Bulletin de Kaspersky sur la sécurité 2023

Prédictions pour 2024 concernant les menaces persistances avancées (APT)

kaspersky BRING ON THE FUTURE

Sommaire

Examen des prévisions faites l'année dernière. 1

L'essor des attaques destructives 1

Les serveurs de messagerie deviennent des cibles prioritaires 1

Le prochain WannaCry 2

Le ciblage des APT se tourne vers les technologies, les producteurs et les opérateurs de satellites 2

Le hack-and-leak est le nouvel ennemi 2

Davantage de groupes APT passeront de Cobalt Strike à d'autres alternatives 2

Programmes malveillants transmis par les ROEM 2

Piratage à l'aide de drones ! 3

Prédictions des menaces persistantes avancées pour 2024 4

La montée des exploits créatifs sur les appareils mobiles, portables et intelligents 4

Création de nouveaux botnets avec des logiciels et des appareils grand public et d'entreprise 4

Les obstacles à l'exécution de code au niveau du noyau sont de plus en plus évités (les rootkits du noyau sont à nouveau chauds) 5

Augmentation des cyberattaques perpétrées par des groupes commandités par des États 5

Hacktivisme dans la cyberguerre : la nouvelle norme dans les conflits géopolitiques 6

Attaques de la chaîne d'approvisionnement en tant que service : accès aux achats groupés des opérateurs 6

Le phishing ciblé amené à se développer avec une IA générative accessible 6

Apparition de nombreux groupes proposant des services de hacking 7

Les systèmes MFT à l'avant-garde des cybermenaces 7

Les menaces persistantes avancées (APT) sont les menaces les plus dangereuses, car elles utilisent des outils et des techniques complexes et sont souvent très ciblées et difficiles à détecter. Dans un contexte de crise mondiale et d'aggravation des affrontements géopolitiques, ces cyberattaques élaborées sont encore plus dangereuses, car les enjeux sont d'autant plus importants.

Au sein de l'équipe internationale de recherche et d'analyse (GReAT) de Kaspersky, nous surveillons plusieurs groupes APT, nous analysons les tendances et essayons d'anticiper leurs évolutions afin de garder une longueur d'avance sur les menaces et assurer ainsi la sécurité de nos clients. Dans ce document, nous passerons en revue les tendances de l'année écoulée pour examiner lesquelles de nos prédictions pour 2023 se sont réalisées et nous tenterons de prédire ce qui nous attend en 2024.

Examen des prévisions faites l'année dernière

L'essor des attaques destructives

En décembre de l'année dernière, peu après la publication de nos prévisions pour 2023, des agences gouvernementales russes auraient été la cible d'un effaceur de données (wiper) nommé CryWiper. Le malware se faisait passer pour un ransomware, exigeant de l'argent des victimes pour « décrypter » leurs données. Cependant, au lieu de chiffrer les données des systèmes concernés, il les a délibérément détruites.

En janvier, ESET a découvert un nouveau wiper, déployé lors d'une attaque en Ukraine via la GPO Active Directory. Ils attribuent ce wiper (SwiftSlicer), au groupe Sandworm (alias Hadès).

En juin, Microsoft a publié un rapport sur une cybermenace nommée Cadet Blizzard, responsable de WhisperGate et d'autres wipers ayant ciblé des agences gouvernementales ukrainiennes au début de l'année 2022. Outre les agences gouvernementales, les forces de l'ordre, les services informatiques et les services d'urgence en Ukraine, cette cybermenace a également ciblé des organisations en Europe, en Asie centrale et en Amérique latine.

Pour faire court, même si le volume n'était pas le même qu'en 2022, il est clair que des attaques importantes ont eu lieu

Pour faire court, même si le volume n'était pas le même qu'en 2022, il est clair que des attaques importantes ont eu lieu.

