SAHER Magazine

Agence Nationale de la Sécurité Informatique

N°10
Mars. 2020

COVID-19 et Sécurité:

Tout ce que vous devez savoir

Houdini

Analyse complète et recommendations

Ryuk

Le ransomware le plus rentable du moment

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

03 Février 2020

16 ème anniversaire de l'ANSI

L'Agence Nationale de la Sécurité Informatique a fêté cette année son 16e anniversaire et ceci est une occasion pour rappeler le rôle fondamental qu'a joué l'agence, depuis sa création en 2004, pour consolider et mettre en oeuvre les piliers de la sécurité informatique en Tunisie à l'ère du digital.

En effet, l'ANSI est aujourd'hui une référence nationale et internationale dans le domaine de la cybersécurité grâce à ses collaborations fructueuses en matière de mise en oeuvre des CERTs et ses missions de sensibilisation tout en exerçant une veille efficace et efficiente sur le cyberespace tunisien.

Outre ses missions principales, l'Agence Nationale de la Sécurité Informatique a toujours misé sur les collaborations académiques et a permis à des centaines d'étudiants de concrétiser leurs connaissances théoriques et pratiques dans le domaine de la sécurité informatique. De plus, chaque l'année, l'ANSI organise et participe à plusieurs Workshops et séminaires car le partage de l'information est la meilleure défense contre les Cyber-menaces.

Enfin, l'année 2019 a été couronnée par l'approbation et la signature de la Stratégie Nationale de Cybersécurité.

06 Février 2020

Workshop :" Blockchain et cybersécurité "

Dans le cadre de la 3ème rencontre des professionnels et des chercheurs dans le domaine de la cybersécurité, l'Agence Nationale de la Sécurité Informatique a organisé un Workshop sous le thème "Blockchain et cybersécurité" en collaboration avec IEEE Tunisie, et ce le 06 Février 2020.

Durant ce Workshop les thèmes suivants ont été abordés :
• "Blockchain et Crypto Monnaies : Concepts de base et Applications" - Hanen Idoudi (ENSI, Univ. Manouba, Tunisia)
• "Blockchain for smart Transactions - Use cases and challenges" - Khalifa Toumi (IRT SystemX, France)
• "Cyber sécurité, confiance et vie privée : Quel rôle peut jouer la Blockchain ?» - Hella Kaffel Ben Ayed (FST, Univ. Tunis El Manar, Tunisia)
• "The impact of Blockchain in Information Security" - Skander Mansouri (Research Student, University of Quebec, Canada)

11 Février 2020

Safer Internet Day

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. 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.

À ce titre, l'Agence Nationale de la Sécurité Informatique adhère à cette compagne dont les objectifs sont :

• Sensibiliser le public au thème "Utiliser Internet en toute sécurité".
• Apporter une aide aux enfants, jeunes, parents et pédagogues grâce à des informations concrètes et des conseils pratiques.
• Favoriser la participation active des institutions, organisations, associations, entreprises, initiatives et particuliers au niveau national et régional.
• Orienter l'attention publique et médiatique sur le thème "Utiliser Internet en toute sécurité" dans le cadre du programme Safer Internet Day.

Durant ces journées, des Workshops ainsi que des sessions de formations ont été réalisés pour sensibiliser les parents et les enfants aux risques d'internet.
L'ANSI a aussi mis à la disposition des parents un guide pour mieux protéger leurs enfants contre les dangers d'internet. Ce guide est disponible via ce lien :

https://www.ansi.tn/actualite/lansi-adh-re-au-safer-internet-day-2020

La clôture de cet évènement a été marquée par la présence du ministre de l'éducation M. Hatem ben Salem ainsi que le DG de l'ANSI, M.Naoufel Frikha, Mme Lamia Zargouni, membre permanent de l'instance nationale de la protection des données personnelles et plusieurs autres hauts cadres.

27 Février 2020

Convention avec OWASP - Tunisia Chapter

Dans le but d'encourager les initiatives visant à enrichir l'écosystème tunisien dans le domaine de la sécurité informatique, l'Agence Nationale de la Sécurité Informatique est fière de vous annoncer qu'un nouveau partenariat a vu le jour avec OWASP - Tunisia Chapter.

Il est à rappeler que le OWASP - Tunisia Chapter (The Open Web Application Security Project) est une organisation à but non lucratif dont l'objectif est de vulgariser les bonnes pratiques dans le domaine de la sécurité applicative. De plus, dans le cadre de ses missions , L'OWASP - Tunisia Chapter a entamé une compagne de sondage à l'échelle nationale sur la sensibilisation à la sécurité des logiciels (Software Security) et qui est destinée aux:

• Professionnels/Développeurs/Experts(Etablissement privé/publique) qui travaillent dans le domaine du Software
• Universitaires enseignant les cours de développement(Coding et génie logiciel…)
• Etudiants/nouveau diplômés ayant un cursus en Software.

À ce titre, vous êtes cordialement appelés à participer au sondage et à le partager en suivant ce lien:

https://docs.google.com/forms/d/e/1FAIpQLSdhYuzbZvAeD5hyTikGkLMUVfPDuTEZuH10qx48zfzF7KFBug/viewform

Pour plus d'informations concernant l'OWASP veuillez consulter : https://owasp.org/www-chapter-tunisia/

28 Février - 1er Mars 2020

Workshop : "IoT meets AI"

Sous le thème "IoT meets AI" l'École Supérieure des Communications de Tunis SUP'COM a organisé un événement durant lequel plusieurs professionnels et chercheurs ont mis en exergue les concepts et les possibilités offertes par l'intelligence artificielle dans l'implémentation des IoT.

Cet événement a été marqué par la participation de plusieurs entités qui opèrent dans le secteur des télécommunications à l'instar de IEEE ainsi que l'Agence Nationale de la Sécurité Informatique.

04 Mars 2020

Workshop mise en place d'un CERT santé

Dans le cadre de sa collaboration avec le Centre Informatique du Ministère de la Santé CIMS, l'Agence Nationale de la Sécurité Informatique a participé à un Workshop traitant la mise en place du CERT santé et ce, le mercredi 4 mars 2020.

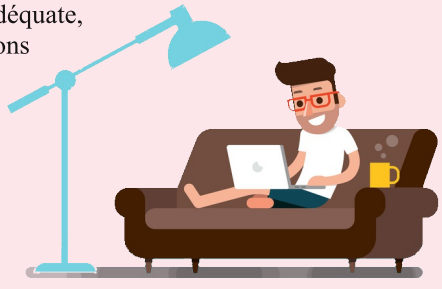
Comment passer au Télétravail

Dans le cas où le télétravail ou le travail collaboratif à distance est envisagé lors de circonstances exceptionnelles ou en cas de force majeur, l'Agence Nationale de la Sécurité Informatique recommande aux dirigeants d'entreprises d'adopter les mesures nécessaires pour leur mise en œuvre.

De ce fait, vous êtes sollicités à :
- Permettre l'accès à distance au réseau de votre établissement via les tunnels VPN (SSL / IPsec).
- Utiliser les canaux classiques de communication et d'échange : Téléphone, Email.
- Déployer des outils de travail collaboratif.
- Adapter vos modalités de contrôle du temps de travail ou de régulation de la charge de travail.
- Préparer l'activation ou le déclenchement de votre plan de reprise et de continuité d'activité (PCA/ PRA)

Pour ceux qui ne disposent pas de solution adéquate, nous vous proposons d'utiliser :

- OPENVPN
- Nextcloud
- Mattermost



L'Agence Nationale de la Sécurité Informatique met aussi à votre disposition une machine virtuelle (VM) sous Debian 10 offrant la solution NextCloud que vous pouvez télécharger via le lien suivant :

https://drive.google.com/file/d/1mTRRkX-OobTC_cV-b64LNgds_ZkAS0wO/view

Si jamais vous avez des difficultés à utiliser cette solution, il est possible de solliciter l'un des experts auditeurs certifiés par l'ANSI dont la liste complète est accessible via notre site web officiel en suivant ce lien :

https://www.ansi.tn/sites/default/files/liste_auditeurs_5.pdf

Un document (sur Slideshare) qui permet d'expliquer la mise en oeuvre de la machine virtuelle est téléchargeable via le lien ci-dessous. Il est fortement recommandé de changer les mots de passe par défaut.

https://www.slideshare.net/ANSItunCERT/nextcloud-tltravail

Pour toute assistance veuillez contacter:

saher@ansi.tn

Houdini:
Le Trojan aux Apparences Trompeuses

Durant l'élaboration des rapports mensuels issus des différentes sondes installées, nous avons remarqué que plusieurs d'entre elles ont détécté un nombre important d'actifs infectés par le malware Houdini. Bien que ce malware parait anodin, mais en réalité il envoie des informations critiques à son serveur C&C.
Dans cet article nous allons présenter ce malware, le type de données qu'il pourrait envoyer et comment s'en prévenir.

H-Worm, également connu sous le nom de Houdini, Jacksbot ou SocGholish est un cheval de Troie d'accès à distance qui a été repéré pour la première fois en 2013. Un allemand qui a comme pseudonyme "Vicswors Bagdad" est soupçonné d'être à l'origine de la propagation du malware Houdini sur les sites Pastebin.
Ce RAT (Remote Access Trojan) partage son infrastructure de commande et de contrôle (C&C) avec NjW0rm, njRat / LV, XtremeRAT et PoisonIvy.
Ses capacités incluent le vol d'informations système et de mots de passe, Keylogging, le téléchargement, le changement de nom de la machine, l'exécution et la suppression de fichiers, la capture d'écran, l'affichage de la webcam, son auto mise à jour et désinstallation.

Moyens de propagation de Houdini
Ce type d´infection se propage soit à travers des campagnes malspam, soit à travers les supports amovibles comme les clés USB, les cartes SD, les téléphones, GPS, tablettes .. Tout support USB contenant de l´espace disque peut être contaminé.
En effet, si le support USB sain est branché sur un PC infecté, où l´infection est active. Celui-ci va automatiquement créer une copie de son code malicieux sur le support USB sain. Une fois contaminé, il devient le vecteur de propagation.

