Secureworks®

Tirer les leçons de la réponse aux incidents
Bilan de l'année 2022

Équipe de recherche Secureworks® Counter Threat Unit™

Table des matières

03 Résumé

04 Points clés

05 Tendances observées

10 Observations sur le paysage des menaces

14 Recommandation

15 Conclusion

Résumé

Entre janvier et décembre 2022, Secureworks® a contribué au confinement et à la remédiation de plus de 500 incidents de sécurité. La visibilité de ces incidents réels a fourni aux chercheurs de Secureworks Counter Threat Unit™ (CTU) un aperçu des menaces émergentes et des tendances en développement que les organisations peuvent utiliser pour guider la prise de décision en matière de gestion des risques, informer sur les meilleures pratiques et prioriser l'allocation des ressources.

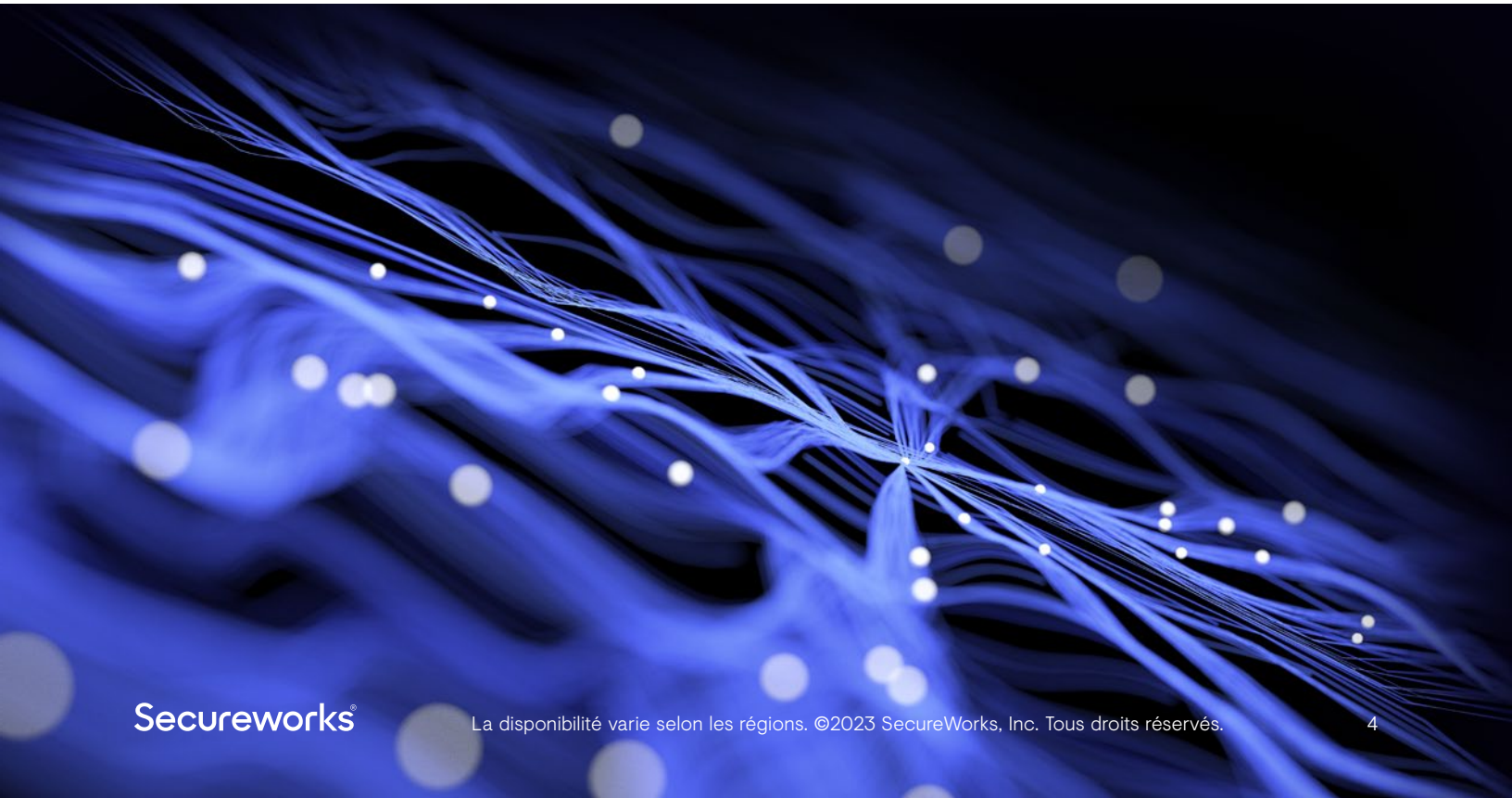
Les motivations et le contexte des missions de réponse aux incidents (RI) varient. Par exemple, la décision d'une organisation d'utiliser des services de RI peut être influencée par les ressources internes de l'organisation, les rapports des médias ou l'entrée de l'organisation dans une période opérationnelle délicate. Par conséquent, les types de menaces observés peuvent ne pas refléter le paysage des menaces dans son ensemble. Malgré ces limites, les données issues des missions de RI révèlent comment les acteurs de la menace pénètrent dans les réseaux, quel est l'impact de cette activité sur les organisations touchées et comment les incidents auraient pu être évités.