Verdict : partiellement réalisée ✔

Les serveurs de messagerie deviennent des cibles prioritaires

En juin, Recorded Future a prévenu que BlueDelta (alias Sofacy, APT28, Fancy Bear et Sednit) avait exploité des vulnérabilités du webmail Roundcube pour pirater plusieurs organisations, notamment des institutions gouvernementales et militaires impliquées dans les infrastructures aéronautiques. Ce groupe a utilisé le conflit russo-ukrainien pour inciter ses cibles à ouvrir des e-mails nuisibles exploitant les vulnérabilités (CVE-2020-35730, CVE-2020-12641 et CVE-2021-44026). À l'aide d'un script malveillant, les pirates ont redirigé les e-mails entrants de leurs cibles vers une adresse e-mail qu'ils contrôlaient, collectant ainsi des données des comptes compromis.

À l'aide d'un script malveillant, les pirates ont redirigé les e-mails entrants de leurs cibles vers une adresse e-mail qu'ils contrôlaient, collectant ainsi des données des comptes compromis

En juillet, nous avons signalé une variante mise à jour d'Owowa utilisée contre des cibles en Russie. Nous avons pu associer le déploiement d'Owowa à une chaîne d'intrusion basée sur les e-mails qui ressemblait à des activités CloudAtlas connues dans une campagne que nous appelons GOFFEE.

En août, TeamT5 et Mandiant, faisant suite à des recherches antérieures traitant de l'exploitation d'une vulnérabilité basée sur l'injection de commandes à distance affectant l'appliance Barracuda Email Security Gateway (ESG) (CVE-2023-2868) par UNC4841, ont fourni plus de détails sur les TTP utilisées par la cybermenace. UNC4841 a déployé un nouveau malware conçu pour maintenir sa présence sur un petit groupe de cibles hautement prioritaires compromises avant la publication du correctif ou peu de temps après. Cela inclut l'utilisation des portes dérobées SKIPJACK et DEPTHCHARGE et du programme de démarrage FOXTROT/FOXGLOVE. La cybermenace a ciblé une grande variété de secteurs. L'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a fourni des IoC supplémentaires associés à l'exploitation du CVE-2023-2868.

Verdict : prédiction réalisée ✔

Le prochain WannaCry

Heureusement pour nous, aucune nouvelle épidémie de cyberattaques ne s'est produite.

Verdict : prédiction non réalisée ✗

Le ciblage des APT se tourne vers les technologies, les producteurs et les opérateurs de satellites

Le seul cas connu d'attaque utilisant des technologies par satellite survenu au cours des dernières années est le piratage du réseau KA-SAT en 2022. Nous n'avons rien vu de tel en 2023.

Verdict : prédiction non réalisée ✗

Le hack-and-leak est le nouvel ennemi

En avril, nous avons signalé KelvinSecurity, un groupe hacktiviste hispanophone. Les motivations du groupe sont sociopolitiques et monétaires mais incohérentes. Les attaques sont dirigées contre des organisations publiques ou privées du monde entier. Les fuites sont souvent vendues sur le Dark web, sur des groupes de messages ou sur les propres plateformes du groupe, certaines sont distribuées gratuitement.

La cybermenace se concentre sur la collecte d'informations à des fins d'espionnage et de hack-and-leak, ciblant des organisations de divers secteurs.

En mai, Ars Technica a signalé que les clés privées de BootGuard avaient été volées à la suite d'une attaque par ransomware contre Micro-Star International (MSI) en mars de cette année (le micrologiciel des PC dotés de puces Intel et avec BootGuard activé ne fonctionnera que s'il est signé numériquement à l'aide des clés appropriées). Si un pirate parvient à obtenir ces clés privées, il pourrait signer son malware afin que le code soit considéré comme fiable et exécuté par les ordinateurs MSI.

En août, Insikt Group, une division de recherche sur les menaces de Recorded Future, a signalé BlueCharlie (anciennement connu sous les noms TAG-53, Blue Callisto, Callisto ou Calisto, COLDRIVER, Star Blizzard (anciennement SEABORGIUM) et TA446), lié par des chercheurs à 94 nouveaux domaines, depuis mars de cette année, suggérant que le groupe modifie activement son infrastructure en réponse aux divulgations publiques sur ses activités. La cybermenace se concentre sur la collecte d'informations à des fins d'espionnage et de hack-and-leak, ciblant des organisations de divers secteurs, tels que le gouvernement, l'enseignement supérieur, la défense et les secteurs politiques, les organisations non gouvernementales (ONG), les militants, les journalistes, les groupes de réflexion et laboratoires nationaux.

