Article paru dans *Mag-Securs* n°29

Tirer les leçons de l'affaire Stuxnet

Tout a-t-il été dit sur le ver Stuxnet ? Sans doute pas. On pourra sans doute en tirer un jour un film à la « James Bond » ou « Mission Impossible ». Faut-il s'en tenir là ? Manifestement non, une telle attaque soulève de nombreuses questions qui doivent remettre en cause certaines certitudes... Peut-être faut-il repenser nos paradigmes en matière de sécurité.

Dossier réalisé par Dominique Ciupa.

La faillite de la Barings Bank, en 1995, causée par le trader Nick Leeson avec 827 millions de livres sterling de pertes a été le thème du film « Trader – l'homme qui a fait sauter la banque de la Reine d'Angleterre » sorti en 2000 avec Erwan McGregor. Au début de l'année 2008, on découvre que la Société Générale passe de très peu à côté de la faillite avec l'affaire « Jérôme Kerviel » : 50 milliards d'euros d'exposition et près de 5 milliards d'euros de pertes[*]. La tourmente financière de l'automne 2008 nous a donné un tout autre tempo : la crise américaine des « subprimes » met en jeu 500 milliards de dollars de valeur fictives ! Et les affaires ne sont pas terminées : Madoff avec 50 milliards de dollars, ou encore le renflouement des finances de l'Irlande avec 85 milliards d'Euros, etc.

Stuxnet pourrait bien être à la SSI ce que Nick Leeson a été au système financier : le premier épisode d'une longue série dont les effets pourraient finir par être très dévastateurs. Le risque encouru par les systèmes industriels est connu depuis de nombreuses années et est régulièrement exposé au cours de grandes conférences comme la Black Hat, la RSA Conférence, ou le FIC. Mais force a été de constater que ce risque était considéré comme non avéré : l'attaque n'avait pas eu lieu… Dès lors, la tentation de classer ce risque comme résiduel, c'est-à-dire acceptable sans vraiment apprécier son impact est fort… La médiatisation de l'attaque Stuxent aura au moins eu le mérite de provoquer une vaste campagne de sensibilisation sur la sécurité des systèmes industriels.

> Les éléments de l'attaque

Il convient naturellement de rester très prudent sur ce que nous savons des véritables objectifs de ce ver. Une tendance générale se dégage toutefois pour supposer que ce malware a été conçu afin de détruire les centrifugeuses de l'usine d'enrichissement d'uranium de Natanz, en Iran. Des faits ont en effet été rapportés par l'AIEA sur un retard de ce programme et le gouvernement iranien a lui-même reconnu l'existence de problèmes. Le code exécutable des commandes des centrifugeuses auraient été modifiées pour changer leur vitesse de rotation et les détruire. Il s'agirait donc d'une attaque sur les systèmes de supervision WinCC de Siemens, qui contrôlent, sur un ordinateur exploité sous Windows, les systèmes Scada (Supervisory Control and Data Acquisition).

L'affaire aurait donc eu un objectif, le blocage, ou au moins un sérieux ralentissement du programme nucléaire iranien. Elle aurait également eu l'appui d'un ou plusieurs états, les Etats-Unis et/ou Israël, des moyens intellectuels importants et sans doute également un travail traditionnel d'agents de terrain.

Ce genre d'attaque ne ressemble cependant pas aux vers que nous avons connus au début des années 2000 et qui se propageaient sur l'Internet. Les équipements d'une centrale nucléaire ou d'une usine d'enrichissement ne sont en effet pas accessibles de l'Internet. Des réseaux spécifiques sont conçus, totalement cloisonnés. Il est même courant de mettre en œuvre des « firewalls-diode » permettant à un équipement de mesures d'envoyer des données vers une salle de contrôle, sans qu'il ne soit possible d'envoyer des ordres à cet équipement pour le perturber, voire de changer son code exécutable.

