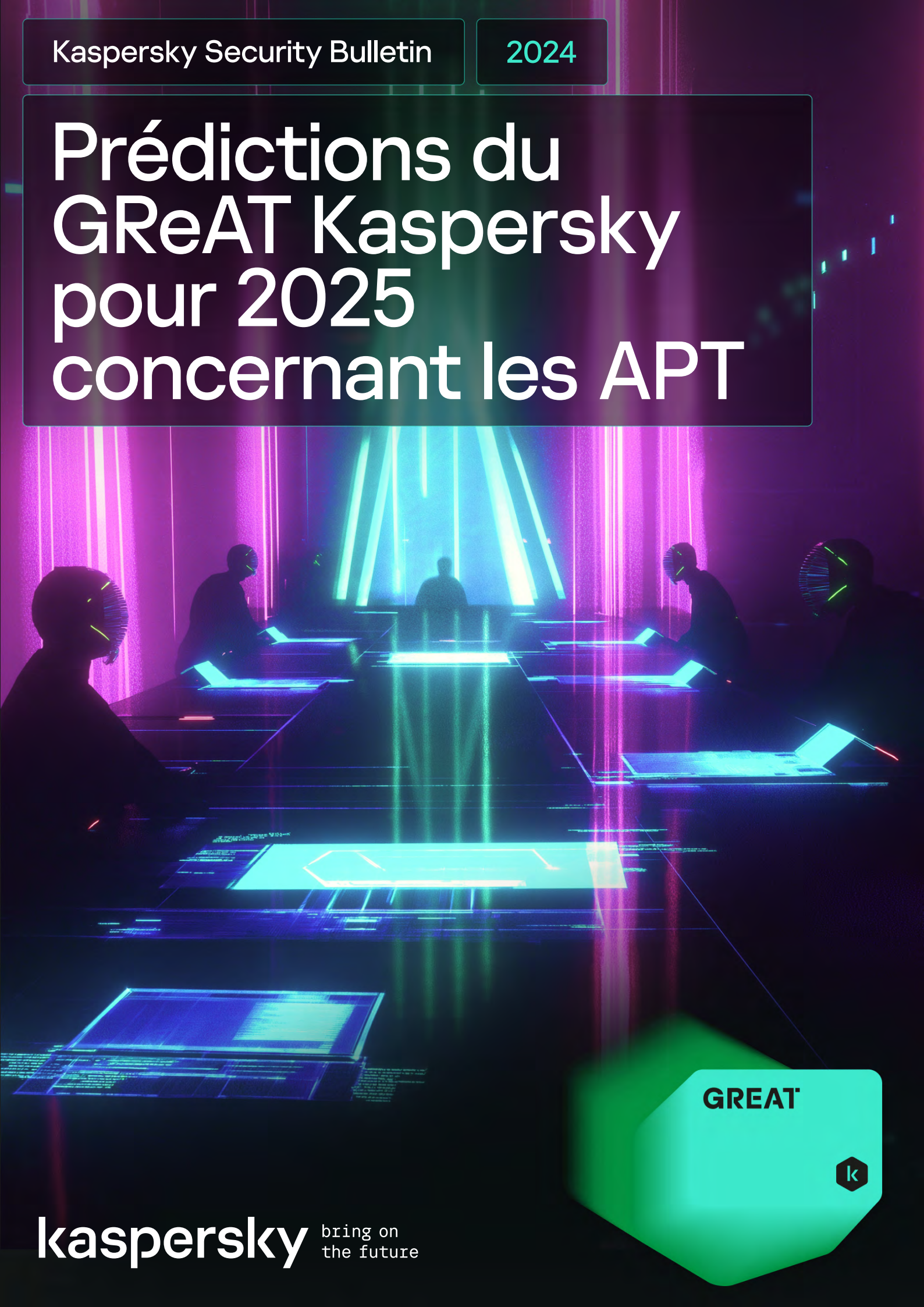
Kaspersky Security Bulletin 2024

Prédictions du GReAT Kaspersky pour 2025 concernant les APT



kaspersky bring on the future

Prédictions du GReAT Kaspersky pour 2025 concernant les APT

Auteurs : Igor Kuznetsov, Giampaolo Dedola, Georgy Kucherin, Maher Yamout, Vasily Berdnikov, Isabel Manjarrez, Ilya Savelev, Joao Godinho

L'équipe Global Research and Analysis (GReAT) de Kaspersky surveille plus de 900 opérations et groupes de menaces persistantes avancées (APT). À la fin de chaque année, nous prenons du recul afin d'évaluer les attaques les plus complexes et les plus sophistiquées qui ont façonné le paysage des menaces au cours de l'année écoulée. Ces informations nous permettent d'anticiper les nouvelles tendances et d'avoir une vision plus claire du paysage des APT pour l'année à venir.