Comportement de Houdini
Une fois l'infection est réussie, le malware envoie diverses informations d'identification sensibles dans le champ User-Agent.

User-Agent:
`{DiskVolumeSerial}<|>{Hostname}<|>{Username}<|>{OS}<|>plus<|>{AV ProductInstalled or nan-av}<|>{USBSpread: true or false}-{CurrentSystemDate}`

La figure 1 illustre le payload de l'infection Houdini
et il attend une réponse de la forme:
`{commande}<|>{param1}<|>{param2}`

comme c'est indiqué dans la figure 2.

Dans le tableau de la figure 3, nous vous montrons un extrait des données envoyées par houdini et capturées par une de nos différentes sondes.

Nouvelle Forme du malware
Le 2 juin 2019, une nouvelle variante du malware Houdini, a été détectée lors de campagnes contre les institutions financières et leurs clients.
Surnommé WSH Remote Access Tool (RAT), il n'a fallu que cinq jours à la

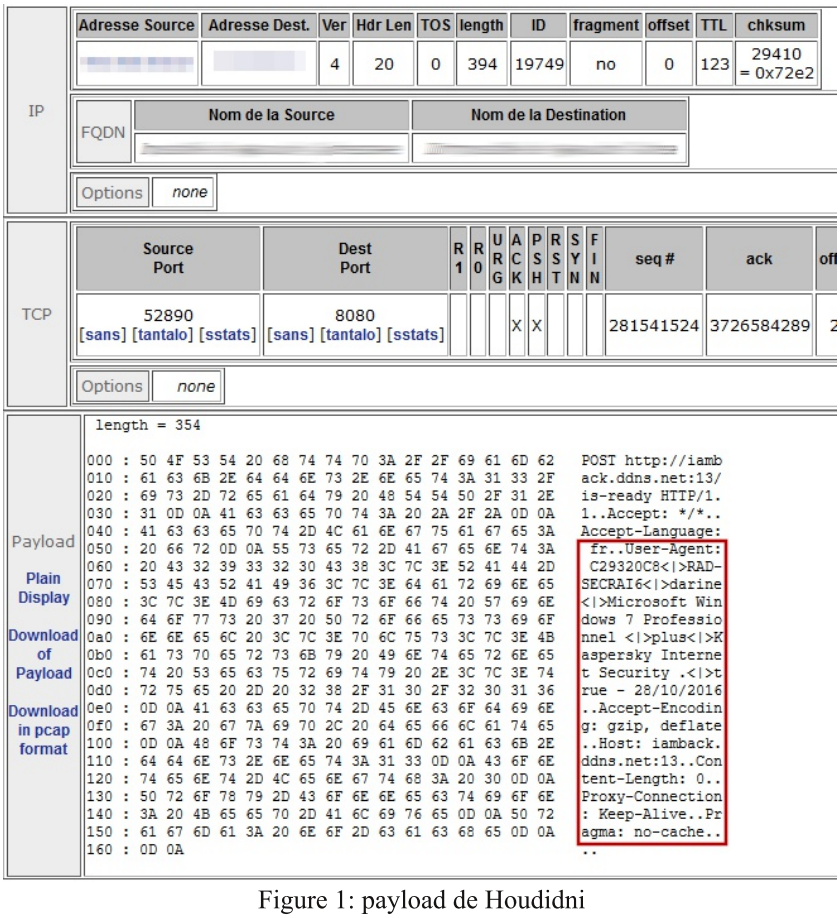


Figure 1: payload de Houdidni

variante pour commencer à rechercher des victimes via des campagnes de phishing, l'objectif global étant le vol d'informations d'identification bancaire en ligne qui peuvent être utilisées pour effectuer des achats frauduleux.
La campagne de phishing se fait passer pour une communication légitime des banques. Les e-mails frauduleux contiennent des fichiers d'archive Web ".MHT" qui agissent de la même manière que les fichiers ".HTML".
Si une victime ouvre la pièce jointe, le fichier, qui contient un lien d'adresse Web, la dirige vers une archive .zip contenant le payload WSH RAT.
WSH RAT est une version de HWorm qui a été portée sur Javascript à partir de la configuration Visual Basic d'origine de HWorm mais agit de la même manière que le malware d'origine. Le cheval de Troie utilise non seulement les mêmes données encodées en Base64 mais également les mêmes chaînes de configuration, avec des variables par défaut nommées et organisées de la même manière pour les deux types de code malveillant.
La charge utile communique d'abord avec son serveur de commande et de contrôle (C&C), contrôlé par l'attaquant, pour demander trois fichiers ".tar.gz" supplémentaires. Cependant, ces fichiers sont en réalité des exécutables PE32 qui fournissent au cheval de Troie un keylogger Windows, une visionneuse d'informations d'identification de messagerie et un module de visualisation d'informations d'identification de navigateur.
La souche de malware est activement vendue dans le DarkWeb avec un abonnement de 50$ par mois.

Commander	La description	Demande de communication générée
exécuter	Exécute la valeur du paramètre en utilisant «exécuter»	-
mise à jour	Remplace la charge utile et redémarre avec le moteur wscript	-
désinstaller	Supprime les entrées de démarrage et la charge utile	-
envoyer	Télécharge le fichier depuis le serveur CnC	POST / est en train d'envoyer <|> {FileURL}…
site-envoyer	Télécharge le fichier depuis l'URL	GET / {FileURL}…
recv	Télécharge le fichier sur le serveur CnC	POST / is-recving <|> {FilePath}…
enum-driver	Envoie toutes les informations sur le lecteur au CnC	POST / is-enum-driver… {DrivePath | DriveType <|>…}
enum-faf	Envoie tous les attributs de fichier et de dossier dans un répertoire spécifié	POST / is-enum-faf… {FolderName | (FileSize) | (d | f) | Attributes <|>…}
enum-process	Envoie toutes les exécutions traitées	POST / is-enum-process… {Nom | PID | Chemin <|>…}
cmd-shell	Exécute la valeur param avec 'cmd.exe / c' et retourne le résultat	POST / is-cmd-shell… {Résultat}
supprimer	Supprime le fichier ou le dossier spécifié dans param	-
processus de sortie	Tue le processus spécifié dans param	-
sommeil	L'appel de veille dans param est passé à eval ()	-

Figure2: Les réponses possibles de Houdini

Recommandations

- Désactiver Windows script hosting
- Installation d'un anti-virus
- Mettre à jour le système d'exploitation
- Analyser automatiquement tout disque amovible avant son utilisation
- Faire attention aux téléchargements et ne pas télécharger de fichiers ou depuis des sites non sûrs.
- Etre attentif avant de cliquer sur un lien notamment provenant des mails, réseaux sociaux, etc.
- Faire des sauvegardes de vos données

Sources

Sondes SAHER
https://cyware.com/news/h-worm-rat-an-insight-into-the-vbs-based-infamous-rat-houdinih-worm-5ddef535/
https://www.fireeye.com/blog/threat-research/2013/09/now-you-see-me-h-worm-by-houdini.html
https://www.zdnet.com/article/new-houdini-malware-targets-banks-with-keylogger-browser-credential-theft/
https://www.malekal.com/comment-securiser-son-pc-virus-dossier/

IP Source	Code Disk	Hostname	Username	OS Version	Free Field	Antivirus	USB - Infection Date
193	Intel(R) Core(TM) i3-4160 CPU @		user	Microsoft Windows 7 Professionnel	plus		true - 31/10/2016
193	Intel(R) Core(TM) i3-4160 CPU @	FIDA	user	Microsoft Windows 7 Professionnel	plus		true - 29/04/2016
193	3EDE05DC	USER-PC	user	Microsoft Windows 7 Professionnel	plus	nan-av	true - 30/09/2015
193	F69F7A49	PC-PC	PC	Microsoft Windows 7 Édition Intégrale	plus	nan-av	true - 07-02-2020
193	DZ-WORM-C81720D3	74		Microsoft Windows 7 Professionnel	WORM OF DZ-47	nan-av	FaLsE - 11/02/2020
193.	38652770	BO	Administrateur	Microsoft(R) Windows(R) Server 2003, Enterp	plus	nan-av	true - 18/04/2016
193	525AE875	07		Microsoft Windows 7 Professionnel	plus	nan-av	true - 10/04/2015
196	886C5B86	P	user	Microsoft Windows 7 Professionnel	plus	nan-av	true - 13/12/2019
196.	2__6A349A87	-PC		Microsoft Windows 7 Professionnel	plus	nan-av	false - 10/02/2020
196	00B3BE2D	ORDINATEUR	user	Microsoft Windows XP Professionnel	plus	nan-av	false - 02/12/2015
196.	D0F7A794	USER	user	Microsoft Windows XP Professionnel	plus	avast! Antivirus .	true - 01/02/2016
196.	74880417	10C7		Microsoft Windows XP Professionnel	plus	nan-av	false - 04/11/2019
196.	BE69211B	PC		Microsoft Windows 7 Professionnel	the KR.joker worm	nan-av	false - 27-09-2018
196.	786807EF		Administrateur	Microsoft Windows XP Professionnel	plus	nan-av	true - 03/03/2015
196.	ACF1A1EB	GL -PC		Microsoft Windows 7 Professionnel	plus	nan-av	true - 29/03/2019
196.	44954955	M -PC		Microsoft Windows 7 Professionnel	plus	nan-av	true - 05/13/2019
196.	4EBA4E23	N -PC		Microsoft Windows 7 Professionnel	plus	nan-av	true - 04/05/2018
196.	A66AA3F8	F -PC		Microsoft Windows 7 Édition Familiale Premi	plus	nan-av	true - 01/24/2018
196.	D61333AE	S -PC		Microsoft Windows 7 Professionnel	plus	nan-av	false - 10/02/2020
196.	5ABE1981	S -PC		Microsoft Windows 7 Professionnel	plus	nan-av	true - 28/06/2018
196.	52D4D7BF	USER-PC	user	Microsoft Windows 7 Professionnel	plus	nan-av	true - 16-12-2016
196.	DZ-WORM-9A4BE558	F -PC		Microsoft Windows 7 Professionnel	WORM OF DZ-47	nan-av	TRue - 11/07/2019
196.	9A4BE558	H	user	Microsoft Windows 7 Professionnel	plus	nan-av	true - 11/10/2014
196.	980D36EA	B PC		Microsoft Windows 7 Professionnel	plus	nan-av	false - 11/02/2020
196.	DE0D460C	E -PC		Microsoft Windows 7 Édition Familiale Basiqu	underworld final	nan-av	false
196.	F29A82B2	N -PC		Microsoft Windows 7 Édition Intégrale	underworld final	nan-av	false
196.	0CFA72C5	S	Administrateur	Microsoft Windows XP Professionnel	plus	ESET NOD32 Antivirus 3.0	true - 28/09/2016

Figure 3: Les infections détéctées par les sondes SAHER

Ryuk:
retour sur le ransomware le plus rentable

Ryuk est un ransomware qui a été identifié le 13 août 2018. Une analyse initiale suggère que la menace a été injectée dans les systèmes via des comptes RDP compromis, mais il est possible qu'il existe une campagne de spam parallèle qui transporte la charge utile du malware sous forme de fichiers DOCX et PDF macro-activés.
Ryuk ne démontre pas de compétences techniques extrêmement avancées, cependant, ce qui le distingue des autres ransomwares, c'est l'énorme rançon qu'il exige.