Points clés:

Les ransomwares post-intrusion ont continué à représenter une menace importante pour les organisations en raison de l'impact élevé que ces attaques peuvent causer. Cependant, les attaques de type Business Email Compromise (BEC) ont dépassé les ransomwares post-intrusion pour devenir le type d'activité à motivation financière le plus communément observé lors des engagements IR de Secureworks en 2022.

Les vulnérabilités des systèmes orientés vers l'internet sont restées un vecteur d'accès initial courant. Toutefois, le pourcentage de missions où le phishing était le vecteur d'accès initial est passé de 13 % en 2021 à 33 % en 2022, probablement en raison d'une augmentation des attaques BEC.

L'authentification multi-facteurs (MFA) et l'hébergement en nuage ont modifié la surface d'attaque, incitant les acteurs de la menace à trouver des moyens créatifs pour contourner les contrôles de sécurité afin d'atteindre leurs objectifs.



Tendances observées

La cybercriminalité continue de représenter la plus grande menace pour les clients de Secureworks, 79 % des incidents étant attribués à des cybercriminels aux motivations financières. En comparaison, les activités hostiles parrainées par le gouvernement ont été observées dans environ 9 % des engagements de Secureworks IR. Les autres incidents étaient dus à des actions délibérées ou accidentelles des employés des organisations. La proportion d'intrusions motivées par des raisons financières a été plus faible que les années précédentes, passant de 85 % en 2021 et 92 % en 2020 (voir figure 1). Cette évolution peut s'expliquer en partie par l'invasion de l'Ukraine par la Russie; il est possible que les cybercriminels ukrainiens et russes aient détourné leur attention vers des opérations d'hacktivisme ciblant des organisations qui soutenaient le pays adverse.

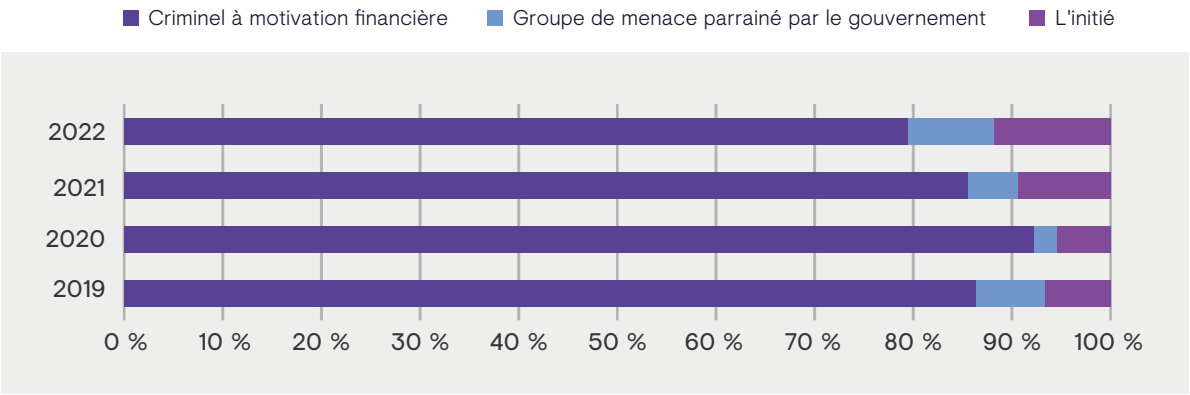


FIGURE 1. *Répartition des types d'acteurs de la menace observés dans les engagements IR de Secureworks de 2019 à 2022. (Source: Secureworks)*

Les incidents à motivation financière survenus en 2022 concernaient des menaces telles que les ransomwares, les BEC et le cryptojacking. L'activité cybercriminelle est opportuniste et motivée par la capacité des acteurs de la menace à maximiser les profits qui peuvent être générés par l'accès non autorisé à des réseaux compromis. C'est pourquoi les attaques basées sur l'extorsion, telles que les ransomwares, ont continué à dominer.

Vecteurs d'accès initiaux

En 2022, l'exploitation des vulnérabilités des appareils connectés à Internet et l'hameçonnage ont été les IAV les plus courantes observées dans les missions IR de Secureworks. Ils représentaient chacun environ un tiers des incidents pour lesquels l'IAV a pu être déterminée (voir Figure 2).