Dans ce premier numéro de la série Kaspersky Security Bulletins, nous passerons en revue les tendances de l'année écoulée, nous réfléchirons aux prédictions que nous avions faites pour 2024, et nous donnerons un aperçu de ce à quoi nous pouvons nous attendre pour 2025.

Les acteurs de menaces ciblées s'intéressent de plus en plus à l'exploitation des vulnérabilités des composants matériels des appareils mobiles

Examen des prévisions faites l'année dernière

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

Notre découverte de l'Opération Triangulation au cours de l'année dernière a mis en lumière une chaîne d'attaque unique impliquant des exploits pour les appareils Apple, y compris ceux fonctionnant sous iOS et watchOS. Ces exploits s'appuyaient sur de multiples vulnérabilités impliquant des modules comme WebKit et le noyau XNU, ainsi que le processeur Apple.

En 2024, comme nous nous y attendions, nous avons continué à observer des attaques impliquant des exploits pour les appareils Apple. À titre d'exemple, en janvier, Apple a signalé que CVE-2024-23222, une vulnérabilité d'exécution de code à distance dans le moteur de navigation de Safari, pouvait avoir été utilisée dans le cadre de cyberattaques. De plus, cet automne, Apple a dévoilé deux autres exploits ayant très probablement été exploités : CVE-2024-23225 pour le noyau XNU, et CVE-2024-23296 pour RTKit.

Quant aux appareils Android, ils restent également des cibles de choix pour les acteurs de menaces sophistiquées. En novembre, Google a en effet publié des informations sur deux vulnérabilités « pouvant faire l'objet d'une exploitation limitée et ciblée » : CVE-2024-43093 et CVE-2024-43047. Il est intéressant de noter que cette dernière vulnérabilité, tout comme l'un des exploits utilisés dans le cadre de l'Opération Triangulation, exploite une faille liée à un processeur matériel. Comme nous pouvons le constater, les acteurs de menaces ciblées s'intéressent de plus en plus à l'exploitation des vulnérabilités des composants matériels des appareils mobiles.

Verdict : prédiction confirmée ✔

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

La communauté internationale de la cybersécurité a commencé à déployer des efforts considérables afin de perturber les serveurs de commande et de contrôle, ce qui rend plus difficile pour les acteurs de la menace (y compris les acteurs de menaces avancées) de mener des activités malveillantes depuis leur infrastructure pendant de longues périodes. Afin de contrer les efforts de ces chercheurs, plusieurs acteurs de menaces avancées ont récemment commencé à créer leurs propres réseaux de botnets et à exploiter ces derniers pour mener à bien des cyberattaques.

À titre d'exemple, en janvier de cette année, le gouvernement américain a démantelé un botnet constitué de routeurs Ubiquiti Edge OS compromis et exploités par l'acteur de la menace Sofacy (dit APT28). Les appareils ont d'abord été infectés par Moobot, un programme malveillant basé sur Mirai, qui a ensuite été utilisé pour déployer des scripts supplémentaires et faciliter des attaques ciblées contre diverses entités, recueillir des identifiants, établir un trafic réseau par proxy, créer des tunnels SSH inversés, héberger des pages d'accueil usurpées, et contrôler d'autres systèmes distants infectés par une porte dérobée en Python.

De plus, en 2024, nous avons constaté que de nombreux acteurs sinophones exploitaient des réseaux de botnets pour mener des attaques ciblées. L'un de ces botnets est Quad7, qui a été installé sur des routeurs compromis par l'acteur Storm-0940 afin de procéder à des pulvérisations de mots de passe. Un autre exemple observé cette année est le site KV-Botnet, qui a été déployé sur des pare-feux, des routeurs et des caméras IP vulnérables et exploité afin de dissimuler les activités malveillantes de Volt Typhoon, acteur à l'origine du site.

