Un livre blanc SANS

Rapport SANS sur les principales nouvelles attaques et menaces

Rédigé par **John Pescatore**

Avril 2020

Sponsorisé par :

InfoBlox

Introduction

L'impact de l'épidémie du COVID-19 a mis en lumière le fait que les incidents dans le monde réel peuvent s'avérer bien plus préjudiciables que les attaques dans le monde virtuel. Cependant, le coronavirus a également mis en avant deux autres points-clés :

- une infrastructure numérique sécurisée et résiliente est nécessaire afin de survivre aux catastrophes médicales et environnementales.
- une réponse doit être apportée aux principaux risques et menaces avant que leur impact ne commence à se faire sentir.

Si l'on peut trouver un peu partout des statistiques dressant une rétrospective du nombre d'attaques lancées dans le cyberespace, il est plus difficile d'obtenir des analyses prévisionnelles sur lesquelles pourraient se fonder les responsables de la sécurité. Dans un contexte économique incertain, il est d'autant plus crucial pour les équipes en charge de la sécurité de hiérarchiser les ressources afin d'accroître l'efficacité de la gestion des menaces connues tout en minimisant les risques liés aux attaques émergentes. Ces 14 dernières années, le panel d'experts SANS spécialisés dans les cinq attaques les plus dangereuses (« Five Most Dangerous Attacks ») comble cette lacune à la RSA Conference[1] annuelle. Le présent livre blanc SANS prend pour point de départ une série de statistiques issues de trois des sources les plus fiables en matière de fuites de données et de logiciels malveillants ; il synthétise ensuite les conseils spécialisés des instructeurs SANS membres du panel RSA et détaille les menaces auxquelles doivent prêter attention les équipes chargées de la sécurité en 2020 et à l'avenir – et comment y remédier.

[1] www.rsaconference.com/

Données de base des fuites et menaces en 2020

Vulnérabilités et attaques ne tiennent pas vraiment compte du calendrier : le Nouvel An ne modifie pas considérablement l'apparition des menaces. Aussi, il est important de revenir en arrière pour comprendre les pratiques devenues courantes et prédire ce que seront vraisemblablement les types et périmètres des nouvelles menaces. Si de nombreux rapports sur les menaces sont publiés tous les ans, seules quelques ressources indépendantes de toute solution de fournisseur spécifique et reposant sur des méthodologies cohérentes sont disponibles année après année.

SANS estime que l'Identity Theft Resource Center (ITRC) Annual Breach Report[2], le Microsoft Security Intelligence Report (SIR)[3] et le Center for Internet Security's Multi-State Information Sharing and Analysis Capability (MS-ISAC)[4] se sont avérés pertinents au fil des ans.

L'ITRC effectue un suivi des informations officiellement publiées sur les fuites de données aux États-Unis depuis 2005 et fait appel à une méthodologie cohérente apportant suffisamment de visibilité et de reproductibilité pour des comparaisons constructives d'une année sur l'autre. Pour près de la moitié des fuites recensées, le nombre d'informations exposées reste inconnu ; la valeur absolue des nombres est donc en-deçà des totaux effectifs mais donne malgré tout un bon aperçu des tendances.

Comme cela est noté dans le Tableau 1, le nombre total de fuites en 2019 a augmenté de 17 % en 2018 après un déclin de 23 % l'année précédente.[5]

Tableau 1. Comparaison ITRC des fuites en 2018 et 2019[6]

Fuites de données et informations exposées par secteur et par an						
	2019			2018		
Secteur	Nombre de fuites	Informations sensibles exposées	Informations non sensibles exposées	Nombre de fuites	Informations sensibles exposées	Informations non sensibles exposées
Entreprises	644	18,824,975	705,106,352	575	438,952,056	1,570,602,391
Médecine/santé	525	39,378,157	1,852	369	10,632,600	2,800
Gouvernement/armée	83	3,606,114	22,747	100	18,447,924	60,085,000
Banque/crédit/finance	108	100,621,770	20,000	135	1,778,658	Non connu
Éducation	113	2,252,439	23,103	78	1,414,624	39,690
Totaux	**1,473**	**164,683,455**	**705,174,054**	**1,257**	**471,225,862**	**1,630,729,881**

À première vue, les données indiquent que le nombre total d'informations sensibles exposées a baissé de 65 %. Cependant, un faible nombre de fuites de très grande ampleur fausse les données. En 2018, la fuite de 383 millions d'informations du système de réservation de la Marriott Corporation a été, à elle seule, responsable de plus du double du nombre total d'informations exposées en 2019. De la même façon, en 2019, une fuite gigantesque – survenue dans la banque Capital One et concernant 100 millions d'informations – a représenté 99 % de la totalité des états financiers exposés l'an passé. Abstraction faite de ces deux fuites titanesques, le nombre total d'informations exposées en 2019 a baissé de 26 % par rapport à 2018. Ces chiffres s'inscrivent dans la continuité de la tendance

[2] "2019 End-of-Year Data Breach Report," www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

[3] www.microsoft.com/securityinsights

[4] www.cisecurity.org/ms-isac/

[5] "SANS Top New Attacks and Threat Report," April 2019, www.sans.org/reading-room/whitepapers/analyst/top-attacks-threat-report-38908, p. 2, Table 1. [Registration required.]

[6] "2019 End-of-Year Data Breach Report," www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

de l'année dernière où les plus petites organisations étaient la cible des menaces. Dans l'ensemble, de nombreuses grandes entreprises ont amélioré leurs défenses contre les attaques reposant sur une installation de logiciels malveillants, rendant ainsi plus difficile l'exfiltration de données de base.

Les données ITRC montrent que les organisations du secteur de la santé ont enregistré une forte croissance à la fois dans le nombre et la taille des fuites. Cette statistique est très parlante étant donnée l'importance des services médicaux requis pour gérer la pandémie de COVID-19. Des rapports du début de l'année 2020 montrent une augmentation du nombre d'attaques contre les services médicaux et les sites connexes.

Le rapport sur les fuites de l'ITRC prend en charge le calcul d'une métrique particulièrement pertinente chaque année : le nombre moyen d'informations exposées par fuite. Les coûts variables pour l'entreprise étant proportionnels au nombre d'informations exposées, cette métrique offre une bonne estimation du coût moyen par incident.

Le nombre moyen d'informations par fuite semble avoir connu une baisse considérable de 70 % pour passer de 374 881 en 2018 à 111 801 en 2019. Toutefois, si l'on fait abstraction des deux fuites gigantesques, ce chiffre correspond à une baisse de seulement 37 % en termes de taille moyenne des fuites.

En ce qui concerne les fuites avec une tranche d'informations exposées comprise entre 50 000et 500 000, une estimation empirique de 100 dollars par information en termes de coûts importants (n'inclut pas les coûts accessoires tels que la fluctuation du cours des actions ou l'atteinte à la réputation) s'est révélée être précise.[7] Ceci indique que le coût moyen d'une faille en 2019 s'élevait à environ 4,4 millions de dollars par rapport à 7 millions en 2018.

