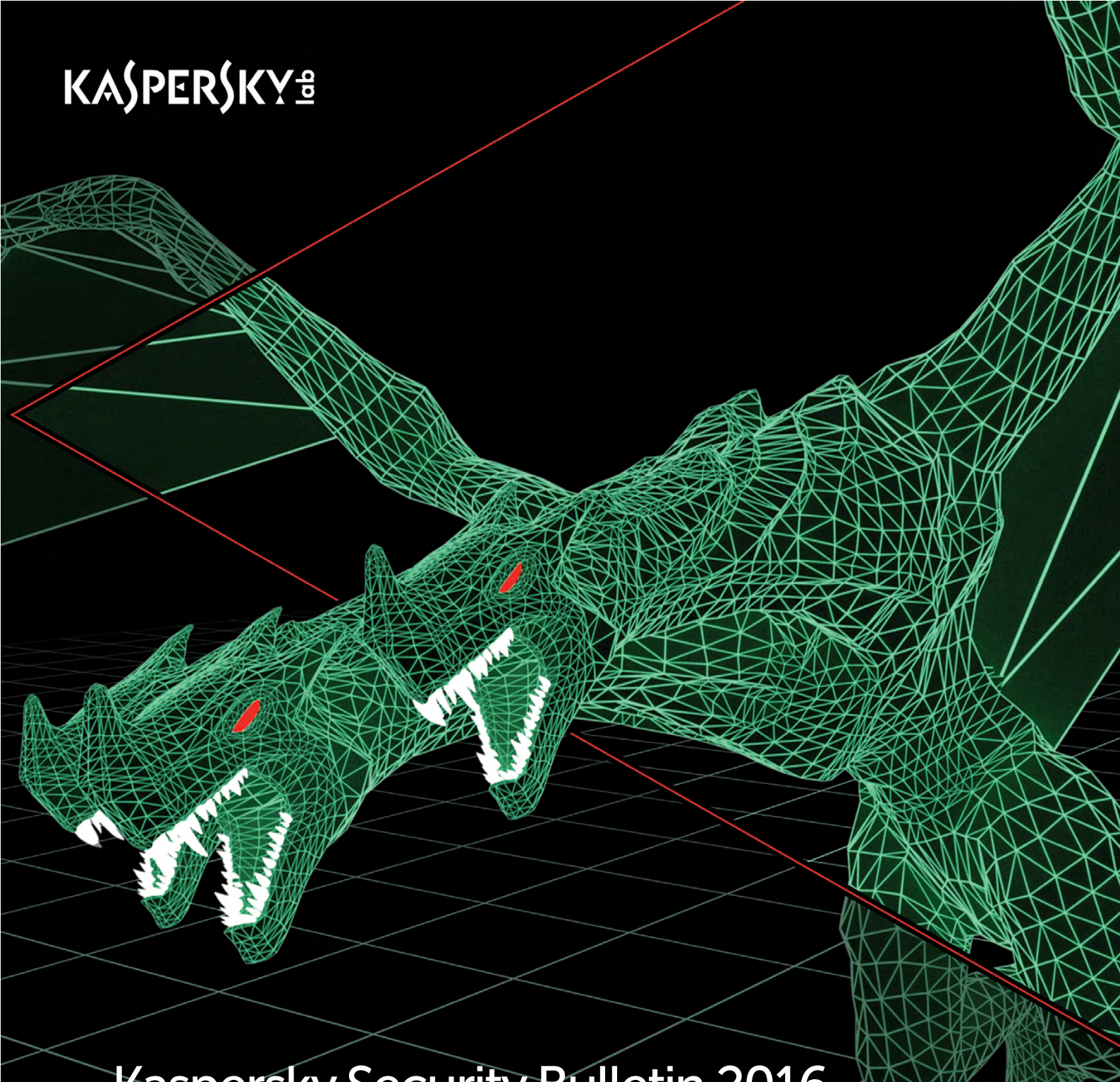
KASPERSKY lab



Kaspersky Security Bulletin 2016

RÉTROSPECTIVE DE L'ANNÉE

David Emm, Roman Unuchek, Kirill Kruglov

GREAT

SOMMAIRE

ATTAQUES CIBLÉES

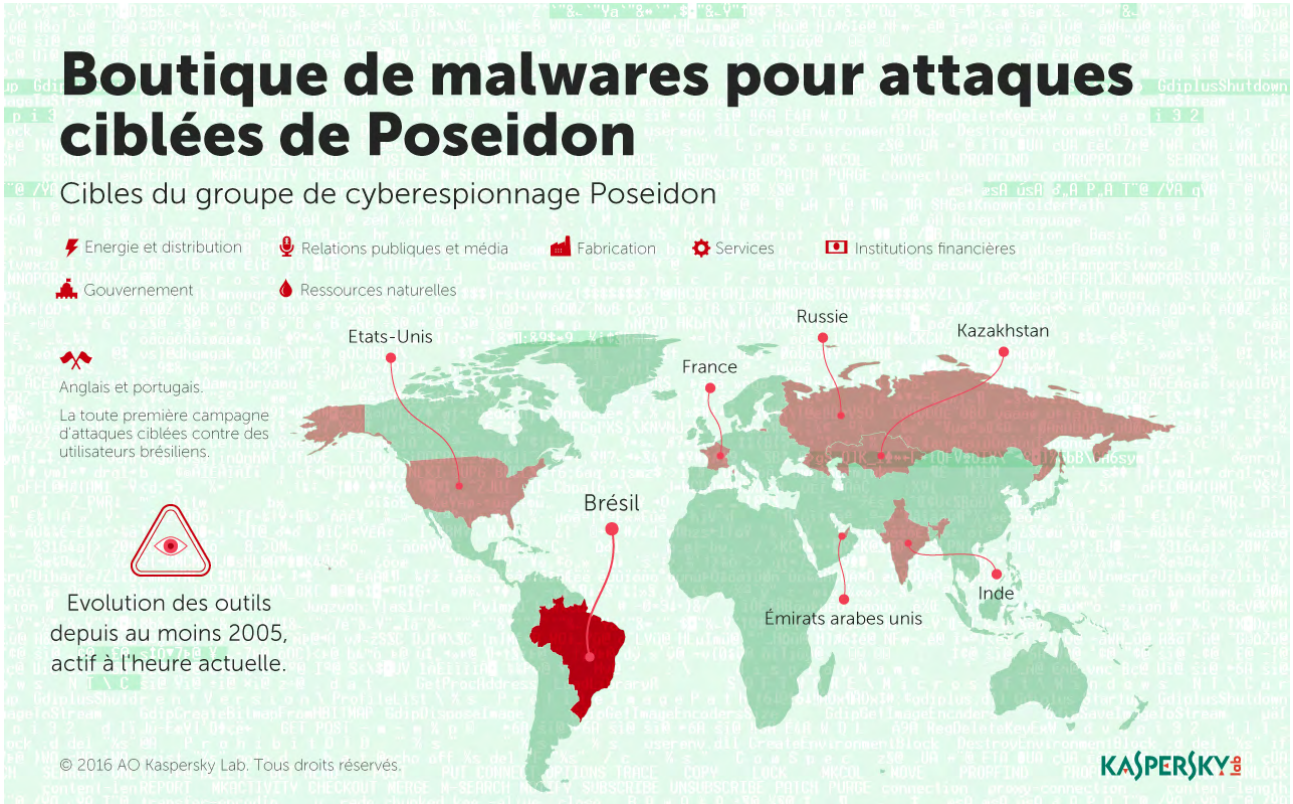
Les attaques ciblées sont bien implantées parmi les menaces et il n'est dès lors pas étonnant de les retrouver dans notre rétrospective annuelle.

Voici les principales campagnes APT que nous avons évoquées cette année.

BlackEnergy

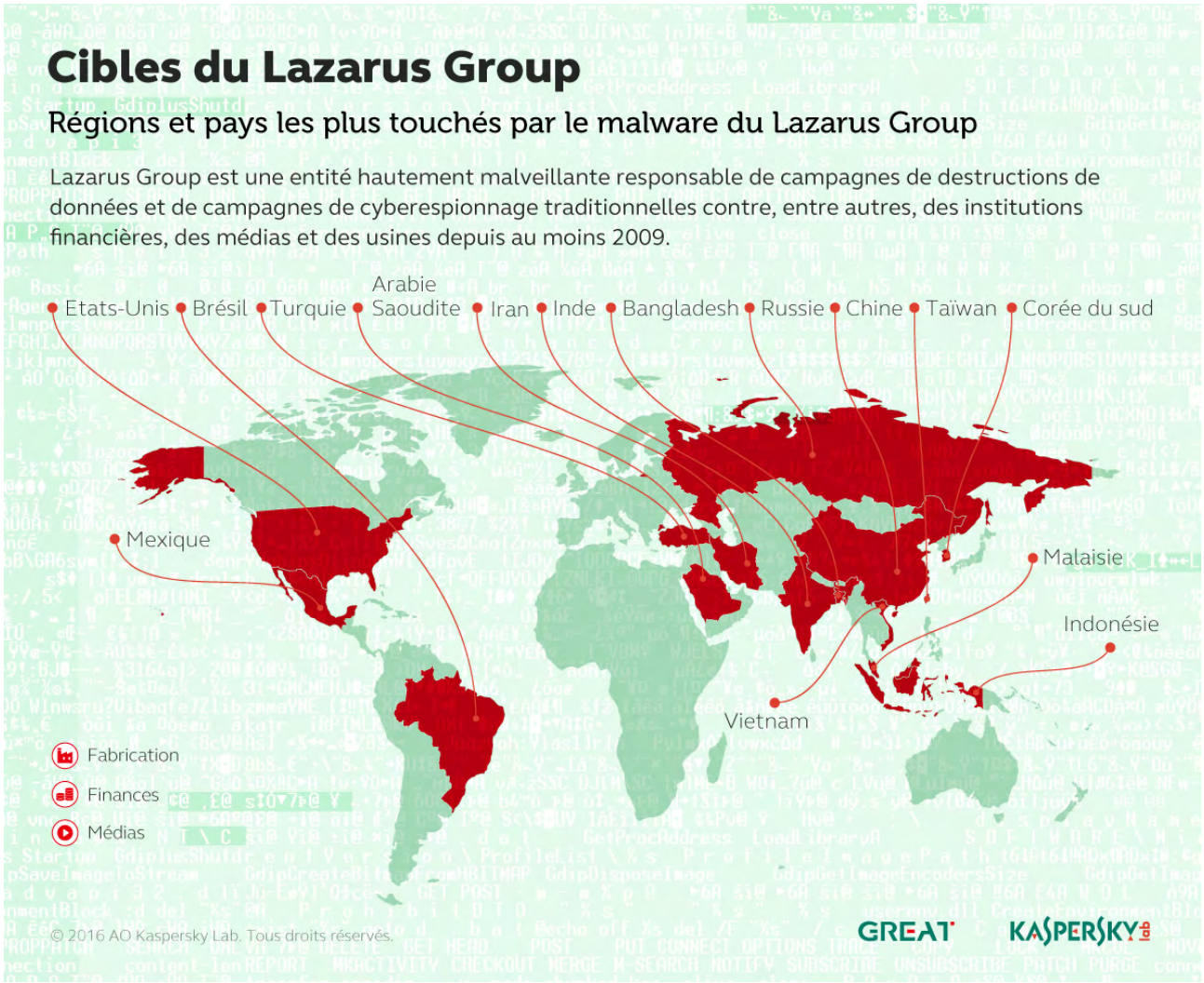
Dans le cadre d'une attaque de grande envergure, BlackEnergy a interrompu la distribution d'électricité, effacé des logiciels et lancé une attaque DDoS

L'année a débuté avec la cyberattaque BlackEnergy contre le secteur énergétique ukrainien. Cette campagne fut unique au niveau des dégâts occasionnés : outre la mise hors service du réseau de distribution d'électricité en Ukraine occidentale, les pirates avaient détruit les données sur les systèmes ciblés et organisé une attaque DDoS par téléphone contre les services d'assistance à la clientèle des sociétés frappées par l'attaque. Les experts de Kaspersky avaient à l'époque levé le voile sur plusieurs facettes de l'activité du groupe à l'origine de l'attaque, et plus particulièrement, ils avaient présenté une analyse de l'outil employé pour pénétrer dans les systèmes ciblés. Si vous souhaitez en savoir plus sur cet incident, nous vous conseillons de lire le rapport concocté par le SANS Institute et l'ICS-CERT du gouvernement américain.



