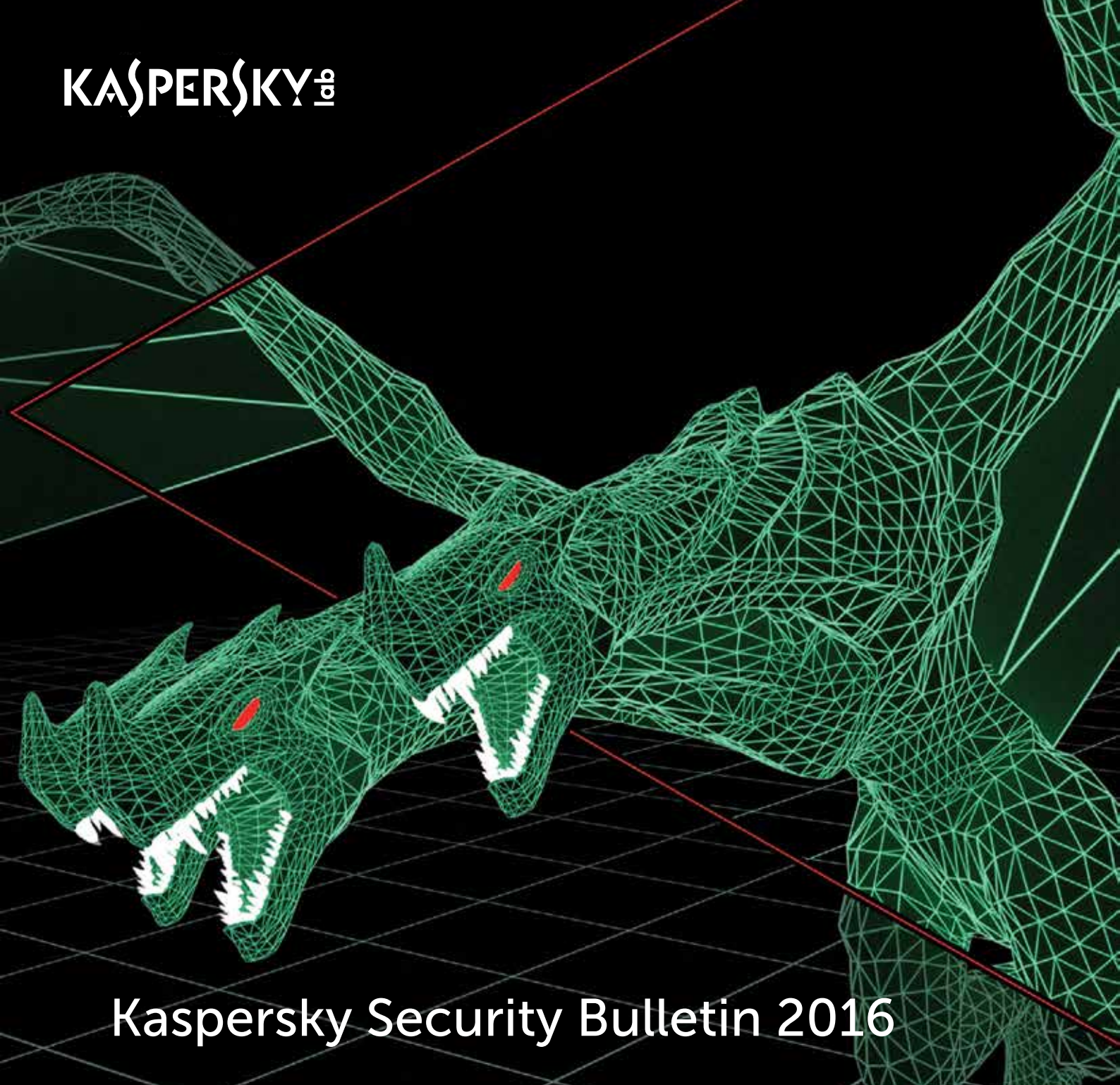
KASPERSKY lab



Kaspersky Security Bulletin 2016

PRÉVISIONS 2017 : ‘LES INDICATEURS DE COMPROMISSION’ SONT MORTS

GREAT

SOMMAIRE

Alors que l'année touche à sa fin, une chose est sûre : elle restera gravée dans les annales de la cyber sécurité. Alors que nous dressons le bilan de certains des événements les plus marquants, nous en profitons pour tenter de voir de quoi sera fait le paysage des menaces en 2017. Nos prévisions sont basées sur les tendances identifiées au cours de nos travaux et sur des observations qui donneront matière à penser aux chercheurs et lecteurs intéressés par la cyber intelligence et le paysage des menaces.