Le rapport ITRC se concentrant sur les fuites, les attaques par déni de service (DoS) ou déni d'accès – telles que les logiciels de rançon et autres corruptions qui n'impliquent pas une exfiltration de données – ne sont pas représentées. Le SIR de Microsoft collecte en continu des informations de plusieurs centaines de millions d'appareils Windows exécutant AutoUpdate et des outils Microsoft intégrés populaires tels que l'outil de suppression de logiciels malveillants, le scanner de sécurité, le composant antivirus Windows Defender et d'autres sources encore. Le SIR de Microsoft est presqu'exclusivement axé sur les attaques contre les PC et serveurs Windows – la majorité des attaques d'utilisateurs réussies ciblant des utilisateurs Windows. En outre, Windows recoupe une grande part du marché des systèmes d'exploitation pour serveurs.

Le SIR est en général publié deux fois par an, mais, au moment de la rédaction du présent livre blanc, Microsoft propose uniquement un site d'analyse de données en ligne plutôt que des rapports en bonne et due forme. Reflétant la tendance sur l'ensemble de l'année 2018, les dernières données du SIR ont montré des baisses dans les simples attaques de logiciels malveillants. Ceci-dit, deux domaines principaux ont continué à enregistrer une augmentation : le hameçonnage et les attaques à base de logiciels de rançon.

[7] www.gartner.com/document/485803 [Inscription requise.]

Des campagnes de hameçonnage extrêmement ciblées

Comme nous l'avons indiqué plus tôt, de nombreuses entreprises ont amélioré leur capacité à prévenir ou à détecter et solutionner plus rapidement les attaques standard avec installation de logiciels malveillants. Ces améliorations de la réactivité des entreprises a conduit les pirates à se concentrer sur les êtres humains vulnérables de l'équation – les utilisateurs de PC ou les administrateurs de serveurs et de services en cloud. La sensibilisation au hameçonnage en entreprise, les programmes de formation et l'adoption de normes plus strictes d'authentification des e-mails et du DNS ont rendu la tâche plus difficile aux pirates recourant au hameçonnage. Les attaques à base de hameçonnage sont malgré tout devenues de plus en plus sophistiquées et ciblées – et ont recours à davantage de « canaux », la messagerie textuelle et vocale p. ex.

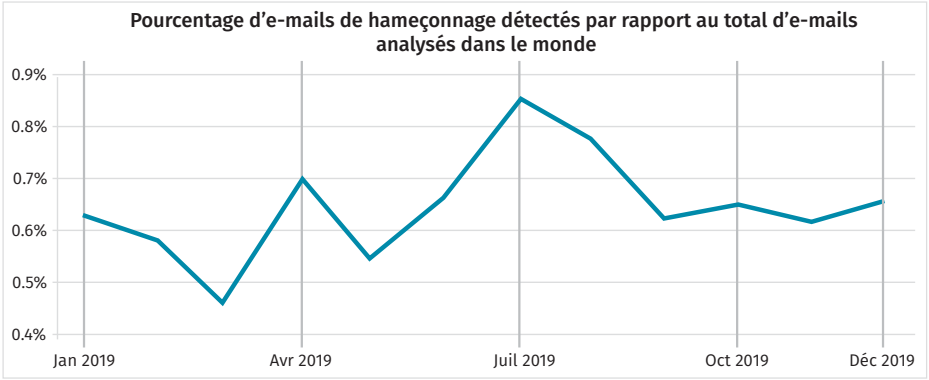

Figure 1. Percentage of
Pourcentage d'e-mails de hameçonnage en 2019 [8]

Les données SIR ne révèlent qu'une croissance minimale année après année des occurrences de hameçonnage (voir la Figure 1), mais on observe des pics correspondant à des « campagnes » – des vagues ciblées de hameçonnage qui se greffent sur des cibles connexes comme le secteur de la santé ou des événements majeurs à l'image du COVID-19. En raison de la distanciation sociale obligatoire, ces attaques vont progresser en parallèle de l'intensification des réseaux sociaux et des systèmes de réunion en ligne qui connaissent actuellement un pic d'utilisation. Ces sites exposent souvent une grande quantité d'informations que les pirates mettent à profit afin de créer des attaques extrêmement ciblées.

Logiciels de rançon : le fléau de l'État et des organisations locales

À présent, presque tout le monde sait ce qu'est un logiciel de rançon9 – des attaques qui cryptent les fichiers de données et/ou les fichiers exécutables afin d'interrompre les activités commerciales et d'exiger le paiement d'une somme (rançon) en échange de la clé de décryptage. Nombre de ces attaques reposaient sur de simples techniques à base de hameçonnage et de logiciels malveillants, et l'amélioration de l'anti-hameçonnage et des solutions EDR (Endpoint Detection and Response) a permis de contrecarrer ces attaques. Toutefois, beaucoup de petites entreprises, en particulier les organisations gouvernementales et locales, n'ont pas été en mesure de réaliser de tels progrès. Les pirates ont rapidement évolué pour s'attaquer à ces structures vulnérables.

[8] « Microsoft Security Intelligence Report: Phishing email detection », www.microsoft.com/securityinsights/Phishing

[9] « OUCH Newsletter: Ransomware », août 2016, www.sans.org/security-awareness-training/ouch-newsletter/2016/ransomware

[10] « Microsoft Security Intelligence Report: Ransomware encounter rates », www.microsoft.com/securityinsights/Ransomware

Résultat : l'amélioration de la stratégie de sécurité de base est la clé pour éviter ou atténuer la plupart des attaques matérielles. Les progrès réalisés en la matière ont entraîné un recul du nombre global de fuites signalées aux États-Unis, ce qu'illustre la Figure 2. La minimisation des vulnérabilités est également la clé pour s'éviter de figurer sur cette liste. Les organisations doivent contrôler les éventuelles vulnérabilités de tous leurs logiciels avant de les déployer dans leurs environnements de production. De plus, elles doivent régulièrement analyser toutes les configurations de leurs serveurs, PC et appareils de réseau afin d'y détecter de potentiels écarts par rapport aux normes de sécurité.

