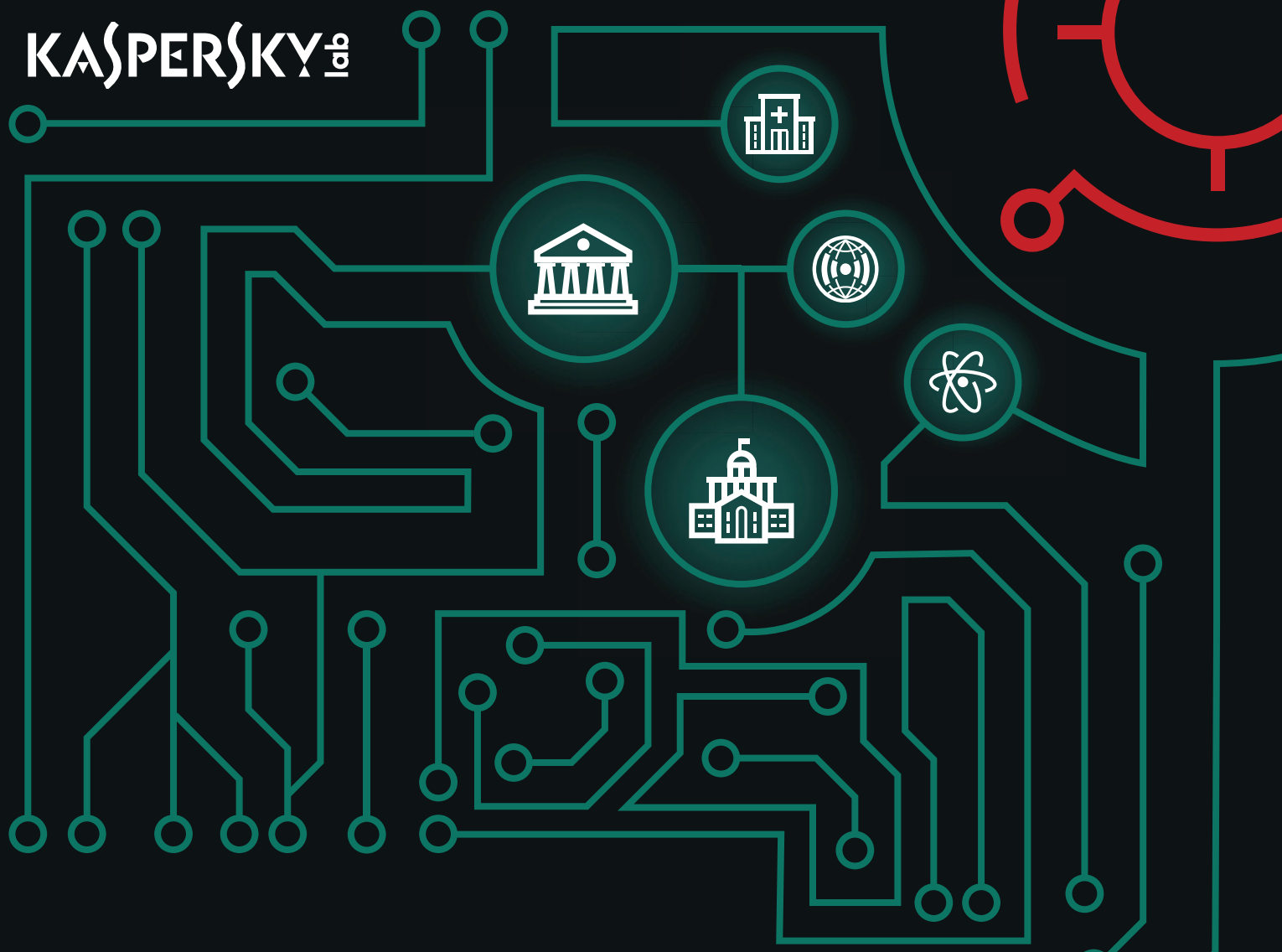
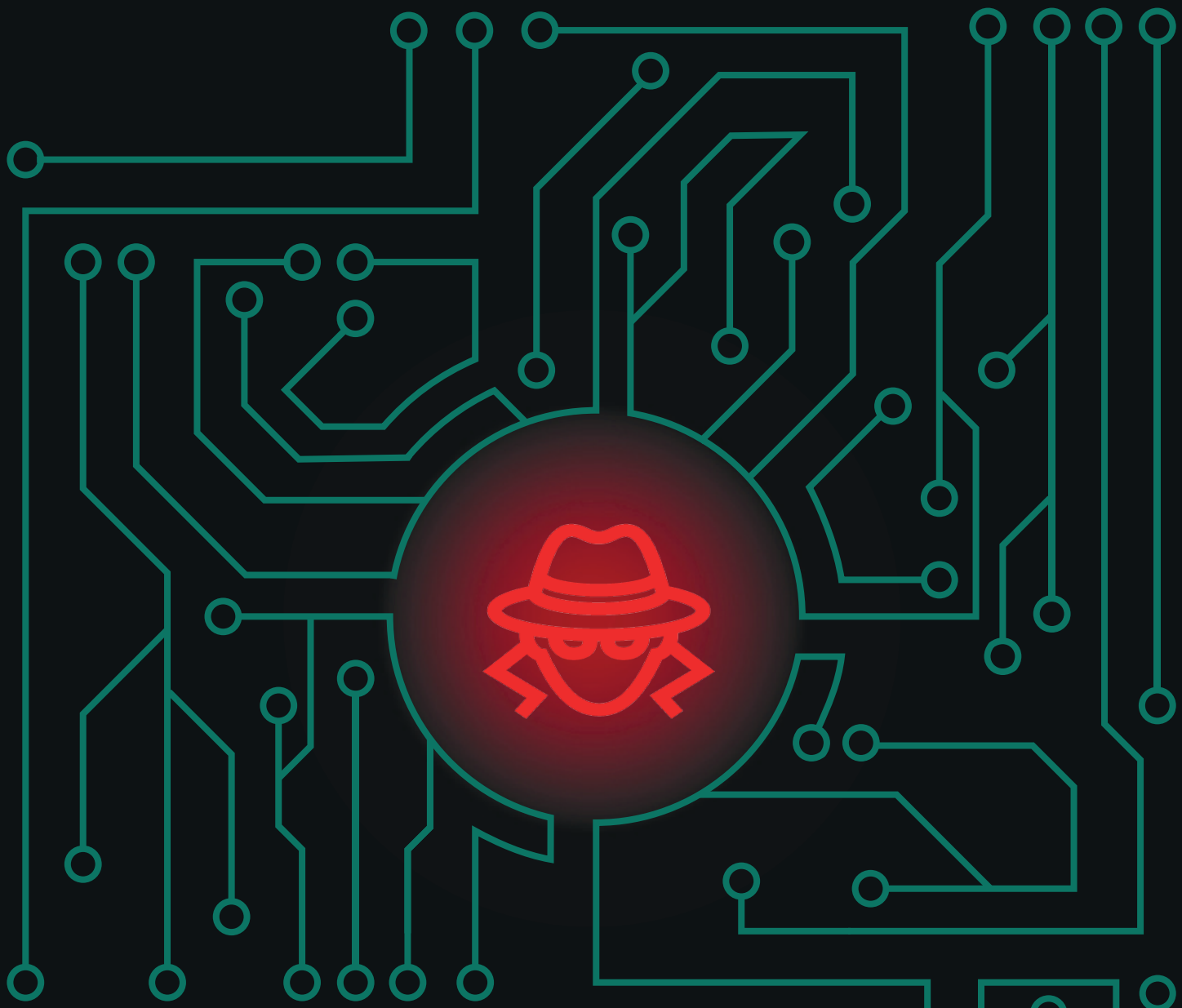
KASPERSKY lab