Opération Blockbuster

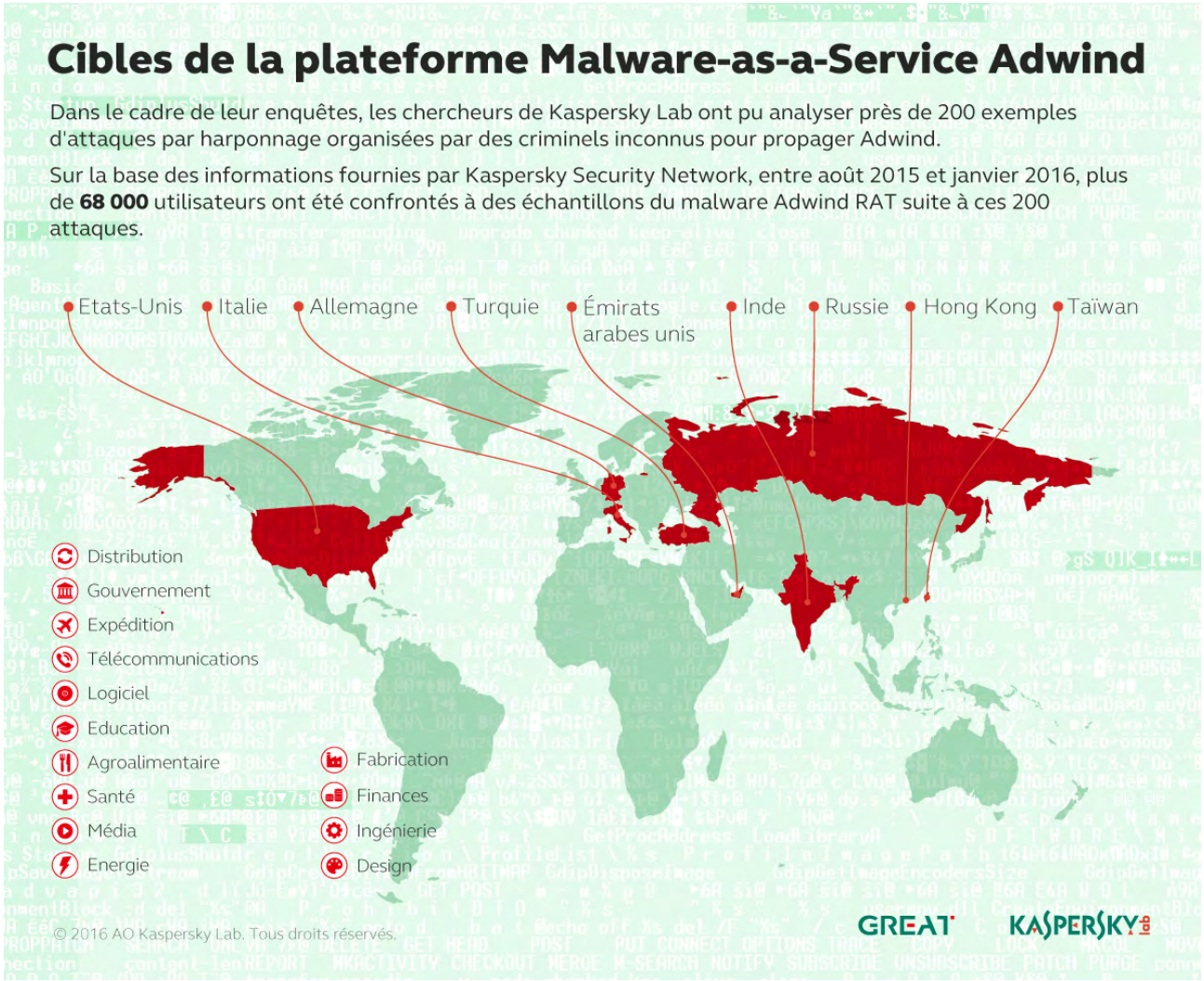
Dans le cadre de l'Opération Blockbuster, plusieurs grandes sociétés spécialisées dans la sécurité de l'information, dont Kaspersky Lab, ont uni leurs efforts pour enquêter sur les activités du groupe Lazarus (notre propre rapport est disponible ici). Lazarus est un gang de cybercriminels qui seraient originaires de la Corée du Nord et qui s'est fait connaître suite à l'attaque organisée contre Sony Pictures en 2014. Ce groupe existe depuis 2009, mais ce n'est qu'après 2011 qu'il a accéléré ses activités. Le groupe Lazarus est à l'origine d'incidents connus comme Troy, Dark Seoul (Wiper) et WildPositron. Le groupe ciblait des entreprises, des institutions financières et des chaînes de radio et de télévision.



Adwind

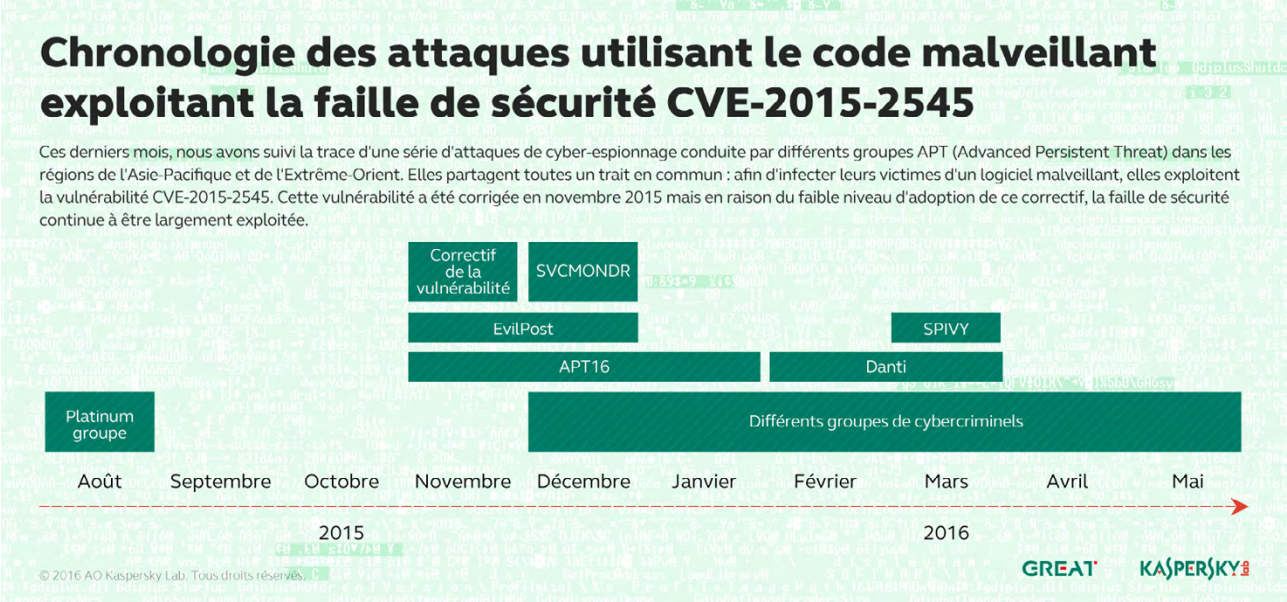
1 800 clients utilisaient le malware à louer d'Adwind

En février, nous avons profité du Security Analyst Summit pour présenter les résultats de notre enquête sur les activités d'Adwind, un outil d'accès à distance (RAT) multiplateforme et multifonction diffusé via un seul service de malware en tant que plateforme. Ce trojan a été rebaptisé à plusieurs reprises depuis son apparition en 2012 : AlienSpy, Frutas, Unrecom, Sockrat, JSocket et jRat. Selon nos calculs, ce malware aurait été utilisé entre 2013 et 2016 dans des attaques qui ont touché plus de 443 000 particuliers et organisations commerciales ou non commerciales à travers le monde. Une des grandes différences entre Adwind et d'autres malwares commerciaux est que celui-ci est diffusé ouvertement en tant que service payant : le client verse un montant déterminé pour pouvoir utiliser le malware. D'après nos estimations, le système comptait près de 1 800 clients à la fin de l'année 2015. Cette plateforme de malware est une des plus grandes à ce jour.



Attaques à l'aide de codes d'exploitation de la vulnérabilité CVE-2015-2545

Au mois de mais, nous avions signalé une vague de campagnes de cyberespionnage menées par différents groupes APT en Extrême-Orient et dans la région Asie-Pacifique. Elles avaient toute un point commun : l'exploitation de la vulnérabilité CVE-2015-2545. Cette faille permet à un attaquant d'exécuter un code arbitraire à l'aide d'une image EPS spécialement conçue pour cette fin. Elle utilise PostScript et peut déjouer les méthodes de protection Randomisation du format de l'espace d'adresse (ASLR) et Prévention de l'exécution des données (PED) intégrées à Windows. On savait déjà que les groupes Platinum, APT16, EvilPost et SPIVY utilisaient ce code d'exploitation. Plus récemment, il a été adopté par les groupes Danti et SVCMONDR. Les différentes campagnes APT qui utilisent cette vulnérabilité sont présentées ici.



Plus de 6 groupes APT ont exploité une même vulnérabilité, corrigée en 2015

Ce qui frappe le plus dans ces attaques, c'est le recours réussi à une vulnérabilité éliminée par Microsoft en septembre 2015. Dans le cadre de nos prévisions pour 2016, nous avions avancé l'idée que les groupes APT consacreraient moins d'efforts au développement d'outils sophistiqués et qu'ils tenteraient d'atteindre leurs objectifs à l'aide de malwares prêts à l'emploi. Et voici une confirmation : recourir à une vulnérabilité connue au lieu de développer un code d'exploitation 0jour.

Les entreprises doivent donc être plus vigilantes dans la gestion des correctifs afin de protéger leur infrastructure informatique.

Opération Daybreak

La campagne de cyberespionnage Opération Daybreak menée par ScarCruft utilisait une vulnérabilité 0jour inconnue : CVE-2016-1010

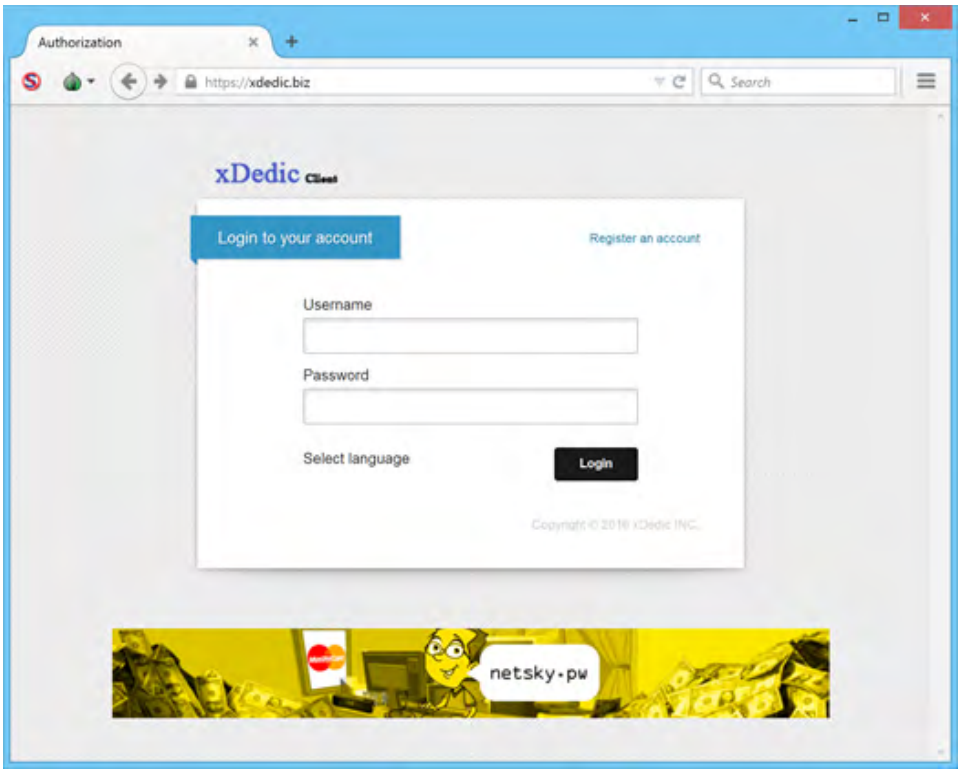
Bien entendu, il y aura toujours des groupes APT qui chercheront à profiter de codes d'exploitation 0jour. Ainsi, nous avons évoqué en juin la campagne de cyberespionnage Opération Daybreak organisée par le groupe ScarCruft. Celle-ci reposait sur un code d'exploitation pour Adobe Flash Player inconnu jusque là (CVE-2016-1010). Ce groupe est relativement récent et demeure encore assez discret. Nous pensons toutefois qu'il pourrait s'agir du groupe à l'origine de la diffusion d'un autre code d'exploitation 0jour (CVE-2016-0147) dont le correctif a été diffusé en avril. Ce groupe a ciblé entre autres des autorités judiciaires et policières asiatiques, une des plus grandes sociétés commerciales au monde, une société de régie publicitaire mobile et de monétisation d'apps aux Etats-Unis, des particuliers en contact avec l'Association internationale des fédérations d'athlétisme et un restaurant établi dans un des principaux centres commerciaux de Dubaï.

S'il est vrai qu'il est impossible de garantir une sécurité à 100 %, nous pouvons toujours adopter la politique qui consiste à renforcer la protection jusqu'au point où le coût de l'organisation d'une attaque contre cette cible poussera les individus malintentionnés à abandonner ou à choisir une autre cible. La meilleure manière de se protéger contre les attaques ciblées consiste à adopter une démarche à plusieurs niveaux qui réunit les technologies traditionnelles de lutte contre les virus et la gestion des correctifs, la détection des intrusions sur l'hôte et une stratégie de liste blanche basée sur le refus par défaut. D'après une étude organisée par l'Australian Signals Directorate, 85 % des attaques ciblées auraient pu être déjouées en suivant quatre stratégies élémentaires d'atténuation des risques : création d'une liste blanche d'applications, mise à jour des applications, mise à jour des systèmes d'exploitation et restriction des privilèges d'administrateur.

xDedic

xDedic était une bourse pour au moins 70 000 serveurs piratés. La majorité des victimes ne s'était rendue compte de rien

Cette année, Kaspersky Lab a mené une enquête sur xDedic, une plateforme cybercriminelle d'échanges. Il s'agit d'un marché noir en ligne qui propose des informations d'identification piratées pour des serveurs à travers le monde, le tout accessible via Remote Desktop Protocol (RDP). Au départ, nous avions pensé que ce marché concernait 70 000 serveurs, mais de nouvelles données en notre possession semblent indiquer que le marché xDedic était bien plus grand et qu'il proposait des informations pour 176 000 serveurs. xDedic propose un moteur de recherche qui permet aux acheteurs potentiels de trouver presque tout parmi des réseaux gouvernementaux ou d'entreprise pour seulement 8 dollars par serveur. Ce prix démocratique permet aux « clients » d'accéder aux données conservées sur ces serveurs et d'utiliser ces derniers comme tête de pont pour d'autres attaques ciblées.



L'existence d'un marché clandestin qui propose des solutions « clé sur porte » n'est pas une nouveauté. Nous observons toutefois une spécialisation plus poussée. Et s'il est vrai que le modèle adopté par les propriétaires de xDedic n'est pas facilement reproductible, il faut s'attendre à ce que d'autres marchés spécialisés voient le jour dans un avenir proche.