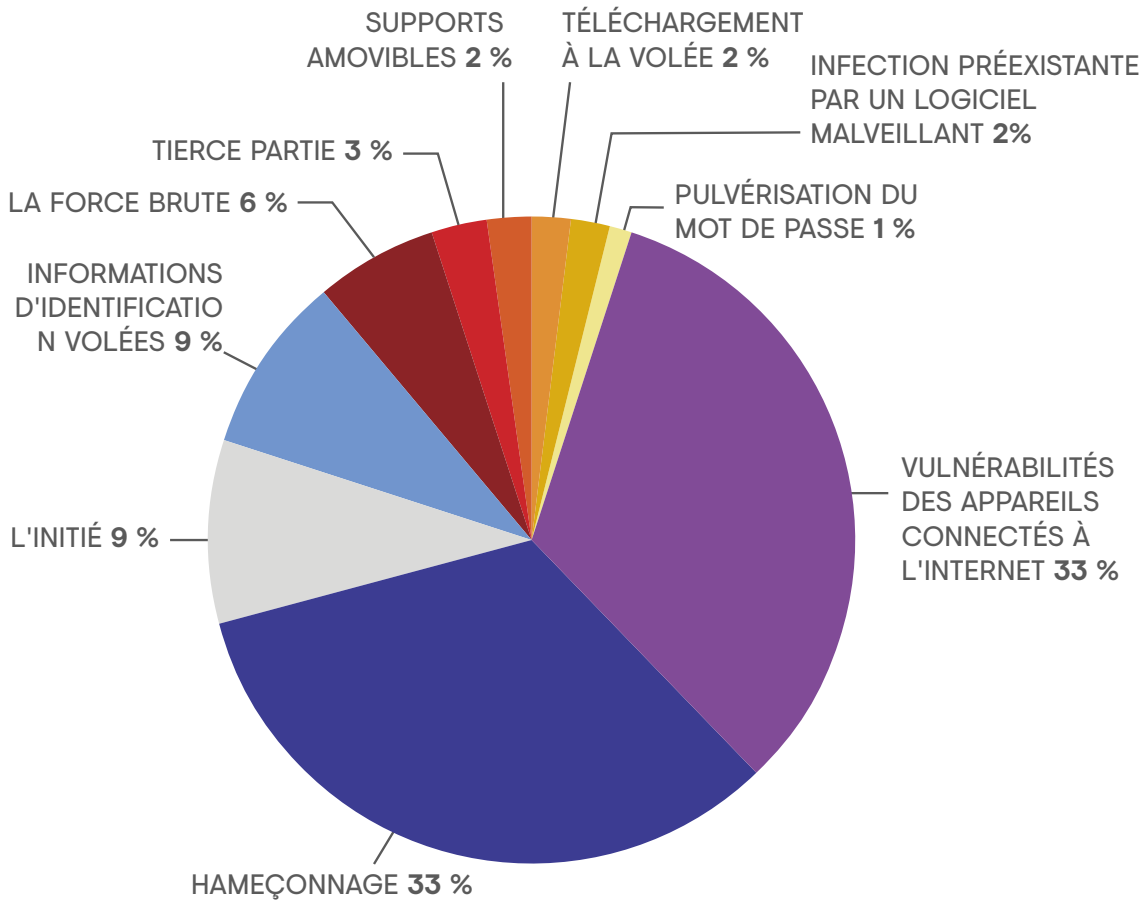


FIGURE 2. *IAVs observés lors des engagements RI en 2022. (Source: Secureworks)*

Mise en correspondance des IAV avec MITRE ATT&CK

Ce tableau met en correspondance ces IAV avec les catégories ATT&CK® de MITRE. Les organisations peuvent utiliser les informations de cette base de connaissances pour organiser et opérationnaliser les données de renseignement sur les menaces.

VECTEUR D'ACCÈS INITIAL (IAV)	CARTOGRAPHIE MITRE ATT&CK
Vulnérabilités des appareils connectés à l'internet	Exploitation des services à distance Exploitation d'une application publique
Informations d'identification (force brute, pulvérisation de mots de passe, informations d'identification volées)	Comptes valides Force brute
Hameçonnage	Hameçonnage Pièce jointe de spearphishing Lien Spearphishing Spearphishing via Service
Accès des tiers	Compromis de la chaîne d'approvisionnement Relation de confiance
Infection préexistante par un logiciel malveillant	Développer les capacités
Téléchargement à la volée	Compromis à l'emporte-pièce

La proportion du total des engagements de Secureworks IR où l'acteur de la menace a utilisé l'hameçonnage comme IAV a augmenté de manière significative par rapport à 2021 (voir Figure 3). Cette augmentation est largement due au fait que le nombre total d'incidents BEC observés a plus que doublé entre 2021 et 2022, l'hameçonnage ayant été identifié comme IAV dans 85 % des incidents BEC de 2022. Dans la plupart des cas, les auteurs de la menace ont envoyé des courriels d'hameçonnage à des milliers de destinataires, parfois au sein de plusieurs organisations.