Kaspersky Security Bulletin

BILAN DE L'ANNÉE 2017

TABLE DES MATIÈRES



UNE ANNÉE AUX CONTOURS FLOUS

David Emm
Principal Security Researcher
Équipe Global Research and Analysis (GReAT)

INTRODUCTION

Les technologies connectées sont partout, elles font partie intégrante de nos vies et offrent aux cybercriminels une surface d'attaque toujours plus grande. Partout dans le monde, les entreprises et les particuliers sont de plus en plus ciblés par les cybercriminels en quête d'argent, de données, ou cherchant à perturber, causer des dégâts physiques, nuire à une réputation ou tout simplement « s'amuser ». L'écosystème des cybermenaces s'est construit, évolue depuis des années et notre bilan annuel des tendances et des incidents de sécurité les plus importants fait partie de cette chronologie qui ne s'arrête jamais.

Le fait le plus marquant de cette année 2017 est la disparition progressive des frontières, les limites traditionnelles entre les différents types de menaces et les différents types de cybercriminels. Il sera intéressant de suivre l'évolution en 2018.

L'attaque ExPetr au mois de juin illustre cette tendance. À première vue, cela semblait être un programme ransomware comme les autres, alors qu'il s'agissait en fait d'un programme détruisant les données. Autre exemple : le groupe Shadow Brokers qui a divulgué du code, mettant ainsi des vulnérabilités avancées soi-disant développées par la NSA à la disposition de groupes criminels qui autrement n'auraient pas eu accès à un code aussi sophistiqué. Mentionnons aussi l'émergence des campagnes de menaces persistantes avancées (APT), qui se concentrent non pas sur le cyberespionnage, mais sur le vol d'argent pour financer les autres activités du groupe APT.

L'évolution des ransomwares en 2017 et l'exploitation par de plus petits groupes de vulnérabilités divulguées par Shadow Brokers sont abordées dans le rapport « Ransomwares : la nouvelle menace », disponible ici. Les autres tendances sont traitées plus en détail ci-dessous.

DES ATTAQUES CIBLÉES

En 2017, les plus grands cyberespions continuent leurs activités, cette fois avec des outils et des stratégies plus difficiles à détecter. Nous avons signalé un grand nombre de campagnes.

Les cybercriminels russophones

Lors du Security Analyst Summit du mois d'avril, des chercheurs de Kaspersky Lab et du King's College London ont présenté leurs découvertes concernant un lien possible entre Moonlight Maze, une attaque de cyberespionnage datant d'il y a 20 ans qui avait ciblé le Pentagone, la NASA et bien d'autres, et Turla, un groupe APT très récent. Les données stockées sur un serveur qui avait été détourné pour servir de proxy par les attaquants de Moonlight Maze les ont aidés à reconstituer les opérations, outils et techniques utilisés par les attaquants initiaux. Ils ont également mené une enquête parallèle sur Turla, notamment parce que les deux opérations ont utilisé des backdoors basés sur LOKI2, un programme sorti en 1996 qui permet d'extraire des données par le biais de canaux cachés. Vous trouverez plus de détails sur leur recherche ici.

Nous avons fourni en août une mise à jour sur une autre APT liée à Turla, que nous appelons WhiteBear. À la mi-2017, WhiteBear ne se concentrait plus seulement sur les ambassades et les consulats du monde entier, mais aussi sur les organisations liées à la défense. Nous soupçonnons fortement que le groupe utilise des e-mails de phishing ciblé pour envoyer des fichiers PDF malveillants à ses victimes. Le module principal, l'orchestrateur de WhiteBear, est particulièrement intéressant. Les attaquants chiffrent/déchiffrent et compressent/décompressent la section des ressources avec RSA+3DES+BZIP2, une procédure unique. La plupart des échantillons de WhiteBear sont signés avec un certificat de signature de code valide émis pour « Solid Loop Ltd », une société britannique. Il s'agit probablement d'une société-écran ou d'une société disparue et les attaquants ont pris cette identité pour se servir du nom et de sa réputation afin de créer des certificats numériques trompeurs.

Les cybercriminels anglophones

Nous avons également découvert en avril la boîte à outils la plus récente des Lamberts, un groupe de cybercriminels comparables à Duqu, Equation, Regin ou ProjectSauron en termes de complexité. Nous avons constaté que ce groupe, qui a été repéré par nos spécialistes de la sécurité en 2014, avait développé un ensemble d'outils d'attaque sophistiqués (comme des backdoors en réseau, plusieurs générations de backdoors modulaires, des outils de collecte et de destruction de données) depuis au moins 2008. Il y a des versions actuellement disponibles pour Windows et OS X avec des variantes blanches, bleues, vertes, noires, roses et grises et nous pensons qu'il est fort possible que d'autres Lamberts existent pour d'autres plateformes, par exemple Linux.

Les cybercriminels sinophones

Nous avons aussi décelé plus de détails techniques sur le groupe Spring Dragon, dont les activités remontent à 2012 et qui fait un usage intensif du phishing ciblé et d'attaques de point d'eau. Les cibles sont notamment les agences gouvernementales importantes, les partis politiques, les établissements scolaires et les télécommunications bordant la mer de Chine méridionale, notamment Taïwan, l'Indonésie, le Vietnam, les Philippines, Hong Kong, la Malaisie et la Thaïlande. Nous avons surtout examiné les backdoors utilisés par le groupe pour voler des données, exécuter des composants de programme malveillant supplémentaires et exécuter des commandes système sur les ordinateurs des victimes. Ceux-ci permettent aux attaquants d'entreprendre de multiples activités malveillantes sur les ordinateurs de leurs victimes. Le groupe possède une grande infrastructure C&C (commande et contrôle) qui comprend plus de 200 adresses IP uniques et domaines C&C.

