Chronique Renaud Bidou – Black Hat 2017 : une conférence qui tient ses promesses

La conférence Black Hat fête son 20e anniversaire cette année.

Elle doit son exceptionnelle longévité non seulement à l'excellente qualité (globalement, il est toujours possible de tomber sur une conférence dont on est en droit de se demander comment elle a bien pu passer le comité de sélection) de ses conférences mais également à l'engouement croissant des professionnels de l'informatique pour la sécurité.

Engouement qui n'est en rien lié à un phénomène de mode mais à une nécessité croissante, devenue vitale ces dernières années.

Entrée en matière avec un usage malicieux d'une technologie à la mode : le machine learning.

Mise en œuvre depuis des années dans les moteurs antispam et plus récemment dans la détection de malware, cette technologie peut également être exploitée pour identifier les cibles les plus pertinentes pour les « attaques au président » (BEC – Business Email Compromise). Ce modèle, construit sur la base des informations personnelles, des données disponibles sur Internet et les réseaux sociaux et de précédents résultats d'attaque, approche les 80 % de fiabilité, maximum admis pour ce type de modèle. Efficace.

Nous continuons avec les systèmes industriels et les attaques lancées contre les power grid d'Ukraine en 2015 et 2016, via le malware Industroyer. Si ce dernier ciblait les infrastructures ukrainiennes, il n'est qu'une implémentation du framework Crashoverride, développé par le groupe Electrum.

Ce framework cible les sous-stations, plates-formes de pilotage des systèmes industriels, et offre des fonctions de backdoor, déni de service, scan et effacement des configuration des systèmes pilotés. Déjà "compatible" avec les protocoles de communication IEC-101 (port série) et IEC-104 (TCP/IP) utilisés en Europe et au Moyen-Orient, certains développements sont en cours pour l'adapter aux protocoles en usage outre-Atlantique… Inquiétant.

Et comme chaque édition apporte son lot d'innovation, la 20e ne déroge pas à la règle avec la présentation de ce qui pourrait rapidement devenir un cauchemar pour la sécurité des SI. Un botnet dont le canal C&C serait le serveur Active Directory de l'entreprise.

Les filtrages, qu'ils soient périmétriques ou par micro-segmentation deviennent inutiles. Pire, l'implémentation ne repose pas sur une faille particulière, mais sur des composants standard du mécanisme : les attributs. En exploitant ces quelque 50 champs de données, il devient presque trivial de créer un canal de communication vers l'ensemble des systèmes compromis du réseau. Sans limite.

Mais Black Hat n'est pas uniquement affaire de hackers. Les auteurs de ShieldFS ont conçu un driver offrant au système de fichier de Windows une surprenante capacité de résistance aux

ransomware.

L'idée est simple, il s'agit d'effectuer une opération de copy-on-write lorsque qu'une activité suspecte est effectuée sur un fichier. La réelle richesse de ce driver, outre son intégration transparente dans l'OS, est l'utilisation d'un modèle comportemental recensant l'activité "normale" de plus de 2 000 applications sur le système de fichiers. Toute divergence est alors détectée et les fichiers protégés.

Mieux, ce modèle s'appuie sur des technologies de machine learning et est entraîné à différents intervalles de temps afin d'identifier qu'un processus précédemment considéré comme bénin a été compromis ou cible d'une injection. Malin.

Efficace, inquiétant, sans limites, malin. Simple résumé de quelques-unes des 60 conférences d'une première journée [celle du 26 juillet, ndlr] qui tient ses promesses.

Vivement demain [ce 27 juillet, donc].

Renaud Bidou est directeur technique Europe du Sud chez Trend Micro. Pour retrouver ses autres chroniques « Sécurité IT » sur ITespresso.fr, c'est par ici.