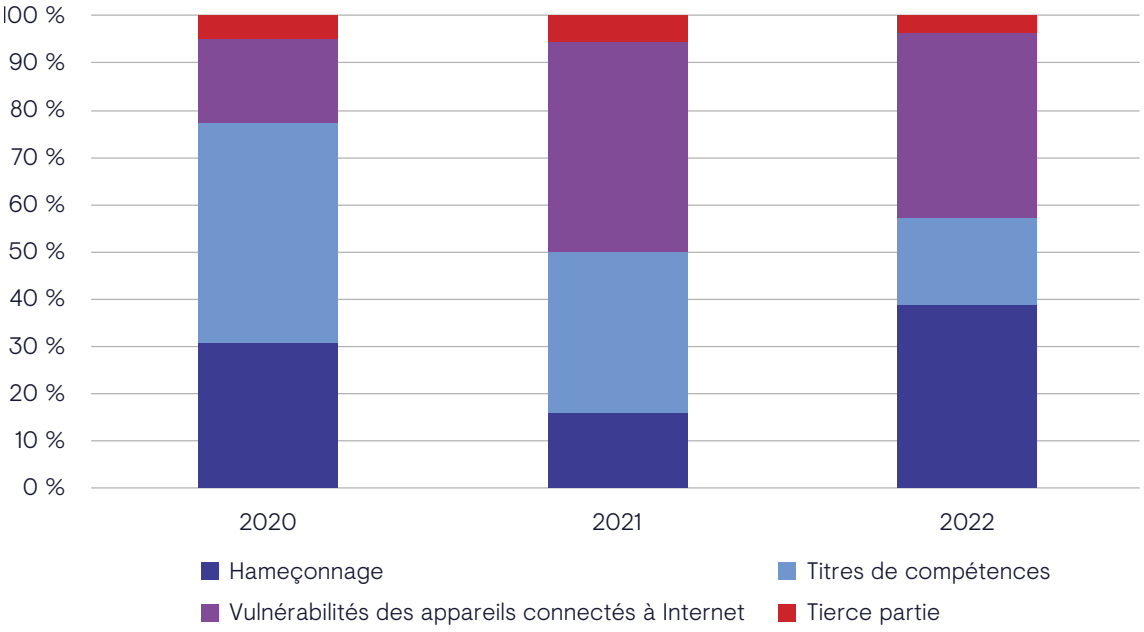


FIGURE 3. *VAI observées entre 2020 et 2022. L'abus d'identifiants englobe le vol d'identifiants, les attaques par force brute et la pulvérisation de mots de passe. (Source: Secureworks)*

À l'heure où nous publions ces lignes, le BEC représente la plus grande menace monétaire pour les organisations. En 2022, l'Internet Crime Complaint Center (IC3) du Federal Bureau of Investigation (FBI) des États-Unis a fait état d'une augmentation de 65 % des pertes exposées identifiées au niveau mondial à la suite d'attaques BEC entre juillet 2019 et décembre 2021. Alors que les gains semblent augmenter, les aspects techniques des systèmes BEC restent relativement simples. La nouvelle des profits potentiels et de la faible barrière à l'entrée a probablement incité d'autres groupes ayant peu ou pas de capacités techniques à commencer à mener des attaques BEC.

La proportion des missions IR de Secureworks impliquant l'exploitation de dispositifs vulnérables orientés vers l'Internet a légèrement diminué en 2022, mais est restée nettement plus élevée qu'en 2020. Secureworks a observé que des acteurs de la menace motivés par des raisons financières et parrainés par le gouvernement utilisaient cette IAV. Dans de nombreux incidents, les acteurs de la menace ont exploité des informations accessibles au public plutôt que d'identifier les vulnérabilités et de développer eux-mêmes le code d'exploitation. Plus précisément, ils ont utilisé des codes d'exploitation de démonstration de concept publiés par des chercheurs en sécurité après que les vulnérabilités ont été rendues publiques et ont pu ensuite effectuer des analyses en masse pour identifier et exploiter de manière opportuniste les appareils vulnérables. Parfois, les appareils restent vulnérables pendant des années avant d'être exploités. En 2022, les chercheurs de la CTU™ ont continué à observer des vulnérabilités très médiatisées telles que ProxyLogon, ProxyShell et Log4Shellexploitées dans des logiciels tiers alors que des correctifs étaient disponibles depuis 2021.

Chine: Les découvertes en matière de vulnérabilité restent dans la famille

Parmi la Chine, la Corée du Nord, l'Iran et la Russie - les pays les plus actifs en matière de cyberespionnage ayant un impact sur les clients de Secureworks - la Chine se distingue par l'ampleur de son ciblage. En 2022, les acteurs chinois de la menace étaient responsables de plus de 90 % des activités parrainées par le gouvernement sur lesquelles les intervenants de Secureworks ont enquêté. Les groupes de menace chinois mènent des activités de cyberespionnage pour soutenir les priorités politiques, militaires et économiques de la Chine. Une part importante des activités des groupes de menace chinois vise également les organisations pour voler la propriété intellectuelle et les secrets commerciaux afin de soutenir les objectifs de développement économique de la Chine.

Les groupes de menace chinois compromettent principalement les réseaux en exploitant les vulnérabilités des appareils connectés à Internet. En 2022, Secureworks a observé des acteurs chinois ciblant des produits et dispositifs tiers tels que Zoho ManageEngine,, Microsoft Exchange, Pulse Secure et des applications personnalisées. Bien qu'une grande partie de cette activité ait exploité des vulnérabilités connues pour lesquelles des correctifs étaient disponibles, l'exploitation massive des serveurs Microsoft Exchange en mars 2021 met en évidence la menace posée par des acteurs chinois armés de connaissances sur les vulnérabilités de type "zero-day".