Ryuk Ransomware est apparu à la mi-août 2018 avec plusieurs attaques ciblées bien planifiées contre de grandes organisations du monde entier, cryptant des données sur des ordinateurs et des réseaux infectés et exigeant le paiement d'une enorme rançon en échange d'un outil de décryptage. Le montant dépend de la taille de l'organisation affectée, tandis que les recherches montrent que les attaquants ont déjà empoché près de 4 millions de dollars en extorsion de fonds de leurs victimes avec une rançon moyenne de 71000 $ en Bitcoin, dix fois le montant généralement demandé par d'autres logiciels malveillants de ce type.

En janvier 2019, le montant de rançon le plus bas demandé par Ryuk était de 1,7 BTC, tandis que le plus élevé était de 99 BTC. Le nombre de transactions connues est de 52 et le produit a été réparti entre 37 adresses BTC.

Méthode d'infection

Auparavant, on supposait que Ryuk était distribué comme une infection primaire via des pièces jointes malveillantes et des RDP insuffisamment protégés. Cependant, le nombre limité d'attaques contre des organisations de haut niveau sélectionnées suggère que Ryuk est distribué et opéré manuellement. Cela signifie que chaque attaque doit être préparée individuellement et soigneusement, ce qui inclut une cartographie réseau étendue et la collecte des informations d'identification. Ces observations suggèrent que les attaquants connaissaient déjà les domaines ciblés via d'autres infections de logiciels malveillants avant de pouvoir installer Ryuk.

Pour confirmer cette théorie, les dernières recherches de janvier 2019 montrent que Ryuk se propage principalement en tant que charge utile secondaire, installée manuellement par des attaquants sur des machines qui ont déjà été infectées par des botnets Emotet et TrickBot. La principale méthode d'infection qu'Emotet utilise est par le biais de campagnes de courrier indésirable avec des documents Microsoft Office joints et corrompus par des scripts malveillants. Les attaquants utilisent diverses techniques d'ingénierie

sociale pour obliger l'utilisateur à ouvrir les pièces jointes et à cliquer sur «Activer le contenu», qui à son tour, lance les scripts malveillants et permet

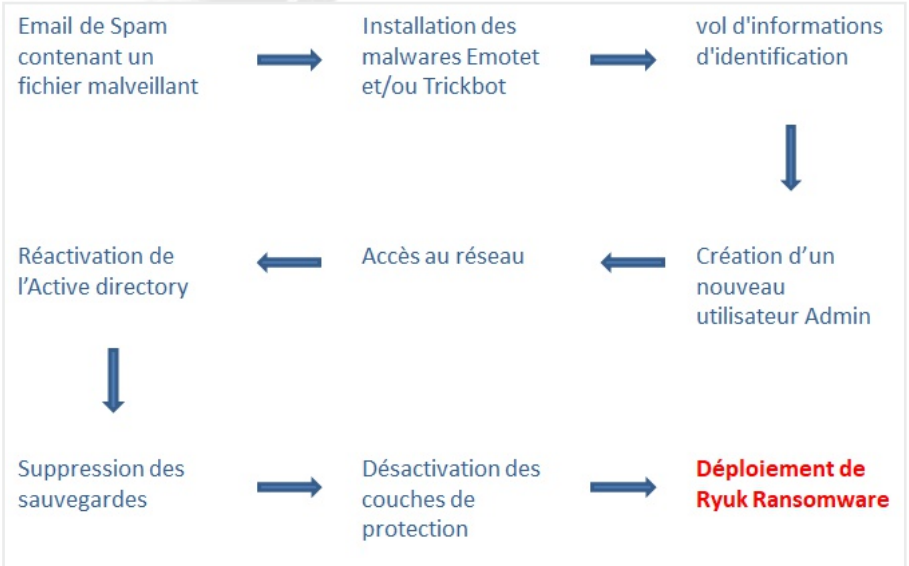


Figure 1: Etapes de l'attaque Ryuk

au malware d'être installé sur la machine cible. L'hypothèse principale est qu'Emotet crée l'infection initiale, se propage latéralement à travers le réseau affecté, puis lance sa propre campagne malveillante, envoyant des logiciels malveillants supplémentaires sur le réseau infecté. Trickbot est ensuite utilisé pour déposer le ransomware Ryuk sur les systèmes des institutions sélectionnées à partir desquelles les attaquants envisagent d'extorquer la rançon.

Emotet et TrickBot possèdent les fonctionnalités de vers, de voleurs de données et de téléchargeurs de programmes malveillants supplémentaires.
La figure 1 illustre les étapes de l'attaque Ryuk.

Note de rançon
Il existe à ce jour, deux variantes de notes de rançon que Ryuk propose aux victimes. cette note est contenue dans un fichier nommé "RyukReadMe.txt" qui est placé sur le bureau, ainsi que dans tous les dossiers.

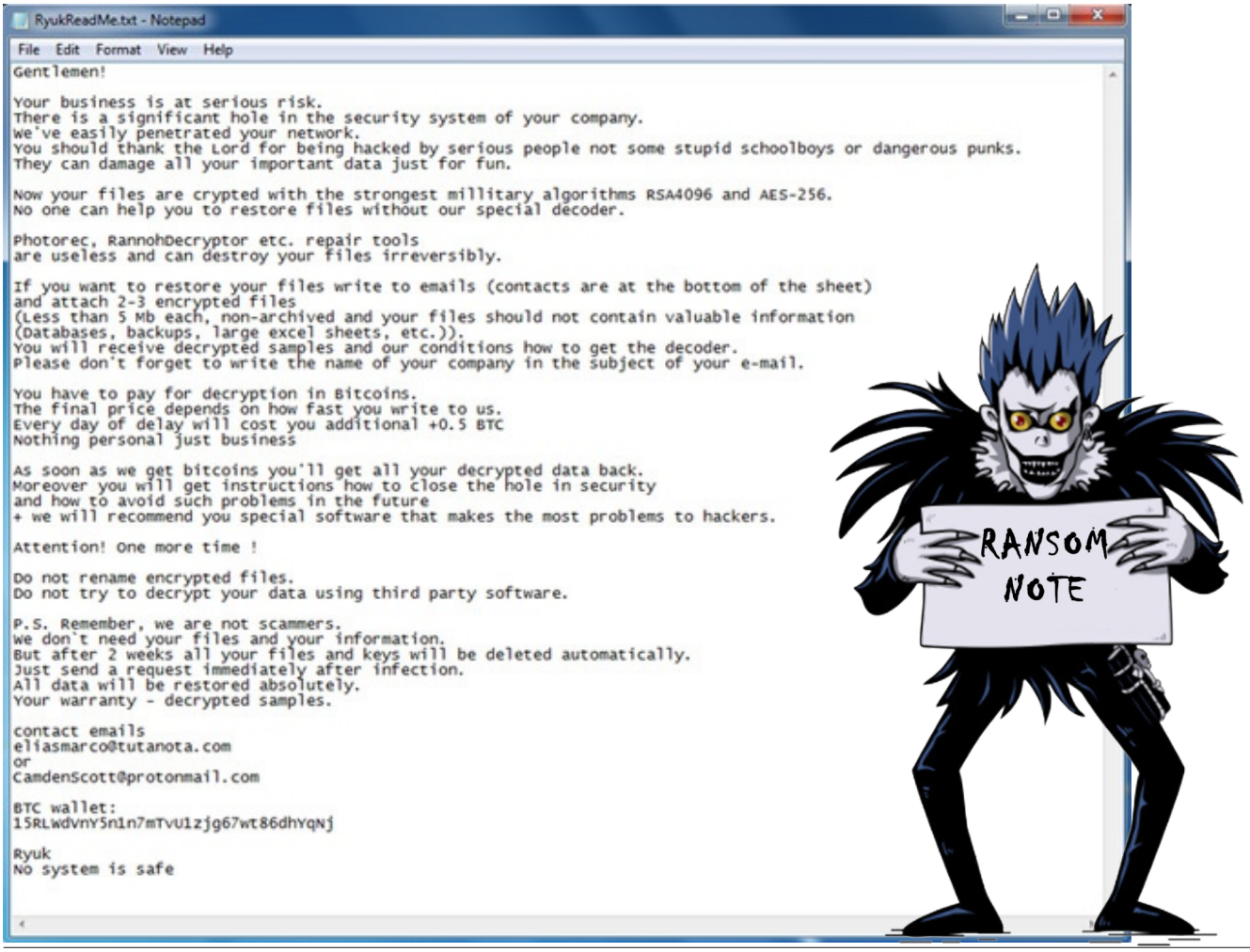
La première est longue, bien écrite et bien formulée, et elle a conduit au paiement de la plus haute rançon enregistrée à ce jour soit 50 BTC. La seconde est beaucoup plus courte et plus simple et exige des montants de rançon allant de 15 BTC à 35 BTC. Cela implique qu'il pourrait y avoir deux niveaux de victimes potentielles que les escrocs ont prévu d'attaquer.