Ces principes sont largement diffusés et sont précisés dans les documents du Nuclear Energy Institute américain, notamment le document NEI0404. L'attaque, dit-on, aurait été menée grâce à des clés USB. La composante humaine a donc été employée… A quel niveau, de quelle manière ? Les choses ne sont pas claires : un agent sur place agissant délibérément ? Ou une contamination en amont de programmes exécutables pour que des techniciens autorisés compromettent ensuite, à leur insu, les commandes des équipements ? Dans la mesure où plusieurs installations ont été infectées dans le monde, le second scénario nous semblerait plus plausible…

Selon la publication israélienne Debka spécialisée dans le renseignement militaire, le professeur iranien Majid Shahriari, chargé de lutter contre Stuxnet a été assassiné en novembre dernier. Le mode opératoire a été celui d'explosifs lancés depuis des motos et d'une fusillade depuis une voiture. Le pouvoir iranien a pour sa part immédiatement accusé les Etats-Unis et Israël, confirmant ainsi l'assassinat du scientifique…

L'analyse du ver Stuxnet a été réalisée par de nombreux experts et on a pu assister à un très important travail d'échanges entre les experts et les éditeurs de solutions anti-malwares. Un rapport très complet a notamment été réalisé par Symantec. Les experts ont identifié l'exploitation de quatre failles « 0 day ». L'exécution d'un payload rendue possible par l'exploitation de la faille LNK non corrigée permettait de compromettre le système en exécutant un code malicieux depuis une clé USB par un appel de lien .ink. Pour l'ensemble de la profession, la combinaison de 4 failles représente un travail exceptionnel et jamais vu à ce jour. Symantec explique que le système de contrôle des fréquences des moteurs entre 807 Hz et 1210 Hz

[*] : Lire *Mag-Securs* n°19 (2e trimestre 2008) – Affaire Société Générale : quelles leçons en tirer ?

étaient visées. Les experts relèvent également que l'attaque exploite l'utilisation d'un mot de passe par défaut. WinCC / PCS7 s'appuie en effet sur une base de données MS SQL qui demande un mot de passe pour établir une communication interne. La vérification ne concerne donc pas l'utilisateur du système et Siemens recommande à ses clients de ne pas changer le mot de passe pour éviter des dysfonctionnements...

L'étude du ver fait encore apparaître que deux certificats ont été volés à JMicron et Realtek. Le système vérifie en effet l'authenticité des codes exécutables auprès d'une autorité de certification : Verisign. Mais le code exécutable modifié disposait des certificats originaux et l'autorité de certification les reconnaissait comme valides ! Comment les certificats ont-ils été volés ? Infiltration, commandos, espionnage, achat de personnes... L'histoire ne le dit pas encore, mais il existe de nombreux films qui montrent cela...

Les experts estiment que ce ver a demandé un travail de 6 mois à un an à une équipe de 6 à 10 personnes. L'analyse du code montre par ailleurs des éléments plus curieux. Il comporterait un fichier nommé « Myrthus », ce qui signifie « l'arbre de Myrthe » en français. Or, on trouve dans la Bible le Myrthe comme étant un symbole de justice : *« au lieu du buisson croîtra le sapin et au lieu de l'épine croîtra le Myrthe : et cela rendra glorieux le nom de l'éternel et sera un signe perpétuel, qui ne sera jamais retranché »*. D'autres experts y ont vu une allusion au *Livre d'Esther*, et donc à la Torah : *« elle s'appelait Hadassah parce qu'elle était juste et que l'on compare au Myrthe ceux qui aiment la justice »*. Hadassah est l'un des noms de la reine Esther qui signifie Myrthe. Le *Livre d'Esther* explique comment la reine Hadassah déjoua les attaques perses destinées à anéantir le peuple juif.

Autre détail issu de l'analyse du code, le ver s'arrêtera de fonctionner le 23 juin 2012. Des experts ont relevé que c'est très exactement 100 ans, jour pour jour, après la naissance d'Alan Turing, connu pour ses travaux sur les ordinateurs, mais aussi pour avoir dirigé une équipe de cryptanalyse durant la seconde guerre mondiale dans le centre de Bletchley Park qui décodait les communications allemandes et a joué un rôle considérable dans la victoire alliée contre le régime nazi...

