Formation Virus et malwares sous Windows

La pollution des ordinateurs par des virus ou des malwares est un risque extrêmement présent tant chez le particulier qu'en entreprise. Cette formation vise à vous expliquer leurs mécanismes d'actions et les différentes façons de s'en protéger ou de les éradiquer sans choisir un outil particulier. Une forte analogie avec le monde médical (symptômes, analyses, diagnostics, traitements, culture biologique) vous permettra d'assimiler facilement les concepts et manipulations techniques effectuées

Objectifs

- Savoir créer un script permettant de vérifier la présence de malwares
- Apprendre à identifier et neutraliser les malwares
- Savoir rechercher la source d'une infection
- Être en mesure de distinguer une infection d'un dysfonctionnement
- Comprendre comment ordonner et optimiser l'éradication d'une infection virale
- Pouvoir sensibiliser les utilisateurs face au social engineering
- Apprendre à élaborer un schéma de protection en adéquation avec les besoins de l'entreprise

Public concerné

- Technicien de maintenance, administrateur réseaux et systèmes ou responsable informatique 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

Une formation de 3 jours

Caractéristiques
Tarif : 1535 € HT par personne
Numéro de formateur : 11753687675
Nombre d'heures : 21
Référence : SR229
Contact : Patrick LE GOFF
Telephone : 01.76.60.66.10
Email : contact@kaptive.com

Paris
21/02/2011
16/05/2011
12/09/2011
19/12/2011

Description des modules

num	Module
1	**1ère partie : vocabulaire et concepts**
2	**Les infections virales**
Détails	- Analogie avec les virus biologiques - Démystifier les virus sans les sous-estimer - Comment classifier 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
3	**Les chiffes des infections**
Détails	- Un ordinateur sur quatre est infecté dans le monde - SPAM le coeur d'un business lucratif - Connaître les risques logistiques pour l'entreprise - Évolution des menaces
4	**2ème partie : panorama des technologies de protections**
5	**Les anti-virus**
Détails	- 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 ?
6	**Les firewalls**
Détails	- 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, ...)
7	**3ème partie : problème viral, logiciel ou matériel ?**
8	**Fonctionnement d'un programme**
Détails	- Programme et DLL - Les injections virales
9	**Fonctionnement "normal" de Windows**
Détails	- 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"
10	**4ème partie : mode d'activation des codes malicieux**

11 Principes d'activation au démarrage

Détails
- 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

12 5ème partie : désactivation manuelle des codes malicieux

13 L'intervention humaine au secours des antivirus

Détails
- 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

14 Suppression des malwares

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

15 6ème partie : Sécuriser son entreprise

16 Le facteur humain

Détails
- 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

17 Les outils

Détails
- 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

18 Le déploiement des solutions

Détails
- 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"