Les autres cybercriminels

En octobre, nos systèmes avancés de prévention des vulnérabilités ont identifié une nouvelle faille « zero-day » Adobe Flash utilisée « In the Wild », diffusée par un document Microsoft Office. La charge finale était la dernière version du programme malveillant FinSpy. Une seule attaque a été observée dans notre base de clients, nous pensons donc que le nombre d'attaques est minime et que celles-ci sont fortement ciblées. Notre analyse de la charge nous a permis de lier cette attaque à un cybercriminel que nous appelons BlackOasis. Nous sommes également certains que ce même groupe est aussi responsable d'une autre faille « zero-day » (CVE-2017-8759) découverte par FireEye au mois de septembre. Nous avons découvert les activités de BlackOasis en mai 2016 lorsque nous enquêtions sur une autre faille « zero-day » Adobe Flash (CVE-2016-4117) qui a été activement exploitée « In the wild ». Des données de Kaspersky Security Network nous ont aussi aidés à identifier deux autres failles semblables utilisées par BlackOasis en juin 2015, qui étaient aussi des « zero-day » à l'époque (CVE-2015-5119 et CVE-2016-0984) : ces chaînes de vulnérabilités envoyaient également des packages d'installation FinSpy. Le groupe BlackOasis cible les personnes impliquées politiquement au Moyen-Orient et d'autres en lien avec la région. Par exemple des personnalités éminentes de l'Organisation des Nations unies, des blogueurs, des militants de l'opposition et des journalistes de la région.

Les autres cybercriminels qui agissent dans l'ombre sont notamment Black Energy, qui se trouve sûrement derrière les attaques de ransomware ExPetr et BadRabbit : les chercheurs pensent qu'il pourrait y avoir un lien entre ExPetr et le ransomware KillDisc de BlackEnergy entre 2015 et 2016.

DES ATTAQUES DESTRUCTRICES

En 2017, nous avons observé une recrudescence des attaques ciblées, conçues pour détruire des données afin de remplacer ou en plus du vol de données.

Plusieurs attaques destructrices ont eu lieu au cours des dernières années, et nous en avons signalé deux autres en 2017 : Shamoon 2.0 et StoneDrill. Shamoon 2.0, un développement du programme malveillant qui aurait été utilisé pour effacer des données sur plus de 30 000 ordinateurs chez Saudi Aramco en 2012, est réapparu en novembre 2016 et au début de l'année 2017 en ciblant des entreprises dans des secteurs économiques et sensibles d'Arabie saoudite. Cette nouvelle version s'accompagne de nouveaux outils et techniques, dont un wiper personnalisé, qui a utilisé des identifiants volés pour effectuer un mouvement latéral au sein de l'organisation. Le wiper, une fois installé dans le réseau, s'active à une date prédéfinie et rend les ordinateurs infectés inutilisables. Shamoon 2.0 comprend également un composant ransomware même s'il n'a pas encore été utilisé « In the Wild ».

Lors d'une enquête sur les attaques Shamoon, nous avons découvert un wiper que nous ne connaissions pas et que nous avons surnommé StoneDrill. Celui-ci semble également prendre pour cible des entreprises en Arabie saoudite. Il existe des ressemblances avec Shamoon ainsi que des fonctions supplémentaires conçues pour empêcher toute détection. L'une des victimes de StoneDrill, observée par Kaspersky Security Network (KSN) était située en Europe (et opère dans le secteur de la pétrochimie), ce qui suggère que les attaquants pourraient bien étendre leurs activités destructrices au-delà du Moyen-Orient. La plus grosse différence entre les deux se trouve dans le processus d'effacement. Shamoon utilise un pilote de disque pour avoir un accès direct au disque dur, alors que StoneDrill injecte le wiper directement dans le navigateur préféré de la victime. StoneDrill comprend également un backdoor qui a déjà été utilisé pour des activités d'espionnage à l'encontre d'un certain nombre de cibles.

Nous ne savons pas si les groupes derrière StoneDrill et Shamoon sont les mêmes ou s'ils ont simplement les mêmes intérêts et qu'ils ciblent les mêmes régions, même si cette dernière hypothèse nous semble plus probable.

Par ailleurs, ExPetr, l'attaque qui réapparaît tout au long de ce bilan annuel, appartient aussi à cette catégorie puisqu'il s'agit d'une opération uniquement conçue dans le but de détruire des données en se faisant passer pour un ransomware. Il est intéressant de se demander si le composant ransomware inutilisé de Shamoon 2.0 devait également servir d'outil de diversion pour une seconde attaque, si nécessaire.

RÉUSSIR SANS COMPLEXITÉ

En 2017, nous avons découvert que les cybercriminels menaient à bien leurs activités, parfois pendant des années, grâce à des campagnes simples et peu sophistiquées.

Les attaques ciblées ne doivent pas être nécessairement très compliquées pour réussir. En janvier 2016, l'arrestation de deux suspects par la police italienne a révélé une série de cyberattaques qui ciblaient des politiciens, des banquiers, des francs-maçons ainsi que des membres importants des forces de l'ordre. Le programme malveillant utilisé lors de l'attaque EyePyramid était simplissime et l'OPSEC des criminels derrière la campagne était faible. Pourtant, les attaquants ont réussi à compromettre les ordinateurs de 1 600 victimes, principalement en Italie, avant que la police ne les appréhende. Bien que le rapport de police n'incluait que très peu d'informations techniques, on y a tout de même trouvé des informations sur des serveurs C&C, des adresses e-mail ainsi que des adresses IP ayant servi à exfiltrer des données volées.

Nous avons utilisé ces informations pour créer une règle YARA afin de trouver dans notre système un échantillon qui correspondrait. Notre première règle YARA a mis en évidence deux échantillons, ce qui nous a permis de créer une autre règle YARA plus précise qui a identifié 42 autres échantillons dans notre collection. Cela nous a permis d'en apprendre plus sur EyePyramid. Les attaques reposent surtout sur le piratage informatique, elles incitent les victimes à ouvrir et à exécuter des fichiers infectés qui se trouvent dans les pièces jointes d'e-mails de phishing ciblé. Les horodatages des échantillons indiquent qu'ils ont été compilés entre 2014 et 2015. Cela signifie que malgré l'absence de complexité technique, les attaquants sont passés inaperçus pendant plusieurs années et ont réussi à voler des gigaoctets de données à leurs victimes.