Verdict : prédiction confirmée ✔

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

Lorsqu'un acteur de la menace réussit à s'introduire dans une machine, il cherche toujours à accroître autant que possible ses privilèges. Plus précisément, l'un des privilèges que les acteurs d'attaques ciblées souhaitent souvent obtenir est l'accès au noyau. Cela permet aux acteurs de la menace de désactiver ou d'altérer les solutions de sécurité, ainsi que d'installer des outils de rootkit afin de mener leurs activités malveillantes en toute discrétion.

En 2024, la technique BYOVD (« bring your own vulnerable driver ») est restée la technique la plus populaire pour accéder au noyau, et a même été plus largement utilisée que les années précédentes. À titre d'exemple, au deuxième trimestre 2024, nous avons constaté une augmentation de 23 % de l'utilisation de la technique BYOVD. Cette augmentation est très probablement due au fait qu'il n'existe à ce jour aucune méthode efficace intégrée aux systèmes d'exploitation pour lutter contre cette technique. Bien que Windows mette en œuvre une liste de blocage des pilotes (drivers) vulnérables, celle-ci est rarement mise à jour (1 à 2 fois par an seulement), ce qui facilite grandement la tâche des acteurs qui exploitent les pilotes vulnérables connus.

Cependant, certaines solutions de sécurité tentent de mettre en œuvre des mécanismes pour empêcher l'exploitation des pilotes vulnérables, obligeant les acteurs de la menace à s'adapter en trouvant des vulnérabilités dans les pilotes Windows déjà installés sur l'appareil susceptibles d'être exploitées afin de mener des opérations dans l'espace du noyau. À titre d'exemple, cette année, Lazarus a exploité CVE-2024-21338, une vulnérabilité dans le pilote AppLocker, afin de déployer le rootkit FudModule.

Verdict : prédiction confirmée ✔

Cette année, nous avons observé une augmentation de 25 % des détections d'attaques APT entre janvier et juin

Augmentation des cyberattaques perpétrées par des groupes commandités par des États

Année après année, nous observons un nombre croissant d'attaques perpétrées par des acteurs de menaces sophistiquées, et 2024 n'a pas fait exception à la règle. À titre d'exemple, cette année, nous avons observé une augmentation de 25 % des détections d'attaques APT entre janvier et juin. Tout au long de l'année, nous avons couvert les attaques les plus intéressantes sur notre blog.

De plus, nous avons constaté que les acteurs de menaces sophistiquées augmentaient non seulement le nombre de leurs campagnes, mais également la qualité de ces dernières. C'est notamment le cas de l'APT Lazarus, et plus particulièrement de ses attaques contre les investisseurs en cryptomonnaies menées au mois de mai.

Ces attaques ont été extrêmement bien orchestrées ; pour les mener à bien, Lazarus a volé le code source d'un jeu informatique lié aux cryptomonnaies, a promu des comptes de réseaux sociaux liés à ce jeu, et a obtenu l'accès à une chaîne unique d'exploits de type zero-day utilisée pour infecter les cibles visitant le site Internet du jeu. Toutes ces activités ont dû nécessiter des mois de travail de la part de cet acteur, ce qui témoigne d'un degré d'organisation exceptionnel.

Verdict : prédiction confirmée ✔

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

Comme nous l'avions prédit, nous avons observé cette année une augmentation des attaques de la part de groupes hacktivistes, en particulier ceux qui opèrent dans le cadre des conflits russo-ukrainien et Israël-Hamas. Dans le cas du conflit russo-ukrainien, les groupes hacktivistes notables que nous avons recensés incluent Twelve, Head Mare et Crypt Ghouls. D'une manière générale, nous avons observé que les hacktivistes du conflit russo-ukrainien sont devenus plus compétents et se sont davantage concentrés sur le fait d'attaquer de grandes structures comme les entités gouvernementales, industrielles et énergétiques. En se concentrant sur de telles cibles, les groupes d'hacktivistes rendent les conséquences de leurs attaques plus visibles pour les citoyens ordinaires.

