zscaler™ | ThreatLabz

Rapport 2022 de ThreatLabz sur l'état des ransomwares

Contenu

Introduction

Si les ransomwares semblent toujours faire la une de l'actualité, il ne s'agit pas seulement d'un parti pris médiatique : l'équipe de recherche Zscaler ThreatLabz a établi que les attaques de ransomwares ont encore augmenté de 80 % entre février 2021 et mars 2022 par rapport à l'année précédente, établissant de nouveaux records tant pour le volume des attaques que pour le coût des préjudices.

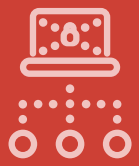
Les ransomwares sont de plus en plus prisés par les attaquants, qui peuvent mener des campagnes de plus en plus rentables en s'appuyant sur trois grandes tendances :

Les attaques de la chaîne d'approvisionnement

qui exploitent les relations de confiance avec les fournisseurs pour pénétrer dans les entreprises et multiplier les préjudices en permettant aux acteurs malveillants de toucher plusieurs (parfois des centaines ou des milliers) victimes en même temps.

Les ransomwares en tant que service

qui utilisent des réseaux affiliés pour diffuser des ransomwares à grande échelle, permettant aux hackers experts en matière de violation de réseaux de partager les bénéfices avec les groupes de ransomwares les plus avancés.



Les attaques à extorsion multiple

qui recourent au vol de données, à des attaques par déni de service distribué (DDoS), aux communications avec les clients, etc. comme autant de tactiques d'extorsion à plusieurs niveaux destinées à augmenter le montant des rançons.

Ces tactiques se cumulent pour causer des dégâts considérables. Les experts du secteur prévoient qu'en 2022, les ransomwares seront la principale tactique utilisée dans le cadre de violations par des tiers et d'attaques contre la chaîne d'approvisionnement, et que le coût mondial des dommages causés par les ransomwares atteindra 42 milliards de dollars d'ici 2024.

Ces tendances ont propulsé les ransomwares encore plus haut sur la liste des priorités en matière de cybersécurité pour les entreprises de tous les secteurs. Selon le rapport 2022 des RSSI d'Aimpoint, le ransomware est la menace la plus préoccupante pour les RSSI du monde entier.

Comment pouvez-vous identifier et vous protéger contre les dernières variantes de ransomware ? Ce rapport devrait vous y aider.

ThreatLabz analyse les données provenant de plus de 200 milliards de transactions quotidiennes et de 150 millions d'attaques quotidiennes bloquées dans l'ensemble de Zscaler Zero Trust Exchange, ainsi que les renseignements sur les menaces fournis par Zscaler ThreatLabz, afin de suivre les familles de menaces les plus répandues, d'identifier les tendances émergentes et d'améliorer les protections des clients de Zscaler. Dans ce rapport, ThreatLabz a analysé les données relatives aux ransomwares du 1er février 2021 au 31 mars 2022, afin d'identifier les familles de ransomwares les plus prolifiques et leurs tactiques. Nous partagerons nos conclusions, nos prédictions et nos conseils pour guider vos stratégies de défense contre les ransomwares.

Résultats clés

Les attaques par ransomware ont augmenté de 80 % en un an, représentant tous les payloads de ransomware observés dans Zscaler Cloud.

Les occurrences de ransomwares à double extorsion ont augmenté de 117 %, ce qui signifie que de plus en plus d'attaques incluent le vol de données dans leurs stratégies. Certains secteurs ont connu une croissance particulièrement élevée des attaques à double extorsion, notamment les soins de santé (643 %), la restauration (460 %), l'exploitation minière (229 %), l'éducation (225 %), les médias (200 %) et la fabrication (190 %).

L'industrie manufacturière a été le secteur le plus ciblé pour la deuxième année consécutive, représentant près de 20 % des attaques de ransomware à double extorsion.

Les attaques par ransomware de la chaîne d'approvisionnement sont en augmentation, tout comme les attaques de la chaîne d'approvisionnement en général. L'exploitation de fournisseurs de confiance permet aux hackers de s'attaquer à un grand nombre d'entreprises en même temps, y compris à celles qui sont dotées de solides protections contre les attaques externes. Les attaques par ransomware de la chaîne d'approvisionnement de l'année dernière comptent notamment les campagnes préjudiciables contre Kaseya et Quanta, ainsi qu'un certain nombre d'attaques qui exploitent la vulnérabilité Log4j.

Les ransomwares en tant que service sont à l'origine d'un plus grand nombre d'attaques. Les groupes de ransomware continuent de recruter des affiliés par le biais de forums criminels clandestins. Ces affiliés mettent en péril de grandes entreprises et déploient le ransomware du groupe, généralement en échange d'environ 80 % des paiements de rançon perçus des victimes. La plupart (8 sur 11) des principales familles de ransomwares de l'année dernière ont proliféré communément via des modèles de ransomware en tant que service.

Les forces de l'ordre sévissent. Un certain nombre des principales familles de ransomwares de l'année dernière, en particulier celles qui ciblent les services essentiels, ont attiré l'attention des organismes chargés de l'application de la loi aux quatre coins du monde. REvil (responsable des célèbres attaques contre Kaseya et JSB), DarkSide (responsable de l'attaque contre Colonial Pipeline) et Egregor (une nouvelle appellation de Maze, la famille de ransomware la plus importante de l'année dernière) ont tous vu leurs actifs saisis par les forces de l'ordre en 2021.

Les familles de ransomwares ne disparaissent pas, elles changent simplement de nom. Sentant la pression croissante des forces de l'ordre, de nombreux groupes de ransomwares se sont dissous et reformés sous de nouvelles bannières, sous lesquelles ils utilisent les mêmes tactiques (ou des tactiques très similaires). DarkSide s'est rebaptisé BlackMatter, DoppelPaymer s'est rebaptisé Grief, et Avaddon s'est rebaptisé Haron et Midas. Evil Corp, sanctionné par le gouvernement américain, a constamment changé de nom pour ses opérations de ransomware.

Le conflit Russie–Ukraine met le monde en état d'alerte. Plusieurs attaques ont été associées au conflit Russie–Ukraine, certaines combinant plusieurs tactiques, notamment de nombreux wipers, dont les ransomwares HermeticWiper et PartyTicket. Jusqu'à présent, la plupart de ces activités ont visé l'Ukraine. Cependant, les agences gouvernementales ont mis les entreprises en garde contre le risque de propagation des attaques à mesure que le conflit persiste.

Zero Trust demeure la meilleure défense. Pour minimiser les risques de violation et les préjudices que peut provoquer une attaque réussie, votre entreprise doit utiliser des stratégies de défense en profondeur qui englobent la réduction de votre surface d'attaque, l'application d'un contrôle d'accès basé sur le principe du moindre privilège, ainsi que la surveillance et l'inspection continues des données dans l'ensemble de votre environnement.

Évolution des ransomwares

Les ransomwares sont un type de logiciels malveillants utilisés par les cybercriminels pour perturber l'entreprise de leur victime. Les ransomwares chiffrent les fichiers importants d'une entreprise, les rendant illisibles puis exigent le paiement d'une rançon pour les déchiffrer. Les demandes de rançon sont souvent proportionnelles au nombre de systèmes infectés et à la valeur des données chiffrées : plus les enjeux sont importants, plus le paiement est élevé.

Fin 2019, les hackers ont fait évoluer leurs tactiques de ransomware pour inclure l'exfiltration de données, communément appelée attaque par ransomware à « double extorsion ». Dans ce type d'attaque, si les victimes choisissent de ne pas payer la rançon pour déchiffrer les données et, au lieu de cela, tentent de restaurer les données à partir d'une sauvegarde, les hackers menacent alors de divulguer les données dérobées.

Fin 2020, certains hackers utilisant des ransomwares ont ajouté une autre couche d'attaque avec des tactiques DDoS qui bombardent le site Web ou le réseau de la victime, créant ainsi une perturbation encore plus importante de l'activité, poussant dès lors la victime à négocier.

En 2021 et au début de 2022, la tendance la plus préjudiciable en matière de ransomware concerne les attaques de la chaîne d'approvisionnement, dans le cadre desquelles l'intrusion d'un fournisseur (généralement un fournisseur de logiciels ou d'autres technologies) ouvre la voie à des attaques de seconde phase contre les entreprises qui dépendent de ses produits. On estime que les attaques de la chaîne d'approvisionnement ont connu un essor de 51 % au cours du dernier semestre de 2021. Les acteurs malveillants ont fait les gros titres grâce à l'exploitation de produits logiciels populaires tels que SolarWinds, Kaseya et Log4j, et nous prévoyons une escalade de cette tendance dans les années à venir.

Séquence d'attaque des ransomwares

Les attaques par ransomware actuelles se déroulent généralement selon les étapes suivantes :

1. **Compromission initiale :** les hackers utilisent divers vecteurs d'intrusion pour accéder aux systèmes, notamment les e-mails d'hameçonnage, l'exploitation des vulnérabilités des outils de réseau privé virtuel (VPN) ou à distance, et l'utilisation de la force brute ou d'informations d'identification dérobées pour accéder aux connexions RDP (Remote Desktop Protocol). Les attaques de la chaîne d'approvisionnement constituent une autre méthode d'infiltration d'une entreprise.

2. **Déplacement latéral :** après avoir obtenu un accès initial, les acteurs malveillants rassemblent des informations sur l'infrastructure des victimes et se déplacent latéralement sur les systèmes réseau, en élevant les privilèges et en établissant des mécanismes de persistance si nécessaire, en cataloguant les données stratégiques à dérober ou à chiffrer et en déposant des payloads de ransomware destinées à être exécutées ultérieurement.

3. **Exfiltration de données :** dans le cas d'une double extorsion, les hackers déroberont ensuite des données sensibles pour les utiliser comme tactique d'extorsion secondaire dans le but d'exiger des paiements de rançon plus élevés. Cela réduit la marge de manœuvre des victimes : même si elles peuvent récupérer les données chiffrées à partir de sauvegardes, elles demeurent confrontées à la menace d'une divulgation des données volées par les cybercriminels.

4. **Exécution du ransomware :** ensuite, les attaquants déploient et exécutent le ransomware, chiffrant les fichiers ciblés sur les systèmes connectés au réseau. Le ransomware met généralement fin aux processus associés aux logiciels de sécurité et aux bases de données afin de maximiser le nombre de fichiers qu'il peut chiffrer. Les sauvegardes de copie fantôme sont aussi généralement supprimées du système pour empêcher la récupération des fichiers. Certaines familles de ransomwares redémarrent également le système compromis en mode sans échec sous Windows pour contourner les logiciels de sécurité avant de chiffrer les fichiers. Après le chiffrement des fichiers, les victimes reçoivent une demande de rançon contenant des instructions concernant le paiement et le déchiffrement de leurs fichiers.

5. **DDoS :** si la victime ne négocie pas, certains groupes de pirates lancent une attaque par déni de service distribué (DDoS) contre le réseau ou le site Web de la victime, perturbant ainsi ses activités commerciales afin d'obtenir un effet de levier supplémentaire.

La figure 1 présente la chaîne d'attaque typique d'un ransomware à extorsion multiple.

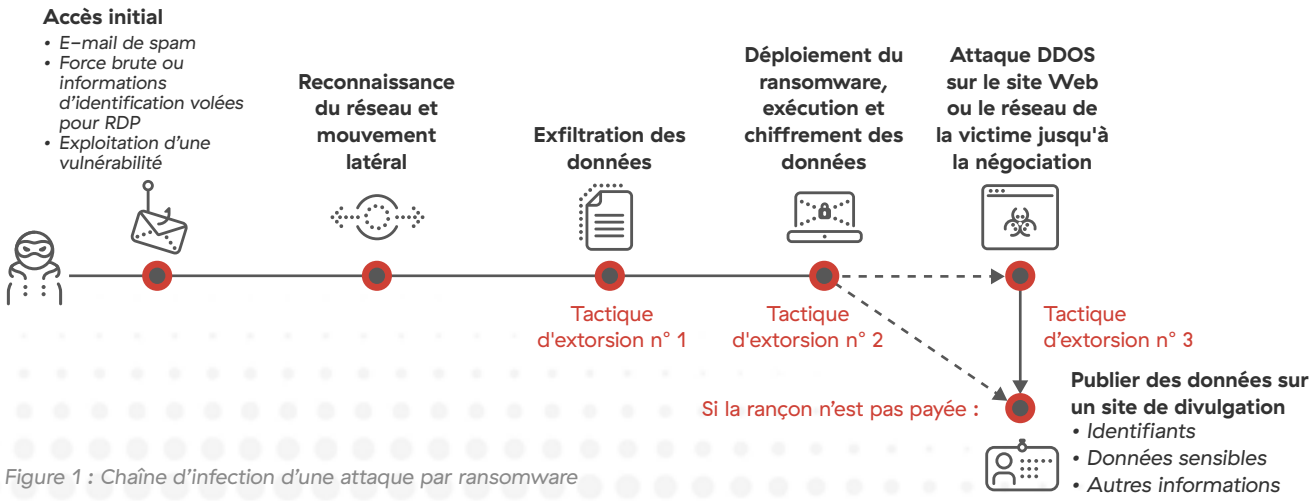


Figure 1 : Chaîne d'infection d'une attaque par ransomware

Statistiques sur les attaques par ransomware en 2021–2022

Le volume élevé de données de transaction sur Zero Trust Exchange apporte une perspective unique sur les tactiques et les victimes des cybercriminels. De février 2021 à mars 2022, ThreatLabz a observé une augmentation de 80 % des payloads de ransomware par rapport à l'année précédente. De plus, nous avons constaté une augmentation de 117 % du nombre de victimes de ransomware à double extorsion, d'après les données publiées sur les sites de divulgation des données des acteurs malveillants.

Secteurs d'activité touchés par les ransomwares

L'industrie manufacturière était déjà le marché le plus ciblé en 2020, comptant pour 12,7 % des attaques de ransomware à double extorsion entre novembre 2019 et janvier 2021. Cette année, le pourcentage d'attaques visant des entreprises manufacturières a encore augmenté pour atteindre 19,5 %, suivi par les services (9,7 %), la construction (8,1 %), le commerce de détail et la vente en gros (7,5 %) et la haute technologie (6,7 %).

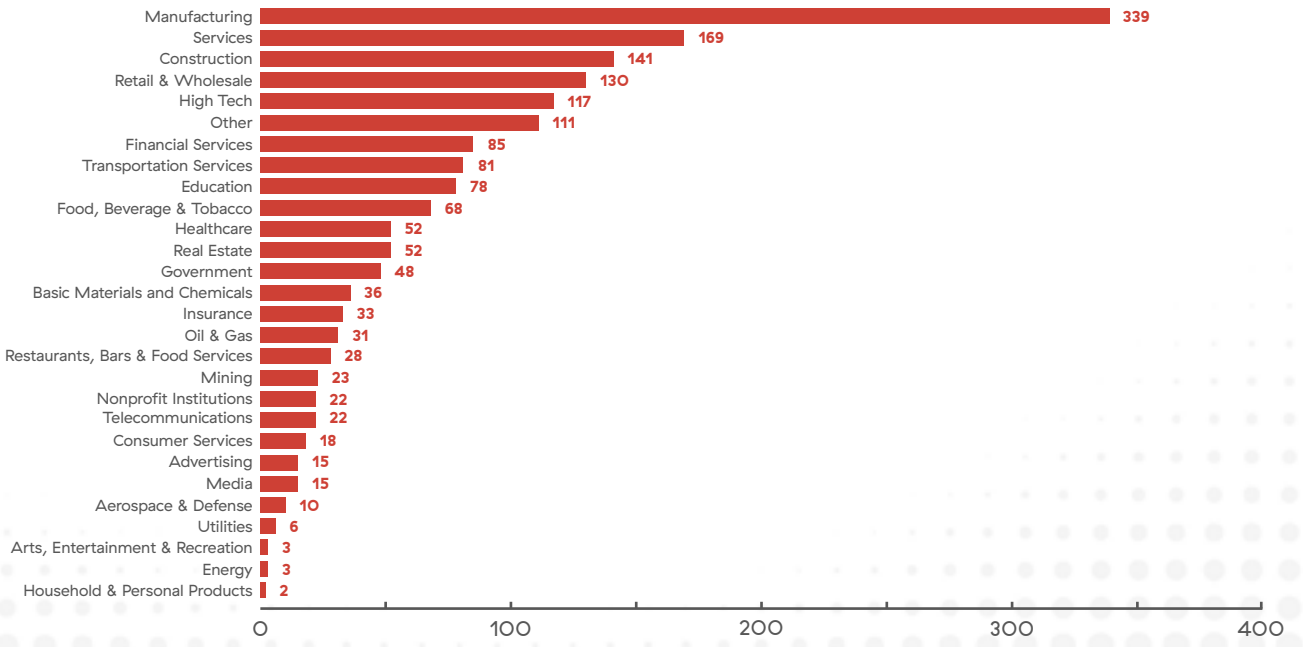


Figure 2 : Infections par ransomware par secteur d'activité

La croissance des attaques par ransomware à double extorsion varie considérablement en fonction du secteur. Dans le rapport de l'année dernière, nous avions constaté un nombre particulièrement faible d'attaques contre les entreprises du secteur de la santé, en raison d'une plus grande vigilance de la part des forces de l'ordre et de l'engagement de plusieurs familles de ransomwares à ne pas cibler le secteur de la santé pendant la pandémie de COVID-19.

Les données de cette année révèlent une situation bien différente. Les attaques de ransomwares à double extorsion contre les soins de santé ont augmenté de 643 % en 2021, bien qu'elles aient commencé avec une base de référence d'attaques très faible en 2020. Plusieurs autres secteurs d'activité présentant des points de départ plus élevés ont également connu une croissance à trois chiffres des attaques, notamment l'éducation (225 %), la fabrication (190 %), la construction (161 %), les services financiers (130 %) et les services (109 %).

Variation en pourcentage des attaques à double extorsion : 2021 vs 2020

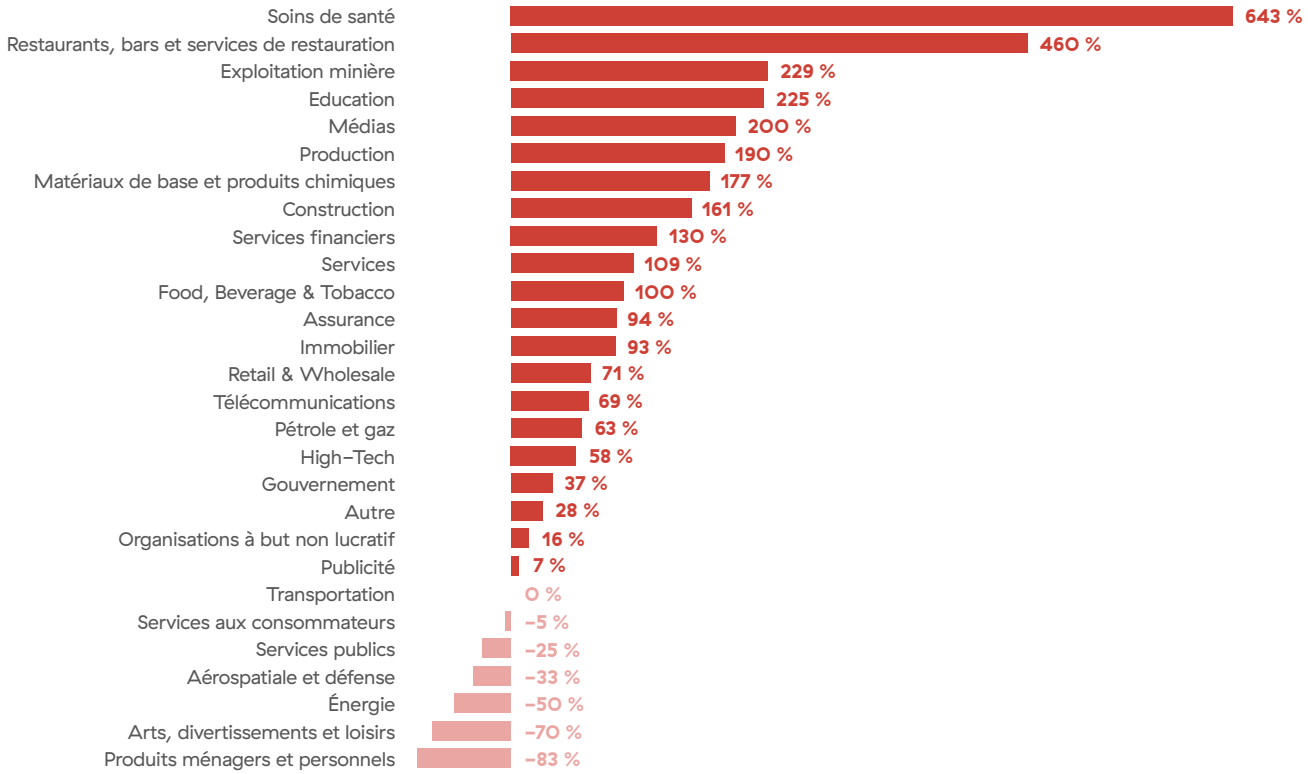


Figure 3 : Variation en pourcentage des attaques à double extorsion par secteur d'activité

Principales familles de ransomwares

Conti et LockBit ont été les familles de ransomwares à double extorsion les plus répandues en 2021, rejointes par une série de nouveaux entrants qui ont fait leur apparition au cours de l'année.

