COMPRENDRE LES MENACES QUI PÈSENT SUR LES PME

La cyberguerre, l'hacktivisme (le cyberactivisme), les attaques par déni de service. Ces thèmes font régulièrement la une de l'actualité, et ne concernent que les multinationales et les gouvernements. Mais est-ce bien vrai ?

Lari Utriainen de F-Secure dresse un portrait des menaces pour les entreprises.

Le monde de la protection des données est complexe et en constante évolution. La plupart des entreprises ont déjà de multiples sujets à traiter, et ne peuvent se doter des connaissances d'un spécialiste en sécurité. Mais, après Stuxnet et Flame, de nombreuses entreprises nous ont contactés pour mieux comprendre le danger planant sur leur activité et leurs données.

Il n'existe pas un seul « type » de menace, mais une multitude

La principale difficulté pour les entreprises consiste à faire la différence entre les cas qui sont matière à grand reportage dans les médias de ceux qui représentent un réel danger pour les PME. Comment déterminer quelles sont les attaques les plus susceptibles d'affecter votre entreprise ?

LE RISQUE LE PLUS IMPORTANT POUR LES PME N'EST PAS LE FAIT D'UN « TYPE » DE MENACE EN PARTICULIER. C'EST CELUI DE LA MENACE OMNIPRÉSENTE ET EN CONSTANTE ÉVOLUTION QUE REPRÉSENTE LA CYBERCRIMINALITÉ.

F-Secure

Ce n'est pas quelque chose qui peut être simplement associé à des individus tels que des « virus » ou du « spam », et ce n'est certainement pas bien identifié dans les médias grand public. Les activités de la cybercriminalité sont extrêmement complexes, et chaque « menace » provient de différentes sources, mêlées à d' autres éléments. La cybercriminalité revêt de nombreuses formes, mais avec un objectif unique, très clair : dérober des données et de l'argent.

Ordinateurs zombies, humains dupés, et des failles que personne ne peut voir

Les cybercriminels fonctionnent selon un mode opératoire précis. Contrecarrés par des mesures de sécurité de plus en plus efficaces - antivirus, filtres anti-spam, protection de la navigation web, etc.... - les cybercriminels recherchent différentes façons d'accéder aux données. Les PME sont ainsi particulièrement vulnérables à certaines formes d'attaques, notamment les botnets (réseaux d'ordinateurs zombies), l'ingénierie sociale (escroquerie), et l'exploitation des vulnérabilités (attaques via des failles de sécurité inconnues).

Botnets : l'exploitation des ressources de votre entreprise par une autre « société »

Les **botnets** sont un problème « classique » pour les PME. Un bot est un ordinateur infecté pouvant être contrôlé à distance, et un botnet est un réseau entier de machines infectées - à la manière d'une armée de zombies contrôlée par un seul individu, et obéissant à son bon vouloir. Dans ce cas, les ressources légitimes d'une entreprise peuvent être accaparées,contrôlées, et utilisées à des fins malveillantes telles qu'envoyer du spam, dérober des données, et même attaquer d'autres sites. Cela peut prendre un certain temps avant que l'entreprise ne s'en aperçoive.

L'individu qui crée le botnet n'est généralement pas celui qui l'utilise - il peut gagner beaucoup d'argent en le vendant au plus offrant, ou même en le louant à l'heure voire à la semaine.

Les PME présentent un environnement idéal pour une utilisation des botnets : elles disposent d'un grand nombre de machines en réseau, et les employés ont tendance à ne pas les éteindre lorsqu'ils partent le soir.

« UN RÉSEAU D'ENTREPRISE DÉTOURNÉ REPRÉSENTE DES RESSOURCES ILLIMITÉES POUR LES CYBERCRIMINELS, » PRÉCISE SEAN SULLIVAN, SECURITY ADVISOR CHEZ F-SECURE LABS.

« C'est une situation dans laquelle les ressources d'une entreprise effectuent le travail des cybercriminels. »

Ingénierie sociale : nous sommes des êtres humains. Les cybercriminels ne le savent que trop.

Les progrès techniques en termes de sécurité ont conduit les cybercriminels à rechercher d'autres moyens de frapper ; quoi de mieux alors que de passer par l'utilisateur ? **L'ingénierie sociale** consiste à manipuler des individus pour qu'ils effectuent certaines actions ou fournissent des informations. En les incitant, par exemple, à installer un fichier, à communiquer leur mot de passe ou leur numéro de

carte bancaire. Les attaques étaient jusqu'à présent assez évidentes (vous souvenez-vous du prince nigérian qui avait besoin de votre numéro de compte bancaire ?), mais sont devenues de plus en plus créatives et sophistiquées, et sont souvent impossibles à distinguer des sources légitimes.

Les logiciels rançonneurs sont un vecteur d'attaque de plus en plus utilisé : un cybercriminel verrouille l'ordinateur d'un utilisateur, et exige un paiement pour le déverrouiller. Cela se fait généralement sous couvert d'un message provenant des autorités, affirmant que l'utilisateur doit payer une amende en raison de la possession de contenus illégaux. « Les utilisateurs doivent contacter leur support informatique », indique Sullivan, « mais ils ne veulent pas le faire, parce que le logiciel malveillant crée une situation embarrassante pour eux. »

Exploitation des vulnérabilités : même les sources dignes de confiance peuvent faire de gros dégâts

C'est probablement la méthode préférée des cybercriminels pour accéder à un ordinateur que **d'exploiter ses vulnérabilités**. Il s'agit tout simplement de trouver une faille de sécurité dans n'importe quel logiciel, puis de l'utiliser pour infecter la machine.

