Kaspersky Security Bulletin

Prédictions de nos chercheurs pour 2022

kaspersky

Prédictions de nos chercheurs pour 2022

Au cours des 12 derniers mois, le style et la gravité des menaces APT ont continué à évoluer. Malgré leur nature en constante évolution, nous pouvons en apprendre beaucoup sur les tendances récentes en matière d'APT, afin de prédire ce qui pourrait nous attendre l'année prochaine.

En nous appuyant sur les connaissances collectives de nos experts, nous avons établi des prédictions clés sur les prochaines attaques des APT, afin d'aider les cibles potentielles à rester sur leurs gardes.

Commençons par examiner les prédictions que nous avons faites pour l'année 2021.

À la fin de l'année, nous avons vu des acteurs d'APT exploiter des marketplaces du deep-web où les pirates vendent l'accès aux entreprises qu'ils ont inflitrées.

Les cybercriminels impliqués dans des APT achèteront l'accès initial aux réseaux à d'autres cybercriminels

L'année dernière, nous avions prédit que les mondes des APT et de la cybercriminalité deviendraient plus perméables sur le plan opérationnel. En particulier, nous nous attendions à ce que les acteurs d'APT exploitent les marketplaces du deep-web où les pirates vendent l'accès aux entreprises qu'ils ont infiltrées. Cette prédiction semble s'être réalisée il y a quelques jours seulement. BlackBerry a publié un rapport centré sur une entité qu'il appelle Zebra 2104 et qui semble être un « agent d'accès initial ». Selon leurs recherches, Zebra 2014 a permis aux exploitants de ransomwares de pénétrer dans les appareils de certaines de leurs victimes. Plus intéressant encore, il semble que l'APT StrongPity ait également utilisé leurs services, bien qu'ils soient entièrement axés sur la collecte d'informations. Comme il s'agit du type d'activité qui se déroule pendant les phases de préparation d'une attaque – des phases sur lesquelles nous n'avons généralement aucune visibilité – il se peut que de telles interactions entre les APT et le monde de la cybercriminalité soient plus nombreuses que nous ne le pensons.

Davantage de pays utilisent des poursuites judiciaires dans le cadre de leur cyberstratégie

En 2020, nous avions prédit que les gouvernements dénonceraient publiquement les cybercriminels pour attirer l'attention sur les activités des groupes d'APT hostiles, une tendance qui a encore évolué l'année dernière. Nous avions également prédit que les pays commenceraient à utiliser toute l'étendue de la loi pour perturber et punir les opérations de leurs adversaires, ce qui s'est avéré tout à fait exact.

Le 15 avril, la Maison-Blanche a officiellement accusé la Russie de l'attaque contre la chaîne d'approvisionnement de SolarWinds. Cette annonce a été accompagnée de sanctions à l'encontre de plusieurs entreprises qui, selon le département du Trésor, étaient impliquées dans le soutien aux opérations offensives.

Le 1er juillet, la NSA, le FBI, la CISA (Cybersecurity and Infrastructure Security Agency) et le NCSC du Royaume-Uni ont publié un avis commun signalant des centaines de tentatives d'intrusion par force brute dans le monde entier attribuées à Sofacy, également connu sous les noms d'APT28 et de Fancy Bear. Parmi les cibles figuraient des agences gouvernementales et militaires, des entreprises de défense, des partis politiques et des cabinets de conseil, des entreprises de logistique, des entreprises du secteur de l'énergie, des universités, des cabinets d'avocats ainsi que des entreprises du secteur des médias.

Le 19 juillet, les États-Unis ont annoncé leur intention de dénoncer les « comportements irresponsables et déstabilisateurs dans le cyberespace » avec le soutien de l'OTAN, de l'UE et du Royaume-Uni. La déclaration de la Maison-Blanche a mentionné en particulier l'exploitation récente des vulnérabilités « zero-day » de Microsoft Exchange. Le ministère américain de la Justice a également inculpé quatre membres présumés d'APT40 pour avoir mené des activités illicites sur des réseaux informatiques.

Les Forces de défense israéliennes (FDI) ont affirmé que des acteurs de la menace ont utilisé le catfishing pour inciter les soldats israéliens à installer des logiciels espions. Les attaquants ont utilisé six profils de réseaux sociaux sur Facebook, Instagram et Telegram pour attirer l'attention de cibles masculines, établir une relation avec elles et enfin les inciter à installer des applications censées offrir une fonctionnalité de chat privé sur leurs téléphones.

