Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

CODE MALVEILLANT– REFLEXES

QU'EST-CE QU'UN CODE MALVEILLANT ?

Programme malveillant (malware en anglais) qui exécute des actions sans le consentement de l'utilisateur

OBJECTIFS DE L'ATTAQUE

- Dérober des informations confidentielles, financières
- Utiliser le système infecté comme vecteur d'attaque
- Générer un revenu (affichage de pub, demande de rançon)
- Espionnage, prise de contrôle à distance

RISQUES

➔ **PERTE ET VOL DE DONNEES**
➔ **ESPIONNAGE**
➔ **INDISPONIBILITE OU NEUTRALISATION DU SYSTEME**

SYMPTOMES

- **BUGS INATTENDUS**
- **SYSTEME LENT**
- **DISQUE DUR ANORMALEMENT ACTIF**
- **ETRANGES FENETRES / AVERTISSEMENTS**
- **DESACTIVATION DES LOGICIELS DE SECURITE**
- **ADRESSES IP BLACKLISTEES**
- **COURRIELS SUSPECTS ENVOYES DEPUIS LE SYSTEME**

VECTEURS D'ATTAQUES

- Courriel avec une pièce jointe
- Connexion directe d'un équipement infecté (clé USB, disque dur, téléphone)
- Navigation sur un site web infecté (exploits pack)
- Infection par le réseau
- Fausse mise à jour, fausse application
- Utilitaire « pirate » permettant une utilisation illicite d'une application payante (crack ou keygen), fichier téléchargé
- Exploitation d'une vulnérabilité

QUOI FAIRE

- **DECONNECTER LE POSTE (NE PAS L'ETEINDRE)**
- **AVERTIR LE REPONSABLE SECURITE**
- **AVERTIR LES TECHNICIENS**
- **DEPOSER PLAINTE AUPRES DE LA POLICE OU DE LA GENDARMERIE**

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

asipsanté
AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

CODE MALVEILLANT– REFLEXES

GRAVE OU PAS ?

Selon ses caractéristiques et ses fonctionnalités, un malware peut indiquer une intrusion présente depuis plusieurs mois. Une enquête est nécessaire afin de déterminer l'étendue des potentiels dégâts.

LES BONNES PRATIQUES

UTILISATEUR

- Ne pas ouvrir les fichiers suspects
- Ne pas utiliser le compte administrateur pour les tâches courantes
- Chiffrer ses données importantes
- Sauvegarder régulièrement ses données

SERVICE INFORMATIQUE

- Mettre en place une sauvegarde automatique
- Prévoir une station hors réseau de l'organisation pour l'analyse de malwares
- Installer les correctifs de sécurité du système et des logiciels tiers
- Avoir correctement configuré les logiciels de sécurité (antivirus, firewall, hips)
- Faire un clone /master du poste de travail
- Utiliser un système de sandbox pour ouvrir des fichiers suspects
- En cas de doute, scanner le fichier suspect avec plusieurs moteurs anti-virus (ex : Virustotal)
- Utiliser un système d'analyse de malwares automatisé (ex : Cuckoo)

REPARER ET ENQUETER

ATTENTION CERTAINS MALWARES PEUVENT ETRE COMPLEXES A DETECTER ET A ANALYSER. L'ANALYSE PEUT NECESSITER DES COMPETENCES SPECIFIQUES.

LES PRINCIPALES ETAPES DE L'ENQUETE •

- **Déconnecter le poste infecté du réseau**
- **Acquérir les données suivantes :**
    - Faire une copie de la mémoire vive
    - Faire une copie physique / snapshot du disque
    - Réaliser une copie de l'image et calculer l'empreinte de l'image réalisée
    - Faire une capture des traces réseaux
    - Récupérer les journaux d'évènements sur les équipements traversés
- **Une fois les données acquises, il est possible de réinitialiser le système :**
    - formatage bas niveau, flash du/des firmware(s)
    - réinstallation du système et applications à partir de sources réputées comme fiables
    - Tentative de réparation des fichiers infectés
- **Monter l'image réalisée sur une station d'analyse dédiée**
- **Analyser l'image avec plusieurs moteurs-antivirus. Faire une copie des fichiers infectés.**
- **En cas de détection de fichiers infectés :**
    - Faire une copie des fichiers infectés
    - Réaliser une analyse dynamique. Attention le malware peut être programmé pour détecter et fausser une analyse dynamique)
    - Réaliser une analyse statique (désassemblage). Attention ceci nécessite des compétences pointues et spécifiques

RESSOURCES

- Analyser la sécurité d'un poste Windows : MBSA
- Analyser un fichier / url avec plusieurs moteurs anti-virus : Virustotal
- Réaliser une analyse dynamique d'un fichier : Malwr, Malware-analyzer
- Déposer plainte : CERT-FR