

Sécurité des systèmes d'information

Virologie

SR – 2015-2016 –



Cas réel

Derniers articles | Archives | Recherche



Cyber espionnage : le piratage de l'Elysée décortiqué

par Stéphane Larcher, le 20 novembre 2012 19:03 ★★★★★

L'Express a mené une longue enquête autour du piratage de l'Elysée survenu au mois de mai dernier. La Présidence de la République aurait été victime de Flame, le ver le plus puissant jamais découvert. Si nos confrères ont raison, d'autres pays alliés ont sans doute été également ciblés.

Pour une fois, tous les chemins ne mènent pas à... Pékin, comme nous le décrivons dans notre dossier du mois consacré à la cyberguerre, mais à Washington. **L'Express** fait cette semaine sa Une sur le piratage de l'Elysée survenu au mois de mai dernier, entre les deux tours de l'élection présidentielle semble-t-il ou encore entre l'élection proprement dite et la passation de pouvoirs. « *Les attaques informatiques sont des actes de guerre* », affirmait le Pentagone au printemps dernier, montrant ainsi les dents contre les attaques qui menaçaient leurs infrastructures ou leurs secrets industriels et commerciaux. Si nous appliquons ces préceptes, devons-nous nous considérer en guerre contre les Etats-Unis puisque notre puissant voisin est clairement désigné par **L'Express** comme responsable de l'attaque survenue au printemps.

Dans un article publié au début du mois d'octobre, nous relations le très grand mutisme du patron de l'ANSSI autour de cette **affaire** et le même silence gêné de la part d'autres interlocuteurs habituellement plus diserts. « *C'est géopolitique* », avions-nous entendu, ce qui nous avait conduit, comme d'autres, à soupçonner une attaque provenant d'un « ami ». **L'Express** semble confirmer cette hypothèse évoquée dès le début par le *Télégramme de Brest* ou encore par Jean Guisnel dans *Le Point*. A l'instar de **L'Express**, nous avons contacté l'ANSSI qui nous a opposé la même fin de non-recevoir et d'autres sources nous ont indiqué que l'affaire était classée "Secret-Défense" et qu'il était donc impossible d'en parler, y compris en préservant leur anonymat.

Scenario possible

1 | Repérer des employés de l'Elysée

Pour le grand public, les pirates se cantonnent à envoyer des e-mails en masse à des adresses glanées sur Internet en se faisant passer pour des [grandes compagnies](#) ou [des banques](#) et inciter les victimes à fournir volontairement leurs informations bancaires.

Dans le cas d'une administration d'Etat comme la présidence de la République, le pirate effectue un travail préalable de repérage. Il identifie des employés de l'Elysée.

Aujourd'hui, rien de plus facile grâce aux réseaux sociaux professionnels. On peut par exemple lister sur le site [LinkedIn](#) les personnes travaillant au palais de l'Elysée. Il n'y a plus qu'à choisir.

2 | Entrer en contact via Facebook

Après avoir déterminé une cible disposant d'un compte Facebook (il s'appellera dans notre exemple Sébastien), notre hacker sélectionne une personne du même service que la victime ne disposant pas d'un compte Facebook (elle s'appellera Diane).

Par l'intermédiaire de ce compte fictif fraîchement créé, le pirate entre en contact avec la cible : la pseudo « Diane » ajoute Sébastien parmi ses « amis ». La proximité induite par le réseau social cumulée à la relation de travail supposée entre les deux internautes empêchent la victime de soupçonner la manœuvre.

3 | Préparer un site de phishing

Pendant ce temps-là, le hacker aura pris soin de mettre en ligne un site imitant le vrai portail intranet de l'Elysée avec une adresse quasi-identique (une lettre en plus ou en moins dans l'URL).

INTRANET

Il s'agit d'un réseau utilisant les mêmes fonctions qu'Internet (IP) mais à l'intérieur d'une entreprise ou d'une organisation. On peut le comparer à un réseau internet local.

Cette page web proposera de renseigner un identifiant et un mot de passe pour accéder à l'intranet. En réalité, le site est programmé pour enregistrer les informations et afficher une page d'erreur.

4 | Inciter la victime à se rendre sur le site

Suivant la fonction et le statut de la personne dont l'identité a été usurpée, via un message sur Facebook, le pirate prétexte une raison pour pousser la cible à se rendre sur l'intranet.

Diane explique à Sébastien qu'un nouveau mode de connexion à partir d'Internet est désormais possible. Elle lui fournit un lien vers ce « nouveau » portail de connexion.

Curieux à l'idée de découvrir cette nouveauté, Sébastien se rend sur le site et y entre ses identifiants. Voyant une page d'erreur s'afficher, il revient vers Diane pour lui expliquer que le système n'est visiblement pas encore opérationnel. Diane s'excuse, le pirate jubile.

