Sécurité et espionnage informatique \ Connaissance de la menace APT

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 février 2015

https://www.bortzmeyer.org/securite-et-espionnage-informatique.html

Auteur(s) : Cédric Pernet
ISBN n°978-2-212-13965-5
Éditeur : Eyrolles
Publié en 2015

Les médias sont plein de récits d'attaques informatiques spectaculaires, où deux lycéens piratent le Pentagone, par des méthodes techniques très avancées, ou bien où une horde de Chinois, forcément fourbes et cruels, s'emparent des plans du dernier avion de combat. Dans la communication sur les attaques informatiques, un sigle s'est imposé : APT pour "*Advanced Persistent Threat*". Peu de gens ont une idée précise de ce que cela veut dire mais c'est en général un synomyme de « attaque qui n'a **pas** été faite par un gusse dans son garage, un après-midi où il s'ennuyait ». Vous voulez en savoir plus ? Alors, je vous recommande le livre de Cédric Pernet, un expert de la question, et qui sait bien expliquer posément ce que sont les APT, dans leur complexité.

Le livre est court, 220 pages, ce qui le rend accessible aux gens curieux mais pressés (et le prix est élevé, à 40 €...) Mais il couvre bien tous les aspects d'une APT. L'auteur discute d'abord d'une définition rigoureuse de ce concept (on a vu plus haut que le terme est souvent utilisé à tort et à travers, en général avec une bonne dose de sensationnalisme). La définition de l'auteur (« une attaque informatique persistante ayant pour but une collecte d'informations sensibles d'une entreprise publique ou privée ciblée, par la compromission et le maintien de portes dérobées sur le système d'information ») ne fait **pas** appel au terme « avancé ». En effet, son analyse est que les APT ne sont pas forcément d'une haute technologie. Elles se caractérisent davantage par la mobilisation de moyens humains importants (des dizaines, voire des centaines de personnes), par la ténacité, par le professionnalisme et le souci du détail, que par la sophistication des techniques utilisées.

L'auteur expose ensuite les différentes phases d'une APT : la phase de reconnaissance, où le groupe d'attaquants rassemble toutes les informations possibles sur sa cible, celle de la compromission initiale, où l'attaquant a trouvé une faille à exploiter pour pénétrer dans le système, par exemple par du hameçonnage ciblé ("*spear phishing*"), une phase de « renforcement des accès et mouvements latéraux », où l'attaquant va mettre en place des moyens de revenir même si la faille originelle est comblée (rappelez-vous qu'une APT prend du temps), et où il va se déplacer dans le système d'information, à la recherche

de nouvelles machines à compromettre, et enfin une phase d'exfiltration des données, où l'attaquant va tenter de faire sortir tous les giga-octets qu'il a obtenu, afin de les rapporter chez lui, mais sans se faire détecter.

Vu du point de vue de l'attaquant, une APT n'est pas forcément "*glamour*" et spectaculaire. La phase de reconnaissance, par exemple, est plutôt routinière. C'est un travail de besogneux, pas de flamboyants "*hackers*". Des tas d'informations sont disponibles publiquement, il faut les récolter. L'auteur note que « une préparation rigoureuse et minutieuse est la clé de la réussite [de l'APT] », ce qui est aussi exaltant qu'une leçon de morale du temps de Jules Ferry (« c'est en travaillant bien qu'on réussit »).

(Au passage, Cédric Pernet parle longuement de l'utilisation de whois et du DNS. Ces outils sont utilisés par les agresseurs en phase de reconnaissance, mais peuvent aussi servir aux investigateurs, cf. mon exposé à CoRI&IN <http://www.cecyf.fr/wp-content/uploads/2014/06/CORIIN-2015-BORTZMEYER-I
pdf>.)

Même la phase de compromission initiale n'est pas forcément glorieuse. Lors d'une APT, on n'utilise pas forcément des attaques premier jour (attaques encore inconnues) : c'est parfois dans les vieux pots qu'on fait les meilleures soupes et certaines APT n'ont utilisé que des vulnérabilités connues depuis des années... et qui ne sont pas toujours patchées.

J'ai noté que, malgré le métier de l'auteur, ce livre ne parle guère de la « réponse à incidents ». Il décrit les APT, pour les solutions et les réactions, il faudra attendre un autre livre.

Le livre se termine par une description de plusieurs APT fameuses et moins fameuses. L'auteur, qui rappelle régulièrement la complexité de ce monde et la difficulté à acquérir des certitudes en béton sur les attaquants et leurs méthodes, se méfie des attributions trop enthousiastes. L'**attribution**, c'est un des exercices les plus difficiles de la lutte contre les APT, c'est tenter de nommer l'attaquant. Comme une attaque numérique ne laisse pas de traces indiscutables (pas d'ADN, pas de mégots de cigarettes, pas d'empreintes digitales), on pourra toujours contester une attribution. D'autant plus que certains n'hésitent pas à ouvrir le feu avant d'être sûr, par exemple lorsque le FBI a accusé le régime nord-coréen d'être derrière l'attaque de Sony <http://www.slate.fr/story/95443/hack-sony-absurde>.

Donc, quelques cas pittoresques traités dans ce livre :

— PutterPanda <http://resources.crowdstrike.com/putterpanda/>, une campagne d'espionnage visant notamment l'aéronautique, et qui viendrait de Chine.
— Careto <http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf>, une campagne d'APT caractérisée par la richesse et la complexité des techniques utilisées (dont certaines achetées aux mercenaires de Vupen).
— Hangover <http://www.symantec.com/connect/blogs/operation-hangover-qa-attacks> qui serait d'origine indienne.
— Flame <http://securelist.com/blog/incidents/34344/> (alias Flamer, alias Wiper, rappelez-vous que les noms sont donnés par les défenseurs, pas par les attaquants, et que plusieurs équipes ont pu analyser la même APT), un système d'espionnage très perfectionné, qui a frappé au MOyen-Orient, et qui serait développé par la même équipe que Stuxnet (que Cédric Pernet ne classe pas dans les APT).

Une APT fameuse manque : celle que la NSA pratique en permanence contre les systèmes informatiques du monde entier...

Pour résumer, un excellent livre, très documenté, sérieux, prudent, et pédagogique, même si je regrette l'abus d'anglicismes (certes très utilisés dans le métier), comme "*0day*" au lieu de « premier jour »,

"*watering hole*" plutôt que « point d'eau », "*sinkhole*" au lieu d'« évier », "*logger*" au lieu de « journaliser », etc. L'auteur a récemment donné un interview à SécuritéOff <http://www.securiteoff.com/cedric-pernet-de-nombreuses-attaques-apt-ne-sont-pas-mediatisees/>.

Une note d'humour pour finir : le dos du livre annonce « Il [l'auteur] est suivi par plus de 3 000 abonnés sur Twitter. » Curieuse métrique : j'ai bien plus d'abonnés, sans pouvoir prétendre au même niveau d'expertise.

Autres compte-rendus de ce livre :

— Article détaillé de Nicolas Caproni <http://www.cyber-securite.fr/2015/02/12/lecture-pour-tout->,
— Un résumé très complet du livre par Bertrand Boyer <http://cybertactique.blogspot.fr/2014/12/lecture-securite-et-espionnage.html>.
— Un troll amusant <http://news0ft.blogspot.fr/2015/02/securite-et-espionnage-informatique.html> sur les condensats utilisés dans le livre.