

Les PME contre la mafia

- retour d'expérience -

Nicolas RUFF

EADS Innovation Works SE/IT

nicolas.ruff (à) eads.net

Introduction

Introduction

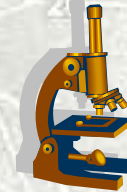
Lundi matin

8:00:42 CET, quelque part dans Paris ...



Une DLL « suspicieuse » est détectée par l'antivirus

8:10:00 CET la souche est capturée pour analyse



- Résultats:

- Un exécutable est résident sur la machine
- Il a été installé depuis une clé USB "infectée"
- Il n'a jamais été détecté par l'antivirus
- Il utilise des techniques "avancées"
 - Ex. NtOpenSection() sur \Device\PhysicalMemory
- Il télécharge régulièrement des composants (DLL) depuis Internet
- Accessoirement, le poste infecté est utilisé pour réaliser des virements bancaires
- ...

Introduction

Vendredi soir

17:42:00 CET, quelque part en proche banlieue ...



Des fichiers PDF « suspects » sont reçus par email

19:00:00 CET le fichier est entièrement décortiqué



- Résultats:
 - Le contexte de l'envoi est "crédible", quoiqu'un peu déplacé
 - Le fichier PDF embarque deux exécutables Win32 (XOR un octet fixe)
 - Le premier nettoie et relance le PDF
 - Le deuxième s'injecte dans Explorer et installe une porte dérobée
 - Aucun outil de sécurité n'a détecté l'attaque
 - Ni au niveau de la passerelle, ni au niveau du poste



Introduction

- « *Lessons learned* »
 - Les antivirus ne détectent pas toutes les attaques
 - Ils détectent environ 30% des attaques actuellement actives sur Internet
 - Source: Cyveillance
 - Les PDF sont dangereux
 - Il faut désactiver JavaScript (au niveau Adobe Reader)
 - Il faut activer DEP (au niveau Windows)
 - Un poste de travail "standard" doit être patché en moyenne tous les 4 jours ...
 - Source: Secunia
 - Les clés USB sont dangereuses
 - Et pourtant indispensables ...
 - Un malware qui a pu s'exécuter en tant qu'administrateur est difficilement désinfectable

Introduction



- Ceci est un retour d'expérience alliant les 3 expériences suivantes:
 - Administration du réseau bureautique d'une TPE
 - Avec plus de 40 postes en libre service
 - Audits et tests d'intrusion dans des TPE/PME
 - TPE/PME = moins de 5 personnes dédiées à l'informatique
 - Cœur de métier sans lien avec l'informatique
 - Activité de réponse aux incidents
 - Analyse de malwares ou de sites compromis
- Une partie des recommandations présentées est déjà appliquée
 - L'autre est dans la "todo liste" 😊
 - Uniquement du concret

Panorama des attaques



- Quelle que soit la taille de votre entreprise, vous êtes victimes d'attaques
 - Opportunistes
 - Ex. sites légitimes infectés
 - Improbables
 - Ex. chargeur de piles ... infecté en usine depuis 3 ans
 - "Plus ou moins" ciblées
 - Ex. message "crédible" envoyé à toutes les adresses connues
 - Advanced Persistent Threats (APT)
 - En gros, un pentesteur qui ne vous envoie pas la facture
- Malwares 2 – technologies de protection 0
 - La meilleure protection semble être ... de ne pas être administrateur de son poste
 - "Faites confiance à Microsoft" ☺

Se protéger au-delà des antivirus

Les contraintes

Contraintes



- Contraintes environnementales (inaliénables)
 - #1 les ressources techniques et budgétaires
 - Les ressources allouées à l'informatique sont faibles
 - Et les ressources allouées à la sécurité quasiment nulles
 - Il est de toute façon difficile de trouver des compétences techniques
 - Les antivirus sont mauvais
 - Ils détectent très peu d'attaques le jour de leur sortie
 - Ils tombent en panne sans raison
 - Exemple:
 - Téléchargez les sources du Framework .NET (<http://referencesource.microsoft.com/netframework.aspx>)
 - Ouvrez le fichier ZIP de 150 Mo contenant les sources
 - Microsoft Security Essentials se plante
 - » Note: ceci est un "0day" ☺
 - Les autres outils de protection sont "expérimentaux"