Ci dessous un aperçu de la première version de la note de rançon.

Sources
https://www.enigmasoftware.com/ryuk-ransomware-removal/
https://news.sophos.com/fr-fr/2019/10/07/-retour-sur-ransomware-ryuk/

Recommandations

- Utilisez des mots de passe forts et déployez une authentification à deux facteurs chaque fois que vous le pouvez
- Protégez les droits d'accès. Ne donnez aux comptes utilisateurs et aux administrateurs que les droits d'accès dont ils ont besoin.
- Faites des sauvegardes régulières, et conservez-les hors site.
- Faites des mises à jour régulières de vos systèmes d'exploitation
- Désactivez RDP si vous n'en avez pas besoin
- Assurez-vous que la protection anti-falsification soit bien activée. Ryuk et d'autres ransomwares tentent de désactiver la protection de vos systèmes endpoint. La protection anti-falsification est conçue pour empêcher qu'un tel incident ne se produise.
- Sensibilisez votre équipe au phishing. Le phishing est l'un des principaux mécanismes de diffusion des ransomwares.



Covid-19 : un virus propice aux pirates

Plusieurs experts en cybersécurité, ont constaté une importante augmentation des attaques informatiques ces dernières semaines, en relaion avec la crise sanitaire et économique liée à l'expansion du Covid-19. Les pirates informatiques ne manquent pas d'imagination pour tromper les utilisateurs, particuliers comme entreprises.

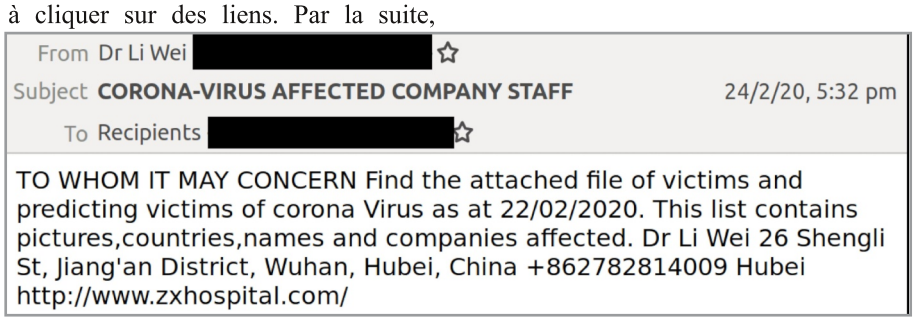
Toujours plus créatifs, des hackers distribuent des chevaux de Troie, des virus, dans des emails d'alerte sur la pandémie de coronavirus.

Ces mails infectés se présentent sous la forme de bulletins officiels émis par des centres de santé publique ou des organismes d'assurance. Ils indiquent aux destinataires qu'ils trouveront plus de détails sur les mesures préventives à adopter contre les infections de coronavirus dans les pièces jointes. Deux clics plus tard, le cheval de Troie est déployé sur l'ordinateur de la victime. Il peut ensuite lui-même installer d'autres types de logiciels malveillants, dont des ransomwares. Il suffit qu'une seule machine soit infectée, pour que le système d'information entier de l'entreprise soit compromis.

Dans cette section, on vous présente quelques attaques pouvant nuire à vos données personnelles.

Diffusion des malwares ou des ransomwares :
Depuis le début de 2020, plusieurs domaines malveillants liés aux coronavirus sont créés. Un grand nombre de ces domaines seront utilisés dans des campagnes de phishing. Lors de la réception d'un email suspect, on vous incite à cliquer sur des liens. Par la suite, vous allez infecter votre machine par l'installation des malwares ou des ransomwares. Par exemple, Malwarebytes Labs a signalé qu'il a déclaré avoir trouvé des variantes du cheval de Troie AzorUlt intégré dans certaines pièces jointes relatives à certains emails COVID-19.

Aussi, DomainTools a signalé la distribution d'une application android intitulé « CovidLock » qui verrouillera le téléphone de l'utilisateur.


From Dr Li Wei [redacted]
Subject CORONA-VIRUS AFFECTED COMPANY STAFF 24/2/20, 5:32 pm
To Recipients [redacted]

TO WHOM IT MAY CONCERN Find the attached file of victims and predicting victims of corona Virus as at 22/02/2020. This list contains pictures,countries,names and companies affected. Dr Li Wei 26 Shengli St, Jiang'an District, Wuhan, Hubei, China +862782814009 Hubei http://www.zxhospital.com/

Vol de données bancaires :
Suite au confinement, le déplacement des gens devient presque impossible. Ils sont invités alors à terminer leurs paiements à distance. Le danger réside ici dans le vol de données bancaires lorsque le pirate se fait passer pour une entité connue (banque, FAI, …) et vous demande d'envoyer vos informations ou bien lorsque vous êtes redirigé vers de fausses pages de paiement.

De plus, certains cybercriminels utilisent une carte mondiale des cas confirmés de coronavirus pour propager leurs malwares. La carte en question révèle en temps réel le nombre et la position géographique des personnes contaminées par le virus. Il s'agit d'un tableau de bord interactif initialement produit par la Johns Hopkins University. Des pirates proposent même sur le Dark Web un kit de piratage lié au coronavirus utilisant cette carte interactive.

Plus grave encore, un hopital universitaire tchèque a été frappé par une cyberattaque en pleine pandémie de COVID-19.
Les responsables de l'hôpital n'ont pas révélé la nature du problème. Cependant, l'incident a été jugé suffisamment grave pour reporter des interventions chirurgicales et rediriger les nouveaux patients vers un autre hôpital universitaire situé à proximité, ont rapporté les médias locaux
L'incident est considéré comme grave et traité avec la plus grande urgence car l'hôpital universitaire de Brno est l'un des plus grands laboratoires de tests COVID-19 de la République tchèque.
Suite à cet incident, des équipes du Centre national tchèque de cybersécurité (NCSC - Czech National Cyber Security Center), de la police tchèque (NCOZ) et du personnel informatique de l'hôpital ont travaillé ensemble pour faire repartir le réseau informatique de l'hôpital.

Un autre établissement de santé, l'Assistance Publique-Hôpitaux de Paris (AP-HP), a été aussi la cible d'une attaque DDOS d'une durée de 1 Heure survenue le dimanche 22 Mars en fin de matinée. Afin de mitiger l'attaque, le prestataire de service a été contraint de bloquer tout accès externe vers les applications et la messagerie de l'AP-HP.
L'Autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) et le ministère de la Santé ont été immédiatement prévenus.

Néanmoins, pour ne pas agraver encore plus une situation déjà critique, certains groupes de hackers viennent de s'engager à ne plus cibler les établissements de santé, notamment les hôpitaux.
Contacté par "Bleeping Computer", deux groupes- DoppelPaymer et Maze- ont affirmé qu'ils ne procéderont à aucune attaque à l'encontre des établissements de santé jusqu'à ce que la crise soit passée. DoppelPaymer a même promis un décryptage gratuit au cas où des infrastructures hospitalières seraient crypté par erreur.

Reste à espérer que ce message aura un impact sur les autres groupes de pirates à travers le monde.

Sources:
https://www.usine-digitale.fr/article/-comment-les-hackers-surfent-sur-le-coronavirus-pour-multiplier-les-actes-malveillants.N940051
https://cyberguerre.numerama.com/2617-coronavirus-des-hackers-profitent-de-linquietude-pour-infecter-des-ordinateurs.html
https://www.lebigdata.fr/covid-19-hackers-virus-carte-coronavirus
https://www.zdnet.com/google-amp/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/
https://www.lci.fr/police/coronavirus-les-hopitaux-de-paris-aphp-victimes-d-une-cyberattaque-deni-de-service-de-hackers-2148857.html
https://siecledigital.fr/2020/03/20/covid-19-les-hackers-promettent-un-repit-aux-hopitaux/
https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

Conseils pour éviter le phishing

Les e-mails de phishing vous incitent à cliquer sur un lien ou à fournir des informations personnelles pouvant être utilisées pour un vol d'identité. Voici quelques conseils pour éviter d'être trompé:

-Faites attention lors de la saisie des informations personnelles (numéro de sécurité sociale, CIN,..) dans les formulaires des portails des pensions ou de facturation en ligne.

-Essayez de vérifier l'identité de l'expéditeur du mail ou du lien.
-Vérifier les noms de domaines des mails reçus.

- Si un mail reçu demande de l'argent pour les tests de coronavirus ou des produits médicaux, traitez-le avec prudence.

- Pendant cette crise, les pirates savent que les gens sont toujours à la recherche de nouvelles informations et exploitent cette situation pour voler de l'argent ou des mots de passe. Par exemple, si vous cherchez des statistiques ou autres informations relatives au coronavirus, nous vous proposons les liens suivants :
• Le site officiel de l'organisation mondiale de la santé :
https://www.who.int/health-topics/coronavirus#tab=tab_1
• Le site développé par Google pour faciliter l'accès au dépistage du Covid-19 :
https://www.google.com/covid19/
• Le site web covid-19.tn lancé par la Junior Entreprise ESEN pour permettre de suivre l'évolution de la pandémie du Coronavirus en Tunisie.
https://covid-19-tn.web.app/
• Le site des statistiques mondiales worldometers :
https://www.worldometers.info/coronavirus/

AWARENESS

RANSOMWARE :: WANNACRY

A few years ago saw the beginning of the Trojan encryptor WannaCry outbreak. It appears to be pandemic — a global epidemic. We counted more than 45,000 cases of the attack in just one day, but the true number is much higher.

In order to prevent infection and the spread of this malware across the network, all Windows systems should be up to date on current patches and antivirus signatures. Additionally, blocking inbound connections to SMB ports (139 and 445) will prevent the spread of the malware to systems still vulnerable to the patched exploit

Prevent the infection from spreading by separating all infected computers from each other, shared storage, and the network.

