script).

• Scanner immédiatement par votre solution antivirale chaque périphérique USB inséré dans votre machine et aussi chaque fichier téléchargé ;

• Vérifier si les connexions de bureau à distance sont désactivées.

POUR QUI ?
Pentesteur, Auditeur

POUR QUOI FAIRE ?
Evaluation des vulnérabilités

CVSS pour évaluer la gravité des vulnérabilités (1ère partie)

Comment évaluer la gravité des vulnérabilités

Si vous avez déjà travaillé sur l'un des outils d'analyse de vulnérabilités tels que Nessus ou OpenVAS, vous allez remarquer certainement que les rapports produits par ces outils donnent une évaluation des failles dans quatre évaluations (critiques, élevée, moyenne, faible), qui sont stockées dans les informations relatives à chacune d'elles à l'avance. Les évaluations sont calculées à l'aide de critères précis utilisés par le système d'évaluation standardisé de la criticité des vulnérabilités « Common Vulnerability Scoring System ». De ce fait, ces évaluations indiquent s'il s'agit d'une faille grave ou d'une faille à faible risque.

Un modèle suivi par des entreprises, appelé « Common Vulnerability Scoring System », est utilisé pour évaluer les vulnérabilités sous de nombreux aspects qui seront abordés dans cet article.

CVSS a été créé par FIRST et en est actuellement à la troisième version. Il est largement utilisé par les entreprises (qu'il s'agisse des entreprises de sécurité qui effectuent des recherches sur la sécurité de l'information ou de grandes sociétés qui ont détecté des failles dans leurs systèmes) afin d'évaluer les vulnérabilités.

Le besoin de CVSS

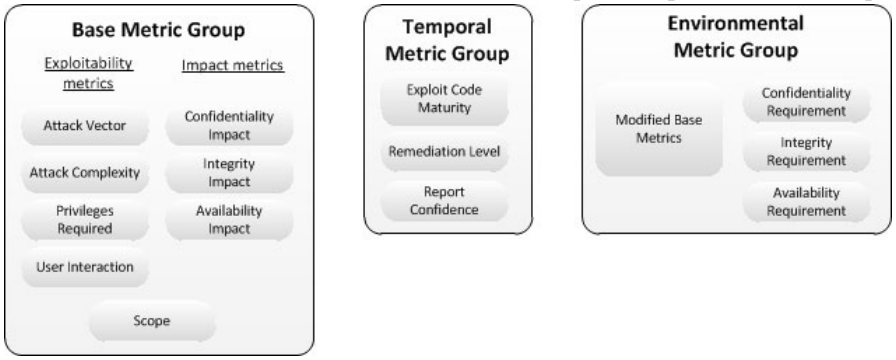
La nécessité d'un système indépendant d'évaluation des vulnérabilités est très importante et doit obligatoirement avoir des normes générales qui se concentrent sur la vulnérabilité elle-même et ne sont pas soumises aux normes de la société qui a découvert la vulnérabilité. CVSS évalue les vulnérabilités et élimine tout aspect subjectif affectant l'évaluation. Les paramètres CVSS se concentrent également sur la faille et l'environnement dans lequel le produit est affecté et les résultats obtenus (severity score) varient cependant d'une entreprise à l'autre.

En effet, s'il existe une faille XSS dans l'un des sites web mais que le pare-feu y répond complètement, elle sera prise en compte dans l'évaluation et réduira le risque, mais le risque peut être très élevé dans une autre entreprise où le pare-feu est absent.

Le processus d'évaluation est un processus de grande envergure et de nombreux aspects doivent être pris en compte lors du calcul du risque à l'aide de CVSS.

Les métriques

CVSS évalue les vulnérabilités en fonction de trois métriques clés et chaque métrique est subdivisée en plusieurs métriques. L'illustration ci-dessous décrit les Métriques CVSS.



Le CVSS est construit à partir de la métrique de base qui nous donne une évaluation du CVSS de base qui sera ensuite pondérée avec la métrique temporelle puis avec la métrique environnementale. Ces trois métriques se définissent comme suit :

• Base : elle est unique et immuable, elle se base sur les qualités intrinsèques de la vulnérabilité.

• Temporelle : elle est unique mais peut évoluer au cours du temps.

• Environnementale : elle est multiple et évolue en fonction de l'environnement informatique. Elle dépend du système informatique dans lequel elle est présente.