Microcin est un autre exemple qui illustre comment les cybercriminels peuvent atteindre leurs objectifs à l'aide d'outils peu élaborés et en choisissant bien leurs victimes. Les attaquants ont utilisé une attaque de point d'eau grâce à une faille dans Microsoft Office. Ils ont compromis un forum hébergeant des discussions sur les hébergements fournis par l'État, auxquels les membres de l'armée russe et leurs familles ont droit. Les attaquants ont créé un fichier exécutable sur l'ordinateur de la victime qui a téléchargé des extensions, ce qui a étendu les fonctionnalités du programme malveillant. Les attaquants ont utilisé un script PowerShell et d'autres utilitaires pour voler des fichiers et des mots de passe trouvés sur l'ordinateur de la victime. Les méthodes utilisées par les criminels ne sont ni compliquées ni coûteuses, mais elles n'en restent pas moins efficaces. Deux éléments dans cette attaque sont particulièrement intéressants. Premièrement, les attaquants ont choisi d'exploiter la faillibilité humaine au lieu de dépenser du temps et de l'argent à développer un code de vulnérabilité pour lancer une attaque directement sur les ressources de la société. Deuxièmement, ils se sont servis d'outils d'entreprise standard pour effectuer un mouvement latéral au sein de l'organisation cible.

VOLER POUR ESPIONNER ?

L'année 2017 a également révélé à quel point les cybercriminels se tournaient vers le vol pour financer le coût de leurs activités.

En février 2016, un groupe de pirates (non identifiés à l'époque) a tenté de voler 851 millions de dollars et a réussi à transférer 81 millions depuis la Banque centrale du Bangladesh. Cette attaque est considérée comme la cyberfraude la plus importante et la plus rentable de tous les temps. Les recherches effectuées par Kaspersky Lab et d'autres groupes ont révélé que les attaques avaient sûrement été menées par Lazarus, un célèbre groupe de cyberespionnage et de sabotage, notamment responsable de l'attaque contre Sony Pictures en 2014 et de plusieurs attaques contre des fabricants, des sociétés médiatiques et financières dans pas moins de 18 pays dans le monde depuis 2009. L'intérêt du groupe pour l'argent est relativement récent et il semblerait qu'une autre équipe au sein de Lazarus, que nous avons surnommée Bluenoroff, soit responsable de la génération de profits illégaux. Nous avons vu jusqu'ici quatre principaux types de cibles : les institutions financières, les casinos, les sociétés qui développent des logiciels d'échanges financiers et celles qui s'occupent des cryptomonnaies.

La campagne la plus notable de Bluenoroff concerne ses attaques contre des institutions financières en Pologne. Les attaquants ont pu compromettre un site Web du gouvernement souvent utilisé par un grand nombre d'institutions financières, ce qui en fait un vecteur d'attaque particulièrement puissant.

Lazarus n'est pas un groupe APT comme les autres. L'envergure de ses opérations est surprenante : il semble que Lazarus exploite une usine de programmes malveillants qui lui permet de créer de nouveaux outils dès que les anciens sont « grillés ». Le groupe utilise diverses techniques d'obfuscation, réécrit ses propres algorithmes, applique des protecteurs de logiciel commercial et utilise ses propres compacteurs clandestins. Tout cela coûte de l'argent, ce qui peut expliquer pourquoi Lazarus s'est diversifié dans le vol.

Le groupe Lazarus semble également être derrière l'épidémie de ransomwares WannaCry de mai 2017, plus de détails sont disponibles dans *Ransomwares : la nouvelle menace*. Nous ne savons toujours pas pourquoi un groupe aussi sophistiqué serait derrière la sortie d'un code malveillant aussi imparfait, incontrôlable et dévastateur.

D'AUTRES ATTAQUES FINANCIÈRES

Les attaques de distributeurs automatiques n'ont pas cessé d'augmenter en 2017, les attaquants ciblent les infrastructures bancaires et les systèmes de paiement en utilisant des programmes malveillants sans fichier très sophistiqués, en masquant les caméras de sécurité et en perçant des trous.

Lors du Security Analyst Summit de cette année, deux de nos chercheurs, Sergey Golovanov et Igor Soumenkov, ont évoqué trois cas où des cybercriminels avaient volé de l'argent provenant de distributeurs automatiques.

Le premier, ATMitch, impliquait la compromission de l'infrastructure de la banque afin de prendre le contrôle du distributeur à distance. Les attaquants ont exploité une vulnérabilité non corrigée pour pénétrer les serveurs de la banque cible. Ils ont utilisé un code source ouvert ainsi que des outils accessibles au public pour infecter les ordinateurs de la banque. Toutefois, le logiciel malveillant qu'ils ont créé ne se trouvait que dans la mémoire et non sur les disques durs, et presque toutes les traces du programme malveillant ont disparu après le redémarrage de l'ordinateur. Suite à l'infection, les attaquants se sont connectés à leur serveur C&C, ce qui leur a permis d'installer à distance un programme malveillant sur les distributeurs. Comme ce programme avait pris la forme d'une mise à jour tout à fait légitime, il n'a pas alerté la banque. Une fois installé, le programme malveillant a cherché les commandes qui contrôlent le distributeur. Le programme malveillant commence par émettre une commande pour savoir combien d'argent se trouve dans le distributeur, puis une autre pour délivrer l'argent qui sera récupéré par une mule attendant devant le distributeur. Pour finir, le programme malveillant efface toutes les traces de son passage.

La deuxième attaque a également commencé avec une demande de la part de la banque. L'argent avait disparu, mais l'historique du distributeur était vide et les criminels avaient masqué la caméra de sécurité, il n'y avait donc aucune trace de l'attaque. La banque a envoyé le distributeur à notre bureau et, après l'avoir démonté, nous avons découvert que les criminels avaient installé un adaptateur Bluetooth sur le distributeur et avaient attendu trois mois que l'historique s'efface. Ils sont ensuite retournés au distributeur, ont masqué les caméras de sécurité et ont utilisé un clavier Bluetooth pour redémarrer le distributeur en mode service et vider son contenu.

