CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

LES MALWARES

LES MALWARES

Les techniques et les usages des malwares

- Même si les malwares ne sont pas spécifiques à Windows, il est important de les présenter :
  - Présentation des grandes familles de malware
  - Présentation de quelques techniques qu'utilisent les malwares
  - Présentation de quelques solutions de protection

LES MALWARES

Les jokes

- Un malware est très rarement conçu pour le plaisir/rigoler mais pour atteindre un objectif
- Quelques applications ont quand même été développées pour le fun pour par exemple, faire éjecter le lecteur CD pour faire office de support de cannette, avoir un mouton qui se balade sur l'écran … etc…
- Il sont à l'origine inoffensifs mais ils sont souvent vecteur de diffusion d'autres malwares qui eux font mal !
- Ne sont pas vraiment des malwares mais certains antivirus les détectent comme tel et les bloquent

⇒Un attaquant utilisera un Joke pour y cacher un malware et attendre une diffusion importante pour le déclencher

LES MALWARES

Les keyloggers

- Le keylogger permet d'enregistrer l'appui des touches du clavier, l'emplacement du clic de la souris et de réaliser des captures d'écran
- Le but est clairement la récupération d'informations :
  - Identifiants et mots de passe
  - Numéros de carte bancaire
  - Ident. de compte bancaire (clavier virtuel par des images)
- Se positionne au niveau driver (GDI)
- Très présent dans les Cyber cafés !!!
- Le mot de passe unique ou par token est une bonne protection

LES MALWARES

Les botnets

- Un botnet est un ensemble de machines compromises qui sont capables de réaliser en même temps des ordres envoyés par un attaquant
- Un botnet peut être constitué de quelques centaines de machines jusqu'à des centaines de milliers de machines
- Les botsnets sont groupés par capacité et par objectif (DDOS, Spam, propagation, calcul distribué, …)
- Les botnets sont souvent gérés par un ou des serveurs centraux qui distribuent les ordres (C&C)
- La location d'un botnet de 1000 PC pour une heure : 9$

LES MALWARES
C&C

- Le Command & Control permet de gérer et lancer des ordres aux machines d'un botnet
- Une machine compromise va vouloir se connecter régulièrement ou constamment à son C&C
- Le C&C est capable de mettre à jour les machines, de récupérer des données, et de leur donner des taches
- Un C&C peut fonctionner en mode distribué
- Si on détruit un C&C ou que l'on bloque le flux réseau, le botnet n'est plus utilisable par l'attaquant

⇒Trouver le trafic d'un C&C permet de bloquer le flux et identifier les postes compromis

LES MALWARES
Deny Of Service

- Une attaque par Deny Of Service permet de rendre un service, une application, un système indisponible
- Parmi les plus anciens et célèbres, on peut citer le Ping de la mort : il suffisait d'envoyer un ping pour faire planter ou rebooter la cible
- L'attaquant utilise un bug dans une application pour réaliser un DOS
- Même dans une architecture est redondé, l'attaque réussira, tous les serveurs sont identiques
- Un DOS peut être atteint par une saturation des ressources (réseau, cpu, mémoire, disque)

LES MALWARES
DDOS

- Pour augmenter les chances de réussite d'un DOS dans le cas de saturation des ressources, les attaquants réalisent des DDOS (Distributed Deny Of Service)
- Les botnets sont utilisés pour réaliser des DDOS
- Le but d'un DOS ou d'un DDOS est de rendre indisponible afin de :
  - nuire à l'image, à un concurrent
  - faire du chantage dans le cas de e-commerce
  - impacter les services ou une économie d'une organisation ou d'un pays
- Peu de solutions permettent d'empêcher un DDOS

LES MALWARES
Le Spam

- Le Spam ou courrier indésirable n'est pas en soit un malware mais les serveurs qui sont utilisés pour émettre ces Spams sont souvent des machines compromises groupées en botnet
- Le malware profite de l'ouverture du port 25 (SMTP) des réseaux ou utilise le serveur de mail de l'hébergeur ou de celui de l'entreprise pour diffuser ses Spams
- Une analyse de trafic sur le port 25 permet à un administrateur d'identifier un problème