La figure 4 montre à quel moment chacune des familles de ransomwares les plus actives de ces dernières années est apparue et a commencé à publier des données sur des sites de divulgation ou des forums de piratage.

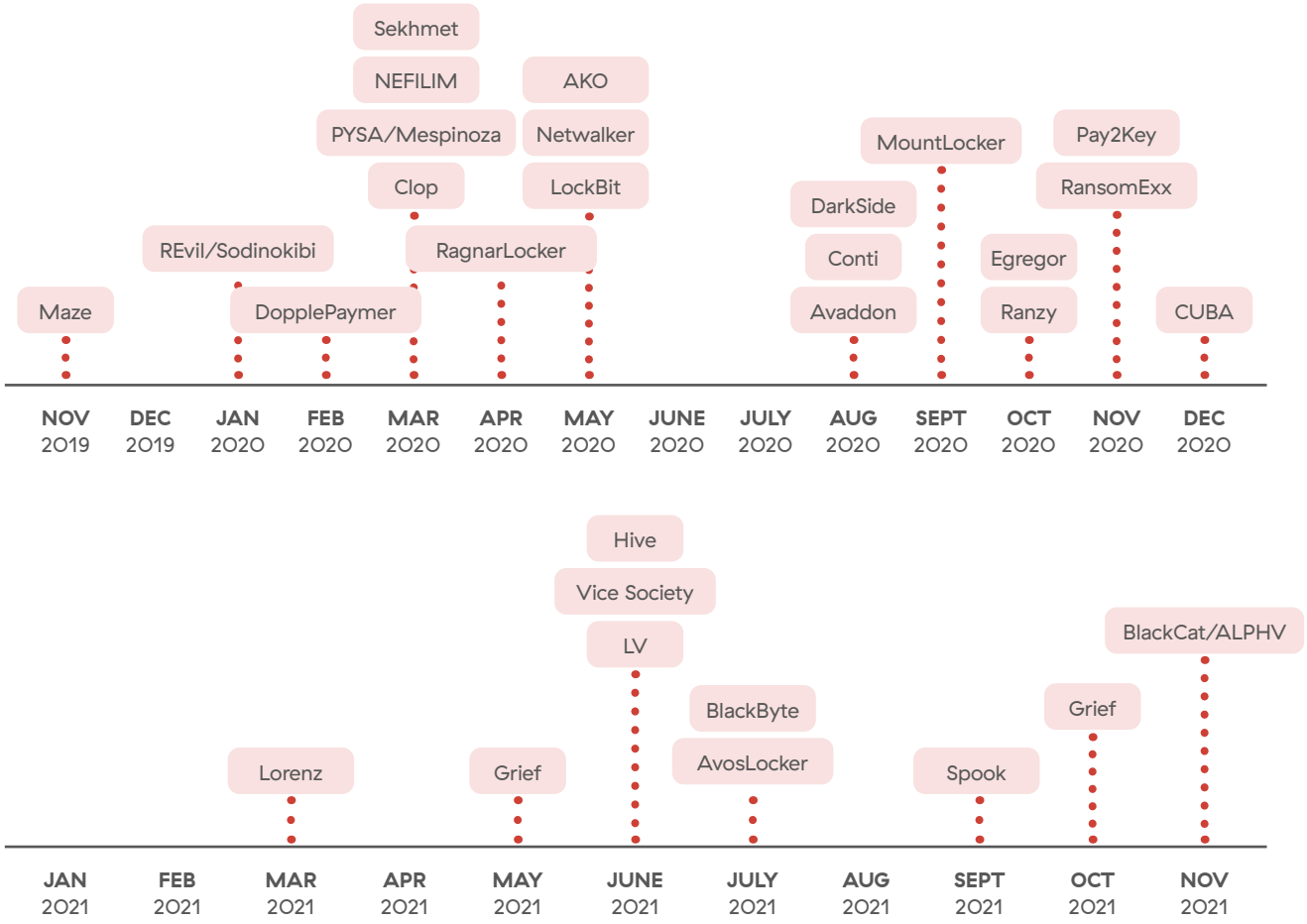


Figure 4 : Chronologie des familles de ransomwares publiant des données sur des sites de divulgation ou des forums de piratage

De nombreuses familles de ransomwares actives en 2021–2022 sont des modèles de ransomware en tant que service (RaaS), ce qui augmente leur distribution par le biais de réseaux d'affiliation. En 2021, nous avons également assisté à la nouvelle appellation de plusieurs familles de ransomwares populaires, comme DoppelPaymer qui s'est rebaptisé Grief, DarkSide qui s'est rebaptisé BlackMatter, et Avaddon qui s'est rebaptisé Haron suivi de Midas (ces deux derniers utilisant le constructeur de ransomwares Thanos).

Conti a été le groupe de ransomwares le plus actif de ces deux dernières années et le plus coûteux de tous les temps : le FBI estime qu'en janvier 2022, plus de 1 000 victimes d'attaques associées au ransomware Conti ont été recensées, le montant total des paiements effectués par les victimes dépassant 150 millions de dollars américains (sans compter les dommages connexes ou les coûts de remise en état). Parmi les victimes de Conti figurent diverses entreprises de services essentiels des secteurs des services financiers, de l'informatique, de l'énergie et des administrations publiques, notamment les services de santé publique d'Irlande et le gouvernement du Costa Rica. En mai 2022, le Département d'État américain a offert une récompense de 10 millions de dollars pour toute information concernant les dirigeants du groupe.

LockBit, anciennement connu sous le nom de ransomware ABCD, s'attaque généralement aux petites et moyennes entreprises, évitant ainsi de faire la une des journaux, à l'exception de l'attaque contre Accenture menée en août 2021. LockBit est un RaaS très répandu qui séduit les hackers en raison de sa vitesse et de ses performances.

La figure 5 montre les familles de ransomwares qui ont touché le plus grand nombre d'entreprises avec des attaques à double extorsion entre février 2021 et mars 2022, sur la base d'informations provenant de sites de divulgation de données.

Attaques par famille de ransomware

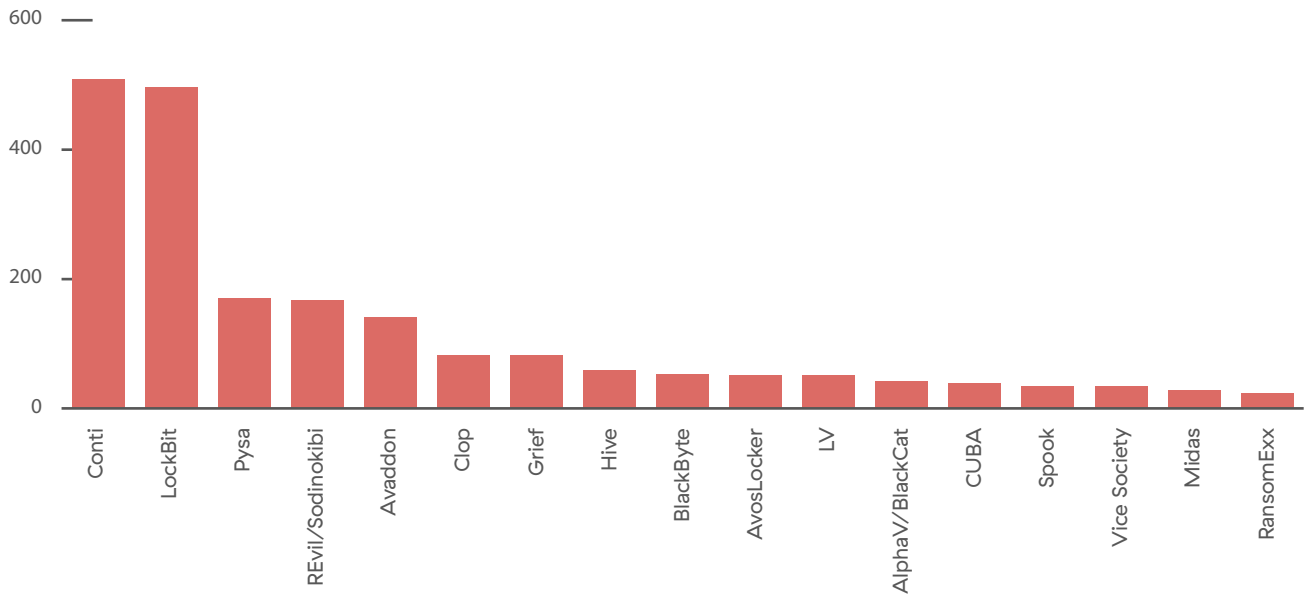


Figure 5 : Attaques par famille de ransomware, février 2021–mars 2022

Prévisions pour 2022–2023

Le nombre de ransomwares en tant que service va continuer à augmenter

Les RaaS ont prouvé leur utilité pour toutes les parties concernées. Les nouveaux développeurs de ransomwares et leurs affiliés utiliseront davantage ce modèle pour mener des attaques qui évoluent rapidement contre des entreprises vulnérables.

L'évolution des modèles de ransomwares entraînera un changement des cibles

Les créateurs de ransomwares et les informations sur les organisations étant disponibles à la vente sur le Dark Web, les hackers ont l'avantage de pouvoir filtrer les profils des sociétés afin d'affiner leurs cibles idéales en fonction des vulnérabilités, des bénéfices et des types de ransomwares. Il faut donc s'attendre à une évolution vers des cibles plus faciles, notamment les petites et moyennes entreprises disposant de moins de contrôles de sécurité, ainsi que les entreprises dont les applications visibles sur Internet présentent des vulnérabilités connues et dont les informations d'identification ont déjà été hameçonnées.

Le temps d'attente va continuer à diminuer

Maintenant que les acteurs malveillants disposent d'un accès facile et bon marché aux profils des sociétés et aux informations d'identification compromises en vente sur le Dark Web, l'époque où les attaquants surveillaient les cibles pendant des mois, voire des années, puis prenaient le temps de les analyser avant de lancer une attaque touche à sa fin. De plus en plus de rapports publics font état de hackers par ransomware qui réduisent leur temps d'observation à quelques jours seulement. Les criminels ont compris que les techniques de détection sont de plus en plus efficaces et que le temps est un facteur essentiel pour la réussite d'une attaque. Les équipes de sécurité doivent par conséquent remédier à cette situation et réduire la détection à quelques jours, quelques heures, voire quelques minutes, pour éviter les violations les plus graves en 2022 et au-delà.

Les attaques contre la chaîne d'approvisionnement vont se multiplier à mesure que les adversaires compromettent les écosystèmes des partenaires et des fournisseurs

Les plus grandes entreprises du monde disposent souvent de la meilleure sécurité possible, mais il n'en va pas forcément de même pour leurs fournisseurs et leurs partenaires, qui ont accès à des réseaux, des systèmes et des informations. Nous l'avons constaté lors de la récente compromission d'Okta par le groupe de pirates informatiques Lapsus$, et lors de la menace de REvil contre Apple via Quanta Computer, l'un des principaux fabricants de produits Apple. Ces groupes et bien d'autres ont utilisé des attaques de la chaîne d'approvisionnement pour accéder à des informations sensibles en amont en utilisant l'accès des fournisseurs sans jamais avoir à violer les mesures de sécurité renforcées de leurs cibles finales.

Les ransomwares peuvent être utilisés en tant que wiper ou en conjonction avec un wiper pour détruire des données

Au début de 2022, les attaques médiatisées contre l'Ukraine comportaient plusieurs types de wiper, dont HermeticWiper et un ransomware de leurre connu sous le nom de PartyTicket. Ce n'est pas la première fois que des ransomwares sont utilisés dans des attaques géopolitiques : NotPetya et Bad Rabbit ont été déployés en 2017 pour attaquer des entreprises ukrainiennes. Les tensions géopolitiques engendrent la menace de ransomwares masqués, de wipers et d'autres tactiques qui offrent aux acteurs malveillants un degré élevé d'anonymat et de déni plausible.

Les anciennes (et nouvelles) vulnérabilités continueront à faire des dégâts

Quelques vulnérabilités majeures ont été découvertes l'année dernière (par exemple, Log4j, PrintNightmare, ProxyShell/ProxyLogon) avec lesquelles les entreprises devront vivre pendant des années. Les hackers continueront de rechercher et d'exploiter des logiciels et des serveurs non corrigés ou obsolètes pour contourner les contrôles de sécurité.

Les familles de ransomwares vont continuer à utiliser de nouvelles appellations

Nous avons observé ce cycle tout au long de l'année 2021 : un groupe de ransomwares réussit une attaque majeure, attire l'attention des forces de l'ordre qui les sanctionnent, puis disparaît et se reforme plus tard sous un nouveau nom. Les ransomwares étant dans le collimateur des forces de l'ordre, ce cycle se poursuivra en 2022 et au-delà.

Les entreprises devront renforcer leur sécurité au-delà de la protection des terminaux

Les groupes de ransomware utiliseront davantage de tactiques pour contourner les antivirus et autres contrôles de sécurité des terminaux. Les entreprises auront encore plus besoin d'une défense en profondeur au lieu de s'appuyer uniquement sur la sécurité des terminaux pour détecter et empêcher les intrusions.

Les développeurs de ransomwares ajouteront davantage de techniques d'obscurcissement des programmes malveillants

Les auteurs de programmes malveillants mettent en œuvre des techniques d'obscurcissement des programmes malveillants pour gêner l'ingénierie inverse et contourner la détection par signature statique. La complexité de d'obscurcissement des programmes malveillants ne cessera de croître avec les techniques avancées, notamment l'aplatissement du flux de contrôle, d'obscurcissement des chaînes polymorphes et l'utilisation de packers basés sur des machines virtuelles.

Les fuites de code source de ransomwares conduiront à des bifurcations

L'année dernière, le code source de plusieurs ransomwares a été divulgué, notamment deux versions de Conti et Babuk. Zscaler ThreatLabz a déjà constaté que le code source de ces deux familles de ransomwares était détourné par des tiers et utilisé dans des attaques. La publication du code source entraînera sans aucun doute des abus de la part d'autres groupes criminels qui n'ont pas l'expertise nécessaire pour concevoir et construire leur propre ransomware à partir de zéro.

Conseils de prévention

Qu'il s'agisse d'une simple attaque par ransomware, d'une attaque à double ou triple extorsion, d'une famille de menaces autonome ou d'une attaque par RaaS exécutée par un réseau affilié, la stratégie de défense est la même : appliquer les principes Zero Trust pour limiter les vulnérabilités, prévenir et détecter les attaques, et limiter le rayon d'action des violations réussies. Voici quelques recommandations de meilleures pratiques pour protéger votre entreprise contre les ransomwares.

1 Retirer vos applications d'Internet.

Les acteurs des ransomwares commencent leurs attaques en effectuant une reconnaissance de votre environnement, en recherchant les vulnérabilités exploitables et en calibrant leur approche. Plus vos applications seront publiées sur Internet, plus vous serez facile à attaquer. Utilisez une architecture Zero Trust pour sécuriser les applications internes et les rendre invisibles aux attaquants.

2 Appliquer une politique de sécurité cohérente pour empêcher la compromission initiale.

Avec des collaborateurs travaillant à distance, il est important de mettre en œuvre une architecture SSE (Security Service Edge) capable d'appliquer une politique de sécurité cohérente, quel que soit le lieu de travail des utilisateurs (au bureau ou à distance).

3 Recourir au sandboxing pour détecter les payloads inconnus.

La détection basée sur la signature ne suffit pas face à l'évolution rapide des variantes et des payloads des ransomwares. Il est indispensable de se protéger contre les attaques inconnues et dérobées au moyen d'un sandbox inline, alimenté par l'IA, qui analyse le comportement plutôt que l'emballage d'un fichier.

4 Mettre en œuvre une architecture ZTNA (Zero Trust Network Access).

Mettez en œuvre une segmentation granulaire utilisateur–application et application–application en négociant l'accès à l'aide de contrôles dynamiques des accès sur la base du moindre privilège pour éliminer les déplacements latéraux. Cela vous permet de minimiser les données susceptibles d'être chiffrées ou dérobées, réduisant ainsi le rayon d'action d'une attaque.

5 Déployer une protection inline contre la pertes de données.

Empêchez l'exfiltration d'informations sensibles à l'aide d'outils et de politiques de protection contre la perte de données basés sur la confiance, afin de déjouer les techniques de double extorsion.

6 Maintenir les logiciels et les formations à jour.

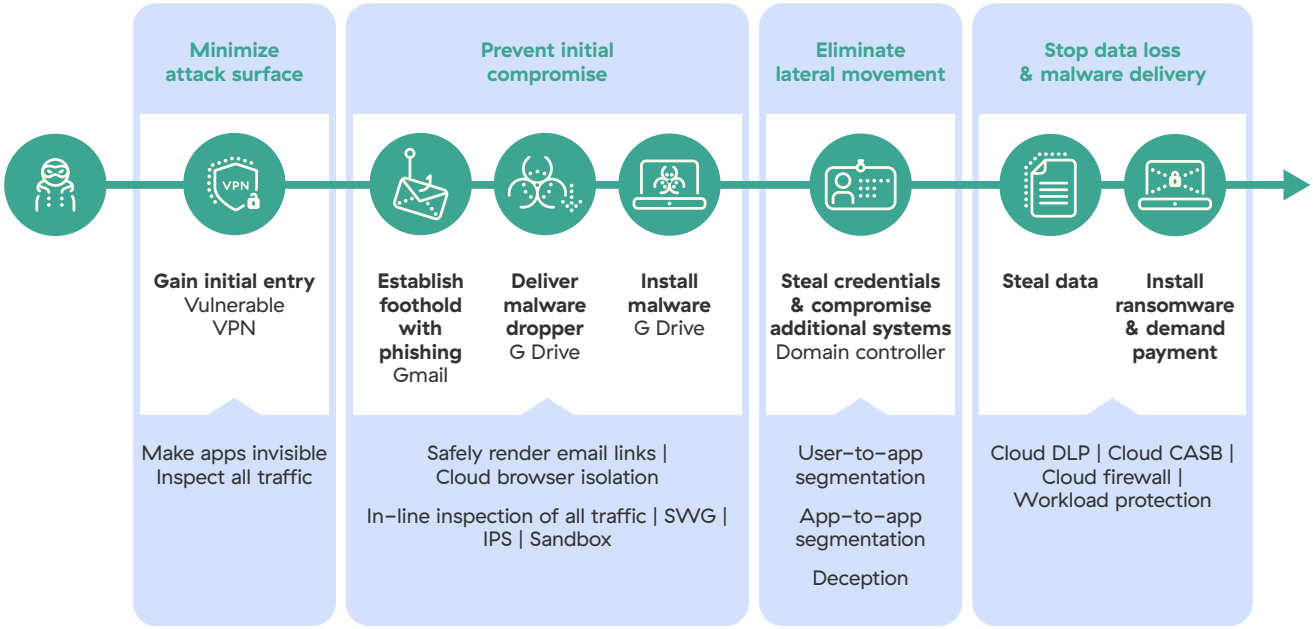
Appliquez des correctifs de sécurité logicielle et former régulièrement les employés sur la sensibilisation à la sécurité afin de réduire les vulnérabilités pouvant être exploitées par les cybercriminels.