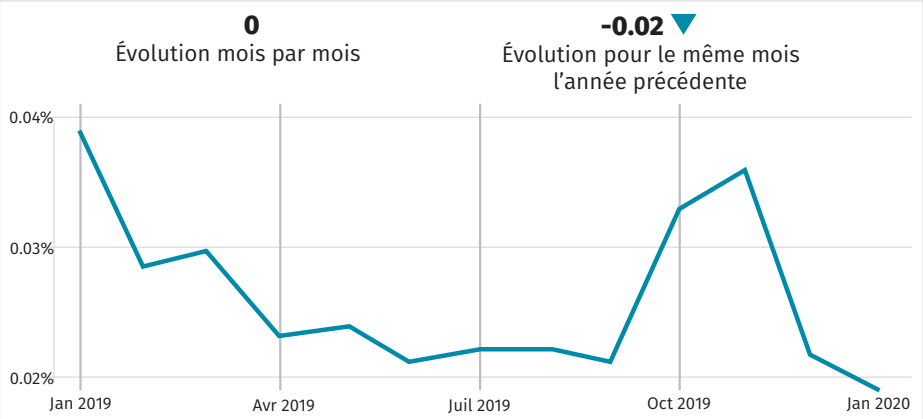

Figure 2. Attaques de logiciels de rançon en 2019[10]

Les attaques qui ont causé le plus de dégâts à chaque société victime sont les attaques extrêmement ciblées – elles continuent à s'intensifier et il est souvent impossible de les prévenir complètement. La clé pour minimiser les dégâts causés par ces attaques ciblées sophistiquées est la détection plus rapide des événements suspects favorisant l'adoption accélérée de mesures d'atténuation plus efficaces. L'utilisation d'outils EDR (Endpoint Detection and Response) et de fonctionnalités avancées comme la technologie d'isolement de navigateur peut renforcer la stratégie de sécurité de base tout en offrant une atténuation ou une prévention des dégâts. L'exploitation et l'analyse d'informations précises et opportunes sur les menaces doivent constituer des apports majeurs dans l'optimisation des processus de sécurité, la mise à jour des stratégies et le processus décisionnel relatif aux ressources de sécurité.

Étude approfondie des logiciels de rançon : organisations étatiques et locales

Le Center for Internet Security gère le MS-ISAC, qui met à disposition des ressources centrales pour la collecte d'informations sur les cybermenaces et le partage d'informations entre les États et les organisations locales et tribales. En 2019, le MS-ISAC a constaté une augmentation de 153 % des signalements d'incidents de logiciels de rançon à l'échelle étatique, locale, tribale et territoriale. Ces incidents ont soit été signalés par la victime, divulgués par un tiers de confiance ou mis en lumière par des rapports publics. La Figure 3 montre la répartition mensuelle (pourcentage) des incidents de logiciels de rançon signalés en 2018 et 2019.

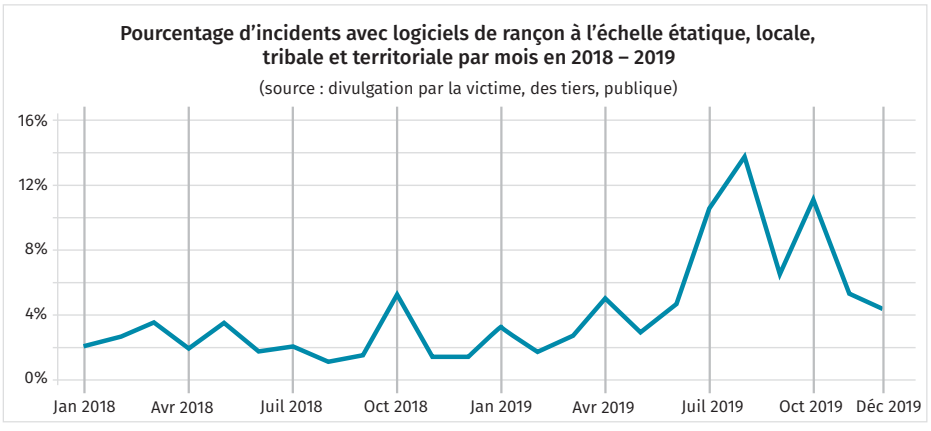

Figure 3. Incidents avec logiciels de rançon en 2018 et 2019[11]

[11] www.cisecurity.org/ms-isac/

[12] www.cisecurity.org/ms-isac/

Le MS-ISAC attribue principalement cette croissance à deux types d'attaques : une hausse dans les cas de logiciels de rançon Ryuk et une augmentation des incidents associés à des pirates soudoyant des fournisseurs de services d'infogérance pour envoyer des logiciels de rançon à leurs clients. Ryuk, Sodinokibi et Phobos ont été les trois variantes de logiciels de rançon les plus signalées en 2019.

Ryuk établit un accès au réseau à l'aide du cheval de Troie bancaire TrickBot. Cette méthode fonctionne car les infections TrickBot sont répandues, souvent inaperçues pendant un certain laps de temps et peuvent s'étendre à un réseau complet.
La variante de logiciel de rançon Sodinokibi est la principale responsable de l'augmentation des infections par les fournisseurs de services d'infogérance, qui tirent parti de la relation de confiance entre les fournisseurs tiers et leurs clients. La variante de logiciel de rançon Phobos, quant à elle, cible généralement des ports RDP (Remote Desktop Protocol) à faible sécurité pour en faire un vecteur d'infection initial, bien que cette technique soit connue depuis plusieurs années des pirates recourant aux logiciels de rançon. Le Tableau 2 montre la répartition de ces variantes en 2019.

Tableau 2. Les 3 principales variantes de logiciels de rançon en 2019[12]

Pourcentage des variantes de logiciels de rançon dans les incidents signalés	
Ryuk	22.7%
Sodinokibi	10.9%
Phobos	2.8%

L'opinion des spécialistes : le panel d'experts SANS des menaces à la RSA Conference 2020

La RSA Conference a fait ses débuts en 1991 et est devenue la plus grande conférence sur la cybersécurité au monde. Ces 14 dernières années, SANS y a présenté un panel d'experts SANS renommés faisant état de leurs opinions sur les attaques les plus dangereuses qui commencent à impacter les entreprises.13 Au fil des ans, les prédictions formulées par les instructeurs SANS lors de ces sessions se sont avérées extrêmement précises quant aux dommages dans le monde réel. Le panel d'experts des menaces de 2020, supervisé par Alan Paller, fondateur de SANS et directeur de recherche, se composait de :

- **Ed Skoudis**, SANS Faculty Fellow et directeur des formations SANS au cyber-range et en équipe
- **Heather Mahalik**, instructeur principal, institut SANS et directeur principal de criminalistique numérique, Cellebrite
- **Dr. Johannes Ullrich**, doyen associé à la recherche, SANS Technology Institute et fondateur et directeur, Internet Storm Center

Le panel d'experts des menaces de 2020 (de g. à dr.) : Ed Skoudis, Heather Mahalik et le Dr. Johannes Ullrich

Chaque expert SANS s'est concentré sur des domaines qu'il jugeait des plus importants pour l'année à venir. Ces domaines-clés incluent la prolifération des boîtes à outils et frameworks de commandes et de contrôles, les attaques « hors sol » (living off the land), la persistance très profonde, les risques croissants liés à la perte – même temporaire – du contrôle physique de leurs appareils mobiles par les utilisateurs et les vulnérabilités

[13] « The Five Most Dangerous New Attack Techniques and How to Counter Them », www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2020, 27 février 2020.

[14] « Applying Security Awareness to the Cyber Kill Chain », 31 mai 2019, www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

dans les contrôles du périmètre de sécurité et les agents Web qui couvrent le périmètre. La section ci-dessous synthétise les vues des experts sur chaque problème et leurs conseils pour éviter ou minimiser les dommages.

