KASPERSKY lab

Kaspersky Security Bulletin 2015

PRÉVISIONS 2016 : LA FIN DU MONDE TEL QUE NOUS LE CONNAISSONS POUR LES APT

GREAT

SOMMAIRE

INTRODUCTION

Alors que l'année touche à sa fin, nous pouvons en profiter pour dresser le bilan de l'évolution du secteur et avancer nos prévisions pour les années à venir. Profitant d'une réunion de nos experts du GReAT (Global Research and Analysis Team) et de l'unité de recherche sur les malwares, nous avons échangé des idées sur les tendances de l'année à venir et au-delà. J'ai désormais le privilège de pouvoir choisir les plus intéressantes et les plus probables. Les perspectives dans notre domaine d'étude qui évolue si rapidement sont bouleversantes et ce ne sont pas les défis intéressants qui vont manquer. La sobriété des idées nous permettra peut-être d'éviter le sensationnalisme de science-fiction et de formuler des prévisions qui se vérifieront à court et long terme.

FINI LES APT

Avant de crier victoire, sachez que nous faisons en fait référence aux dimensions "Avancée" et "Persistante" que les auteurs de menaces seraient ravis d'abandonner au profit de la furtivité globale. Nous estimons que la persistance va devenir de moins en moins cruciale et que les groupes APT vont se concentrer davantage sur les malwares résidant dans la mémoire ou les malwares sans fichiers. L'objectif recherché est de réduire les traces laissées dans un système infecté et par conséquent, d'éviter la détection. Une autre démarche consistera à limiter l'accent placé sur les malwares avancés. Au lieu d'investir dans des bootkits, des rootkits et des malwares personnalisés qui sont finalement détectés par les équipes de recherche, nous nous attendons à ce que les groupes APT adoptent la réorientation de malwares prêts à l'emploi. Ainsi, la plate-forme de malware n'est pas condamnée quand elle est découverte. En plus, cette formule permet de masquer l'acteur et ses intentions dans le flot des usages traditionnelles des outils d'accès à distance disponibles dans le commerce. Au fur et à mesure que la gloire tirée des cyber-capacités va perdre de son éclat, c'est le concept de rendement des investissements qui justifiera la majorité des décisions prises par les hackers d'Etat et rien ne vaut un investissement initial minimum pour maximiser le rendement de l'investissement.

RANSOMWARES : LE CAUCHEMAR CONTINUE

Nous nous attendons à ce que la réussite des ransomwares atteigne de nouvelles frontières. Le ransomware possède deux avantages par rapport aux menaces bancaires traditionnelles : l'obtention directe d'argent et le coût par victime relativement bas. Ceci s'explique par une réduction de l'intérêt de la part de tiers dotés de bonnes ressources comme les banques et le faible niveau de plaintes enregistrées par les autorités judiciaires et policières. Nous nous attendons non seulement à ce que les ransomwares gagnent du terrain sur les trojans bancaires, mais également à ce qu'ils migrent vers de nouvelles plates-formes. Nous avons déjà vu de modestes tentatives d'introduction de ransomwares parmi les appareils mobiles (Simplelocker) et Linux (Ransom.Linux.Cryptor, Trojan-Ransom.FreeBSD.Cryptor), mais la plate-forme qui fait probablement le plus rêver les individus malintentionnés est OS X. Nous nous attendons à ce que les ransomwares franchissent le Rubicon et ciblent des Macs, exigeant au passage des montants dignes d'un Mac. À plus long terme, nous pouvons réfléchir à la probabilité de l'émergence des ransomwares dans l'Internet des Objets. Nous ne pouvons nous empêcher de nous poser la question suivante : Combien seriez-vous prêt à payer pour pouvoir utiliser à nouveau votre télévision ? Votre frigo ? Votre voiture ?