L'unanimité n'est cependant pas de mise entre tous les experts SSI de la planète. En Israël, on trouve des spécialistes qui dénoncent une campagne de communication hostile à leur pays et qui minimisent les capacités de Stuxnet. En France, Daniel Ventre, ingénieur au CNRS et directeur de la collection « Cyberconflits et Cybercriminalité » aux éditions Hermès-Lavoisier, se montre très circonspect vis-à-vis de nombreuses conclusions qui sembleraient avérées pour le plus grand nombre. « *L'attaque n'était pas ciblée,* souligne-t-il, *elle a touchée l'Inde, l'Indonésie, la Russie, les Etats-Unis et la Chine ! Son origine étatique n'est pas démontrée : un travail de 10 ingénieurs pendant 10 mois est à la portée d'une entreprise, ou d'un groupe d'étudiants !* » Dans son rapport sur Stuxnet, Symantec met toutefois en évidence que le plus grand nombre d'attaques se trouve bien manifestement en Iran, très loin devant les autres pays...

> Un risque sur les centrales françaises ?

Le risque a été pris au sérieux par les autorités françaises de possibles effets sur nos centrales nucléaires, en France. L'IRSN a publié le 30 septembre une note d'analyse sur Stuxnet.[*]

On y lit que seul le réacteur nucléaire EPR en construction à Flamanville utilise un système de contrôle-commande Siemens. Son éventuelle sensibilité à des logiciels tels que Stuxnet doit donc être prise en compte dans l'analyse de sûreté. La propagation du ver Stuxnet nécessite que les ordinateurs de supervision exploitent Windows et que les logiciels de supervision soient ceux de la gamme PCS 7/WinCC de Siemens.

L'IRSN poursuit en expliquant le besoin d'une démarche globale d'analyse critique de sûreté, avec une analyse technique systématique et détaillée des systèmes, dont les dysfonctionnements peuvent influencer la sûreté d'une installation nucléaire. Pour le réacteur EPR, explique encore l'IRSN, EDF a retenu la gamme « SPPA-T2000 » de Siemens, basée sur sa technologie « S5 » plus ancienne et radicalement différente de sa technologie « WinCC / S7 » visée par Stuxnet. Les ordinateurs de supervision du réacteur EPR de Flamanville ne sont pas basés sur le système d'exploitation Windows et n'utilisent pas les logiciels WinCC et PCS 7 ; le ver Stuxnet est donc sans influence sur eux. Et l'IRSN poursuit en précisant que l'analyse de sûreté de la plateforme SPPA-T2000 de Siemens a permis de vérifier d'avance qu'elle présentait les propriétés qui garantissent, entre autres, son immunité aux logiciels malveillants, et en particulier au ver Stuxnet. Le Système de Protection de l'EPR, le plus important des systèmes de sûreté, est développé à partir d'une autre technologie nommée Teleperm XS. Cette technologie d'Areva ne comporte pas les logiciels ciblés par Stuxnet et ses

(*) : *www.irsn.fr/FR/Actualites_presse/Communiques_et_dossiers_de_presse/Pages/20100930-Ver_informatique_Stuxnet_peut_il_menacer_centrales_nucleaires_françaises.aspx*

automates de sûreté n'ont aucune interface qui permettrait à un logiciel malveillant de l'infecter.
Voici qui est rassurant£ ou très inquiétant, car rien ne dit qu'un autre malware ne pourrait, lui, aboutir à mener une attaque contre des sites français... Il faut continuer à réaliser des études de sécurité très strictes.

> Approfondir les principes des analyses de risques et les paradigmes de la sécurité