NOS RÉALISATIONS

Nos prévisions de l'année dernière ont été justes et certaines se sont même matérialisées plus tôt que prévues. Pour vous rafraîchir la mémoire, voici quelques-unes de nos prévisions les plus notables :

Menaces APT : Nous nous attendions à une perte d'intérêt pour la persistance et à l'utilisation renforcée de techniques de dissimulation basées sur l'emploi d'attaques ciblées de malwares. Nous avons en effet pu observer une augmentation des malwares sans fichier ou in-memory ainsi qu'une multitude d'attaques ciblées contre des activistes et des sociétés qui reposaient sur des malwares standard comme NJRate et Alienspy/Adwind.

Augmentation des attaques contre les banques : Quand nous avions envisagé l'expansion prochaine de la criminalité financière au plus haut niveau, notre hypothèse incluait parmi les cibles des institutions telles que la bourse. Mais ces prévisions se sont matérialisées avec les attaques contre le réseau SWIFT, qui ont permis aux individus malintentionnés d'empocher des millions grâce à un malware bien placé et bien étudié.

Attaques Internet : Plus récemment, le milieu souvent ignoré des périphériques Internet de qualité médiocre connectés à Internet a fait parler de lui avec un réseau botnet composé d'objets connectés qui a provoqué des pannes chez de grands fournisseurs de services Internet et des perturbations chez les utilisateurs qui comptaient sur un fournisseur DNS spécifique.

Humiliation : Les escroqueries visant à porter atteinte à la réputation des victimes se sont poursuivies alors que des divulgations stratégiques et génériques ont provoqué des problèmes personnels, politiques et de réputation de tous les côtés. Nous devons bien admettre que l'ampleur des attaques et le choix de certaines des victimes de ces fuites nous ont surpris.

QUE NOUS RÉSERVE DONC 2017 ?

Ces APT qui font trembler

Implants passifs et sur-mesure

Bien qu'il soit difficile d'amener les grandes entreprises à se protéger, il est de notre devoir de reconnaître quand les mesures proposées commencent à perdre de leur efficacité. Les indicateurs de compromission sont un excellent moyen de partager les caractéristiques de malwares déjà connus comme les hash, les domaines ou des spécificités d'exécution qui permettront aux services de sécurité informatique d'identifier une infection active. Toutefois, l'élite des cyber espions a déjà trouvé la parade à ces mesures généralisées, comme en témoigne le cas récent de l'APT ProjectSauron, une plate-forme de malware véritablement sur-mesure dont chaque fonction est modifiée pour s'adapter à la victime. Dans un tel scénario, détecter une attaque ne permet pas de détecter les autres. Cela ne veut pas dire pour autant que les services de sécurité informatique sont privés de moyens, mais le temps est venu de promouvoir une adoption plus généralisée des bonnes vieilles règles YARA qui permettent de réaliser des analyses dans l'ensemble de l'entreprise, d'inspecter et d'identifier les caractéristiques des fichiers binaires au repos et d'analyser la mémoire à la recherche de fragments d'attaques connues.