MISER CONTRE LA MAISON : DES CRIMES FINANCIERS DE TRÈS HAUT NIVEAU

La fusion de la cybercriminalité et des APT a donné des ailes aux criminels financiers qui sont passé élégamment des attaques contre les clients des banques aux attaques directes contre les institutions financières. L'année dernière aura été riche en attaques contre des systèmes de terminaux de point de vente ou des distributeurs automatiques de billets, sans oublier l'audacieuse campagne de Carbanak qui a permis de dérober des centaines de millions de dollars. Ici aussi, nous nous attendons à ce que les cybercriminels s'intéressent aux nouveautés comme les alternatives de systèmes de paiement (ApplePay et AndroidPay) dont les taux d'adoption en augmentation devraient offrir de nouveaux moyens d'obtenir rapidement de l'argent. La bourse, le Graal en matière de cybercriminalité financière, suscite également des convoitises. S'il est vrai que les attaques frontales peuvent donner des résultats rapidement, il ne faut pas négliger la possibilité d'interférences plus subtiles, comme des attaques contre les algorithmes par boîte noire utilisés dans le trading haute fréquence afin de garantir des gains prolongés tout en réduisant la probabilité d'être attrapé.

ATTAQUES CONTRE LES ÉDITEURS DE SOLUTIONS DE SÉCURITÉ

Au fur et à mesure de l'augmentation des attaques contre les éditeurs de solution de sécurité, nous nous attendons à voir émerger des techniques de compromission d'outils d'ingénierie inverse standard comme IDA et Hiew, d'outils de débogage comme OllyDbg et WinDBg ou d'outils de virtualisation comme VMware Suite et Virtual Box. CVE-2014-8485, une vulnérabilité dans la mise en œuvre des "chaînes" dans Linux, constitue un exemple de la vulnérabilité des outils de recherche en sécurité complexes que des attaquants motivés pourraient choisir d'exploiter au moment de cibler les chercheurs eux-mêmes. Dans le même ordre d'idée, le partage d'outils de recherche libres via des référentiels de code tels que Github est un domaine qui laisse la porte ouverte aux abus car bien souvent, les utilisateurs choisiront un code et l'exécuteront sur leur système sans réfléchir. Nous devrions peut-être nous méfier également des mises en œuvre répandues du cryptosystème PGP (Pretty Good Privacy), adopté avec enthousiasme par la communauté de la sécurité des informations.

SABOTAGE, EXTORSION ET HUMILIATION

Depuis les diffusions de photos de célébrités nues jusqu'aux attaques contre Sony et Ashley Madison en passant par l'incident HackingTeam, nous ne pouvons nier l'augmentation du nombre de cas de doxing, d'humiliation et d'extorsion. Les hacktivistes, les criminels et les attaquants étatiques ont tous adopté la divulgation stratégique de photos privées, d'informations, de listes de clients et de codes pour humilier leur cible. Alors que certaines de ces attaques sont stratégiquement ciblées, d'autres sont purement opportunistes et profitent d'une cybersécurité médiocre pour faire croire à une prouesse technique. Malheureusement, la croissance exponentielle de ce genre de pratique va se maintenir.

EN QUI PEUT-ON AVOIR CONFIANCE ?

La confiance est peut-être le bien le plus rare actuellement sur Internet. L'abus de ressources de confiance ne fera que la rendre encore plus rare. Les attaquants vont continuer à utiliser des bibliothèques open source ou des ressources reprises sur les listes blanches pour réaliser leurs actes malveillants. Nous nous attendons à des attaques contre une autre forme de confiance, celle inspirée par les ressources internes d'une société. Quand les attaquants cherchent à étendre leur implantation dans un réseau infecté, ils peuvent cibler des ressources limitées à l'intranet de la société et organiser des attaques selon la technique du waterholing contre des portails SharePoint, de fichiers ou ADP. Nous allons peut-être même observer un nouveau développement dans l'abus déjà généralisé des certificats de confiance alors que les attaquants mettent en place une autorité de certification qui délivrera des certificats à leurs malwares.