La troisième attaque, qui, comme celles susmentionnées, a commencé lorsque la banque nous a demandé d'enquêter sur un vol de distributeur, s'est avérée beaucoup moins élaborée. Nous avons trouvé un trou, d'environ 4 cm de diamètre, percé à côté du clavier numérique. Peu après, nous avons entendu parler d'attaques semblables en Russie et en Europe. Lorsque la police a appréhendé un suspect avec un ordinateur portable et des câbles, tout est devenu clair. Nous avons démonté le distributeur pour savoir ce que l'attaquant essayait de faire avec ce trou. Nous avons trouvé un en-tête à 10 broches connecté à un bus qui lui-même connectait tous les composants du distributeur et dont le faible chiffrement pouvait être facilement déchiffré. Une seule partie du distributeur pouvait contrôler toutes les autres ; et comme il n'y avait aucune authentification entre chaque partie, il était facile d'en remplacer une sans que les autres s'en rendent compte. Cela nous a coûté environ 15 $ et un peu de temps pour créer un circuit imprimé tout simple, capable de contrôler le distributeur et de délivrer de l'argent après l'avoir connecté au bus série. Corriger ce problème n'est pas simple, selon nos chercheurs. Appliquer des correctifs nécessite une mise à jour du matériel et cela ne peut pas se faire à distance : un technicien doit se rendre auprès de tous les distributeurs affectés pour l'installer.

Plus récemment, nous avons découvert une nouvelle attaque ciblée sur les institutions financières, principalement des banques en Russie, mais aussi en Malaisie et en Arménie. Les attaquants derrière le cheval de Troie Silence utilisent une approche semblable à Carbanak. Ils obtiennent un accès permanent au réseau interne de la banque, réalisent des enregistrements vidéo des activités quotidiennes des employés pour connaître les procédures de la banque et les logiciels installés, puis se servent de ces informations pour voler de l'argent. Le vecteur de l'infection est un e-mail de phishing ciblé avec une pièce jointe malveillante. Toutefois, un aspect intéressant de l'attaque Silence est que les cybercriminels avaient déjà compromis l'infrastructure bancaire afin d'envoyer leurs e-mails de phishing ciblé à partir d'adresses d'employés de banque réels pour ne pas éveiller la suspicion des futures victimes.

LA CHAÎNE D'APPROVISIONNEMENT COMME TREMPLIN

Une menace émergente pour les entreprises en 2017 qui ne va qu'augmenter en 2018.

Cette année, nous avons vu un certain nombre d'attaques « tremplin » dans lesquelles les attaquants compromettent une société qui fait partie de la chaîne d'approvisionnement d'une autre société, en tirant parti du fait qu'elles sont plus faciles à atteindre. C'était l'une des caractéristiques les plus notables dans l'attaque ExPetr au mois de juin : les attaquants ont ciblé spécifiquement une société qui fournissait un logiciel de comptabilité à des entreprises ukrainiennes. La plupart des victimes étaient situées en Ukraine, mais l'attaque a eu une incidence sur des sociétés du monde entier. Parmi elles, Maersk, première compagnie maritime et plus grand armateur de porte-conteneurs du monde. L'entreprise a indiqué dans son rapport de résultats qu'elle s'attendait à des pertes comprises entre 200 et 300 millions de dollars à la suite d'« interruptions d'activité importantes » causées par l'attaque ExPetr. On citera également FedEx, qui a révélé que les opérations de son unité TNT Express en Europe ont été « grandement affectées » par l'attaque, générant pour l'entreprise des pertes de revenus d'environ 300 millions de dollars.

Les attaquants derrière ShadowPad, signalée au mois d'août, ont adopté une approche similaire en obtenant l'accès au réseau de NetSarang, un distributeur de logiciels de gestion de serveurs très populaire, dans le but de compromettre certains de ses clients, dont des sociétés dans le domaine des services financiers, de l'énergie, de la vente au détail, de la technologie et des médias. Les attaquants ont modifié l'une des mises à jour afin d'inclure un backdoor conçu pour permettre aux attaquants de télécharger et d'exécuter des codes arbitraires, créer des processus et garder un système de fichiers virtuels dans le registre, le tout chiffré et stocké dans des endroits uniques pour chaque victime.

Une autre attaque dans la chaîne d'approvisionnement est survenue en septembre, lorsque des attaquants ont compromis une mise à jour de l'utilitaire de nettoyage Windows CCleaner, publié par Avast. Ils ont modifié le programme d'installation de CCleaner 5.3 pour qu'il installe un programme malveillant sur les ordinateurs des personnes qui téléchargeaient l'utilitaire. Le programme malveillant, signé avec un certificat valide, est resté actif pendant un mois et a infecté environ 700 000 ordinateurs. Les attaquants ont utilisé un processus d'infection en deux étapes : la première a fourni un profil de la victime aux serveurs C&C des attaquants, tandis que la seconde était réservée à des cibles bien précises.

L'INTERNET DES OBJETS PIRATÉS

Un an après le botnet Mirai en 2016, le botnet Hajime a été capable de compromettre 300 000 appareils connectés, une campagne parmi tant d'autres qui concernait les appareils et les systèmes connectés.

Nous sommes aujourd'hui entourés d'appareils intelligents. Cela inclut les objets de la vie courante comme les téléphones, les téléviseurs, les thermostats, les réfrigérateurs, les babyphones, les bracelets de fitness et les jouets pour enfants. Mais cela comprend aussi les voitures, les appareils médicaux, les caméras de surveillance et les horodateurs. Certaines maisons sont désormais conçues pour être « intelligentes ». Un réseau wifi omniprésent connecte tous les appareils, c'est ce que l'on appelle l'Internet des objets (IoT). Ces objets sont conçus pour faciliter notre quotidien. Toutefois, un monde d'objets connectés signifie une plus grande surface d'attaque pour les cybercriminels. À moins que les appareils connectés soient protégés, les données personnelles qu'ils échangent peuvent être compromises, ciblées par des attaques ou utilisées lors d'attaques.

Nous en avons été témoins en octobre 2016, lorsque le botnet Mirai a été utilisé pour bloquer toute une partie d'Internet en prenant le contrôle d'appareils connectés (par ex. les lecteurs DVD, les caméras de surveillance et les imprimantes). En avril de cette année, les attaquants derrière le botnet Hajime ont compromis plus de 300 000 appareils, même si, pour le moment, il n'a pas été utilisé dans un but malveillant : il est possible que les attaquants aient simplement voulu attirer l'attention sur le manque incroyable de sécurité sur certains appareils connectés. Les chercheurs ont pointé du doigt beaucoup d'exemples d'appareils non sécurisés connectés à l'Internet des objets. Des inquiétudes concernant le risque qu'un attaquant utilise la poupée My Friend Cayla ont conduit la Federal Network Agency, le chien de garde des télécommunications allemandes, à suggérer que les parents ayant acheté la poupée la détruisent à cause des risques qu'elle représente. Lors du Security Analyst Summit, l'expert en sécurité Jonathan Andersson a montré comment un attaquant talentueux pouvait créer un appareil pour prendre le contrôle d'un drone en quelques secondes. Pirater un drone peut sembler improbable, mais leur utilisation n'est plus une simple activité de niche : en décembre dernier, Amazon a testé l'utilisation de drones pour livrer des colis.