Stuxnet nous enseigne surtout qu'il est nécessaire d'approfondir nos principes d'analyse de risque. Nous sommes en effet habitués à nous interroger sur l'origine des menaces auxquelles nous devons faire face et à en écarter de nombreuses pour conserver des systèmes simples. Or, si nous retenons le scénario que Stuxnet visant les centrifugeuses iranienne, nous devons aussi reconnaître que pour réaliser sa contamination et atteindre son objectif, il a dû se répandre dans la nature et peut encore causer des dégâts sur des équipements d'autres industries. Le code utilisé par Siemens n'est-il pas aussi utilisé dans d'autres équipements industriels comme il est souvent l'usage ? Dès lors le fait de ne pas avoir identifié d'ennemis directs ne veut pas dire qu'il n'existe pas une exposition à une attaque extrêmement sophistiquée... La notion de dégâts ou de pertes collatérales bien connues dans les opérations militaires peuvent aussi exister dans nos entreprises.
Nous devons de même intégrer le fait que des attaques étatiques, même si elles ne sont pas totalement avérées, doivent être aujourd'hui considérées comme plausibles.
Beaucoup d'analyses de risque se concentrent sur la disponibilité des systèmes. Il faut que l'entreprise produise, vende et se fasse payer. Des moyens importants sont mis dans les sauvegardes, la lutte anti-incendie, les plans de reprise d'activité. Dans de nombreuses grosses PME, l'analyse de risque se limite d'ailleurs souvent à ce stade. La confidentialité des informations est souvent prise en compte en raison d'enjeux commerciaux, de contraintes réglementaires, par exemple pour les données de santé, ou encore de questions de souveraineté nationale. Là aussi, les moyens sont en général mis en œuvre sont parfois importants : chiffrement, traçage des logs, infrastructure de gestion de clés, etc.
Le contrôle de l'intégrité des programmes et codes exécutables ne suscite pour sa part qu'un niveau de préoccupation assez bas. Certes, toutes les entreprises admettent qu'il faut mettre des antivirus... encore que sur le Macintosh et les serveurs Unix / Linux la pratique soit encore exceptionnelle ! La défense en profondeur est parfois prise en compte, avec un logiciel anti-malware sur le poste de travail et un second sur la passerelle de l'entreprise, voire un troisième sur le serveur de messagerie si celui-ci est hébergé. Il est aussi souvent d'usage de contrôler l'accès à certains équipements en interdisant et en bloquant de nombreux accès : par exemple en supprimant les ports USB.
Ensuite, il existe les solutions de signatures des codes par différents procédés : RSA, courbes elliptiques, etc. Le système suppose la mise en place d'une infrastructure de gestion de clé IGC, ou PKI. On trouve malheureusement parfois des contrôles d'intégrité qui ne sont basés que sur un simple hash du code. Le code est envoyé avec son empreinte MD5, ou SHA1 : à la réception le système vérifie que le code et l'empreinte sont cohérentes. Cela n'empêche pas un éventuel attaquant de modifier le code et d'envoyer une nouvelle empreinte... Ce n'est pas sérieux !
Le cas de l'attaque Stuxnet nous révèle un autre scénario : celui du vol de certificats. L'autorité de certification ne sert plus à rien et l'IGC est détruite... Les premières traces d'une attaque ressemblant à ce qu'est devenu Stuxnet remontent, selon le rapport de Symantec, à fin 2008. La vulnérabilité permettant l'exécution de code distant dans le spooler d'imprimantes partagées date d'avril 2009. Une pré-version de Stuxnet est découverte en juin 2009. Le 25 janvier 2010, le driver Stuxnet est signé avec un certificat paraissant « valide » appartenant à RealTek Semiconductor Corp. Le 16 juillet 2010, Verisign révoque le certificat de Realtek Semiconductor Corp. Le 17 juillet 2010, ESET identifie à nouveau Stuxnet signé avec un certificat provenant de JMicron Technology Inc. Verisign ne révoquera ce certificat que le 22 juillet... Bref, l'ICG fournie avec Verisign est restée perméable durant de longs mois...
Mais ces scénarios sont-ils intégrés aujourd'hui dans nos analyses de risques ? Ne faut-il pas changer de paradigmes ? Trouver une autre façon de s'assurer de l'intégrité d'un code exécutable ?
L'interdiction de toute connexion sur une machine ne tient pas toujours face aux exigences de l'exploitation. On a déjà vu des systèmes avec des ports USB noyés dans la résine, mais il reste toujours un moment où on doit mettre à jour les logiciels, et alors...
Prétendre qu'un certificat ne sera jamais volé n'est pas non plus très sérieux. Ne faut-il pas aller plus loin avec d'autres mesures de sécurité et une défense en profondeur accrue ? ■

Le bilan Stuxnet pour les éditeurs d'antivirus

Entretien avec Pierre-Marc Bureau, chercheur-analyste chez ESET, Michel Lanaspèze, expert chez Sophos, et David Grout, expert chez McAfee.