Les chercheurs en vulnérabilités basés en Chine ont historiquement dominé les concours mondiaux visant à exploiter des vulnérabilités précédemment inconnues. Cependant, le gouvernement chinois a mis en œuvre des réglementations en 2017 pour interdire aux chercheurs chinois de participer à ces concours. Les particuliers et les entreprises chinoises sont également tenus de signaler les vulnérabilités au gouvernement dans les deux jours suivant leur découverte. Ces réglementations offrent au gouvernement chinois un accès potentiellement exclusif aux vulnérabilités zero-day qui pourraient être exploitées par des groupes de menaces parrainés par le gouvernement.

Comprendre la surface d'attaque du périmètre du réseau de votre organisation et mettre en œuvre un processus robuste de correction des vulnérabilités connues sont des éléments clés d'une approche de défense en profondeur de la sécurité du réseau. La mise en œuvre d'une solution de détection et de réponse (EDR) peut être efficace pour identifier l'activité associée à l'exploitation des vulnérabilités de type "zero-day". Cette activité peut inclure des relations anormales entre les processus parent-enfant ou des mouvements latéraux.

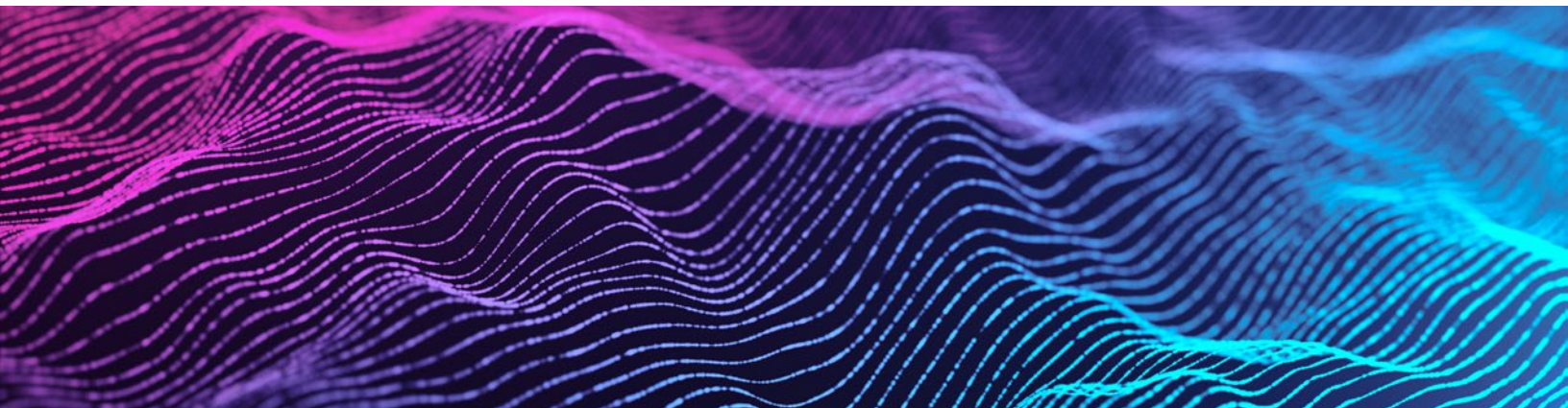
Observations sur le paysage des menaces

Les engagements de Secureworks IR en 2022 ont permis de comprendre les tendances du paysage des menaces.

Une baisse de l'activité des ransomwares?

En 2022, il y a eu 57 % de moins d'engagements de Secureworks IR impliquant des ransomwares. Outre l'impact potentiel de l'invasion de l'Ukraine par la Russie sur la cybercriminalité, il existe plusieurs autres explications possibles à cette baisse apparente de l'activité des ransomwares:

- Les groupes de ransomware cherchent à maximiser leurs revenus tout en évitant les intrusions à fort impact et très médiatisées qui attirent l'attention du gouvernement et des forces de l'ordre. La réponse du gouvernement américain en 2021 aux attaques très médiatisées contre Colonial Pipeline, JBS, et Kaseya a entraîné des coûts importants pour les groupes de ransomwares responsables. Les services répressifs du monde entier ont poursuivi ces groupes de ransomware ainsi que d'autres, arrêtant dans certains cas des individus liés à l'activité malveillante. Pour éviter de subir le même sort, certains groupes de ransomwares ont proactivement mis fin à des projets existants et ont changé de nom.
- Les organisations pourraient mettre en œuvre des solutions EDR qui identifient les activités précurseurs des ransomwares. Ces solutions contrecarrent le déploiement ultérieur des ransomwares en détectant le cadre antagoniste Cobalt Strike et d'autres tactiques, techniques et procédures (TTP) communes à de nombreux groupes de ransomwares.
- Il est possible que les groupes de ransomware ciblent des organisations moins médiatisées qui ne font pas appel à des ressources externes de réponse aux incidents lors d'une intrusion. Ce ciblage pourrait expliquer pourquoi les rapports de tiers montrent une réduction globale des paiements de ransomware en 2022. Il est probable que ces organisations paient une rançon moins élevée, si elles en paient une.
- Les organisations pourraient mettre en œuvre des solutions EDR qui identifient les activités précurseurs des ransomwares. Ces solutions contrecarrent le déploiement ultérieur des ransomwares en détectant le cadre antagoniste Cobalt Strike et d'autres tactiques, techniques et procédures (TTP) communes à de nombreux groupes de ransomwares.