Nous avons également observé le même type d'activité de la part des hacktivistes opérant dans le cadre du conflit entre Israël et le Hamas. À titre d'exemple, une attaque récente observée dans ce contexte a été une attaque DDoS visant le système de paiement par carte de crédit d'Israël. Ce qui est particulièrement intéressant concernant les cyberattaques relatives à ce conflit, c'est que leur cible s'est étendue bien au-delà de la zone de conflit. À titre d'exemple, cette année, le groupe hacktiviste pro-palestinien BlackMeta a attaqué le site Internet Archive, qui n'a rien à voir avec le conflit.

Verdict : prédiction confirmée ✔

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

Cette année, nous n'avons pas observé d'attaques contre la chaîne d'approvisionnement ayant causé des dommages importants à leurs cibles. Cependant, une attaque contre la chaîne d'approvisionnement particulièrement notable au cours de l'année 2024 a été l'attaque par backdoor de XZ Utils, que nous avons abordée dans un article de blog en trois parties. Étant donné que cette backdoor affectait plusieurs distributions Linux populaires, les conséquences de cette attaque auraient été bien pires si elle n'avait pas été repérée par la communauté. Nous aurions pu assister à une vente des accès aux réseaux des entreprises compromises à des acteurs de menaces avancées.

Verdict : prédiction non confirmée ✖

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

Depuis l'émergence de l'IA générative, de nombreux acteurs de la menace, qu'ils soient motivés par des raisons financières ou soutenus par des États, ont commencé à exploiter cette technologie pour rendre leurs attaques plus efficaces. Cela vaut tout particulièrement pour les attaques de phishing, car les outils d'IA générative sont désormais capables de créer des emails de phishing bien rédigés et correctement imagés.

Un cas notable d'utilisation de l'IA dans le cadre d'une campagne ciblée a été l'attaque infructueuse de l'entreprise KnowBe4, dans laquelle un pirate informatique censé appartenir au groupe de menace Lazarus a utilisé l'IA pour tromper le service des ressources humaines dans le cadre d'une candidature à un poste. À titre d'exemple, dans le cadre de cette candidature, le pirate informatique a utilisé une photo d'archive manipulée à l'aide d'outils d'IA afin de la rendre plus crédible. Avec l'aide de l'IA, il a réussi à tromper l'entreprise, à obtenir le poste et à accéder au réseau interne de l'entreprise ; cependant, les tentatives de piratage ultérieures ont été rapidement repérées par le SOC de l'entreprise.

Verdict : prédiction confirmée ✔

Apparition de nombreux groupes proposant des services de hacking

Si nous avons vu de nouveaux groupes proposant des services de piratage apparaître dans le monde des crimewares, nous n'avons pas observé de nouveaux acteurs notables de la menace motivés par des considérations commerciales et menant des cyberattaques sophistiquées similaires à celles couramment perpétrées par les APT.

Verdict : prédiction non confirmée ✖

Les systèmes MFT à l'avant-garde des cybermenaces

L'année dernière, des incidents impliquant des systèmes MFT comme MOVEit et GoAnywhere ont causé de sérieux dommages aux entreprises compromises. Bien que ces attaques aient eu lieu il y a un an, leur impact sur les entreprises concernées se fait encore sentir aujourd'hui. À titre d'exemple, il y a quelques jours, des données personnelles liées à des employés d'Amazon, qui auraient fuité au cours de l'attaque de la vulnérabilité MOVEit, ont été divulguées sur un forum de cybercriminalité.

Cette année, la communauté de la cybersécurité a également découvert plusieurs vulnérabilités dans les systèmes MFT (Managed File Transfer) qui sont exploitées sur le terrain. L'une d'entre elles est CVE-2024-0204, qui permet aux pirates informatiques de contourner l'authentification dans le système MFT GoAnywhere. Un autre exemple est CVE-2024-5806, une vulnérabilité similaire dans MOVEit Transfer. Cependant, cette année, la communauté de la cybersécurité était bien mieux armée pour contrer les attaques contre les systèmes MFT, de sorte que les conséquences des attaques impliquant ces vulnérabilités n'ont pas été aussi dramatiques que l'année dernière.

