Comment la NSA déploie des logiciels malveillants

Nouvelles révélations, nouvelles précautions

Nous reprenons ici l'article récemment publié par KoS, il s'agit de la traduction française de l'article de l'Electronic Frontier Foundation : How The NSA Deploys Malware: An In-Depth Look at the New Revelations par : Sphinx, KoS, Scailyna, Paul, Framatophe et 2 auteurs anonymes

– – – – – –

Nous avons longtemps suspecté que la NSA, la plus grande agence d'espionnage du monde, était plutôt douée pour pénétrer les ordinateurs. Désormais, grâce à un article de Bruce Schneier, expert en sécurité qui travaille avec The Guardian sur les documents de Snowden, nous avons une vision bien plus détaillée de la manière dont la NSA utilise des failles pour infecter les ordinateurs d'utilisateurs ciblés.

La méthode utilisée par la NSA pour attaquer les gens avec des logiciels malveillants est largement utilisée par les criminels et les fraudeurs ainsi que par les agences de renseignement, il est donc important de comprendre et de se défendre contre cette menace pour éviter d'être victime de cette pléthore d'attaquants.

Comment fonctionnent les logiciels malveillants exactement ?

Déployer un logiciel malveillant via le Web nécessite généralement deux étapes. Premièrement, en tant qu'attaquant, vous devez attirer votre victime sur un site web que vous

contrôlez. Deuxièmement, vous devez installer un logiciel sur l'ordinateur de la victime pour prendre le contrôle de sa machine. Cette formule n'est pas universelle, mais c'est souvent ainsi que les attaques sont exécutées.

Pour mener à bien la première étape, qui consiste à amener un utilisateur à visiter un site sous le contrôle de l'attaquant, ce dernier peut envoyer à la victime un courriel avec un lien vers le site web concerné : c'est ce que l'on appelle une attaque par hameçonnage (*phishing*). La NSA aurait parfois eu recours à ce type d'attaque, mais nous savons à présent que cette étape était généralement accomplie via une méthode dite de « l'homme du milieu » (*man-in-the-middle*)[1]. La NSA contrôle un ensemble de serveurs dont le nom de code est « Quantum », situés sur les dorsales Internet et ces serveurs sont utilisés pour rediriger les cibles vers d'autres serveurs contrôlés par la NSA et chargés d'injecter le code malveillant.

Dans ce cas, si un utilisateur ciblé visite, par exemple, le site yahoo.com, son navigateur affichera la page d'accueil ordinaire de Yahoo! mais sera en réalité en communication avec un serveur contrôlé par la NSA. La version malveillante du site web de Yahoo! demandera au navigateur de l'utilisateur d'adresser une requête à un autre serveur contrôlé par la NSA et chargé de diffuser le code néfaste.

Quand un utilisateur ciblé visite un site web mal intentionné, quels moyens l'attaquant utilise-t-il pour infecter l'ordinateur de la victime ? Le moyen le plus direct est probablement d'amener l'utilisateur à télécharger et à exécuter un logiciel. Une publicité intelligemment conçue s'affichant dans une fenêtre pop-up peut convaincre un utilisateur de télécharger et d'installer le logiciel malveillant de l'attaquant.

Toutefois, cette méthode ne fonctionne pas toujours et repose sur une initiative de l'utilisateur visé, qui doit télécharger et installer le logiciel. Les attaquants peuvent choisir

plutôt d’exploiter des vulnérabilités du navigateur de la victime pour accéder à son ordinateur. Lorsqu’un navigateur charge une page d’un site, il exécute des tâches telles que l’analyse du texte envoyé par le serveur et il arrive souvent qu’il charge des greffons (plugins) tels que Flash pour l’exécution de code envoyé par le serveur, sans parler du code JavaScript que peut aussi lui envoyer le serveur. Or, les navigateurs, toujours plus complexes à mesure que le web s’enrichit en fonctionnalités, ne sont pas parfaits. Comme tous les logiciels, ils ont des bogues, et parfois ces bogues sont à la source de vulnérabilités exploitables par un attaquant pour prendre le contrôle d’un ordinateur sans que la victime ait autre chose à faire que visiter un site web particulier. En général, lorsque les éditeurs de navigateurs découvrent des vulnérabilités, ils les corrigent, mais un utilisateur utilise parfois une version périmée du navigateur, toujours exposée à une attaque connue publiquement. Il arrive aussi que des vulnérabilités soient uniquement connues de l’attaquant et non de l’éditeur du navigateur ; ce type de vulnérabilité est appelée *vulnérabilité zero-day*.