Scenario possible

5

Infester le réseau

Une fois les codes de Sébastien récupérés, notre pirate accède à l'Intranet de l'Elysée. A partir de ce moment, il lui suffit d'y introduire un « ver ». En général, il s'agit de documents dont l'ouverture déclenche l'infection de l'ordinateur sur lequel il a été ouvert.

C'est ce qu'affirme L'Express : l'Intranet de l'Elysée aurait été infecté par un vers similaire au [virus Flame](#) soupçonné d'avoir été utilisé [par les Etats-Unis](#) et Israël à partir de 2007 pour espionner l'Iran, la Syrie, le Soudan et l'Arabie saoudite.

Selon Vitaly Kamluk, un employé de l'antivirus Kaspersky interrogé par L'Express, ce code malveillant permet de « collecter des fichiers, de réaliser des captures d'écran et même d'activer le microphone d'un PC. »

6

Récupérer les données exfiltrées

Ultime étape : récupérer les données. Flame fait ainsi transiter les informations via une multitude de serveurs aux quatre coins du monde. Ce système permet en théorie d'empêcher de remonter jusqu'au pirate.

Une fois les données récupérées, il ne reste que deux options :

- **récupérer la prime de fin de mission** si le hacker est à la solde d'un gouvernement ou d'une entreprise ;
- **vendre ces informations aux enchères** si le pirate travaille en freelance.



Virologie

Les possibilité d'un virus

Que peut faire un virus ?



From [profile picture]

VIRUS : Do not open a message with an attachment called Invitation Fb regardless of who sent it. It is a virus that opens an Olympic torch and will take the whole hard disk C of your computer. This virus has been received from a friend: Delete the **invitation** immediately. This VIRUSES classified by Microsoft as the most destructive virus ever, and there is no fix for this yet. PLEASE circulate THIS!!

4 minutes ago · ·



PLEASE CIRCULATE THIS NOTICE TO YOUR CONTACTS!

In the coming days, you should be aware! Do not open any message with an attachment called: Invitation FACEBOOK, regardless of who sent it.

It is a virus that opens an Olympic torch that burns the whole hard ...disc C of your computer.

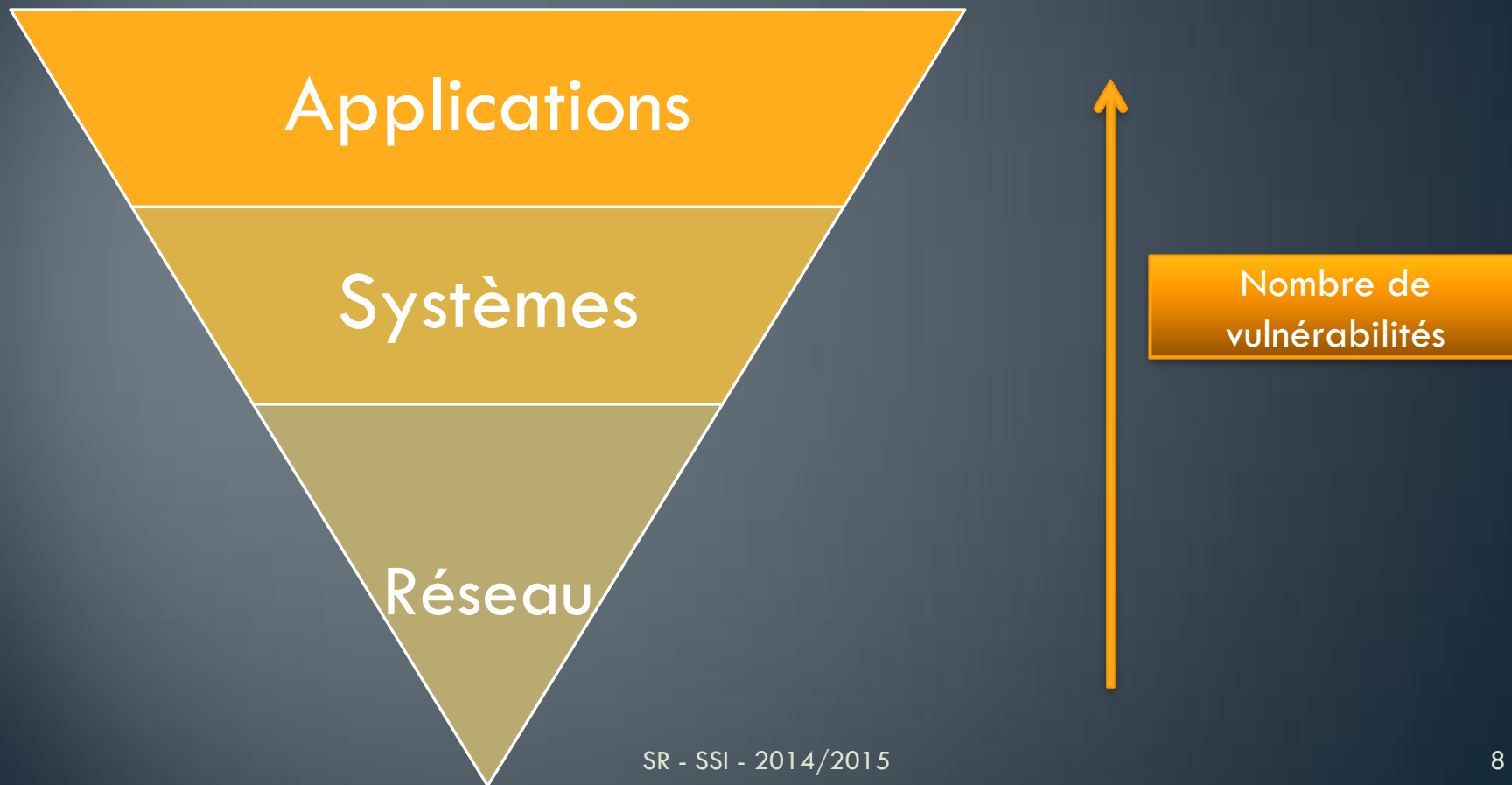
This virus will be received from someone you had in your address book .. If you receive a mail called: Invitation FACEBOOK, though sent by a friend, DO NOT OPEN IT and DELETE IT IMMEDIATELY