Verdict : prédiction **partiellement** confirmée ✔

Prédictions des menaces persistantes avancées pour 2025

L'hacktivisme s'est renforcé grâce à cette stratégie, et nous pouvons donc nous attendre à voir des campagnes mieux organisées et plus influentes à l'avenir

Les alliances hacktivistes se multiplieront en 2025

Ces dernières années, les groupes d'hacktivistes ont commencé à lier étroitement leurs opérations à des conflits sociopolitiques. Alors que leurs premiers efforts visaient principalement à attirer l'attention du public, nous les voyons aujourd'hui poursuivre des objectifs plus substantiels ayant un impact sur le monde réel, comme le ciblage des systèmes GNSS (Global Navigation Satellite Systems).

Cette année, nous avons vu l'hacktivisme évoluer, avec des groupes formant des alliances et créant des forums aux motivations communes. Ces alliances ne se limitent pas aux conflits militaires ; en guise d'exemple, nous pouvons citer la formation de la « Holy League », qui prétend réunir 70 groupes de pirates informatiques actifs. Des alliances hacktivistes émergent également en réponse à des événements ponctuels, comme lorsque des hacktivistes se sont unis pour dégrader des sites Internet français en réponse à l'arrestation du PDG de Telegram, Pavel Durov.

Si un objectif commun peut unir et motiver des actes malveillants, le partage d'outils et d'infrastructures constitue également un élément important de ces alliances, permettant d'atteindre des objectifs encore plus ambitieux.

L'hacktivisme s'est renforcé grâce à cette stratégie, et nous pouvons donc nous attendre à voir des campagnes mieux organisées et plus influentes à l'avenir, qui pourraient même inclure le déploiement de ransomwares. Dans certains cas, les attaques des hacktivistes peuvent révéler un manque de fonds alloués à la sécurité des structures qu'ils attaquent.

L'IoT deviendra un vecteur d'attaque croissant pour les APT en 2025

La multiplication rapide des appareils IoT, qui devraient passer de 18 milliards aujourd'hui à 32 milliards d'ici 2030, implique des défis à la fois en matière d'innovation et en matière de renforcement de la sécurité. À mesure que les appareils intelligents de type caméras, interrupteurs et prises de courant se généralisent, une multitude de nouvelles connexions à Internet apparaît, chacune d'entre elles présentant des vulnérabilités potentielles.

De nombreux appareils IoT sont contrôlés par des serveurs distants, mais les pratiques de sécurité des entreprises qui gèrent ces serveurs sont souvent floues, ce qui a pour conséquence de créer de nouveaux vecteurs d'attaque potentiels sur leur infrastructure. De plus, les appareils IoT fonctionnent souvent sur des systèmes intégrés dotés de micrologiciels qui peuvent être facilement analysés pour y déceler des vulnérabilités. De nombreux appareils plus anciens reposent sur des bibliothèques obsolètes présentant des failles de sécurité connues, ce qui les expose à un risque d'exploitation.

La multiplication des applications mobiles permettant de contrôler ces appareils accroît encore les risques. Avec autant d'applications disponibles, il est difficile de vérifier la légitimité de chacune d'entre elles, ce qui permet aux pirates informatiques de diffuser de fausses applications pour prendre le contrôle d'appareils IoT. Les risques liés à la chaîne d'approvisionnement constituent également une source d'inquiétude ; des acteurs malveillants peuvent implanter des programmes malveillants au cours du processus de fabrication, comme cela a déjà été observé pour certains boîtiers de télévision Android.

Le principal problème est l'absence de contre-mesures. Les équipes de défense travaillent presque à l'aveugle, n'ayant aucune visibilité sur ces appareils. Par rapport à l'année dernière, la situation ne s'est pas améliorée, et nous ne pouvons que nous attendre à ce que les pirates informatiques continuent à tirer parti du grand nombre d'appareils non protégés.

S'il se peut que le nombre d'attaques contre la chaîne d'approvisionnement ne progresse pas, il est certain que nous assisterons à une augmentation du nombre de découvertes de telles attaques

Les attaques contre la chaîne d'approvisionnement des projets open source progresseront

L'une des campagnes les plus marquantes de cette année a été l'attaque par backdoor de XZ, un outil de compression open source largement utilisé dans des distributions Linux populaires. Les pirates informatiques ont eu recours à des techniques d'ingénierie sociale afin d'obtenir un accès permanent à l'environnement de développement des logiciels et sont passés inaperçus pendant des années. Cette affaire met en évidence certains aspects critiques de l'écosystème actuel des logiciels open source, dans lequel de nombreux projets importants sont administrés simplement par une poignée de développeurs (ou parfois même par un seul développeur), qui sont souvent incapables de se défendre contre des groupes d'APT sophistiquées soutenus par des États.