Contact the National Agency for Computer Security - tunCERT
incident@ansi.tn

CORONAVIRUS :: COVID19

Coronavirus disease 2019 (COVID-19) is a respiratory illness that can spread from person to person. The virus that causes COVID-19 is a novel coronavirus that was first identified during an investigation into an outbreak in Wuhan, China

HOW CAN I HELP PROTECT MYSELF?

- Avoid close contact with people who are sick.
- Avoid touching your eyes, nose, and mouth with unwashed hands.
- Wash your hands often with soap and water for at least 20 seconds. Use an alcohol-based hand sanitizer that contains at least 60% alcohol if soap and water are not available.

IS THERE A TREATMENT?

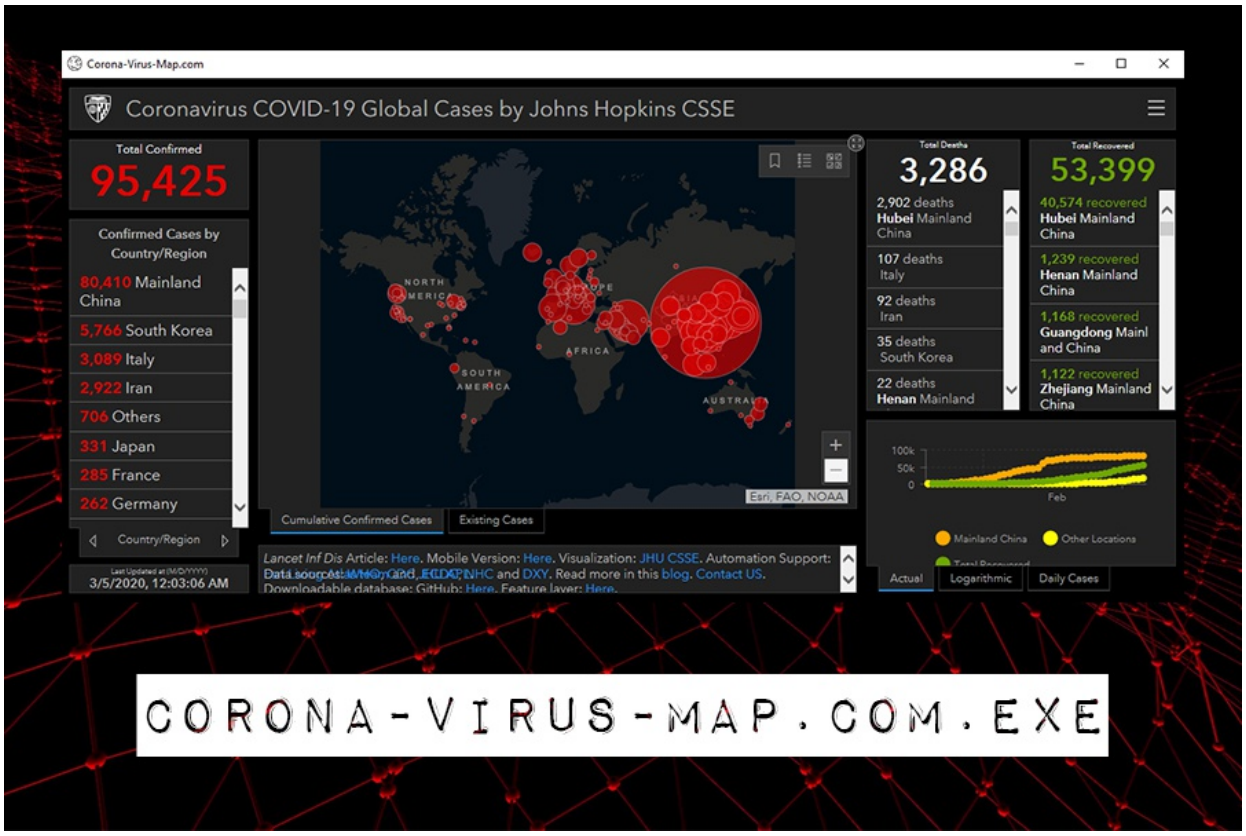
Stay home when you are sick.

There is no specific antiviral treatment for COVID-19. People with COVID-19 can seek medical care to help relieve symptoms.

CALL 190

Corona-virus-map.com.exe
un malware qui exploite l'épidémie de COVID-19

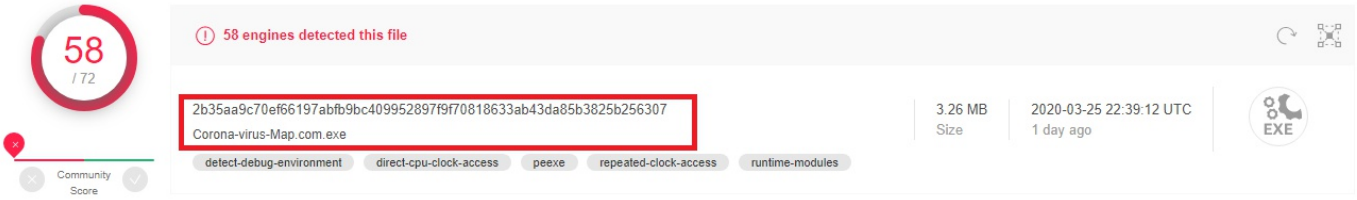
Depuis le début de la crise, c'est la carte interactive de l'université John Hopkins qui s'est affirmée comme une référence pour suivre l'avancée de l'épidémie sur la planète. Mais, au même temps, de nombreux autres sites ont vu le jour.



C'est en misant sur cette profusion d'informations que des hackers ont déployé un site vérolé. Les internautes qui peuvent y accéder à travers un moteur de recherche sont invités à télécharger une carte et ensuite à la lancer sur leur ordinateur. Le fichier contient, comme promis, une carte affichant en temps réel, les infections et décès liés au coronavirus sur la planète. Mais, en même temps, à l'insu des utilisateurs, un malware s'installe aussi sur l'ordinateur. Celui-ci, baptisé «Coronavirus Maps» et découvert par «MalwareHunterTeam» le 03 Mars 2020.

Une fois installée, cette fausse application active un code malveillant qui est connu sous le nom de «AZORult» et qui se vend depuis au moins 2016 dans le dark web par des hackers russes.

Ce code malveillant vole l'historique de navigation, les cookies, les mots de passe et les cryptomonnaies. Certaines variantes d'AZORult créent également une porte dérobée permettant aux pirates de se connecter sur la machine grâce au Remote Desktop Protocol (RDP).

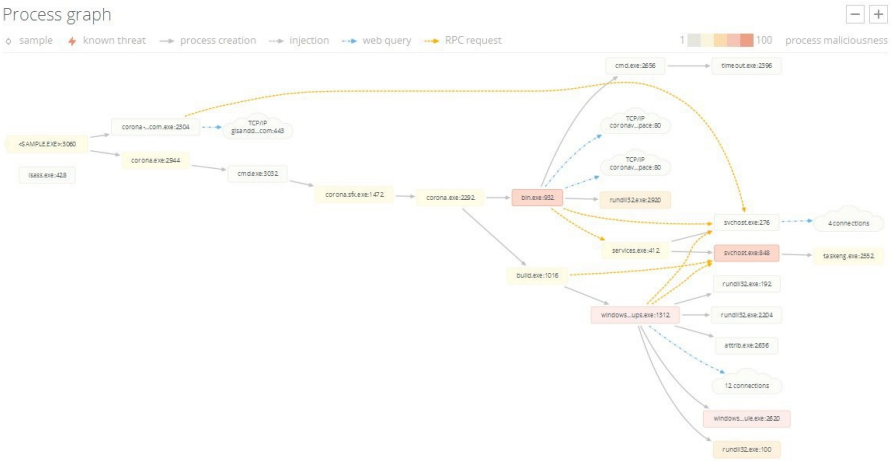


Résumé

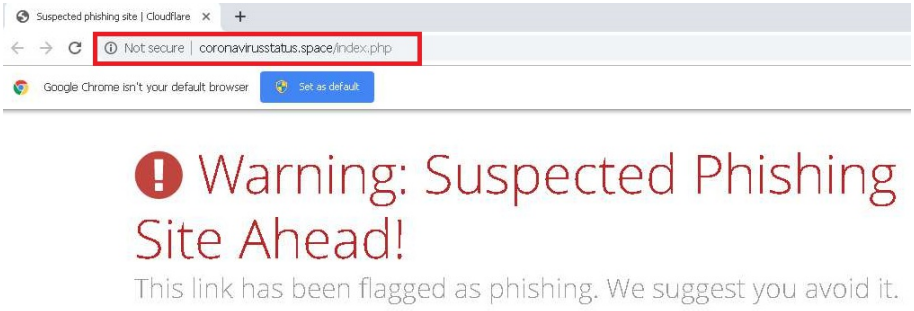
Nom	Corona-virus-map.com.exe
Aussi connu sous le nom	Carte des coronavirus
En relation	Corona.exe, Bin.exe
Type	Fichiers malveillants, cheval de Troie
Malwares associés	AZORult Banking Trojan, qui a été repéré pour la première fois en 2016
Particularités	Cette version de l'AZORult était vendue entre 200 $ et 700 $ sur les forums souterrains
Taille du fichier	3,26 Mo
Distribution	La principale source de distribution de logiciels malveillants s'est avérée être un site Web www.corona-virus-map.com, bien que les chercheurs disent que les courriers indésirables sont également utilisés pour diffuser des logiciels malveillants.
Activité	Tout comme les autres versions d'AZORult, ce virus est programmé pour voler diverses informations de la machine infectée, y compris les informations d'identification, les numéros de carte de crédit, les cookies, les données du portefeuille crypté, etc.
Dangers	La fonctionnalité prolongée des logiciels malveillants sur la machine peut entraîner diverses ramifications négatives, notamment des pertes financières, l'installation d'autres logiciels malveillants et même le vol d'identité
Résiliation	Pour supprimer l'infection de l'ordinateur, les utilisateurs doivent effectuer une analyse complète du système avec un logiciel anti-malware sophistiqué, tel que SpyHunter 5 ou Malwarebytes
Actions supplémentaires	Les victimes doivent surveiller leurs opérations bancaires en ligne afin d'éviter les transactions non sollicitées et réinitialiser tous les mots de passe qu'ils ont utilisés pendant l'infection. En outre, la réinitialisation du navigateur doit être effectuée pour se débarrasser des paramètres prédéfinis. Enfin, si Windows souffre de divers dysfonctionnements, Reimage pourrait corriger les entrées de registre endommagées et d'autres problèmes pour réparer la machine

Analyse technique: Principe de fonctionnement

Une fois exécuté, Corona-virus-map.com.exe créera un autre binaire sous le nom de Corona.exe et sera placé dans plusieurs emplacements différents à l'intérieur du dossier %AppData%. Ce processus exécute ensuite plusieurs autres processus, notamment bin.exe, timeout.exe et build.exe. De plus, le logiciel malveillant effectuera plusieurs autres modifications du système, y compris la modification au registre Windows, pour commencer ses tâches malveillantes.