7 Disposer d'un plan de réaction.

Préparez–vous au pire avec une cyber–assurance, un plan de sauvegarde des données et un plan de réaction dans le cadre de votre programme global de continuité des activités et de reprise après sinistre.

Pour maximiser vos chances de vous prémunir des ransomwares, vous devez adopter des défenses en couches capables de perturber l'attaque à chaque étape, de la reconnaissance à la compromission initiale, au déplacement latéral, au vol de données et à l'exécution du ransomware.

Stopping ransomware with zero trust



Principales tendances des ransomwares

Attaques de la chaîne d'approvisionnement

Qu'est-ce qu'une attaque de la chaîne d'approvisionnement ?
Les attaques de la chaîne d'approvisionnement, parfois appelées attaques de la chaîne de valeur ou attaques de tiers, sont des attaques contre les fournisseurs d'une entreprise afin d'obtenir un accès. La plupart des grandes entreprises disposent de contrôles de sécurité sophistiqués qui empêchent toute infiltration. Les attaquants ont donc trouvé un moyen d'entrer par le biais des fournisseurs de ces entreprises.

Les attaques de la chaîne d'approvisionnement exploitent la confiance qui règne entre les entreprises légitimes dans le cadre d'opérations commerciales normales. Les hackers installent une porte dérobée dans un produit que leur cible utilise, ce qui leur permet de s'infiltrer dans son réseau sans être détectés, généralement par le biais de correctifs ou de mises à jour logicielles automatiques, appelés mises à jour « trojanisées ». Une fois dans le réseau, les attaquants peuvent espionner, dérober des données, implanter d'autres programmes malveillants et perturber les opérations.

Ces attaques exigent un haut degré de planification et de sophistication et peuvent avoir un impact dévastateur sur les entreprises situées dans le rayon d'action de l'attaque initiale.

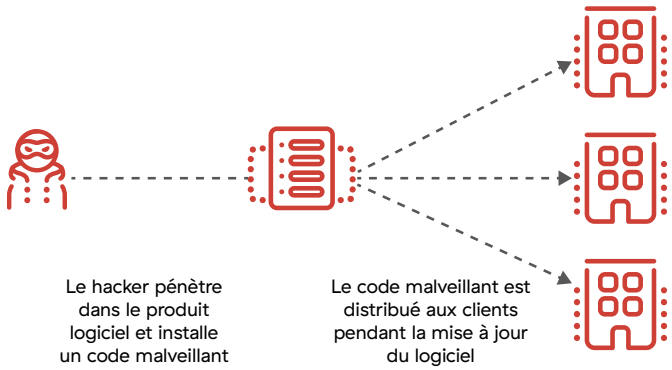


Figure 6 : Attaque de la chaîne d'approvisionnement

Ransomware de la chaîne d'approvisionnement de Kaseya
Le 2 juillet 2021, la société de logiciels de gestion informatique Kaseya a révélé un incident de sécurité affectant sa version sur site du logiciel Kaseya VSA, une plateforme qui permet aux fournisseurs de services gérés (MSP) d'effectuer la gestion des correctifs, des sauvegardes et la surveillance des clients pour leurs usagers. Environ 70 MSP auraient été touchés par cette attaque, avec un impact en aval sur 1 500 petites et moyennes entreprises.

Le pirate à l'origine de cette attaque a identifié et exploité une vulnérabilité de type Zero-Day dans le serveur Kaseya VSA qui lui a permis d'envoyer un script malveillant à tous les clients gérés par ce serveur. Le script a été utilisé pour diffuser le ransomware REvil/Sodinokibi qui a chiffré des fichiers sur les systèmes affectés.

Chaîne d'approvisionnement de Quanta Computer
En avril 2021, REvil a attaqué Quanta Computer, le plus grand fabricant d'ordinateurs portables au monde et l'un des principaux fabricants de produits Apple. Quanta a refusé de payer une rançon de 50 millions de dollars, ce qui a conduit REvil à cibler Apple et d'autres clients de Quanta pour obtenir la rançon. REvil a divulgué 21 captures d'écran de schémas de MacBook et a menacé de publier d'autres données d'Apple et d'autres sociétés jusqu'à ce qu'Apple ou Quanta paie la demande de rançon.

Ransomware Log4j

En décembre 2021, la fondation Apache Software a publié un avis de sécurité concernant une vulnérabilité d'exécution de code à distance (CVE-2021-44228) dans sa fameuse bibliothèque de journalisation Log4j. Cette vulnérabilité permet à un attaquant de télécharger et d'exécuter un payload malveillant en soumettant une requête spécialement conçue au système vulnérable. L'attaquant peut alors contrôler les messages de journalisation ou les paramètres des messages de journalisation pour exécuter un code arbitraire chargé à partir de serveurs LDAP lorsque la substitution de recherche de messages est activée. Log4j est incorporé dans de nombreux sites Web, applications et frameworks populaires, ce qui étend la portée de son impact. Plusieurs attaques ransomware ont émergé exploitant cette vulnérabilité :

Ransomware NightSky
Le 4 janvier 2021, des hackers ont exploité la vulnérabilité Log4j dans un système tourné vers internet et exécutant VMware Horizon, et ont déposé le ransomware NightSky.

Khonsari
De multiples attaques ont été observées utilisant des exploits Log4j sur des systèmes Windows afin de déployer le ransomware Khonsari.

Conti
Le groupe Conti a également exploité la vulnérabilité Log4j pour exécuter des attaques par ransomware. AdvIntel a découvert que le groupe analysait et ciblait les versions vulnérables de Log4j de VMware vCenter, se déplaçant latéralement à partir des sessions Cobalt Strike existantes vers les réseaux de victimes américains et européens.

TellYouThePass
Des hackers ont exploité la vulnérabilité de Log4j pour déployer et exécuter le ransomware TellYouThePass dans des systèmes Windows et Linux.

Ransomware en tant que service

Le Dark Web est devenu un endroit très populaire pour les groupes de menaces qui vendent leurs produits aux criminels en puissance. Nous avons détaillé l'impact de ces places de marché sur d'autres types d'attaques, comme la croissance de l'hameçonnage en tant que service dans le rapport 2022 de ThreatLabz sur l'état de l'hameçonnage.

Le RaaS est devenu incroyablement populaire, et il est désormais à l'origine de la plupart des attaques de ransomware modernes. De fait, 8 des 11 principales familles de ransomwares de l'année dernière utilisent des écosystèmes RaaS.

Le modèle RaaS implique deux parties : les opérateurs et les affiliés. Les opérateurs sont les groupes malveillants qui développent le ransomware. Les affiliés ciblent leurs victimes, exécutent le ransomware et fixent les exigences.

Les opérateurs recrutent les affiliés et leur fournissent le ransomware et les outils nécessaires à son exécution, l'accès à un site de divulgation de données, une aide à la négociation et d'autres formes de soutien, en échange d'environ 70 à 80 % des bénéfices des attaques.

Ce modèle est profitable aux deux parties. Les affiliés obtiennent tout ce dont ils ont besoin pour exécuter des attaques par ransomware très efficaces sans avoir à développer quoi que ce soit eux-mêmes. Cette solution est séduisante tant pour les criminels qualifiés qui économisent du temps et des ressources de développement que pour les criminels peu qualifiés qui, sans cela, ne seraient pas en mesure d'exécuter une telle attaque. Les opérateurs de ransomware peuvent augmenter considérablement l'ampleur de leurs opérations et, par conséquent, leurs profits.

Le RaaS a augmenté à la fois le volume et les dommages des attaques :

- **Augmentation du volume des attaques par ransomware :** davantage d'affiliés entreprennent d'exécuter des ransomwares car leur développement requiert désormais moins de temps et de compétences.
- **Augmentation du montant des rançons due à la double extorsion :** le RaaS inclut une composante de double extorsion dans le cadre de laquelle les acteurs malveillants dérobent des données et menacent de les publier sur un site de divulgation de données si la rançon n'est pas payée. Cela augmente le montant de la rançon et le taux de succès du paiement.

Attaques géopolitiques

Les responsables de la sécurité du monde entier sont sur leurs gardes face à une augmentation des attaques par ransomware consécutive au conflit Russie-Ukraine.

En mars 2022, le président des États-Unis, Joe Biden, a publié une mise en garde contre le risque de cyberattaques malveillantes visant les États-Unis en réponse aux sanctions économiques infligées à la Russie. Il a demandé que des mesures immédiates soient prises pour renforcer les cyberdéfenses des entreprises des secteurs public et privé.

8 des 11 principales familles de ransomwares de 2021 utilisent des écosystèmes RaaS.

Au moment de la rédaction de ce rapport, plusieurs attaques par ransomware ont été menées contre l'Ukraine et/ou associées à ce conflit :

1. **Ransomware PartyTicket :** ce ransomware basé sur Go a été utilisé conjointement avec le programme malveillant HermeticWiper pour cibler des entreprises en Ukraine. PartyTicket est peu sophistiqué et contient un chiffrement imparfait qui peut être déchiffré et inversé, ce qui nous amène à penser qu'il a été développé comme un leurre pour détourner l'attention d'HermeticWiper.
2. **Ransomware Conti :** la Cybersecurity and Infrastructure Security Agency (CISA), le Federal Bureau of Investigation (FBI), la National Security Agency (NSA) et les services secrets des États-Unis ont publié un nouvel avis sur Conti, un groupe de ransomware lié à la Russie. Leur mise en garde indique que « les acteurs de la cybermenace Conti restent actifs et que le nombre d'attaques par ransomware Conti contre des entreprises américaines et internationales s'élève à plus d'un millier ». Fin février, Conti a publié deux déclarations sur son site de divulgation, promettant de soutenir le gouvernement russe en réponse au « bellicisme occidental et aux menaces américaines d'utiliser la cyberguerre contre les citoyens de la Fédération de Russie. »

Démantèlements par les forces de l'ordre

Les organismes chargés de l'application de la loi du monde entier accordent une attention accrue aux familles de ransomware, en particulier celles qui causent des dommages étendus. Plusieurs démantèlements de familles de ransomware à fort impact ont été menés avec succès en 2021 et au début de 2022.

Démantèlement de REvil
REvil est l'une des familles de ransomware les plus notoires de ces deux dernières années. Elle a fait parler d'elle après des attaques majeures contre Kaseya et JSB. À la suite de l'attaque de Kaseya, le FBI avait prévu de démanteler les serveurs de REvil. Cependant, il n'a jamais pu concrétiser son projet : peu après cette attaque critique, en juillet 2021, REvil a mis fin à ses activités et les hackers ont disparu. Cette disparition s'est avérée brève, puisque les activités de REvil ont repris en septembre 2021.

En janvier 2022, le gouvernement russe a apparemment démantelé le groupe de hackers REvil, en arrêtant ses membres à la demande des États-Unis. Le Service fédéral de sécurité russe (FSB) a perquisitionné 25 adresses, détenu 14 membres du groupe REvil et saisi 426 millions de roubles, 600 000 dollars américains, 500 000 euros, 20 voitures de luxe et du matériel informatique. Cependant, REvil est réapparu en avril 2022, attaquant les entreprises avec une version actualisée du ransomware.

Démantèlement de DarkSide
Le 6 mai 2021, le groupe de ransomware DarkSide a exécuté une attaque par ransomware très médiatisée sur Colonial Pipeline, le plus grand oléoduc des États-Unis. Les agences fédérales ont pris des mesures et, dans les deux semaines suivant l'attaque, un acteur malveillant connu sous le nom de UNKN a annoncé que DarkSide avait été fermé, car il avait perdu l'accès aux serveurs et sa cryptomonnaie avait été transférée sur un compte inconnu. Le ministère de la justice a annoncé qu'il avait saisi 63,7 bitcoins soit environ 2,3 millions de dollars américains.

Démantèlement d'Egregor
Le groupe de ransomware Egregor, anciennement connu sous le nom de Maze, a été démantelé grâce à la coopération des forces de l'ordre le 9 février 2021. Des agences d'Ukraine, de France et des États-Unis ont fermé le site de divulgation d'Egregor, arrêté des membres du groupe et saisi des ordinateurs liés à des attaques par ransomware. Egregor avait extorqué environ 80 millions de dollars américains à plus de 150 sociétés victimes.

Nouvelles appellations des ransomwares

Les exploitants de ransomwares ont utilisé de nouvelles appellations à un rythme élevé au cours de l'année écoulée. Ces nouvelles appellations sont souvent causées par un intérêt indésirable de la part des forces de l'ordre et des médias, ainsi qu'à des sanctions qui limitent la capacité des groupes à percevoir des rançons.

DoppelPaymer, rebaptisé Grief
Début mai 2021, l'activité du ransomware DoppelPaymer a considérablement diminué. Bien que le site de divulgation de DoppelPaymer soit toujours en ligne, aucun nouvel avis de victime n'a été publié depuis le 6 mai 2021. En outre, aucun avis de victime n'a été mis à jour depuis la fin du mois de juin. Cette accalmie est probablement une réaction à l'attaque par ransomware de Colonial Pipeline qui a eu lieu le 7 mai 2021. Toutefois, cette pause apparente est imputable au groupe malveillant à l'origine de DoppelPaymer, qui a rebaptisé le ransomware sous le nom de Grief. Les deux variantes du ransomware partagent le même code malveillant, et les sites de divulgation sont très similaires. Le portail de demande de rançon de Grief présente quelques différences par rapport à celui de DoppelPaymer. En particulier, le mode de paiement de la rançon est effectué en Monero (XMR) au lieu de bitcoin (BTC). Ce changement de cryptomonnaie peut être une réponse au FBI qui a récupéré une partie du paiement de la rançon de Colonial Pipeline.

Les groupes de ransomwares changent d'appellation pour contourner les sanctions et détourner l'attention des forces de l'ordre.

Darkside, rebaptisé BlackMatter
Après la fermeture de DarkSide en mai 2021, une nouvelle famille de ransomware baptisée BlackMatter est apparue fin juillet. La routine de chiffrement utilisée dans le ransomware et le texte du site de divulgation des données indiquent que BlackMatter est une nouvelle appellation de DarkSide.

BlackMatter a cessé ses activités en novembre 2021. Le groupe a publié un message de cessation des opérations sur son portail RaaS qui stipulait : « En raison de certaines circonstances insolubles liées à la pression des autorités (une partie de l'équipe n'est plus disponible, d'après les dernières nouvelles), le projet est fermé ».

Nouvelle appellation du ransomware basé sur Thanos Annoncé sur le Dark Web comme un RaaS, le ransomware Thanos a été identifié pour la première fois en février 2020. Le créateur de Thanos a subi une perte de données, et au cours des deux années suivantes, une série de nouvelles variantes ont été développées. La variante Prometheus du ransomware est apparue en février 2021. En septembre, Prometheus a été rebaptisé Spook. Tous deux présentent des messages de rançon et des sites de divulgation de données similaires, et contiennent l'identifiant de clé de signature de Thanos.

En juillet 2021, un autre ransomware dérivé de Thanos, appelé Haron, a été découvert. Le ransomware Haron présente des similitudes frappantes avec le ransomware Avaddon. Haron et Avaddon partagent des points communs dans leurs demandes de rançon, leurs sites de négociation et leurs sites de divulgation de données. En octobre 2021, une autre variante appelée Midas a été découverte. Il s'agit d'une version rebaptisée du ransomware Haron.

Nouvelle appellation d'Evil Corp
Le gang Evil Corp, également connu sous le nom d'Indrik Spider, est connu pour diverses activités malveillantes. Il a créé des chevaux de Troie bancaires tels que Dridex, ce dernier étant utilisé pour diffuser leur ransomware BitPaymer.

L'Office of Foreign Assets Control (OFAC) du département du Trésor américain a sanctionné les membres d'Evil Corp pour les dommages causés par son programme malveillant Dridex, affirmant qu'il a infligé plus de 100 millions de dollars de préjudice à des banques et institutions financières dans plus de 40 pays. À la suite de ces sanctions, les sociétés de négociation de ransomware ont refusé de faciliter le paiement de rançons pour le compte d'Evil Corp par crainte d'amendes ou de poursuites judiciaires de la part du département du Trésor américain. Pour contourner les sanctions, Evil Corp a découvert une échappatoire simple en rebaptisant son ransomware.

Evil Corp a diffusé le ransomware WastedLocker en juin 2020, le ransomware Hades en décembre 2020 et le ransomware Phoenix en mars 2021. En mai 2021, ils ont continué à rebaptiser leur ransomware sous le nom de PayloadBin, se faisant passer pour un autre acteur malveillant qui n'était pas soumis aux mêmes sanctions.

Nouvelle appellation de Rook
Le ransomware Rook a été repéré en novembre 2021, sur la base de la fuite du code source du ransomware Babuk. En décembre 2021, une variante de Rook a été rebaptisée Night Sky, qui a été utilisée par le groupe d'acteurs malveillants DEV-0401, basé en Chine, pour cibler des réseaux d'entreprise dans le cadre d'attaques par ransomware à double extorsion exploitant la vulnérabilité Log4Shell. En janvier 2022, Rook et Night Sky ont cessé leurs activités, et le ransomware Pandora est apparu. D'après les similitudes de code, Pandora est également une version rebaptisée de Rook.

Principales vulnérabilités utilisées dans les attaques par ransomware

Vulnérabilités de ProxyLogon Les ransomwares
BlackKingdom et DearCry ont combiné quatre exploits différents de la vulnérabilité de ProxyLogon pour s'introduire et chiffrer les réseaux de leurs victimes. Cette tactique a été utilisée pour accéder aux serveurs Microsoft Exchange, dérober des e-mails et déployer d'autres portes dérobées. Les vulnérabilités ProxyLogon incluent CVE-2021-26855 (vulnérabilité SSRF, pour Server-Side Request Forgery, dans Exchange), CVE-2021-26857 (vulnérabilité de désérialisation non sécurisée dans le service Unified Messaging), CVE-2021-26858 (vulnérabilité d'écriture de fichier arbitraire après authentification dans Exchange) et CVE-2021-27065 (vulnérabilité d'écriture de fichier arbitraire après authentification dans Exchange). Microsoft a corrigé ces vulnérabilités en mars 2021.

Une chaîne d'attaque type qui permet à un hacker d'exécuter du code à distance sur le port 443 exposé : les hackers utilisent la vulnérabilité CVE-2021-26855 pour contourner l'authentification de Microsoft Exchange et se faire passer pour un utilisateur. L'attaquant envoie une requête POST modifiée pour tout fichier dans le répertoire qui est lisible sans authentification, où le fichier du répertoire n'est pas requis. L'attaquant s'authentifie dans le panneau de contrôle Exchange (ECP) et écrase tout fichier dans le système ciblé en utilisant les vulnérabilités CVE-2021-26858 ou CVE-2021-27065. Après ces exploits, un attaquant peut exécuter du code à distance en utilisant le shell Web sur le serveur Exchange.

Vulnérabilité d'échange ProxyShell
Le ransomware Conti exploite la vulnérabilité de Microsoft Exchange Server pour s'introduire dans le réseau de la victime. Les vulnérabilités de l'échange ProxyShell sont une combinaison des

vulnérabilités CVE-2021-34473 (vulnérabilité d'exécution de code à distance de Microsoft Exchange Server), CVE-2021-34523(vulnérabilité d'élévation des privilèges de Microsoft Exchange Server) et CVE-2021-31207 (vulnérabilité de contournement des fonctions de sécurité de Microsoft Exchange Server). Microsoft a corrigé ces vulnérabilités entre avril et mai 2021, mais Conti continue de cibler les serveurs non corrigés pour exécuter du code à distance. La chaîne d'infection de ce ransomware peut être consultée dans ce rapport, dans les analyses des gangs de ransomware BlackByte, AvosLocker et Hive. Le ransomware LockFile cible également ces vulnérabilités pour se déployer.

PrintNightmare
Les acteurs du ransomware exploitent les vulnérabilités PrintNightmare pour cibler des systèmes Windows. Les vulnérabilités PrintNightmare sont une combinaison des vulnérabilités CVE-2021-34527 et CVE-2021-34481, des vulnérabilités d'exécution de code à distance dans le service de spouleur d'impression de Windows qui effectue incorrectement les opérations de fichiers privilégiés et permet aux attaquants d'exécuter du code à distance avec des privilèges SYSTEM.