La NSA dispose d’un ensemble de serveurs sur l’internet public désignés sous le nom de code « FoxAcid », dont le but est de déployer du code malveillant. Une fois que des serveurs Quantum ont redirigé une cible vers une URL spécialement forgée et hébergée sur un serveur FoxAcid, un logiciel installé sur ce serveur se sert d’une boîte à outils d’exploitation de failles pour accéder à l’ordinateur de l’utilisateur. Cette boîte à outils couvre vraisemblablement des vulnérabilités connues, utilisables contre des logiciels périmés, et des vulnérabilités *zero-day*, en règle générale réservées à des cibles de haute valeur [2]. Nos sources indiquent que l’agence utilise ensuite ce code malveillant initial pour installer d’autres logiciels à le plus long terme.

Quand un attaquant réussit à infecter une victime avec du code

malveillant, il dispose d'ordinaire d'un accès complet à l'ordinateur de cette dernière : il peut enregistrer les saisies du clavier (qui peuvent révéler mots de passe et autres informations sensibles), mettre en route la webcam ou lire n'importe quelle donnée conservée sur cet ordinateur.

Que peuvent faire les utilisateurs pour se protéger ?

Nous espérons que ces révélations pousseront les éditeurs de navigateurs à agir, que ce soit pour renforcer leurs logiciels contre les failles de sécurité ou pour tenter de détecter et de bloquer les URL utilisées par les serveurs FoxAcid.

Entre-temps, les utilisateurs soucieux de leur sécurité s'efforceront de suivre des pratiques de nature à assurer leur sécurité en ligne. Gardez toujours vos logiciels à jour, en particulier les greffons des navigateurs tels que Flash, qui nécessitent des mises à jour manuelles. Assurez-vous de bien faire la différence entre les mises à jour légitimes et les avertissements sous forme de pop-ups qui se font passer pour des mises à jour. Ne cliquez jamais sur un lien suspect dans un courriel.

Les utilisateurs qui souhaitent aller un pas plus loin – selon nous, tout le monde devrait se sentir concerné –, utiliseront l'activation en un clic de greffons Flash ou Java de manière à ce que ces derniers ne soient exécutés sur une page web qu'à la condition que l'utilisateur l'approuve. Pour Chromium et Chrome, cette option est disponible dans Paramètres => Afficher les paramètres avancés => Confidentialité => Paramètres du contenu => Plug-ins.

La même chose peut être faite pour Firefox à l'aide d'une extension comme Click to Play per-element. Les greffons peuvent également être désactivés ou complètement désinstallés. Les utilisateurs devraient également utiliser un bloqueur de publicité afin d'empêcher les requêtes superflues

du navigateur destinées aux publicitaires et aux pisteurs du web. Ils devraient en outre utiliser l'extension HTTPS Everywhere afin d'utiliser le chiffrement des connexions associées à HTTPS sur le plus de sites possibles.

Si vous êtes un utilisateur prêt à supporter quelques désagréments au bénéfice d'une navigation plus sûre, regardez du côté de NotScripts (Chrome) ou de NoScript (Firefox), qui permettent de limiter l'exécution des scripts. Cela signifie qu'il vous sera nécessaire d'autoriser par un clic l'exécution des scripts un à un. JavaScript étant très répandu, attendez-vous à devoir cliquer très souvent. Les utilisateurs de Firefox peuvent s'orienter vers une autre extension utile, RequestPolicy, qui bloque le chargement par défaut des ressources tierces sur une page. Ici aussi, votre navigation ordinaire pourrait être perturbée car les ressources tierces sont très utilisées.

Enfin, pour les plus paranoïaques, HTTP Nowhere permettra de désactiver l'ensemble du trafic HTTP, avec pour conséquence que votre navigation sera entièrement chiffrée et, par la même occasion, limitée aux seuls sites offrant une connexion HTTPS.

Conclusion

Le système de la NSA pour déployer les logiciels malveillants n'a rien de particulièrement novateur, mais avoir un aperçu de la façon dont il opère devrait aider les utilisateurs et les éditeurs de logiciels et de navigateurs à mieux se défendre contre ces types d'attaques, et contribuer à une meilleure protection de tous contre les criminels, les agences de renseignement et une pléthore d'autres attaquants. C'est pourquoi nous jugeons vital que la NSA soit transparente quant à ses capacités et aux failles ordinaires de sécurité auxquelles nous sommes exposés – notre sécurité en ligne en dépend.

1. Le terme « homme du milieu » est parfois réservé aux attaques sur les connexions sécurisées par cryptographie, par exemple au moyen d’un certificat SSL frauduleux. Dans cet article, toutefois, on entend plus généralement toute attaque où l’attaquant s’interpose entre un site et la victime.
2. D’après l’article de The Guardian, « Les exploits les plus précieux sont réservés aux cibles les plus importantes ».