about a minute ago

Projet aurora

- Vidéo

Vulnérabilités les plus fréquentes





Virologie

Surface d'attaque

Vulnérabilités les plus fréquentes

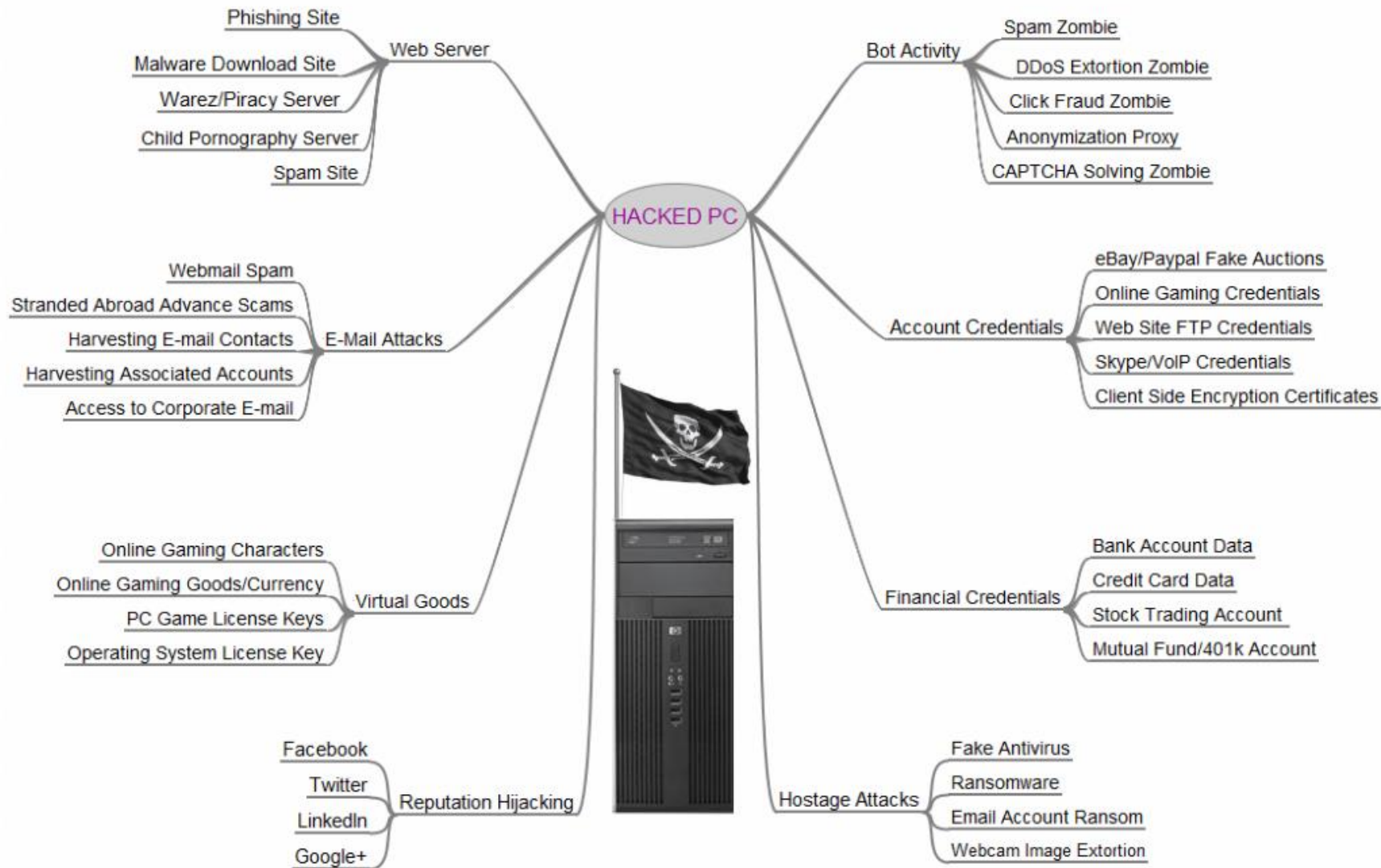
- Clients :
 - Navigateur Web, plugins (flash, quicktime) , ActiveX
 - Machine virtuelle java
 - Acrobat Reader, MS Office
 - Windows Media player, Real Player, iTunes
 - Messagerie électronique
- Application Web :
 - Injections SQL
 - XSS, CSRF
 - Modification de path
 - Injection de code
 - Interface admin non protégées