Pour nos trois experts, les médias ne se sont pas saisis de l'histoire de Stuxnet très tôt. La complexité de cette menace et de son histoire en est probablement en partie la cause. Les détails de son fonctionnement ainsi que ses cibles ont été publiés au compte-goutte.

C'est le fait que la cible soit constituée d'infrastructures SCADA qui a créé le mouvement dans les médias explique Michel Lanaspèze. La plupart des laboratoires de recherche explique-t-il traitent plus de 60 000 nouveaux échantillons de malware chaque jour, ce qui leur laisse peu de temps pour analyser les intentions possibles d'un code malveillant : leur mission première est de détecter et bloquer les menaces, avant d'analyser et d'expliquer les conséquences possibles des attaques.
David Grout ajoute que les éléments nouveaux les plus forts autour de cette attaque sont surtout liés au fait qu'elle était scrupuleusement ciblée. Elle rentre dans une famille d'attaques spécifiques qui se nomment APT (Advanced Persistant Threat) qui ont un objectif unique, et qui sont écrites et dédiées à cet objectif. Le ver, poursuit David Grout, utilisait de surcroît une combinaison de facteurs qui permettent aujourd'hui de penser que les auteurs de ce ver avaient des moyens importants :

- Des signatures numériques spécifiques permettant de bypasser les contrôles applicatifs.
- L'utilisation d'un grand nombre de vulnérabilités inconnues ou non publiées.
- Une connaissance d'un niveau Expert des environnements Siemens PCL.
- Le besoin d'une première intervention manuelle sur le système pour lancer l'attaque.

Ce ver est extrêmement intéressant dans sa complexité ajoute-t-il :

- Une utilisation de 4 zero-day exploits (par exemple : ms10-046 – lnk/shortcut vulnerability, ms10-061 – print spooler vulnerability).
- Des drivers signés et valides (par exemple : mrxcls.sys).
- Le premier rootkit PCL (Programmable Logic Control).
- Des rootkit Windows.

- Des techniques avancées pour éviter les détections AV.
- Des techniques de propagation.
- Des mises à jour et des mutations (par exemple via des connexions sur *www.todaysfutbol.com* ou en peer to peer).