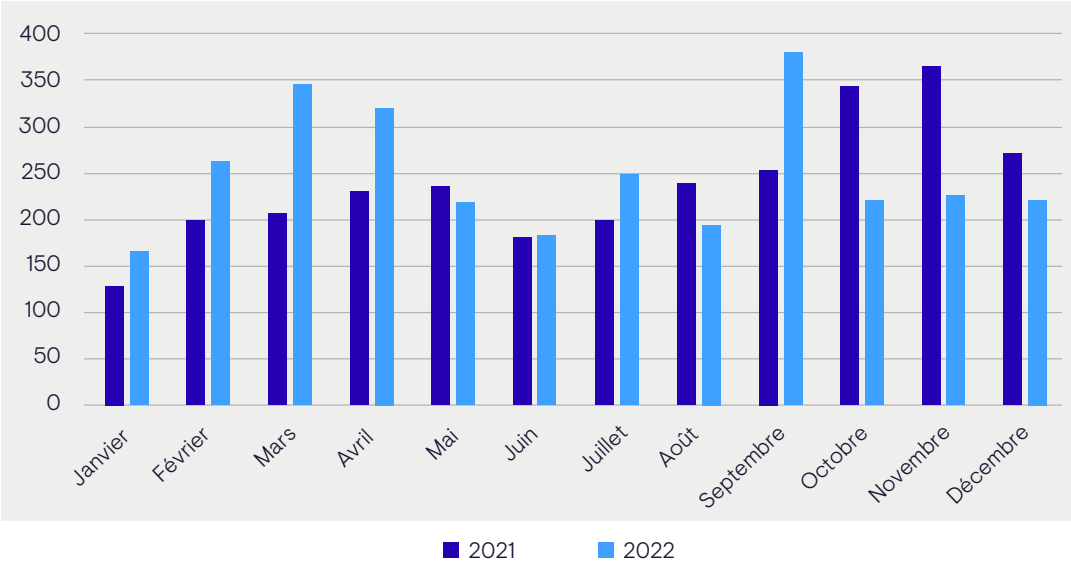


FIGURE 4. *Victimes ajoutées aux sites de fuite de ransomware en 2021 et 2022. (Source: Secureworks)*

Toutefois, les prédictions concernant la disparition imminente des opérations de ransomware en tant que service (RaaS) ne se sont pas concrétisées en 2022. Le nombre de victimes répertoriées sur les sites de fuite de ransomware surveillés par les chercheurs de la CTU n'a pas diminué de manière significative entre 2021 et 2022, malgré des fluctuations mensuelles (voir figure 4).

L'analyse par la CTU des tendances dans le paysage des ransomwares " name-and-shame " a révélé que les opérations RaaS continuaient à toucher un grand nombre de victimes. Le groupe de menace GOLD MYSTIC, motivé par des considérations financières, a publié 920 noms de victimes sur son site de fuite LockBit en 2022, ce qui représente près de 33 % du nombre total de victimes publiées sur l'ensemble des sites de fuite de ransomwares au cours de l'année. Rien qu'en septembre, 228 victimes de LockBit ont été ajoutées. Cette activité accrue pourrait être liée aux déclarations d'un représentant présumé de GOLD MYSTIC selon lesquelles LockBit 3.0 comprendrait des fonctionnalités améliorées et une infrastructure élargie.

Parmi les autres opérations prolifiques de ransomware, citons ALPHV (également connu sous le nom de BlackCat), Conti et Black Basta. En novembre, Secureworks a enquêté sur de multiples intrusions où le logiciel malveillant Qakbot a conduit au déploiement de Black Basta. Le groupe de menace GOLD REBELLION, qui exploite Black Basta, a publié la première victime sur son site de fuite en avril. Dans les incidents analysés, l'exfiltration de données et le déploiement de ransomware ont eu lieu dans les 24 heures suivant l'accès initial. Les chercheurs de la CTU recommandent aux organisations d'examiner les TTP de ces incidents et de vérifier que leurs contrôles de sécurité permettront d'atténuer ces menaces. En particulier, les défenseurs du réseau devraient mettre en place des contrôles pour détecter et bloquer Qakbot.

L'AMF n'est pas un contrôle de sécurité "vite fait bien fait".

