



LOGICIELS MALVEILLANTS



Toundra



www.cases.lu

CASES - Cyberworld Awareness and Security Enhancement Services

SCÉNARIO

Vous recevez un e-mail de la part d'un gestionnaire d'une grande entreprise internationale. Il s'adresse à vous en particulier et vous parle d'une éventuelle collaboration. Vous connaissez la firme et vous vous sentez honoré. De ce fait, vous n'hésitez pas à ouvrir le PDF envoyé en pièce jointe. Deux semaines plus tard, vous n'avez reçu aucune nouvelle du CEO... Mais vous vous retrouvez dans le collimateur de votre service IT. Des données sensibles sur les serveurs internes ont été compromises à partir de votre ordinateur.

Comment cela a-t-il pu arriver?

Des individus et des entreprises entières sont quotidiennement victimes de logiciels malveillants.

Dans notre scénario, c'était un Cheval de Troie qui était caché dans le fichier PDF.

Il s'est discrètement installé sur l'ordinateur et a pris le contrôle du système afin d'avoir accès aux données sensibles.

Le courrier électronique ne provient donc pas du CEO d'une grande entreprise, mais de cybercriminels qui exploitent des faiblesses humaines ciblées.

Les logiciels malveillants appartiennent au top 3 des menaces informatiques contre les entreprises, avec le spam et le phishing.¹ Les virus, les vers et les chevaux de Troie contaminent des terminaux, des pages web et des réseaux entiers. Ils provoquent des pertes de données énormes.

Rappelez-vous qu'ils sont généralement envoyés par des liens redirigeant vers des sites malveillants, par des pièces jointes dans des e-mails ou par d'autres supports contaminés (clés USB, CD, et autres supports amovibles).

GAINS POUR L'ATTAQUANT

- Dommages causés à la victime dus à la destruction ou à la modification de données
- Accès à des données sensibles ou secrètes
- Avantages économiques

¹) Enquête Kaspersky, «Global Corporate IT Security Risks: 2013».

CONSÉQUENCES POUR LA VICTIME

- Pertes financières directes
- Perte de temps et coûts supplémentaires liés à la suppression des logiciels malveillants et l'amélioration des mesures de protection.
- Perturbation de la production
- Vol d'identité
- Perte de contrôle
- Atteinte à l'image, perte de crédibilité
- Implication involontaire dans des activités illégales
- Perte ou divulgation de données sensibles

LA VULNÉRABILITÉ EXPLOITÉE

Il faut souvent plusieurs jours au meilleur **programme antivirus** pour enregistrer un nouveau malware dans sa base de données. Les cybercriminels se servent de cette avance ! Souvent, ce n'est même pas nécessaire, car de nombreuses personnes utilisent un programme antivirus qui n'est pas mis à jour régulièrement ou bien n'en utilisent aucun!

De cette manière, les programmes malveillants peuvent s'introduire dans les ordinateurs ou les réseaux sans rencontrer d'obstacle.

Les cybercriminels utilisent également les **faiblesses techniques** des sites web (souvent mal entretenus) pour accéder au CMS (système de gestion de contenu). Résultat : des logiciels malveillants sont introduits dans le site et exploitent des vulnérabilités du navigateur des visiteurs pour se propager. Un site d'entreprise qui reçoit des milliers de visites chaque jour peut de cette façon propager involontairement des programmes malveillants.

Des annonces pop-up, des liens et des pièces jointes dans des e-mails peuvent être utilisés comme appât. La curiosité et l'orgueil sont des **faiblesses humaines** qui sont exploitées pour inciter les visiteurs à cliquer sur des liens aussi attractifs que dangereux.

Pour viser une personne spécifique individuellement, les cybercriminels utilisent généralement l'ingénierie sociale et le phishing.

Les virus sont généralement programmés de sorte qu'ils endommagent des données, les modifient ou même les suppriment. Pour se propager, ils utilisent des canaux de communication comme les réseaux d'entreprise, l'e-mail ou un support amovible. Les virus ont besoin de l'interaction humaine.

Les vers agissent comme des virus mais n'ont pas besoin d'une intervention humaine. Ils peuvent utiliser un « moteur » (automatisme) pour exécuter leur programme malveillant et se reproduire.

Les chevaux de Troie permettent à l'attaquant de s'ouvrir un accès permanent à la machine de la victime. Il existe une grande variété de chevaux de Troie. Certains ouvrent simplement un accès à des fichiers de la machine, d'autres permettent une véritable interaction avec la machine infectée depuis Internet ou un réseau local.

MESURES DE PROTECTION

- Informez vos collaborateurs sur les programmes malveillants et les autres menaces informatiques.
- Équipez tous les ordinateurs et les serveurs (quel que soit leur système d'exploitation) de programmes antivirus. Utilisez de préférence un antivirus différent pour les ordinateurs et pour les serveurs afin d'augmenter la probabilité de détecter les logiciels malveillants.
- Mettez régulièrement votre système de protection à jour (de préférence de manière automatique).
- N'installez aucun logiciel sans autorisation du responsable informatique.
- Ne démarrez pas de programme et n'ouvrez pas de fichier que vous avez reçu dans un e-mail inopiné, même si l'expéditeur est connu.
- Ne cliquez pas sur des liens dans les e-mails ou les réseaux sociaux, surtout s'ils sont inattendus voire suspects.
- Créez des copies de sauvegarde pour prévenir la perte définitive de vos données.

- Les filtres web peuvent empêcher les infections des ordinateurs en empêchant de visiter des sites web malicieux ou de mauvaise réputation.
- Tenez-vous au courant des failles de sécurité et des faiblesses dans les logiciels actuels. Utilisez les correctifs de sécurité (patches) proposés par les éditeurs pour corriger ces faiblesses.
- Chiffrez les données et les communications sensibles sur votre ordinateur. De cette manière, en cas d'infection, le risque de perte de confidentialité sera considérablement réduit.

SOS - QUE FAIRE SI ÇA ARRIVE ?

- La direction informatique doit être immédiatement informée.
- La machine infectée doit être isolée et retirée du réseau. Elle ne doit plus être utilisée tant qu'elle n'a pas été totalement désinfectée.
- La désinfection à l'aide d'un live CD antivirus est rapide et pratique. Mais elle n'est pas à cent pour cent efficace.
- Pour plus de certitude, il est recommandé d'effectuer une réinstallation complète de l'ordinateur.
- Essayez de déterminer exactement les dégâts et de restaurer les fichiers perdus si nécessaire.



Pour plus d'informations visitez :

cases.lu/infection

Plus de conseils en matière de sécurité de l'information :

www.cases.lu - help@cases.lu