Contraintes

- Contraintes environnementales (inaliénables)
 - #2 les utilisateurs
 - Les utilisateurs en savent plus que "l'informaticien"
 - Ils tentent de dépanner les problèmes eux-mêmes
 - Et font les morts en cas d'échec
 - La sensibilisation est vouée à l'échec
 - Les utilisateurs choisissent des mots de passe faibles
 - Ex. 123456 – utilisé par presque 10% des comptes en ligne
 - Les utilisateurs paniquent si le système leur pose une question
 - Et répondent "oui" en général
 - Notons que certains systèmes en tiennent compte ☺
 - Les utilisateurs installent tout ce qu'ils peuvent
 - Les logiciels n'exigent plus d'être "admin" pour s'installer
 - Ex. Skype, Chrome, FireFox ...
 - Le problème des "Portable Apps"

Contraintes

- Contraintes environnementales (inaliénables)
 - #3 l'environnement
 - Une grande quantité de clés USB sont infectées
 - Autorun + ".EXE"
 - Mais il est illusoire de vouloir bloquer ou contrôler les ports USB
 - Internet est hostile
 - *Vraiment* hostile
 - Les éditeurs d'applications sont hostiles
 - Applications boguées
 - Lenteur des correctifs
 - Pas de prise en compte des contraintes d'administration
 - Adobe: on aimerait avoir des fichiers ADM/ADMX, MSI/MSP, etc.

Se protéger au-delà des antivirus

Plan d'action



Plan d'action

- Il est absolument nécessaire de prendre en compte toutes les contraintes précédentes
 - ... pour définir un schéma de protection réaliste
 - ... sauf à être en mode "CYA security"
 - (c) Bruce Schneier
- Par exemple
 - Inutile d'exiger des autres ce que vous n'appliqueriez pas à vous-même
 - Ex. blocage des ports USB, interdiction de LinkedIn, etc.



Plan d'action

- Mes idées
 - Limiter ce qui s'exécute
 - Sans pour autant bloquer complètement l'utilisateur
 - Auditer ce qui s'est exécuté
 - Identifier les anomalies

Plan d'action - limiter



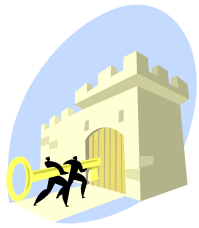
- Configuration Windows
 - Règle #1: l'utilisateur ne doit pas être administrateur du poste
 - Les malwares actuels sont trop difficiles à désinfecter
 - Infection du noyau
 - Infection d'exécutables
 - Infection du secteur de boot
 - Même sous Windows XP, cette position est tenable
 - Pas besoin d'être paranoïaque
 - Il suffit de bloquer les exécutions "directes"
 - Autorisation des ".MSI"
 - Il n'existe pas de virus ".MSI" à ma connaissance
 - Outils tiers
 - Ex. SudoWin, Superior SU, ...

Plan d'action - limiter



- Configuration Windows
 - Règle #2: W ^ X pour les fichiers exécutables
 - L'essentiel des malwares actuels vont lancer un ".EXE" à un moment ou un autre
 - Appelé "*Dropper*", "*Stage 2*", etc.
 - Utilisation astucieuse des stratégies de restriction logicielle
 - Windows XP ► *Software Restriction Policies* (SRP)
 - Windows Seven ► AppLocker (beaucoup mieux !)
 - Interdire l'exécution depuis
 - » %UserProfile% (ou au moins %AppData% et %Temp%)
 - » E:\ ... Z:\ (clés USB)
 - Bonus: signature des applications autorisées
 - » Très simple à mettre en œuvre !