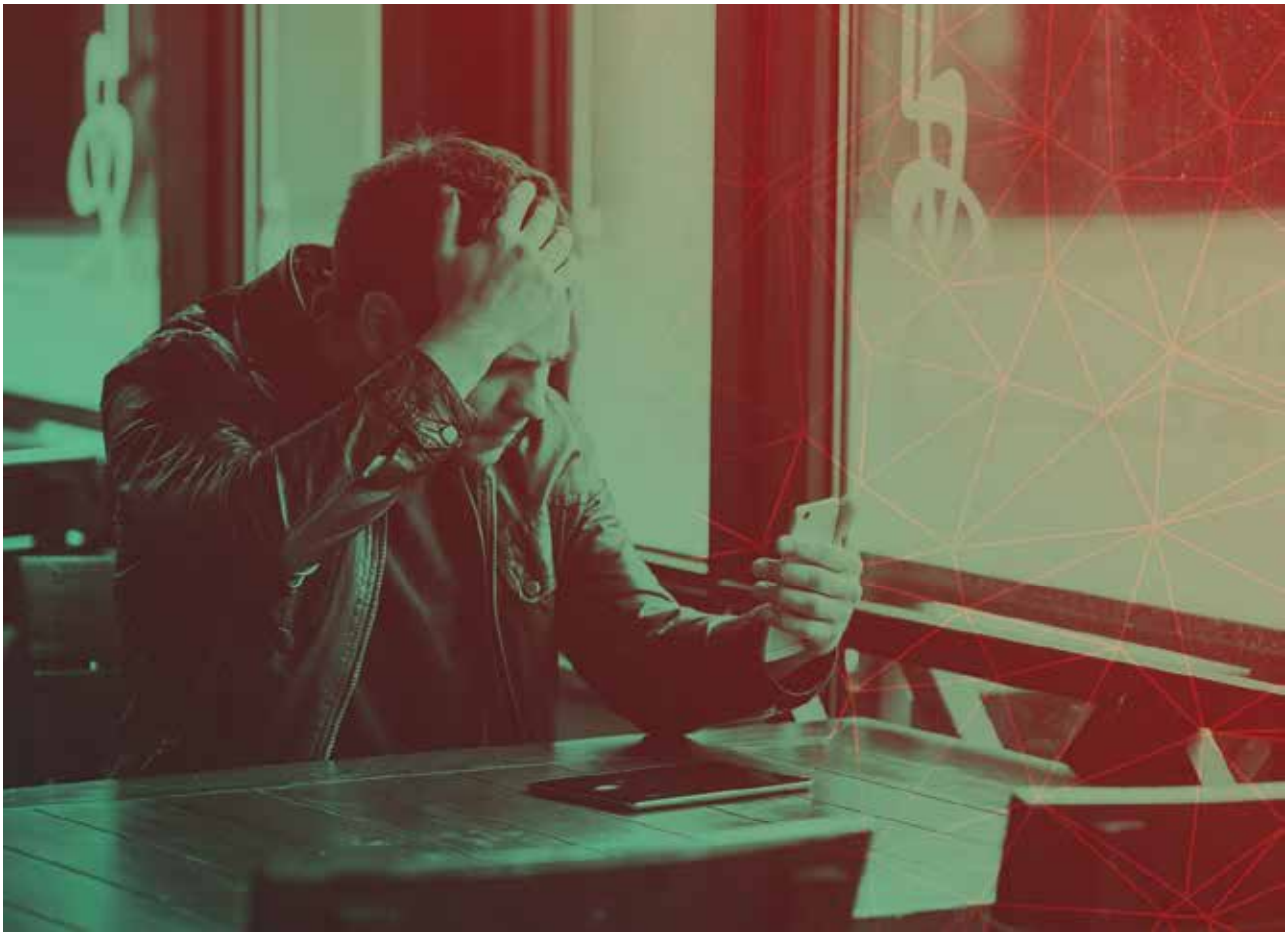
ProjectSauron a également affiché une autre caractéristique de pointe qui devrait se généraliser : l'implant passif. Une backdoor réseau in-memory ou un pilote avec backdoor dans un passerelle Internet ou sur un serveur Internet qui attend silencieusement les octets magiques qui l'activeront. Tant que l'implant passif n'a pas été réveillé par ses maîtres, il affiche peu ou pas d'indices externes d'une infection en cours et par conséquent il a peu de chance d'être découvert, si ce n'est par le plus paranoïaque des défenseurs ou dans le cadre de la réaction à un incident plus large. Il ne faut pas oublier que ces implants ne disposent pas d'une infrastructure de commande prédéfinie et constituent ainsi une tête de pont plus anonyme. Il s'agit donc de l'outil par excellence pour les attaquants les plus prudents, qui doivent pouvoir accéder rapidement à un réseau ciblé.

Infections éphémères

Alors que PowerShell devient chaque jour un peu plus parfait pour les administrateurs, il constitue également une aubaine pour une multitude de développeurs de malwares intéressés par le déploiement furtif, le mouvement latéral et les capacités de reconnaissances qui ne seront probablement pas remarqués par les configurations standard. Un petit malware PowerShell stocké in-memory ou dans la base de registres pourrait certainement faire de gros dégâts dans les systèmes Windows modernes. Nous allons même plus loin et nous nous attendons à voir des infections éphémères, œuvres de malwares résidant en mémoire conçus pour la reconnaissance et la collecte d'informations d'authentification et qui ne sont pas intéressés par la persistance. Dans les environnements très sensibles, des attaquants furtifs peuvent être heureux à l'idée de pouvoir travailler jusqu'à ce qu'un redémarrage élimine l'infection si cela limite le risque de soupçons ou de pertes d'exploitation résultantes de la détection du malware par les défenseurs et des chercheurs. Les infections éphémères vont mettre en évidence la nécessité d'intégrer des techniques heuristiques proactives et sophistiquées dans les solutions de pointe de lutte contre les malwares (cf. System Watcher).