L'authentification multifactorielle est l'un des moyens les plus efficaces d'atténuer les attaques basées sur les informations d'identification et de réduire la probabilité d'une compromission du réseau. L'augmentation du nombre d'organisations mettant en œuvre l'AFM pourrait expliquer pourquoi les intervenants de Secureworks ont observé une baisse des vols d'informations d'identification en tant qu'IAV en 2022. Cependant, alors que de plus en plus d'organisations adoptent l'AMF, les acteurs de la menace découvrent des moyens innovants de la contourner ou de concentrer leur attention sur d'autres IAV.

En 2022, les engagements de Secureworks IR ont révélé que les acteurs BEC tentaient de contourner le MFA à l'aide de diverses techniques. Les acteurs BEC ont réussi à contourner le MFA en envoyant des demandes d'authentification que la victime approuve sans les vérifier. Dans les attaques de fatigue MFA, qui pourraient gagner en popularité, un acteur de la menace tente à plusieurs reprises de se connecter au même compte à l'aide d'informations d'identification volées. Ce comportement envoie de nombreuses demandes de push MFA à l'appareil mobile du propriétaire du compte, et l'afflux peut conduire le propriétaire du compte à approuver la demande d'authentification.

Dans un incident, un acteur de la menace a obtenu les noms d'utilisateur et les mots de passe Office 365 d'une organisation par hameçonnage. L'acteur de la menace a ensuite obtenu l'accès à certains comptes après avoir soumis les utilisateurs à une attaque de fatigue MFA. L'organisation a détecté cette activité et a rapidement remédié à l'intrusion. Cet incident souligne l'importance de surveiller l'accès aux ressources clés de l'entreprise, même lorsque des contrôles de sécurité fondamentaux tels que le MFA sont en place. L'un des moyens d'atténuer le risque d'attaques par lassitude est de mettre en œuvre des notifications MFA qui demandent à l'utilisateur d'entrer un code plutôt que de choisir "confirmer" ou "approuver". Heureusement, nombre de ces attaques échouent parce que l'utilisateur refuse la demande ou signale l'incident à son organisation.

Bien que cet incident ait concerné des appareils d'entreprise, la collecte de données d'entreprise à partir d'appareils personnels à l'aide de voleurs d'informations constitue une menace croissante pour les organisations. Les appareils personnels ont souvent des contrôles de sécurité plus faibles que les appareils appartenant à l'entreprise et peuvent contenir des informations d'identification de l'entreprise qui pourraient être utilisées dans des attaques de fatigue MFA ou fournir une IAV dans le réseau de l'entreprise. Les acteurs de la menace ont également démontré des capacités d'interception MFA telles que les campagnes de phishing qui incitent un utilisateur à visiter un site Web se faisant passer pour un site d'entreprise légitime et à saisir ses informations d'identification et le code de deuxième facteur à partir de son appareil. Les défenseurs du réseau devraient envisager de mettre en œuvre une MFA résistante à l'hameçonnage, telle que des jetons physiques, afin de prévenir ce type d'attaque.

Les acteurs de la menace mettent à jour leur savoir-faire pour les technologies de l'informatique dématérialisée

La pandémie de COVID-19 a accéléré le passage à des solutions gérées en nuage pour de nombreuses organisations. Ces solutions ont souvent été mises en œuvre à la hâte et sans tenir pleinement compte des implications en matière de sécurité. Les organisations peuvent bénéficier des contrôles de sécurité offerts par ces fournisseurs de services en nuage, mais ces contrôles doivent être mis en œuvre correctement. Les intervenants de Secureworks enquêtent souvent sur des intrusions où les contrôles de sécurité fondamentaux étaient absents ou mal configurés. Même lorsque les contrôles de sécurité sont en place, les environnements en nuage peuvent encore présenter des vulnérabilités que les acteurs de la menace pourraient exploiter pour s'implanter.

À mesure que les entreprises adoptent des services basés sur le cloud, les acteurs de la menace sont contraints de développer de nouvelles techniques pour atteindre leurs objectifs post-intrusion. Les intervenants de Secureworks ont découvert un probable groupe de cyberespionnage

chinois qui passait d'un réseau sur site compromis au locataire Azure Active Directory (AD) de l'organisation lorsque les deux systèmes synchronisaient les comptes. L'acteur de la menace a obtenu un accès initial au réseau sur site en exploitant les vulnérabilités ProxyShell sur un serveur Microsoft Exchange orienté vers l'internet. Après avoir accédé au locataire Azure AD, l'acteur de la menace a enregistré une application à locataire unique avec des autorisations API Exchange Web Services (EWS) qui lui ont permis d'accéder aux boîtes aux lettres de l'organisation à partir d'Exchange Online.

Que l'environnement d'une organisation soit sur site, basé sur le cloud ou une solution hybride, il n'est aussi solide que son maillon le plus faible. Cet exemple renforce la nécessité fondamentale pour les défenseurs du réseau d'atténuer les risques en fonction de l'évolution de la surface d'attaque. Les chercheurs du CTU recommandent aux défenseurs du réseau de comprendre quelles données leurs journaux collectent à partir des environnements en nuage et comment les données sont conservées. Une journalisation appropriée, idéalement dans une plateforme de journalisation centralisée et gérée, offre une visibilité sur l'activité des utilisateurs dans un environnement en nuage et dans l'ensemble du domaine de l'organisation. Les données de journalisation peuvent révéler des activités inhabituelles et donner un aperçu de la portée et de l'impact d'une intrusion, ce qui est essentiel pour une remédiation efficace.