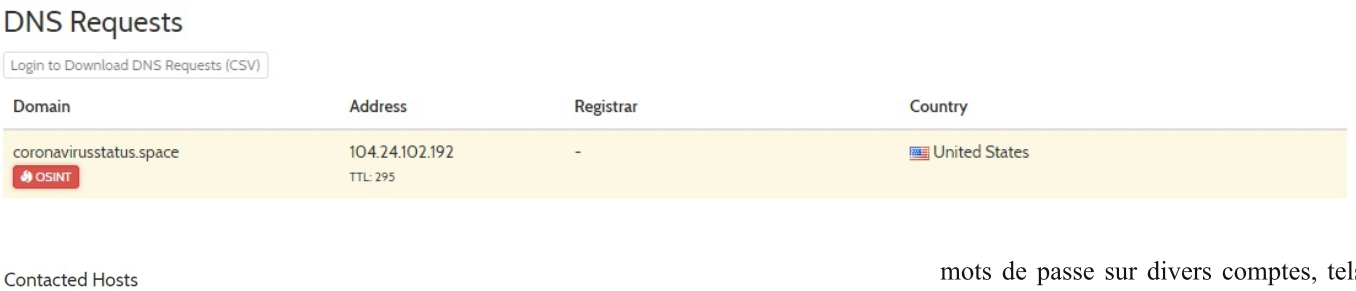


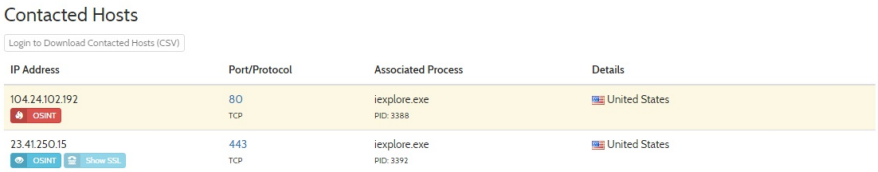
Le vecteur d'infection était probablement l'url « http://coronavirusstatus.space/index.php »



Le processus d'infection est beaucoup plus sophistiqué que cela, et la suppression d'un seul fichier n'aboutira à rien. Comme mentionné précédemment, les logiciels malveillants modifient considérablement le registre Windows, importent des fichiers malveillants, établissent une communication réseau, créent de nouveaux services, etc. Ainsi, pour une suppression complète de Corona-virus-map.com.exe, utiliser un logiciel anti-malware qui peut reconnaître cette menace.

Étant donné que le virus Corona-virus-map.com.exe génère un cheval de Troie bancaire, il est essentiel de prendre d'autres mesures après l'avoir supprimé de la machine infectée. Vous devez immédiatement modifier vos mots de passe sur divers comptes, tels que les e-mails, Steam, les services bancaires en ligne, etc. De plus, vous devez également annuler votre carte de crédit si des transactions non sollicitées commencent à l'inonder.





Corona-virus-map.com et Android

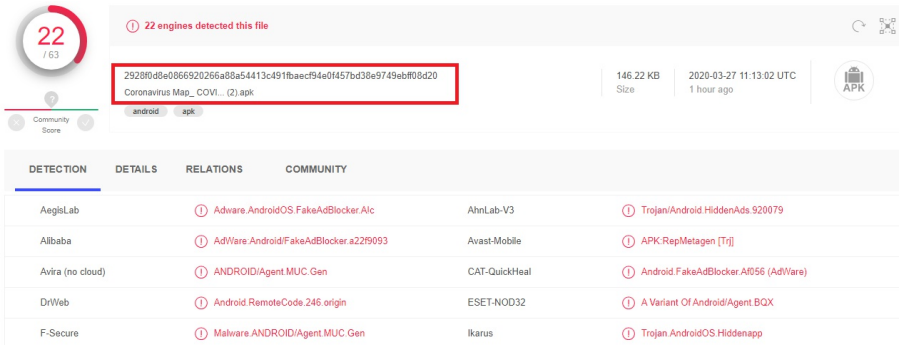
Le 27/03/2020 « MalwareHunterTeam » ont annoncé que l'application "Coronavirus Map_ COVI... (2).apk » active des codes malveillants qui infectent les systèmes Android

Mettre fin au malware Corona-virus-map.com.exe de votre ordinateur

Pour supprimer Corona-virus-map.com.exe de votre ordinateur, la fermeture manuelle du fichier ne suffira pas.

Source

https://twitter.com/malwrhunterteam



Comment guider vos enfants sur Internet?

Internet est un espace que les enfants se sont approprié très rapidement, et qui leur permet d'apprendre et de s'amuser. Et même s'il n'est pas toujours facile d'être à leurs côtés, il existe des solutions très simples pour les accompagner dans leur utilisation d'Internet.

L'antivirus, premier outil indispensable au quotidien

La sécurité sur Internet nous concerne tous, mais les enfants sont naturellement plus exposés aux risques liés aux sites malveillants et à la présence de virus sur le Web.

Le premier réflexe à adopter est donc d'installer sur votre ordinateur un antivirus efficace tel que ESET Internet Security®, qui protégera efficacement toute la famille. Vos enfants peuvent ainsi naviguer en toute sécurité, sans craindre qu'une action involontaire ne mette en danger votre ordinateur.

Installer un logiciel de contrôle parental

Il est aujourd'hui possible de trouver toutes sortes de contenus sur Internet, et certains de ces contenus ne sont pas destinés à un jeune public. Pour vous assurer que vos enfants ne risquent pas de tomber sur des contenus inappropriés, ESET Internet Security® inclut un outil de contrôle parental. Celui-ci vous permet de bloquer l'accès à plus de 20 catégories de sites Internet en fonction de l'âge de votre enfant, mais aussi d'ajouter manuellement d'autres sites qui ne vous sembleraient pas adaptés. Bien sûr, les paramètres du logiciel sont protégés par mot de passe, afin que les jeunes geeks en herbe ne soient pas tentés de le désactiver.

Mots de passe: donnez les bon reflexes à vos enfants !

Comme les adultes, les enfants peuvent être amenés à communiquer des informations personnelles sur Internet, pour s'inscrire sur un site pour enfants

ou sur les réseaux sociaux, par exemple. Il est donc important de leur apprendre dès leur plus jeune âge à protéger correctement ces données, en créant des mots de passe à la fois uniques et simples à retenir. Voici quelques conseils pour créer un mot de passe efficace :

• Plus un mot de passe est long (minimum 8 caractères), plus il est efficace : privilégiez une « phrase de passe », pour augmenter le nombre de caractères tout en facilitant la mémorisation
• Utilisez des caractères spéciaux (@, #, !, etc.), mais évitez de les utiliser en substitution de certaines lettres trop évidentes (comme le @ pour le A, par exemple)
• Évitez les mots du dictionnaire et les mots de passe évidents (123456, motdepasse, etc.)
• Modifiez vos mots de passe régulièrement, et privilégiez un mot de passe différent pour chaque compte.

Avec vos enfants, vous pouvez rendre l'exercice ludique en vous basant sur un poème appris à l'école ou en inventant une phrase de toutes pièces. C'est également le moment de leur rappeler qu'il n'est pas nécessaire de tout partager sur Internet, et que certaines choses doivent rester confidentielles.

En parlant à vos enfants des risques et de la manière de s'en prémunir, tout en vous équipant d'une solution complète telle qu'ESET Internet Security®, vous protégerez efficacement toute la famille et pourrez ainsi laisser vos enfants naviguer en toute sérénité.

Source:
https://www.eset.com/fr/about/newsroom/conseils/conseils/comment-guider-vos-enfants-sur-internet/

Un mot de passe plus complexe en quatre étapes

123456, motdepasse, 12345678, azerty, 12345 … sont les 5 mots de passe les plus utilisés. En dépit du fait que de plus en plus de personnes comprennent que la cybercriminalité est une menace croissante et que les violations de données sont monnaie courante, les usagers continuent à utiliser des mots de passe de faible protection pour leur simplicité à les retenir.

Pourtant, c'est grâce à ce genre de techniques que les cybercriminels pénètrent dans vos ordinateurs. Un petit effort est donc nécessaire pour mieux se protéger. La solution? Oubliez les mots de passe car ils sont faciles à craquer et pas assez forts pour offrir une sécurité appropriée. Cela est particulièrement le cas des mots de passe d'un seul mot.

Par quoi remplacer les mots de passe?
Par les « phrases de passe » ! Plus longues, plus complexes et faciles à retenir, elles vous aideront à être plus sûr et sécurisé. Voici un guide pratique sur la façon de créer une phrase de passe.