LES MALWARES

Le Phishing

- L'Hameçonnage est un email qui essaie de se faire passer pour un email officiel (banque, opérateur, EDF, …) en incitant l'utilisateur à se connecter avec ses identifiants sur un faux site ressemblant au vrai et si possible d'entrer ses numéros de carte bleu
- Même techniques de diffusions que pour le Spam
- Les faux sites sont souvent hébergés sur des machines compromises
- La vérification du nom de domaine et du certificat du site est une des seules protection pour l'utilisateur
- Ne pas cliquer sur les liens dans un email, toujours retaper l'url dans le navigateur

LES MALWARES

Le ransomware

- Le but d'un rançongiciel est de prendre en otage des données personnelles ou sensibles et de demander une rançon pour les rendre
- Certains rançongiciel ne font que bloquer démarrage de la machine, mais d'autres vont jusqu'à chiffrer le disque dur ou les données personnelles
- Dans le cas du chiffrement, l'utilisation de la dernière sauvegarde est la seule solution
- Dans le cas du paiement, il peut arriver que l'attaquant n'abandonne pas son pigeon au premier paiement, il n'aura alors qu'un bout de la clé de déchiffrement et il devra repayer pour avoir la suite de la clé et peut être sans jamais avoir la clé complète

LES MALWARES
RAT

- Un RAT (Remote Administration Tool) permet la prise de main à distance
- Un RAT peut être légitime, cela peut être un outil déployé par le support informatique de la société
- Un attaquant qui souhaite se connecter quand il souhaite à une machine compromise va installer un RAT et va essayer de la cacher tout en le gardant accessible

⇒L'outil RAT légitime de doit pas pouvoir être utilisé par un attaquant

LES MALWARES

Le Minage

- Avec la popularité des BitCoins le minage est devenu une activité lucrative
- Le but de l'attaquant est d'utiliser la puissance de calcul des machines compromises pour créer des Bitcoins
- Utilisation de Botnets dédiés au minage
- Les impacts sont sur les performances des machines car les ressources de la machine sont partagées et surtout un coût financier lié à la consommation en énergie
- La surveillance de la charge des machines d'un réseau permet de détecter cet usage illégitime

LES MALWARES

Cassage de mot de passe distribué

- Le cassage de mot de passe est plus ancien et utilise des techniques similaires au minage
- Utilisation de la puissance de calcul pour essayer toute les possibilités de mots de passe, chaque machine d'un botnet essaie en parallèle un échantillon
- Le cassage de mot de passe est plus difficile à détecter au niveau de charge ou de la consommation électrique car il peut ne durer que quelques minutes ou quelques heures

LES MALWARES

Le Rootkit

- Le « trousse à outil pirate » est en ensemble d'outils que va installer un attaquant ou un ver afin d'avoir tout se qu'il lui faut pour se dissimuler et rester persistant
- Un Rootkit va par exemple modifier explorer.exe pour ne pas afficher à l'utilisateur certains fichiers ou dossiers dans lequels seront présents les binaires comme un RAT ou un Keylogger
- Un Rootkit évolué modifie les structures dans le noyau pour cacher les processus et les fichiers. Il devient difficile à détecter même pour un antivirus car il est au plus bas niveau.