Dropping Elephant

Dropping Elephant a démontré la puissance redoutable d'une ingénierie sociale rondement menée

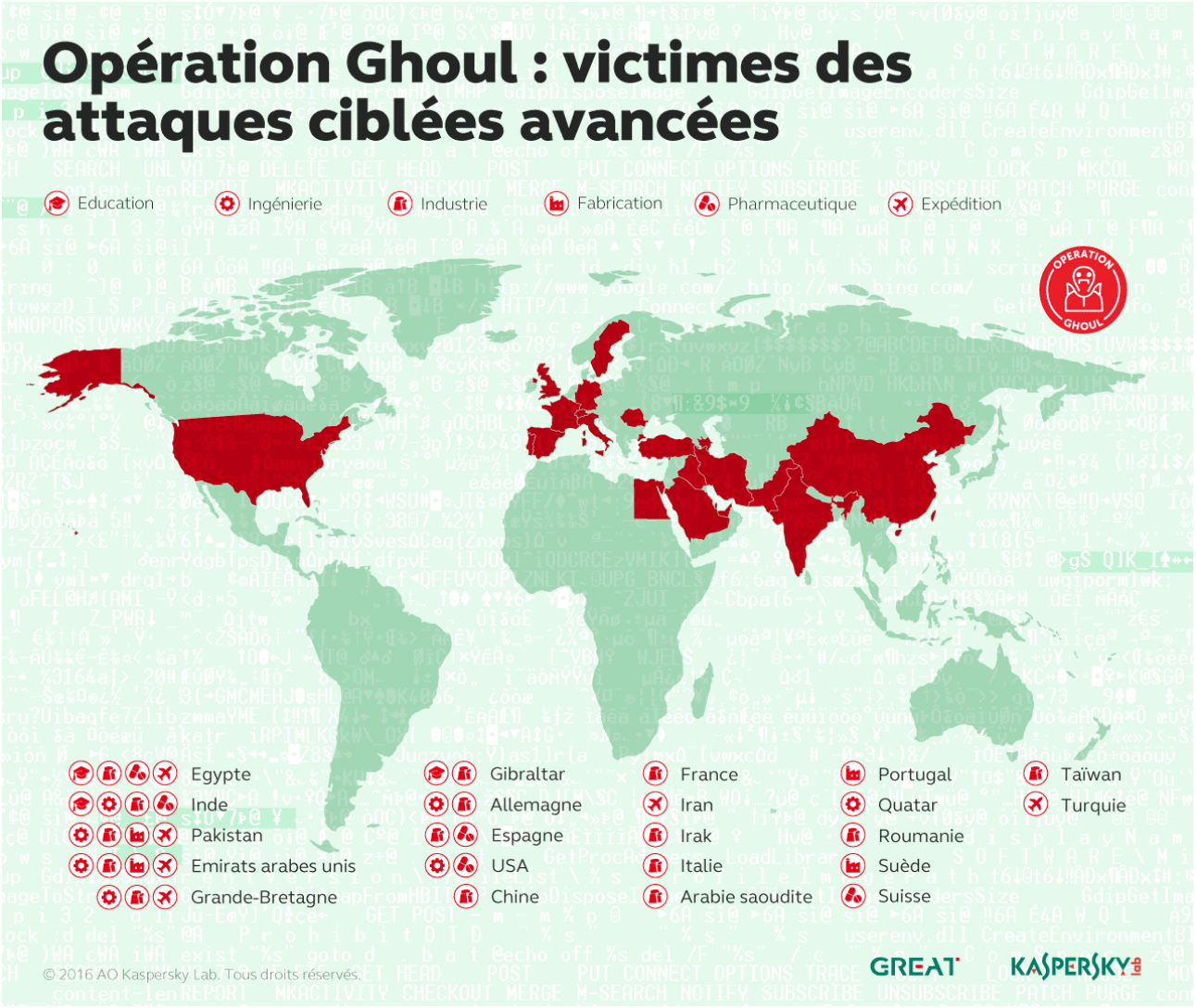
Les campagnes d'attaques ciblées ne doivent pas forcément être à la pointe du progrès pour être efficaces. Au mois de juillet, nous vous parlions d'un groupe baptisé Dropping Elephant (connu également sous les noms de « Chinastrats » ou « Patchwork »). Grâce à un cocktail composé d'ingénierie sociale, d'un ancien code d'exploitation et d'un malware PowerShell, ce groupe a réussi à voler des données sensibles auprès de ses victimes qui appartenaient à des organisations diplomatiques et économiques importantes impliquées dans les relations étrangères chinoises. Les attaquants utilisent un mélange de messages de harponnage et d'attaques selon la technique du « point d'eau ». Les succès remportés par le groupe Dropping Elephant sont étonnants car le ciblage de ces victimes de haut vol n'impliquait aucun code d'exploitation 0jour, ni aucune technique de pointe. Au contraire, Dropping Elephant démontre une fois de plus que des investissements modestes et l'utilisation d'outils génériques peuvent être d'une efficacité redoutable quand ils sont associés à des techniques d'ingénierie sociale très bien étudiées.

Les probabilités de réussite de telles attaques peuvent être réduites via l'application des mises à jour de sécurité et l'amélioration de la prise de conscience du personnel sur les questions de sécurité.

Opération Ghoul

Opération Ghoul a confirmé cette efficacité avec une campagne de phishing ciblée avec précision et un malware commercial

L'efficacité de l'ingénierie sociale pour aider les attaquants à s'introduire dans une organisation ciblée a également été confirmée par Opération Ghoul, le groupe à l'origine d'une série d'attaques que nous avons évoquées en juin 2016. Les attaquants avaient envoyé des messages de harponnage avec des pièces jointes malveillantes. Ces messages, qui semblaient provenir d'une banque établie aux Emirats arabes unis, étaient destinés principalement aux cadres intermédiaires et supérieurs de différentes entreprises. Le message offrait des conseils de paiement de la banque et possédait un document SWIFT en pièce jointe. Dans la réalité, l'archive contenait un malware. Sur la base des informations obtenues après avoir appliqué la technique du sink-hole à certains serveurs de commande, nous avions pu affirmer que la majorité des organisations ciblées étaient actives dans les secteurs de l'industrie et de l'ingénierie. Mais il y avait également des organisations issues du transport, du secteur pharmaceutique, de la fabrication, du commerce et de l'enseignement.



Le malware utilisé par le groupe Operation Ghoul repose sur le kit de logiciel espion commercial Hawkeye, en vente livre sur le dark Web. Une fois installé, le malware recueille les données intéressantes sur l'ordinateur de la victime, y compris les frappes au clavier, les données du Presse-papier, les informations d'authentification sur les serveurs FTP, les données des comptes dans les navigateurs, les clients de messagerie instantanée, les clients de messagerie électronique et les informations sur les applications installées.

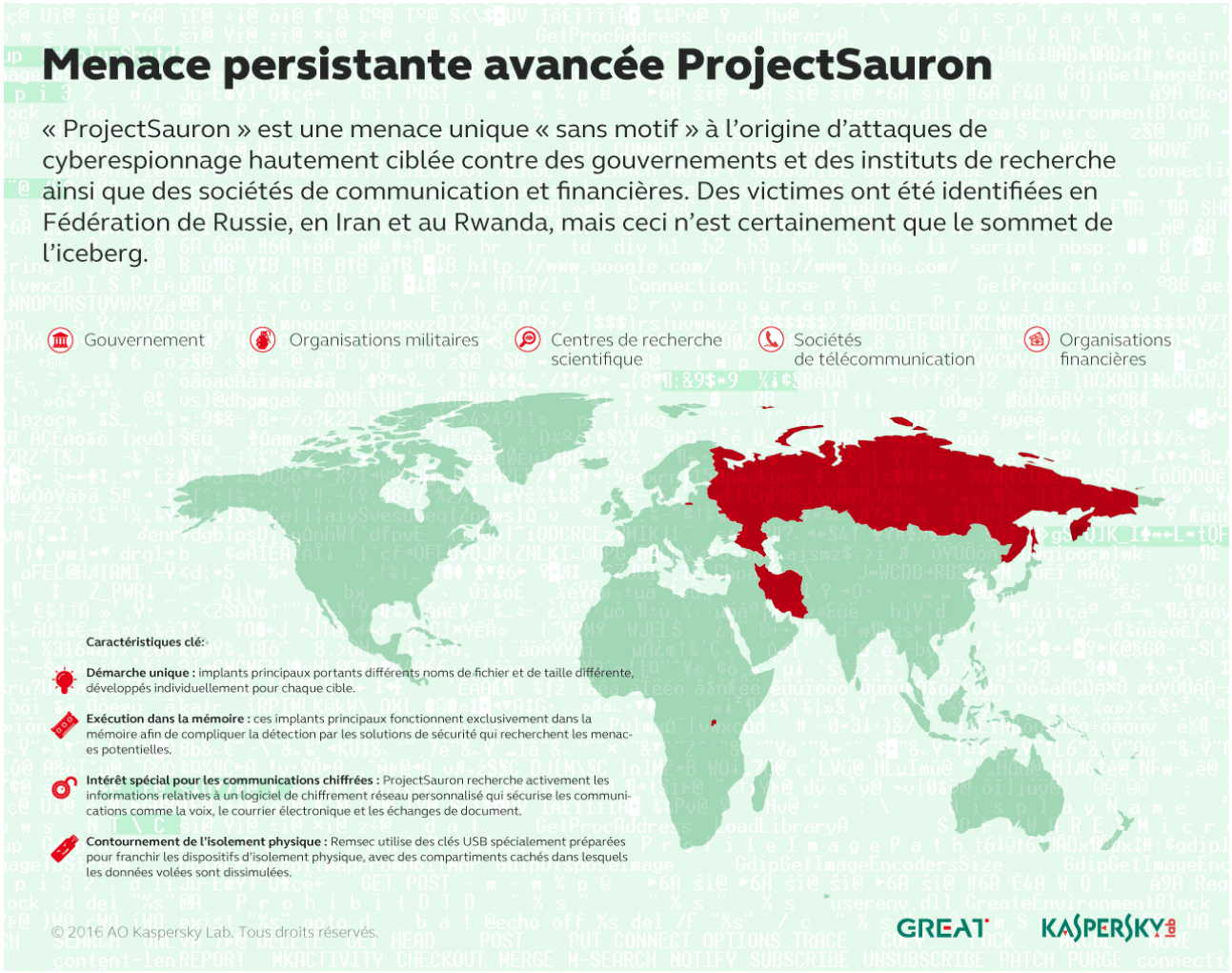
Les succès répétés de l'ingénierie sociale en tant que méthode d'accès à l'intérieur des entreprises souligne la nécessité d'éduquer le personnel et de placer la formation au cœur des stratégies de sécurité.

ProjectSauron

ProjectSauron a révolutionné le secteur à tout jamais avec sa plateforme d'espionnage modulaire dotée d'outils uniques pour chaque victime

Au mois de septembre, nous avons découvert ProjectSauron, un groupe actif depuis juin 2011 et spécialisé dans le vol de données confidentielles d'organisations établies en Russie, en Iran et au Rwanda ainsi que probablement dans d'autres pays.

Les coûts impliqués, la complexité, la persistance et l'objectif de l'opération (à savoir voler des données secrètes dans des organisations liées au gouvernement) laissent supposer que la campagne ProjectSauron est sponsorisée par un Etat. Les aspects techniques montrent que les attaquants ont tiré des enseignements d'autres attaques très sophistiquées dont Duqu, Flame, Equation et Regin au point d'adopter certaines des techniques les plus révolutionnaires et d'améliorer les tactiques pour ne pas être découverts. Chaque élément malveillant est personnalisé pour une cible donnée, ce qui lui ôte toute valeur en tant qu'indicateur de compromission pour toute autre victime.



Caractéristiques clés de ProjectSauron :

1. ProjectSauron est une plateforme modulaire conçue pour mener des campagnes de cyberespionnage à long terme.
2. Tous les modules et les protocoles de réseau adoptent des algorithmes de chiffrement robustes comme RC6, RC5, RC4, AES, Salsa20, etc.
3. Il emploie un moteur de script Lua modifié pour mettre en œuvre la plateforme principale et ses plug-ins.
4. Il y a au moins 50 types de plug-in différents.
5. Le groupe derrière ProjectSauron est très intéressé par les logiciels de chiffrement de communication largement utilisés dans les organisations gouvernementales ciblées. Il vole les clés de chiffrement, les fichiers de configuration et les adresses IP des serveurs d'infrastructure clé en rapport avec le logiciel de chiffrement.
6. Il est également capable d'extraire les données des réseaux placés derrière un air gap à l'aide de périphériques de stockage USB préparés à cette fin et dotés d'une zone de stockage invisible pour le système d'exploitation.
7. La plateforme utilise abondamment le protocole DNS pour extraire les données et générer des rapports en temps réel.
8. Ce groupe APT a débuté ses opérations dès juin 2011 et est demeuré actif jusqu'en avril 2016.
9. Le vecteur d'infection initiale employé pour pénétrer dans le réseau des victimes reste inconnu à ce jour.
10. Les attaquants utilisent des canaux de distribution de logiciel légitimes pour le déplacement latéral dans les réseaux infectés.

L'utilisation une fois de méthodes uniques comme le serveur de commande, les clés de chiffrement, etc. en plus de l'adoption de technologies de pointe issues d'autres grands groupes de menace, est une nouveauté.

La seule protection efficace contre de telles menaces consiste à déployer plusieurs couches de sécurité, avec des capteurs capables de détecter la moindre anomalie dans le flux de travail de l'organisation, sans oublier la collecte de renseignements sur les menaces et les analyses d'investigation numérique. Si vous souhaitez en savoir plus sur les méthodes à votre disposition pour lutter contre ces menaces, consultez cette page.

MENACES FINANCIÈRES

Le ciblage des clients d'une banque demeure la manière la plus directe pour un cybercriminel de gagner de l'argent. En général, les attaquants se tournent vers l'ingénierie sociale pour amener leurs victimes à divulguer des informations personnelles ou à installer un malware qui récoltera les données personnelles, comme les mots de passe, indispensables pour accéder aux comptes en banque. En 2016, les solutions de Kaspersky Lab ont bloqué l'exécution de malwares capable de voler de l'argent via les systèmes de banque électronique sur **2 871 965** périphériques.

Ceci étant dit, les cybercriminels ne visent pas que les clients des banques. Nous avons en effet observé au cours de ces dernières années une augmentation du nombre d'attaques directes contre des banques et autres institutions financières. La plus célèbre d'entre elles est probablement Carbanak qui utilisait des techniques d'infiltration propres aux attaques ciblées pour voler de l'argent. Nous avons recensé cette année d'autres attaques contre des institutions financières.