Espionnage mobile

De nombreux auteurs de menaces ont utilisé les implants mobiles par le passé, dont Sofacy, RedOctober et CloudAtlas, ainsi que des clients de HackingTeam et la suite présumée de malware iOS NSO Pegasus. Toutefois, ceux-ci ont participé à des campagnes qui reposent principalement sur des toolkits pour ordinateurs. Dans la mesure où l'usage des ordinateurs décline au profit de celui des technologies mobiles, nous nous attendons à voir une augmentation des campagnes d'espionnage mobile. Ces campagnes vont certainement profiter d'une diminution de l'attention et de la difficulté d'obtenir des outils d'enquête pour les systèmes d'exploitation mobiles les plus récents. La confiance vis-à-vis de la signature de code et des vérifications d'intégrité ont gelé la visibilité pour les chercheurs en sécurité dans le milieu mobile, mais cela ne va pas dissuader des attaquants déterminés et bien équipés désireux de trouver des proies dans cet espace.



L'avenir des attaques financières

Nous avons appris que vous aimeriez cambrioler une banque...

Le secteur financier a été secoué par les attaques audacieuses organisées cette année contre le réseau SWIFT ; elles ont débouché sur des butins de plusieurs millions de dollars. Il s'agissait d'une évolution naturelle pour des intervenants comme le gang Carbanak et peut-être d'autres auteurs de menaces intéressants. De tels cas demeurent l'œuvre d'acteurs influencés par les APT et qui font preuve d'un certain panache, en plus d'une capacité démontrée. Sont-ils vraiment les seuls intéressés par l'idée de voler d'importantes sommes d'argent aux banques ?

Au fur et à mesure que l'intérêt pour la cybercriminalité va augmenter, nous nous attendons à voir émerger des intermédiaires pour ces cambriolages SWIFT dans les plans clandestins bien établis du monde des activités criminelles à plusieurs intervenants. Pour réaliser un de ces coups, il faut obtenir un accès initial, posséder un logiciel spécialisé, s'armer de patience et mettre en place un système de blanchiment d'argent. Chacune de ces étapes offre une opportunité pour des criminels déjà établis qui pourront monnayer leurs services. L'élément manquant ici sera le malware spécialisé pour lancer les attaques contre le réseau SWIFT. Nous nous attendons à ce que de telles attaques soient offertes via la vente de ressources spécialisées sur des forums clandestins ou dans le cadre de formules « as a service ».

Systèmes de paiement résilients

L'attrait pour les nouveaux systèmes de paiement va intéresser les criminels. Toutefois, les systèmes semblent résistants car aucune attaque d'ampleur n'a été enregistrée. Cette bonne nouvelle pour le consommateur représente toutefois un casse-tête pour les fournisseurs de système de paiement car les cybercriminels cherchent à les cibler à l'aide d'attaques directes menées contre l'infrastructure du système de paiement. Que ces attaques débouchent sur des pertes financières directes ou sur de simples perturbations, elles devraient se multiplier.