Les trois métriques principales sont constituées d'autres métriques et chaque métrique comporte une étude et un score permettant de calculer le résultat final du risque. Le résultat obtenu par chaque vulnérabilité est compris entre zéro et dix.

- De 0 à 3,9 : faible risque
- De 4,0 à 6,9 : risque moyen
- De 7,0 à 8,9 : haut risque
- De 9,0 à 10,0 : critique

Calculatrice CVSS

Il existe une calculatrice qui peut être utilisée pour calculer le degré de gravité de la faille. Le processus d'évaluation de chaque métrique doit être effectué par la bonne personne, par exemple, les métriques de l'environnement ne peuvent pas être évaluées par une personne ne connaissant pas bien l'environnement de la faille.

• Calculatrice FIRST : https://www.first.org/cvss/calculator/3.0

• Calculatrice NIST : https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Enfin, si vous souhaitez en savoir plus sur CVSS, vous pouvez consulter le guide de FIRST ici :

https://www.first.org/cvss/specification-document

Présentation du Chatbot SAHER-BOT

SAHER-BOT est un chat bot de cyber sécurité orienté threat, développé dans le cadre d'un stage d'été par Radhouane Bel Hadj Yahia, étudiant en deuxième année Licence Appliquée en Télecommunications à l'ISET'Com.

SAHER-BOT offre deux catégories de fonctions à l'utilisateur:
La catégorie A donne des informations sur un CVE donné
La catégorie B permet à l'utilisateur d'utiliser des scripts de pentesting

En se focalisant sur la catégorie A, elle offre 4 sous catégories:

- La 1ère permet de faire une recherche par thèmes ou par catégorie (attaque / vulnérabilité / défaillance), une description et une solution correspondante au thème de recherche sont fournies par SAHER-BOT.

- La 2ème permet la recherche d'un CVE sous le format "CVE-annee-id". Dans ce cas, la solution donne les informations et les références nécessaires au CVE recherché.

- La 3ème sous catégorie permet à l'utilisateur d'effectuer une recherche sur les dernières actualités concernant les vulnérabilités dans le monde. SAHER-BOT donne dans ce cas les informations relatives aux 100 dernières vulnérabilités, Zero-Day compris.

- La 4ème option effectue une recherche sur les 100 dernières actualités de la CyberSécurité dans le monde.

La catégorie B intitulée pratiques et scripts: offre a son utilisateur 7 services:

```
>menu
A-Ask For Informations (Description+Solution) or for a CVE
B-Use our feature scripts

>b
You can choose wich the attack detection script you want to run :
If you want to go back type no
b1-Detect NmapScan
b2-Network Analyzer
b3- IP lookup
b4-Test a WebSite's trust factor
b5-Test a hash file for virus and hybrid check
b6-Track Ransomware
b7-Track Malware
>
```

- Detect NmapScan: SAHER-BOT peut détecter les tentatives de scan Nmap sur la machine victime, dans ce cas le chatbot génère une alerte avec l'adresse ip et d'autres informations sur l'intrus.

- Network Analyzer: SAHER-BOT procéde à l'analyse de tous les paquets entrants/sortants du réseau et s'il trouve un paquet malveillant il génère une alerte.

- IP Lookup: SAHER-BOT donne la possibilité de localiser une adresse ip. Il permet d'analyser l'adresse ip ainsi que détecter sa localisation.

- Test a WebSite's trust factor: ce service permet de verifier la réputation d'un site web.

- Test a hash file for virus and hybrid check: permet de faire des tests sur le Hash d'un fichier avec virus scan et Hybrid check.

- Track Ransomware: SAHER-BOT peut localiser le ransomware d'après la base de csv de ransomware tracker feeds.

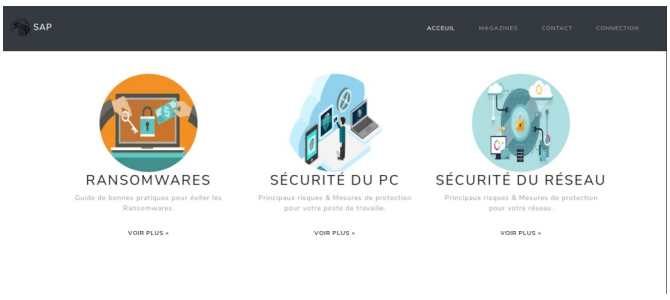
- Track Malware: ce service donne la possibilité de localiser un Malware d'après la base des malwares de urlhause, l'utilisateur tape le tag du malware voulu et le robot fait apparaître toutes les informations nécessaires.