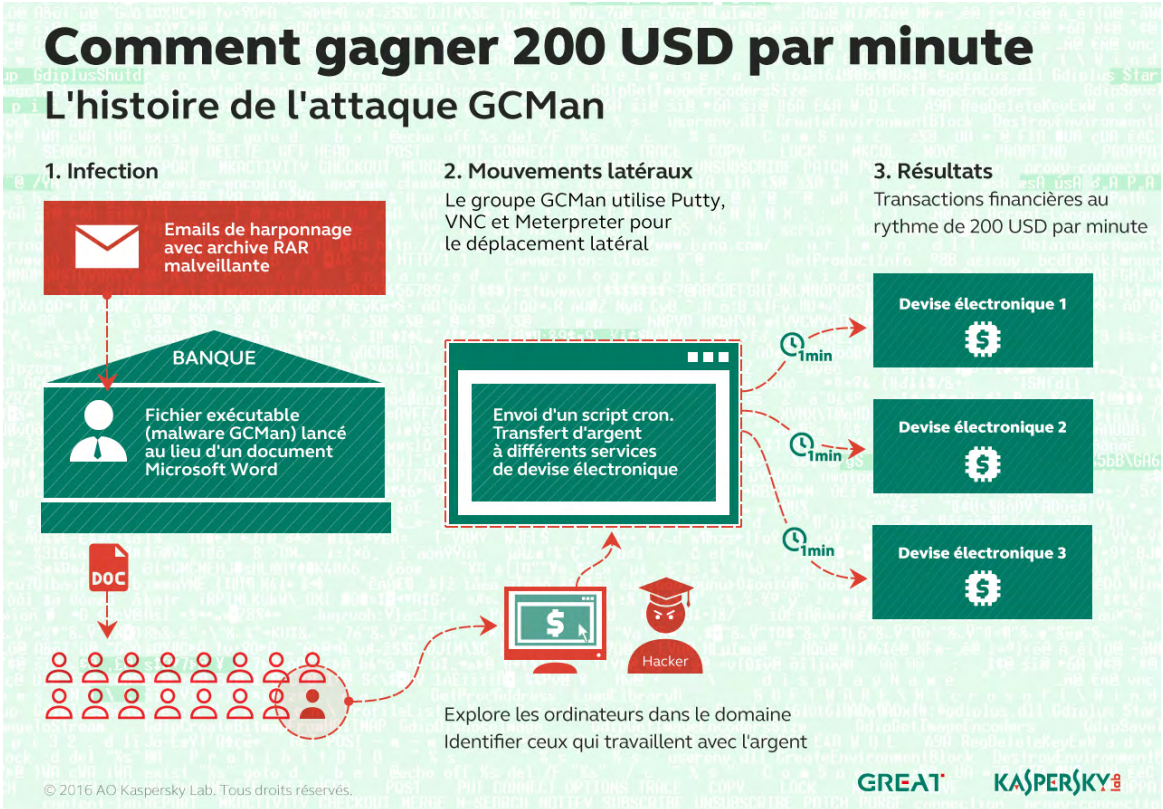
Metel organisait des attaques ciblées contre des banques, puis envoyait des équipes pendant la nuit pour retirer l'argent dans les DAB

En février 2016, Kaspersky Lab a dévoilé les activités d'autres groupes APT qui ciblaient des institutions financières. Le groupe à l'origine de Metel a utilisé le harponnage et des codes d'exploitation pour navigateur afin d'infiltrer le réseau interne de banques et de prendre les commandes d'ordinateurs clé au sein de l'infrastructure informatique de la banque. Ce niveau d'accès permettait aux criminels d'automatiser l'annulation des transactions dans les distributeurs automatiques de billets (DAB) : les membres du gang pouvaient utiliser des cartes de débit pour voler de l'argent via des DAB sans affecter le solde de la carte. Ils pouvaient ainsi réaliser de multiples transactions sur différents DAB. Notre enquête a déterminé que les membres du gang parcouraient les rues de plusieurs villes russes la nuit en voiture et volaient de l'argent dans les DAB de différentes banques. Ils travaillaient toujours de nuit et volaient l'argent en différents endroits. Nous avons détecté la présence de Metel dans plus de 30 institutions financières, mais notre équipe de réaction face aux incidents a pu nettoyer les réseaux infectés avant que le groupe n'ait eu le temps de provoquer des dégâts trop importants. Ceci étant dit, les cybercriminels à l'origine de Metel sont toujours actifs et nous pensons que ce malware est probablement beaucoup plus répandu.

METEL : GARDER SON SANG FROID ET ANNULER LES TRANSACTIONS

*TOUS LES NOMS DE CE TABLEAU SONT FICTIFS. TOUTE RESSEMBLANCE EST PUREMENT FORTUITE.

GCMAN (baptisé ainsi parce que le malware repose sur du code compilé à l'aide du compilateur GCC) est un autre exemple dans cette catégorie. Le groupe s'infiltre dans les institutions financières à l'aide de messages de harponnage contenant un fichier RAR malveillant. L'ouverture de l'archive entraîne l'exécution d'un fichier exécutable qui débouche sur l'infection initiale. Une fois que le groupe a mis un pied dans l'organisation, il utilise des outils légitimes pour test de pénétration comme Putty, VNC et Meterpreter afin de pouvoir réaliser des déplacements latéraux dans l'organisation jusqu'il trouve des ordinateur stratégiques qu'il pourra utiliser pour transférer l'argent vers des services de devise électronique. Pour ce faire, les attaquants implantent un script Cron sur un des serveurs de la banque (Cron est un programmateur utilisé dans les systèmes d'exploitation Unix) qui leur permet de réaliser des transactions financières au rythme de 200 dollars par minute. Ce script est invoqué toutes les minutes pour envoyer de nouvelles transactions directement à un système de traitement de paiements en amont. Heureusement pour elles, les institutions financières ont remarqué l'activité suspecte et ont annulé les transactions. Si cela n'avait pas été le cas, les attaquants auraient réussi à transférer de l'argent à plusieurs services de devise électronique sans devoir consigner ces transactions dans un système de la banque. Les chercheurs de Kaspersky Lab ont travaillé avec trois institutions financières en Russie qui avaient été infectées par le malware CGMAN. Ceci étant dit, nous pensons que cette menace est beaucoup plus répandue.



CGMAN a passé 18 mois à récolter des informations auprès des victimes infectées avant de passer à l'attaque avec des outils légitimes pour le déplacement latéral

Nous avons appris que la véritable attaque avait eu lieu 18 mois avant la détection du malware. Le groupe avait exécuté une attaque par injection SQL dans un logiciel commercial exécuté sur un des serveurs Internet public de la banque et il était repassé 18 mois plus tard afin d'exploiter les informations recueillies et d'infiltrer la banque. Deux mois avant cet incident, un individu avait essayé différents mots de passe pour un compte d'administrateur sur un serveur de la banque : les attaquants étaient persistants, mais ils se limitaient à seulement trois tentatives par semaine le samedi et ce, pour ne pas attirer l'attention des équipes de sécurité au sein des institutions ciblées. Les activités du groupe GCMAN attirent l'attention sur une tendance émergente parmi les différentes menaces en circulation, à savoir l'utilisation d'outils légitimes au lieu de modules de malware personnalisés.

> Les outils légitimes sont tout aussi efficaces, déclenchent moins de fausses alarmes et garantissent une rentabilité de l'investissement plus rapide pour les cybercriminels. Il est primordial que les équipes chargées de la sécurité de l'information en tiennent compte au moment de revoir leur stratégie de sécurité d'entreprise.

Vous trouverez ici de plus amples informations sur les campagnes Metel et GCMAN.

Bien entendu, les banques ne fonctionnent dans l'isolement, chacune de son côté. Les transferts d'argent internationaux requièrent un réseau interbancaire appelé SWIFT (Society for Worldwide Interbank Financial Telecommunication).

Après le vol de 100 millions de dollars, de nombreuses banques ont été obligées d'améliorer leurs procédures d'authentification et de mise à jour du logiciel SWIFT

En février 2016, des pirates ont exploité les données d'accès au réseau SWIFT d'employés de la banque centrale du Bangladesh et ont envoyé à la branche new-yorkaise de la Réserve fédérale des Etats-Unis des requêtes frauduleuses de transfert de plusieurs millions de dollars vers plusieurs banques asiatiques. Les pirates ont ainsi réussi à transférer 81 millions de dollars américains sur un compte de la Rizal Commercial Banking Corporation aux Philippines et 20 millions supplémentaires sur un compte de la Pan Asia Banking. Les pertes auraient pu être bien supérieures si un employé de la Réserve fédérale n'avait pas remarqué une faute de frappe dans une des demandes de transfert : les pirates avaient écrit « fandation » au lieu de « foundation ». La banque centrale du Bangladesh pu ainsi arrêter d'autres transactions pour une montant de 850 millions de dollars. L'article est accessible ici. D'autres attaques organisées à l'aide de données d'identification SWIFT volées ont été signalées depuis le vol de la banque centrale du Bangladesh.

Le groupe à l'origine de Metel n'a pas été le seul à viser les DAB. Le malware pour DAB n'est pas un phénomène récent, mais le nombre de malwares de ce type a augmenté au cours de ces dernières années. Avant 2016, le cas le plus marquant avait été celui de Tyupkin. Des attaquants avaient obtenu un accès physique au DAB et ils avaient introduit un CD de démarrage pour prendre les commandes de la machine..

En mais 2016, nous avions signalé l'apparition d'une nouvelle version du malware pour DAB Skimmer. Ce rapport était la conclusion d'une enquête que nous avions réalisée l'année antérieure suite à un incident. L'origine de ce malware remonte à 2009. Depuis lors, il a été revu, à l'instar des tactiques des cybercriminels qui l'utilise. La nouvelle version cible des DAB à travers le monde. Nous avons enregistré des attaques aux Emirats arabes unis, en France, aux Etats-Unis, en Russie, à Macau, en Chine, aux Philippines, en Espagne, en Allemagne, en Géorgie, en Pologne, au Brésil et en République tchèque.

Les DAB non sécurisés sont devenus une cible de choix pour les cyberattaques

Au lieu d'adopter la méthode qui a fait ses preuves et qui consiste à installer un faux lecteur de carte sur le DAB, les attaquants ont préféré ici prendre les commandes du DAB. Tout d'abord, ils installent le malware Skimmer sur le DAB, soit via un accès physique, soit en attaquant le réseau interne de la banque. Le malware infecte la partie centrale du DAB, à savoir la partie responsable de l'interaction avec l'infrastructure générale de la banque, le traitement de la carte et la distribution des billets. A la différence d'un skimmer traditionnel, aucun élément physique ne laisse penser que le DAB est infecté. Les attaquants peuvent donc capturer en toute quiétude les données des cartes utilisées sur le DAB, y compris le numéro compte du client et le code PIN de la carte) ou voler de l'argent directement.

Le cybercriminel « réveille » le DAB infecté en introduisant une carte qui contient des enregistrements spécifiques sur une bande magnétique. Après avoir lu la carte, Skimmer est en mesure d'exécuter une commande codée en dur ou de recevoir des instructions via un menu spécial activé par la carte. L'interface utilisateur de Skimmer apparaît uniquement après que la carte a été éjectée et seulement si le cybercriminel saisit le code de session correct dans les 60 secondes. Le menu contient 21 options, dont la distribution de billets, la collecte des détails des cartes introduites dans le DAB, la suppression automatique et la réalisation de mises à jour. Le cybercriminel peut enregistrer les détails des cartes sur la puce de sa propre carte ou imprimer les données récoltées.

Les attaquants évitent d'attirer l'attention. Au lieu de retirer l'argent directement sur le DAB, une action qui entraînerait une détection immédiate, ils préfèrent attendre, parfois plusieurs mois. Dans la majorité des cas, ils utilisent les données recueillies pour cloner des cartes plus tard. Ils utilisent ces cartes clonées sur d'autres DAB non infectés et retirent de l'argent sur les comptes des victimes d'une manière qui permet de brouiller toute piste vers le DAB compromis.

L'augmentation du nombre d'attaques contre des DAB au cours des dernières années s'inscrit dans l'évolution naturelle de la méthode bien établie qui repose sur l'utilisation de skimmers physiques pour voler les données des cartes introduites dans les DAB qui ont été altérés. Malheureusement, de nombreux DAB tournent sous des systèmes d'exploitation qui présentent de nombreux points faibles au niveau de la sécurité. C'est pour cette raison que la sécurité physique est encore plus importante.

Kaspersky Lab a formulé plusieurs recommandations pour aider les banques à se protéger. Les voici : réalisation d'analyses antivirus à intervalle régulier ; adoption des technologies de liste blanche ; utilisation d'une bonne stratégie de gestion des dispositifs ; adoption du chiffrement de disque complet ; protection par mot de passe de la BIOS des DAB ; mise en œuvre du démarrage depuis le disque dur et isolement du réseau des DAB du reste du l'infrastructure de la banque. Un de nos experts a réalisé une analyse détaillée de la conversion malveillante des DAB en machines à sous et a avancé quelques pistes sur les mesures à adopter pour sécuriser ces dispositifs.

Les nouveaux skimmers biométriques visent la nouvelle génération de systèmes d'authentification : reconnaissance des empreintes, de l'iris et des veines de la paume de la main

Bien entendu, nous ne nous contentons pas de réaliser des enquêtes sur des incidents qui ont eu lieu. Nous étudions également les technologies émergentes et les manières dont elles pourraient être détournées par les cybercriminels. Nous avons publié il y a peu les résultats de notre enquête sur les méthodes potentielles d'authentification, dont l'authentification sans contact via NFC, les mots de passe à usage unique et les données biométriques. Vous serez peut-être surpris d'apprendre que nous avons identifié 12 fabricants qui proposent déjà de faux lecteurs d'empreintes digitales (skimmers biométriques) et au moins trois autres vendeurs qui étudient les moyens qui pourraient permettre aux criminels d'obtenir les données des systèmes de reconnaissances des veines de la paume et d'iris. Le rapport est disponible ici.

L'INTERNET DES OBJETS

Le risque de tout connecter, malgré tout — en 2016, tout est dit, n'est-ce pas ?