Boîtes à outils et frameworks de commandes et de contrôles

Ed Skoudis a pour la première fois souligné la prolifération d'outils et de frameworks de commandes et de contrôles (C2) utilisés par les pirates. Les menaces les plus avancées procèdent en suivant des phases distinctes définies dans le modèle populaire Cyber Kill Chain® décrit pour la première fois par Lockheed Martin.14 Souvent, le pirate utilise des techniques simples pour faire une première incursion dans une cible via l'installation d'un fichier exécutable de logiciel malveillant limité. Cet exécutable fait ensuite intervenir des sites C2 contrôlés par le pirate via des connexions qui utilisent des techniques évitant toute détection. Les sites C2 téléchargeront alors des exécutables plus avancés et ciblés afin de lancer un logiciel de rançon, une exfiltration de données ou des attaques de surveillance à long terme.

> *« Nous avons assisté à une explosion du nombre et de la sophistication des outils à la disposition des pirates l'année écoulée. Il existe une pléthore d'outils différents que les pirates peuvent utiliser pour contrôler les systèmes qu'ils ont corrompus au sein d'environnements cibles. La bonne nouvelle est que ces outils sont également accessibles à des fins d'analyse par les testeurs d'intrusion et les équipes qui testent les stratégies de défense de l'entreprise. »*
>
> —Ed Skoudis

La conception et le développement d'une fonctionnalité C2 est une entreprise sophistiquée, souvent hors de portée de pirates moins talentueux. Les boîtes à outils et frameworks C2 offrent des composants modulaires, de sorte que les attaques ciblées et évasives deviennent accessibles à tous les pirates informatiques. Il existe une pléthore d'outils différents que les pirates peuvent utiliser pour contrôler les systèmes qu'ils ont corrompus au sein d'environnements cibles. La connaissance de ces outils est primordiale pour que les testeurs d'intrusion puissent émuler des adversaires et que les équipes rouges comprennent les stratégies et les techniques appliquées. Toutefois, ces outils sont si nombreux qu'il peut être difficile de les trier.

C'est pourquoi Jorge Orchilles, instructeur SANS, et de nombreux autres volontaires ont constitué ce qu'ils appellent la « C2 Matrix ».15 Ce site Web vous permet d'analyser tous les différents canaux C2 publiquement, gratuitement, voire commercialement, à la disposition des pirates pour contrôler leurs logiciels malveillants au sein d'un environnement cible. Il répertorie l'ensemble des différents outils et dispose d'un écran interactif que vous pouvez utiliser pour voir les différents ensembles de fonctionnalités, notamment les différentes manières de communiquer sur le réseau, et d'autres tâches. C'est un outil d'apprentissage sensationnel.

Atténuation : afin de se défendre contre des attaques recourant à ces outils, Skoudis a indiqué que les équipes en charge de la sécurité doivent surveiller et contrôler de manière proactive le trafic sortant de leurs environnements. L'an passé, Skoudis avait mentionné Rita, un outil gratuit de Black Hills Information Security qui analyse le trafic réseau afin de détecter toute activité suspecte.16 Cette année, il a insisté sur DeepBlueCLI de l'instructeur SANS Eric Conrad.17 Il s'agit d'un autre outil gratuit auquel vous intégrez les journaux d'événements Windows à des fins d'analyses variées. Écrit en PowerShell, il

[15] www.thec2matrix.com/about

[16] www.blackhillsinfosec.com/projects/rita/

[17] https://drive.google.com/file/d/0ByeHgv6rpa3gNU4wLVZKNjd4cTA/edit

vous indique quels événements lui semblent suspects, p. ex. en détectant des attaques de pulvérisation de mot de passe ou des tentatives erronées de mot de passe, ou en vous indiquant des activités sous-jacentes au sein de l'environnement cible.

Le traçage et le contrôle d'applications contribuent grandement à la protection contre les frameworks C2, car ils limitent les éléments que le pirate peut exécuter sur le système cible. Toutefois, les entreprises ont habituellement du mal à déployer un traçage d'applications performant et les pirates ont appris comment imiter des applications autorisées pour échapper aux contrôles moins rigoureux.

Attaque hors sol

Skoudis a également décrit les attaques « hors sol » (living off the land), une expression formulée pour la première fois par Christopher Campbell et Matt Graeber. L'idée ici est d'utiliser les ressources et fonctionnalités d'un système d'exploitation pour qu'il s'attaque lui-même, puis de se servir de ce système comme rampe de lancement pour attaquer d'autres cibles. Skoudis dit de cette technique qu'elle consiste à « retourner le système d'exploitation contre lui-même comme un rootkit. » Et effectivement, les pirates utilisent des éléments du système d'exploitation pour attaquer ce dernier, en gardant à l'esprit l'interprétation que fera un analyste SOC lorsqu'il analysera ces événements. Le pirate manipule l'analyste en créant des effets malveillants qui ressemblent à une activité normale du système.

Skoudis a salué le bien-fondé du projet Living Off The Land Binaries And Scripts (LOLBAS), qui tente de documenter tous les codes binaires, scripts et bibliothèques pouvant être utilisés pour les techniques « hors sol ».[18] Il comprend plus de 100 exécutables différents pour Linux, macOS et Windows permettant aux pirates d'attaquer ces systèmes de l'intérieur. Cette liste inclut tous les codes binaires, scripts et bibliothèques connus qui pourraient être utilisés par des pirates talentueux et testeurs d'intrusion/équipes rouges, avec une orientation sur les manières de contourner les contrôles d'applications comme nous l'avons indiqué précédemment.

Atténuation : outre le traçage, les équipes mauves sont le domaine-clé souligné par Skoudis permettant une détection et une atténuation efficaces des attaques hors sol. Les équipes bleues sont les équipes en charge des opérations de sécurité qui conçoivent, déploient et gèrent les contrôles de sécurité. Les équipes rouges sont les testeurs d'intrusion et les « adversaires amicaux » qui mettent à l'épreuve les défenses des équipes bleues et leur font des retours sur les vulnérabilités mises en évidence. Les équipes mauves recoupent les efforts combinés de ces deux groupes pour examiner les nouvelles techniques des pirates telles que LOLBAS, développer des barrières défensives plus efficaces et étudier la résistance de ces dernières face aux attaques des équipes rouges. Ceci peut accélérer considérablement la mise sur le marché dans une optique de nouvelles stratégies défensives efficaces. Voir la Figure 4.