La vulnérabilité existe dans la fonction Pointer et imprimer des systèmes Windows, et permet à des utilisateurs non privilégiés de mettre à jour ou d'installer des imprimantes à distance. Microsoft a publié des mises à jour pour PrintNightmare en juillet et en août 2021 afin de corriger ces vulnérabilités.

Lors d'une attaque, un groupe de ransomware a exploité les vulnérabilités PrintNightmare et a déposé le ransomware Vice Society. Dans une autre campagne, les hackers ont exploité PrintNightmare et ont déposé le ransomware Magniber.

SonicWall SMA 100
En janvier 2021, SonicWall a confirmé une vulnérabilité d'injection SQL dans son produit Secure Mobile Access SMA 100 Series, qui permettait aux attaquants d'accéder aux informations d'identification et aux sessions de connexion, ainsi que d'accéder aux appareils vulnérables en utilisant des requêtes non authentifiées et spécialement conçues. Elle\a été corrigée par SonicWall en février 2021.

Elle a été découverte après que le groupe malveillant UNC2447 a utilisé cette faille pour attaquer un réseau ciblé et déployer le ransomware à double extorsion FIVEHANDS dans les systèmes des victimes. L'acteur malveillant a utilisé cette vulnérabilité de type Zero-Day pour s'introduire dans le réseau et y déposer la porte dérobée SOMBRAT, ainsi que d'autres outils pour s'implanter, effectuer une reconnaissance et exfiltrer des données, notamment les balises Cobalt Strike, Adfind, BloodHound, Mimikatz, PC Hunter et Rclone. À la fin de l'attaque, UNC2447 a déposé et exécuté le ransomware FIVEHANDS pour chiffrer les données du système ciblé, puis a tenté d'extorquer de l'argent en menaçant de publier les données sur des forums de hackers.

Dispositif NAS QNAP
Une nouvelle variante du ransomware eChOraix a ciblé les dispositifs de stockage en réseau (NAS) de Quality Network Appliance Provider (QNAP) et les dispositifs NAS de Synology. Dans la chaîne d'attaque, l'attaquant a exploité la vulnérabilité CVE-2021-28799 dans les appareils NAS de QNAP. La vulnérabilité d'autorisation incorrecte a été signalée dans les périphériques NAS de QNAP exécutant HBS 3 (Hybrid Backup Sync) et permet à l'attaquant de se connecter à un appareil à distance.

Les 11 familles de ransomwares les plus répandues

Voici un aperçu de 11 familles de ransomwares différentes et de leurs séquences d'attaques. Ces familles de ransomwares ont fait le plus grand nombre de victimes en 2021 et en 2022, et représentent parfaitement l'état actuel des ransomwares contre lesquels votre entreprise doit se défendre. Pour chaque famille, nous fournirons un bref historique, un résumé de leurs tactiques (y compris les cartographies de MITRE ATT&CK), ainsi que quelques statistiques sur les industries ciblées.

Conti

Le ransomware Conti a été repéré pour la première fois en février 2020. Conti est parfois qualifié de RaaS, mais ses affiliés sont essentiellement des employés, plutôt que des affiliés qui s'inscrivent, utilisent un portail pour gérer la page et perçoivent une part des bénéfices. Conti et Ryuk partagent un code similaire, ce qui laisse penser que Conti est probablement le successeur du ransomware Ryuk. Conti a été le ransomware le plus répandu en 2021.

Chaîne d'infection :
Conti a utilisé une série de mécanismes d'accès initial dans le cadre de diverses campagnes.

1. Il a été distribué par le biais d'e-mails de spam contenant des pièces jointes ou des liens malveillants qui téléchargent ensuite TrickBot, IcedID, BazarLoader ou Cobalt Strike pour permettre de s'introduire dans le système.
2. L'accès initial se fait également en exploitant des vulnérabilités connues telles que Log4j, ProxyShell, ou en utilisant des informations d'identification RDP (Remote Desktop Protocol) trop faibles.

Après la compromission, Conti utilise Cobalt Strike, Mimikatz et d'autres outils de post-exploitation pour dérober des informations d'identification et s'implanter sur le réseau. Les acteurs malveillants de Conti utilisent Metasploit, Netscan et d'autres outils de red teaming pour obtenir des informations sur le réseau et les contrôleurs de domaine. Après avoir obtenu les informations nécessaires, les acteurs malveillants peuvent utiliser AnyDesk, PsExec ou d'autres utilitaires à distance pour se déplacer latéralement. Les acteurs malveillants de Conti exfiltrent les données à l'aide de Rclone ou d'autres outils, et enfin déploient et exécutent le ransomware Conti pour chiffrer les données, comme le montre la figure 7 ci-dessous.

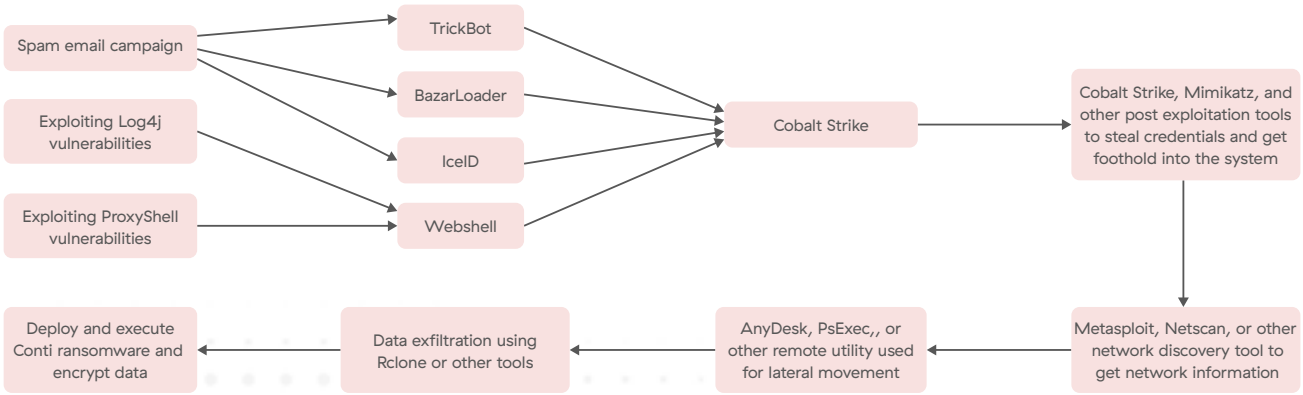


Figure 7 : Anatomie d'une attaque par ransomware Conti

La première version de Conti utilisait les algorithmes RSA et AES pour le chiffrement. Cependant, AES a ensuite été remplacé par le chiffrement ChaCha.

Fin janvier 2022, ThreatLabz a identifié une version actualisée du ransomware Conti dans le cadre de ses activités de suivi des ransomwares à l'échelle mondiale. Cette mise à jour a été publiée avant une fuite massive du code source et des journaux de chat de Conti le 27 février 2022, qui a été publiée par un chercheur ukrainien après l'invasion de l'Ukraine. La nouvelle version de Conti a ajouté de nouveaux arguments de ligne de commande qui permettent à Conti de redémarrer le système en mode sans échec sous Windows avec le réseau activé, puis de commencer le chiffrement. En démarrant en mode sans échec, Conti peut maximiser le nombre de fichiers chiffrés, car les applications professionnelles telles que les bases de données ne sont vraisemblablement pas en cours d'exécution. Conti a également mis à jour les extensions des fichiers chiffrés pour y inclure des caractères majuscules et minuscules ainsi que des chiffres. Il modifie également le fond d'écran du bureau de la victime après le chiffrement des fichiers.

La figure 8 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de Conti.

Infections par Conti par secteur d'activité

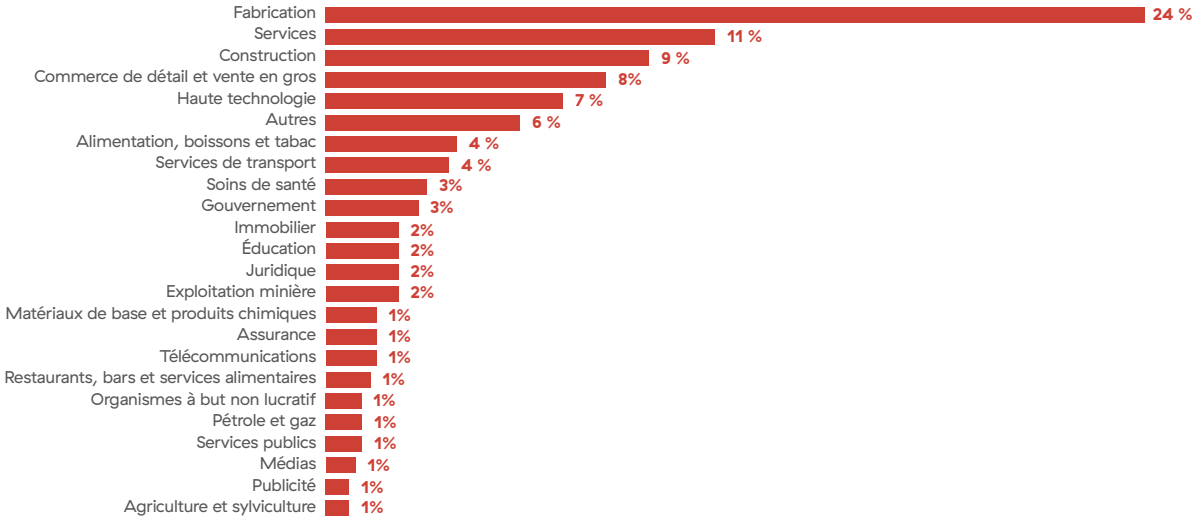


Figure 8 : Infections par Conti par secteur d'activité

Conti a créé son propre site de divulgation de données en août 2020. Si une entreprise ne paie pas la rançon demandée, Conti publiera ses données piratées.

Figure 9 : Site de divulgation de données de Conti

Conti : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Collecte	Exfiltration	Impact
Lien d'hame-çonnage	Interface de ligne de commande	Exécution du démarrage ou de l'ouverture de session automatique	Manipulation des jetons d'accès	Supprimer l'obscurcisse-ment/Décoder des fichiers ou des informations	Découverte de la configura-tion du réseau système	Transfert latéral d'outil	Archivage des données collectées	Exfiltration automatisée	Données chiffrées pour Impact
Pièce jointe d'hameçonnage	Exécution via chargement du module		Exploitation pour l'élévation des privilèges	Altération des défenses	Découverte du système à distance	Services à distance	Données du système local	Exfiltration à travers un service Web	Inhiber la récupération du système
Exploiter l'application destinée au public	Modules partagés			Injection de processus	Découverte de fichiers et de répertoires				Arrêt/ redémarrage du système
Comptes valides	Exécution utilisateur				Découverte de logiciels de sécurité				Défacement
Compromission de la chaîne d'approvision-nement					Interrogation du registre				

LockBit

Le ransomware LockBit est apparu pour la première fois en septembre 2019 sous le nom de ransomware ABCD, nommé d'après son extension « .abcd ». Une nouvelle version est apparue début 2020, qui ajoute l'extension « .lockbit » aux fichiers chiffrés. En 2020, LockBit a rejoint le cartel Maze et a commencé à publier les données des victimes sur le site de divulgation des données de Maze. En septembre 2020, lorsque Maze a mis fin à ses activités, LockBit a lancé son propre site de divulgation des données, comme l'illustre la figure 10.

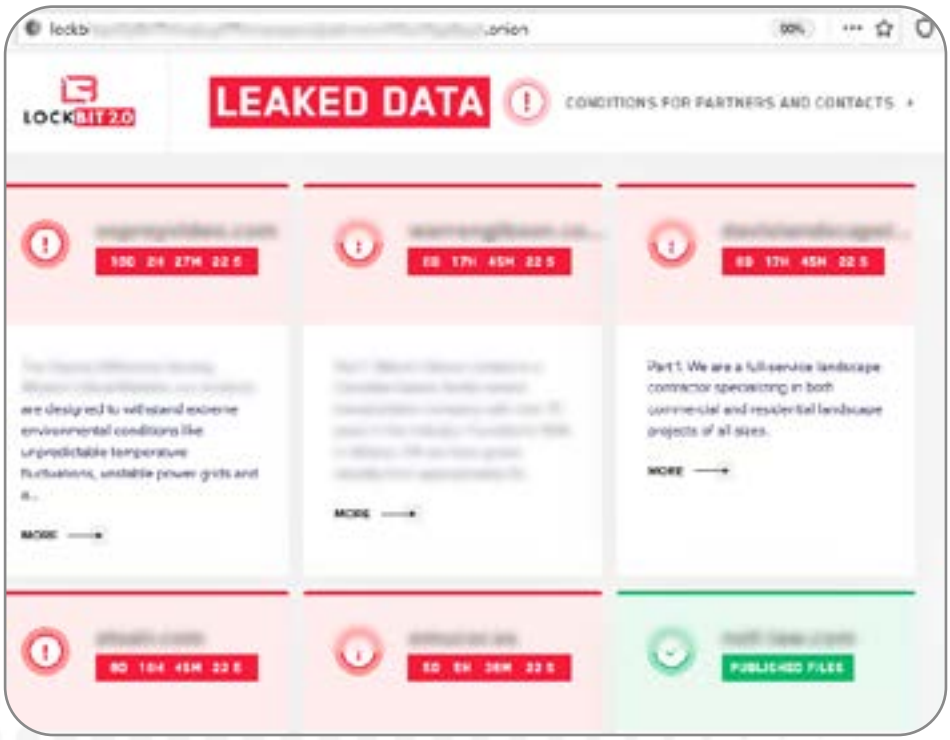


Figure 10 : Site de divulgation de données LockBit

En juin 2021, LockBit a publié une nouvelle version appelée LockBit 2.0. En juillet 2021, LockBit 2.0 a commencé à publier les données des sociétés victimes sur son site de divulgation des données. Il utilise le modèle RaaS. LockBit a démarché des affiliés qui étaient employés par ses entreprises cibles et avaient un accès légitime au réseau. LockBit a été distribué par le biais de campagnes de spam contenant des pièces jointes ou des liens malveillants.

LockBit a également réussi à obtenir un accès en utilisant la force brute pour obtenir des informations d'identification RDP ou VPN, via des comptes RDP compromis, et en exploitant la vulnérabilité CVE-2018-13379 de Fortinet VPN.

Chaîne d'infection :
au cours de la première attaque LockBit 2.0 observée, le hacker a utilisé un compte RDP piraté pour accéder au système ciblé. Il a ensuite utilisé un scanner réseau pour récupérer des informations sur le réseau et localiser les contrôleurs de domaine. L'acteur malveillant a utilisé StealBit pour exfiltrer les données, Process Hacker et PC Hunter pour mettre fin aux processus et services liés à la base de données, ainsi que d'autres outils. Il a utilisé un fichier de commandes pour désinstaller les produits de sécurité et désactiver les journaux d'événements de Windows et les fonctions de Windows Defender. Enfin, LockBit a utilisé les stratégies de groupe de Windows pour distribuer et exécuter le ransomware LockBit 2.0.

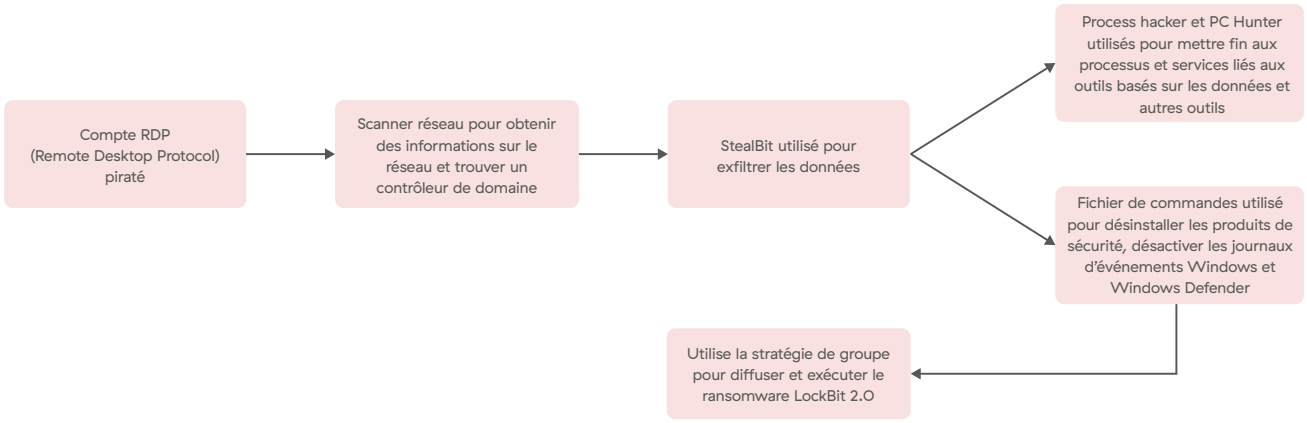


Figure 11 : Anatomie d'une attaque par ransomware LockBit

L'efficacité de LockBit explique en partie sa popularité : LockBit possède la méthode de chiffrement la plus rapide, car il utilise une approche de chiffrement multithread et ne chiffre que 4 Ko de données pour chaque fichier. Il utilise une combinaison d'algorithmes RSA et AES pour chiffrer les fichiers. LockBit a publié une variante Linux et VMware ESXi en octobre 2021. Celle-ci utilise une combinaison d'algorithmes AES (Advanced Encryption Standard) et ECC (Elliptic-Curve Cryptography) pour chiffrer les données.

La figure 12 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de LockBit.

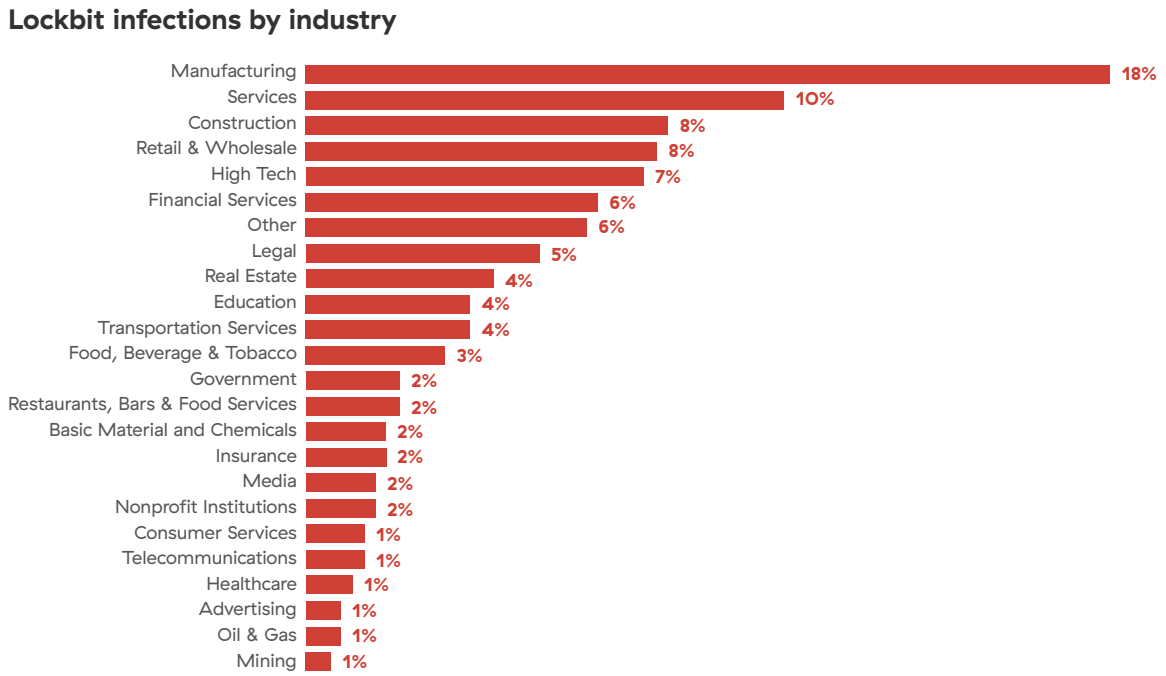


Figure 12 : Infections par LockBit par secteur d'activité

LockBit : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Collecte	Exfiltration	Impact
Lien d'hameçonnage	Interface de ligne de commande	Exécution du démarrage ou de l'ouverture de session automatique	Abus du mécanisme de contrôle d'élévation : contournement du contrôle du compte utilisateur	Supprimer l'obscurcisse-ment/Décoder des fichiers ou des informations	Découverte de la configura-tion du réseau système	Transfert latéral d'outil	Archivage des données collectées	Exfiltration à travers un service Web	Données chiffrées pour Impact
Pièce jointe d'hameçonnage				Altération des défenses : désactiver ou modifier des outils	Découverte du système à distance	Services à distance	Données du système local		Inhiber la récupération du système
Comptes valides				Suppression des indicateurs sur l'hôte : effacer les journaux d'événements de Windows	Découverte de fichiers et de répertoires				Défacement
Exploiter l'application destinée au public				Modification de la politique de domaine : modification de la politique de groupe	Découverte de logiciels de sécurité				
Compromission de la chaîne d'approvision-nement									

PYSA/Mespinoza

Le ransomware PYSA, également connu sous le nom de Mespinoza, a été repéré pour la première fois en octobre 2019. Il s'attaque à un large éventail de secteurs dans le monde, mais est connu en particulier pour ses attaques sur des « cibles faciles » telles que l'éducation et les hôpitaux.