Le 24 septembre, l'UE a publié une déclaration concernant une campagne de désinformation appelée « Ghostwriter », en cours depuis mars 2017, destinée à discréditer l'OTAN. La campagne consisterait à s'introduire dans des sites Web d'information ou des comptes de réseaux sociaux de responsables gouvernementaux afin de publier de faux documents, de fausses nouvelles ainsi que des opinions trompeuses destinés à influencer les élections, à perturber les écosystèmes politiques locaux et à susciter la méfiance à l'égard de l'OTAN. Malgré les menaces, l'UE a finalement décidé de ne pas imposer de sanctions.

Dans l'ensemble, nous avons clairement observé un changement : les cyberincidents sont désormais traités par des moyens juridiques, comme des mises en accusation, plutôt que par des voies diplomatiques.

D'autres entreprises de la Silicon Valley prendront des mesures contre les agents « zero-day »

Peu après que nous ayons publié les prévisions de l'année dernière, Microsoft, Google, Cisco et Dell se sont joints à Facebook dans leur bataille juridique contre NSO. Les actions en justice sont toujours en cours.

Peu après que nous ayons publié les prévisions de l'année dernière, Microsoft, Google, Cisco et Dell se sont joints à Facebook dans leur bataille juridique contre NSO. Les actions en justice sont toujours en cours et, à notre connaissance, aucune autre action en justice n'a été engagée contre d'autres fournisseurs de logiciels de type « zero-day » ou d'intrusion.

En bref, notre prédiction s'est immédiatement avérée exacte, mais il est possible que la Silicon Valley attende les résultats de ce premier essai avant de s'attaquer à d'autres agents. Le 3 novembre, cependant, le ministère américain du Commerce a envoyé un signal très fort au marché relatif à la vulnérabilité « zero-day » en ajoutant plusieurs sociétés (NSO, Positive Technologies, COSEINC, Candiru) à la liste des entités accusées d'activités contraires à la sécurité nationale des États-Unis, en raison du « trafic de cyberoutils ». Pour le moment, on ne sait pas quelle incidence cette décision aura sur les procédures en cours.

Ciblage accru des structures de réseau (network appliances)

Lorsque nous avons écrit cette prédiction, nous pensions principalement à une poursuite de toutes les activités malveillantes visant les structures VPN. Comme indiqué dans la première section de cet article, les vulnérabilités logicielles les plus répandues ont fini par avoir une incidence sur différents programmes (comme Microsoft Exchange). Cependant, nous avons observé certains acteurs de menaces, comme APT10, qui exploitaient ces vulnérabilités pour détourner des sessions VPN.

Cette prédiction s'est toutefois concrétisée d'une autre manière. Une campagne très intéressante orchestrée par APT31 a vu le jour en 2021. L'acteur de la menace y exploite un réseau de routeurs SOHO infectés (plus particulièrement les modèles Pakedge RK1, RE1 et RE2) et l'utilise comme réseau d'anonymisation et comme hébergeur de C2.

L'émergence des vulnérabilités 5G

L'année 2020 a été marquée par des tensions accrues autour du développement de la technologie 5G. Nous nous attendions à ce qu'elles s'aggravent, et qu'elles se manifestent notamment en 2021 par la découverte et la publication de vulnérabilités dans des produits liés à la 5G, voire dans le protocole lui-même. Le litige semble s'être limité à la sphère juridique, mais des recherches intéressantes ont tout de même été menées, identifiant les problèmes de sécurité qui pourraient autoriser les attaquants à extraire des informations d'identification ou de localisation.

Réclamer de l'argent « en proférant des menaces »

La réponse au problème des ransomwares est de plus en plus organisée.

Les tactiques de ransomwares « améliorées » mises en place depuis 2019 se sont révélées suffisamment efficaces pour faire partie intégrante de l'arsenal des criminels. Toutefois, à en juger par les diverses arrestations effectuées et les déclarations communes de nombreux organismes et responsables de l'application de la loi, il est clair que la réponse au problème des ransomwares est de plus en plus organisée. En octobre, le gouvernement américain a mené des opérations offensives pour perturber les activités de REvil.