Ransomware sale et menteur

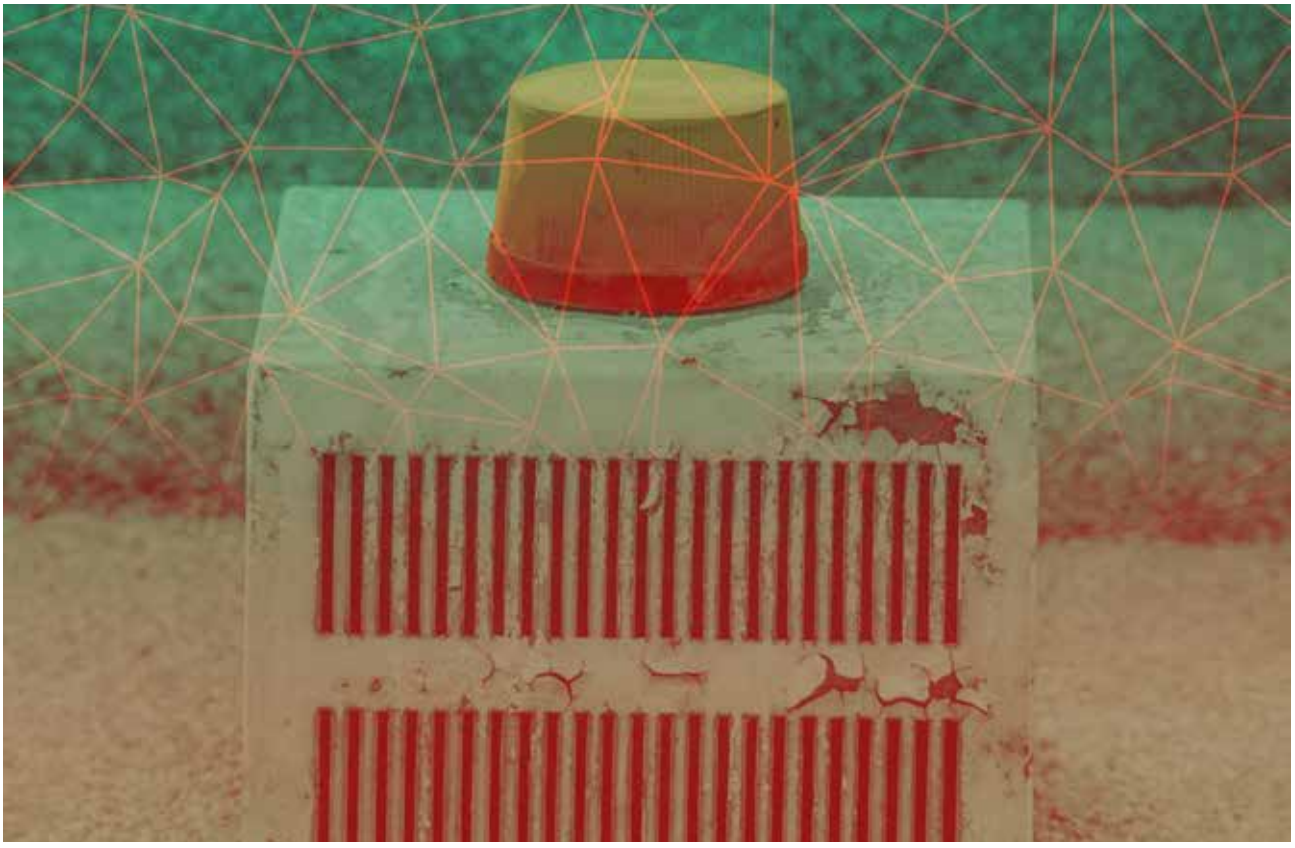
S'il est vrai que nous détestons les ransomwares (et pour de bonnes raisons), ils fonctionnent grâce à une relation de confiance improbable entre la victime et l'agresseur. Cet écosystème criminel repose sur le fait que l'agresseur respectera le contrat tacite conclu avec la victime, à savoir que les fichiers seront restitués une fois que le paiement aura été réalisé. Les cybercriminels ont affiché un surprenant semblant de professionnalisme en respectant cette promesse et c'est cela qui a permis à l'écosystème de se développer. Toutefois, alors que la popularité de ce type d'attaque continue d'augmenter et que des criminels moins scrupuleux entrent en scène, il faut s'attendre à voir des ransomwares dépourvus de l'assurance qualité ou des capacités de codage générales pour tenir cette promesse.

Il faudra compter sur l'émergence de ransomwares de type « script kiddies » qui bloquent l'accès aux fichiers ou au système ou qui suppriment simplement les fichiers, amènent la victime à payer la rançon et ne rendent rien en retour. À ce moment, la distinction entre ransomware et attaque avec effacement des données sera minime et l'écosystème des ransomwares commencera à ressentir les effets d'une « crise de confiance ». Il n'est pas dit que cela dissuade des équipes plus importantes et plus professionnelles de poursuivre leurs campagnes d'extorsion. Toutefois, l'idée selon laquelle payer la rançon est acceptable pourrait disparaitre.

Le gros bouton rouge

Le célèbre Stuxnet avait peut-être ouvert une boîte de Pandore en accélérant la prise de conscience de la vulnérabilité des systèmes industriels, mais il avait été développé soigneusement dans l'optique d'un sabotage prolongé contre des cibles très particulières. Cependant, alors que l'infection se propageait à travers le monde, des contrôles imposés sur la charge utile ont limité les dégâts collatéraux et l'Apocalypse industrielle n'a pas eu lieu. Toutefois, depuis lors, la moindre rumeur ou information sur un accident industriel ou une explosion inexpliquée s'accompagne d'une théorie de cyber-sabotage.

Ceci étant dit, un accident industriel fruit d'un cyber-sabotage est du domaine du possible. Alors que les infrastructures critiques et les systèmes de production sont toujours connectés à Internet, souvent avec une protection négligeable, voire nulle, ils se transforment en cibles appétissantes pour les attaquants dotés des ressources nécessaires qui cherchent à provoquer le chaos. Il faut toutefois noter que ces attaques requièrent un certain niveau d'aptitude et d'intention. Il est probable qu'une attaque de cyber-espionnage se déroule dans le cadre d'un contexte géopolitique tendu et que les auteurs de menaces bien établies se fixent comme objectif la destruction ou la perturbation ciblées de services essentiels.