Chaîne d'infection

PYSA parvient à une compromission initiale par le biais d'e-mails de spam ou d'informations d'identification RDP compromises. Ensuite, les acteurs malveillants collectent des informations sur le réseau grâce à des outils d'analyse tels que Port Scanner et Advanced IP Scanner, développés par Famatech Corp. Les hackers utilisent des outils de post-exploitation comme Mimikatz, PowerShell Empire, Koadic et PsExec pour dérober des informations d'identification et se déplacer latéralement. L'outil WinSCP a été utilisé pour exfiltrer les données des systèmes des victimes. Un script PowerShell désactive les logiciels de sécurité, puis supprime les clichés instantanés (« shadow copy ») et les points de restauration du système, empêchant ainsi les victimes de restaurer leurs données. Enfin, le hacker déploie et exécute le ransomware PYSA et chiffre les données de la victime.

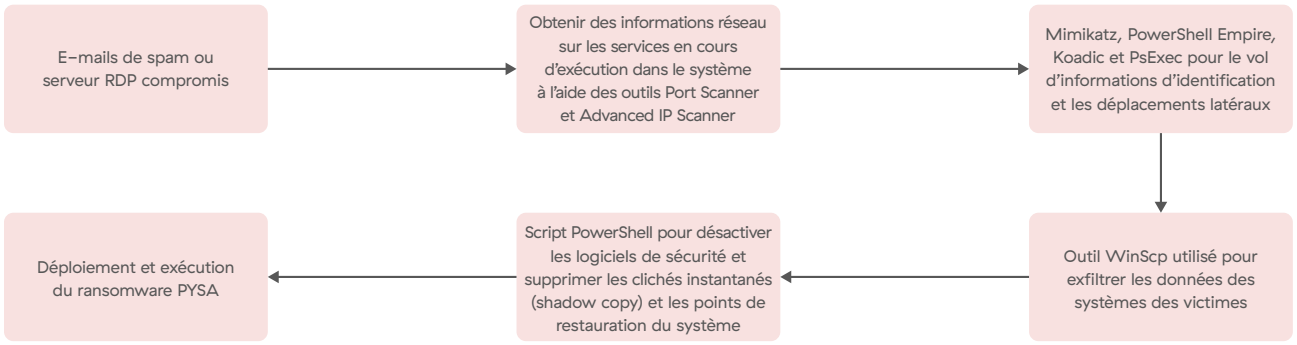


Figure 13 : Anatomie d'une attaque par ransomware PYSA

18 % des attaques par PYSA visaient des établissements d'enseignement.

PYSA utilise une combinaison d'algorithmes RSA et AES-CBC pour chiffrer les fichiers.

La figure 14 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de PYSA/Mespinoza.

Infections par PYSA/Mespinoza par secteur d'activité

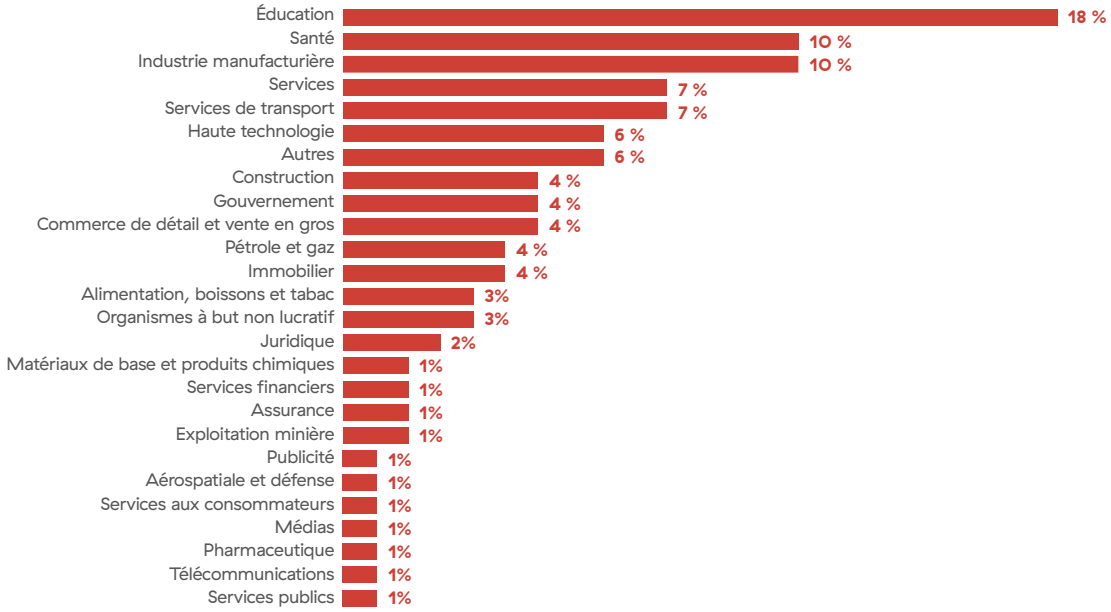


Figure 14 : Attaques PYSA/Mespinoza par secteur

PYSA publie les données volées sur son site de divulgation (voir figure 15) si la victime ne paie pas de rançon.

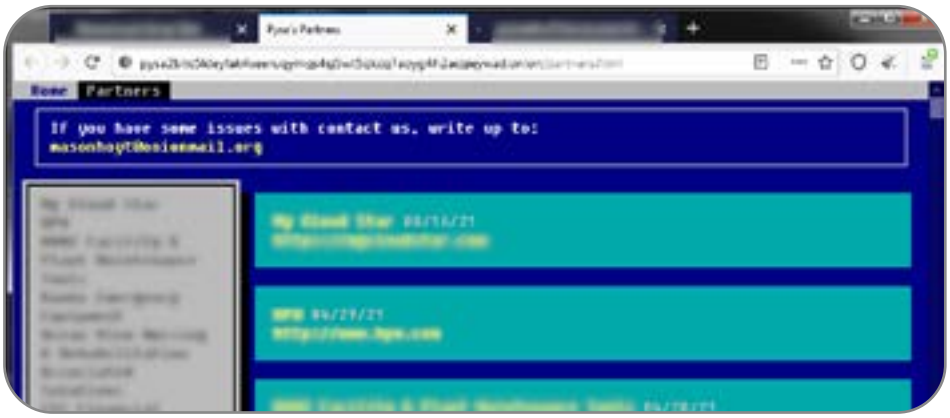


Figure 15 : Site de divulgation de données PYSA/Mespinoza

PYSA/Mespinoza : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Collecte	Exfiltration	Impact
Lien d'hame-çonnage	Interface de ligne de commande	Exécution du démarrage ou de l'ouverture de session automatique	Manipulation des jetons d'accès	Supprimer l'obs-curcissement/ Décoder des fichiers ou des informations	Découverte de la configura-tion du réseau système	Transfert latéral d'outil	Archivage des données collectées	Exfiltration à travers un protocole alternatif	Données chiffrées pour impact
Pièce jointe d'hameçonnage	Exécution via chargement du module	Tâche/travail programmé(e)		Altération des défenses	Découverte du système à distance		Données du système local	Exfiltration à travers un service Web	Inhiber la récupération du système
Comptes valides	Exécution utilisateur			Modification de la politique de domaine : modification de la politique de groupe	Découverte de fichiers et de répertoires				
					Découverte de logiciels de sécurité				
					Interrogation du registre				

REvil/Sodinokibi

Le ransomware REvil (alias Sodinokibi) a été repéré pour la première fois en avril 2019 et a été l'un des groupes malveillants les plus actifs au cours des dernières années. REvil utilise également un écosystème RaaS. REvil a commencé la double extorsion en janvier 2020, en publiant d'abord des données sur un forum de piratage. En février 2020, les hackers de Sodinokibi ont lancé leur propre site de divulgation des données, comme l'illustre la figure 16.

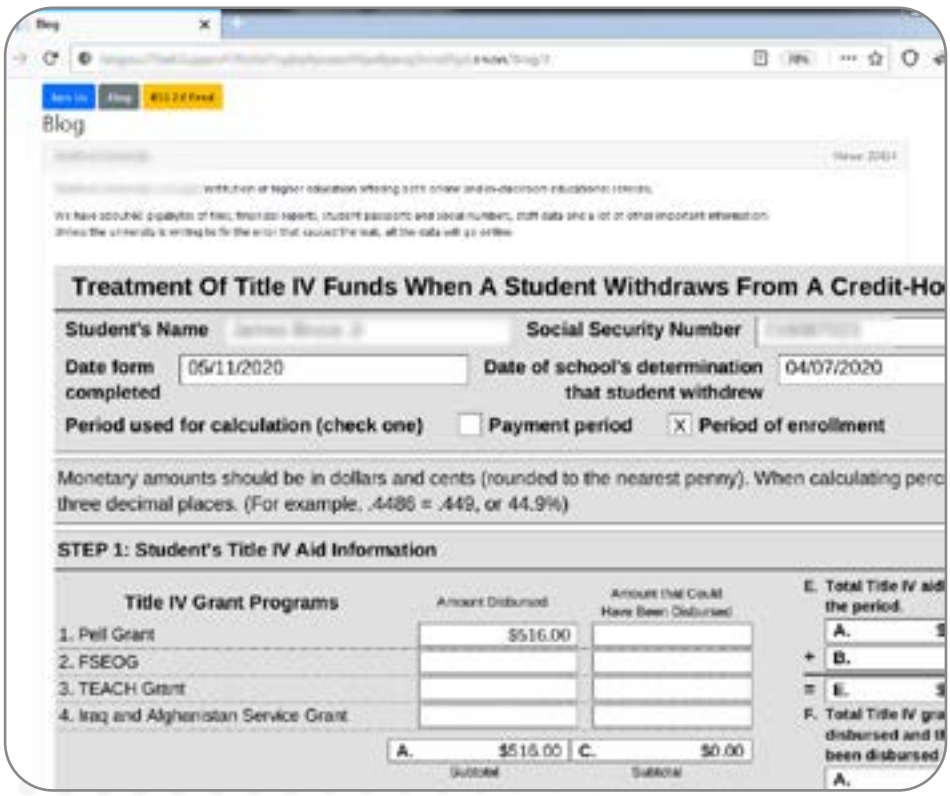


Figure 16 : Site de divulgation de données REvil/Sodinokibi

Ils ont également expérimenté la vente aux enchères de données volées sur leur site de divulgation, mais sans succès.

Le groupe malveillant REvil a exploité une vulnérabilité de type Zero-Day dans le serveur VSA de Kaseya en juillet 2021. Le serveur VSA de Kaseya compromis a été utilisé pour envoyer un script malveillant à tous les clients gérés par ce serveur VSA.

Comme mentionné précédemment, les membres de REvil ont apparemment été arrêtés par les forces de l'ordre russes en janvier 2022. Cependant, le ransomware a été mis à jour et l'infrastructure a été remise en ligne en avril 2022, date à laquelle les attaques de REvil ont repris.

Chaîne d'infection

Les affiliés de REvil ont utilisé divers mécanismes d'accès initial, notamment des e-mails de spam, des kits d'exploitation, des comptes RDP compromis et des exploits de vulnérabilité. Une campagne type commence par un e-mail de spam contenant une pièce jointe malveillante. Une fois ouverte, la pièce jointe malveillante télécharge un cheval de Troie tel que IcedID, qui sert de point de pivot pour un déplacement latéral. Comme le montre la figure 17, les affiliés de REvil utilisent une variété d'outils différents comme Cobalt Strike, SharpSploit, Mimikatz et d'autres outils de post-exploitation pour dérober des informations d'identification. En outre, les affiliés collectent des informations sur le réseau à l'aide de Netscan, BloodHound, AdFind et d'autres outils de découverte du réseau. Les attaquants se déplacent latéralement en utilisant l'accès PsExec ou RDP. L'exfiltration de données est réalisée à l'aide de FileZilla, Rclone, MEGAsync ou FreeFileSync. Avant de déployer le ransomware, les affiliés de REvil utilisent PC Hunter, Process Hacker, KillAV, et/ou d'autres scripts pour mettre fin aux processus et services liés aux logiciels de sécurité. Enfin, l'acteur malveillant déploie le ransomware REvil et chiffre les données.

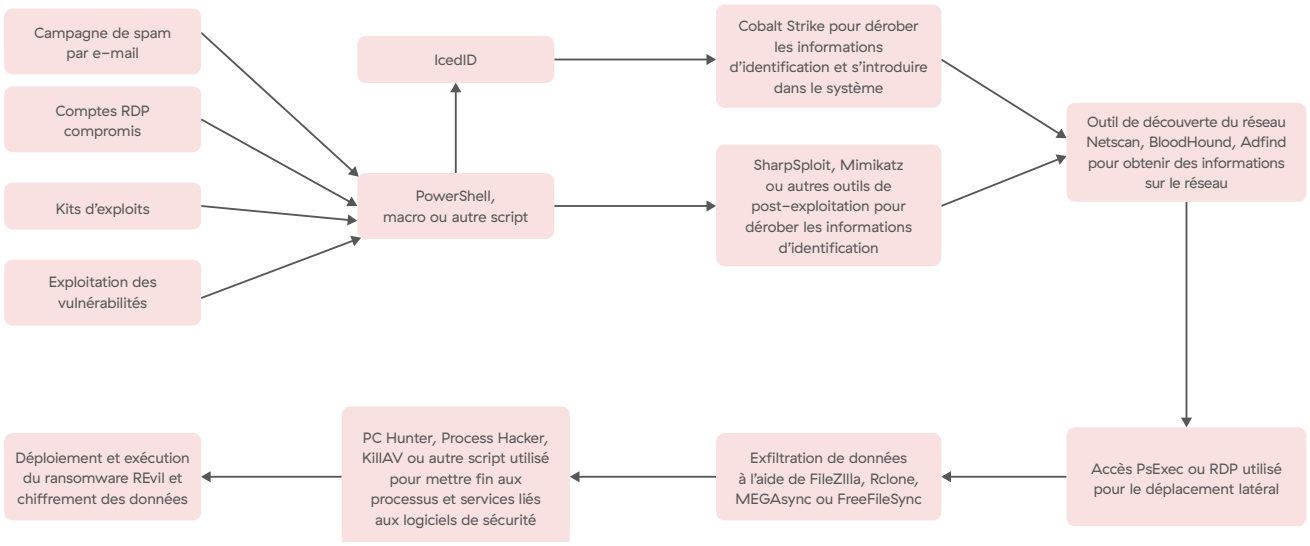


Figure 17 : Chaîne d'attaque REvil/Sodinokibi

REvil exploite la cryptographie asymétrique sur les courbes elliptiques (ou ECC, Elliptic-Curve Cryptography), en utilisant Curve25519 en combinaison avec Salsa20, pour chiffrer les fichiers.

La figure 18 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de REvil.

REvil/Sodinokibi infections by industry

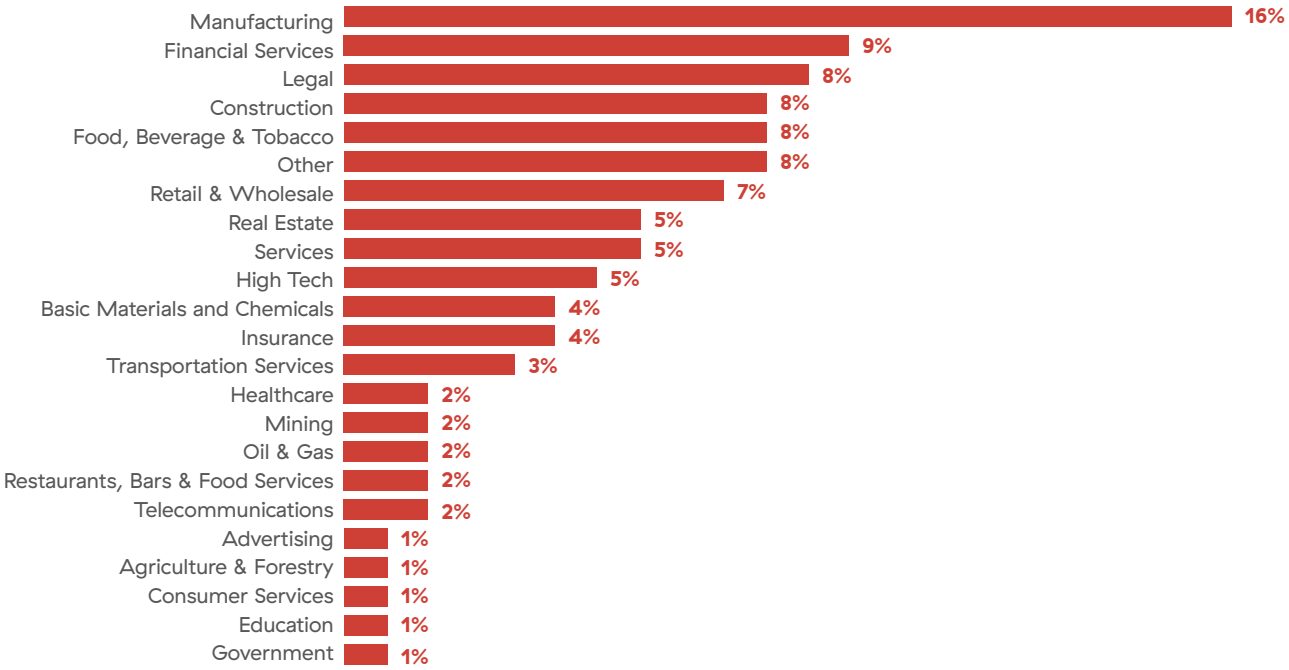


Figure 18 : Infections par REvil/Sodinokibi par secteur d'activité

REvil/Sodinokibi : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Collecte	Exfiltration	Impact
Lien d'hameçonnage	Interface de ligne de commande	Exécution du démarrage ou de l'ouverture de session automatique	Manipulation des jetons d'accès	Supprimer l'obscurcisse-ment/Décoder des fichiers ou des informations	Découverte de la configura-tion du réseau système	Transfert latéral d'outil	Archivage des données collectées	Exfiltration automatisée	Données chiffrées pour impact
Pièce jointe d'hameçonnage	Exécution via chargement du module	Détourner le flux d'exécution	Détourner le flux d'exécution	Altération des défenses	Découverte du système à distance	Services à distance	Données du système local	Exfiltration à travers un service Web	Inhiber la récupération du système
Exploiter l'application destinée au public	Modules partagés		Exploitation pour l'élévation des privilèges		Découverte de fichiers et de répertoires				Arrêt/ redémarrage du système
Compromis furtif	Exécution utilisateur				Découverte de logiciels de sécurité				Défacement
Comptes valides					Interrogation du registre				
Compromission de la chaîne d'approvision-nement									

Avaddon

Le ransomware Avaddon a été repéré pour la première fois en juin 2020 et a été très actif à cette époque. Avaddon était encore une famille de ransomwares qui utilisait l'écosystème RaaS. En janvier 2021, Avaddon a ajouté le DDoS à ses opérations comme tactique de triple extorsion. Avaddon menait des attaques DDoS soit sur le site Web soit sur le réseau de la victime pour encourager cette dernière à négocier avec ses opérateurs et exiger des montants de rançon plus élevés.

Chaîne d'infection
Avaddon obtenait l'accès par le biais de différents affiliés qui ont utilisé une variété de vecteurs pour la compromission initiale. Avaddon a été le ransomware le plus largement diffusé dans des campagnes de spam et des kits d'exploitation, mais certains affiliés ont utilisé des attaques par force brute ou des identifiants RDP et VPN compromis pour accéder aux réseaux.