Recommandation

À la suite des engagements IR, Secureworks fournit des recommandations granulaires sur les contrôles de sécurité qui auraient permis de minimiser l'impact de l'incident, en conseillant aux clients de donner la priorité à ces contrôles afin d'éviter que l'incident ne se reproduise. Les contrôles de sécurité qui font souvent défaut dans les environnements compromis comprennent le déploiement complet d'une solution EDR, la conservation et l'analyse centralisées des journaux sur l'hôte, le réseau et les ressources en nuage, ainsi que le filtrage Web basé sur la réputation et la détection réseau pour les domaines et les adresses IP suspects.

Conclusion

Les chercheurs de la CTU suivent les menaces et les comportements observés lors des engagements IR afin de comprendre la nature et l'évolution des différentes menaces. Grâce au développement de contre-mesures, à l'analyse périodique des tendances et aux rapports tactiques ad hoc sur les activités observées lors des engagements IR, les chercheurs de la CTU et les intervenants en cas d'incident de Secureworks fournissent en permanence aux clients de Secureworks une protection, des informations et des conseils tirés d'incidents réels.

À propos de Secureworks Incident Response

L'équipe de réponse aux incidents de Secureworks offre un large éventail d'expertise, de renseignements sur les cybermenaces et de technologies spécialisées pour aider les organisations à se préparer et à répondre avec succès aux cyberincidents. Secureworks peut aider les organisations en mettant à leur disposition des responsables sur place (sous réserve des restrictions applicables en matière de déplacement en cas de pandémie) ou à distance pour les aider à répondre à un incident. Les experts de Secureworks travaillent en étroite collaboration avec les équipes internes par le biais de services de réponse aux incidents d'urgence, d'évaluations de la chasse aux menaces, d'exercices sur table et d'une gamme d'autres services de préparation aux incidents - tous conçus pour vous aider à mettre en place un programme de réponse aux incidents et à résoudre les incidents de manière efficace et efficiente à grande échelle.

À propos de Secureworks

Secureworks (NASDAQ : SCWX) est un leader mondial de la cybersécurité qui protège les progrès de ses clients grâce à Secureworks Taegis™, une plateforme analytique de sécurité native dans le cloud qui s'appuie sur plus de 20 ans de recherche et de renseignements sur les menaces réelles, améliorant ainsi la capacité des clients à détecter les menaces avancées, à rationaliser et à collaborer sur les enquêtes, et à automatiser les bonnes actions.

www.secureworks.com

Sources

Abrams, Lawrence. "MFA Fatigue: Hackers' new favorite tactic in high-profile breaches." Bleeping Computer. 20 septembre 2022.

Asokan, Akshaya. "Microsoft Exchange Flaw: Attacks Surge After Code Published." GovInfoSecurity. 20 mars 2021.

Chainanalysis. "Ransomware Revenue Down As More Victims Refuse to Pay." 19 Janvier 2023.

Dignan, Larry. "Colonial Pipeline cyberattack shuts down pipeline that supplies 45% of East Coast's fuel." ZDNET. 8 mai 2021.

Hageman, Mitchell. "Secureworks CTU identifies increase in stolen credential sales." SecurityBrief Asia. 5 décembre 2022.

Makortoff, Kalyeena. "World's biggest meat producer JBS pays $11m cybercrime ransom." The Guardian. 10 juin 2021.

Microsoft. "HAFNIUM targeting Exchange Servers with 0-day exploits." 2 mars 2021.

Red Hot Cyber. "RHC interviews LockBit 3.0. 'The main thing is not to start a nuclear war'." 26 juillet 2022.

Secureworks. "Azure Active Directory Flaw Allows SAML Persistence." 18, 2023.

Secureworks. "BRONZE STARLIGHT Ransomware Operations Use HUI Loader." 23 juin 2022.

Secureworks. "How to Prevent Multi-factor Authentication Bypass." 7 juin 2022.

Secureworks. "Kaseya VSA Software Under Active Attack." 3 juillet 2021

Secureworks. "Log4Shell: Easy to Launch the Attack but Hard to Stick the Landing?" 17 décembre 2021.

Secureworks. "Secureworks FAQ: Russian Activity in Ukraine." 24 février 2022.

Secureworks. "Think MFA is Hack-Proof? Think Again." 30 avril 2020.

Tsai, Orange. "From Pwn2Own 2021: A New Attack Surface on Microsoft Exchange - ProxyShell!" Zero Day Initiative. 18 août 2021.

U.S. Cybersecurity & Infrastructure Security Agency (CISA). "Implementing Phishing-Resistant MFA." Octobre 2022.

U.S. Federal Bureau of Investigation. "Business Email Compromise: The $43 Billion Scam." 4 mai 2022.