Il est extrêmement rare, ajoute Pierre-Marc Bureau, de voir un ver informatique exploiter une faille de sécurité jusqu'alors inconnue. C'est le premier malware à attaquer des infrastructures critiques. Un logiciel malveillant cherche habituellement à infecter le plus de systèmes possibles. Stuxnet devait pour sa part pénétrer un ou des réseaux hautement sécurisés. L'utilisation de plusieurs certificats volés pour se propager sans attirer de suspicion constitue aussi un fait nouveau.
Ce ver était complètement inconnu et se propageait par des vecteurs d'infection nouveaux, il était donc très difficile à détecter. Une fois le fichier soumis aux éditeurs d'antivirus, poursuit Pierre-Marc Bruneau, une détection a été ajoutée et maintenant les échantillons de Stuxnet sont détectés au même titre que tout autre « vulgaire malware ». Stuxnet utilise les mêmes technologies que d'autres malwares quand il s'installe sur un système, c'est-à-dire un ensemble de fichiers « Portable Executable » (PE).
Michel Lanaspèze confirme cette analyse. « *Les antimalwares, dit-il, sont très efficaces pour détecter et bloquer les malwares connus. Ils sont également efficaces, mais dans une moindre mesure, pour bloquer les malwares inconnus.* » Dès que Stuxnet a été identifié, la plupart des éditeurs de solutions anti-malwares ont rapidement mis à jour leurs solutions pour bloquer cette nouvelle menace et prévenir la diffusion de l'infection.
« *Pratiquement toutes les solutions antimalware intègrent des techniques qui vont bien au-delà des classiques « signatures » pour prévenir les infections de malwares inconnus* » poursuit encore Michel Lanaspèze. Par exemple, les techniques de protection comportementale, le HIPS etc... Ces techniques font l'objet d'innovations constantes, et c'est leur perfectionnement qui permettra de réduire l'impact des attaques « zero-day ». Il faut cependant garder à l'esprit qu'une protection efficace à 100 % contre toutes les menaces inconnues restera sans doute un Graal inatteignable, et c'est donc dans la mise en place de techniques de protection complémentaires (contrôle des accès réseaux, détection des intrusions, gestion des vulnérabilités etc.) et la capacité à réagir rapidement et efficacement à des attaques originales qu'il faut rechercher une réponse à de telles attaques.
Pour Pierre-Marc Bureau, une meilleure collaboration entre les éditeurs de sécurité et les communautés d'utilisateurs permettrait sans doute que dès qu'un fichier potentiellement malveillant est identifié, il serait soumis aux éditeurs d'antimalwares pour analyse. Cette collaboration favoriserait l'identification des menaces qui seraient alors plus rapidement détectées. De plus ajoute-t-il, plusieurs solutions peuvent également être envisagées pour sécuriser les systèmes d'exploitation ; n'oublions pas que, sans les failles inconnues exploitées par Stuxnet, il ne se serait pas propagé aussi longtemps sans être découvert.
Mais Pierre-Marc Bureau fixe aussi les limites de ce que peut faire un antivirus. « *Nos antivirus,* déclare-t-il, *ne doivent toutefois pas être responsables du contrôle de la signature de code.* » Cette tâche devrait être effectuée par le système d'exploitation. Dans le cas Stuxnet, la plus grande faille a été que JMicron et Realtek se soient fait voler leurs certificats et qu'ils n'aient pas rapporté cette fuite d'information. Ce manquement a mis des milliers d'utilisateurs, qui font confiance à leurs certificats, en danger.
Pour David Grout, la prévention contre de telles attaques passe par une combinaison de contrôle applicatif par liste blanche, d'antivirus, d'antirootkit, mais aussi de sécurité physique d'accès au matériel permettrait de limiter ce type d'attaque.
« *Il existe aujourd'hui,* explique encore David Grout, *deux principaux types d'attaques qui sont les vers et virus pour monsieur tout le monde et les nouvelles générations qui ciblent des actifs spécifiques : Stuxnet, Zeus, Aurora en font partie. D'où aujourd'hui le besoin primordial, de suivre et monitorer son infrastructure si celle-ci présente un attrait pour l'extérieur, certes les coûts ne sont pas anodins mais le risque est fort et le jeu en vaut surement la chandelle. Bon nombre de sociétés ont aujourd'hui classé l'antivirus dans la catégorie des outils de commodités ; je pense qu'elles sont dans le faux ; la donnée de l'entreprise vaut plus que jamais de l'or : concurrence sur brevet, avance technologique, revenu...* »
« *Pour conclure,* termine David Grout, *il faut savoir estimer correctement la criticité de la cible que l'on souhaite protéger pour y mettre les bons niveaux de protections et les moyens, ce n'est pas parce qu'un OS n'est que peu connu ou qu'une application n'est que peu attaquée que celles-ci ne peuvent pas attirer un public averti.* »
« *Enfin, cette affaire montre,* nous dit Michel Lanaspèze, *qu'il est légitime de se poser des questions sur la sécurité des certificats dans la mesure où il semble que Stuxnet ait pu être porteur de certificats qu'il n'était pas autorisé à utiliser.* »
« *Il semble évident,* termine pour sa part Pierre-Marc Bureau, *que dans le futur la validation d'intégrité d'un système sera en partie validée par un composant hardware. Par contre, je n'ai pas la compétence pour imaginer comment ces mécanismes seront déployés. La défense en profondeur, la séparation de privilèges, l'isolation de systèmes critiques, le contrôle d'accès sont toutes des solutions connues qui protègent efficacement les systèmes informatiques.* » ■