Verdict : prédiction réalisée ✔

Davantage de groupes APT passeront de Cobalt Strike à d'autres alternatives

Nous surveillons de près des outils similaires, dont BruteRatel, mais Cobalt Strike est toujours utilisé comme cadre de référence pour les attaques.

Verdict : prédiction non réalisée ✗

Programmes malveillants transmis par les ROEM

En septembre, The Citizen Lab a publié un rapport concernant la grande figure de l'opposition égyptienne, Ahmed Eltantawy. Cet homme politique est devenu la cible d'une attaque « zero-day » inédite visant à infecter son téléphone avec un logiciel espion.

Au cours des mois d'août et de septembre, The Citizen Lab a rapporté qu'Eltantawy avait subi une forme plus dangereuse d'attaque par injection réseau, qui ne nécessitait aucune action de sa part, même un clic.

Le rapport du Citizen Lab a mené un examen pour déterminer où l'injection avait précisément eu lieu sur le réseau. Il a déterminé que le point d'injection se situait à la connexion entre deux opérateurs de télécommunications égyptiens. En s'appuyant uniquement sur des données techniques, le laboratoire n'a pas pu déterminer le côté de la connexion sur lequel le boîtier intermédiaire était positionné. Néanmoins, les chercheurs du Citizen Lab soupçonnaient que l'attaque impliquait probablement une intégration avec l'une des bases de données d'abonnés des fournisseurs.

Selon le Citizen Lab, l'attaque contre Eltantawy aurait nécessité l'installation du système PacketLogic sur le réseau du fournisseur de services de communication d'Eltantawy en Égypte, même si les chercheurs n'ont pas accusé le FAI de complicité dans l'attaque.

Verdict : prédiction réalisée ✔

Piratage à l'aide de drones !

Bien qu'il y ait eu un rapport public sur des drones utilisés pour pirater un réseau Wi-Fi en 2022, il n'existe aucun récit d'événements similaires se produisant en 2023.

Verdict : prédiction non réalisée ✘

Prédictions des menaces persistantes avancées pour 2024

Examinons maintenant les possibles prochaines menaces persistantes avancées.

La montée des exploits créatifs sur les appareils mobiles, portables et intelligents

L'année écoulée a été marquée par une découverte importante : « Opération Triangulation », une nouvelle campagne d'espionnage remarquablement furtive ciblant les appareils iOS, dont ceux de nos confrères.

L'année écoulée a été marquée par une découverte importante : « Opération Triangulation », une nouvelle campagne d'espionnage remarquablement furtive ciblant les appareils iOS, dont ceux de nos confrères. Au cours de l'enquête, notre équipe a identifié cinq vulnérabilités dans iOS, dont quatre « zero-day ». Ces vulnérabilités n'affectaient pas seulement les smartphones et les ordinateurs portables, mais s'étendaient également aux appareils portables et aux gadgets smart home, notamment l'Apple TV et l'Apple Watch. À l'avenir, nous pourrions nous attendre à des cas plus occasionnels d'attaques avancées visant à exploiter des appareils grand public et la technologie smart home. Les appareils iOS ne sont peut-être pas les seules cibles : d'autres appareils et systèmes d'exploitation pourraient également faire face au même risque.

Les cybermenaces considèrent le fait d'étendre leur surveillance pour inclure des appareils tels que les caméras domestiques intelligentes, les systèmes de voiture connectés et bien plus encore. Beaucoup de ces gadgets, nouveaux et anciens, sont sensibles en raison de vulnérabilités, de mauvaises configurations ou de logiciels obsolètes, ce qui en fait des cibles attrayantes et faciles pour les pirates.