Étape 1 - Ajouter des mots pour créer une phrase
Disons que vous aimez lire. Ajouter quelques mots autour de lui afin qu'il ait un sens pour vous d'une manière significative :

Jaimelire

Voilà un bon début, mais il serait préférable d'ajouter une précision :

Jaimelirewelivesecurity

Étape 2 - Ajouter des capitales
Votre phrase de passe telle qu'elle est actuellement est beaucoup plus forte que le mot de passe d'origine. Cependant, elle a besoin de plus de détails. Ajouter des capitales, comme si vous souhaitiez insister sur chaque mot:

JaimeLireWeLiveSecurity

Étape 3 - Ajouter de la ponctuation
Considérez cette étape comme un élément décoratif, comme si vous étiez en train d'imaginer votre phrase de passe visuellement.

JaimeLireWeLiveSecurity!

Etape 4 - Ajouter des espaces pour plus de complexité
Beaucoup de personnes ne sont pas conscientes du fait que vous puissiez ajouter des espaces à votre mot de passe. Cela le rend beaucoup plus complexe:

J'aime lire WeLiveSecurity!

Ces quatre étapes vous permettent à partir d'un mot de passe faible, d'obtenir un mot de passe fort, plus complexe.

Il est également important de se rappeler les conseils suivants pour une sécurité supplémentaire de votre mot de passe :

• Eviter les mots de passe courts et préférer les phrases de passe longues
• Ne jamais réutiliser un ancien mot de passe
• Utiliser l'authentification à deux facteurs pour plus de sécurité
• Avoir une phrase de passe différente pour chaque compte
• Changer régulièrement les phrases de passe
• Utiliser un gestionnaire de mot de passe fiable

Et vous, quel est le pire mot de passe que vous ayez inventé ? Combien de fois avez-vous oublié votre mot de passe ?

Source:
https://www.eset.com/fr/about/newsroom/conseils/conseils/un-mot-de-passe-plus-complexe-en-quatre-etapes/

5 conseils pour sécuriser vos achats en ligne

Pour beaucoup d'entre nous, acheter en ligne est devenu un réflexe qui simplifie le quotidien : voyage, vêtements, courses alimentaires… Tout ou presque peut aujourd'hui s'acheter sur Internet. Mais au moment de payer, comment garantir la sécurité d'une transaction ? Voici 5 conseils à suivre pour se prémunir contre les risques de piratage.

Conseil n° 1 : vérifiez l'URL du site Internet

L'URL, c'est l'adresse d'un site Internet. Lorsque vous effectuez un paiement en ligne, elle doit impérativement commencer par « https:// ». Cela signifie que le site Internet est sécurisé. De plus, votre navigateur doit vous indiquer, au moyen d'un symbole en forme de cadenas, que la sécurité est bien établie entre votre ordinateur et le site que vous consultez. Si vous avez un doute sur le site qui vous demande vos coordonnées bancaires, il vaut mieux faire demi-tour.

Conseil n° 2 : faites vos achats uniquement sur votre ordinateur personnel

Ce conseil est a priori évident, mais il est important de le rappeler : vous vous apprêtez à transmettre des données sensibles, telles que votre numéro de carte bleue ou votre adresse personnelle. Il est dès lors déconseillé d'utiliser un ordinateur public, ou même l'ordinateur d'un ami. Il suffirait alors qu'un logiciel malveillant soit installé pour que vos données privées soient récupérées par des cybercriminels.

Conseil n° 3 : utilisez un navigateur sécurisé, l'outil idéal pour protéger vos données

Même si le site sur lequel vous vous apprêtez à payer vous paraît fiable et

que vous utilisez un réseau sécurisé, il se peut que des pirates informatiques parviennent à contourner les sécurités pour voler votre numéro de carte bleue. L'idéal est donc d'utiliser un navigateur sécurisé, comme celui inclut dans la solution ESET Internet Security®. Grâce à cet outil, vos données sont cryptées directement entre le clavier et le navigateur, ce qui empêche toute possibilité de récupération de vos données bancaires.

Conseil n° 4 : privilégiez les réseaux privés

Les réseaux publics doivent, par essence, être faciles d'accès : c'est pourquoi ils sont le plus souvent dépourvus de toute protection. On comprend donc facilement pourquoi il vaut mieux ne pas utiliser ce type de réseau pour effectuer un achat en ligne. Un hacker pourrait facilement accéder à votre ordinateur et à ce que vous y faites, et donc dérober sans difficulté votre numéro de carte bleue.

Conseil n° 5 : évitez d'enregistrer vos données en ligne, ou protégez-les efficacement

De plus en plus de sites Internet vous proposent d'enregistrer votre numéro de carte bleue dans votre compte, afin que vous n'ayez pas à les saisir à nouveau à chaque achat. C'est une fonctionnalité très pratique – surtout sur les sites sur lesquels vous achetez souvent, mais attention : l'accès à votre compte doit absolument être protégé par un mot de passe fort pour éviter que ces données trop soient facilement récupérables par les cybercriminels. Voici quelques conseils pour créer un mot de passe efficace :

• Privilégiez un mot de passe long (minimum 8 caractères), voire une « phrase de passe », pour augmenter le nombre de caractères sans compliquer la mémorisation
• Ajoutez des caractères spéciaux, mais évitez les substitutions trop évidentes, telles que @ pour remplacer un A
• Évitez d'utiliser des mots du dictionnaire ou des mots de passe évidents tels que 123456, motdepasse, etc.
• Changez vos mots de passe régulièrement, et n'hésitez pas à en utiliser un différent pour chaque compte.

Source:
https://www.eset.com/fr/about/newsroom/conseils/conseils/5-conseils-pour-securiser-vos-achats-en-ligne/

CONTRIBUTION: Tounsi Chaima, INSAT

Mon enfant est en confinement : quelles mesures de sécurité à prendre

En cette période de confinement, l'usage des écrans semble être la meilleure alternative à la vie qu'on a eu pré-coronavirus. Chez les enfants, en particulier, cet usage est même plus excessif que chez les adultes.

Devant cette explosion numérique, beaucoup de parents posent la question légitime : Faut-il avoir peur des écrans?

Les écrans développent-ils une addiction ?
Indéniablement. Les écrans se présentent comme étant un portail vers l'autonomie, la socialisation et le divertissement, bref, une rupture avec la solitude et la dépendance matérielle. Les outils de connaissances, les jeux vidéos, et les dernières tendances sont mis à disposition sans restreinte. Ainsi, ces appareils peuvent causer, notamment sur des personnalités fragiles ou en cours de construction, un sentiment de rassurance et de réconfort, de plaisir d'accomplissement de soi, et par suite d'addiction.

Quels risques peuvent menacer mon enfant en ligne ?
Sans accompagnement et sans encadrement, l'enfant ou l'adolescent est une victime facile aux personnes malicieuses. Pour les plus jeunes, le typosquattage et le piégeage peuvent amener les enfants dans des endroits inappropriés et désagréables sur le Web, parfois choquantes pour leur âge. D'autant plus, l'hameçonnage (Le phishing) c'est-à-dire l'utilisation d'e-mails qui tentent d'inciter les gens à cliquer sur des liens ou des pièces jointes malveillants, deviennent un risque pour les enfants.

Ceux-ci peuvent être particulièrement difficiles à détecter pour eux, car souvent, le message semble provenir d'une personne légitime,
soit via les courriels (le spam), les textes et les fonctions de clavardage des jeux et des mondes virtuels, mais souvent ces courriels contiennent des liens dangereux.

Pour les adolescents, le danger est un peu plus flagrant puisque c'est l'ado lui-même qui le cause sans en être conscients. Sous prétexte de ludisme et de divertissement, la jeunes se sont habitués à se prendre en photos, à photographier chaque instant de leur vie et à les mettre en ligne. Ce que les jeunes, voire même les adultes ignorent, c'est qu'à travers ces "simples" photos, non seulement leur vie privée mais aussi leur géolocalisation, leurs données biométriques et leur entourage seront tous exposés à des inconnus d'intentions malveillantes. Un autre risque ne devrait pas vous échapper, chers parents, un risque que même FBI avait considéré comme risque majeur : les Cyber prédateurs. Ces jours-ci, les prédateurs traquent souvent les plus jeunes sur Internet, profitant de leur innocence, du manque de supervision d'un adulte et abusant de leur confiance pour des objectifs de vol, de violence et de harcèlement physique et/ou moral.

Quelle cybersécurité pour protéger les enfants en ligne ?
Vous ne pouvez pas garder un œil sur les habitudes d'Internet de votre enfant à chaque minute de la journée, mais vous pouvez faire certaines choses de manière proactive pour garantir sa

sécurité et sa confidentialité en ligne.

L'un des moyens les plus simples de protéger vos enfants contre le contenu inapproprié en ligne est de définir des filtres qui affectent les sites vers lesquels ils peuvent naviguer.

Bien que vous ne puissiez pas toujours voir les sites auxquels vos enfants accèdent, vous pouvez bloquer automatiquement les sites inappropriés à l'avance. Les dispositifs de sécurité dotés de bloqueurs de sites vous permettent de bloquer des sites sur n'importe quel appareil qui se connecte au réseau domestique, mais ils peuvent également vous permettre de filtrer les sites que vos enfants consultent pour s'assurer que leur comportement en ligne est approprié et sûr.

Une autre façon de protéger vos enfants en ligne est de fixer des limites de temps à leur utilisation d'Internet. Lorsque vous contrôlez la durée et la fréquence de connexion de vos enfants, vous serez mieux en mesure de vous assurer qu'ils ne passent pas trop de temps en ligne, ce qui réduit le risque qu'ils visitent des sites qui ne sont pas sûrs ou sains.

En outre, vous devez strictement respecter la signalétique PEGI lorsque vous achetez un jeu vidéo pour votre enfant. La recommandation d'âge et les descripteurs de contenu vous permettent de vous assurer que le jeu est approprié à l'âge du joueur.

En bref, le meilleur moyen de protéger vos enfants est la sensibilisation. Dites

à vos enfants que toutes les informations qu'ils publient en ligne composent leur empreinte numérique et y restent, peu importe si leur profil est accessible au public ou privé. De nombreux enfants ont tendance à partager leur vie et celle de leur famille, les parents doivent donc souligner à quel point ceci peut être dangereux. Il y a des criminels qui utilisent OSINT (opensource intelligence) sur les réseaux sociaux pour perpétrer diverses fraudes, donc c'est certainement une mauvaise idée de laisser vos enfants donner trop de détails personnels.