Et le problème ne concerne pas uniquement les objets utilisés au quotidien par les consommateurs. Les entreprises qui n'avaient pas besoin de se soucier de cybersécurité auparavant doivent à présent faire face à des cyberattaques. On peut citer par exemple le secteur de la santé. Les informations médicales qui avaient toujours existé sous forme papier se trouvent maintenant dans des bases de données, des portails et des équipements médicaux. Le danger réside dans le fait que l'attaque d'un hôpital connecté pourrait entraîner non seulement le vol de données des patients, mais aussi la modification des données de diagnostic, ce qui pourrait générer des erreurs dans la prescription d'un traitement ou d'un médicament. Plus tôt cette année, nous avons analysé les dangers potentiels et avons fourni des recommandations sur la sécurisation des installations médicales.

FUITES DE DONNÉES

L'année 2017 a connu la violation de données chez Equifax, entre autres, avec des millions d'entrées exposées. Les répercussions se feront encore ressentir pendant des années.

Les informations personnelles sont un bien précieux, il n'est donc pas surprenant que les cybercriminels prennent pour cible les fournisseurs de services en ligne, à la recherche d'un moyen pour obtenir des données qu'ils peuvent vendre ou utiliser pour de futures attaques visant des consommateurs ou des entreprises. Une fois encore, nous pouvons constater que cette année est émaillée de fuites de données. On citera notamment Yahoo (ou plus exactement un rapport d'une fuite qui a eu lieu précédemment, en 2013), Avanti Markets, Election Systems & Software, Dow Jones, America's Job Link Alliance et Equifax. La fuite de données d'Uber en octobre 2016 et qui a exposé les données de 57 millions de clients et automobilistes n'a été révélée qu'en novembre 2017.

Certaines de ces attaques ont entraîné le vol d'un grand nombre de données. Dans la plupart des cas, les fuites étaient totalement prévisibles. Les incidents chez Election Systems & Software et concernant le Dow Jones (ainsi que d'autres qui ne sont pas énumérés ci-dessus) résultaient d'une mauvaise configuration des seaux d'Amazon Web Services. Dans le cas de la violation d'America's Job Link Alliance, les pirates ont exploité une vulnérabilité connue dans une application Web. La fuite chez Equifax provenait d'une vulnérabilité qu'Oracle avait corrigée plusieurs mois avant l'attaque, mais le correctif n'avait pas été appliqué.

CONCLUSION

Au cours de cette année 2017, bien des choses se sont révélées très différentes de ce qu'elles auraient dû être. Les ransomwares deviennent des wipers ; les logiciels d'entreprise de confiance deviennent des armes ; les cybercriminels se servent d'outils d'une simplicité navrante tandis que des attaquants bien plus bas dans la chaîne alimentaire mettent la main sur des outils hautement sophistiqués. Ces sables mouvants dans le paysage des cybermenaces constituent un défi croissant pour les experts en sécurité.

Et ce n'est pas seulement un problème pour les entreprises. Comme l'a montré le nombre croissant des attaques de la chaîne d'approvisionnement cette année, n'importe quelle entreprise peut devenir une victime, surtout lorsqu'elle entre dans la ligne de mire d'un cybercriminel cherchant à s'approprier ses données client. Une sécurité fiable à 100 % n'existe pas, mais les entreprises et les particuliers peuvent appliquer de nombreuses mesures pour assurer leur sécurité.

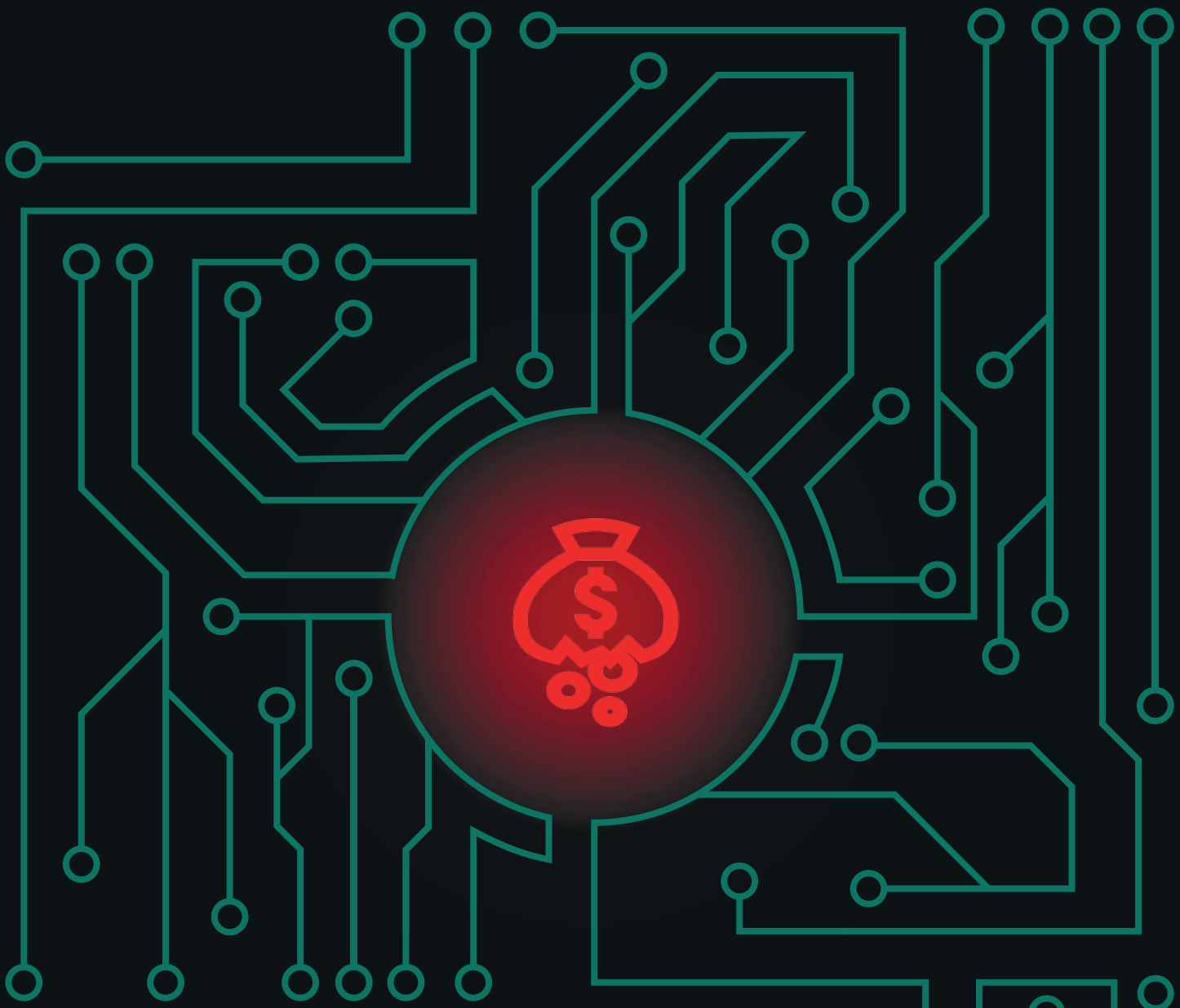
La meilleure défense contre les attaques ciblées est une approche multi-niveaux, qui associe les technologies contre les programmes malveillants traditionnels à une gestion des correctifs, un système de détection des intrusions, une stratégie de blocage par défaut et de listes blanches ainsi qu'une threat intelligence, en ce qui concerne la protection en tant que processus constant assisté par des outils et une expertise. Vous abonner à nos rapports de surveillance des APT vous donnera accès à nos enquêtes et nos découvertes en direct, ainsi qu'à des données techniques complètes. N'oubliez pas les « correctifs » pour les vulnérabilités humaines. Le piratage informatique demeure un point d'entrée essentiel pour les cyberattaquants, il est donc primordial d'éduquer et de communiquer avec les salariés.