Dans une chaîne d'attaque type, Avaddon accédait à un courtier initialement infecté par le biais d'informations d'identification compromises et utilisait des logiciels malveillants personnalisés, tels que les shells Web BlackCrow et DarkRaven, pour s'infiltrer dans le système ciblé. Avaddon utilisait SystemBC pour accéder aux hôtes compromis, puis Mimikatz et SharpDump pour dérober les informations d'identification. L'acteur malveillant effectuait une analyse du réseau après l'exploitation à l'aide de SoftPerfect Network Scanner, PowerSploit et Empire. Pour les déplacements latéraux, les affiliés d'Avaddon utilisaient RDP et Windows Scheduled Tasks pour la persistance. Avant de déposer le principal payload du ransomware, les acteurs malveillants exfiltraient des données à l'aide de MEGAsync et mettaient fin aux processus et services liés aux logiciels de sécurité. Enfin, les pirates déposaient et exécutaient le payload Avaddon et chiffrent les systèmes ciblés.

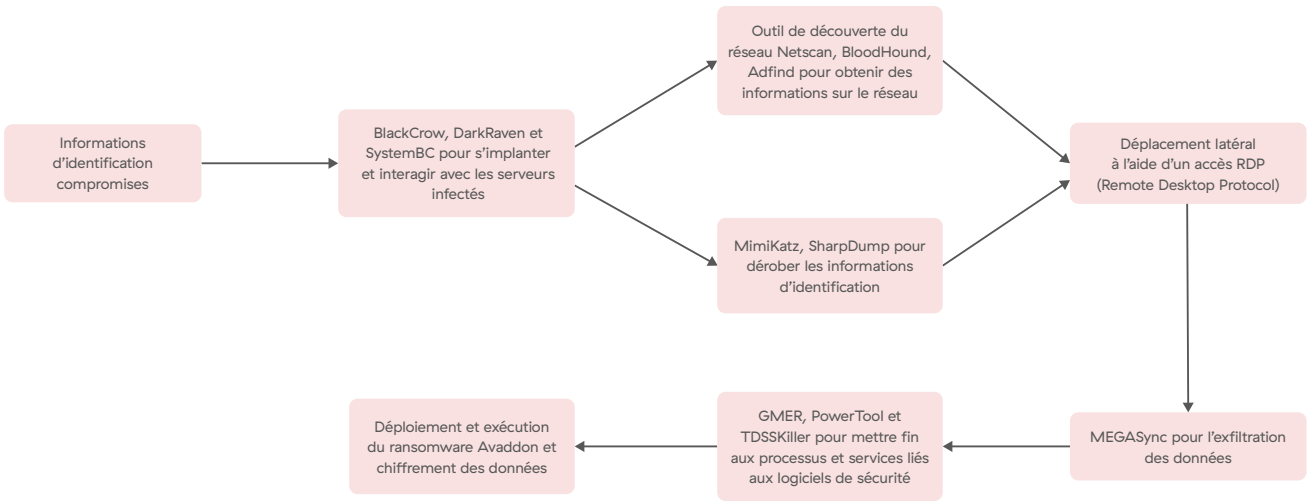


Figure 19. Anatomie d'une attaque par ransomware Avaddon

Avaddon utilisait une combinaison d'algorithmes RSA et AES pour chiffrer les fichiers. En février, un chercheur a publié un décrypteur gratuit après avoir découvert une faille, qu'Avaddon a ensuite corrigée. En juin 2021, Avaddon a mis fin à ses activités et a publié les clés de déchiffrement des victimes, permettant à Emsisoft de créer un décrypteur pour le ransomware Avaddon.

À l'instar des autres familles de ransomwares évoquées précédemment, Avaddon a suivi cette tendance consistant à créer des sites Web d'exposition de données, lançant le sien en août 2020, comme indiqué dans la figure 20.

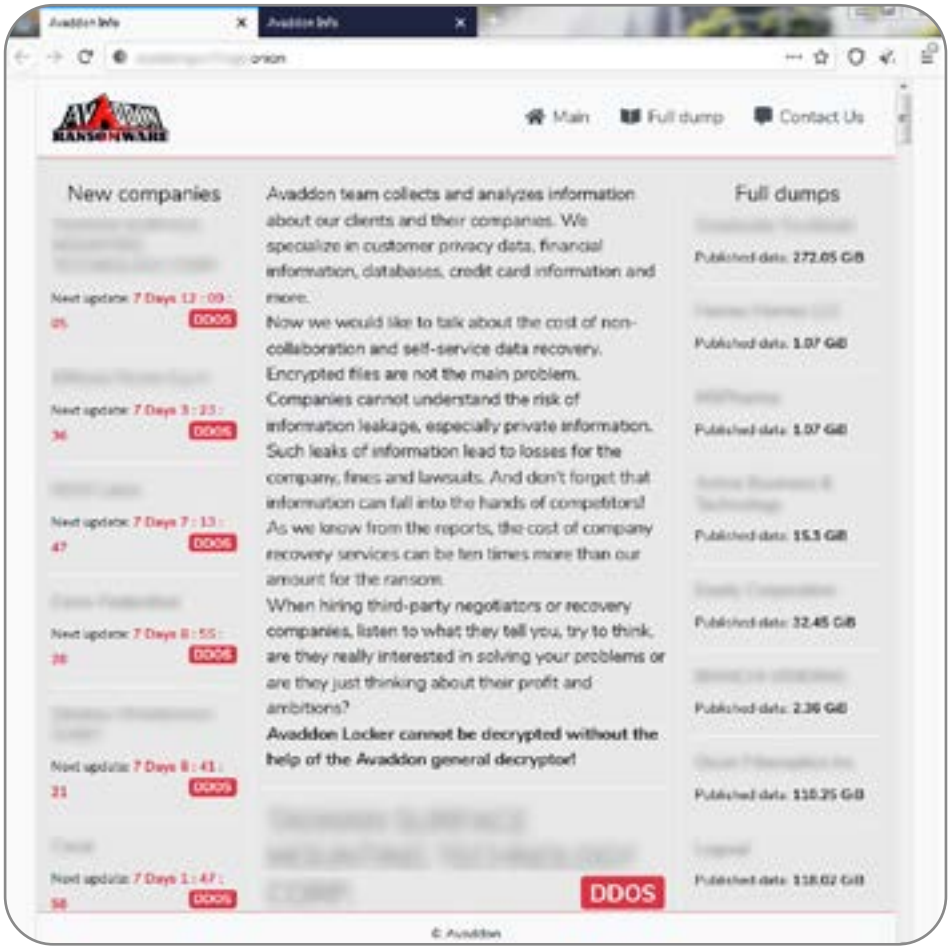


Figure 20 : Site de divulgation de données Avaddon

Après la fermeture d'Avaddon en juin 2021, le groupe malveillant a relancé ses attaques en utilisant le constructeur du ransomware Thanos. Le groupe malveillant a rebaptisé Avaddon avec Haron et, en octobre 2021, a rebaptisé à nouveau le ransomware sous le nom de Midas.

La figure 18 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide d'Avaddon.

Infections par Avaddon par secteur d'activité

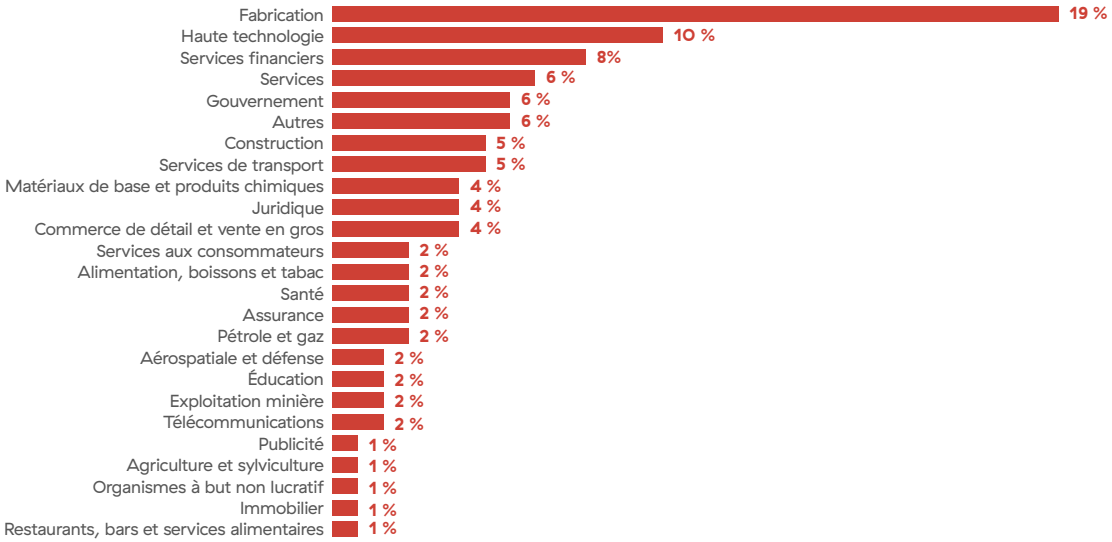


Figure 21 : Infections par Avaddon par secteur d'activité

Avaddon : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Collecte	Exfiltration	Impact
Lien d'hameçonnage	Interface de ligne de commande	Exécution du démarrage ou de l'ouverture de session automatique	Comptes valides	Supprimer l'obscur-cissement/ Décoder des fichiers ou des informations	Découverte de la configura-tion du réseau système	Transfert latéral d'outil	Archivage des données collectées	Exfiltration à travers un protocole alternatif	Données chiffrées pour impact
Pièce jointe d'hameçonnage	Tâche/travail programmé(e)	Comptes valides		Altération des défenses	Découverte du système à distance	Services à distance : protocole de bureau à distance	Données du système local		Inhiber la récupération du système
Exploiter l'application destinée au public	Exécution utilisateur			Injection de processus	Découverte de fichiers et de répertoires				
Compromis furtif				Suppression de l'indicateur sur l'hôte	Découverte de logiciels de sécurité				
Comptes valides				Suppression de l'indicateur sur l'hôte	Découverte de logiciels de sécurité				

Clop

Le ransomware Clop a été repéré pour la première fois en février 2019. En mars 2020, Clop a commencé à utiliser la double extorsion, en diffusant les données volées des entreprises compromises qui n'ont pas payé de rançon sur leurs sites de divulgation de données, comme le montre la figure 22.

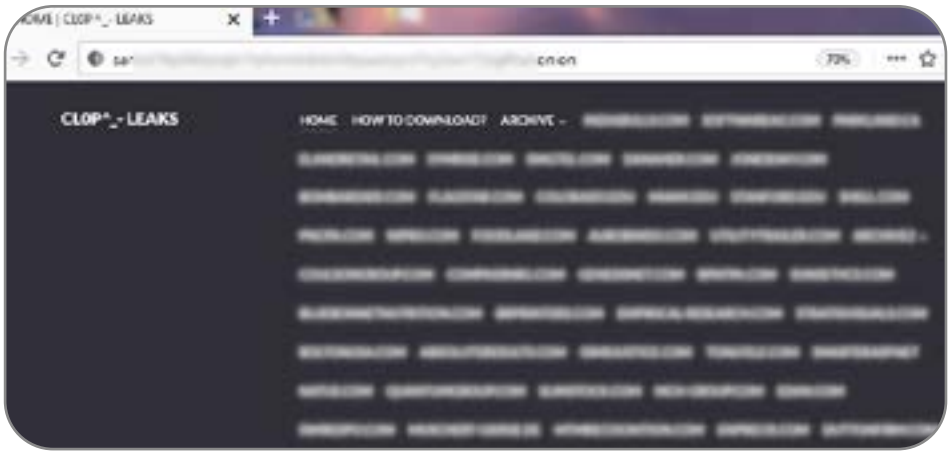


Figure 22 : Site de divulgation de données Avaddon

Le groupe Clop concentre principalement ses actions sur les grandes entreprises. ThreatLabz a observé que le groupe de ransomwares Clop demandait des rançons à huit chiffres et refusait même des offres de paiement de rançon de plusieurs millions de dollars.

Le ransomware Clop a été initialement déployé par les groupes malveillants TA505 et FIN11. Clop a été largement diffusé dans des campagnes de spam menées par l'acteur malveillant TA505. ThreatLabz a observé plusieurs attaques Clop exploitant la vulnérabilité SolarWinds Serv-U CVE-2021-35211, qui permet l'exécution de code à distance avec des privilèges élevés, pour l'accès initial. Le groupe malveillant FIN11 a exploité plusieurs vulnérabilités dans l'appliance de transfert de fichiers (FTA) d'Accellion, répertoriées sous les noms de CVE-2021-27101, CVE-2021-27102, CVE-2021-27103 et CVE-2021-27104. FIN11 dépose ensuite le shell Web DEWMODE, qui exfiltre les données avant de déposer et d'exécuter le ransomware Clop.

Clop a mené des attaques de haut niveau, qui ont causé un préjudice estimé à 500 millions de dollars en novembre 2021 .

Chaîne d'infection

Un exemple d'attaque par TA505 a permis de compromettre le système par le biais d'un spam contenant une pièce jointe HTML. La pièce jointe redirigeait l'utilisateur vers un fichier XLS qui déposait ensuite le chargeur Get2. Le chargeur téléchargeait d'autres payloads comme SdBot, FlawedAmmy, FlawedGrace et Cobalt Strike. Après avoir pris pied sur le réseau et volé et exfiltré des données, le groupe malveillant a déployé et exécuté le ransomware Clop, comme le montre la figure 23.

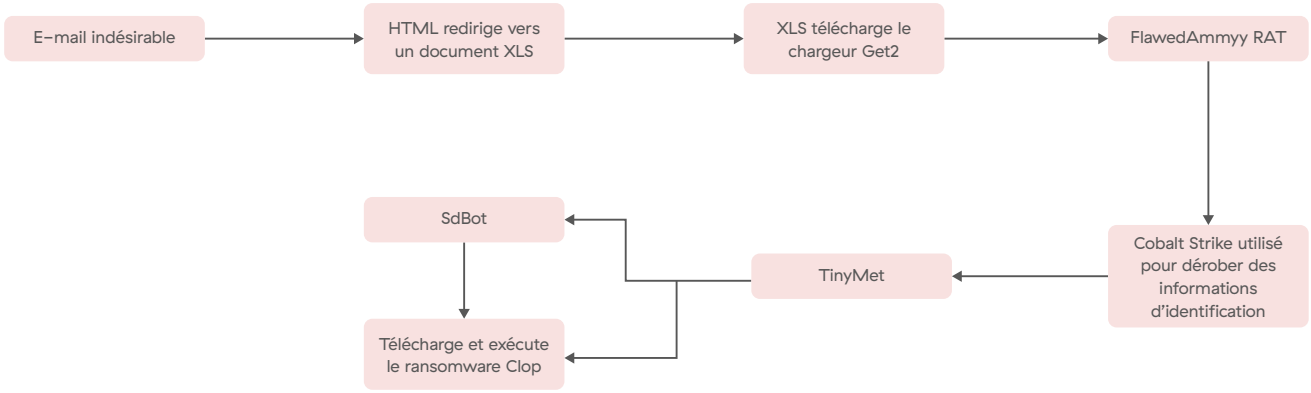


Figure 23 : Anatomie d'une attaque par ransomware Clop

Clop utilise une combinaison d'algorithmes AES et RSA pour chiffrer les fichiers.

La figure 24 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de Clop.

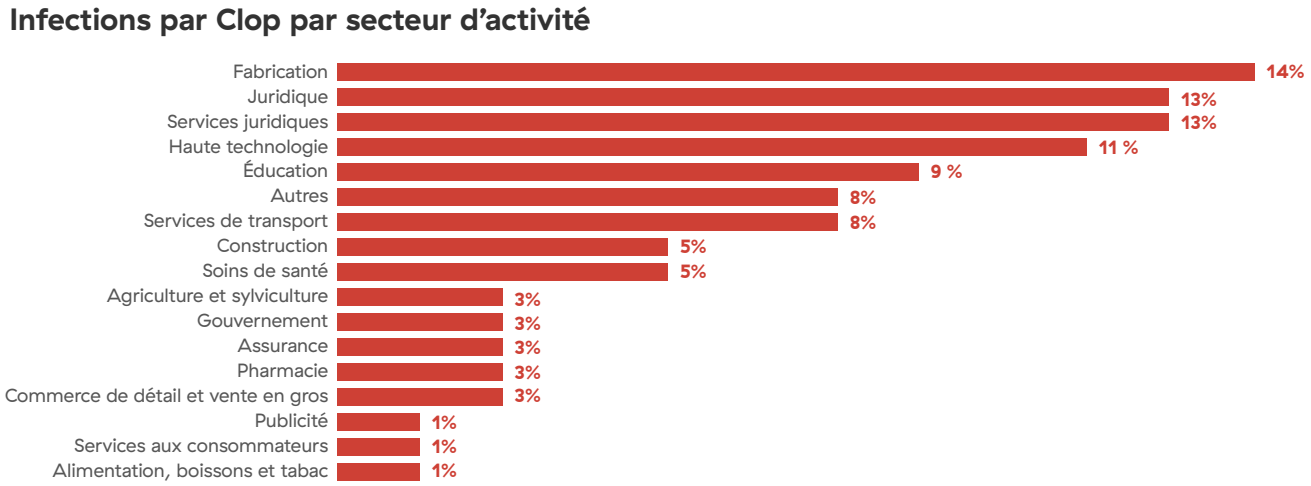


Figure 24 : Infections par Clop par secteur d'activité

Clop : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Exfiltration	Impact
Comptes valides	Interface de ligne de commande	Exécution de démarrage ou de connexion automatique	Manipulation des jetons d'accès	Usurpation d'identité : signature de code non valide	Découverte de la configuration du réseau système	Transfert latéral d'outil	Exfiltration automatisée	Données chiffrées pour impact
Pièce jointe d'hameçonnage	Exécution utilisateur	Créer ou modifier un processus système : service Windows	Contourner le contrôle de compte d'utilisateur	Altération des défenses : désactivation ou modification des outils	Découverte du système à distance	Services à distance	Exfiltration à travers un service Web	Inhiber la récupération du système
Exploiter l'application destinée au public	API Native		Exploitation pour l'élévation des privilèges	Supprimer l'obs-curcissement/ Décoder des fichiers ou des informations	Découverte de fichiers et de répertoires			
Compromission de la chaîne d'approvision-nement				Injection de processus : injection DDL	Interrogation du registre			
				Exécution de commande indirecte	Découverte de logiciels de sécurité			

Grief

Le ransomware Grief est une nouvelle appellation de DoppelPaymer, dont l'activité a considérablement diminué en mai 2021 à la suite de l'attaque de Colonial Pipeline. Le ransomware Grief présente de nombreuses similitudes avec DoppelPaymer, notamment un code de ransomware et des sites Web de divulgation de données partagés. La figure 25 présente un exemple de capture d'écran du site de divulgation de Grief.

Figure 25 : Site de divulgation de données Grief

Le portail de demande de rançon de Grief présente quelques différences avec celui de DoppelPaymer. En particulier, le mode de paiement de la demande de rançon est effectué en Monero au lieu de Bitcoin. Ce changement de cryptomonnaie peut être une réaction à la saisie par le FBI d'une partie du paiement de la rançon de Colonial Pipeline, qui avait été effectuée en bitcoins.

Chaîne d'infection

Le ransomware Grief a été déployé sur des systèmes précédemment infectés par Dridex, dont se sert le hacker avant d'utiliser Cobalt Strike et de déployer et exécuter le payload du ransomware Grief. Grief utilise une combinaison d'algorithmes RSA 2048 bits et AES 256 bits pour chiffrer les fichiers.

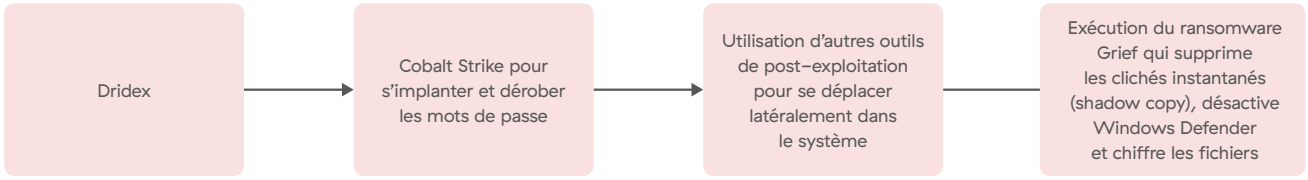


Figure 26 : Anatomie d'une attaque par ransomware Grief

La figure 27 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de Grief.

