Virus et Malwares sous Windows

Lien : https://innov-systems.com/formation/virus-et-malwares-sous-windows

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC185

CATÉGORIE
Sécurité Wifi/IOT et Malware

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Etre capable d'identifier et neutraliser les malwares ou virus
- Savoir rechercher la source d'une infection
- Être en mesure de distinguer une infection d'un dysfonctionnement
- Pouvoir sensibiliser les utilisateurs face au social engineering
- Apprendre à élaborer un schéma de protection en adéquation avec les besoins de l'entreprise

POUR QUI ?

- Techniciens
- Administrateurs système ou réseau

Innov Systems

Programme détaillé

1 / Les concepts de base

- Les infections virales : notion
- Qu'entend-on par infections virales ?
- Notions virus
- Démystifier les virus sans les sous-estimer
- La jungle des noms (backdoor, vers, cheval de Troie, bot/botnet...)
- Classification des menaces : virus, vers, cheval de Troie, rootkit, backdoor...
- Principes généraux de fonctionnement des menaces par « famille »
- Les vecteurs d'infection les plus répandus
- 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

2 / Les chiffes des infections

- 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

3 / Se protéger : L'antivirus et le par-feu

- L'anti-virus
- Virus et anti-virus : principes de fonctionnement
- Différence de détection : "Virus in the wild" et "virus Zoo"
- Les types de détection : séquentielle, générique, heuristiques, comportementale, bac à sable...
- Les Packers : UPX, FSG, Upack, Armadillo, Themida...

Innov Systems

- Les fausses alertes
- Les anti-virus en ligne sont-ils efficaces ?
- Le pare-feu
- Concepts des connexions réseaux
- Le rôle du firewall dans la détection
- Que peut-il détecter ?
- Ses limites
- Le problème de l'injection des applications tierces
- Les applications sensibles (IE, mails, P2P, ...)

4 / Les mécanismes d'infection

- Fonctionnement d'un programme
- Relation avec DLL
- Les injections de code
- Comment détecter une infection au démarrage ? Les bons outils
- 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 appropriés pour identifier un processus "anormal"
- Les infections et la base de registre

5 / Mode d'activation des codes malicieux

- 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

Inov Systems

6 / 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
- 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 ?

7 / Mieux vaut prévenir que guérir

- Sensibiliser les utilisateurs
- Les informations à diffuser aux utilisateurs
- Les sauvegardes et les points de restauration
- Exemple de contamination liée à une connexion administrateur
- Les procédures à mettre en place
- Les outils
- Choisir ses systèmes de sécurité
- Choisir les bons outils
- 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 »

Inov Systems

- Les solutions de type « Appliance »

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

12 au 15 Jan. 2027	Présentiel - Casablanca
09 au 12 Mars 2027	Présentiel - Casablanca
04 au 07 Mai 2027	Présentiel - Casablanca
29 Juin au 02 Juil. 2027	Présentiel - Casablanca
31 Août au 03 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems

Innov Systems — Tous droits réservés