Toute entreprise détenant des données personnelles est obligée de les sécuriser efficacement. Lorsqu'une fuite donne lieu au vol d'informations personnelles, les entreprises doivent alerter leurs clients pour qu'ils puissent prendre des mesures et limiter les dégâts potentiels.

Enfin, et c'est là le plus important, ne sous-estimez jamais la puissance des bases de sécurité comme les mots de passe forts, les mises à jour régulières des logiciels et déconnecter les fonctions qui n'ont pas besoin d'être connectées. Cela est déjà très efficace pour protéger les appareils connectés, qu'il s'agisse d'une imprimante chez vous ou d'un équipement médical important.

L'année 2017 nous a beaucoup appris, surtout en ce qui concerne les entreprises. Nous verrons en 2018 si nous avons bien retenu la leçon.

Pour les consommateurs, la principale menace reste les attaques contre les appareils mobiles. La section suivante porte sur l'évolution de cette menace au cours de l'année 2017.



LES MENACES MOBILES EN 2017

Roman Unuchek
Senior Malware Analyst

INTRODUCTION

Pour les consommateurs, les attaques contre les appareils mobiles comptent certainement parmi les menaces les plus virulentes, surtout pour les utilisateurs d'appareils Android. En 2017, des applications contenant des chevaux de Troie ont été téléchargées plus de 10 000 fois, menant à des publicités agressives, des attaques de ransomwares ou des vols par SMS et des facturations WAP. Les attaques contre les appareils mobiles ont trouvé de nouvelles astuces pour ne pas être détectées, tromper les solutions de sécurité et exploiter de nouveaux services. En 2016, ces applications étaient souvent accessibles par le biais de sources de confiance comme Google Play Store.

Voici un résumé des principales menaces mobiles en 2017.

LES PROGRAMMES MALVEILLANTS CHERCHANT À OBTENIR UN ACCÈS RACINE

Ces dernières années, les programmes malveillants cherchant à obtenir un accès racine constituent la plus grande menace pour les utilisateurs d'Android. Ces chevaux de Troie sont non seulement très sophistiqués, avec beaucoup de capacités, mais aussi très populaires. Leur principal objectif est de montrer aux victimes autant de publicités que possible et d'installer puis de lancer discrètement des applications promues. Dans certains cas, les fenêtres publicitaires intempestives et agressives peuvent rendre l'appareil tout bonnement inutilisable.

Ce type de programme malveillant essaie généralement d'obtenir un accès racine en exploitant des vulnérabilités de l'appareil ou en se servant des droits obtenus lors d'une précédente infection. L'accès racine permet au cheval de Troie de faire à peu près tout ce qu'il veut et surtout d'installer des modules pour s'infiltrer partout, afin que le programme malveillant ne puisse pas être supprimé, même après avoir restauré l'appareil aux paramètres d'usine.

La diffusion de chevaux de Troie cherchant à obtenir un accès racine n'est pas rare sur Google Play Store : Dvmap (Trojan.AndroidOS.Dvmap.a) a été installé à partir de Google Play Store plus de 50 000 fois, injectant ses codes malveillants dans les bibliothèques système ; et nous avons détecté presque 100 applications infectées par le cheval de Troie Ztorg mises en ligne sur Google Play, dont une ayant été installée plus d'un million de fois. Ces applications ont obtenu un accès racine en exploitant d'anciennes vulnérabilités bien connues sur des appareils non mis à jour. Elles ont ensuite installé des modules dans les répertoires système pour devenir ineffaçables et installer discrètement des applications.

Bien que le nombre d'utilisateurs attaqués par de tels programmes malveillants ait chuté en 2017 par rapport à 2016, près de la moitié (12) des 30 chevaux de Troie les plus populaires sur Android cette année étaient de ce type, contre 22 en 2016. Nous associons surtout cette chute de popularité des chevaux de Troie s'attaquant à l'accès racine à une baisse d'utilisation des anciens appareils Android, puisque ces chevaux de Troie sont incapables d'exploiter les vulnérabilités des smartphones et des tablettes modernes pour obtenir un accès racine.

Toutefois, cela ne signifie pas que les cybercriminels derrière ces chevaux de Troie ont cessé leurs activités. Certains ont simplement cessé de chercher à obtenir un accès racine, mais continuent de montrer des publicités et de télécharger des applications. En outre, il est toujours difficile de retirer ces applications de l'appareil, car elles peuvent s'infiltrer dans les fonctionnalités système.

Nous avons également découvert que le cheval de Troie Ztorg avait commencé à explorer de nouvelles façons d'obtenir de l'argent, par exemple en attaquant des systèmes de paiement mobiles. Nous avons trouvé deux applications avec cette fonctionnalité malveillante qui partagent des dizaines de milliers d'installations depuis Google Play Store. Ces applications ont pu envoyer des SMS surtaxés et effacer tous les SMS entrants, volant ainsi silencieusement de l'argent sur le compte mobile de la victime. En outre, au cours de notre recherche, nous avons constaté que certains modules supplémentaires de Ztorg utilisaient un fichier JS pour pouvoir aussi voler de l'argent par le biais d'attaques de détournement de clic sur des sites de facturation WAP.