Vulnérabilités les plus fréquentes

- Failles systèmes (MS14-021 == CVE-2014-1776)
- Bruteforce, mot de passe faible ou par défaut, sessions nulles
- SGBD
- Faille antivirus
- Logiciel d'infrastructure (annuaire, sauvegarde, supervision, déploiement...)

Une menace permanente

- 0-day, c'est plus ce que c'était
- Une surface d'attaque élevé au niveau des utilisateurs
- Une attaque ciblé ne pourra pas être empêché
- Prendre en compte la compromission d'un poste client dans la réflexion SSI





Virologie

Historique

1982

- Elk Cloner
 - Virus,
 - Pour Apple II
 - Développé par un étudiant
 - Propagation :
 - Par disquettes, « auto-exécution »
 - Infecte le secteur de démarrage (« MBR »)
 - Affiche un poème selon le nombre de démarrages
 - Pas d'antivirus à cette époque... ☹
- NB : Retrait récent par Apple de la mention « pas de codes viraux » sur son site...

1988

- Ver Xerox
 - Premier ver réseau
 - Expérience malheureuse
 - Recherche de machines libres (« idle ») à travers le réseau
 - But : réutiliser la puissance de calcul perdue
 - Nommée « early experience with a distributed computation »
 - Expérimentation de recherche de machines : OK
 - Expérimentation de vérification du status : OK
 - Mais... au final, le ver plante les machines 1 à 1
 - Dénis de service généralisé et progressif.

2003

- Professionnalisation de la virologie
- Worm Blaster (=Nachi/Lovesan), en août
 - RCE sous Win 2000 + XP
 - Instabilité pour NT4 et 2003 Server = > reboot !
 - Seule l'action des FAI a pu le ralentir...!
 - Cible : DDoS sur windowsupdate.com, 15/08
 - Propagation par dépassement de tampon dans RPC DCOM, à distance.
 - Messages cachés = > d'où son nom.
 - Auteur de la variante B arrêté



Virologie

typologie

Typologie de virus

- Dropper / planteur = téléchargeur
 - Programme capable d'implanter exécutable malveillant
 - Ex: utilisé en exploitation de failles de sécurité
 - Composant générique, téléchargement « à jour »
 - Association courante « trojan dropper »

Typologie de virus

- Trojan horse / Cheval de Troie (« troyen »):
 - /!\ pas malveillant (transporteur)
 - Transporte une charge... qui peut-être maline !
 - Histoire du DivX (Pro)...
- Backdoor / porte dérobée
 - Implanté secrètement sur une machine
 - Permet un accès à distance
 - Niveau système d'exploitation ou logiciel simple
 - Ex : Fonction de suppression de logiciels sur mobiles ?

Typologie de virus

- BHO = Browser Helper Object / Extension du navigateur
 - Ex : Google toolbar, Bing toolbar
 - Aussi nommé browser hijacker
 - Composant chargé avec le navigateur
 - Interagit avec session
 - Peut modifier des données
 - Peut modifier des réglages du navigateur
 - Peut impacter le comportement réseau
 - Ex : FakeVLCAddon...