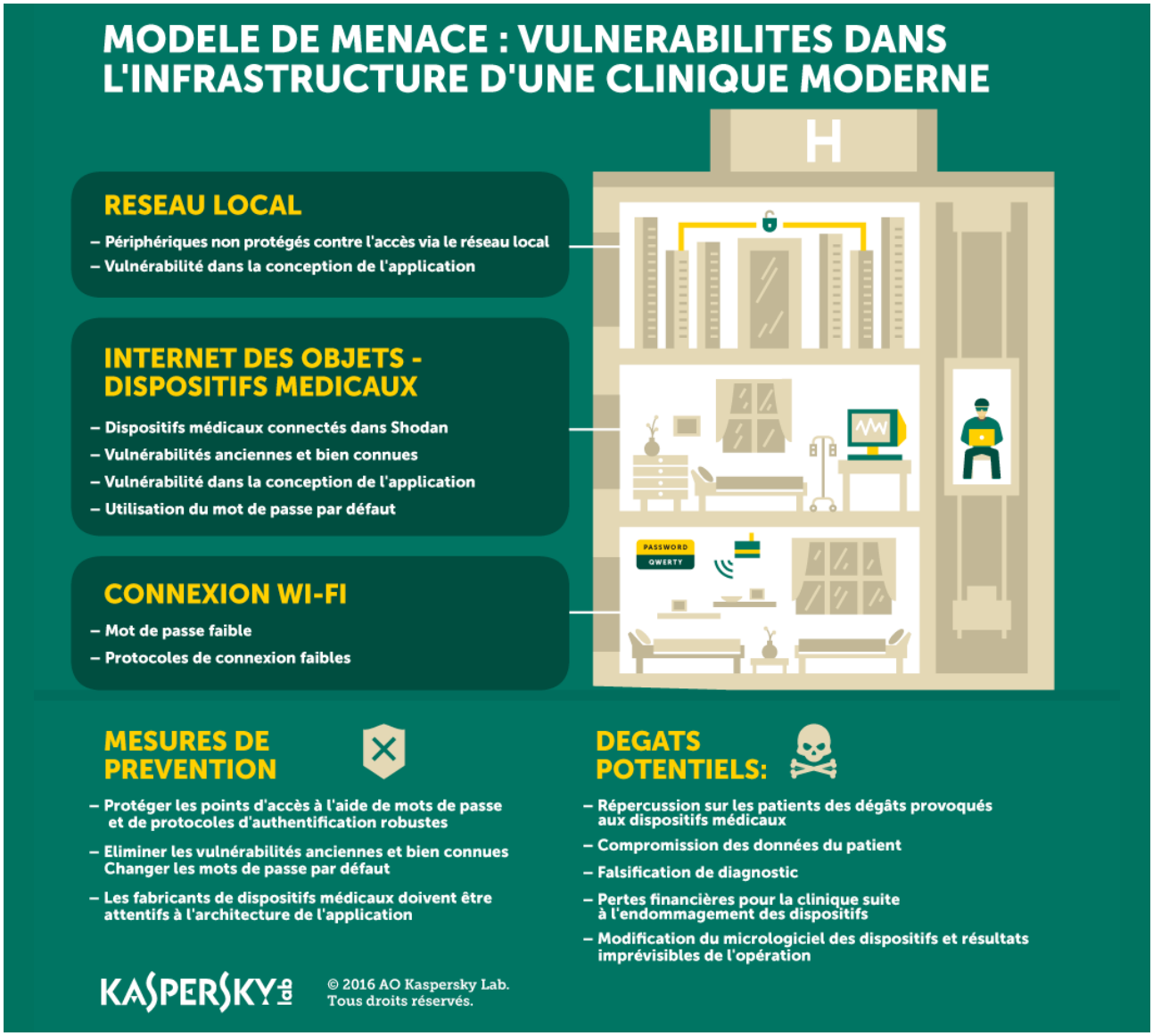
Aujourd'hui, les appareils intelligents sont partout. Un nombre croissant d'appareils ménagers de tous les jours sont également intelligents, qu'il s'agisse de téléphones, de téléviseurs, de thermostats, de réfrigérateurs, de moniteurs de surveillance de bébés, de bracelets connectés, voire de jouets pour enfants. Même les maisons peuvent être « intelligentes » dès la conception. La liste ne se limite aux objets que l'on retrouve chez soi. On peut y ajouter également les véhicules, les dispositifs médicaux, les caméras de vidéosurveillance et les parcmètres. Le réseau Wi-Fi omniprésent (même s'il n'est pas toujours aussi omniprésent qu'on le souhaiterait) connecte ces appareils à Internet, dans le cadre de l'Internet des objets (IdO).

Ces objets ont été conçus pour nous faciliter la vie. Dans la mesure où les objets connectés de tous les jours sont en mesure de récolter et de transférer des données automatiquement sans interaction avec un être humain, ils sont plus efficaces. Toutefois, cette réalité des objets de tous les jours connectés représente de nouvelles opportunités d'attaques pour les cybercriminels. Si les appareils de l'IdO ne sont pas sécurisés, les données personnelles qu'ils échangent peuvent être compromises. Ils peuvent être victimes d'attaques, mais ils peuvent également devenir complices, à leur insu.

Malheureusement, la sécurité est un concept difficile à vendre. Les appareils connectés sont produits par différents fabricants. Sur le marché libre, cela signifie que le rendement des investissements est un élément critique. Sur un marché concurrentiel, tout ce qui simplifie la vie du client a priorité. De plus, la connectivité est souvent ajoutée à un réseau de communication préexistant qui avait été mis en place sans penser à la sécurité. Donc, la sécurité est rarement, voire pas du tout, prise en compte lors de la phase de conception. Les faits nous montrent que les questions de sécurité ont souvent été traitées après qu'un incident malheureux a démontré l'impact d'une faiblesse de la sécurité.

Au cours de ces dernières années, des chercheurs ont mis en évidence des problèmes de sécurité existants dans différents appareils connectés. Vous vous souviendrez peut-être de l'article publié par un de nos chercheurs en sécurité qui avait analysé sa propre demeure afin de voir si elle était vraiment à l'abri des menaces cybernétiques. L'année dernière, Charlie Miller et Chris Valasek ont démontré comment il était possible d'accéder aux systèmes critiques d'une Jeep Cherokee via une connexion sans fil, au point de prendre les commandes du véhicule et de provoquer une sortie de route. Vasilios Hioureas de chez Kaspersky Lab et Thomas Kinsey de chez Exigent Systems ont réalisé une étude sur les faiblesses potentielles au niveau de la sécurité des systèmes de vidéosurveillance. Plus récemment, un fabricant a signalé une vulnérabilité dans une de ses pompes à insuline qui permettrait à un attaquant de désactiver le dispositif ou de modifier la dose. Il y a également eu des interrogations sur certains objets plus communs comme des jouets pour enfants, des moniteurs de surveillance pour bébés et des sonnettes.

Au mois de février, nous avons démontré à quel point il serait facile de trouver un hôpital, d'accéder à son réseau interne et de prendre les commandes d'un dispositif d'IRM afin d'obtenir les données personnelles des patients, leur protocole de traitement et d'accéder au système de fichiers du dispositif d'IRM. Sergey Lozhkin, un de nos chercheurs, a présenté les résultats de ses travaux lors du Security Analyst Summit de cette année et il s'est plus particulièrement attardé sur les facteurs clé qui ont un impact sur la sécurité des systèmes hospitaliers. Tout d'abord, les dispositifs médicaux connectés à Internet possédaient toujours le mot de passe par défaut. Certains tournaient sous Windows XP et étaient exposés à des dizaines d'anciennes vulnérabilités qui n'avaient pas été éliminées et qui pouvaient être exploitées pour compromettre les systèmes d'un hôpital. Ensuite, ces dispositifs médicaux n'étaient pas séparés du réseau local de l'hôpital. Autrement dit, après avoir établi la connexion au réseau Wi-Fi de l'hôpital, protégé par un mot de passe faible, il était possible d'obtenir un accès complet à ces dispositifs. Troisièmement, les vulnérabilités au niveau de l'architecture du logiciel signifiaient qu'il était possible, après la connexion au dispositif et l'authentification par défaut, d'accéder à l'interface de contrôle et aux dossiers personnels et médicaux des patients de l'hôpital. De plus, il y avait un interpréteur de commandes dans l'interface utilisateur qui permettait d'accéder au système de fichiers du dispositif. Vous pouvez lire le rapport ici.



Les hôpitaux doivent adopter des mesures pour sécuriser leurs systèmes :

- Protection des points de connexion externes à l'aide de mots de passe robustes.
- Mise à jour des stratégies de sécurité de l'information, développement de l'évaluation des vulnérabilités et des systèmes de correctif.
- Protection des applications des dispositifs médicaux dans le réseau local à l'aide de mots de passe pour résister à un accès non autorisé dans une zone de confiance.
- Adoption d'une solution de sécurité globale pour protéger l'infrastructure contre les malwares et les pirates.
- Sauvegarde à intervalle régulier des informations critiques et conservation d'une copie hors ligne.

L'étude consacrée aux capteurs de trafic a démontré que le concept de la « sécurité via l'obscurité » n'est pas applicable au monde connecté

Nous avons publié en avril les résultats d'une étude que nous avions réalisée sur les capteurs de trafic qui ont fait leur apparition ces dernières années dans les villes russes et ailleurs. Ces capteurs peuvent contribuer au respect des limitations de vitesse : les détecteurs de radar des conducteurs réagissent aux signaux des nouveaux capteurs de la même manière qu'aux signaux des pointeurs radar de la police de la route. Mais ces capteurs n'ont pas été installés pour cette raison-là. Ils récoltent des données brutes sur la circulation (nombre de véhicules sur chaque voie, vitesse moyenne, etc.) et les transmettent aux autorités municipales dans le but d'alimenter les analyses.

Les villes intelligentes constituent un écosystème ouvert complexe dans lequel la sécurité doit être présente dès la conception

Denis Legezo, auteur de l'étude, a découvert que le trafic de données n'était pas protégé et qu'il pouvait être manipulé. Aucune autorisation n'était requise, sauf pour Bluetooth, et cette dernière n'était pas configurée correctement. Le fabricant des capteurs de trafic que nous avons étudiés n'hésite pas à coopérer avec les ingénieurs de maintenance. Un volume important d'informations relatives aux périphériques est accessible sur le site officiel du fabricant et ailleurs.

C'est élément est positif. La « sécurité via l'obscurité » est dénuée de sens : n'importe quel attaquant déterminé parviendra à trouver le système de commande et accéder au logiciel d'ingénierie. Il est donc préférable de miser sur l'ouverture, l'offre de grosses récompenses et une réaction rapide pour éliminer toute vulnérabilité détectée, ne serait-ce que parce que le nombre de chercheurs sera toujours supérieur au nombre d'employés dans n'importe quel service de sécurité de l'information. Vous pouvez lire le rapport ici.

La majeure partie des périphériques qui contribuent à la ville intelligente masque le système d'exploitation derrière une interface publique. Ils possèdent néanmoins des faiblesses qui permettent l'accès des attaquants

Les villes d'aujourd'hui constituent des écosystèmes complexes de plusieurs centaines de composants différents, y compris des composants numériques. La ville intelligente vise à simplifier la vie des citoyens et à améliorer leur sécurité. Le détournement de la fonction d'origine est un fléau qui touche n'importe quel outil mis à notre disposition. Nous avons partagé en septembre les résultats de nos recherches sur différentes facettes de la ville intelligente. Denis Makrushin et Vladimir Dashchenko ont présenté leur conclusions dans un rapport rédigé dans le cadre du soutien apporté par Kaspersky Lab à l'initiative « Securing Smart Cities », une initiative internationale non commerciale qui a vu le jour pour réunir des experts dans le domaine des technologies de sécurité de l'information dans la ville intelligente. Les bornes d'achat de billets dans les cinémas, les bornes de location de vélo, les postes de renseignement dans les organisations publiques, les bornes de réservation et d'informations dans les aéroports et les terminaux de divertissement pour les passagers des taxis ont peut-être chacun des aspects différents, mais ils se ressemblent tous à l'intérieur. Chacune de ces bornes est un périphérique Windows ou Android. La principale différence par rapport aux périphériques ordinaires est le mode d'exécution « kiosque » du logiciel sur les bornes publiques qui sert également d'interface utilisateur. Le logiciel permet d'accéder aisément aux fonctions spécifiques de la borne tout en limitant l'accès à d'autres fonctions du système d'exploitation du périphérique, dont le lancement d'un navigateur et l'affichage d'un clavier virtuel. Un attaquant qui obtiendrait l'accès à ces fonctions pourrait compromettre le système de nombreuses manières, comme s'il se trouvait face à un PC. La recherche a confirmé que presque tous les kiosques numériques publics contiennent une ou plusieurs faiblesses en matière de sécurité qui permettent à un attaquant d'accéder aux fonctions masquées du système d'exploitation. Vous pouvez lire le rapport ici.

Le numérique intervient de plus en plus dans différents aspects de notre vie quotidienne. Si la sécurité n'est pas prise en compte au moment de la conception, les dangers potentiels peuvent être surprenants et les initiatives visant à rectifier les mesures de sécurité ne sont pas toujours simples à mettre en œuvre. Pour qu'une ville intelligente ne constitue pas un danger pour les gens qui y habitent, elle doit être traitée comme un système d'informations qui requiert une approche personnalisée et un savoir.

Des appareils électroménagers ont tendu une embuscade à Internet

Au mois d'octobre, des cybercriminels ont utilisé un réseau de zombies composés d'appareils ménagers de l'Internet des objets (caméras IP, enregistreurs vidéo numériques, caméras de surveillance et imprimantes) pour lancer une attaque DDoS contre Dyn, un prestataire de services DNS qui compte Twitter, Amazon, PayPal, Netflix et d'autres sociétés parmi ses clients. Suite à ces attaques, les sites de ces entreprises ont été mis hors service ou ont connu des problèmes intermittents. Les attaquants avaient infecté les périphériques vulnérables avec le malware Mirai. Ce malware avait déjà été utilisé dans le cadre d'une attaque DDoS qui avait ciblé le blog de Brian Krebs, un chercheur en sécurité et qui est considérée comme l'attaque DDoS la plus puissante de tous les temps (dans la mesure où le code source de Mirai a été publié récemment en ligne, l'attaque contre Dyn n'a pas nécessairement été organisée par les mêmes personnes). D'après les estimations qui circulent, le réseau de zombies Mirai compterait 550 000 bots. Les attaquants ont utilisé le mot de passe par défaut pour accéder aux périphériques en ligne. Une fois que le code malveillant était enregistré dans le périphérique, celui-ci rejoignait les rangs du réseau de zombies Mirai. Comme dans toute attaque DDoS, les auteurs ont utilisé les périphériques compromis pour submerger le site des victimes avec du trafic et perturber le fonctionnement normal.

Cette attaque, à l'instar d'autres incidents qui ont impliqué des périphériques compromis de l'Internet des objets, a joué sur fait que les utilisateurs modifient rarement les informations d'identification définies par défaut sur leur nouveau périphérique intelligent. Cela simplifie la tâche des attaquants : il leur suffit de trouver le mot de passe par défaut. De plus, bon nombre de périphériques n'ont pas de mise à jour du micrologiciel. Les périphériques de l'Internet des objets sont également intéressants pour les cybercriminels car ils demeurent connectés en permanence.