LE DÉTOURNEMENT DE CLIC SUR LES SITES DE FACTURATION WAP

Ils ne sont pas les seuls à cibler les services de paiement par facturation WAP. En 2017, nous avons observé une augmentation de ces logiciels malveillants. Cette fonctionnalité ne date pas d'hier : Trojan-SMS.AndroidOS.Podec attaquait déjà des services de facturation WAP en 2015, mais nous avons vu beaucoup de nouveaux chevaux de Troie devenir populaires en 2017. Le nombre d'utilisateurs attaqués était 2,4 fois plus élevé qu'en 2016.

La plupart de ces chevaux de Troie reçoivent des URL depuis leurs centres de commande. Ils peuvent ouvrir ces liens ou même les visiter à l'insu de la victime, parfois en utilisant des fichiers JS spéciaux pour cliquer sur des boutons sur les pages Web visitées. Ces pages Web peuvent être publicitaires et généralement inoffensives pour la victime (à moins qu'elles n'impliquent des publicités malveillantes comme celles répandues par les chevaux de Troie Ztorg), mais parfois elles peuvent contenir du contenu facturé WAP et nous avons découvert des fichiers JS spécialement créés pour cliquer sur ces pages de facturation WAP.

Généralement, les opérateurs de réseau mobile utilisent leurs propres pages Web pour effectuer les transactions de paiement WAP, mais ces chevaux de Troie peuvent contourner ces pages en cliquant sur les boutons « J'accepte ». Un autre niveau de sécurité réside dans les notifications SMS concernant les transactions, mais elles peuvent aussi être contournées puisque la plupart des chevaux de Troie sont capables d'effacer les SMS entrants à l'insu de la victime.

LES PROGRAMMES MALVEILLANTS BANCAIRES

Les programmes malveillants bancaires se présentent aussi avec de nouvelles fonctionnalités et nous avons découvert en 2017 de nouvelles techniques servant à voler de l'argent. Certaines modifications de FakeToken ont attaqué plus de 2 000 applications financières. Ce cheval de Troie recouvre des applications de confiance de fenêtres de phishing pour voler les identifiants de l'utilisateur et nous avons découvert des modifications de FakeToken qui se sont attaquées à des applications de réservation de taxis, de billets et d'hôtels ainsi qu'à une application permettant de régler des amendes.

Généralement, les mises à jour Android contiennent de nouvelles fonctionnalités de sécurité dont le but principal est de protéger les utilisateurs et d'empêcher les programmes malveillants de faire des dégâts. Mais les logiciels malveillants trouvent toujours un moyen de contourner ces fonctionnalités de sécurité. En juillet 2017, nous avons découvert que Svpeng (Trojan-Banker.AndroidOS.Svpeng.ae) pouvait s'octroyer n'importe quelle permission en s'introduisant dans les services d'accessibilité.

Les « services d'accessibilité » sont une fonctionnalité système qui permet aux développeurs de créer des applications pour les utilisateurs ayant un handicap ou qui sont temporairement incapables d'interagir totalement avec un appareil. Néanmoins, le cheval de Troie en question demandait aux utilisateurs de l'autoriser à utiliser ces services d'accessibilité pour ensuite s'octroyer toutes les permissions dont il avait besoin pour envoyer des SMS, consulter la liste des contacts, passer des appels, etc. En plus de cela, le cheval de Troie recouvrait discrètement d'autres applications et s'ajoutait à la liste des administrateurs de l'appareil. Il a réussi à empêcher sa désinstallation en cliquant sur des boutons dans les dialogues système. Grâce aux services d'accessibilité, le cheval de Troie a également pu voler des données saisies dans les interfaces utilisateur d'applications et même fonctionner comme un enregistreur de frappe.

En août 2017, nous avons trouvé une autre modification du cheval de Troie Svpeng. Celle-ci s'introduisait aussi dans les services d'accessibilité, mais son objectif principal était de verrouiller l'appareil, chiffrer les fichiers de la victime et faire une demande de rançon pour débloquer et déchiffrer les données. Cette fonctionnalité n'est pas nouvelle pour les programmes malveillants bancaires, le cheval de Troie FakeToken possède également une modification qui lui permet de chiffrer des fichiers.

Globalement, Svpeng (Trojan-Banker.AndroidOS.Svpeng.q) a été le cheval de Troie bancaire et mobile le plus populaire de 2017, même si le nombre de victimes a été divisé par 1,5 par rapport à 2016. On peut également citer Asacub (Trojan-Banker.AndroidOS.Asacub), un autre cheval de Troie populaire diffusé par des SMS indésirables. Il y a eu trois fois plus de modifications d'Asacub (12) parmi les 30 programmes malveillants bancaires les plus populaires en 2017 contre seulement quatre en 2016.

LA MONTÉE ET LA CHUTE DES RANSOMWARES

Dans la première moitié de 2017, nous avons observé une hausse considérable du nombre de fichiers ransomwares mobiles : les packages d'installation se sont multipliés par 1,6 par rapport à toute l'année 2016. Mais, après juin 2017, le nombre est retombé à des niveaux antérieurs. La grande majorité (83 %) des ransomwares mobiles à l'origine de cette hausse appartenaient à la famille des Congur (Trojan-Ransom.AndroidOS.Congur). La plupart d'entre eux sont de simples chevaux de Troie qui demandent les droits d'administration de l'appareil puis changent ou définissent un nouveau code d'accès à l'appareil. Ils affichent ensuite un message en chinois qui demande à la victime de les contacter sur QQ, un service de messagerie populaire en Chine.

Les ransomwares mobiles n'ont pas beaucoup changé en 2017 ; la plupart utilisent encore les mêmes techniques pour bloquer les appareils. Nous n'avons pas vu beaucoup de cas d'utilisateurs attaqués avec des chiffreurs mobiles.

CONCLUSION

Plus nous nous servons d'appareils mobiles, plus nous verrons les programmes malveillants proliférer et évoluer. C'est une course sans fin entre les attaquants, les développeurs de logiciels d'appareils et le secteur de la sécurité. Mais ces attaques ne sont pas une fatalité, il existe beaucoup de choses que les utilisateurs peuvent faire pour se protéger et protéger leurs appareils ainsi que leurs données. Cela implique notamment d'utiliser des boutiques en ligne de confiance et de se renseigner sur le développeur d'une application avant de la télécharger. L'utilisation d'une solution de sécurité fiable, telle que Kaspersky Mobile Antivirus : Web Security & Applock est également recommandée.

KASPERSKY lab