Typologie de virus

- Adware / publiciel = logiciel publicitaire
 - ADvertising + softWARE
 - Affiche des publicités
 - Activité fondée sur des éléments contextuels...
 - Navigation
 - Documents, ...
 - Peut être binaire ou simple librairie
 - Association courante : BHO adware
 - Caractéristique virale de furtivité, ou non

Typologie de virus

- Spyware / espioniciel
 - logiciels conçus pour collecter de l'information.
 - Certains proches des adwares, mais pas que redirection vers publicités ciblées
 - récupère infos nominatives et personnelles pour approche marketing par e-mail, courrier postal, téléphone.
 - Possibilité ensuite de monnayer les fichiers constitués.
 - Les autres = véritables logiciels espions enregistrant secrètement + retransmettant activité du PC
 - Souvent légitimes (ex : contrôle parental), mais détournés de leur but premier = > utilisés pour vrai espionnage.
 - Tendance dans les couples (voir plus loin)

Typologie de virus

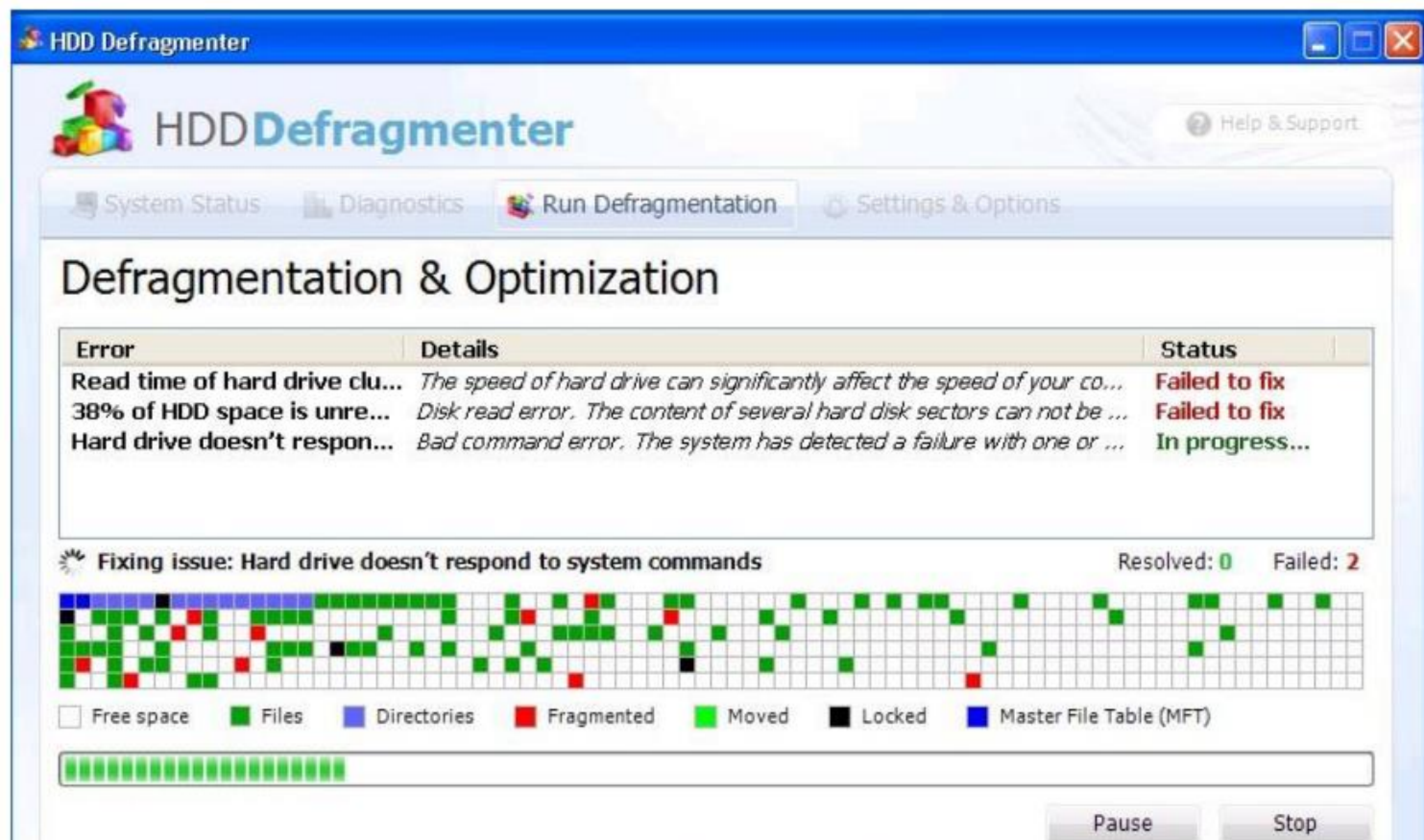
- Ransomware (CRYPTOLOCKER)
 - Chiffre les données personnelles
 - Une fois le chiffrement complet : popup demandant de payer
 - Délais avant suppression de la clé → peu de temps de réaction
 - Service « professionnel »
 - (numéro de téléphone de support en cas de problème...)
 - Variante pour NAS
 - SYNOLOCKER

