

## Virus et malwares sous Windows

### Objectif :

Au fil des années la pollution des ordinateurs par des virus ou des malwares est devenue un fait incontournable et un risque toujours présent tant chez le particulier qu'en entreprise. Cette formation antivirus et malware cherche à vous faire comprendre leurs mécanismes d'actions et les différentes façons de se protéger ou de les éradiquer sans choisir un outil particulier. On retrouvera une forte analogie avec le monde médical (symptômes, analyses, diagnostics, traitements, culture biologique) qui vous permettra d'assimiler clairement les concepts et manipulations techniques effectuées. Vous serez à même de réparer rapidement un poste sans tout réinstaller comme on le fait trop souvent en première solution.

A la fin de cette formation, vous saurez :

- Créer un script permettant de vérifier la présence de malwares
- Eviter le formatage en cas d'infection
- Identifier et neutraliser les malwares
- Rechercher la source d'une infection
- Distinguer une infection d'un dysfonctionnement
- Ordonner et optimiser l'éradication d'une infection virale
- Sensibiliser les utilisateurs face au social engineering
- Elaborer un schéma de protection en adéquation avec les besoins de l'entreprise

### Participants :

Technicien de maintenance, administrateur réseaux et systèmes, responsable informatique, ou particulier souhaitant maîtriser le comportement et l'éradication des virus et malwares.

### Pré-requis :

Bien connaître l'utilisation du poste de travail sous Windows et les bases de la configuration du réseau.

**Durée : 3 jours (21 heures)    Référence : MVMW**

### Contenu de la formation :

#### Vocabulaire et concepts

##### *Les infections virales*

Analogie avec les virus biologiques

Démystifier les virus sans les sous-estimer

Comment classer les menaces : virus, vers, cheval de Troie, rootkit, backdoor?

Principes généraux de fonctionnement des menaces par « famille »  
Les vecteurs d'infection (media, réseau, poste itinérant, Web, ?)  
Désactivation et contournement des sécurités  
Le social engineering  
Botnet et ordinateurs zombies (fonctionnement et raison d'être)  
Le Cross Scripting et les dangers du Web

#### **TRAVAUX PRATIQUES**

*Infection de fichier et visualisation des symptômes en hexadécimal*  
*Réalisation d'un cheval de Troie*  
*Utilisation d'un backdoor et déstabilisation du firewall*  
*Manipulation d'un rootkit*  
*Installation de Spyware et visualisation de phishing*

#### **Les chiffres des infections**

Un ordinateur sur quatre est infecté dans le monde  
SPAM le cœur d'un business lucratif  
Connaître les risques logistiques pour l'entreprise  
Evolution des menaces

### **Panorama des technologies de protections**

#### **Les anti-virus**

Virus et anti-virus, le jeu du chat et de la souris  
Différence de détection : « Virus in the wild » et « virus Zoo »  
Détection séquentielle, générique, heuristiques, comportementale, bac à sable?  
Packer : le talon d'Achille des antivirus  
Les faux positifs  
Les anti-virus en ligne sont-ils efficaces ?

#### **TRAVAUX PRATIQUES**

*Utilisation d'un bac à sable avec un spyware*  
*Mise en difficulté des détections antivirus*  
*Blocage d'anti-virus en ligne*

#### **Les firewalls**

Concepts des connexions réseaux  
Le rôle du firewall dans la détection  
Les limites du firewall logiciel ou matériel  
Le problème de l'injection des applications tierces  
Les applications sensibles (IE, mails, P2P, ?)

#### **TRAVAUX PRATIQUES**

*Contournement d'un firewall*

### **Problème viral, logiciel ou matériel ?**

#### **Fonctionnement d'un programme**

Programme et DLL  
Les injections virales

## TRAVAUX PRATIQUES

*Injection virale et conséquences*

### **Fonctionnement « normal » de windows**

Démarrage du système (boot, noyau, bureau, services,?)  
Tour d'horizon des principaux services (svchost, explorer, winlogon, ?)  
Les signes d'une infection  
Les outils pour identifier un processus « anormal »

## TRAVAUX PRATIQUES

*Méthodologie d'utilisation d'outils spécialisés  
Recherche d'un malware maître et désactivation*

## Mode d'activation des codes malicieux

### **Principes d'activation au démarrage**

Réactivation du virus à chaque démarrage  
Liste des fichiers sensibles  
Base de registre et les clés du paradis viral  
La limite du mode sans échec  
Les failles de compatibilité ascendante Windows  
Multiplication des entrées, question de survie

## TRAVAUX PRATIQUES

*Tester et comprendre les entrées sensibles de Windows*

## Désactivation manuelle des codes malicieux

### **L'intervention humaine au secours des antivirus**

Méthodologie de vérification et outils à utiliser  
Liste des fichiers système à vérifier  
Les entrées favorites des virus dans la base de registres  
Les outils complémentaires à la détection

## TRAVAUX PRATIQUES

*Création d'un script de vérification  
Méthodologie de lecture du rapport de script*

### **Suppression des malwares**

Identifier « l'infection mère »  
Neutraliser les processus malveillants maîtres  
Eradiquer « l'éternel retour »  
Prise en compte d'effets combinés sur de multiples infections  
Supprimer les résiduels inactifs  
Peux-t-il être trop tard ?

## TRAVAUX PRATIQUES

*Utilisation du script face aux infections  
Interprétation des résultats du rapport de script  
Méthodologie d'identification les sources d'infection*

## **Sécuriser son entreprise**

### ***Le facteur humain***

- Les informations à diffuser aux utilisateurs
- Les erreurs à ne pas commettre lors des sauvegardes
- Exemple de contamination liée à une connexion administrateur
- Les protocoles de vérification à mettre en place

### ***Les outils***

- Choisir ses systèmes de sécurité
- Faire le tri dans les solutions proposées (payantes et gratuites)
- Positionnement des sécurités dans le réseau
- Outils de tests de sécurité

### ***Le déploiement des solutions***

- Contrôler les applications installées sur les machines utilisateurs
- Déployer des solutions cohérentes
- Contrôler les postes itinérants
- Les solutions de type « Proxy »
- Les solutions de type « Appliance »

### **TRAVAUX PRATIQUES**

*Mise en place d'un schéma idéal pour son entreprise*