Un autre aspect notable de cette tendance émergente est la méthode de transmission « silencieuse » des failles. Dans « l'opération Triangulation », des failles ont été discrètement transmises via iMessage et activées sans interaction de l'utilisateur. Au cours de l'année à venir, nous pourrions voir des méthodes alternatives de transmission des failles, telles que :

- – la méthode zéro clic via les messageries multiplateformes populaires, permettant des attaques sans interaction avec la victime potentielle
- – la méthode en un clic avec transmission de liens malveillants via SMS ou applications de messagerie, où les victimes peuvent déclencher des attaques sans le savoir en ouvrant ces liens
- Des pirates interceptant le trafic réseau, par exemple en exploitant les réseaux Wi-Fi, une méthode moins courante mais efficace

Pour se protéger contre les attaques complexes et les menaces ciblées, la protection des appareils personnels et professionnels est essentielle

Pour se protéger contre les attaques complexes et les menaces ciblées, la protection des appareils personnels et professionnels est essentielle. Des solutions telles que les plateformes XDR, SIEM et MDM, en plus des antivirus traditionnels, permettent une collecte de données centralisée, accélèrent l'analyse et relient les événements de sécurité provenant de diverses sources, offrant ainsi une réponse rapide aux incidents compliqués.

Création de nouveaux botnets avec des logiciels et des appareils grand public et d'entreprise

C'est un fait bien connu : des vulnérabilités persistent dans les logiciels et appareils couramment utilisés, utilisés dans des cadres professionnels ou personnels. De nouvelles vulnérabilités graves et critiques sont découvertes de temps en temps. Selon Statista, en 2022, le nombre de vulnérabilités découvertes (plus de 25 000) a battu tous les records. Souvent, des ressources limitées sont consacrées à la recherche des vulnérabilités, et celles-ci ne sont pas toujours corrigées rapidement. Cela suscite des inquiétudes quant à l'émergence potentielle de nouveaux botnets furtifs et à grande échelle, capables de mener des attaques ciblées.

La création d'un botnet implique l'installation furtive de logiciels malveillants sur une multitude d'appareils à l'insu de leurs propriétaires. Les groupes APT peuvent trouver cette tactique intrigante pour plusieurs raisons. Tout d'abord, cela permet aux pirates de dissimuler la nature ciblée de leurs attaques derrière des attaques apparemment à grande échelle, ce qui rend difficile pour les victimes de déterminer l'identité des pirates et leur motivation. De

plus, les botnets implantés dans des appareils ou des logiciels grand public, ou appartenant à des organisations légitimes, masquent la véritable infrastructure des pirates. Ils peuvent fonctionner comme des serveurs proxy, des hubs intermédiaires C2 (commande et contrôle) et, en cas de mauvaise configuration du réseau, des points d'entrée potentiels dans les organisations.

Les attaques lancées par des botnets ne se limiteront pas aux groupes APT et pourraient également être adoptées par des cybercriminels

Les botnets eux-mêmes ne constituent pas un nouvel outil d'attaque. Par exemple, il y a quelques années, un botnet de plus de 65 000 routeurs domestiques a été utilisé comme proxy pour un trafic malveillant pour d'autres botnets et APT. Un autre exemple, apparu avec la généralisation du télétravail, concerne les campagnes APT ciblant les travailleurs à distance en infectant leurs routeurs avec un cheval de Troie d'accès à distance (RAT) de type botnet. Compte tenu du nombre important de vulnérabilités révélées récemment, nous nous attendons à voir de nouvelles attaques de ce type au cours de l'année à venir.

Les attaques lancées par des botnets ne se limiteront pas aux groupes APT et pourraient également être adoptées par des cybercriminels. La dissimulation de ces attaques rend leur détection plus délicate, tout en offrant aux pirates de nombreuses opportunités d'infiltrer et d'établir une présence au sein de l'infrastructure de l'organisation.

Les obstacles à l'exécution de code au niveau du noyau sont de plus en plus évités (les rootkits du noyau sont à nouveau chauds)