Le meilleur conseil que l'on peut offrir aux utilisateurs de périphériques de l'Internet des objets à domicile est de veiller à modifier les mots de passe par défaut sur tous les périphériques (privilégier des mots de passe uniques et complexes) pour éviter tout accès à distance. Cela vaut aussi pour les routeurs domestiques qui constituent la passerelle d'accès à votre réseau domestique. A la lumière de ces informations, certains utilisateurs pourraient être tentés de déconnecter tous les périphériques, mais dans le monde d'aujourd'hui qui est de plus en plus connecté, cette solution n'est pas réaliste. Ceci étant dit, il est toujours prudent de passer en revue les fonctions d'un périphérique intelligent et de désactiver celles que vous n'utilisez pas. En général, une bonne politique de gestion des mots de passe peut être très efficace pour maintenir les cybercriminels à l'écart de vos périphériques. Ce genre d'attaque à grande échelle rappelle également aux fabricants qu'ils doivent considérer la sécurité comme une partie intégrante de la conception et non pas comme un ajout ultérieur.

MENACES MOBILES

La principale menace mobile en 2016 auront été les trojans publicitaires capables d'utiliser les privilèges de superutilisateur (root) pour infecter l'appareil. Bien que l'obtention des privilèges de superutilisateur n'est pas une nouveauté pour ces malwares, de plus en plus de trojans sous Android ont commencé à les utiliser en 2016 car une fois dotés de ces droits, ils peuvent tout faire sur l'appareil. Afin d'obtenir les privilèges de superutilisateur sur un appareil, les trojans doivent exploiter des vulnérabilités dans le système. Vu que de nombreux appareils ne sont pas mis à jour selon un intervalle régulier, ils ne reçoivent pas les correctifs qui éliminent ces vulnérabilités. Par conséquent, nous nous attendons à une augmentation du nombre de trojans qui vont utiliser les privilèges de superutilisateur et à un renforcement de leur complexité.

Les mises à jour récentes pour Android contenaient non seulement des correctifs de vulnérabilités, mais aussi de nouvelles fonctions de sécurité, que les trojans ont vite appris à contourner. Nous estimons que ces contournements des nouvelles mesures de sécurité vont se répandre. Certaines de ces fonctions pourraient perturber les attaques de malwares mobiles de la catégorie Trojan-Ransom. Ceux-ci pourraient dès lors adapter leur comportement en conséquence.

Malware de rootage

Les trojans mobiles les plus répandus et les plus dangereux en 2016 ont été les trojans publicitaires capables d'obtenir les privilèges de superutilisateur sur l'appareil. La majorité d'entre eux appartient aux familles Trojan.AndroidOS.Ztorg et Trojan.AndroidOS.Iop.

Ils ont maintenu leur croissance en 2016, allant jusqu'à doubler leur représentation dans le Top 30 des trojans les plus répandus (22 positions en 2016 contre 11 en 2015).

Pour obtenir les privilèges de superutilisateur, ils peuvent utiliser différents codes d'exploitation ou tout simplement utiliser les privilèges de superutilisateur si l'appareil a déjà été rooté.

Plus de trojans mobiles ont décroché des privilèges de superutilisateur pour éviter la suppression et installer des logiciels publicitaires et du malware

Ils utilisent ces privilèges principalement pour deux raisons. Tout d'abord, ils peuvent ainsi se dissimuler dans le dossier système, ce qui rend leur suppression pratiquement impossible. Certains sont même capables d'infecter l'image de récupération, ce qui empêche toute suppression via une réintialisation d'usine. Ensuite, ils exploitent les privilèges de superutilisateur pour installer et lancer discrètement différentes apps qui se caractérisent par un affichage agressif de publicités. Ces nouvelles apps installées sont en grande majorité des apps non malveillantes avec des publicités, mais il y a eu malgré tout plusieurs cas d'installation de nouveaux malwares, dont la backdoor modulaire Backdoor.AndroidOS.Triada qui injecte le processus Zygote. Ce faisant, il atteint la persistance et peut modifier les SMS envoyés par d'autres applications pour voler l'argent de l'utilisateur. Grâce aux privilèges de superutilisateur, ce trojan peut littéralement tout faire, notamment remplacer des adresses Internet dans les navigateurs.

.

Un appareil qui a été infecté par une app publicitaire devient pratiquement inutilisable en raison de la quantité écrasante de publicités énervantes et d'apps installées. Ces trojans sont très difficiles à supprimer et ils peuvent même acheter de nouvelles apps dans Google Play et les installer discrètement.

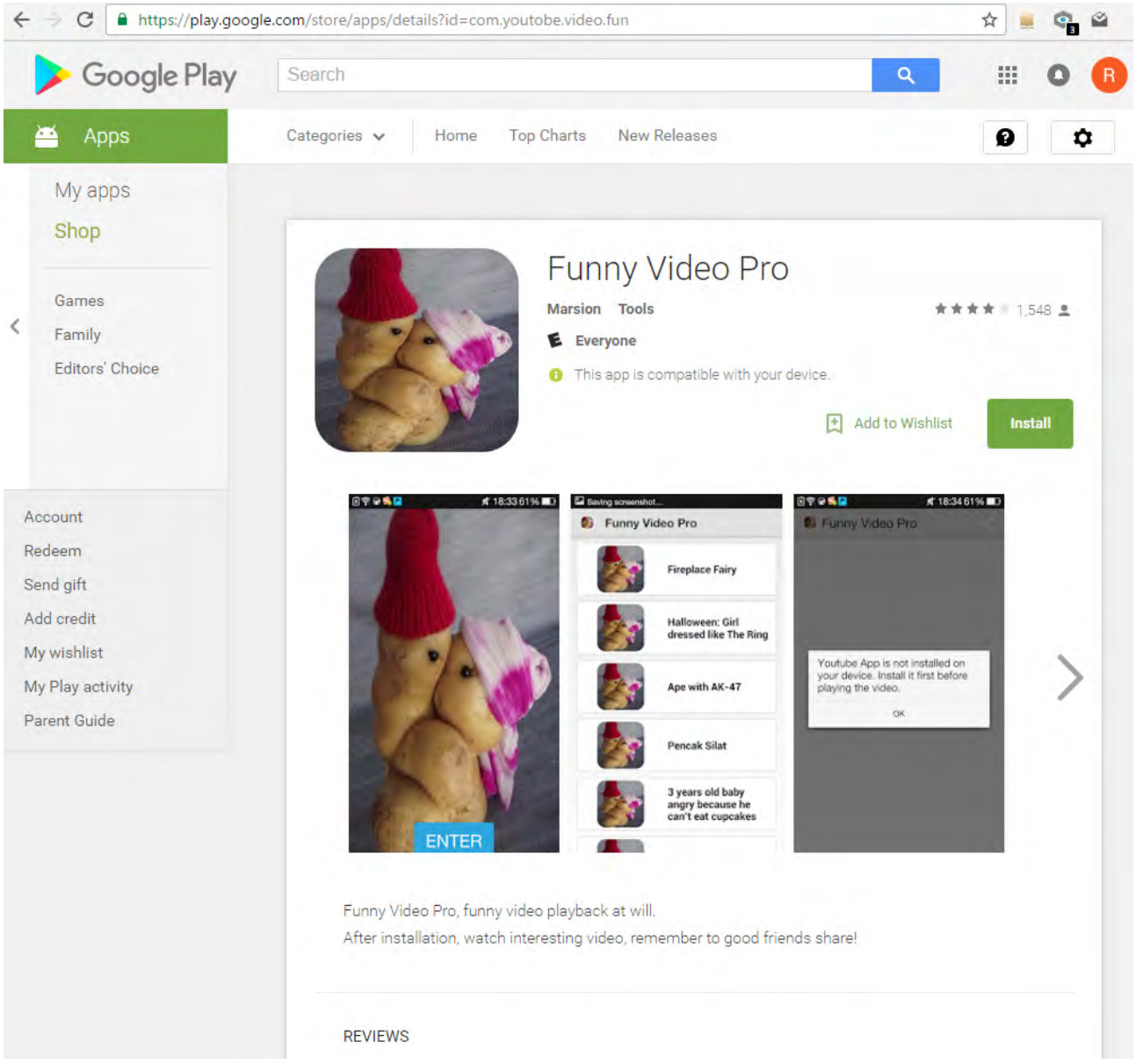
Elles sont en général diffusées par des magasins tiers, mais parfois elles sont préinstallées sur des appareils bon marché. Cette année, nous avons pu observer la distribution via Google Play Store : dans certains cas, des apps infectées ont été installées plus de 100 000 d'après les statistiques de Google Play Store. On retiendra plus particulièrement le cas des cybercriminels qui ont obtenu plus de 500 000 installations de Google Play Store : ils avaient utilisé un guide pour Pokemon GO infecté, détecté sous Trojan.AndroidOS.Ztorg.am.

Trojan.AndroidOS.Ztorg.ad dans Google Play Store

Les cybercriminels utilisent toujours Google Play Store

Un malware diffusé via Google Play Store a été téléchargé des centaines de milliers de fois

Les cybercriminels n'ont pas abandonné l'utilisation de Google Play Store pour diffuser les malwares. Rien qu'au cours d'une semaine du mois d'octobre, nous avons détecté plus de dix nouvelles apps dans Google Play Store qui avaient été infectées par Trojan.AndroidOS.Ztorg.am, une nouvelle modification de Trojan.AndroidOS.Ztorg.ad. Bon nombre de ces nouvelles applications comptaient plus de 100 000 installations.



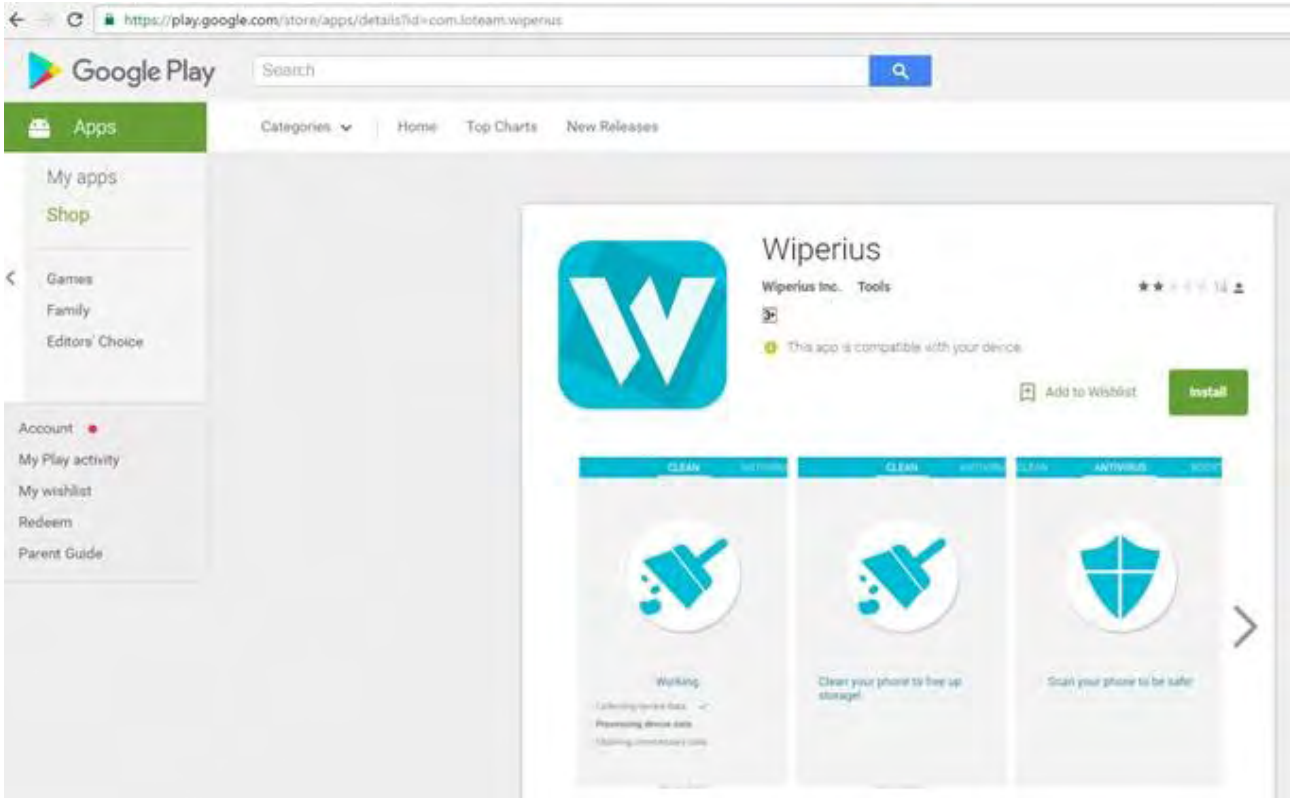
Trojan.AndroidOS.Ztorg.am dans Google Play Store

Un trojan sous Android était installé et mis à jour en tant qu'app saine avant de diffuser une mise à jour infectée chez les utilisateurs

Les malwares de rootage ne sont pas les seuls à être diffusés via Google Play Store. Il y a également des malwares de la catégorie Trojans-PSW. En octobre 2015, nous avions détecté Trojan-PSW.AndroidOS.MyVk.a dans Google Play Store. Cette app infectée avait été installée plus de 100 000 fois et ressemblait à une app qui permettait d'écouter de la musique depuis le réseau social VKontakte. Mais en réalité, elle volait les informations d'identification des membres de ce réseau social. Au fil de l'année, les cybercriminels ont chargé à plusieurs reprises de nouvelles modifications de ce trojan dans Google Play. Pour déjouer la sécurité, ils chargeaient d'abord une app saine et dépourvue de fonctions nuisibles. Ensuite, ils chargeaient quelques mises à jour saines et à un moment donné, ils chargeaient une version infectée. Ils ont employé cet algorithme au moins deux fois.