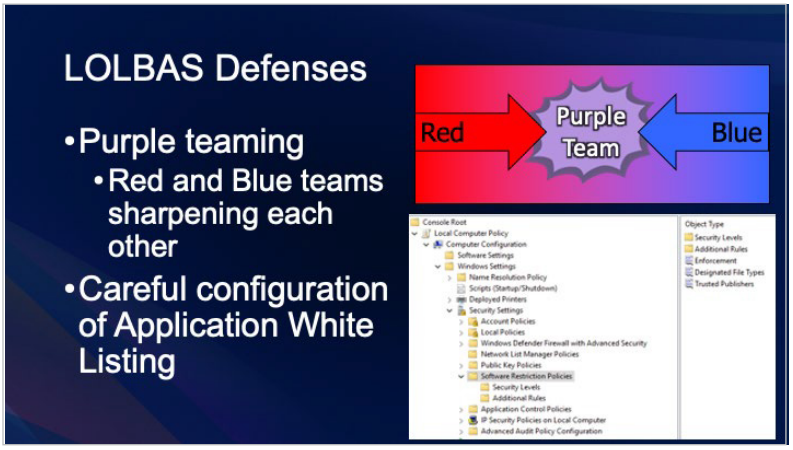

Figure 4. Défenses binaires et scripts hors sol (LOLBAS)[19]

[18] « Living Off The Land Binaries and Scripts (and now also Libraries) », https://github.com/LOLBAS-Project/LOLBAS/blob/master/README.md

[19] « The Five Most Dangerous New Attack Techniques and How to Counter Them », www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2020, 27 février 2020.

Persistance très profonde

Le dernier domaine détaillé par Skoudis concernait ce qu'il a appelé la persistance très profonde, essentiellement les fonctionnalités malveillantes enfouies dans les équipements, accessoires ou composants. Rubber Ducky en est un vieil exemple : il s'agit d'une clé USB pré-programmée qui, une fois connectée à une cible, émule un clavier et saisit des commandes dans le système pour ouvrir une fenêtre de terminal, y saisir un code de logiciel malveillant, enregistrer ce dernier et l'exécuter.

Le FBI a récemment lancé une alerte concernant des clés USB corrompues réceptionnées par des citoyens américains et accompagnées de promesses de gains après visionnement de publicités présentes sur le support.

Plutôt révolutionnaire à l'époque, cette technique a désormais été intégrée ce qui se présente comme un simple câble USB. Une version appelée USB Ninja est disponible pour la modique somme de 99 dollars à ceux d'un câble de charge de smartphone, mais ce modèle possède des fonctionnalités semblables à Rubber Ducky ; le produit inclut également un pont sans fil vers le réseau cible. Rubber Ducky et USB Ninja ne sont que deux exemples parmi d'autres. Les techniques pour incruster ces fonctionnalités malveillantes dans n'importe quel système pouvant se connecter (physiquement ou sans fil) à une cible ou pour les intégrer dans un produit ne connaissent pas de limites.

Atténuation : Skoudis a indiqué plusieurs niveaux d'atténuation :

renforcer la sensibilisation des utilisateurs. Les utilisateurs doivent savoir comment utiliser uniquement des appareils et câbles USB provenant du service informatique ou sous blisters de fournisseurs fiables.

soumettre à un examen minutieux les fournisseurs avec lesquels votre organisation n'a encore jamais collaboré et proposant des services à faible coût ou gratuits, et tester leurs produits dans un environnement sécurisé. Une gestion renforcée des risques liés aux fournisseurs est importante pour les entreprises faisant l'acquisition d'appareils (même de simples câbles) qui seront raccordés à ou installés sur des systèmes commerciaux critiques.

J'ai reçu une clé USB infectée par la voie postale !

Un jour de février, j'ai trouvé une petite enveloppe brune dans mon courrier que je ramenais à la maison. L'étiquette pré-imprimée ne contenait aucune adresse de retour et il n'y avait qu'un code-barres – aucun timbre ni affranchissement. Malgré tout, l'enveloppe ressemblait exactement au colis que l'on reçoit lorsque l'on commande un petit objet en ligne en provenance de Chine transitant par les services postaux américains.

À l'intérieur se trouvait une clé USB de 16 Go d'une marque que je ne connaissais pas, accompagnée d'une feuille de papier pliée contenant des instructions et un code-barres 2D. Les instructions me disaient de raccorder la clé à mon ordinateur, de cliquer sur l'une des récompenses affichées et de me rendre sur eBay pour l'acheter – ce serait gratuit ! Je pouvais sinon utiliser le code-barres 2D si je préférais réaliser l'opération depuis mon téléphone.

En tant que professionnel formé dans le secteur de la sécurité, j'ai toujours répété à tout le monde de se montrer prudent avec les clés USB d'origine inconnue, un peu comme le chewing-gum que nous mâchions après d'autres quand nous étions enfants. Vous n'aimeriez pas en ramasser un du sol et le porter à votre bouche, alors ne branchez pas à la « bouche » de votre ordinateur une clé USB de source inconnue.

J'ai pris des photos de tous ces éléments et me suis rendu sur les sites du FBI et des services postaux américains afin de signaler l'incident. Je n'ai eu aucun retour (hormis un accusé de réception de mon signalement). Une semaine plus tard, j'ai détruit la clé USB en mille morceaux, puis je l'ai jetée par mesure de précaution. Ce n'est que lorsque j'ai commencé mon travail sur le présent rapport que j'ai pris conscience qu'il existait des campagnes à grande échelle reposant sur cette approche.

– John Pescatore

[20] « From Spyware to Ninja Cable », 9 sept. 2019, www.darkreading.com/risk/from-spyware-to-ninja-cable/a/d-id/1335710, 27 février 2020.

vos partenaires de chaîne logistique et vous-même devez être vigilants et garantir la sécurité de la chaîne logistique pour tout ce qui a trait aux produits et services de votre entreprise.

Appareils mobiles : bonnes et mauvaises nouvelles

Mahalik a axé son travail sur les vecteurs d'attaques souvent négligés spécifiques aux téléphones mobiles : les pertes prévues et imprévues du contrôle physique de l'appareil. Les cas prévus surviennent lorsque l'utilisateur achète un nouveau téléphone ou en reçoit un nouveau au travail. Qu'arrive-t-il aux données sur ces téléphones et à l'accès pré-authentifié aux applications Web, services en cloud et VPN d'entreprise ? Nous constatons une pléthore d'exemples de ventes de smartphones sur eBay ou Craigslist où l'acheteur découvre ensuite une mine d'informations. L'ancien téléphone peut également être retourné au transporteur dans le cadre d'un échange contre un nouveau modèle et se retrouver dans un autre pays où il sera recyclé – peut-être même avant que les informations sensibles qu'il contient ne soient supprimées de l'appareil.

Mahalik a ensuite expliqué comment les *pertes imprévues d'appareil* sont soumises à l'attaque de débridage (jailbreak) d'iOS **`Checkm8`** sortie en septembre 2019.[21] À chaque fois qu'un utilisateur perdait le contrôle physique de l'appareil, ce dernier pouvait être corrompu. L'un des scénarios comportant le plus gros risque est celui des téléphones mobiles laissés dans les chambres d'hôtel ou temporairement confisqués par les agents d'aéroport dans les pays aux programmes de cybersécurité particulièrement actifs et agressifs. **Tous les appareils** iOS d'Apple exécutant les chipsets Apple A5 à A11 (soit principalement tous les appareils Apple de 2017, y compris l'iPhone 4 à X) sont vulnérables à **`Checkm8`**. Il s'agit d'une vulnérabilité bootrom décrite par le chercheur l'ayant mise en lumière comme « ne pouvant jamais être corrigée ».