Avec l'introduction de mesures de sécurité modernes telles que KMCS (Kernel Mode Code Signing), PatchGuard, HVCI (Hypervisor-Protected Code Integrity) et l'architecture Secure Kernel dans les récentes versions de Windows, Microsoft avait pour objectif de réduire la prédominance des rootkits et des attaques similaires de bas niveau. Ces méthodes d'attaque classiques étaient répandues auparavant par une multitude de variantes de rootkits. Au cours des dernières années, nous avons observé de nombreux acteurs APT et groupes de cybercriminalité exécuter avec succès leur code avec le mode noyau des systèmes ciblés, malgré la présence de ces nouveaux mécanismes de protection. Plusieurs violations du programme de compatibilité matérielle Windows (WHCP) signalées cette année ont conduit à des violations du modèle de confiance du noyau Windows. En juin 2021, le rootkit Netfilter a été signalé, après quoi Microsoft a publié un avis précisant qu'il était utilisé comme moyen permettant de tromper la géolocalisation au sein de la communauté gaming de Chine. Bitdefender a ensuite dévoilé FiveSys en octobre 2021, un rootkit principalement utilisé pour cibler les joueurs en ligne dans le but principal de voler des informations d'identification et de détourner des achats dans le jeu. Ensuite, Mandiant a signalé le dernier abus connu qui a révélé le malware Poortry, qui avait été utilisé dans un certain nombre de cyberattaques, y compris des incidents basés sur des ransomwares. En juillet 2023, nous avons signalé en privé de nouvelles variantes signées FiveSys.

Nous prévoyons une augmentation de trois vecteurs clés qui permettront aux cybermenaces de bénéficier de cette capacité :

- Augmentation du trafic de certificats EV et de signature de code volés sur le marché noir
- Augmentation des abus de comptes de développeurs pour signer un code malveillant via les services de signature de code Microsoft comme WHCP
- Augmentation continue du BYOVD (Bring Your Own Vulnerable Driver) dans l'arsenal de TTP actuel des pirates

Augmentation des cyberattaques perpétrées par des groupes commandités par des États

À l'avenir, nous anticipons une recrudescence des cyberattaques parrainées par des États à mesure que les tensions géopolitiques s'accentuent

L'année dernière, le monde a connu plus de 50 conflits armés, le nombre le plus élevé depuis la Seconde Guerre mondiale, selon les estimations de l'ONU. Toute confrontation politique inclut désormais intrinsèquement des éléments cybernétiques, devenus des éléments dans chaque conflit, cette tendance étant appelée à évoluer encore davantage. Les attaques APT de BlackEnergy en Ukraine sont un exemple marquant des dix dernières années, connues pour leurs actions destructrices contre les entreprises de médias, compromettant les systèmes de contrôle industriel et se livrant au cyberespionnage. Le paysage actuel des acteurs potentiels impliqués dans les cyberconflits est vaste, allant des activités de la campagne APT de CloudWizard dans la zone de conflit russo-ukrainien à une série de cyberattaques déclenchées par les récentes agressions liées au conflit israélo-Hamas. Il s'agit, par exemple, de

cyberattaques contre des organisations israéliennes des secteurs de l'énergie, de la défense et des télécommunications par une cybermenace basée à Gaza surnommé « Storm–1133 » (comme rapporté par Microsoft) et le ciblage des utilisateurs d'Android dans Israël avec une version piratée de l'application RedAlert - Rocket Alerts. Un groupe de pirates informatiques nommé Predatory Sparrow a refait surface au milieu du conflit en cours après près d'un an d'absence, selon les rapports de CyberScoop.

À l'avenir, nous anticipons une recrudescence des cyberattaques parrainées par des États à mesure que les tensions géopolitiques s'accentuent. Cela ne se limitera pas aux infrastructures critiques, aux secteurs gouvernementaux ou aux entreprises de défense du monde entier ; les organes de presse seront également de plus en plus menacés. Dans ce climat de tensions géopolitiques accrues, les organes médiatiques peuvent être choisis comme cibles par ceux qui cherchent à les utiliser à des fins de contre-propagande ou de désinformation.

Les pirates se concentreront principalement sur le vol de données, la destruction des infrastructures informatiques et l'espionnage à long terme. Les actions de cybersabotage devraient également se multiplier. Les attaquants ne se contenteront pas de chiffrer des données ; ils les détruiront, représentant une menace importante pour les organisations vulnérables aux attaques à des fins politiques. Enfin, dans le cadre des cyberconflits, il faut s'attendre à des attaques ciblées contre certains individus ou groupes, notamment des drones localisant les cibles, des logiciels malveillants utilisés pour les écoutes clandestines, etc.