Un Internet surpeuplé réagit

Une brique d'un autre nom

Nous alertons depuis longtemps sur les faiblesses de sécurité de l'Internet des objets, et nos craintes se sont révélées justes. Comme nous avons pu le voir avec le réseau botnet Mirai récemment, la faiblesse de la sécurité des appareils connectés inutilement à Internet constitue une aubaine pour les individus malintentionnés qui veulent provoquer le chaos en ayant peu ou pas de chance d'être pris. S'il est vrai que l'étape suivante ne surprendra pas les experts de la sécurité de l'information, elle pourrait se révéler particulièrement intéressante car nous prévoyons que des pirates justiciers vont prendre eux-mêmes les choses en mains.

L'approche qui consiste à corriger les vulnérabilités connues et signalées est peu remise en question, venant ainsi valider le travail ardu (et souvent non rémunéré) des chercheurs en sécurité. Si les fabricants de périphériques connectés continuent à proposer des appareils qui ne sont pas protégés et qui sont à l'origine d'un large éventail de problèmes, il est probable que des pirates justiciers décident de résoudre le problème eux-mêmes. Et il n'existe pas de meilleure manière de troubler la quiétude des fabricants que d'organiser la mort logicielle ou matérielle en masse des périphériques vulnérables. Si les réseaux de zombies IdO continuent de provoquer des attaques DDoS ou de diffuser du spam, la réponse immunitaire de l'écosystème pourrait très bien décider de désactiver ces appareils, au grand dam des consommateurs et des fabricants. Nous sommes peut-être les témoins de l'avènement de l'Internet des briques.

Les boîtes clignotantes silencieuses

Les divulgations choquantes de ShadowBrokers contenaient une multitude de codes d'exploitation opérationnels pour plusieurs fabricants de pare-feu de renom. Des cas d'exploitation dans la nature ont été signalés peu de temps après et les fabricants se sont empressés de comprendre les vulnérabilités exploitées et de les éliminer. Il est toutefois encore trop tôt pour mesurer toute l'ampleur des conséquences. Qu'est-ce que les attaquants ont pu gagner avec ces codes d'exploitation à disposition ? Quel type d'implant pourrait se trouver dans les périphériques vulnérables ?

Si nous allons au-delà de ces codes d'exploitation en particulier (tout en tenant compte de la découverte, à la fin de l'année 2015, d'une backdoor dans ScreenOS de Juniper), nous sommes confrontés à la problématique plus grande de l'intégrité des périphériques qui devra faire l'objet de recherches plus poussées au niveau des appareils critiques pour les périmètres d'entreprise. La question est toujours ouverte : « Pour qui votre pare-feu travaille-t-il ? »

Mais qui êtes-vous ?

Nous sommes particulièrement intéressés par les campagnes sous fausses bannières et les opérations de guerre psychologique et c'est sans surprise que nous prévoyons des évolutions dans ce domaine...