> *« Nous sommes tous accros à nos téléphones, mais nous les perdons temporairement bien trop souvent. Des exploits comme Checkm8 et Checkra1n ont accru la nécessité d'améliorer nos méthodes de protection des appareils mobiles. »*
>
> – Heather Mahalik

Sorti peu de temps après, l'exploit **`Checkra1n`**, utilisé pour la vulnérabilité Checkm8, permet aux utilisateurs de débrider leurs propres téléphones et de contourner les mécanismes de l'App Store d'Apple – faisant céder les barrages pour les logiciels malveillants sur iPhone.[22] **`Checkra1n`** permet en outre aux pirates d'installer des programmes malveillants sur iPhone dès lors qu'ils ont un accès physique à l'appareil.

Mahalik a ensuite décrit un autre scénario qui met à mal une amélioration potentielle de la sécurité – reposant sur l'utilisation de la messagerie textuelle vers un téléphone mobile en tant qu'authentification à deux facteurs (2FA). Le problème survient lorsqu'un utilisateur change de téléphone ou d'opérateur et que, pour diverses raisons, il récupère un nouveau numéro de téléphone plutôt que d'opter pour un transfert de son ancien numéro. Tous les services 2FA utilisés sont rattachés à l'ancien numéro de téléphone, permettant à la personne qui met la main sur l'ancien numéro de téléphone de corrompre la 2FA et de s'approprier les comptes appartenant à l'utilisateur. Une fois le numéro modifié, la course est engagée.

[21] « New Checkm8 jailbreak released for all iOS devices running A5 to A11 chips », 24 sept. 2019, www.zdnet.com/article/new-checkm8-jailbreak-released-for-all-ios-devices-running-a5-to-a11-chips/

[22] « Just-Released Checkra1n iPhone Jailbreak Stirs Security Concerns », https://threatpost.com/checkra1n-jailbreak-stirs-concerns/150182/

Atténuation : Mahalik a énuméré une série d'étapes simples visant à réduire le risque d'apparition de ces attaques sur téléphones mobiles :

1. **Verrouillez votre téléphone.** Activez le déverrouillage par reconnaissance digitale ou faciale si votre appareil prend ces fonctions en charge et activez le verrouillage automatique sur la valeur la plus courte possible.
2. **Désactivez les vieux téléphones.** Si vous obtenez un nouveau téléphone, demandez au service informatique ou à l'opérateur de nettoyer l'ancien téléphone – ou détruisez-le à l'aide d'un marteau (et profitez-en pour soulager votre stress).
3. **Utilisez des téléphones « propres » à l'international.** Donnez des téléphones aux données nettoyées à tous les cadres voyageant dans des pays considérés comme étant à risque de cyberespionnage pendant toute la durée de leur déplacement. À leur retour, récupérez ces téléphones et nettoyez-les.
4. **Réinitialisez les appareils vulnérables.** Vous devez a minima réinitialiser les appareils iOS vulnérables après toute perte de contrôle physique.
5. **Ne modifiez pas les numéros des téléphones mobiles si cela n'est pas nécessaire.** Si vous vous apprêtez à modifier les numéros (y compris si vous donnez votre ancien téléphone à vos enfants), ouvrez chacune des applications pour lesquelles vous utilisez 2FA. Désactivez la fonction temporairement jusqu'à l'obtention du nouveau numéro ; activez à nouveau 2FA avec le nouveau numéro.

« Un périmètre à haute sécurité reste incontournable pour minimiser votre exposition aux attaques ; mais cette année deux tendances ont révélé des faiblesses dans les contrôles de sécurité existants et accru la nécessité d'adopter des stratégies plus agressives pour les agents Web installés sur les appareils des utilisateurs. »

– Dr. Johannes Ullrich

Les pirates décèlent des vulnérabilités dans les produits de sécurité

Dr. Johannes Ullrich s'est concentré sur deux domaines où les pirates trouvaient des vulnérabilités dans les produits de sécurité et sur les intrusions des périmètres de sécurité rendues possibles par la mauvaise qualité d'écriture des agents Web persistants. Le périmètre conventionnel a considérablement évolué ces dernières années, au fur et à mesure que les employés sont devenus plus mobiles et que les applications commerciales ont de plus en plus été hébergées à l'externe dans le cloud (au lieu d'être implantées dans les locaux du centre de données sur site). Le périmètre moderne est toujours dépendant des pare-feux et VPN de périphérie, mais il intègre de plus en plus souvent une empreinte de sécurité soit sur l'endpoint de l'utilisateur, soit dans un service de sécurité de cloud proxy entre l'utilisateur et les applications critiques.

La première tendance dans les menaces mise en évidence par Ullrich était l'exploitation exacerbée des vulnérabilités identifiées dans les produits de sécurité critiques utilisés dans le périmètre, p. ex. les pare-feux et les VPN.[23]

En avril 2019, Pulse Secure a publié des correctifs pour son produit d'accès à distance VPN Pulse Connect Secure.[24] Les vulnérabilités incluaient des failles de codage bien connues telles que le cross-site scripting, les dépassements de tampon et les injections de code

[23] www.cvedetails.com/vulnerability-list/vendor_id-15824/product_id-33650/Pulsesecure-Pulse-Connect-Secure.html

[24] www.us-cert.gov/ncas/alerts/aa20-010a

qui permettaient aux pirates de bénéficier d'une autorisation d'accès. En décembre 2019, Citrix a publié CVE-2019-19781, qui détaillait une traversée de répertoire dans Citrix (NetScaler) Application Delivery Controller qui permettait une exécution de fichiers à distance.[25] Des exploits ont été développés contre ces deux failles dès la mi-janvier 2020, comme l'illustre la Figure 5.