LES MALWARES

Les vers

- Le but principal d'un ver est de se propager
- Les phases que réalisent un ver en boucle :
  - Recherche d'un cible exploitable
  - Exploitation d'une faille sur la cible pour s'installer
  - Mise à jour de la faille pour éviter une surcontamination
  - Installation d'une back door
  - Analyse du contenu de la machine
  - Réalisation d'une action en fonction de son rôle (destruction, botnet, ddos, vol de données, keylogueur,…)
- Un des plus médiatisé : « I love you » (mail avec pièce jointe + envoi à tout le carnet d'adresses)

LES MALWARES
Multi-malware

- Un malware évolué est constitué de plusieurs malwares, chacun ayant un rôle bien défini :
  - Trouver et pénétrer un système (faille d'un application)
  - Elever les privilèges (faille du système)
  - Désactiver des protections (AV, mise à jour)
  - Installer un Rootkit (outils, dissimulation et résilience)
  - Gérer les autres malwares en lien avec un C&C (mise à jour, rapport d'état, déploiement, nettoyage)
  - Réaliser des tâches (Spam, DDOS, Espionnage, Minage, …)
- « Un malware peut en cacher un autre »
- Une machine compromise va évoluer dans le temps pour résister aux mises à jour des antivirus et en fonction des besoins des attaquants

LES MALWARES
Les malwares dormants

- **En fonction des objectifs d'un attaquant, une machine ne réalisera pas d'actions dès qu'elle est compromise**
- **La machine compromise sera utilisée pour :**
  - **Une attaque massive d'une organisation ou d'un état au même moment souvent à usage unique**
  - **Etre vendue en masse (botnet) sur le marché « Dark »**
  - **Etre vendue à concurrent pour du vol technologique**
  - **Ne jamais être utilisée car :**
    - Machine limitée en ressources (modem 56k, très rarement connecté)
    - C&C inaccessible (flux bloqué, serveur éteint par la police)
    - Détection que la machine est un pot de miel
    - Bug dans le malware

LES MALWARES

Les failles 0-Day

- Un faille Zero-Day est une faille d'un logiciel ou d'un système pour lequel il n'y a pas encore de correctif car la faille n'est pas encore connue de l'éditeur
- Un système à jour ne permet pas de se protéger contre une attaque utilisant un 0-Day
- Dès qu'un 0-Day est utilisé, suite à une investigation ou à un pot de miel, elle est diffusée par les CERTs au travers de CVEs pour que les éditeurs puisse sortir le plus rapidement possible un patch
- Il existe un marché « Dark » des 0-Day (5000 à 250000 €)
- HachingTeam : société spécialisée en outils d'attaque et de 0-day à destination des gouvernements, elle s'est fait piratée et de nombreux 0-Day ont fuités

LES MALWARES
La back door

- La « Back door » est un accès prévu par le développeur d'une application ou d'un système afin de pouvoir s'y connecter plus tard sans le consentement de l'utilisateur et à son insu
- Par exemple, certains constructeurs de routeur adsl grand public ont ajouté dans le code un login/password qui leur permet de se connecter avec les droits root
- L'un des risques, est la découverte par des attaquants de la back door
- Un attaquant peut aussi patcher une application pour y intégrer une back door

=> La meilleure protection est l'audit de code (open source)