Si l'affaire de XZ n'a rien de surprenant, elle met en lumière un problème réel. Elle a ainsi attiré l'attention de la communauté de la cybersécurité et de divers autres organismes, qui chercheront probablement à améliorer la surveillance de leurs projets open source. S'il se peut que le nombre d'attaques contre la chaîne d'approvisionnement ne progresse pas, il est certain que nous assisterons à une augmentation du nombre de découvertes d'attaques existantes contre la chaîne d'approvisionnement.

Les programmes malveillants C++ et Go s'adapteront à l'écosystème des logiciels open source

Les projets open source adoptant de plus en plus les dernières versions de C++ et Go, les acteurs de la menace devront adapter leurs programmes malveillants à ces langages largement répandus. En 2025, nous pouvons nous attendre à une augmentation significative des groupes d'APT et des cybercriminels qui migreront vers ces langages, tirant parti de leur présence croissante dans les projets open source.

Alors que les autres langages de programmation continueront à être moins utilisés, C++ et Go deviendront les langages les plus courants pour le développement de programmes malveillants, les pirates informatiques exploitant les forces et les vulnérabilités de ces langages afin d'infiltrer les systèmes et de contourner les défenses de sécurité.

Nous pensons que l'utilisation des LLMs deviendra une pratique courante pour les pirates informatiques, de la même façon que les équipes de défense intègrent de plus en plus l'IA et les outils de machine learning à leurs stratégies de cybersécurité

L'utilisation de l'IA par des acteurs affiliés à des États progressera

L'année dernière, nous avions prédit que les groupes d'APT exploiteraient l'IA pour améliorer leurs attaques de phishing ciblé. Depuis, OpenAI a déclaré avoir clôturé des comptes liés à des acteurs de la menace affiliés à des États, mettant en évidence comment les groupes APT (Advanced Persistent Threat) utilisent déjà des modèles de langage de grande taille (LLM) pour des attaques de spear-phishing, la traduction de texte, la génération de scripts et la recherche en source ouverte afin de créer du contenu plus ciblé. Notre découverte la plus récente a révélé que Lazarus utilisait des images générées par IA pour promouvoir un faux site de jeu qui exploitait une vulnérabilité de type zero-day de Chrome, dans le but de voler de la cryptomonnaie.

Nous pensons que l'utilisation des LLMs (modèles de langage de grande taille) deviendra une pratique courante pour les pirates informatiques, de la même façon que les équipes de défense intègrent de plus en plus l'IA et les outils machine learning à leurs stratégies de cybersécurité. Les pirates informatiques utiliseront probablement les LLMs à des fins de reconnaissance, ces derniers pouvant automatiser le processus d'identification de vulnérabilités et de collecte d'informations sur des technologies spécifiques, permettant ainsi aux pirates informatiques de trouver plus facilement les points faibles de leurs cibles. Ils s'appuieront davantage sur l'IA pour créer des scripts malveillants et générer des commandes lors des activités de post-exploitation, afin d'augmenter leurs chances de réussite.

Les pirates informatiques tenteront sans doute également de dissimuler leurs activités à des entreprises comme OpenAI en créant des LLMs locaux ou en masquant leur comportement sur les plateformes publiques, par exemple en recourant à plusieurs comptes, en faisant preuve de prudence au niveau de leurs entrées et en limitant les données partagées avec des plateformes d'entreprise comme Google, OpenAI, Microsoft, etc.

Des deepfakes seront utilisés par les groupes d'APT

Une attention particulière doit être accordée à la multiplication des deepfakes, qui évoluent rapidement et présentent des risques importants. Jusqu'à présent, nous avions tendance à considérer les vidéos, les images et les voix comme des sources d'information fiables. Cependant, à mesure que la technologie des deepfakes s'améliore et devient plus accessible, cette confiance est de plus en plus remise en question. En 2024, des deepfakes ont été utilisés dans le cadre d'escroqueries très médiatisées, par exemple lorsque la voix d'un PDG a été imitée et associée à des séquences YouTube lors d'appels vidéo afin de tromper ses employés, ou lorsque diverses vidéos et autres séquences accessibles publiquement ont été exploitées pour créer une nouvelle fausse vidéo afin de tromper un employé d'une entreprise de Hong Kong et de l'amener à effectuer un virement d'environ 25,5 millions de dollars.