Typologie de virus

- Rogueware / logiciel contrefait
 - Appelé aussi scareware
 - Faux logiciel, exemples :
 - Antivirus
 - Codec, lecteur multimédia,
 - Visionneuse (Flash...)
 - Téléchargeur « gratuit », « accéléré », ...
 - En hausse, donc rentable !
 - Ex : GPCode, demande de rançon pour MdP des docs ! [K Labs]
 - +500 000 variantes de faux antivirus [Sophos, 2011]

Exemple : FakeSysDef

Figure 38. Win32/FakeSysdef pretends to find computer problems and offers to fix them for a fee



Typologie de virus

- Greyware = PUP = Potentially Unwanted Program / application potentiellement indésirable
 - Pas de volonté de nuire
 - Utilisation pouvant être détournée :
 - perturber l'utilisateur,
 - (secrètement) modifier le niveau de sécurité de son système et porter atteinte à la confidentialité de ses activités et de ses données
 - Ex : barres d'outils, P2P, jeux, téléchargeurs...

Your personal files are encrypted!



Private key will be destroyed on
10/27/2013
1:22 AM

Time left
43 : 40 : 06

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt the files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>



Virologie

Technique de contournement d'AV

Wrapper

- Wrapper = « emballage »
 - Terme générique : marier 2 exécutables ensemble
 - Autres termes : binder, EXE joiner,
 - Outil pour automatiser la jonction entre programme légitime, et code malin
 - Sans écrire une ligne de code...
 - Souvent détecté (par défaut) par moteurs AV

Wrapper

- Wrapper (suite) :
 - Peut regrouper N fichiers programmes
 - Peut embarquer du code statique
 - Extrait à l'endroit choisi par le dev
 - Peut chiffrer le code embarqué
 - Déchiffré à la volée, à l'exécution
 - Code illisible pour l'AV... et pour les analystes ☹
 - Routines de (dé)chiffrement référencées par AV
 - Modification des routines par les codeurs...
 - Ex : Exe2vbs, Trojan Man (+ crypt), AFX Lace...

Packer

- Packer = compresseur / chiffreur
 - Parfois inclus dans les « wrappers »
 - Fichier stocké compressé/chiffré sur disque
 - 2 parties :
 - Compresseur/chiffreur, extérieur au programme initial
 - Décompresseur/déchiffreur, intégré au programme final
 - Légitime ? Protection de propriété intellectuelle
 - Malin ? Échapper aux moteurs AV...
 - Ex : UPX ! (tester sur VirusTotal...)

Wrapper/packer

- Wrapper/packers?
 - Compétition entre MàJ des signatures AV, et modification des wrappers
 - Quelquefois, le code viral est le même, seul le wrapper change
 - Pour l'AV, le code « vu » est différent...
 - Cascade :
 - Téléchargeur prend données uniques liées à la machine
 - Ex : numéros de série, dates d'installation, dates de dossiers, etc
 - Téléchargeur télécharge ensuite le vrai code viral,
 - dont le wrapper a été adapté aux données récupérées = > clé
 - Le code chiffré ne pourra être déchiffré que sur la victime !
 - Analyse du code complexifiée...

Virologie

BotNet

BotNet

- pilotage en central (« Robots Network ») par un C&C (Command and Control) (pilotage direct ou indirect)
 - Canal simple : IRC, serveur HTTP (compromis ?), DNS...
 - Peer to peer : utilisation de TOR possible
 - Autres : page Facebook, Twitter, etc.
- toute commande venant du central est exécutée
 - Téléchargement de code viral supplémentaire, mise à jour,
 - Attaque de site Internet, ou d'infrastructures,
 - Envoi discret de contenus indésirables (spam, phishing)

BotNet


- Rentabilisation :
 - Vol d'informations, de documents,
 - Chantage au déni de service,
 - Fraudes (bancaire : vol de comptes / CB)
 - Création / achat / location sur demande de :
 - codes malveillants personnalisés
 - Infrastructures BotNet déjà prêtes
 - Proxy web pour anonymiser la source d'une attaque
 - SPAM, XSS, SQLi, RCE, bruteforce...
- Architecture robuste, répartie
 - Utilisation de l'ADSL de particuliers,
 - Et liens Internet d'entreprises (contrôle flux sortants...?)

BotNet

- Qui est responsable de la machine infectée ?
 - L'entreprise l'est... mais le particulier ?
 - Difficulté de la mission de l'ANSSI
 - Cas de machines « attaquantes » sur le territoire FR
 - Répartition géographique
 - Différences de lois et arsenal juridique entre pays
 - /!\ Attention aux conclusions hâtives
 - IP attaquantes Chinoises, Russes, etc... qui est le vrai pilote ?
 - Solution globale complexifiée, rallongée !