Hacktivisme dans la cyberguerre : la nouvelle norme dans les conflits géopolitiques

L'« hacktivisme » constitue un autre exemple d'intégration numérique dans les conflits. Il est difficile d'imaginer un conflit futur sans l'implication de cyberactivistes. Les cyberactivistes peuvent influencer la cybersécurité de plusieurs manières. Premièrement, ils peuvent mener de véritables cyberattaques, notamment des attaques DDoS, voler ou détruire des données, effacer des sites Web, etc. Ensuite, les cyberactivistes peuvent faire de fausses déclarations de piratage, entraînant des enquêtes inutiles et une accoutumance aux alertes pour les analystes SOC et les chercheurs en cybersécurité. Par exemple, dans le conflit en cours entre Israël et le Hamas, un groupe de cyberactivistes a affirmé avoir attaqué la centrale électrique privée israélienne de Dorad début octobre. Bien que des recherches ultérieures révélèrent que les données publiées avaient déjà été divulguées par un autre groupe en juin 2022, il a fallu du temps et des ressources pour découvrir qu'aucune nouvelle fuite ne s'était produite. Des deepfakes sont également utilisés, des outils facilement accessibles utilisés pour usurper l'identité et diffuser de fausses informations, ainsi que d'autres cas très médiatisés, tels que des pirates informatiques interrompant les émissions de la télévision d'État iranienne durant des manifestations. Dans l'ensemble, alors que les tensions géopolitiques s'aggravent sans accalmie prévue à court terme, nous nous attendons à voir une recrudescence des activités hacktivistes, visant à la fois la destruction et la désinformation.

Il est difficile d'imaginer un conflit futur sans l'implication de cyberactivistes

Attaques de la chaîne d'approvisionnement en tant que service : accès aux achats groupés des opérateurs

Il existe une tendance croissante selon laquelle les pirates atteignent leurs objectifs par l'intermédiaire de fournisseurs, d'intégrateurs ou de développeurs. Cela signifie que les petites et moyennes entreprises, souvent dépourvues de protection solide contre les attaques APT, deviennent des passerelles permettant aux pirates informatiques d'accéder aux données et aux infrastructures des principaux acteurs, leurs cibles réelles. Pour illustrer l'ampleur des attaques contre les chaînes d'approvisionnement, telles que nous en sommes témoins aujourd'hui, on pourrait rappeler les fuites via Okta en 2022 et 2023. Cette société de gestion d'identité sert plus de 18 000 clients dans le monde, chacun d'entre eux pouvant potentiellement être compromis.

Les petites et moyennes entreprises deviennent des passerelles permettant aux pirates d'accéder aux données et aux infrastructures des principaux acteurs, leurs cibles réelles

Les mobiles derrière ces attaques peuvent varier, allant du gain financier au cyberespionnage, rendant cette menace encore plus préoccupante. Par exemple, le célèbre groupe APT Lazarus a perfectionné ses capacités d'attaque des chaînes d'approvisionnement. Ce qui est encore plus remarquable est la découverte que la célèbre porte dérobée Gopuram, déployée lors du tristement célèbre piratage de 3CX visant des victimes du monde entier, se trouve sur les machines des victimes aux côtés d'AppleJeus, une porte dérobée attribuée à Lazarus. Cette attaque était très ciblée et a montré un intérêt particulier dans les sociétés de cryptomonnaie, ce qui pourrait indiquer que le réel objectif des pirates était l'argent.

Alors que les attaques contre les chaînes d'approvisionnement par des pirates deviennent de plus en plus fréquentes, 2024 pourrait marquer le début d'une nouvelle phase dans les activités qui y sont liées. La tendance peut évoluer de diverses manières. Tout d'abord, des logiciels open source populaires pourraient être utilisés pour cibler des développeurs d'entreprise spécifiques. En outre, le marché noir pourrait introduire de nouvelles offres, notamment des packages d'accès ciblant des éditeurs de logiciels et fournisseurs de services informatiques. Par conséquent, ceux qui souhaitent orchestrer des attaques contre une chaîne d'approvisionnement, et ayant accès à un vaste pool de victimes potentielles, peuvent alors choisir leurs cibles avec soin pour lancer des attaques à grande échelle. Ce faisant, les pirates portent potentiellement l'efficacité des attaques sur une chaîne d'approvisionnement à un tout nouveau niveau.