La raison pour laquelle ces attaques sont si efficaces tient à la psychologie humaine : en effet, lorsqu'une personne entend une voix qu'elle reconnaît, elle fait instinctivement confiance au message. Par le passé, l'usurpation d'identité vocale n'était pas considérée comme une menace majeure, ce qui explique pourquoi ces escroqueries peuvent être si convaincantes. Cependant, l'avènement des technologies de l'IA a complètement changé la donne. Aujourd'hui, grâce à de nouveaux services, il est possible de générer de fausses vidéos et de faux enregistrements vocaux à partir de quelques échantillons réels, qui peuvent être facilement récupérés sur des profils de réseaux sociaux ou par le biais d'autres méthodes de reconnaissance.

Si les cybercriminels ont déjà utilisé le clonage de voix par IA dans le cadre d'escroqueries, nous nous attendons à ce que les APT intègrent de plus en plus cette technologie à leur boîte à outils pour usurper l'identité de personnes importantes, en créant des messages ou des vidéos très crédibles afin de tromper des employés, de voler des informations confidentielles ou de mener d'autres activités malveillantes.

À mesure que les pirates informatiques deviennent plus habiles pour exploiter les vulnérabilités de faible niveau, la complexité de ces attaques est susceptible d'augmenter, et nous pourrions voir apparaître des techniques encore plus sophistiquées

Modèles d'IA avec Backdoor

L'adoption généralisée des modèles d'IA par les entreprises de divers secteurs fait de ces modèles une cible de plus en plus attrayante pour les cybercriminels et les acteurs de la menace soutenus par des États. La large diffusion de modèles d'IA open source et perfectionnés augmente le risque de voir ces modèles attaqués par un cheval de Troie (Trojan) ou par une Backdoor.

En 2025, nous verrons très probablement des groupes d'APT cibler des modèles et des ensembles de données d'IA open source populaires, en y introduisant du code malveillant ou des biais qui pourraient être difficiles à détecter et largement partagés.

Les exploits BYOVD (« bring your own vulnerable driver ») seront de plus en plus présents dans les campagnes d'APT

Comme nous l'avons déjà mentionné, la technique BYOVD (« bring your own vulnerable driver ») est devenue une tendance en 2024. Cette technique permet aux pirates informatiques d'exploiter des vulnérabilités des pilotes (drivers) afin d'accéder à des privilèges, de contourner les mesures de sécurité et de déployer des charges utiles sophistiquées dans le cadre de campagnes de ransomwares et d'attaques APT.

Les pilotes (drivers) jouent un rôle essentiel dans la communication entre le matériel et les logiciels, mais ils peuvent également servir de passerelle puissante pour les pirates informatiques, en particulier lorsqu'ils sont exploités au niveau du noyau. Les pilotes vulnérables permettent aux pirates informatiques d'exécuter du code malveillant avec des niveaux de privilèges élevés, ce qui peut conduire sur le long terme à un espionnage, à un vol de données et à une infiltration des réseaux. Bien que certains fournisseurs de solutions de sécurité mettent en œuvre divers mécanismes pour empêcher ces attaques, leur sophistication est difficile à contrer par des mesures de sécurité traditionnelles. Ces pilotes sont des logiciels légitimes qui peuvent être nécessaires pour faciliter le fonctionnement normal du système, ce qui rend difficile la distinction entre leur utilisation légitime et leur utilisation malveillante. Il n'est pas non plus facile de s'assurer qu'ils sont utilisés uniquement à des fins légitimes.

Cette tendance devrait se poursuivre en 2025. À mesure que les pirates informatiques deviennent plus habiles pour exploiter les vulnérabilités de faible niveau, la complexité de ces attaques est susceptible d'augmenter, et nous pourrions voir apparaître des techniques encore plus sophistiquées, comme l'exploitation de pilotes obsolètes ou tiers qui ne sont généralement pas soumis à un examen minutieux en vue d'y déceler des failles de sécurité.