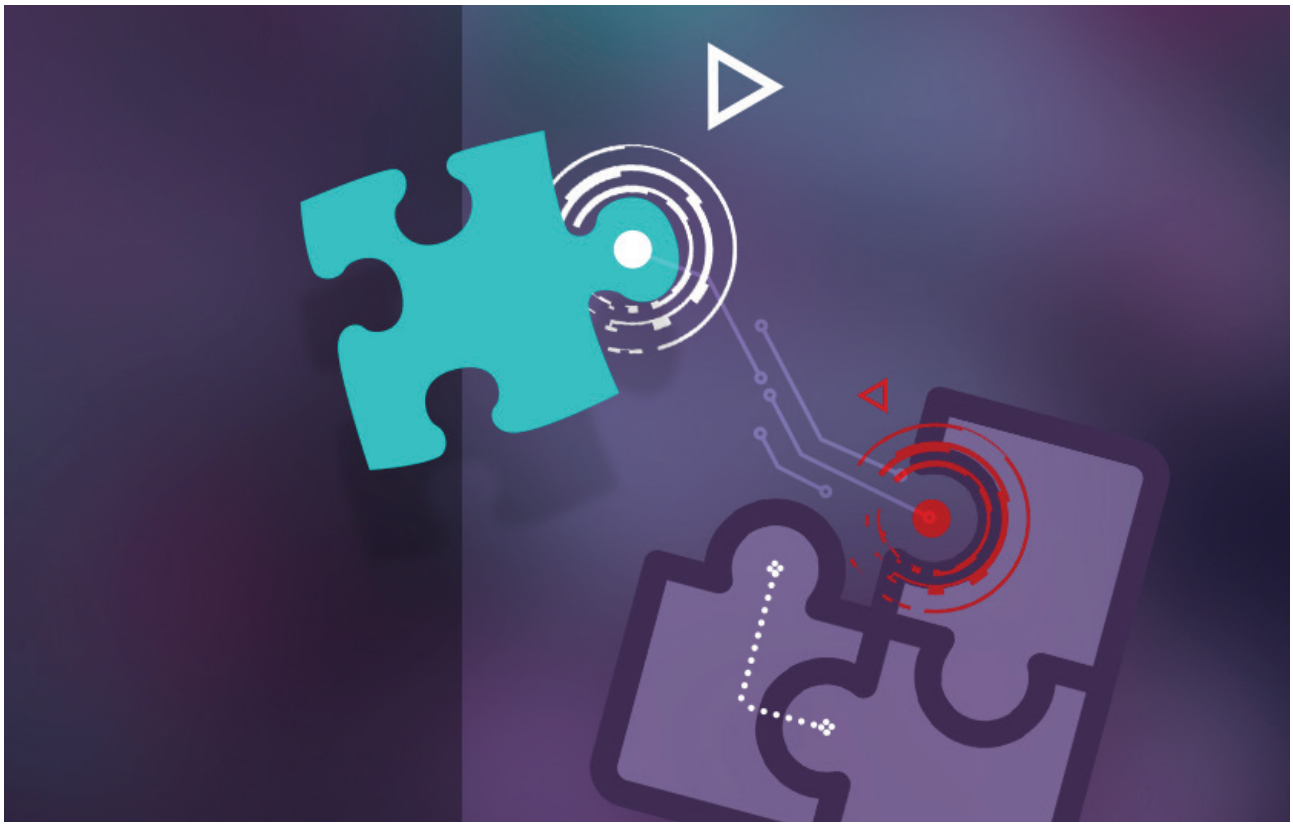
EVOLUTION DES ACTEURS APT

La rentabilité du cyber espionnage n'a pas échappé à nos ennemis et comme nous nous y attendions, des mercenaires ont fait leur apparition. Cette tendance va s'accentuer afin de répondre aux demandes en cyber-capacités non seulement des sociétés, mais également des acteurs APT connus qui cherchent à sous-traiter des tâches moins critiques sans exposer leurs outils et leur infrastructure à des risques. Nous pourrions jouer avec le concept d' « APT as a service », toutefois nous devons nous attendre à l'évolution des attaques ciblées en vue d'offrir un « Accès as a service », ce qui est plus intéressant. Il s'agit de la vente d'un accès à des cibles importantes qui sont déjà entre les mains de mercenaires.

