

## FORMATION VIRUS ET MALWARES



### **Public :**

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**

### **Travaux pratiques :**

Les exercices et les démonstrations de ce cours permettent aux participants de manipuler des malwares et ainsi d'étudier leur comportement. Ces infections en milieu contrôlé ont pour vocation d'apprendre à effectuer des désinfections ciblées sans passer par le formatage et les méthodes de scan classiques qui s'avèrent longues et fastidieuses. La création d'un script de vérification permet à chacun d'appréhender concrètement les zones où les malwares ont l'habitude de se dissimuler.

## ■ Vocabulaire et concepts

Les infections virales

Démystifier les virus sans les sous-estimer

Pourquoi classer les menaces : virus, ver, cheval de Troie, rootkit, backdoor...

Principes généraux de fonctionnement des menaces par famille

Le social engineering et les techniques employées

Botnet et ordinateurs zombies (fonctionnement et raison d'être)

Le Cross Scripting et les dangers du Web

Les vecteurs d'infection (media, réseau, poste itinérant, Web, ...)

Désactivation et contournement des sécurités

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

## ■ Les tendances actuelles des infections

Pourquoi autant d'infections furtives

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

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,

Technologie du Bac à sable

PACKER et MUTEX le talon d'Achille des antivirus

Les faux positifs

Les limites des scan anti-virus classiques

- TP : Utilisation d'un bac à sable avec un spyware
- TP : Mise en difficulté des détections antivirus
- TP : Blocage 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, ...)

- TP : Contournement des firewalls logiciels par les malwares
- TP : Contournement des firewalls réseaux par les malwares

## ■ Problème viral, logiciel ou matériel ?

Fonctionnement d'un programme  
Programme et DLL  
Les injections virales

- TP : 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 »

- TP : Méthodologie d'utilisation d'outils spécialisés
- TP : Infection réelle d'ordinateur
- TP : Observation de la propagation de plusieurs malwares

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

- TP : Tester 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

- TP : Création d'un script de vérification
- TP : Méthodologie de lecture du rapport de script

## ■ Suppression ciblée 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 ?

- TP : Utilisation du script face aux infections
- TP : Interprétation des résultats du rapport de script
- TP : Méthodologie d'identification des d'infections
- TP : Désinfection ciblée sans formatage de plusieurs familles : trojan, virus, rootkit, spywares, etc...

## ■ Sécuriser son entreprise

Le facteur humain

Les informations à diffuser aux utilisateurs

Les paramétrages des postes itinérants

Exemple de contamination liée à une connexion administrateur

Les protocoles de vérification à mettre en place

Choisir ses systèmes de sécurité

Positionnement des sécurités dans le réseau

Contrôler les applications installées sur les ordinateurs en interne

Contrôler les postes itinérants

Les solutions de type « Proxy anti-virus »

Les solutions de type « Appliance anti-virus »

- TP : Installation de Proxy sécurisé
- TP : Utilisation de HIPS
- TP : Paramétrage optimum des anti-virus
- TP : Mise en place d'un schéma idéal pour son entreprise

Formation Virus et Malwares - PEGASE SECURE  
copyright © 2007 - 2012

<http://n284289.copyrightfrance.com>

<http://www.pegase-secure.com> - [formation@pegase-secure.com](mailto:formation@pegase-secure.com)

**PEGASE SECURE**

Entreprise française. Siret : 508 497 34400012