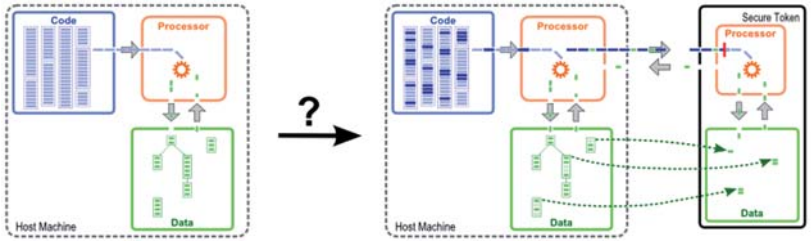
Changement de paradigme pour garantir l'intégrité du code avec la société Validy

Lors du Forum International de la Cybercriminalité, fin mars début avril dernier, la rédaction de Mag-Securs avait rencontré la société Validy. Nous connaissions déjà cette entreprise et nous étions intéressés à ses technologies en 2005. Nos discussions en mai et juin avec elle ont alors porté sur les possibilités de garantir l'intégrité d'un code exécutable.

La société Validy Net Inc. a été créée en 1998 par une équipe française dans l'Etat d'Oregon aux Etats-Unis. Ses fondateurs s'étaient connus au sein de la pépinière d'entreprises de l'Ecole Polytechnique à Palaiseau, X Pôle, autour du projet HyperParall Technologie, prédécesseur du HPC actuel et des ordinateurs dépassant de nos jours le Petaflop.
Gilles Sgro est issu du monde de la direction des systèmes d'informations. Jean-Christophe Cuenod est diplômé de l'ENS, rue d'Ulm, de la promotion 1981, option physique. Christophe Vedel, Docteur en informatique et diplômé de l'Ecole Polytechnique de la promotion 1986.
Validy Net Inc a investi au total 9 millions de dollars, dont 2 millions ont été consacré à la protection de la propriété intellectuelle. Sa filiale française, Validy SA, a déposé une dizaine de brevets dont la couverture mondiale représente un portefeuille d'une centaine de brevets et demandes de brevets. Validy Net Inc a été finaliste cette année de l'American Security Challenge.

> Combiner protection hardware et software

Validy s'est intéressée aux solutions de défense du code informatique. Pour cela, elle utilise un composant matériel sécurisé qui va exécuter une partie des opérations de l'application à la place du processeur principal de l'ordinateur. Ce dernier ne peut pas fonctionner sans obtenir le résultat des calculs de ce composant matériel. Cette technologie s'attaque donc au risque inhérent de la mise en œuvre d'un code exécutable dans un système. Un compilateur pour Java a ainsi été développé par Christophe Vedel pour « spliter » l'exécutable en deux : une partie pour le processeur principal et l'autre pour le coprocesseur de sécurité.
Les techniques de signatures des codes exécutables servent aujourd'hui à réduire le risque de compromission pour l'amener à un niveau résiduel, c'est-à-dire acceptable. Toutefois nous expliquait Jean-Christophe Cuenod en mai dernier (avant la médiatisation de l'affaire Stuxnet et juste après notre rencontre au FIC 2010), on a tort de considérer ce risque résiduel comme étant seulement potentiel : il est d'ores et déjà avéré ! Pour les systèmes embarqués, soumis à l'attaque éventuelle de l'utilisateur (ou d'un attaquant à l'insu de l'utilisateur), il y a longtemps que des systèmes de signatures ont été subvertis par diverses méthodes. La Xbox utilise ainsi des signatures pour n'accepter de charger que des jeux autorisés par Microsoft© et cette protection a sauté ! Plus récemment, l'iPhone d'Apple n'accepte théoriquement que le chargement d'applications signées provenant de l'Apple



Programme **sans** protection

Programme **avec** protection

Store. Il est cependant possible de « jailbreaker » son iPhone pour lui permettre d'exécuter à peu près n'importe quoi. Dans les deux cas, des améliorations logicielles et/ou matérielles ont permis à leur fabriquant de reprendre temporairement l'avantage pour les nouvelles séries de machines vendues, mais pas de reprendre le contrôle des machines subverties.