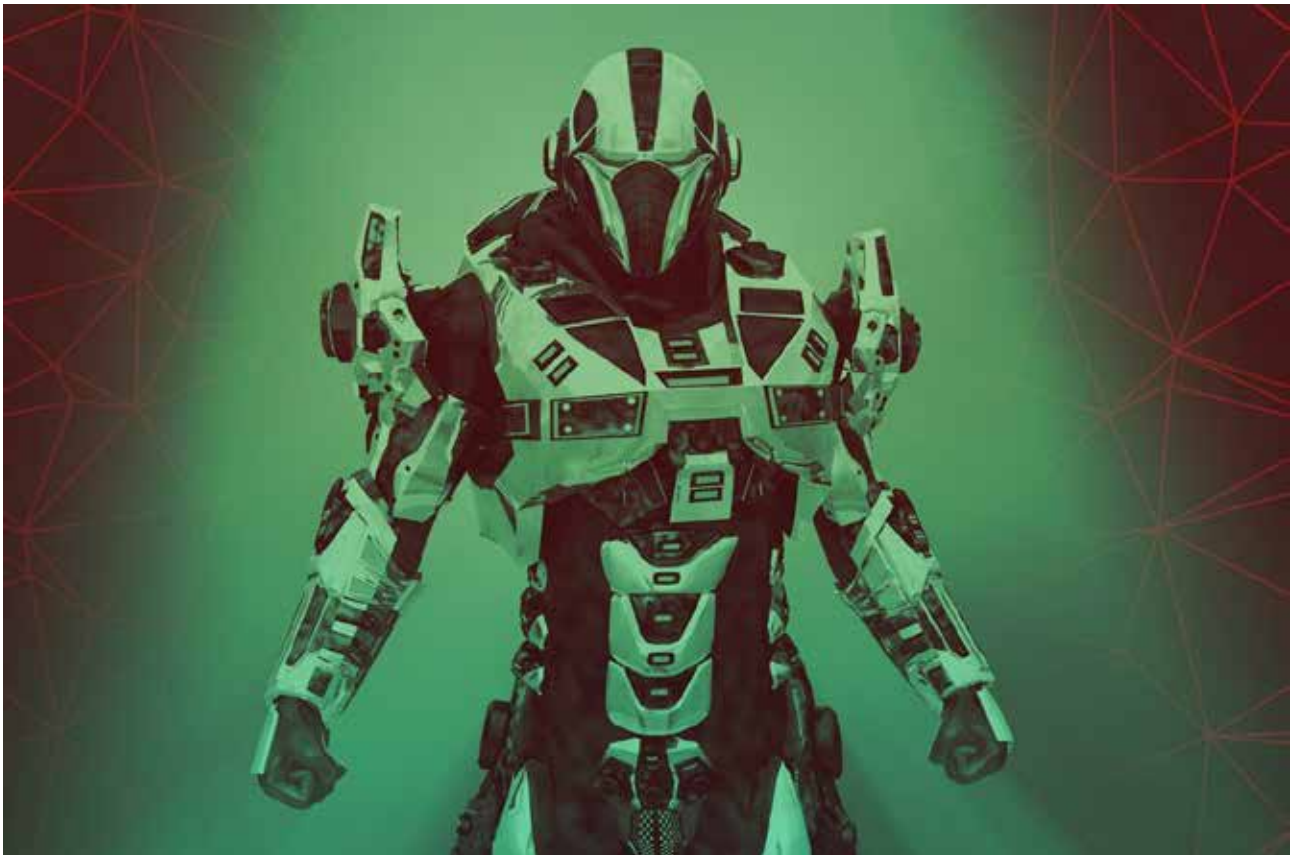
Guerre de l'information

La création de faux site pour des divulgations ciblées et des opérations d'extorsion ont été explorées en premier par des groupes comme Lazarus et Sofacy. Après quelques mois d'une utilisation très remarquée et réussie, nous nous attendons à ce que la popularité des campagnes de guerre de l'information augmente dans le but de manipuler l'opinion et de provoquer un chaos généralisé autour de processus populaires. Les auteurs de menaces intéressés par la divulgation de données piratées n'ont pas grande chose à perdre un créant une histoire via un groupe d'hacktivistes établis ou créés ; l'attention est détournée de l'attaque en elle-même vers le contenu des révélations.

Le danger à ce stade ne se situe pas au niveau du piratage ou de la violation de la vie privée. Non, le danger vient du fait que les journalistes et les citoyens préoccupés peuvent s'habituer à accepter les données divulguées comme des faits pertinents. Des acteurs plus rusés pourraient chercher à influencer un résultat en manipulant des données ou en les omettant. La vulnérabilité face à ces campagnes de guerre de l'information n'a jamais été aussi élevée et nous espérons que le bon sens prévaudra alors que ces techniques sont adoptées par de plus en plus d'acteurs (ou par les mêmes acteurs utilisant des identités différentes).

La promesse de la dissuasion

Dans la mesure où les cyberattaques jouent un rôle de plus en plus grand dans les relations internationales, leur attribution va occuper une place essentielle dans la définition des ouvertures géopolitiques. Les institutions gouvernementales éprouvent des difficultés à se mettre d'accord pour identifier les normes d'attribution qui seront suffisantes pour les démarches ou les condamnations publiques. Etant donné la vision fragmentée des différentes institutions publiques et privées, une attribution précise est pratiquement impossible. Il est possible que dans ce cas, une « attribution floue » sera considérée comme suffisante. S'il est vrai qu'il faut faire extrêmement attention, il ne faut pas oublier de prévoir des conséquences pour celui qui s'avance sur le terrain des cyberattaques. Une des plus grandes questions est de veiller à ce que la riposte n'engendre pas des problèmes complémentaires alors que les auteurs d'attaques rusés trompent les parties qui cherchent à attribuer l'attaque. Il ne faut pas non plus oublier que l'augmentation de la probabilité d'une riposte et de conséquences va s'accompagner d'une augmentation sensible des abus des malwares open-source et commerciaux. Des outils tels que Cobalt Strike et Metasploit, par exemple, ouvrent la porte à de plausibles dénégations, ce qui n'est pas le cas des malwares de source fermée.



Doubler la mise sur les campagnes sous fausses bannières

que les exemples fournis dans le rapport sur les opérations sous fausses bannières incluaient des cas d'APT, aucun cas d'opération sous fausse bannière authentique n'a été observé à ce jour. Nous voulons dire par cela, une opération soigneusement et entièrement mise en place par l'auteur A dans le style et avec les ressources de l'acteur B, dans le but de provoquer la riposte de la victime contre l'acteur B qui n'aurait pourtant rien à se reprocher. Il est possible que les chercheurs n'ont tout simplement pas remarqué de tels comportements, mais ces opérations ne prendront tout leur sens que le jour où il y aura vraiment une riposte en cas de cyberattaque. Le jour où la riposte (divulgation, sanction ou exploitation des réseaux informatiques tiers de représailles) deviendra plus fréquente et impulsive, il faudra s'attendre à l'organisation de véritables opérations sous fausse bannière.