Si l'on se penche davantage sur l'avenir du cyber espionnage, nous estimons que les membres de groupes APT bien établis (les 1 % du monde des APT si vous voulez) vont sortir de l'ombre. Ce phénomène pourrait se manifester de deux manières : dans le secteur privé avec la prolifération du « hacking back » (défense active) ou en partageant leurs connaissances avec la communauté des experts en sécurité de l'information, par exemple en participant à nos conférences pour faire connaître leur version de l'histoire. En attendant, nous pensons que la Tour de Babel des APT va intégrer de nouvelles langues.

L'AVENIR D'INTERNET

L'infrastructure d'Internet en elle-même a montré des signes de fatigue ces dernières années. Les préoccupations relatives aux réseaux de zombies massifs composés de routeurs, au détournement et au dampening BGP, aux attaques DNS en masse ou aux attaques DDoS via serveurs traduisent un manque de responsabilité et d'application de mesures à l'échelle mondiale. Si l'on passe aux prévisions à plus long terme, on peut se demander à quoi ressemblera Internet si ce concept de « village mondial interconnecté » continue de perdre de sa superbe. Nous pourrions vivre une balkanisation d'Internet avec l'introduction de frontières nationales. À ce stade, les préoccupations relatives à la disponibilité pourraient porter sur les attaques contre les jonctions de service qui garantissent l'accès entre des sections différentes ou sur des tensions géopolitiques qui viseraient les câbles qui relient de grands pans d'Internet. Il se peut même que nous assistions à l'émergence d'un marché noir de la connectivité. Alors que les technologies qui garantissent l'existence des « zones d'ombre » d'Internet continuent de susciter l'intérêt et d'être largement adoptées, il est possible que les développeurs impliqués dans les marchés, les échanges et les forums clandestins continuent de développer leurs technologies pour maintenir vraiment la clandestinité.