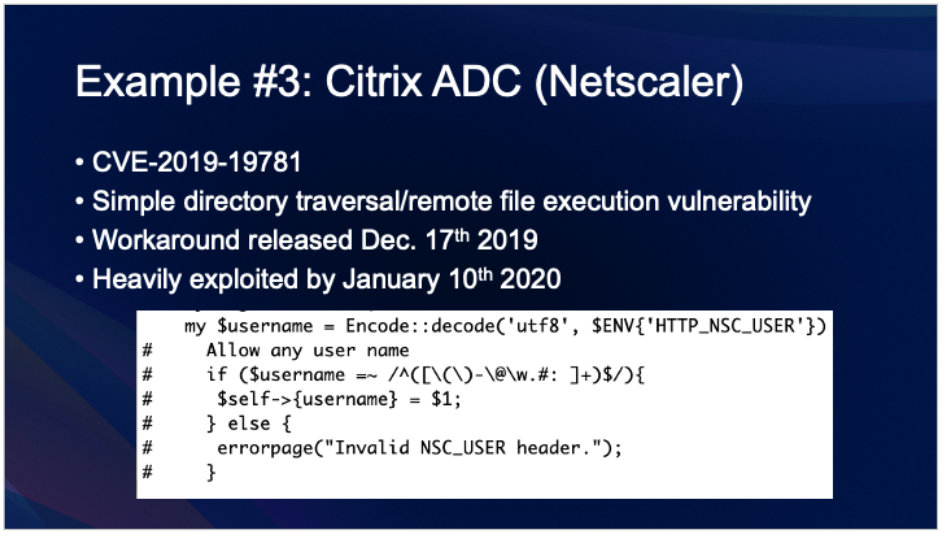

Figure 5. Synthèse de l'exploit Citrix ADC (NetScaler)[26]

De la même façon, en juillet 2019, Palo Alto Networks a publié une série de correctifs[27] pour le système d'exploitation PAN OS tournant sous tous les produits de pare-feux nouvelle génération Palo Alto Networks. Ces correctifs solutionnent des failles critiques liées à des injections de code et à du cross-site scripting. Des vulnérabilités critiques supplémentaires liées à des injections de code et à une élévation des privilèges dans PAN OS ont été signalées en novembre et décembre 2019, y compris CVE-2019-1744028, une restriction indue de la vulnérabilité des communications qui permettait aux pirates de bénéficier d'un accès racine sur un appareil exécutant PAN OS. Palo Alto Networks a attribué la sévérité la plus élevée possible (10) à cette vulnérabilité, indiquant ainsi qu'un correctif immédiat était crucial.

Les vulnérabilités critiques à n'importe quel niveau de logiciels ou d'applications indispensables pour l'entreprise sont assurément très dangereuses et doivent être corrigées dès que possible. Malheureusement, un grand nombre de processus et systèmes d'installation de correctifs en entreprise n'intègre pas de dispositifs de réseau et de sécurité (ou autre) bloquant l'installation d'agents ou l'accès facilité à ces agents.

Atténuation : Ullrich a indiqué que le conseil usuel de limiter et surveiller l'accès aux interfaces d'administration reste essentiel, mais s'avère insuffisant lorsque les vulnérabilités peuvent être exploitées hors de l'interface d'administration ou depuis un autre serveur de sécurité critique tel que le VPN utilisé pour garantir l'accès à l'interface.

Étapes complémentaires recommandées :

- soupesez longuement la démonstration de tests de sécurité par le fournisseur et évaluez la simplicité d'application des correctifs dans les appels d'offres en lien avec les dispositifs de sécurité.
- dans le cadre d'un éventuel test de démonstration précédant ou suivant la fourniture de la solution, essayez de faire vous-même des tests si vous disposez de testeurs d'intrusion dans vos équipes.
- limitez votre exposition aux attaques en désactivant tous les services et fonctionnalités inutiles.
- définissez et testez rapidement des processus et stratégies de correctifs pour les produits de sécurité critiques. Ceci peut nécessiter de surveiller sites Web et listes de diffusions de plusieurs fournisseurs.

[25] https://support.citrix.com/article/CTX267027

[26] « The Five Most Dangerous New Attack Techniques and How to Counter Them », www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2020, 27 février 2020.

[27] https://security.paloaltonetworks.com/?sort=-date

Agents Web persistants et peu sécurisés

Le second secteur d'attaque mentionné par Ullrich est la prolifération d'agents Web persistants. Les applications PC client lourd traditionnelles ont été remplacées par le navigateur, qui fait office de client universel. Dans une certaine mesure, ce changement allait dans le sens de la sécurité – avoir un nombre restreint d'applications plus ou moins sécurisées sur l'appareil de l'utilisateur est une bonne chose. Il aurait été bon que le navigateur reste un client léger simple pour la visualisation HTML sur les sites Web.

Cependant, les navigateurs sont devenus des mini-systèmes d'exploitation poids lourds avec extensions, applettes, barres d'outils BHO (browser « helper » objects) et toutes sortes d'exécutables à télécharger pour « améliorer » l'expérience utilisateur – tout du moins pour améliorer la capacité du serveur à prendre en charge des interactions complexes avec l'utilisateur. Bien entendu, ces outils augmentent considérablement l'exposition aux attaques, que les pirates n'hésitent pas à exploiter.

Les exemples mentionnés par Ullrich incluaient les systèmes de réunions en ligne appréciés du grand public comme Cisco WebEx, Zoom et d'autres encore, ainsi que de nombreux sites Web d'assistance de fournisseurs et d'entreprises. Ces services demandent à l'utilisateur d'autoriser l'installation d'un agent ; parfois, les agents sont pré-installés par le fournisseur du PC lui-même. L'agent écoute les requêtes HTTP et le navigateur peut envoyer une requête JavaScript à cet agent et demander des informations de n'importe quelle application exécutée sur le système. Lorsque l'utilisateur est sur le site légitime et si le code de l'agent est sécurisé, tout est parfait. Cependant, si l'utilisateur est trompé par l'une des innombrables attaques de hameçonnage et se rend sur le mauvais site, ce dernier peut à présent charger le même JavaScript que celui chargé par le site Web d'assistance technique et envoyer des requêtes entraînant une corruption totale du PC de l'utilisateur. La situation s'est déjà produite. Il ne s'agit pas d'une simple attaque théorique.

Atténuation : pour Ullrich, la première étape consiste à savoir quels dispositifs d'écoute HTTP actifs sont exécutés sur votre PC.[29] Toutefois, nombre de ces dispositifs d'écoute peuvent être utilisés par les services informatiques et l'assistance technique – vous ne pouvez pas vous contenter de tous les supprimer. Les pare-feux basés sur l'hôte, les solutions EDR (Endpoint Detection and Response) et les passerelles Web sécurisées peuvent également fournir une couche de contrôle.

De plus, si vos applications d'entreprise intègrent une utilisation d'agents Web dans vos produits et services, assurez-vous que votre code évite les vulnérabilités communes aux logiciels d'application Web telles que celles répertoriées dans le Top 10 de la fondation OWASP.[30] A minima, veillez à ce que le logiciel de l'agent contrôle et limite l'origine des requêtes.

Très rapidement en 2020, nous avons été rappelés à l'ordre : la mise en œuvre de précautions d'hygiène standard est décisive comme point de départ contre les

[28] https://security.paloaltonetworks.com/CVE-2019-17440

[29] « Netcat Cheat Sheet: Pocket Reference Guide », www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

[30] « OWASP Top Ten », https://owasp.org/www-project-top-ten/

menaces de niveau supérieur. Il en va de même pour la cybersécurité : l'hygiène de sécurité de base – disposer d'un inventaire précis des logiciels et de l'équipement, exécuter rapidement les correctifs, sensibiliser les utilisateurs aux risques liés aux nouvelles technologies que sont les smartphones et les services en cloud – reste l'élément-clé. Le Center for Internet Security Critical Security Controls[31] est un framework communautaire largement reconnu qui compile une liste hiérarchisée des processus et contrôles de sécurité constituant des points de départ efficaces pour réagir à de nombreuses attaques détaillées dans le présent livre blanc.