CP :: OS statistics

173.242.112.135/office/obi/server/cp.php?m=stats_os

 **Citadel**
Universal Spyware System

● OS statistics

Online?

Information:

Current user: admin
28.12.2013
20:20:44 @ Europe/Berlin

Statistics:

Summary
OS
Installed Software

Botnet:

Bots
Web-Injects
Scripts
VNC

Reports:

Search in database
Favorite reports
Search in files
View screenshots
View videos
CMD Parser
Jabber notifier

Services

Notes
Crypt exe

System:

Information
Options

OS list for botnet: [All] >>

XP, SP 3	58
Seven, SP 1	41
XP, SP 2	37
Seven	30
Seven x64, SP 1	15
Seven x64	8
Unknown x64	4
Unknown	3
Vista, SP 2	2
Vista	2
Server 2003, SP 2	1
Server 2003, SP 1	1
Vista, SP 1	1
Vista x64, SP 1	1
Server 2008 x64, SP 2	1

Virologie

Rootkit vs bootkit

Persistence

- Rootkit
 - Terme détourné de son usage initial...
 - Historiquement : sous Unix, suite d'outils permettant d'obtenir droits « root »
 - porte dérobée avec accès privilégié,
 - détournement de commandes comme "ls"
 - Sous Windows, maintenant : programme implémentant fonctions de furtivité
 - Intercepter les pointeurs d'appel de fonctions systèmes
 - Cacher certains processus, fichiers, etc
 - Evasion des moteurs antivirus.

rootkit

- 5 types
 - Micrologiciel/matériel (ex : BIOS, Firmware carte réseau)
 - Hyperviseur (système d'origine lancé comme invité du rootkit)
 - Niveau noyau (ex : driver)
 - Niveau bibliothèque (remplacement de libproc.a pour filtrer le retour de ls / ps) - hooking
 - Niveau applicatif (remplacement de programme légitime)

Bootkit

- Infection d'une zone avant le boot de l'OS
- Permet de s'enfouir plus profondément dans le système
- Permet de persister même après suppression des fichiers infectés
 - Voir après formatage



Virologie

APT

Notions APT

- Advanced Persistent Threat
 - Catégorie d'attaque mettant en jeu divers techniques/outils
 - arsenal = > notion de « avancée »
 - Pas nécessairement outils évolués...
 - Notion, volonté importante de furtivité
 - Pas opportuniste
 - Scénarisation de l'attaque
 - Rester « sous le seuil radar »
 - Attaquants motivés, dotés de moyens

APT

- Controverse sur origine du terme
 - Probablement DoD (2006)
 - Dossier impactant l'US Air Force
- Pas uniquement l'apanage d'un Etat...!
- Mais des cas réels :
 - Israël « prestataire de services » pour USA ?
 - Attaques StuxNet, Flame, DuQu...
- Souvent un ensemble de différentes techniques et d'outils
 - Utilisation de plusieurs « Odays »

APT

- Gain pas toujours immédiat
 - Nécessité de rester non détecté pendant une longue période
- Cibles
 - Industriels importants
 - Gouvernements, politique
 - Communication, énergie...
- Intérêts
 - Commercial
 - Compétitivité
 - Technologies
 - ...

APT – exemple concret

- Cible : Multinationale
 - 3^{ème} infection
 - Toujours le même vecteur d'attaque :
 - Utilisateur clique sur un lien qui ouvre un fichier ADOBE
 - Utilisateur admin de sa station
- Une compte de service tourne avec un compte admin de domaine sur tous les postes (HP openview)
 - Exploitation de la mémoire de LSASS.EXE
 - Compromission d'AD (fichiers détectés sur certains AD)
- Source de l'APT : irrécupérable
 - Visible uniquement dans les logs
- Données exfiltrées par connexion SSL (trâces sur le proxy)

APT vs Attaques traditionnelles

Attaques « Traditionnelles »

- Elles sont généralement menées par un pirate ou un petit groupe de pirates.
- Leurs impacts varient (souvent mineurs et rarement majeurs).
- La cible est généralement découverte de façon opportuniste.
- Les objectifs ne sont pas forcément définis. Ils vont jusqu'où le système permet d'aller, et là où les données sont intéressantes.
- Les compétences du pirate varient (du script-kiddie au blackhat guru)
- La furtivité n'est pas une priorité (tout dépend du niveau de compétences de l'attaquant).
- Les attaques sont souvent menées contre des systèmes faiblement patchés, ou mal/peu administrés.
- La recherche du gain (si tant est qu'il y en ait un) est rapide.
- Les pirates recherchent généralement une sorte de reconnaissance après leurs méfaits.