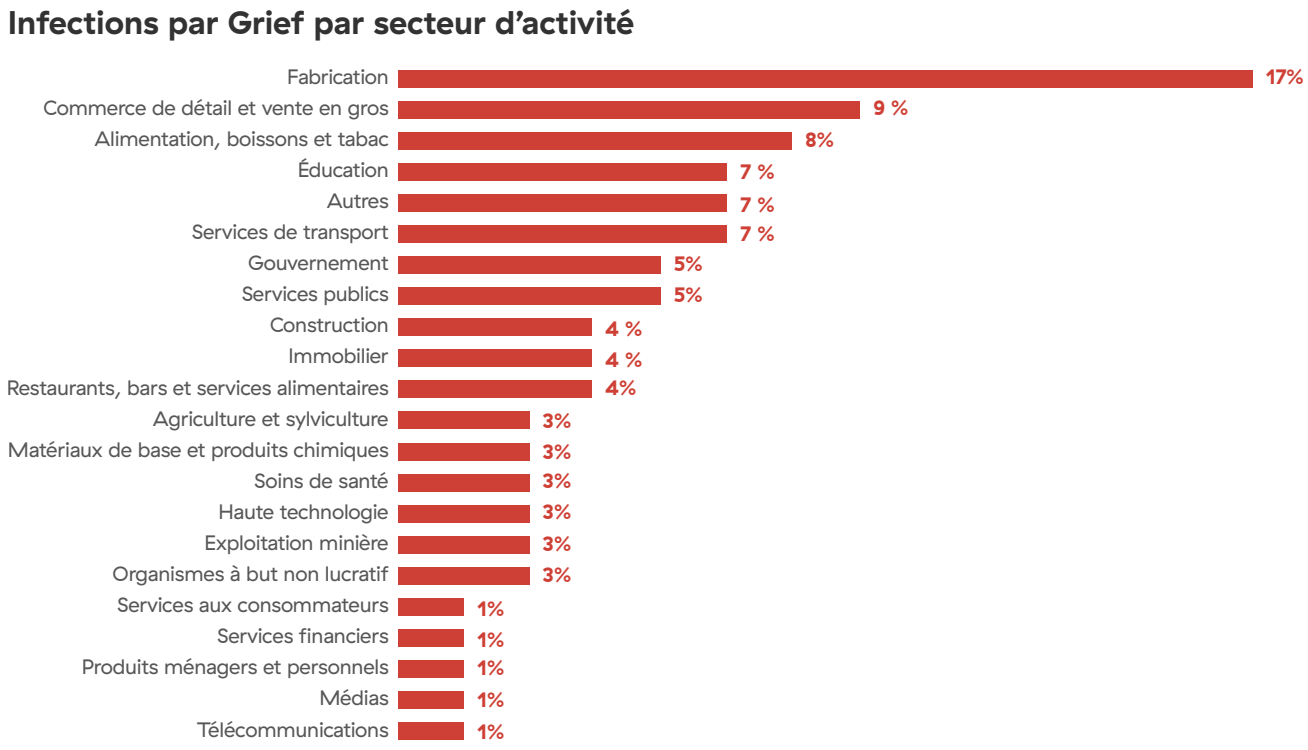


Figure 27 : Infections par Grief par secteur d'activité

Grief : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Exfiltration	Impact
Comptes valides	Interface de ligne de commande	Exécution du démarrage ou de l'ouverture de session automatique : clés d'exécution du registre/ dossier de démarrage	Injection de processus	Détournement du flux d'exécution : détournement de l'ordre de recherche DLL	Découverte de la configuration du réseau système	Transfert latéral d'outil	Transfert programmé	Données chiffrées pour impact
Pièce jointe d'hameçonnage	Exécution utilisateur	Tâche/travail programmé(e)		Supprimer l'obs-curcissement/ Décoder des fichiers ou des informations	Découverte du système à distance			Inhiber la récupération du système
	Modules partagés			Altération des défenses : désactivation ou modification des outils	Découverte de fichiers et de répertoires			Arrêt/ redémarrage du système
				Usurpation d'identité : correspond à un nom ou à un emplace-ment légitime	Découverte de logiciels de sécurité			

Hive

Le ransomware Hive a été repéré pour la première fois en juin 2021 et utilise un modèle RaaS. Il utilise plusieurs mécanismes afin d'obtenir un accès initial, notamment des e-mails de spam malveillants, des informations d'identification VPN divulguées et des exploits de vulnérabilité dans les ressources externes. L'infection initiale commence par l'exploitation des vulnérabilités ProxyShell présentes dans Microsoft Exchange Server. Les vulnérabilités ProxyShell sont une combinaison des vulnérabilités CVE-2021-34473 (vulnérabilité d'exécution de code à distance de Microsoft Exchange Server), CVE-2021-34523 (vulnérabilité d'élévation des privilèges de Microsoft Exchange Server) et CVE-2021-31207 (vulnérabilité de contournement des fonctions de sécurité de Microsoft Exchange Server).

Chaîne d'infection

Le hacker crée un brouillon d'e-mail dans une boîte aux lettres, accompagné d'une pièce jointe contenant le shell Web codé. Il exporte ensuite l'ensemble de la boîte aux lettres (brouillon d'e-mail malveillant inclus) au format de fichier PST avec une extension ASPX. Ceci permet aux hackers de déposer des shells Web sur des serveurs vulnérables. Le shell Web télécharge le script PowerShell qui contient le payload codé de Cobalt Strike. Il télécharge ensuite d'autres stagers et s'implante dans le système de la victime. Il utilise ensuite Mimikatz pour dérober les hachages NTLM et exploite une tactique pass-the-hash (PtH) pour accéder au compte de contrôle du domaine. Hive effectue d'autres déplacements latéraux via RDP en utilisant les informations d'identification volées. Il scanne le réseau avec le scanner SoftPerfect Network et obtient des informations supplémentaires. Enfin, il déploie et exécute le ransomware Hive et chiffre les données.

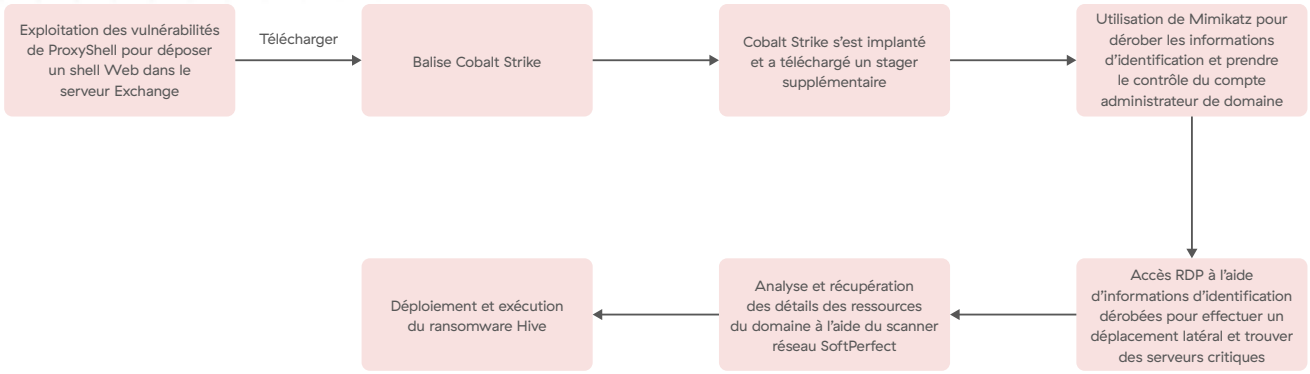


Figure 28 : Chaîne d'attaque Hive

Les versions antérieures du payload du ransomware Hive étaient écrites en langage de programmation Go et utilisaient une combinaison d'algorithmes RSA et AES pour chiffrer les fichiers. Des versions plus récentes de Hive sont écrites en langage de programmation Rust et utilisent Curve25519 et ChaCha20 pour le chiffrement des fichiers.

Les affiliés de Hive exfiltrent également les données des victimes avant de chiffrer les fichiers. Une capture d'écran du site de divulgation des données de Hive est présentée à la figure 29.

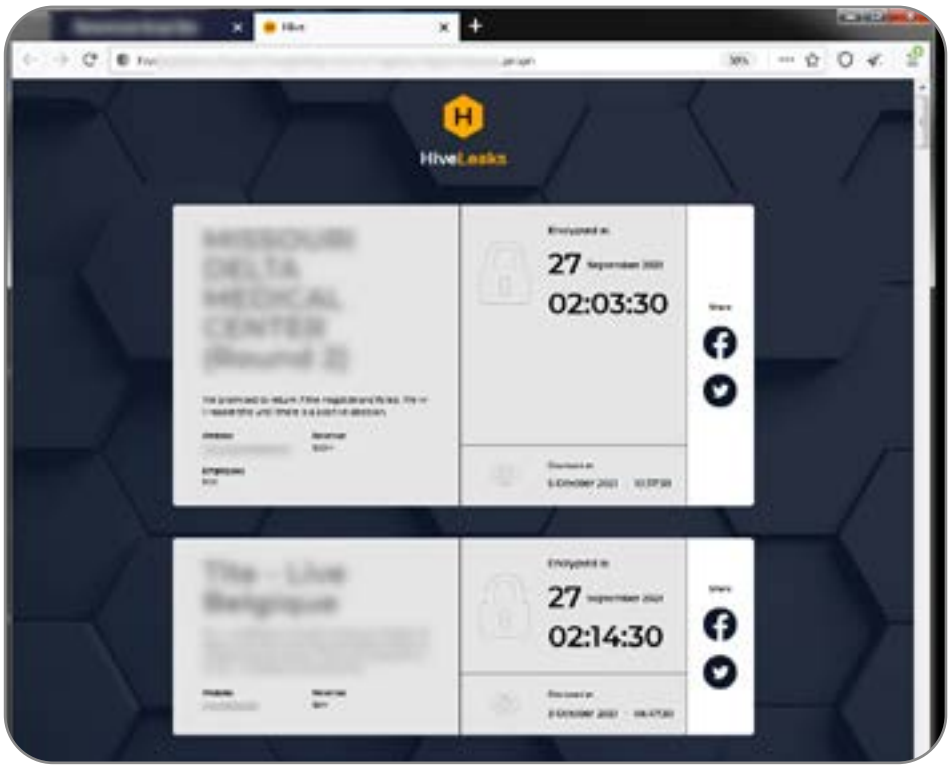


Figure 29 : Site de divulgation de données Hive

La figure 30 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de Hive.

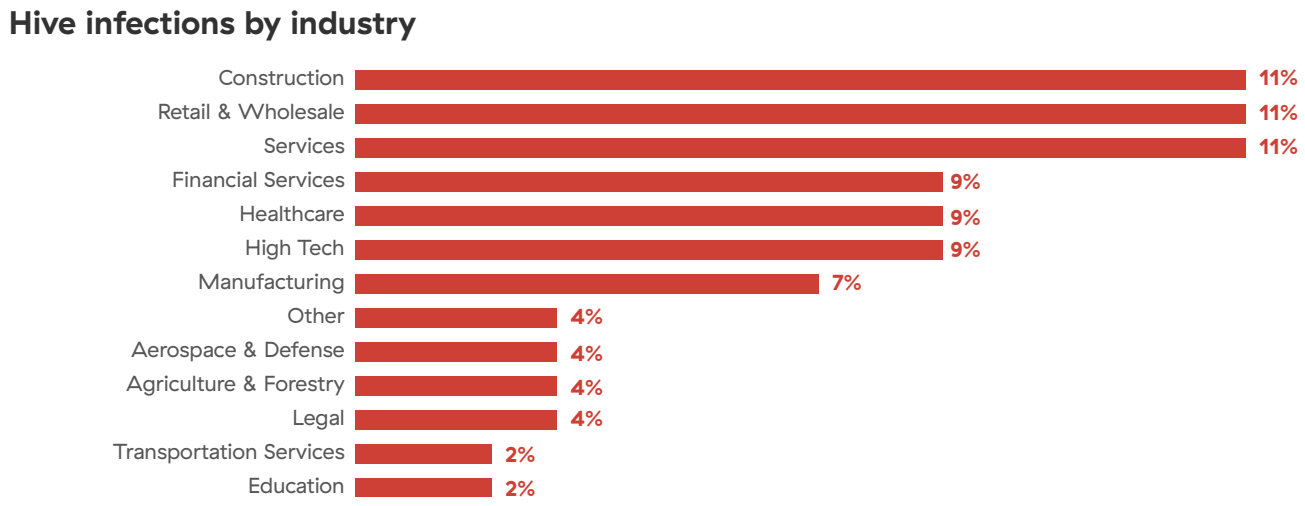


Figure 30 : Infections par Hive par secteur d'activité

Hive : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Exfiltration	Impact
Services externes à distance	Interface de ligne de commande	Comptes valides : comptes de domaine	Comptes valides	Effacer les journaux d'événements Windows	Découverte de la configuration du réseau système	Remote Desktop Protocol	Transfert programmé	Données chiffrées pour impact
Pièce jointe d'hameçonnage	Exécution utilisateur	Créer un compte : compte de domaine	Comptes de domaine	Altération des défenses : désactivation ou modification des outils	Découverte du système à distance	Services à distance		Inhiber la récupération du système
Exploiter l'application destinée au public			Exploitation pour l'élévation des privilèges	Supprimer l'obs–curcissement/ Décoder des fichiers ou des informations	Découverte de fichiers et de répertoires			
					Interrogation du registre			
					Découverte de logiciels de sécurité			

BlackByte

BlackByte est un autre groupe RaaS qui a fait une apparition remarquée en juillet 2021. Il a été initialement écrit en C#, puis redéveloppé en langage de programmation Go aux alentours de septembre 2021. La version basée sur Go présente de nombreuses similitudes avec la version C#, notamment les commandes exécutées pour effectuer la propagation latérale, l'élévation des privilèges et le chiffrement de fichiers.

Les campagnes BlackByte commencent par exploiter les vulnérabilités ProxyShell présentes dans Microsoft Exchange Server.

Chaîne d'infection
Le hacker crée un brouillon d'e-mail dans une boîte aux lettres. L'e-mail comporte une pièce jointe qui contient le shell Web codé. Le hacker exporte ensuite l'ensemble de la boîte aux lettres (brouillon d'e-mail malveillant inclus) au format de fichier PST avec une extension ASPX. Ceci permet aux hackers de déposer des shells Web sur des serveurs vulnérables.

Le shell Web est ensuite utilisé pour déposer une balise Cobalt Strike sur le serveur Exchange ciblé. Cobalt Strike et d'autres outils de post-exploitation sont utilisés pour dérober les informations d'identification et accéder aux comptes de service afin de s'infiltrer dans le système. Par ailleurs, BlackByte installe l'outil RDP AnyDesk. AnyDesk est utilisé pour les déplacements latéraux et pour déposer Cobalt Strike dans le contrôleur de domaine infecté. Enfin, Cobalt Strike déploie et exécute le ransomware de BlackByte.

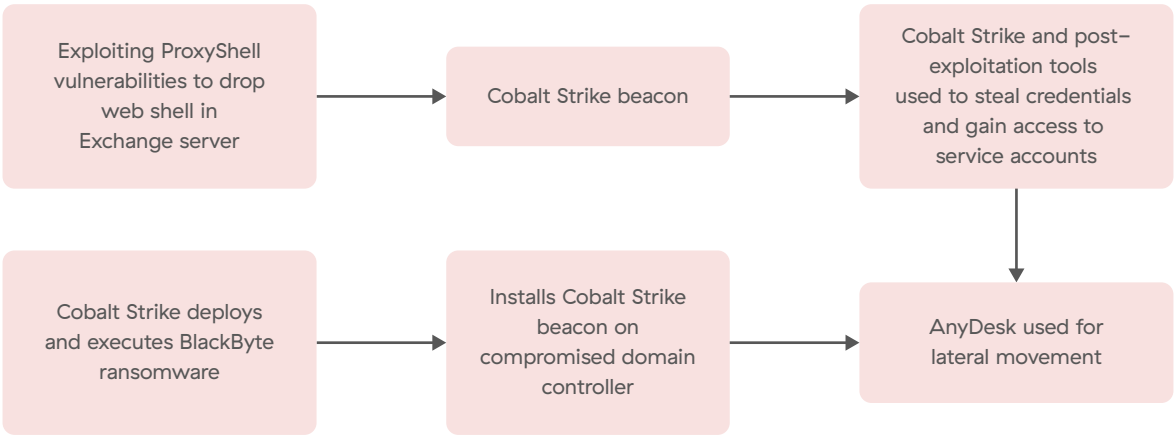


Figure 31 : Anatomie d'une attaque par ransomware BlackByte

L'accès initial est effectué par l'exploitation des vulnérabilités de ProxyShell afin de déposer un shell Web sur le serveur Exchange. Le shell Web télécharge la balise Cobalt Strike. Cobalt Strike dérobe ensuite les informations d'identification et installe l'outil RDP AnyDesk. AnyDesk est utilisé pour le déplacement latéral et dépose Cobalt Strike dans le contrôleur de domaine infecté. Cobalt Strike est ensuite utilisé pour déployer et exécuter le ransomware BlackByte.

BlackByte utilise une combinaison d'algorithmes AES et RSA pour chiffrer les fichiers. Les versions les plus récentes de BlackByte utilisent Curve25519 ECC pour le chiffrement asymétrique et ChaCha20 pour le chiffrement symétrique des fichiers.

Les acteurs malveillants BlackByte exfiltrent également les données des victimes avant de chiffrer les fichiers. Une capture d'écran du site de divulgation des données de BlackByte est présentée à la figure 32.

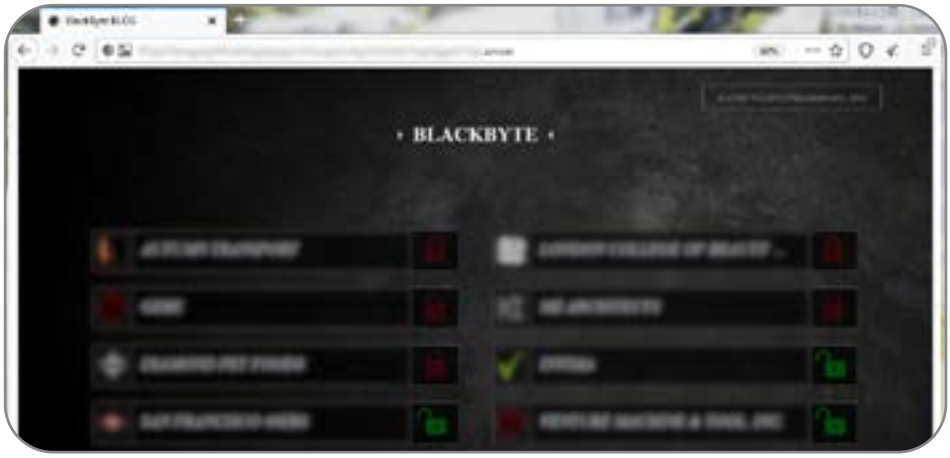


Figure 32 : Site de divulgation de données BlackByte

La figure 33 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de BlackByte.