Le phishing ciblé amené à se développer avec une IA générative accessible

Les chatbots et les outils d'IA générative sont désormais répandus et accessibles. Cette tendance n'est pas passée inaperçue auprès des pirates développant leurs propres chatbots black-hat basés sur des solutions légitimes. Par exemple, WormGPT, un modèle de langage explicitement conçu pour un usage malveillant, prétendait être basé sur le modèle de langage open source GPTJ. D'autres modèles, comme xxxGPT, WolfGPT, FraudGPT, DarkBERT et bien d'autres, ne disposent pas des restrictions de contenu présentes dans les solutions légitimes, ce qui les rend attrayants pour les pirates qui exploitent ces modèles à des fins malveillantes.

Au cours de l'année à venir, les pirates devraient concevoir de nouvelles méthodes pour automatiser l'espionnage de leurs cibles

L'émergence de ces outils facilitera probablement la production massive de messages de phishing ciblés, servant souvent de première étape à l'APT et à d'autres attaques. L'importance va au-delà de la capacité de rédiger rapidement des messages convaincants et bien écrits. Cela comprend également la possibilité de générer des documents destinés à usurper l'identité et d'imiter le style d'individus spécifiques, tels qu'un partenaire commercial ou le collègue d'une victime. Au cours de l'année à venir, les pirates devraient concevoir de nouvelles méthodes pour automatiser l'espionnage de leurs cibles. Cela peut inclure la collecte automatique de données provenant de la présence en ligne de la victime, telles que les publications sur les réseaux sociaux, les commentaires dans les médias ou des colonnes rédigées : tout contenu associé à l'identité de la victime. Ces informations seront ensuite traitées à l'aide d'outils génératifs pour concevoir des messages texte ou audio avec le style et la voix de l'individu en question.

Dans le même temps, l'importance de la sensibilisation à la cybersécurité et des mesures préventives, notamment les renseignements sur les menaces, ainsi qu'une surveillance et une détection proactives, continuera de croître.

Apparition de nombreux groupes proposant des services de hacking

Les groupes de hackers mercenaires (ou « hack-for-hire ») se spécialisent dans l'infiltration de systèmes et proposent des services de vol de données. Leur clientèle comprend des détectives privés, des cabinets d'avocats, des concurrents et ceux qui ne possèdent pas les compétences techniques nécessaires pour conduire de telles attaques. Ces cybermercenaires font ouvertement la publicité de leurs services et ciblent les entités d'intérêt.

L'un de ces groupes, suivi par notre équipe mondiale de recherche et d'analyse (GReAT), est DeathStalker. Il se concentre sur les cabinets d'avocats et les sociétés financières, fournissant des services de piratage et agissant comme un courtier d'informations plutôt que d'opérer comme une APT traditionnelle. Ils utilisent des e-mails de phishing ciblé contenant des pièces jointes malveillantes pour prendre le contrôle des appareils des victimes et voler des données sensibles.

Ces groupes sont constitués de hackers expérimentés, organisés, avec des responsables gérant leurs propres équipes. Ils font de la publicité sur les plateformes du Dark Web et emploient diverses techniques, notamment des logiciels malveillants, du phishing et d'autres méthodes d'ingénierie sociale. Ils s'adaptent pour éviter d'être détectés en utilisant des communications anonymes et des VPN, et en provoquant divers incidents, allant des fuites de données aux atteintes à la réputation. Les services des groupes de hackers mercenaires vont généralement au-delà du cyberespionnage et s'étendent à l'espionnage commercial. Ils peuvent recueillir des données sur des concurrents, par exemple sur les transactions de fusions et acquisitions, les plans d'expansion, les données financières et les informations sur les clients.

Cette approche prend de l'ampleur au niveau mondial et nous prévoyons qu'elle évoluera au cours de l'année à venir. Il est possible que certains groupes APT étendent leurs opérations en raison de la demande pour de tels services, car ils ont besoin de générer des revenus pour soutenir leurs activités et rémunérer leurs agents.