Les coupables? La plupart du temps, les anciens logiciels non patchés.

« VOS LOGICIELS SONT LA PORTE D'ENTRÉE DE VOTRE PC, » PRÉCISE SULLIVAN.

« Les logiciels qui ne sont plus à jour sont comme une porte grande ouverte à toutes sortes d'attaques, et même depuis des sources pourtant inoffensives. » Les bannières publicitaires, affichées notamment sur les sites auxquels la plupart des utilisateurs font confiance (exemple: les journaux), sont spécifiquement conçues pour exploiter des plugins tels que Java ou Flash. Ils recherchent tous les moyens possibles pour infecter la machine et installer des programmes malveillants qui dérobent des données, transforment la machine en bot, ou la verrouillent pour exiger une rançon.

À l'avenir, ce type d'attaque sera encore plus rapide

Sean Sullivan prévoit une accélération des attaques liées aux vulnérabilités, et particulièrement de ce qu'on appelle les exploitations « zero-day » pour lesquelles aucun correctif ni aucun patche n'existe à ce jour.

« Les failles seront exploitées si rapidement que les éditeurs de logiciels ne seront pas en mesure de suivre», et « l'ère des attaques zero-day ne fait que commencer. » Les tentatives d'exploitation des vulnérabilités représentent 58% du top 10 des détections du premier semestre 2013 ; 45% de ces attaques concernent Java. Il suffit qu'un utilisateur se rende sur un site web infecté, même avec les dernières versions d'IE7, IE8 ou IE9, pour que des cybercriminels prennent le contrôle de sa machine.

C'est un bon exemple d'une menace qui ne bénéficie pas d'une large couverture médiatique, restant principalement abordée par les blogs techniques. La plupart des entreprises n'en ont probablement jamais entendu parler. Dans de telles situations, la première précaution consiste à cesser d'utiliser le produit affecté jusqu'à ce qu'un correctif approprié soit publié.

La cyberguerre va-t-elle entraîner des dommages collatéraux ?

Comme mentionné précédemment, les attaques telles que celles menées par Flame font la une des actualités. Pour résumer, Flame ressemble à une arme de cyberguerre utilisée pour les attaques entre les gouvernements. Sous la forme que nous lui connaissons actuellement, Flame n'atteindra pas la plupart des utilisateurs moyens. Mais les techniques utilisées le feront certainement. Les programmeurs de Flame ont utilisé des méthodes avancées de ciblage des ordinateurs, puis ont fait croire au système d'exploitation que Microsoft avait créé les mises à jour.

À l'heure actuelle, la plupart des cybercriminels n'ont pas besoin d'être aussi inventifs. Mais dès qu'ils découvriront qu'ils peuvent obtenir un meilleur retour sur investissement ou défaire mieux que leur concurrents, ils commenceront à employer ces techniques.

Comme Sean Sullivan l'a indiqué, « La R&D d'aujourd'hui est l'application pratique de demain. » Le gros du travail ayant été fait, les méthodes utilisées par Flame seront sûrement reprises et adoptées par les syndicats du crime. Nous devons nous tenir prêts.

Soyez vigilant. Ne paniquez pas.

Qu'est-il important de savoir dans cet environnement en mutation rapide ?

Vérifiez naturellement que votre entreprise dispose d'une solide protection antivirus et anti-spam, d'une protection de la navigation web. Et ce, pour l'ensemble de son environnement, que ce soit pour les ordinateurs portables et les ordinateurs de bureau, mais aussi pour les serveurs et les mobiles.

Il est particulièrement important pour les PME d'utiliser les toutes dernières versions de tous ses logiciels, c'est-à-dire les systèmes d'exploitation, les plugins tels que Flash et Java, Microsoft Office et les navigateurs web utilisés, et pas seulement pour les logiciels de sécurité.

Enfin, rapprochez-vous d'un expert qui saura vous guider dans vos choix de protection et qui est au fait des dangers.

En bref, si tous les logiciels que vous utilisez sont à jour et que vos solutions de sécurité couvrent toutes les couches de votre entreprise, vous serez en mesure de consacrer votre temps et vos ressources aux priorités de votre entreprise.

À propos de l'auteur

Lari Utriainen est chef de produit chez F-Secure. Il est spécialisé dans l'adéquation des offres aux besoins en sécurité informatique des PME.

À propos de F-Secure

F-Secure est une entreprise internationale dont le siège social est situé à Helsinki en Finlande. Fondée en 1988, la société est pionnière dans le domaine de la sécurité. Représentée aujourd'hui dans plus de 100 pays, F-Secure dispose de 18 succursales et plus de la moitié de ses collaborateurs travaillent en dehors de la Finlande. Nous sommes un partenaire de confiance auprès de plus de 200 opérateurs, ainsi qu'un des leaders des solutions de sécurité pour entreprises dans le monde, grâce à un réseau étendu de partenaires revendeurs.