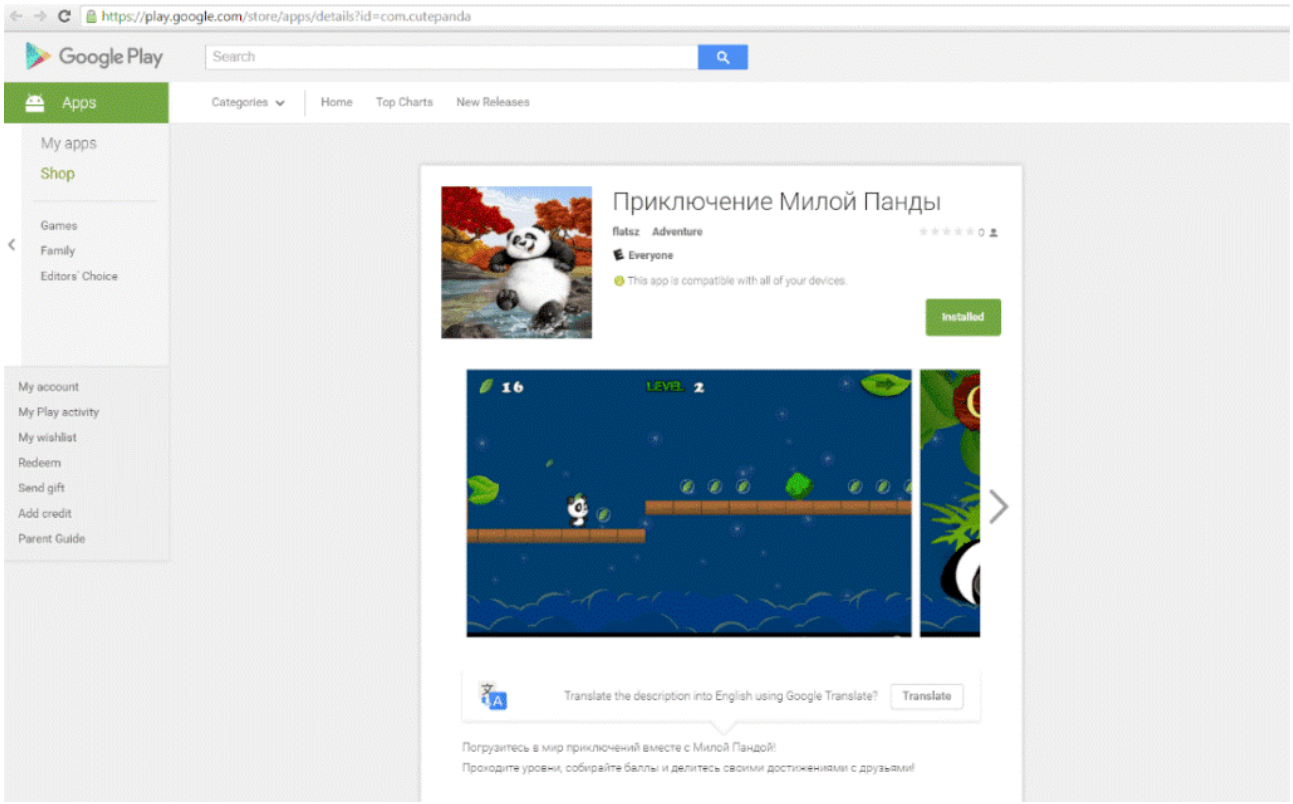
HEUR:Trojan-Spy.AndroidOS.Instealy.a est un autre exemple de malware de vol de données d'identification disponible sur Google Play Store. Ces apps malveillantes prétendaient permettre aux utilisateurs de voir qui avait consulter leur profil ; mais en réalité, elles exploitaient abusivement le processus d'authentification pour se connecter à Instagram.

D'autres catégories de malwares ont été diffusées via Google Play Store en plus des malwares de rootage et de Trojan-PSW. Nous avons remarqué que certains cybercriminels avaient adopté ce canal pour diffuser Trojan-Ransom.AndroidOS.Pletor.d.



Trojan-Ransom.AndroidOS.Pletor.d dans Google Play Store

A l'origine, la famille Trojan-Ransom.AndroidOS.Pletor chiffrait les fichiers de l'utilisateur sur l'appareil infecté. Cette modification, quant à elle, se contente de bloquer l'appareil infecté et d'exiger le paiement d'une rançon. Il est intéressant de constater que Pletor a été créé par le même groupe cybercriminel auquel on doit le trojan bancaire mobile Acecard. En décembre 2015, ce groupe avait utilisé Google Play Store pour diffuser Trojan-Downloader.AndroidOS.Acecard.b, un trojan qui télécharge et installe Trojan-Banker.AndroidOS.Acecard.a.



Une page de Trojan-Downloader.AndroidOS.Acecard.b dans Google Play Store

Pas seulement dans Google Play Store

Alors que les trojans publicitaires exécutaient des codes d'exploitation après l'infection pour obtenir les privilèges de superutilisateur, nous avons enregistré quelques rares cas où le malware utilisait des codes d'exploitation pour la diffusion.

Nos collègues de chez Bluecoat ont détecté Trojan-Ransom.AndroidOS.Fusob qui était distribué par des codes d'exploitation. Le kit d'exploitation était capable de télécharger et d'installer des apps malveillantes. Quelque temps plus tard, nous avons détecté des cybercriminels qui tentaient d'exploiter des vulnérabilités bien connues pour diffuser un malware.

Des trojans ont été diffusés également via des régies publicitaires

Une autre méthode intéressante a également été utilisée pour propager l'infection de Trojan-Banker.AndroidOS.Svpeng. Ici, les cybercriminels ont utilisé la régie publicitaire Google AdSense pour diffuser Trojan-Banker.AndroidOS.Svpeng.q. Svpeng est capable de voler les détails de la carte bancaire de la victime via des fenêtres de phishing ainsi que d'intercepter, supprimer et envoyer des messages texte. Grâce à sa distribution via une des régies publicitaires les plus populaires en ligne, Svpeng est devenu le trojan bancaire le plus répandu sous Android en 2016. Il est également devenu le deuxième trojan le plus populaire au classement général, derrière les trojans de rootage.

Contournement des fonctions de sécurité

Comme nous l'avons déjà dit, certains trojans ont découvert en 2016 de nouvelles manières de contourner certaines des fonctions de sécurité sous Android.

Les versions récentes d'Android demandent à l'utilisateur de confirmer tout envoi d'un SMS à un numéro surtaxé. Le petit trojan SMS superpose son propre écran sur cette boîte de dialogue, sans recouvrir les boutons de la fenêtre originale.

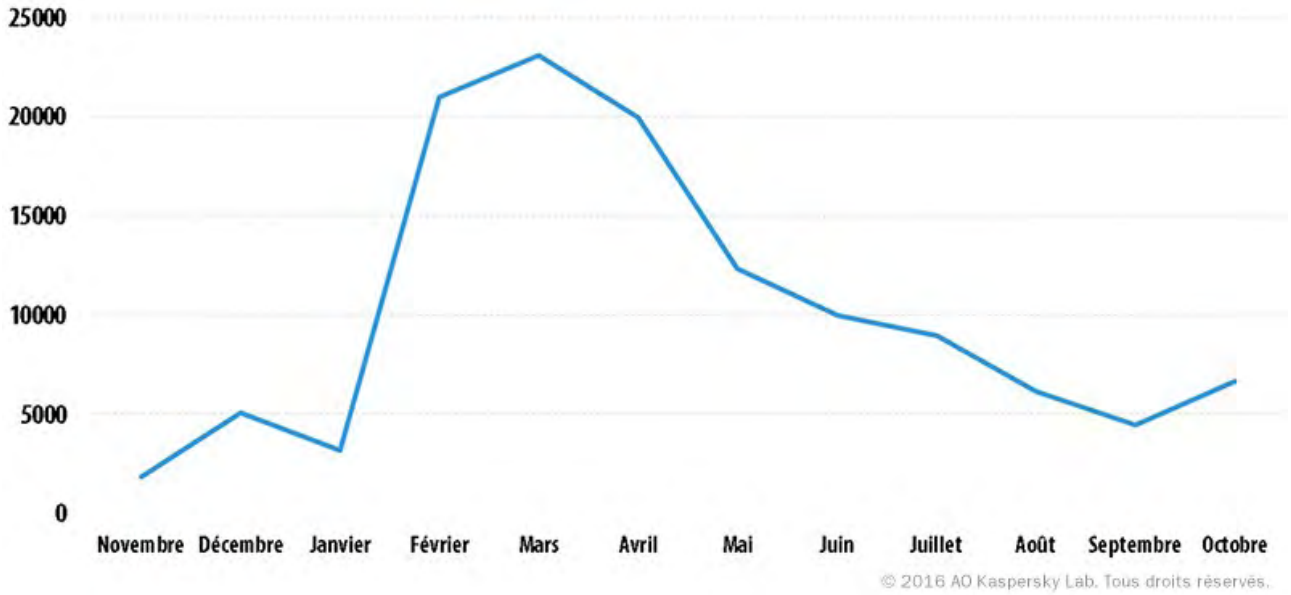
Une technique similaire a été adoptée par Trojan-Banker.AndroidOS.Asacub. Dans ce cas, le Trojan superpose sa fenêtre, avec des boutons, sur la fenêtre normale du système et demande les privilèges d'administrateur. Le trojan masque ainsi le fait qu'il sollicite une augmentation de privilèges dans le système à l'insu de l'utilisateur et amène l'utilisateur à approuver ces privilèges. De plus, le trojan Asacub possède des fonctions de messagerie SMS et a commencé à proposer ses services pour remplacer l'application SMS standard de l'appareil. Le trojan peut ainsi contourner les restrictions système introduites pour la première fois dans Android 4.4, mais il peut également supprimer ou masquer tout SMS entrant.

Les trojans Gugi et Asacub ont réussi à contourner de nouvelles fonctions de sécurité d'Android

Nous avons détecté en 2016 une nouvelle modification du trojan bancaire Trojan-Banker.AndroidOS.Gugi.c qui peut déjouer deux nouvelles fonctions de sécurité ajoutées à Android 6 : l'autorisation pour la superposition d'écran et la demande d'autorisation dynamique pour les activités dangereuses des applications comme les envois de SMS ou la réalisation d'appels. Cette nouvelle version n'exploite aucune vulnérabilité : elle ne repose que sur l'ingénierie sociale.

Ransowmare mobile

Trojan-Ransom.AndroidOS.Fusob aura été le représentant le plus populaire de la catégorie Trojan-Ransom en 2016. Il a été activement diffusé en Allemagne, aux Etats-Unis et au Royaume-Uni. Il ne fonctionne pas dans les pays de la CEI et dans les pays voisins. En général, les criminels exigent une rançon comprise entre 100 et 200 dollars pour débloquer l'appareil. La rançon doit être payée à l'aide de code de cartes iTunes prépayées. La popularité de ce trojan a explosé entre novembre 2015 et mars 2016 : au cours de cette période, le nombre d'utilisateurs attaqués a été multiplié par 12. Ce nombre est revenu ensuite au niveau du nombre d'utilisateurs attaqués l'année dernière.



Nombre d'utilisateurs uniques attaqués par Trojan-Ransom.AndroidOS.Fusob

Alors que le nombre d'utilisateurs attaqués par des malwares bancaires mobiles est supérieur à celui des utilisateurs attaqués par des ransomwares mobiles, on observe une situation contraire dans le nombre de paquets d'installation récoltés : depuis le 2e trimestre 2016, les chiffres pour la catégorie Trojan-Ransoms sont supérieurs à ceux de la catégorie Trojan-Bankers.

Le ransomware mobile préfère superposer sa fenêtre sur le contenu au lieu de chiffrer les données car ces dernières sont souvent sauvegardées

A la différence du premier trojan ransomware mobile qui chiffrait les fichiers des utilisateurs et exigeait une rançon pour le déchiffrement, les trojans ransomwares pour Android plus récents ne chiffrent pas les fichiers des utilisateurs. Ils se contentent de superposer leur fenêtre sur celle des autres apps. Ils masquent même les boîtes de dialogue du système. Le chiffrement du contenu des mobiles n'a pas la cote car les données des utilisateurs de l'appareil mobile sont bien souvent sauvegardée dans le cloud. Les trojans ransomwares réguliers qui superposent leur fenêtre sur toutes les autres donnent également de bons résultats et il est très difficile de se débarrasser d'un tel trojan.

Trojan-Ransom.AndroidOS.Congur, une des familles de ransomwares les plus populaire en Chine, bloque l'appareil infecté d'une autre manière : il sollicite les privilèges d'administrateur juste après le démarrage, puis change le code PIN ou en configure un nouveau (si l'utilisateur n'employait pas de code PIN). L'utilisateur est ensuite invité à prendre contact avec les cybercriminels via le service de messagerie QQ afin d'obtenir le nouveau code PIN. La simplicité de la méthode n'enlève rien à son efficacité.

Le trojan ransomware est un des trojans les plus simples au niveau technique et les plus efficaces. Voilà donc pourquoi nous nous attendons à ce qu'ils maintiennent leur progression et à ce que le nombre de familles Trojan-Ransom augmente également l'année prochaine.

FUITES DE DONNÉES

Les données personnelles ont de la valeur et il n'est dès lors pas étonnant que les cybercriminels ciblent les prestataires de services en ligne, dans l'espoir de voler de gros volumes de données lors d'une seule attaque. Nous nous sommes habitués à la succession de fuites de données signalées dans les médias. Cette année n'aura pas fait exception à la règle. Des fuites de données ont frappé beautifulpeople.com, Tumblr, forum de pirates nulled.io (ce qui montre que les systèmes légitimes ne sont pas les seules victimes), Kiddicare, VK.com, Sage, le forum officiel de DotA 2, Yahoo, Brazzers, Weebly et Tesco Bank.

Certaines de ces attaques ont débouché sur le vol d'imposants volumes de données, ce qui a souligné les lacunes de nombreuses entreprises en matière de protection. La sécurité ne peut se limiter au seul périmètre de l'entreprise.

La sécurité absolue est un leurre et il est impossible de garantir qu'un système ne sera pas piraté, surtout si l'attaque bénéficie d'un complice à l'intérieur ou si une personne au sein de l'entreprise est amenée par une ruse à réaliser une action qui met en danger la sécurité de l'entreprise.

Ceci étant dit, toute organisation qui détient des données personnelles se doit d'adopter des mesures de protection efficace. Celles-ci doivent prévoir notamment le hachage et le salage des mots de passe des clients et le chiffrement d'autres données sensibles.