• Attaques APT

- Elles sont dites à « signaux faibles » mais leur impact est majeur (Low-frequency & high-impact)
- Elles sont basées sur des objectifs et une stratégie (pas d'improvisation)
- Les techniques employées sont sophistiquées.
- Elles nécessitent de la coordination entre les pirates qui les conduisent.
- Elles nécessitent des bonnes compétences techniques (pas tout le temps)
- L'attaque doit rester furtive
 - Ne pas générer de bruits (sous le radar)
- Le gain financier ou industriel n'est pas immédiat
 - L'attaque doit durer jusqu'à l'atteinte de l'objectif.
 - Dans le cas de vol d'information et d'exfiltration de données, cela peut être très long.
- Elles ont un coût non-négligeables
 - Exit les script-kiddies et les hackers en quête de notoriété
 - A priori elles sont orchestrées par le crime organisé, des groupes militants, voire des Etats

Anatomie d'une attaque APT

- Préparation de l'attaque et des objectifs
- Elaboration de la stratégie d'attaque
- Intrusion furtive dans l'infrastructure de la cible
- Repérage et état des lieux de l'écosystème cible (scan, capture réseau, etc.)
- Compromission de systèmes, récupération d'identifiant, de comptes, d'adresse
- Exécution de code (backdoors, chevaux de Troie, proxy, etc.) et déploiement d'outils (ex. RAT, kits etc.)
- Recherche de nouvelles cibles & développement de codes malveillants ciblés
- Utilisation de privilèges obtenus pour accéder aux données
- Exfiltration des données (protocoles légitimes, emails, covert-channels)

Virologie : code viral ciblé

- Problème : découverte 1 à 3 ans après le début !
 - Quid des traces ?
 - rotation des journaux... quand ils sont activés !!
 - Quid des contrôles ?
 - flux « suspects » sortant en HTTPS ?
 - Qu'est-ce qui a été vraiment ciblé ?
 - Qu'est-ce qui a vraiment été exfiltré ?
 - Jusqu'où l'intrusion a-t-elle pu aller ?
 - Quid des comptes admin, notamment AD...?

Virologie : code viral ciblé

- Développement sur mesure
 - Cibles déjà définies par commanditaire
 - Entité gouvernementale
 - Entreprise avec enjeu particulier
 - Acteur vital pour le pays, la zone économique
 - Acteur majeur niveau économique
 - Guerre concurrentielle « avancée »
 - But final, réel ?
 - Atteinte à l'information, vol
 - Destruction / altération au passage ?
 - Manifestation :
 - Défacement de portails, affichage de bannières, etc
 - Paralysie des services : visible ou non

Virologie : code viral ciblé

- Prise en compte de l'architecture cible
 - Systèmes d'exploitation utilisés
 - Windows ?
 - Versions ? SP ? 32/64 bits ?
 - Autres ? Apple / Linux ?
 - Solutions de sécurité présentes
 - Antivirus ? Quel éditeur ? Quelle version ?
 - Prestation temporelle : passer à travers moteur + signature
 - Pare-feu / sondes
 - Trafic encapsulé, obfusqué, chiffré
 - Proxies ?
 - Codage des adresses IP dans le code source du virus, ...
 - Bien plus difficile à détecter et stopper !
 - Un antivirus n'est pas toute la sécurité.....

Exemples d'APT

- Codes viraux ciblés ? (NB : analyse pas terminée !)
 - Stuxnet
 - Premier missile numérique ? (Centrales nucléaires iraniennes)
 - Quelques imprécisions de cible...
 - Signature électronique volée = > furtivité AV
 - DuQu
 - Réel but : Préparer une future attaque ?
 - Vol d'infos sur systèmes de contrôle industriel (ICS)
 - Vol frappes au clavier, certificats électroniques, infos système
 - Oday MS Word (polices TrueType) – MS11-087
 - Presque identique à Stuxnet (code source), portée différente
 - Auto-désinstallation après 36 jours
 - Flamer
 - Complexe et surtout imposant. Record de taille : 20Mo !
 - Outil ultime d'espionnage !
 - Intercepte : emails, PDF, MS Office, AutoCAD, audio, écran, Skype...
 - 100 Millions de dollars de coût
 - « kill » command envoyée et exécutée après révélations dans la presse IT
 - Faux certificat « Microsoft Enforced Licensing Intermediate PCA », collision MD5 !
 - S'adapte à l'antivirus local, pour limiter risque de détection
 - Emet des balises en Bluetooth pour repérer d'autres machines infectées

Les réseau hors ligne sûr ?

- Vidéo stuxnet