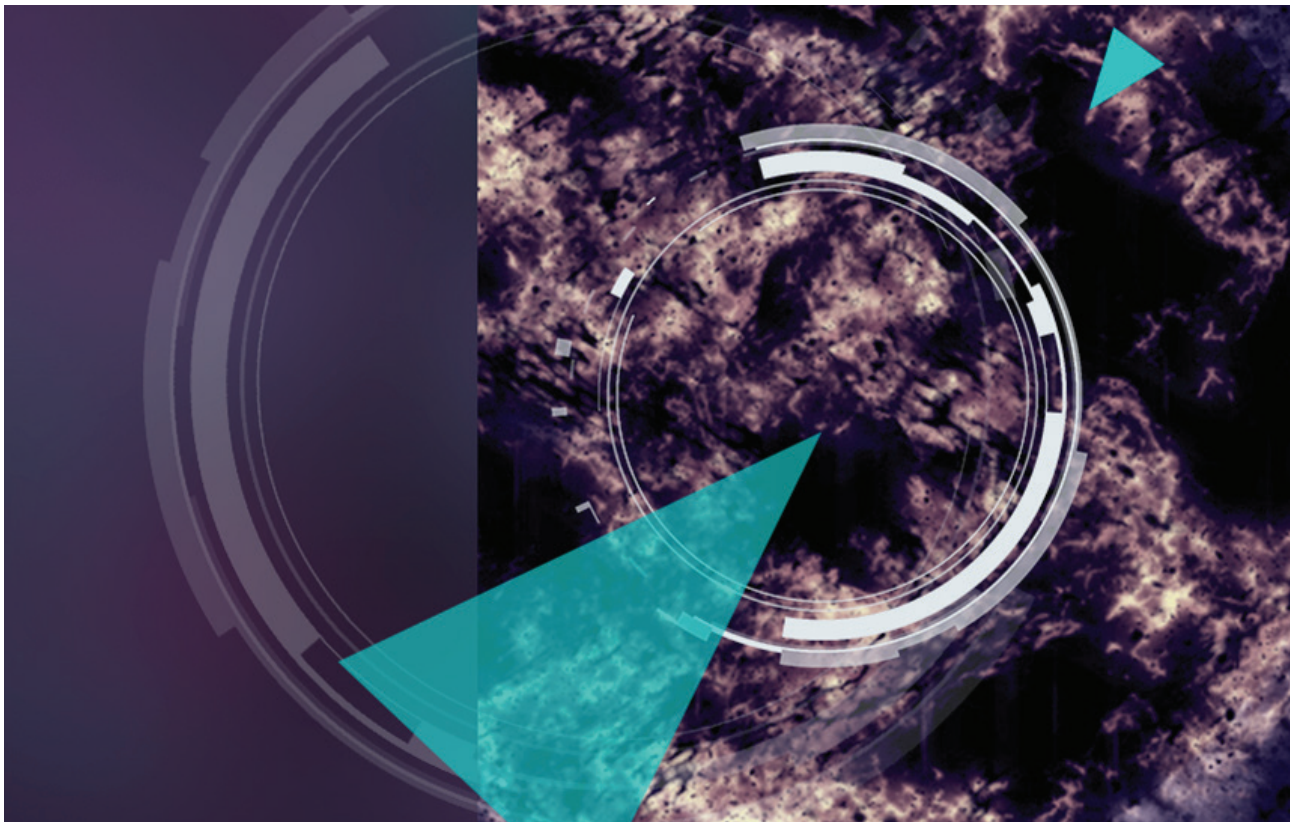


L'AVENIR DU TRANSPORT

Alors que des investissements et des capacités de recherche de pointe sont consacrés au développement de véhicules autonomes destinés à un usage personnel ou professionnel, nous allons voir une augmentation du nombre de systèmes distribués pour la gestion des itinéraires et du trafic d'un volume important de tels véhicules. Il se peut que ces attaques ne se concentrent pas sur les systèmes de distribution en eux-mêmes, mais bien sur l'interception et la substitution des protocoles sur lesquels ils reposent (une preuve de concept des vulnérabilités du système de communication par satellite Global Star a été présentée par un chercheur du Synack lors de la conférence BlackHat de cette année). Les intentions possibles de telles attaques seront le vol de biens de grande valeur ou des dommages cinétiques provoquant des pertes en vies humaines.

LA CRYPTOPOCALYPSE EST PROCHE

Pour conclure, nous nous devons d'insister sur l'importance des normes de chiffrement dans le maintien de la fonction d'Internet en tant qu'outil de partage d'informations et de transactions dont les promesses sont inégalées. Ces normes de chiffrement reposent sur la supposition que la puissance de calcul requise pour décrypter le résultat chiffré est simplement au-delà de nos moyens combinés en tant qu'espèce. Mais que va-t-il se passer le jour où ces capacités de calcul font passer au paradigme suivant comme semblent nous le promettre les prochaines découvertes de l'informatique quantique ? S'il est vrai que ces capacités quantiques ne seront pas directement à la disposition des cybercriminels, cette évolution annonce la fin de la fiabilité des normes de chiffrement actuelles et la nécessité de concevoir et de mettre en place « le chiffrement post quantique ». Etant donné le taux d'adoption ou la mise en œuvre médiocre du chiffrement de haute qualité dans son état actuel, nous ne prévoyons pas de transition en douceur pour contrecarrer les échecs de chiffrements à grande échelle.



Viruslist, la ressource pour la recherche technique, les analyses et réflexions des experts Kaspersky Lab.

Suivez-nous

Site Kaspersky Lab

Blog Eugène Kaspersky

Blog Kaspersky Lab B2C

Blog Kaspersky Lab B2B

Service info sécurité Kaspersky Lab

Académie Kaspersky Lab

Twitter.com/
kasperskyfrance

Facebook.com/
kasperskylabfrance

AO Kaspersky Lab, Rueil, France
www.kaspersky.fr

Informations sur la sécurilté online :
www.viruslist.com/fr
www.kaspersky.fr/entreprise-securite-it/

Informations sur les partenaires proches de chez vous :
http://www.kaspersky.fr/partners