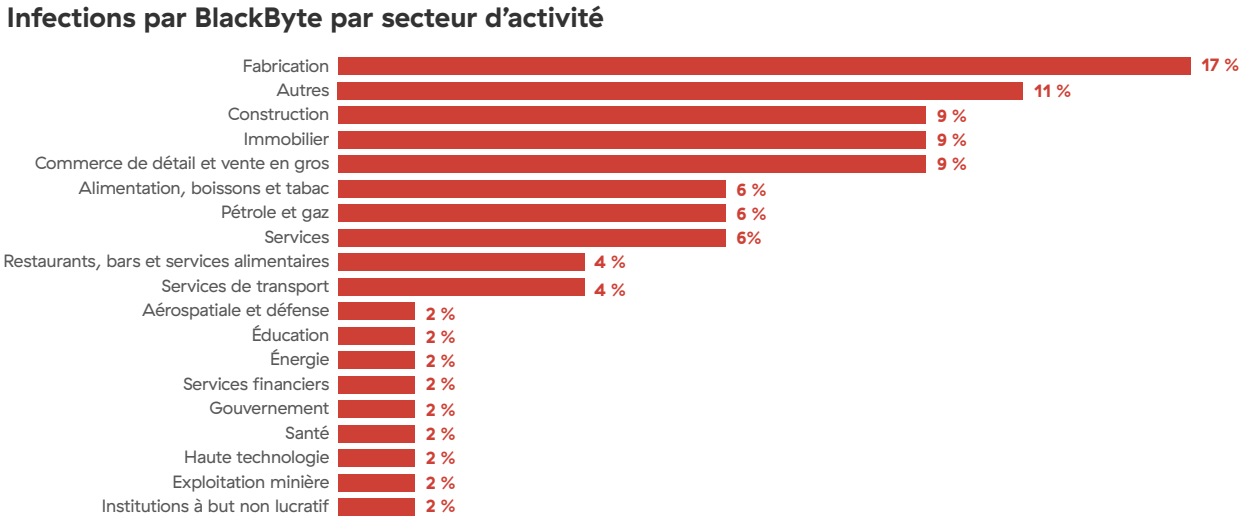


Figure 33 : Infections par BlackByte par secteur d'activité

BlackByte : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Exfiltration	Impact
Pièce jointe d'hameçonnage	Interprète de commandes et de scripts	Créer ou modifier un processus système : service Windows	Comptes de domaine	Altération des défenses : désactivation ou modification des outils	Découverte de la configuration du réseau système	Transfert latéral d'outil	Transfert programmé	Données chiffrées pour impact
Exploiter l'application destinée au public	API Native		Exploitation pour l'élévation des privilèges	Supprimer l'obs-curcissement/ Décoder des fichiers ou des informations	Découverte du système à distance			Inhiber la récupération du système
	Exécution utilisateur			Modifier le registre	Découverte de fichiers et de répertoires			
					Interrogation du registre			
					Découverte de logiciels de sécurité			

AvosLocker

Le ransomware AvosLocker est un groupe RaaS qui a fait une apparition remarquée en juillet 2021. Tout comme Hive et BlackByte, l'infection initiale commence par l'exploitation des vulnérabilités ProxyShell CVE-2021-34473, CVE-2021-34523 et CVE-2021-31207 présentes dans le serveur Microsoft Exchange.

Chaîne d'infection
Le hacker crée un brouillon d'e-mail dans une boîte aux lettres. L'e-mail comporte une pièce jointe qui contient le shell Web codé. Le hacker exporte ensuite l'ensemble de la boîte aux lettres (brouillon d'e-mail malveillant inclus) au format de fichier PST avec une extension ASPX. Ceci permet aux hackers de déposer des shells Web sur des serveurs vulnérables.

Les shells Web sont ensuite utilisés pour déposer Cobalt Strike sur le serveur Exchange infecté. Cobalt Strike et Rclone sont utilisés pour dérober les informations d'identification et exfiltrer les données vers des serveurs distants.

L'attaque installe AnyDesk RDP pour accéder à plusieurs systèmes, en se déplaçant latéralement. Elle dépose plusieurs scripts de commandes pour modifier et supprimer les clés de registre liées aux logiciels de sécurité. Elle désactive également Windows Update et Windows Defender.

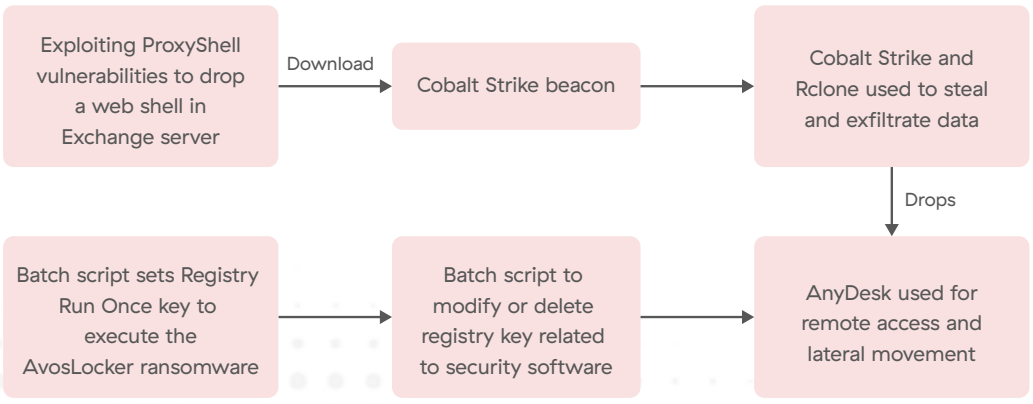


Figure 34 : Anatomie d'une attaque par ransomware AvosLocker

Enfin, AvosLocker redémarre le système en mode sans échec sous Windows, après quoi le ransomware commence à chiffrer les fichiers. En démarrant en mode sans échec, AvosLocker peut maximiser le nombre de fichiers chiffrés, car les applications professionnelles telles que les bases de données ne sont probablement pas en cours d'exécution. Par conséquent, ces applications n'auront pas de descripteur de fichier ouvert qui pourraient empêcher le chiffrement des fichiers. En outre, de nombreux logiciels de sécurité (les programmes antivirus, par exemple) ne sont pas chargés par défaut lorsque le système fonctionne en mode sans échec. La capacité de chiffrer des fichiers en mode sans échec de Windows est une caractéristique qui a été observée dans d'autres familles de ransomware, notamment Conti, REvil et BlackMatter.

AvosLocker utilise une combinaison d'algorithmes RSA et AES pour chiffrer les fichiers. AvosLocker a créé une version Linux de son ransomware qui cible VMware ESXi.

Après l'attaque, le hacker menace de publier les données de la victime sur un site de divulgation de données et, dans certains cas, menace et exécute une attaque DDoS sur le réseau de la victime pendant la négociation. Une capture d'écran du site de divulgation des données d'AvosLocker est présentée à la figure 35.

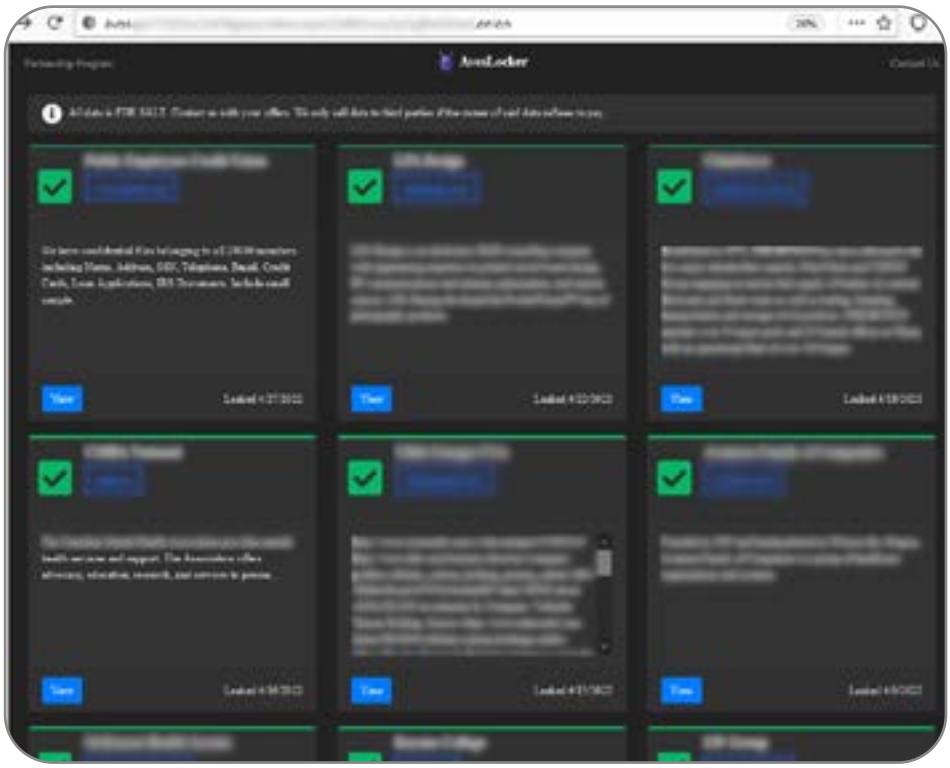


Figure 35 : Site de divulgation de données AvosLocker

La figure 36 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide d'AvosLocker.

Infections par AvosLocker par secteur d'activité

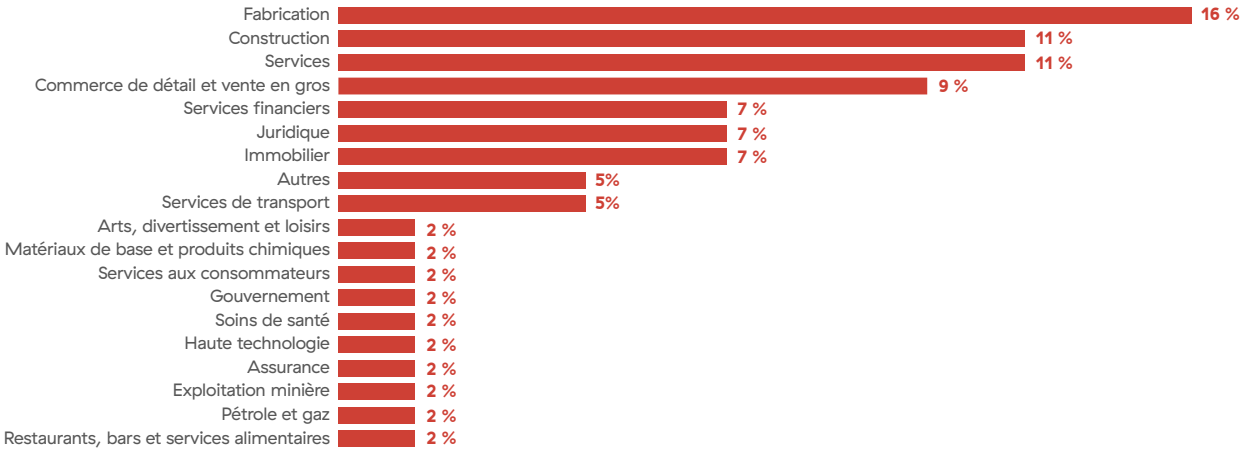


Figure 36 : Infections par AvosLocker par secteur d'activité

AvosLocker : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Exfiltration	Impact
Pièce jointe d'hameçonnage	Interface de ligne de commande	Exécution du démarrage ou de l'ouverture de session automatique : clés d'exécution du registre/ dossier de démarrage	Comptes de domaine	Altération des défenses : désactivation ou modification des outils	Découverte de la configuration du réseau système	Transfert latéral d'outil	Transfert programmé	Données chiffrées pour impact
Exploiter l'application destinée au public	Exécution utilisateur	Tâche/travail programmé(e)	Exploitation pour l'élévation des privilèges	Supprimer l'obs–curcissement/ Décoder des fichiers ou des informations	Découverte du système à distance			Inhiber la récupération du système
					Découverte de fichiers et de répertoires			Arrêt/ redémarrage du système
					Découverte de logiciels de sécurité			

BlackCat/ALPHV

BlackCat, alias ALPHV, est une opération RaaS qui a été repérée pour la première fois aux alentours de novembre 2021. BlackCat a utilisé le langage de programmation RUST, qui permet d'améliorer les performances et la fiabilité du traitement simultané.

Chaîne d'infection
L'infection initiale commence par l'utilisation d'informations d'identification compromises pour accéder aux systèmes réseau des victimes. Au départ, le ransomware utilise Cobalt Strike, des scripts PowerShell et des scripts de commandes pour s'introduire dans le réseau de la victime. Une fois qu'il a obtenu l'accès, il compromet les comptes administrateurs dans Active Directory. Il utilise ensuite des objets de stratégie de groupe (GPO) malveillants pour diffuser et exécuter le ransomware. Il utilise également Microsoft Sysinternals et d'autres outils administratifs dans le cadre de son attaque.

Figure 37 : Anatomie d'une attaque par ransomware BlackCat/ALPHV

BlackCat a ajouté la tactique DDoS à son mode opératoire. BlackCat mène des attaques DDoS soit sur le site Web soit sur le réseau de la victime pour encourager cette dernière à négocier avec ses opérateurs et exiger des montants de rançon plus élevés. Une capture d'écran du site de divulgation des données de BlackCat est présentée à la figure 38.

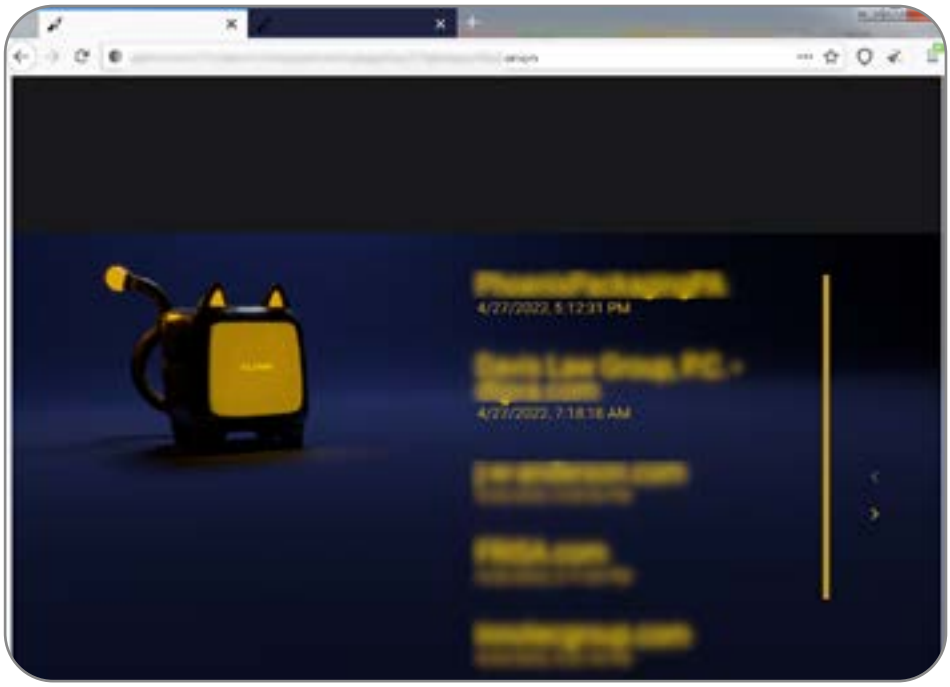


Figure 32 : Site de divulgation de données BlackCat/ALPHV

La figure 39 présente les secteurs d'activité ciblés par les attaques à double extorsion menées à l'aide de BlackCat/ALPHV.

BlackCat/ALPHV infections by industry

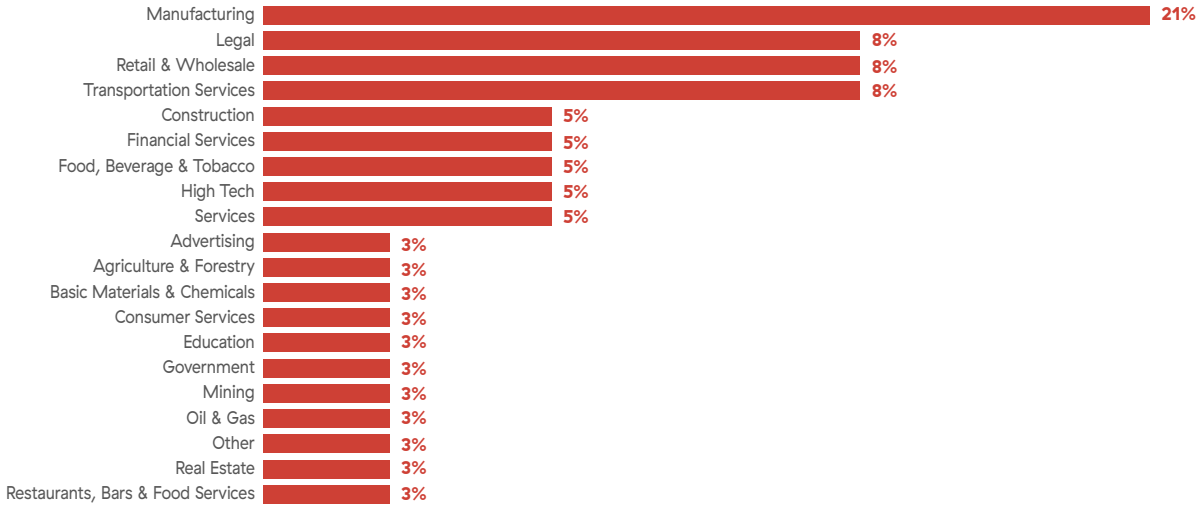


Figure 39 : Infections par BlackCat/ALPHV par secteur d'activité

BlackCat : Tactiques et techniques MITRE ATT&CK

Accès initial	Exécution	Persistance	Élévation des privilèges	Évasion de défense	mutuelle	Déplacement latéral	Exfiltration	Impact
Comptes valides	Interprète de commandes et de scripts	Exécution du démarrage ou de l'ouverture de session automatique : clés d'exécution du registre/ dossier de démarrage	Comptes de domaine	Altération des défenses : désactivation ou modification des outils	Découverte de la configuration du réseau système	Transfert latéral d'outil	Transfert programmé	Données chiffrées pour impact
	Exécution utilisateur	Tâche/travail programmé(e)	Exploitation pour l'élévation des privilèges	Supprimer l'obs–curcissement/ Décoder des fichiers ou des informations	Découverte du système à distance			Inhiber la récupération du système
				Modification de la politique de domaine : modification de la politique de groupe	Découverte de fichiers et de répertoires			
					Découverte de logiciels de sécurité			

À propos de ThreatLabz

ThreatLabz est la branche de recherche en sécurité de Zscaler. Cette équipe de premier ordre est responsable de la chasse aux nouvelles menaces et s'assure que les milliers d'organisations qui utilisent la plateforme mondiale Zscaler sont toujours protégées. En plus de la recherche sur les programmes malveillants et de l'analyse comportementale, les membres de l'équipe sont impliqués dans la recherche et le développement de nouveaux modules prototypes pour la protection avancée contre les menaces sur la plateforme Zscaler, et effectuent régulièrement des audits de sécurité interne pour s'assurer que les produits et l'infrastructure de Zscaler répondent aux normes de conformité de sécurité. ThreatLabz publie régulièrement des analyses approfondies des menaces nouvelles et émergentes sur son portail, research.zscaler.com.

Restez informé des recherches de ThreatLabz en vous abonnant dès aujourd'hui à notre bulletin d'information Trust Issues.

Zscaler Zero Trust Exchange a été désigné par Gartner comme une plateforme SSE (Security Service Edge) de premier plan, qui apporte une protection contre les ransomwares à chaque étape de la chaîne d'attaque, afin de considérablement réduire le risque d'attaque et d'atténuer les préjudices potentiels.

Zscaler intègre en natif des fonctionnalités de pointe pour :

Minimiser la surface d'attaque

L'architecture de Zscaler, basée sur un proxy cloud natif, réduit la surface d'attaque en dissimulant les applications internes à Internet, éliminant ainsi les vecteurs d'attaque potentiels.

Empêcher l'intrusion

Zscaler assure l'inspection et l'authentification complètes de tout le trafic, y compris le trafic chiffré, pour empêcher que les acteurs malveillants ne puissent s'infiltrer, en utilisant des outils tels que l'isolation du navigateur et le sandboxing inline afin de protéger les utilisateurs contre les menaces inconnues et dérobées.

Éradiquer le mouvement latéral

Zscaler connecte en toute sécurité les utilisateurs et les entités directement aux applications, et non aux réseaux, pour éliminer toute possibilité de mouvements latéraux, et entoure vos applications de leurres réalistes et sophistiqués pour faire bonne mesure.

Arrêter la perte de données

Zscaler inspecte tout le trafic sortant vers les applications cloud afin d'empêcher le vol de données, et utilise les capacités du Cloud Access Security Broker (CASB) pour identifier et corriger les vulnérabilités des données au repos.

Pour en savoir plus, visitez notre page dédiée à la protection Zscaler contre les ransomwares.

zscaler™ | Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients, avec une meilleure sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.fr