Cette pression croissante et la menace existentielle qu'elle représente se reflètent dans les tendances actuelles de l'écosystème des ransomwares. Les tactiques de chantage impliquant des données volées ont fait leurs preuves et ne sont probablement pas la cible actuelle des groupes criminels.

Des attaques plus perturbatrices

Cette prédiction s'est avérée exacte. L'un des cyberévénements les plus emblématiques de 2021 a été l'attaque par ransomwares contre Colonial Pipeline. Au cours de l'attaque, les équipements gérant le pipeline ont été touchés, ce qui a entraîné d'importants problèmes d'approvisionnement aux États-Unis. Cette infrastructure était si importante que la victime s'est sentie obligée de payer une rançon de 4,4 millions de dollars. Heureusement, 2,3 millions de dollars ont été récupérés par le ministère américain de la Justice.

En juillet 2021, un wiper inédit (Meteor) a paralysé le système ferroviaire iranien. Pour couronner le tout, les utilisateurs bloqués étaient invités à adresser leurs plaintes par téléphone aux autorités locales, ce qui a probablement eu des répercussions sur la qualité du service d'une autre fonction gouvernementale. Plus tard, en octobre, une attaque similaire a eu une incidence sur toutes les stations-service du pays. Aucun groupe n'a revendiqué la responsabilité de l'une ou l'autre de ces attaques.

Les attaquants vont continuer d'exploiter la pandémie

En 2020, nous avons vu de multiples groupes d'APT cibler des institutions universitaires et des centres de recherche impliqués dans le développement de vaccins contre la COVID-19. Il s'agit notamment de DarkHotel et d'APT29 (alias CozyDuke et CozyBear) avec leur programme malveillant WellMess (tel qu'attribué par le NCSC [National Cyber Security Centre] britannique). Cette année, nous avons vu plusieurs groupes d'APT tenter d'utiliser des leurres liés à la COVID-19 dans leur ciblage, comme ScarCruft, LuminousMoth, EdwardsPhesant, BountyGlad, Kimsuky et ReconHellcat. Un groupe d'activités intéressant que nous avons repéré et que nous avons pu attribuer ultérieurement à un acteur connu sous le nom de SideCopy, visait des organisations diplomatiques et gouvernementales en Asie et au Moyen-Orient en utilisant des leurres liés à la COVID-19 ainsi que des sites Web compromis hébergeant des fichiers HTA et JS malveillants. De multiples aspects de la campagne, notamment la chaîne d'exécution, les programmes malveillants utilisés, les chevauchements d'infrastructures ainsi que les chemins PDB et autres TTP, nous rappellent d'autres groupes opérant dans la même région, par exemple SideWinder, OrigamiElephant, Gorgon group ou encore Transparent Tribe. Pourtant, aucune des similitudes trouvées n'a été suffisamment probante pour attribuer l'ensemble de ces activités à des acteurs connus.

À présent, nous tournons notre attention vers l'avenir. Voici les développements qui, selon nous, pourraient voir le jour en 2022.

Le secteur privé soutient un afflux de nouveaux acteurs dans le domaine des APT

Cette année, l'utilisation de logiciels de surveillance développés par des fournisseurs privés a suscité un vif intérêt, comme indiqué ci-dessus. Compte tenu de la rentabilité potentielle de cette activité et des conséquences que ces logiciels peuvent avoir sur les personnes visées, nous pensons que les fournisseurs de ces logiciels joueront un rôle plus important, du moins jusqu'à ce que les gouvernements cherchent à réglementer l'utilisation de ceux-ci. Certains signes indiquent que cette tendance se dessine déjà. En octobre 2021, le Bureau de l'industrie et de la sécurité (BIS) du ministère américain du Commerce a introduit une règle finale provisoire qui définit quand une licence d'exportation sera exigée pour les logiciels de surveillance commerciaux : l'objectif est d'empêcher la distribution d'outils de surveillance aux pays soumis au contrôle des armes, tout en autorisant la poursuite des recherches et des transactions légitimes en matière de sécurité.

Parallèlement, **les fournisseurs de logiciels malveillants et le secteur de la sécurité offensive s'efforceront de soutenir les anciens acteurs, mais également les nouveaux, dans leurs opérations.**

Alors que les terminaux sous Android sont en proie à de nombreux programmes malveillants cybercriminels, iOS est surtout dans la ligne de mire du cyberespionnage avancé financé par des États-nations.