Les consommateurs n'ont aucun contrôle sur la sécurité des données personnelles qu'ils transmettent aux prestataires de services en ligne. Ils peuvent toutefois limiter les dégâts liés à une éventuelle atteinte à la sécurité chez un prestataire en ligne en veillant à toujours utiliser des mots de passe uniques et complexes : le mot de passe idéal compte au moins 15 caractères et doit être composé de lettres, de chiffres et de symbole de l'ensemble du clavier. Si la sélection d'un mot de passe robuste vous semble difficile voici quelques astuces qui vous aideront à créer des mots de passe sûrs et faciles à utiliser. Vous pouvez également opter pour une application de gestion des mots de passe qui s'occupera automatiquement de l'ensemble de ces détails.

Le vol de données chez LinkedIn a révélé l'existence d'un million de comptes qui utilisaient le mot de passe « 123456 »

Malheureusement, les utilisateurs choisissent bien trop souvent des mots de passe faciles à deviner et ils emploient le même mot de passe pour plusieurs comptes. Cela signifie que si le mot de passe d'un compte est compromis, les autres identités en ligne de la victime deviennent vulnérables. Cette problématique a reçu l'attention du public en mai 2016 après qu'un pirate connu sous le pseudo « Peace » a tenté de vendre 117 millions d'adresses email et de mots de passe de LinkedIn qui avaient été volés quelques années auparavant. Plus d'un million de ces mots de passe volés correspondaient à « 123456 ».

En juillet, nous sommes revenus sur l'impact de la fuite de données chez Ashley Madison, un an après l'attaque qui avait entraîné la fuite de données de clients et nous avons formulé quelques conseils aux personnes qui pensent trouver l'amour en ligne (et de bons conseils pour gérer n'importe quel compte en ligne).

La problématique des mots de passe refait surface de manière cyclique. Si les mots de passe que nous choisissons sont trop faciles à deviner, nous nous exposons au vol d'identité. Le problème est aggravé par le fait que nous avons tendance à utiliser le même mot de passe pour différents comptes en ligne. C'est la raison pour laquelle de nombreux prestataires de service, dont Apple, Google et Microsoft, proposent désormais un système d'authentification à deux facteurs. Autrement dit, les clients doivent saisir un code généré par un token ou envoyé à un appareil mobile pour pouvoir accéder au site, ou du moins pour modifier les paramètres du compte. Certes, l'authentification à deux facteurs améliore la sécurité, mais uniquement si elle est obligatoire.

Vu l'impact potentiel que peut avoir une fuite de données, il n'est pas étonnant de voir que les autorités de réglementations s'intéressent de près au problème. Ainsi, au Royaume-Uni, l'Information Commissioner's Office (ICO) a récemment imposé une amende record de 442 279 EUR à TalkTalk pour « ne pas avoir mis en œuvre les mesures de cybersécurité les plus élémentaires » suite à des attaques menées contre la société en octobre 2015. D'après l'ICO, cette amende doit « servir de mise en garde pour les autres et leur rappeler que la cybersécurité n'est pas le problème du service informatique mais du conseil d'administration ».

Le Règlement général sur la protection des données de l'UE, qui entrera en vigueur en mai 2018, obligera les entreprises à signaler les fuites de données au régulateur, avec à la clé d'importantes amendes pour ne pas avoir sécurisé comme il le fallait les données personnelles. Ce règlement est présenté ici. On espère qu'il motivera les entreprises à signaler les fuites de données en temps opportuns. La question a à nouveau refait surface cette année après que Dropbox a envoyé un avis à bon nombre de ses clients pour les inviter à modifier leur mot de passe. L'attaque contre Dropbox en 2012 avait entraîné la fuite non seulement d'adresses email, mais également de mots de passe. A l'époque, Dropbox avait signalé le vol des adresses email à ses clients, mais n'avait rien dit pour les mots de passe. Heureusement, le hachage et le salage avaient été appliqués à ces mots de passe et qui plus est, Dropbox utilise la vérification à deux étapes.

Plusieurs entreprises espèrent pouvoir se débarrasser tout simplement des mots de passe. Ainsi, Apple a mis en œuvre l'autorisation par empreintes digitales pour les achats sur iTunes et les paiements dans Apple Pay. Samsung a annoncé son intention d'introduire la reconnaissance d'empreinte digital, de la voix et de l'iris sur Samsung Pay. Amazon a annoncé le paiement par selfie (« Selfie-pay »). MasterCard et HSBC ont quant à elles annoncé le recours à la reconnaissance faciale et vocale pour l'autorisation des transactions. Le principal atout de ses méthodes est de remplacer un élément que les clients **doivent mémoriser** (un mot de passe) par un élément qui les **accompagne**, sans possibilité de court-circuiter le processus (comme c'est le cas lorsqu'ils choisissent un mot de passe faible).

L'authentification par d'autres méthodes que les mots de passe est un problème de taille pour la sécurité

Pour beaucoup, les données biométriques représentent la solution pour l'avenir. Toutefois, elles ne constituent pas forcément une solution miracle en matière de sécurité. Les données biométriques peuvent être imitées comme nous l'avons déjà dit (ici, ici et ici) ; et les données biométriques peuvent également être volées. Il serait plus utile d'envisager le remplacement des noms d'utilisateur par des données biométriques, et non pas les mots de passe. En fin de compte, l'authentification à plusieurs facteurs est essentielle en ce sens où elle combine un élément que vous connaissez, un élément que vous avez et un élément qui vous compose.

CYBERSÉCURITÉ INDUSTRIELLE : MENACES ET INCIDENTS

Nous ne pouvons pas dire que l'année 2016 aura été remarquable en termes de quantité ou de gravité des incidents de cybersécurité dans le milieu industriel. Il y a quand même eu plusieurs cas intéressants que nous aimerions survoler dans ce rapport.

Incidents

Cette année, nous avons eu vent de deux incidents de cybersécurité dans des centrales nucléaires. Le premier cas a été enregistré à la fin du mois d'avril lorsque la société qui exploite la centrale nucléaire de Gundremmingen a signalé une infection du ver Kido (également connu sous le nom de Conficker) sur les ordinateurs du système de commande de l'unité B. Ce système de commande fait partie du dispositif de chargement des crayons de combustible nucléaire. Heureusement, le ver n'a eu aucun impact sur les procédures technologiques et n'a pas provoqué de dégâts dans la centrale nucléaire.

Les autorités de supervision pertinentes et le Bureau fédéral allemand de la sécurité de l'information ont été informés. Tous les systèmes et dispositifs critiques ont été vérifiés et aucun autre indice d'infection par un malware n'a été découvert. Suite à cet incident, les mesures de sécurité ont été renforcées. L'incident a été classé dans la catégorie N (normale) conformément aux critères de rapport adoptés en Allemagne. D'après l'échelle internationale des événements nucléaires et radiologique (INES), il s'agit d'un incident de niveau 0 (en dessous de l'échelle/sans importance pour la sûreté).

La source de l'infection n'a pas été dévoilée, mais un porte-parole de la centrale nucléaire a déclaré qu'environ 18 périphériques USB amovibles infectés par le ver Kido avaient été découverts dans le réseau des bureaux. Il a également précisé que l'infection n'aurait pas pu provoquer de graves dégâts car tous les systèmes de commande critiques de la centrale sont dissociés et l'ensemble de l'architecture du système est conçue pour résister aux dénis de service et est à l'abri des manipulations.

S'il est vrai que l'infection par Kido n'a pas provoqué de graves dégâts dans ce cas-ci (heureusement), il serait stupide de penser que seul un malware ciblé et conçu spécialement pour cette tâche pourrait être dangereux. Alors que l'année 2015 touchait à sa fin, des sous-stations du réseau de distribution d'électricité ukrainien ont été victimes d'une cyberattaque particulièrement bien coordonnée. Les adversaires avaient adressé des messages de phishing avec des codes d'exploitation à des individus qui travaillaient dans les services administratif ou informatique des compagnies d'électricité. Dès les premières infections d'ordinateurs, les adversaires ont accédé au réseau des technologies opérationnelles et ont réussi à perturber la distribution d'électricité. Ce qui est important dans ce cas, c'est que les attaquants ont éliminé toutes les possibilités d'accès à distance au réseau de distribution. Ils ont éliminé certains logiciels d'ingénierie et endommagé les secteurs d'amorçage du système pour empêcher toute administration et réparation à distance.

Ce qu'il faut retenir, c'est que même si le malware n'a aucun impact sur les processus technologiques, mais qu'il est en mesure de provoquer un déni de service pour les systèmes d'assistance critique tels que SCADA, la passerelle OPS, l'accès à distance, etc., le système de contrôle industriel continuerait probablement à fonctionner conformément à sa configuration la plus récente, mais il serait impossible de commander ou de rectifier les processus en cas d'accident ou de situation d'urgence.

Les attaques contre les systèmes de contrôle industriel qui ne sont pas signalées aux experts en sécurité ne peuvent pas être analysées et par conséquent, aucune leçon ne peut être tirée

Il y a quelques mois de cela, Yukiya Amano, le directeur de l'Agence internationale de l'énergie atomique (AIEA) a dévoilé qu'une centrale nucléaire avait été attaquée par des pirates il y a 2 ou 3 ans. Il a déclaré : « Cela a vraiment eu lieu et cela a occasionné certains problèmes. S'il est vrai que la centrale n'a jamais dû interrompre ses activités, il a fallu adopter des mesures de précaution ». Le problème ici n'est pas uniquement un problème de cybersécurité qui pourrait perturber les opérations d'une centrale nucléaire. Il s'agit aussi du problème plus sérieux de l'absence de communications et de transparence entre les utilisateurs de systèmes de contrôle industriel et les spécialistes de la cybersécurité. Au bout du compte, les experts en cybersécurité n'ont aucune chance de pouvoir analyser le problème, tandis que les propriétaires et les fabricants de systèmes de contrôle industriel ne pourraient pas adopter des mesures d'atténuation des risques de manière proactive.

Malware sur automate programmable industriel : preuve de concept

Une preuve de concept de ver pour automate programmable industriel a été présentée ce mois d'août par des chercheurs de chez OpenSource Security dans le cadre de la conférence BlackHat. Le ver créé uniquement comme une programmation pour automate programmable industriel peut identifier lui-même les automates dans le réseau et se propager d'un automate à l'autre. Il est également capable de manipuler les entrées et les sorties des automates programmables, de provoquer un déni de service pour un automate, de se connecter à des serveurs de commande et de faire office de proxy dans la propagation d'une attaque.

Les techniques employées pour infecter un automate programmable industriel constituent la partie la plus intéressantes de cette preuve de concept. La preuve de concept a été créée pour des contrôleurs Siemens S7-1200 qui sont dotés de la fonction de protection de l'accès. Quand cette fonction est activée, il est possible de définir un mot de passe à l'aide du protocole S7CommPlus pour contrôler l'accès à l'automate programmable industriel. Il est dès lors impossible de lire ou de modifier le code de l'automate programmable industriel sans autorisation. La protection de l'accès est toutefois désactivée par défaut. Quand la fonction est activée, l'infection de l'automate programmable industriel par un ver est possible uniquement si le mot de passe est obtenu par force brute ou s'il est volé ou détourné d'une autre manière.

Par contre, si la fonction de protection de l'accès est désactivée, l'automate programmable industriel peut toujours compter sur deux autres mécanismes de protection :

- Il s'agit d'abord de la protection intellectuelle qui interdit l'extraction et les modifications de l'automate programmable industriel depuis un dispositif.
- Vient ensuite la protection contre les copies qui empêche le dédoublement du programme de l'automate programmable industriel sur un autre dispositif PLC.

La vérification de l'accès pour les deux mécanismes de protection (protection intellectuelle et « protection contre les copies ») a été mise en œuvre du côté client (dans le portail TIA), ce qui signifie qu'un simple outil créé par l'attaquant peut lire et écrire des blocs sur l'automate programmable industriel en évitant les processus d'authentification. Siemens a publié un avis et a fourni un correctif pour le micrologiciel S7-1200.

La leçon à retenir ici est que n'importe quel dispositif brut ou auteur de menace muni d'un accès à un réseau de système de contrôle industriel pourrait compromettre aisément tous les systèmes de commande. Qui plus est, les dispositifs avec automate programmable industriel sont plus vulnérables aux attaques (surtout les dénis de service) car ils s'attendent à communiquer uniquement avec le SCADA ou le logiciel d'ingénierie. La protection contre l'accès non autorisé, les mauvaises saisies ou les manipulations malveillantes est faible, voire inexistant.

Vulnérabilités 0jour dans le logiciel et le matériel des systèmes de contrôle industriels

D'après les données de ICS CERT des Etats-Unis, près de 427 rapports de vulnérabilités ont été remis au cours de l'exercice fiscal 2015 (d'octobre 2015 à septembre 2016), contre 245 pour l'année antérieure. Environ 25 pour cent de ces vulnérabilités sont liées à des validations de saisie incorrecte et 27 pour cent, à des contrôles d'accès médiocres. Une autre catégorie importante de vulnérabilités, en rapport avec la configuration et l'exploitation, est souvent ignorée par les fabricants. Les vulnérabilités telles que les informations d'identification par défaut, les paramètres de sécurité par défaut (qui sont souvent désactivés), les API dissimulées ou les fonctions non documentées sont extrêmement dangereuses car leur exploitation ne requiert pas une grande expertise technique et elles offrent un accès étendu au système de contrôle.

L'écart entre le signalement d'une vulnérabilité dans un système de contrôle industriel et la diffusion d'un correctif est souvent trop long

Malheureusement, trop de temps s'écoule entre le moment où une vulnérabilité est signalée à un fabricant et le moment où le correctif est diffusé. Parfois, ce correctif n'est jamais produit car le vendeur affirme que le produit vulnérable n'est plus pris en charge. Du point de vue d'un propriétaire d'un système de contrôle industriel, cela entraîne un coût élevé pour la modernisation ou un risque énorme de compromission.

En conclusion, nous voulons attirer l'attention sur l'importance pour les communautés de chercheurs en sécurité de contribuer à la cybersécurité des systèmes de contrôle industriel. Au cours des dernières années, nous avons observé un développement incroyable de l'intérêt pour la sécurité des systèmes de contrôle industriel. Chaque année, plusieurs rapports de recherche, ainsi que des outils et des cadres sont publiés. Par exemple, au début de cette année, nous avons publié notre propre compte rendu des menaces contre la cybersécurité industrielle. De telles initiatives permettent à des spécialistes de la cybersécurité dans des domaines autres que les systèmes de contrôle industriel d'intervenir dans le débat et de partager leurs expériences et leurs connaissances.

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