Les systèmes MFT à l'avant-garde des cybermenaces

À mesure que le paysage numérique continue d'évoluer, la complexité et la sophistication des cybermenaces changent également

À mesure que le paysage numérique continue d'évoluer, la complexité et la sophistication des cybermenaces changent également. Les systèmes de transfert de fichiers gérés (MFT) se trouvent au cœur de cette évolution, étant conçus pour transporter en toute sécurité des données sensibles entre des organisations. Abritant une multitude d'informations confidentielles, notamment la propriété intellectuelle, les dossiers financiers et les données clients, les solutions MFT sont devenues indispensables dans les opérations commerciales modernes. Elles facilitent un partage fluide des données aussi bien en interne qu'en externe, devenant ainsi la pierre angulaire d'une organisation plus efficace. Cependant, ce rôle central les place également dans la ligne de mire des cyberadversaires, en particulier des auteurs de ransomwares, cherchant sans relâche à exploiter les vulnérabilités numériques à des fins d'extorsion.

Les incidents impliquant des systèmes MFT, tels que MOVEit et GoAnywhere, en 2023, ont mis en lumière les possibles failles de ces conduits de transfert de données critiques. La fuite MOVEit orchestrée par le groupe de ransomwares Cl0p et l'exploitation de la plateforme GoAnywhere MFT de Fortra ont mis en évidence comment une seule vulnérabilité pouvait être exploitée pour exfiltrer des données sensibles, perturber le fonctionnement et exiger une rançon.

À l'avenir, les menaces affectant les systèmes MFT sont sur le point de s'intensifier. L'attrait du gain et la possibilité de provoquer des perturbations opérationnelles importantes entraîneront probablement une recrudescence des attaques ciblées contre des systèmes MFT. L'architecture complexe des systèmes MFT, associée à leur intégration dans des réseaux d'entreprise plus larges, abrite potentiellement des failles de sécurité susceptibles d'être exploitées. À mesure que les cyberadversaires continuent de perfectionner leurs compétences, l'exploitation des vulnérabilités des systèmes MFT devrait devenir un vecteur de menace plus important.

L'évolution des cybermenaces ciblant les systèmes MFT souligne une réalité : le nombre de fuites de données et d'extorsion financière importantes possibles continuera d'augmenter. Les incidents de 2023 nous rappellent brutalement les vulnérabilités inhérentes aux systèmes MFT et la nécessité urgente de prendre des mesures de cybersécurité robustes pour protéger ces canaux de transfert de données critiques.

L'exposé de 2023 est un appel clair aux organisations pour qu'elles renforcent leur appareil de cybersécurité autour des systèmes MFT

À la lumière de cela, il est fortement conseillé aux organisations d'entreprendre des examens complets de leurs solutions MFT afin d'identifier et de réduire les possibles failles de sécurité. La mise en œuvre de solutions robustes de prévention des pertes de données (DLP), le chiffrement des données sensibles et le renforcement de la sensibilisation à la cybersécurité sont des étapes avisées pour renforcer les systèmes MFT contre les cybermenaces émergentes. À mesure que l'horizon des cybermenaces continue de s'élargir, des mesures proactives de cybersécurité englobant les systèmes MFT seront primordiales pour protéger les données des organisations et garantir une résilience opérationnelle face à l'évolution des cybermenaces.

L'exposé de 2023 est un appel clair aux organisations pour qu'elles renforcent leur appareil de cybersécurité autour des systèmes MFT. Alors que nous avançons dans un avenir où les cybermenaces sont vouées à devenir plus perfectionnées, il incombe aux organisations de garder une longueur d'avance, en garantissant l'intégrité et la sécurité de leurs systèmes MFT afin de contrecarrer les intentions néfastes de leurs cyberadversaires.

En 2024, cette tendance devrait se poursuivre avec l'adoption probable du CRA et l'adoption par davantage de pays de mesures réglementaires pour garantir la cybersécurité des chaînes d'approvisionnement.

Telles sont nos prédictions pour l'année 2024. Dans un an, nous verrons lesquels se sont concrétisés et lesquels ne l'ont pas été.

Actualités sur les cybermenaces :
www.securelist.fr
Actualités dédiées à la sécurité informatique :
business.kaspersky.com

www.kaspersky.fr