Les appareils mobiles exposés à de nombreuses attaques

Les programmes malveillants visant les appareils mobiles ne cessent de faire parler d'eux depuis plus de dix ans. Ce phénomène a été fortement corrélé à la popularité des systèmes d'exploitation dominants. À ce jour, les deux systèmes d'exploitation les plus populaires pour les appareils mobiles sont iOS et Android (ainsi que d'autres clones fondés sur Android/Linux). Dès le départ, ils ont adopté des philosophies très différentes : alors qu'iOS s'appuie sur une boutique App Store fermée qui n'autorise que les applications approuvées, Android est plus ouvert et autorise les utilisateurs à installer des applications tierces directement sur les appareils. Il en résulte de grandes différences dans le type de programmes malveillants ciblant les deux plateformes.

Alors que les terminaux Android sont victimes de nombreux programmes malveillants de nature cybercriminelle (même s'ils ne sont pas exempts d'attaques APT), iOS est surtout dans la ligne de mire du cyberespionnage avancé financé par des États-nations. En 2021, Pegasus Project a donné une nouvelle dimension au monde autrement obscur des attaques de type « zero-click » d'iOS. Par ailleurs, le nombre de vulnérabilités de type « zero-day » signalées sur iOS a été supérieur à celui de toutes les autres années.

Du point de vue des attaquants, les appareils mobiles sont des cibles idéales : ils voyagent presque partout avec leurs propriétaires, ils contiennent des informations concernant la vie privée de ceux-ci, et les infections sont très difficiles à prévenir ou à détecter. Contrairement aux PC ou aux Mac, où l'utilisateur a le choix d'installer une suite de sécurité, ces produits sont soit bridés, soit inexistants sur iOS. Il en résulte une occasion extraordinaire pour les APT, qu'aucun adversaire financé par un État ne voudra manquer. **En 2022, nous observerons des attaques plus complexes contre des appareils mobiles exposés et fermés, qui seront accompagnées de l'inévitable démenti des auteurs.**

Davantage d'attaques contre les chaînes d'approvisionnement

Cette année, nous avons constaté des attaques notables contre les chaînes d'approvisionnement. Plus haut, nous avons évoqué l'adoption de cette approche par les cybercriminels impliqués dans des APT. Cependant, nous avons également constaté que les cybercriminels profitent des faiblesses de la sécurité des fournisseurs pour compromettre les clients de l'entreprise compromise. Parmi les exemples frappants, citons l'attaque d'un réseau d'oléoducs américains en mai, celle d'un producteur mondial de viande en juin ainsi que le ciblage des MSP (fournisseurs de services gérés) et de leurs clients au mois de juillet. Ces attaques représentent une violation de la confiance à un point précis de la chaîne d'approvisionnement. Elles sont particulièrement précieuses pour les attaquants parce qu'elles constituent un tremplin vers de nombreuses autres cibles en un seul coup. C'est pourquoi les **attaques contre les chaînes d'approvisionnement seront une tendance croissante en 2022 et au-delà.**

Exploitation continue du télétravail

De nombreux employés continueront probablement de travailler à domicile dans l'avenir. Cela sera une occasion pour les attaquants de compromettre les réseaux d'entreprise.

Malgré l'assouplissement des règles de confinement liées à la pandémie dans diverses régions du monde, de nombreux employés continuent de travailler à domicile, et il est probable qu'ils continueront à le faire dans l'avenir. Cela restera une occasion pour les attaquants de compromettre les réseaux d'entreprise. Il s'agit notamment de l'utilisation de l'ingénierie sociale pour obtenir des informations d'identification et des attaques par force brute sur les services d'entreprise dans l'espoir de trouver des serveurs mal protégés. En outre, comme de nombreuses personnes continuent d'utiliser leur propre appareil, plutôt que de cibler des appareils sécurisés par les équipes informatiques des entreprises, **les attaquants chercheront de nouvelles occasions d'exploiter les ordinateurs domestiques non protégés ou non mis à jour comme vecteur d'entrée dans les réseaux d'entreprise.**

Augmentation des intrusions d'APT dans la région META, notamment en Afrique

Le principal moteur de cette évolution sera l'augmentation générale des tensions géopolitiques, qui entraînera un accroissement des activités cyberoffensives reposant sur l'espionnage. La géopolitique a toujours été le principal facteur contribuant (parmi d'autres facteurs, comme l'économie, la technologie et les affaires étrangères) à influencer les cyberintrusions dans le but de voler des données confidentielles à des fins de sécurité nationale. Malgré la situation actuelle liée à la pandémie qui a des répercussions sur le monde entier, les tensions géopolitiques ont considérablement augmenté au Moyen-Orient et en Turquie au moins depuis le mois de janvier 2020, et elles continueront probablement sur cette lancée.