SAHER Awareness Platform

SAHER Awaress Platform (ou SAP) est un projet développé par Shedy Chered, étudiant en deuxième année Licence Appliquée en Télecommunications à l'ISET'Com, dans le cadre d'un stage d'été.

Pendant le mois de juillet en tant que stagiaire au sein de l'ANSI, encadré par monsieur Mondher Smii, on a travaillé sur une plateforme de sensibilisation de cyber sécurité appelée SAP (SAHER AWARENESS PLATFORM) qui a pour objectif de sensibiliser les individus à la sécurité en ligne et les informer des étapes à suivre pour se protéger en ligne.

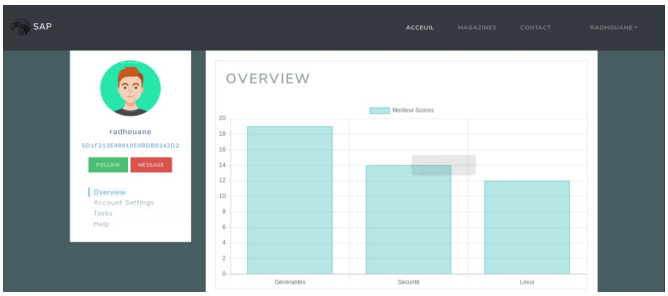
SAP est une plateforme qui offre :
- L'adoption des meilleures pratiques
- La rétention des connaissances
- L'interaction de l'utilisateur



Elle est composée de 2 principaux éléments pour la sensibilisation:
- Les guides de bonnes pratiques qui sont rédigés et maintenus par des professionnels en cyber sécurité.
- Les challenges qui sont des collections de QCM portant sur plusieurs domaines de cyber sécurité et de l'IT en général.

Les challenges ne sont accessibles qu'aux utilisateurs possédant un compte sur la plateforme car le résultat de chaque challenge sera enregistré sur notre base de données pour que l'utilisateur puisse suivre sa progression.

Donc après la création d'un compte et l'authentification, l'utilisateur aura accès aux challenges ainsi qu'à la page du profil où il y aura une vue d'ensemble pour les scores obtenus pour les différents challenges de la plateforme.



La plateforme contient aussi la collection complète de SAHER Magazine, qui traite les actualités de la Cyber sécurité à l'échelle nationale et internationale, avec la possibilité de téléchargement en format PDF.

Attention au nouveau ransomware « FileCoder » ciblant les systèmes Android

Récemment, un nouveau ransomware baptisé « Filecoder » a été découvert sur le net et visant les systèmes Android 5.1 ou ultérieures. Avant de procéder au cryptage des fichiers, Filecoder commence par l'auto-propagation via des SMS contenant des liens malveillants aux contacts trouvés sur le système de chaque victime. Afin de maximiser sa portée, Filecoder est capable de personnaliser ses SMS. En effet, il dispose de 42 modèles de messages, choisit la version qui convient à la langue du système infecté et ajoute à la fin le nom du contact de sa victime expéditrice.

Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

• Maintenir la mise à jour automatiquement de vos systèmes Android.

• Eviter d'installer des applications depuis des sources non fiables et non officielles.

• Installer puis activer l'application « Web Of Trust (WOT) » pour vous renseigner sur la fiabilité des sites web visités.

• Scanner votre appareil immédiatement par un anti-virus mis à jour après l'installation de chaque nouvelle application.

• Analyser régulièrement l'activité de votre appareil pour bloquer les menaces potentielles et se protéger contre les applications dangereuses (Voir le Centre d'aide Nexus).

• Installer une solution anti-spam pour contrer les messages suspects mobiles (Exemples: Liste des anti-spam sous Android).