Une grande partie des attaques détaillées cette année par les experts SANS est localisée dans des domaines où les nouvelles technologies remettent fortement en question la façon dont l'informatique a traditionnellement régenté et géré logiciels et équipements. Les attaques hors sol utilisent la normalisation des systèmes d'exploitation pour la retourner contre eux. Les applications Web persistantes ne sont pas des logiciels émis par le service informatique qui, souvent, n'en a même pas connaissance. Les smartphones se positionnent depuis longtemps dans la zone floue entre utilisation personnelle et professionnelle. Les atténuations des attaques détaillées par les instructeurs consistent essentiellement à combler ces failles – à l'aide de nouvelles sources d'information afin d'augmenter ou de mettre à niveau les contrôles de sécurité bien connus avec des techniques avancées permettant de minimiser les nouvelles zones à risque. En matière d'endpoints, le renforcement de la gestion des privilèges, de la prévention, de l'isolation d'applications, de la détection de la fidélité et des capacités d'intervention doit faire l'objet d'une évaluation. Sur les réseaux, des contrôles du trafic plus stricts et spécifiques aux applications, ainsi qu'un filtrage plus agressif à l'entrée et à la sortie reposant sur les saisies à risque sont requis. Pour les appareils mobiles, il est essentiel de sensibiliser et de former les utilisateurs quant aux risques de perte de contrôle sur les appareils et au raccordement à des appareils physiques ou connexions non fiables.

Fil conducteur commun aux domaines à risque des trois experts où de nouvelles approches et des changements radicaux sont absolument nécessaires : la sécurité de la chaîne logistique. Alors que l'impact de l'épidémie de COVID-19 va se répercuter sur les années à venir, des chaînes logistiques déjà complexes vont changer de plusieurs manières. Si les craintes liées aux déplacements à l'international peuvent entraîner un raccourcissement de certaines chaînes logistiques, la demande accrue de télétravail va en compliquer d'autres. La priorité des équipes en charge de la sécurité est d'avoir voix au chapitre lors de la mise à jour ou en œuvre des plans de résilience et de survie des chaînes logistiques.

SANS Security Awareness Work-from-Home Deployment Kit,
www.sans.org/security-awareness-training/sans-security-awareness-work-home-

[31] www.cisecurity.org/controls/ [Inscription requise.]

deployment-kit

« SANS Five Most Dangerous Attack Techniques » 2019 Mise à jour et suivi, www.sans.org/the-five-most-dangerous-new-attack-techniques

« How to Evict Attackers Living Off Your Land », www.darkreading.com/edge/theedge/how-to-evict-attackers-living-off-your-land/b/d-id/1337420

« Checkm8 used to jailbreak iPhone X running iOS 13.1.1 », https://appleinsider.com/articles/19/09/29/checkm8-used-to-jailbreak-iphone-x-running-ios-1311

« Remote Code Execution on most Dell computers », https://d4stiny.github.io/Remote-Code-Execution-on-most-Dell-computers/

« What you Need To Know About The Critical Citrix Gateway (Netscaler) Vulnerability CVE-2019-19781 », 31 décembre 2019, https://www.sans.org/webcasts/about-critical-citrix-gateway-netscaler-vulnerability-cve-2019-19781-112990 [Registration required.]

Liens des sponsors

Anomali

« Rise of Legitimate Services for Backdoor Command and Control », www.anomali.com/resources/anomali-labs-reports/rise-of-legitimate-services-for-backdoor-command-and-control

« COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication », www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication

« COVID-19: With Everyone Working from Home, VPN Security Has Now Become Paramount », https://forum.anomali.com/t/covid-19-with-everyone-wokring-from-home-vpn-security-has-now-become-paramount/4672

Cyberinc

« Isla – Use Cases: Ransomware », https://cyberinc.com/browser-isolation/ransomware

« Isla – Use Cases: Phishing », https://cyberinc.com/browser-isolation/phishing

InfoBlox

« Securing Remote Workers in the Age of Teleworking », https://info.infoblox.com/resources-whitepapers-securing-remote-workers-in-the-age-of-teleworking [Registration required.]

« Cyber Threat Reports »,
https://www.infoblox.com/cyber-intelligence-unit/cyber-threat-reports/ [Subscription required.]

« Protect Your Network, Brand and Customers with Custom Lookalike Domain Monitoring », www.infoblox.com/resources/solution-notes/protect-your-network-and-customers-with-lookalike-monitoring

« What's Lurking in the Shadows 2020: Exposing how IoT devices open a portal for chaos across the network »,
www.infoblox.com/resources/whitepaper/whats-lurking-in-the-shadows-2020 [Inscription requise.]

« Remote Office Networks Pose Business and Reliability Risk: A Survey of IT Professionals »,
www.infoblox.com/resources/whitepaper/remote-office-networks-pose-business-and-reliability-risk-survey [Inscription requise.]

« An Introduction to MITRE ATT&CK »,
www.infoblox.com/resources/whitepaper/introduction-to-mitre-attck [Inscription requise.]

« An Introduction to Zero Trust: A Compelling Cybersecurity Strategy for Defending the Enterprise »,
www.infoblox.com/resources/whitepaper/an-introduction-to-zero-trust [Inscription requise.]

« Adopting NIST Cyber Security Framework using Foundational Network Infrastructure »,
www.infoblox.com/resources/whitepaper/adopting-nist-cyber-security-framework [Inscription requise.]

Unisys

« Four Reasons to Kill The VPN: Security, Speed, Simplicity and Savings »,
https://assets.unisys.com/documents/global/povpapers/pov_200184_fourreasontokillthevpn.pdf

Verodin

« Verodin 2020 Security Effectiveness Report: Executive Summary »,
https://www2.verodin.com/2020SecurityReport_ExecutiveSummary [Inscription requise.]

« Verodin Security Instrumentation Platform »,
https://www.fireeye.com/solutions/verodin-security-instrumentation.html

À propos de l'auteur

John Pescatore a rejoint SANS en tant que directeur des technologies émergentes en janvier 2013, après plus de 13 années aux fonctions d'analyste en chef de la sécurité chez Gartner et en tant qu'animateur de groupes de conseil chez Trusted Information Systems et Entrust, 11 années chez GTE, et plusieurs années de service au sein de la National Security Agency – où il concevait des systèmes sécurisés de reconnaissance vocale – et de l'agence United States Secret Service – où il développait des systèmes sécurisés de communication et de surveillance. John a témoigné devant le Congrès à propos de la cybersécurité, a été nommé parmi les 15 personnes les plus influentes en matière de sécurité en 2008 et est ingénieur en cryptologie certifié par la NSA.

Sponsor

SANS souhaite remercier le sponsor de ce livre blanc :

Infoblox
NEXT LEVEL NETWORKING