L'Afrique est devenue la région qui s'urbanise le plus rapidement et qui attire des millions de dollars d'investissements. Parallèlement, de nombreux pays du continent occupent une position stratégique en matière de commerce maritime. Ce constat et l'amélioration continue des systèmes de défense dans cette région nous amènent à penser que **l'année 2022 sera marquée par des attaques APT majeures dans la région META, notamment en Afrique.**

Explosion des attaques contre la sécurité dans le cloud et les services externalisés

Les fournisseurs de services dans le cloud regroupent désormais suffisamment de données pour attirer l'attention des acteurs étatiques, et deviendront les principales cibles d'attaques complexes.

De plus en plus d'entreprises intègrent l'informatique dans le cloud à leurs modèles commerciaux en raison du côté pratique et évolutif qu'elle offre. Le mouvement devops a conduit de nombreuses entreprises à adopter des architectures logicielles reposant sur des microservices et s'exécutant sur des infrastructures tierces – des infrastructures qui ne sont généralement protégées que par un mot de passe ou une clé API.

Ce nouveau paradigme a des implications en matière de sécurité que les développeurs ne comprennent peut-être pas entièrement, sur lesquelles les défenseurs ont peu de visibilité et que les APT n'ont pas vraiment étudiées jusqu'à présent. Nous pensons que ces derniers seront les premiers à rattraper leur retard.

Au sens large, cette prédiction concerne les services externalisés, comme les services de modification de documents en ligne, le stockage de fichiers, l'hébergement d'emails, etc. Les fournisseurs **tiers de services dans le cloud regroupent désormais suffisamment de données pour attirer l'attention des acteurs étatiques, et deviendront les principales cibles d'attaques complexes.**

Le retour des attaques de bas niveau : les bootkits sont de nouveau à la mode

Les implants de bas niveau sont souvent écartés par les attaquants en raison du risque inhérent de provoquer des défaillances du système et du degré de complexité requis pour les créer. Les rapports publiés par Kaspersky tout au long de l'année 2021 indiquent que la recherche offensive en matière de bootkits est bien réelle : soit les gains obtenus l'emportent désormais sur les risques, soit le développement de bas niveau est devenu plus accessible. Nous nous attendons à découvrir des implants plus avancés de ce type en 2022. En outre, **à mesure que Secure Boot se répand, les attaquants devront trouver des exploits ou des vulnérabilités dans ce mécanisme de sécurité pour le contourner** et continuer à déployer leurs outils.

Les États clarifient leurs pratiques acceptables en matière de cyberdélits

Certains pays publieront leur taxonomie en matière de cyberdélinquance, en détaillant précisément les types de vecteurs d'attaque et de comportements interdits.

Au cours de la dernière décennie, l'ensemble du secteur a observé une tendance à la politisation croissante du cyberespace, notamment en ce qui concerne la cyberguerre. L'année dernière, nous avions prédit que les mises en accusation légales feraient partie intégrante de l'arsenal des États occidentaux pour infliger un coût aux opérations de leurs adversaires.

Toutefois, un problème se pose : les États qui dénoncent les cyberattaques dont ils sont victimes sont en même temps connus pour mener les leurs. Pour que leurs protestations aient du poids, ils devront établir une distinction entre les cyberattaques qui sont acceptables et celles qui ne le sont pas. En 2022, nous pensons que certains **pays publieront leur taxonomie en matière de cyberdélinquance, détaillant précisément quels types de vecteurs d'attaque (par exemple, la chaîne d'approvisionnement) et de comportements (par exemple, les comportements destructeurs, les comportements ayant une incidence sur les infrastructures civiles, etc.) sont interdits.**

Actualités sur les cybermenaces :
www.securelist.fr
Actualités dédiées à la sécurité informatique :
https://www.kaspersky.fr/blog/category/business/

kaspersky.fr

kaspersky BRING ON THE FUTURE