Source
https://tuncert.ansi.tn/publish/content/-news.asp?idn=150

Les vulnérabilités signalées par tunCERT durant le mois de Juillet

Référence	Date découverte	Titre
tunCERT/Vuln.2019-261	25/07/2019	Systèmes Linux Ubuntu
tunCERT/Vuln.2019-260	24/07/2019	Produits Apple
tunCERT/Vuln.2019-259	23/07/2019	Produits Fortinet
tunCERT/Vuln.2019-258	18/07/2019	Noyau Drupal
tunCERT/Vuln.2019-257	18/07/2019	Cisco IOS Access Points Software
tunCERT/Vuln.2019-256	18/07/2019	Cisco FindIT Network Management Software
tunCERT/Vuln.2019-255	18/07/2019	Cisco Vision Dynamic Signage Director
tunCERT/Vuln.2019-254	17/07/2019	Windows Defender Application
tunCERT/Vuln.2019-253	17/07/2019	Moodle
tunCERT/Vuln.2019-252	17/07/2019	Oracle Fusion Middleware
tunCERT/Vuln.2019-251	17/07/2019	Oracle E-Business Suite
tunCERT/Vuln.2019-250	17/07/2019	Produits Oracle MySQL
tunCERT/Vuln.2019-249	17/07/2019	Oracle VM VirtualBox
tunCERT/Vuln.2019-248	17/07/2019	Produits Oracle et systèmes Sun
tunCERT/Vuln.2019-247	17/07/2019	Produits Oracle Java SE
tunCERT/Vuln.2019-246	17/07/2019	Oracle Database Server
tunCERT/Vuln.2019-245	16/07/2019	Google Chrome
tunCERT/Vuln.2019-244	15/07/2019	Mozilla Thunderbird
tunCERT/Vuln.2019-243	12/07/2019	Juniper: Junos OS
tunCERT/Vuln.2019-242	11/07/2019	Cisco ASA and FTD Software
tunCERT/Vuln.2019-241	10/07/2019	Produits Intel
tunCERT/Vuln.2019-239	10/07/2019	Mozilla Firefox
tunCERT/Vuln.2019-237	10/07/2019	Adobe Dreamweaver
tunCERT/Vuln.2019-236	10/07/2019	Microsoft Exchange Server
tunCERT/Vuln.2019-235	10/07/2019	Microsoft: Outils de développement
tunCERT/Vuln.2019-234	10/07/2019	Noyau des systèmes Microsoft Windows
tunCERT/Vuln.2019-233	10/07/2019	VMware ESXi
tunCERT/Vuln.2019-232	10/07/2019	Microsoft Office
tunCERT/Vuln.2019-231	10/07/2019	Microsoft Edge
tunCERT/Vuln.2019-230	10/07/2019	Internet Explorer
tunCERT/Vuln.2019-229	04/07/2019	Cisco Application Policy Infrastructure Controller
tunCERT/Vuln.2019-228	04/07/2019	Cisco Unified Communications Manager
tunCERT/Vuln.2019-227	04/07/2019	Cisco Jabber pour Windows
tunCERT/Vuln.2019-226	04/07/2019	Cisco Enterprise NFV Infrastructure Software
tunCERT/Vuln.2019-225	04/07/2019	Cisco Nexus 9000 Series Fabric Switches
tunCERT/Vuln.2019-224	04/07/2019	Cisco Managed Switches (200, 300, and 500 Series)
tunCERT/Vuln.2019-223	04/07/2019	Cisco Web Security Appliance
tunCERT/Vuln.2019-222	03/07/2019	Google Android
tunCERT/Vuln.2019-221	03/07/2019	Produits VMware
tunCERT/Vuln.2019-220	02/07/2019	F5 BIG-IP
tunCERT/Vuln.2019-219	01/07/2019	Systèmes Linux Ubuntu

Source: https://tuncert.ansi.tn/publish/module/listvulnerabilite.asp

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Parce que le partage du savoir est la clé de la réussite dans le domaine de la sécurité_informatique, l'Agence Nationale de la Sécurité Informatique est fière de vous annoncer la parution d'une nouvelle rubrique de son magazine mensuel "**SAHER Magazine**" intitulée "Cyber-agora".

Cyber-agora sera un espace ouvert aux contributions des professionnels, étudiants et académiciens évoluant dans le domaine de la sécurité informatique. À ce titre, une adresse E-mail sera mise à votre disposition pour y envoyer vos articles qui, après leur vérification par les équipes de l'ANSI, seront publiés dans les prochaines éditions de SAHER Magazine.

Il est à noter que le contenu des articles doit être unique sachant qu'une vérification anti-plagiat sera réalisée avant toute publication officielle. Enfin, si l'article est sélectionné, son auteur serait crédité.

Veuillez nous envoyer vos contributions à cette adresse : **sahermag@ansi.tn**

49 avenue Jean Jaurès, 1000 Tunis

(+216) 71 846 020

ansi@ansi.tn
incident@ansi.tn
saher@ansi.tn
cert-tcc@ansi.tn
audit@ansi.tn
sahermag@ansi.tn