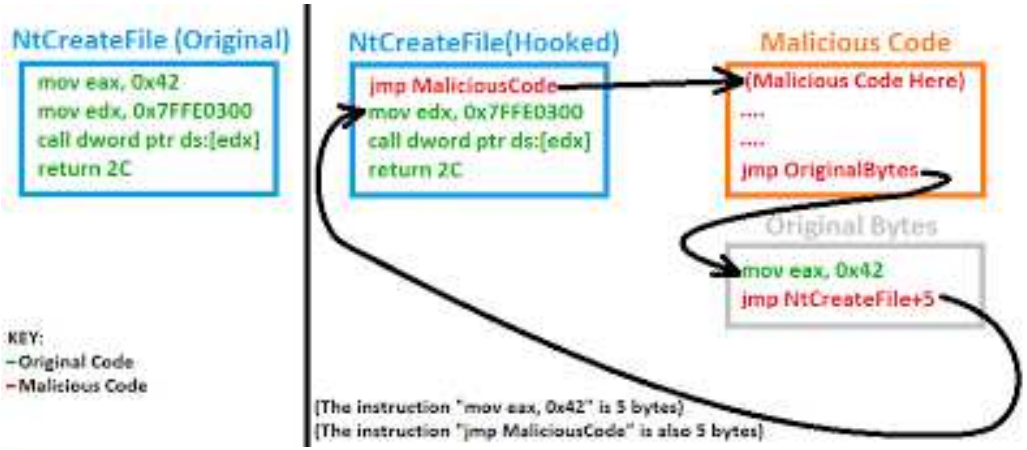
LES MALWARES

Les packageurs

- Les packageurs (Packers) permettent de compresser et de chiffrer un binaire. Le nouveau binaire généré est capable de s'auto-décompresser et déchiffrer lors de l'exécution
- En plus de complexifier l'étude du malware, cette technique rend l'analyse des binaires par les antivirus presque impossible
- Les antivirus détectent et alertent sur la présence d'un packageur dans un binaire mais pas du malware packagé

Le Hooking

- La technique de hooking permet de modifier un appel système afin que du code soit exécuté avant l'appel système
- Légitimement , les antivirus réalisent le Hooking pour analyser les fichiers lors de leurs accès
- Les malwares utilisent cette technique pour bloquer l'accès ou cacher des fichiers ou des processus



LES MALWARES
Canal Caché

- Le canal caché est un canal de communication qui permet la fuite d'informations sans être vu et en passant à travers les protections (firewall, proxy, …)
- Une résolution DNS peut permettre d'exfiltrer quelques octets, sur plusieurs mois cela peut faire des Gigabits
- Les ruptures de protocole permettent de bloquer les canaux cachés
- D'autre canaux cachés non réseau existent : Utilisation du courant électrique (consommation), du haut parleur sur une fréquence inaudible, d'une image JPG, …
- Un canal caché perfectionné est très difficile à détecter surtout si l'attaquant est patient

LES MALWARES
Usurpation d'identités

- Un attaquant n'a pas obligatoirement besoin d'augmenter ses privilèges pour nuire, les identifiants et les données de l'utilisateur suffisent
- Eléments récupérable :
  - Cookies du navigateur (réutilisation possible sans auth.)
  - Mots de passe enregistrés dans le navigateur
  - Identifiants d'applications (Gtalk, Skype, Steam, DropBox, client de mail, VPN, …)
  - Clés privés de l'utilisateur (SSH, GPG)
  - Codes Wifi, identifiants de partages réseau
  - Mails ou données utilisateur sensibles (avis d'impots, scan de passeport, numéro de sécurité sociale)

LES MALWARES

Les antivirus

- Un antivirus détecte des malwares sur la base de la signature de binaire et non sur des techniques d'attaque
- Dépendant de la base de signature de l'éditeur
- Joue au chat et à la souris avec les développeurs de malware
- Un antivirus installe un driver afin d'être au niveau noyau pour analyser les accès disques du système. Ce driver peut avoir des bugs et donc apporter des failles, rendre instable Windows et surtout ralentir le système
- L'AV est malheureusement indispensable mais ne permet de se protéger que les malwares connus

LES MALWARES
Les HIDS

- Un HIDS (Host Intrusion Detection System) est un système qui va analyser l'activité de la machine, de l'utilisateur
- Eléments surveillés :
  - Processus, ressources réseau consommées
  - Commandes utilisés, horaire, changement de privilèges
  - Structures interne aux noyaux, modification de la base de registre, table d'adressage des interruptions
  - Périphériques utilisés (USB)
  - Logs du système
- Souvent en complément d'un AV mais difficile à déployer car il faut le configurer en fonction de chaque système

LES MALWARES

Ce qu'il faut retenir

- Aucun malware ou programme n'est inoffensif, il peut cacher ou déployer d'autres malwares
- Un malware peut avoir de graves conséquences (vol de CB, vol de brevets, destructions, …)
- L'humain est un des principal maillon faible, il faut le former, le reformer et le reformer
- Il faut mettre à jour, protéger et surtout surveiller son infrastructure et ses postes
- Ne pas négliger les sauvegardes (Bannir le disque USB)
- Les malwares rapportent énormément à la Mafia