N'oubliez pas que la protection concerne aussi leur santé mentale et psychologique. Rappelez-les régulièrement que les comportements malveillants en ligne ne viennent pas uniquement des étrangers comme des criminels et des pirates. L'intimidation à l'école s'est étendue pour devenir en ligne (Cyberharcèlement ou Cyberbullying), il peut provenir de camarades de classe et de pairs. C'est pourquoi il est important que les parents convainquent leurs enfants de les informer immédiatement dès qu'ils subissent des cyberharcèlements.

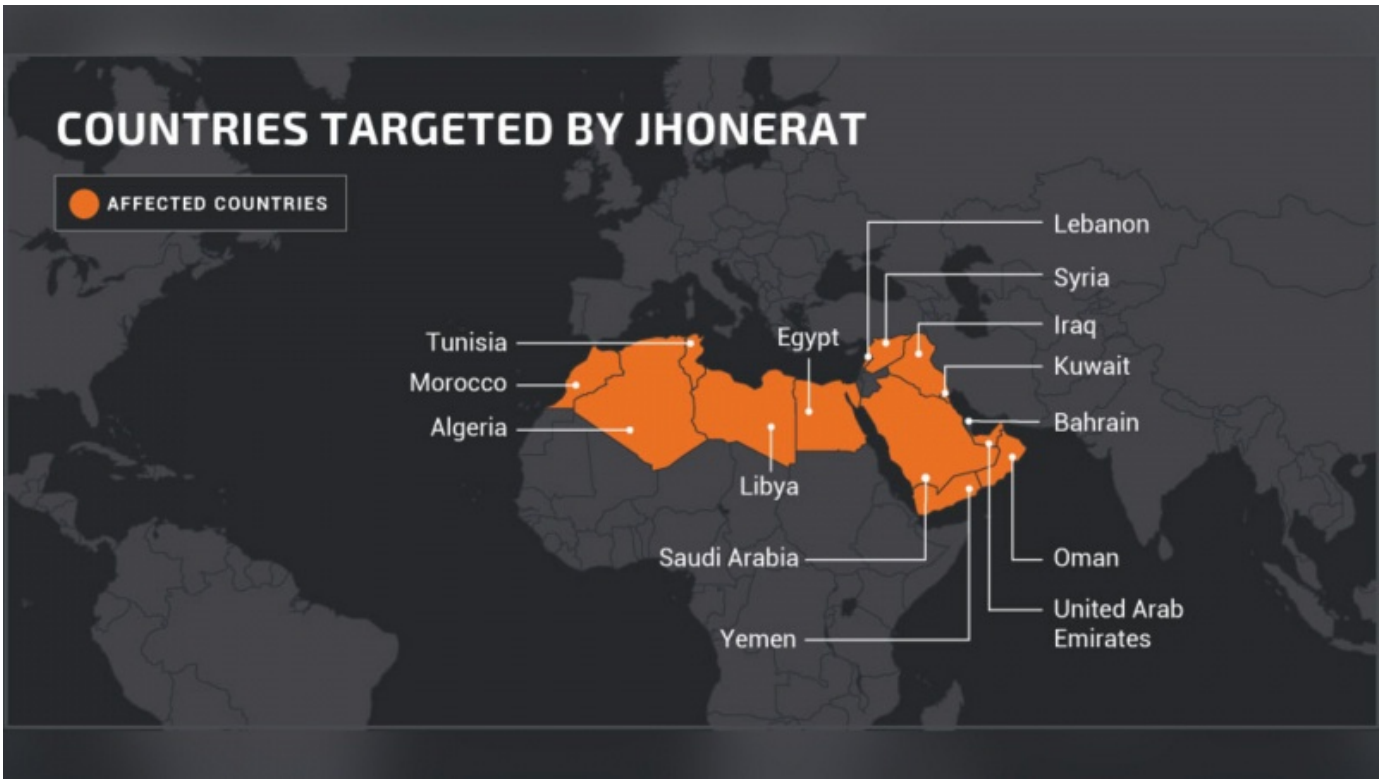
Que recommandez vous?

Éloignez vous des écrans. Vous êtes l'inspiration principale de vos enfants, ne les blâmez pas s'ils font pareil. En contre-partie, apprenez à vos enfants l'utilisation d'Internet à but d'apprentissage, de socialisation saine, et de divertissement pendant un temps restreint et limité. Pour le reste du temps, pratiquez d'autres activités loin du monde virtuel : pratiquez du sport ensemble à la maison, lisez des livres, faites du bricolage, etc.

Évidemment, la sécurité passe par un comportement responsable. Mais étant donné que l'enfant n'est pas vraiment conscient ni projectif des conséquences de ses actes, c'est votre rôle principal, chers parents, d'éduquer au mieux vos enfants.

Tounsi Chaima,
Etudiante à l'INSAT et Secrétaire Générale de Securinets.

Attention au malware « JHONERAT»



Récemment, un nouveau malware baptisé « JhoneRAT »a été découvert sur le net et ciblant particulièrement les pays arabes y compris la Tunisie. En effet, ce malware est un cheval de Troie développé en « Python », capable de s'échapper à la détection des anti-virus et les environnements de sandbox et qui utilise les services Cloud: Google Drive, Twitter, ImgBB et Google Forms pour télécharger les commandes d'attaque, transférer les informations personnelles des victimes et de prendre le contrôle total des machines infectées à distance. En outre, la méthode d'infection par JhoneRAT se fait en incitant les victimes à ouvrir des e-mails contenant des documents Microsoft Word malicieux. Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

• Sauvegarder régulièrement vos données sensibles sur des disques durs externes.
• Mettre à jour régulièrement votre système d'exploitation, vos navigateurs Web et aussi votre solution anti-malware.
• Mettre à jour les logiciels Adobe Flash Player et JAVA avec les dernières versions.
• 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.
• Appliquer des règles de contrôle d'accès rigoureuses à vos ressources partagées sur votre réseau.

Source
https://www.ansi.tn/veille/alertes-de-securite/attention-au-malware-jhonerat

Attention aux messages hoax

Nous attirons votre attention d'ignorer les messages parlant d'une vidéo intitulée « DANCE OF THE DAD » qui a été diffusée via les réseaux sociaux: « URGENT – Dites à tous les contacts de votre liste de ne pas accepter une vidéo appelée DANCE OF THE DAD. Il est un virus qui formate votre mobile. Attention, il est très dangereux. Ils ont annoncé aujourd'hui à la radio. Transmettre à autant que vous le pouvez. » Ces messages sont des hoax. Il n'y a pas de rapports crédibles sur un virus comme celui décrit. De ce fait, nous vous conseillons d'être vigilant et de suivre les mesures suivantes :

• Ignorer complètement tous les messages qui ont l'air d'être différents et qui présentent des fautes d'orthographe ou de frappe.
• 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.
• Eviter d'installer vos logiciels, applications ou extensions depuis des sources non fiables.

Source
https://www.ansi.tn/veille/alertes-de-securite/attention-aux-messages-hoax

Attention aux messages de phishing

Profitant de l'état de confinement sanitaire et le besoin actuel au télétravail, des cybercriminels internationaux ont lancé des campagnes de Phishing via les réseaux sociaux en incitant les internautes à communiquer leurs données personnelles pour participer aux jeux pièges comme les tirages au sort en ligne pour gagner soit un forfait Internet de 50 GB ou plus par mois, soit un stock alimentaire (Coca Cola) d'un mois, etc…
De ce fait, l'Agence Nationale de la Sécurité Informatique – ANSI vous recommande d'être vigilent et vous conseille de suivre les mesures préventives suivantes :

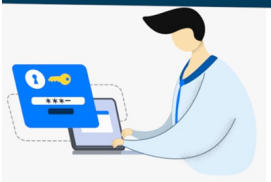
- Se renseigner sur la fiabilité des publicités ou des jeux en ligne en contactant immédiatement les publicateurs par téléphone avant d'y participer.
- Vérifiez l'authenticité des expéditeurs avant la lecture de chaque message reçu via les réseaux sociaux et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'ils contiennent et supprimer les immédiatement.
- Pour les messages qui demandent vos données personnelles, vérifiez s'ils comportent des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'ils contiennent et supprimer les immédiatement.
- Installez les extensions suivantes dans votre navigateur web pour vérifier la fiabilité des sites web visités et bloquer les annonces publicitaires douteuses:

• https://www.mywot.com/
• https://netcraft.app/browser/
• https://adblockplus.org/fr/

Dans le cadre de la mise en oeuvre du télétravail, il est crucial d'opter pour une stratégie de gestion des paramètres d'accès afin de se protéger contre les attaques sur les mots de passe.

Mise en oeuvre du télétravail
Consignes pour renforcer la sécurité des paramètres d'accès

1 Il faut choisir un mot de passe qui n'est pas lié à votre **identité** (CIN, Date de naissance..) avec, au minimum, **8 à 12 caractères** incluant des chiffres, des lettres et des symboles.



2 Il ne faut jamais demander à **une tierce personne** de créer un mot de passe pour vous, il faut immédiatement changer les mots de passe créés par défaut ou qui vous ont été communiqués par l'administrateur.

3 Dans le cadre du télétravail, il faut prevoir l'augmentation de la **fréquence de changement des mots de passe** (chaque 10 jours idéalement).

4 Beaucoup d'utilisateurs **stockent leurs mots de passe** dans des documents texte sur leurs ordinateurs ou même sur papier, cette pratique est à bannir pour éviter la perte ou le vol des paramètres d'accès.

5 Il ne faut jamais **utiliser le même mot de passe** pour différentes plateformes(email, vpn...) ou des comptes personnels ou professionnels, il est conseiller d'utiliser des mots de passe uniques pour chaque accès.

6 Il faut opter pour l'**authentification forte** (ou à 2 facteurs) car elle permet d'optimiser la sécurité des paramètres d'accès.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam

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

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

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

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

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

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

49 avenue Jean Jaurès, 1000 Tunis

(+216) 71 846 020

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