Plan d'action - limiter



- Configuration Windows
 - Règle #3: défense en profondeur
 - Activer DEP (idéalement en mode "OptOut")
 - Déployer IE8 (en remplacement d'IE6)
 - Il reste des milliers d'options de configuration
 - Bravo à ceux qui avaient désactivé le sous-système NTVDM !
 - Mais globalement les guides de sécurisation sont dépassés par la complexité du système

Plan d'action - limiter



- Configuration des applications
 - C'est l'enfer ...
 - Produits Adobe
 - L'accès aux ".msi" est soumis à accord de licence et de confidentialité
 - Acrobat: désactiver JavaScript
 - Mais l'utilisateur se voit proposé de le réactiver
 - Ne protège que contre les PDF en IFRAME (c'est déjà bien)
 - Flash: aucune prévention sérieuse des risques
 - Java: l'enfer à mettre à jour
 - Heureusement Java ne sert plus à rien aujourd'hui
 - Les applications qui en ont besoin embarquent leur propre JVM
 - RealPlayer, QuickTime, etc.
 - Leur faire la guerre: le ratio utilité/risque est trop faible

Plan d'action - auditer



- Journalisation Windows
 - Très utile à journaliser: "création/destruction de processus"
 - Si ACROREAD.EXE lance SUCHOST.EXE puis IEXPLORE.EXE
 - dans un intervalle de quelques secondes ...
 - ... alors vous avez un problème !
 - Avantage(s)
 - Il est possible de retrouver les exécutable même s'ils sont dissimulés par un "rootkit"
 - Journaliser: "événements système"
 - Permet de détecter les applications en écoute sur le réseau
 - ... même si le pare-feu Windows est désactivé

Plan d'action - auditer



- Exploitation du journal d'évènements
 - Outils standards
 - Interface avec WMI
 - Notification sur nouvel évènement
 - XP: API de notification (Windows Event Collector)
 - Vista+: il est possible de déclencher une "tâche" sur un évènement donné
 - Note: un produit de sécurité sérieux utiliserait l'API `PsSetCreateProcessNotifyRoutine()`
 - Mais cela nécessite d'écrire un driver ...

- Sur mon poste
 - 8 Mo de journal sécurité = 3 semaines d'activité

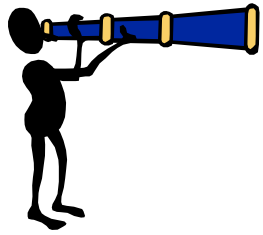
- Comprendre comment vient l'infection
 - Un poste infecté permet de "vacciner" tous les autres

Plan d'action - identifier



- Détection des anomalies
 - Une partie essentielle !
 - Et presque la plus facile ...
 - Quelques heuristiques
 - HIPS
 - Intégrité de la clé Run (ou équivalents)
 - » cf. Sysinternals Autoruns
 - Intégrité de la configuration réseau (DNS, LSP)
 - BHO chargés dans Internet Explorer
 - Nombre d'évènements par jour dans les journaux Windows
 - NIPS
 - Détection de trafic suspect
 - » Ex. outils OurMon, BotHunter, Snort, Malware Domains, ...
 - Inventaire logiciels
 - Crash logiciels
 - *Corporate Error Reporting (CER)*

Plan d'action



- Quand tout va bien ...
 - Bonne nouvelle ! C'est le moment ...
 - De lire les logs
 - D'inspecter une machine au hasard
 - Quels nouveaux logiciels ont-ils pu apparaître ?
 - De tester un nouvel outil
 - De faire de la veille sur Internet

Conclusion

Conclusion

- Défendre un réseau d'entreprise devient une mission impossible
 - La quantité, le niveau technique et la motivation des attaquants croît exponentiellement
 - L'essentiel de la défense repose sur le sérieux des éditeurs de logiciels
 - Le modèle économique actuel ne permet pas de leur faire confiance
 - Le "Cloud" fera-t-il mieux ?
- Heureusement, le RSSI consciencieux réalise déjà l'impossible
 - Pour les miracles, prévoir un délai

Conclusion

- Quelles perspectives pour la sécurité à moyen terme ?
 - Contraintes légales sur les éditeurs
 - Obligations de qualité / de correction, maintien en conditions de sécurité, ...
 - Contraintes légales sur les sociétés
 - Directives Nationales de Sécurité, obligation de divulgation des pertes de données, ...
 - Informatique en mode "Cloud"
 - Implication de l'ANSSI auprès des PME
 - CSPN, OzSSI, ...
 - Minitel 2.0
 - Fin du monde
- ... tout reste possible !