> Ne pas bâtir la confiance sur un élément extérieur non maîtrisé

De plus ajoutait Jean-Christophe Cuenod, quand la protection est centralisée (ndlr : c'est le cas de l'autorité de certification d'une IGC), la faire sauter ouvre tout le système. « *Notre solution porte pour sa part sur chaque système pris individuellement, ce qui découragera les attaquants...* »

Le problème de taille restant selon Jean-Christophe Cuenod, est celui de la confiance dans la vérification, donc in fine dans l'autorité de certification. Il existe deux voies d'attaque :

- le bypass de la vérification par corruption du programme de vérification ou de sa base de données de clés publiques ;
- le changement du code entre le moment de sa vérification et de son exécution.

Toutes sortes d'attaques tout à fait classiques peuvent être utilisées à cet effet. Selon la situation, on peut penser à :

- Le programme de vérification V est utilisé pour vérifier le programme P. Un bug de sécurité est repéré dans le programme P qui doit donc être remplacé par une version corrigée, signée et transmise par le réseau. L'attaque est la suivante : avant le remplacement de P par sa version corrigée, l'attaquant se sert de la faiblesse de P pour écrire un « exploit » et prend le contrôle de la machine le temps de modifier V en Vbad en substituant une clé publique. Dorénavant tout code provenant de l'attaquant est considéré comme légitime.
- L'attaquant a l'accès physique à la machine. Grâce à cet accès physique, il boote non pas le système standard, mais un logiciel permettant l'accès direct au file-system. Il se sert de cet accès pour changer V en Vbad ou même directement changer le programme P. La difficulté de ce type d'attaque dépend du type de hardware. Sur un PC elle est triviale et utilisée de manière « routinière » en bootant sur un « live CD » pour changer un mot de passe oublié. Sur les consoles de jeu, un « mod chip » à quelques euros permet le même résultat. Sur des machines telles que les smartphones, la miniaturisation est un frein pour le hacker de base mais n'arrête pas un attaquant déterminé.

Ces attaques ont déjà été utilisées avec succès à de multiple reprises pour désactiver des antivirus et seront sans nul doute employées avec le même succès pour désactiver les systèmes de vérification de signatures.

Prenons comme autre exemple un VPN réalisé avec des boîtiers dédiés. Ceux-ci établissent une enceinte sécurisée (walled garden), mais ne répondent pas à la problématique d'authentification du code. Si dans l'enceinte sécurisée, un seul des participants devient attaquant, volontairement ou non, les boîtiers ne servent plus à rien !

Juste pour prendre un exemple concret, si un employé travaillant dans l'enceinte sécurisée a envie de suivre les matchs la coupe du monde de football et installe un dongle 3G sur sa machine, le trou ainsi créé dans l'enceinte peut être béant et permettre une compromission massive.

Pour résumer « La confiance ne se transmet pas ». Si vous voulez avoir confiance dans un programme, vous ne pouvez pas vraiment compter sur un mécanisme extérieur à ce programme pour vous garantir son intégrité.

> La vérification est intrinsèque au système : c'est une auto-signature sans autorité de certification

C'est là que Validy Technology diffère de tous les autres systèmes que je connaisse : La vérification est intrinsèque au programme lui-même. La solidité dépend uniquement de :

- la qualité de la mise en œuvre hardware (robustesse du jeton à toutes les attaques envisageables) ;
- la qualité de la mise en œuvre software (nombre de variables cachées, entropie, taux de couverture, qualité des transformations du programme par le post-compilateur...) ;
- la disponibilité ou non pour l'attaquant d'un système lui servant à l'apprentissage.

La valeur ajoutée de notre solution est que sa solidité ne dépend donc pas d'hypothèses sur des programmes ou des mécanismes extérieurs. C'est tout simple mais extrêmement important conclut Jean-Christophe Cuenod qui met ainsi à bas la robustesse des IGC proposant ainsi un changement total de paradigme en matière de SSI pour garantir l'intégrité d'un code. C'est applicable aux programmes de Siemens visés par Stuxnet...

Les effets du ver Stuxnet commençaient à être médiatisés en juillet, puis explosaient en septembre après notre échange, en mai-juin, avec Jean-Christophe Cuenod, Gilles Sgro et Christophe Vedel... ■