Quand nous en serons arrivés là, nous pouvons nous attendre à ce que les campagnes sous fausses bannières justifient des investissements plus importants encore, pouvant aller jusqu'à la divulgation d'infrastructures ou de toolkits propriétaires jalousement gardés en vue d'une utilisation massive. De cette manière, des auteurs de menaces rusés pourraient engendrer une confusion momentanée chez les chercheurs et les défenseurs car les script kiddies, les hacktivistes et les cybercriminels seraient soudainement capable d'utiliser les outils propriétaires d'un auteur de menace avancée, ce qui donnerait le couvert de l'anonymat dans la multitude des attaques et réduirait les capacités d'attribution de l'attaque.

Qu'est-ce que la vie privée ?

Retirer le voile

La suppression de ce qui reste de l'anonymat dans le cyberespace est attrayante pour les publicitaires et les espions. Pour les publicitaires, le suivi à l'aide de cookies persistants s'est révélé être une technique appréciable. Elle va certainement poursuivre son développement et s'associer à d'autres widgets et autres éléments innocents ajoutés aux sites Web et qui permettent aux entreprises de suivre chaque utilisateur lorsqu'il franchit leur domaine et d'obtenir ainsi une vue d'ensemble de leurs habitudes de navigation (cf. ci-après).

Dans d'autres régions du monde, le ciblage des activistes et le suivi des activités sur les réseaux sociaux qui « incitent à l'instabilité » vont continuer à inspirer une sophistication surprenante alors que des entités aux ressources importantes vont continuer à découvrir des sociétés inconnues et curieusement bien placées qui proposent des nouveautés pour surveiller les dissidents et les activistes dans toutes les régions de l'Internet. Ces activités sont particulièrement intéressées par les tendances sur les réseaux sociaux pour des régions entières et l'impact des dissidents. Nous verrons peut-être même un auteur qui osera s'attaquer à un réseau social pour s'attaquer à un filon de données personnelles et d'informations incriminantes.

Le réseau publicitaire d'espionnage

Les réseaux publicitaires constituent la seule technologie qui permet l'organisation d'attaques vraiment ciblées. Le placement est entièrement motivé par l'aspect financier et les réglementations sont quasi inexistantes, comme en témoigne les attaques récurrentes de diffusion de malwares via des publicités sur des sites de renom. En raison de leur nature, les réseaux publicitaires offrent un excellent profilage des cibles via la combinaison des adresses IP, des empreintes du navigateur, des sites d'intérêt et de la sélectivité des connexions. Ce genre de données permet à un attaquant d'injecter une charge utile chez une victime spécifique ou de rediriger celle-ci vers la charge utile en question. Il évite ainsi les infections collatérales et la disponibilité continue des charges utiles qui attirent souvent l'attention des chercheurs en sécurité. Nous nous attendons dès lors à ce que les acteurs les plus évolués du cyber espionnage arrivent à la conclusion que la création ou l'approbation d'un réseau publicitaire est un investissement modeste qui pourrait être très rentable et qui permettrait de toucher les victimes tout en protégeant leurs outils les plus récents.

L'émergence du pirate justicier

Après la divulgation des données de HackingTeam en 2015, le mystérieux Phineas Fisher a publié un guide pour les apprentis pirates dans lequel il expliquaient comment mettre hors service les organisations injustes et les sociétés douteuses. Ceci évoque le sentiment latent qui veut que la puissance asymétrique du pirate justicier est une arme pour le bien, même si la divulgation de HackingTeam a fourni des vulnérabilités 0jour actives à des équipes APT et peut-être même encouragé de nouveaux clients. Alors que les conspirations s'intensifient pour ces élections, alimentées par la croyance en la divulgation de données comme contrepoids dans la balance de l'information, il faut s'attendre à ce que le nombre de pirates justiciers qui utilisent les divulgations de données et les fuites organisées contre des organisations vulnérables augmente.

Securelist

Retrouvez ici les recherches et analyses de nos experts en sécurité informatique, sur les virus, les hackers, les spams...

Notre site web

Nota Bene – Le blog d'Eugène Kaspersky

Kaspersky Daily — Infos, Trucs et astuces pour les utilisateurs

Kaspersky Business Blog – Des infos pertinentes sur la sécurité informatique

Threatpost – Le site numéro 1 pour des infos exclusives sur la sécurité informatique

Kaspersky Academy