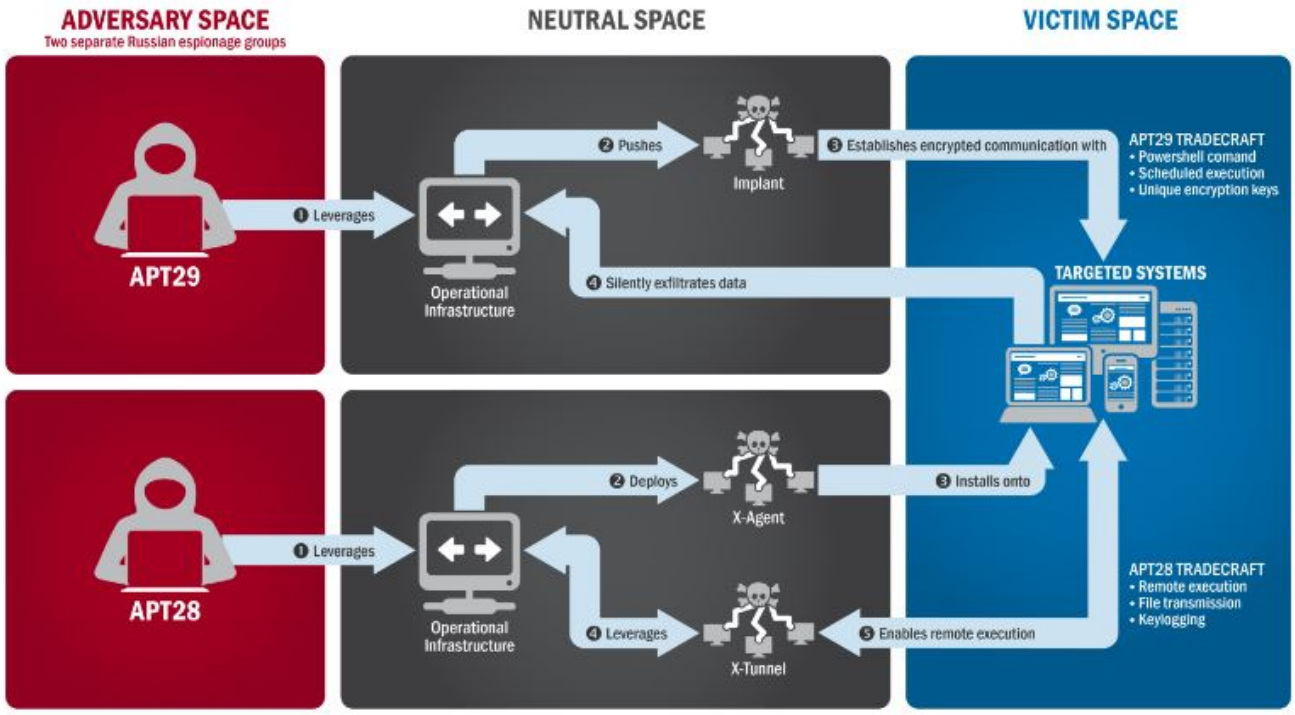
Piratage des élections U.S. : tout a commencé par du spearphishing

En parallèle des sanctions visant la Russie (avec l'expulsion de 35 diplomates russes annoncée par l'administration Obama en fin de semaine dernière), le FBI et le Department of Homeland Security (ou DHS, l'équivalent de notre ministère de l'Intérieur) ont dévoilé leur rapport officiel sur les opérations de hacking qui ont entouré la récente élection présidentielle aux Etats-Unis. Sans surprise, ce document, qui renferme des détails techniques sur les outils et techniques employées, pointe la responsabilité directe des services de renseignement civils et militaires russes dans cette opération, que les enquêteurs américains ont baptisée Grizzly Steppe.

Cette désignation sans ambiguïté d'un responsable – ou « attribution » en jargon- est inhabituelle dans le domaine cyber, comme le reconnaît d'ailleurs le rapport. Mais ce dernier souligne que ses certitudes s'appuient sur « *des indicateurs techniques* » relevés par la communauté du renseignement U.S., le Homeland Security, le FBI, des entreprises privées ainsi que « *d'autres entités* », non précisées.

APT28 + APT29

Selon le gouvernement, l'opération Grizzly Steppe est bien l'œuvre de deux groupes, tous deux impliqués dans le hacking du Parti démocrate. Le premier, APT29 (ou Cozy Bear, apparemment lié aux renseignements civils russes, le FSB), s'est immiscé dans les systèmes de cette organisation dès l'été 2015, tandis que le second, APT28 (ou Fancy Bear, probablement associé aux renseignements militaires russes, le GRU), l'y a rejoint au printemps 2016.



« *A l'été 2015, dans une campagne de spearphishing, APT29 a envoyé des e-mails contenant des liens malveillants à plus de 1 000 destinataires, dont de multiples victimes au sein du gouvernement U.S.*, écrivent

le FBI et le DHS. *APT29 utilisait des domaines légitimes, dont certains associés à des organisations américaines ou des institutions du monde de l'éducation, pour héberger des malwares et envoyer des e-mails infectieux ciblés. Au cours de cette campagne, APT29 est parvenu à compromettre un parti politique américain.* » Le rapport explique qu'au moins une des personnes ciblées a activé un lien renvoyant à un malware, conduisant à l'infection des systèmes du parti démocrate. Une fois dans la place, APT29 a pu s'installer durablement sur les systèmes en question, y gagner des privilèges élevés, répertorier les comptes Active Directory et enfin exfiltrer des e-mails via des connexions chiffrées.

Au printemps 2016, le même parti politique a été la cible d'une seconde campagne de spearphishing, orchestrée cette fois par APT28 selon le rapport officiel. Cette fois, les e-mails malveillants demandaient aux destinataires de modifier leur mot de passe sur un webmail… sauf qu'évidemment le lien proposé renvoyait vers un site contrôlé par les pirates, imitant un service légitime. « *En exploitant les crédences ainsi recueillies, APT28 a été en mesure de se ménager des accès et de dérober des données, conduisant probablement à l'exfiltration d'informations de plusieurs responsables du parti* », écrivent le DHS et le FBI. Rappelons que les Etats-Unis soupçonnent la Russie d'avoir transmis ces informations volées à Wikileaks afin de polluer la campagne démocrate. Le rapport du DHS et du FBI n'indique toutefois pas si les deux opérations étaient liées ou orchestrées, certains éléments déjà diffusés donnant à penser que APT28 a infecté le parti démocrate sans savoir que APT29 s'y était déjà introduit.

Hacking du réseau électrique ? Voire…

Selon le rapport, les campagnes de spearphishing de APT28 et APT29 étaient encore en cours en novembre 2016, quelques jours après l'élection. Le DHS et le FBI livrent une série d'indicateurs de compromission (IP, hash de fichiers, signature Yara) afin de faciliter le travail de détection des administrateurs systèmes. Les enquêteurs américains demandent notamment aux organisations de se montrer très vigilantes avec leurs sites Web publics. Selon eux, ces derniers constituent des cibles privilégiées par APT28 et APT29, qui y recherchent des vulnérabilités de type cross-site scripting (XSS) ou injection SQL.

Notons que la publication de ce rapport a entraîné un mini-mouvement de panique, un des indicateurs de compromission associés à l'opération Grizzly Steppe ayant été détecté chez un opérateur électrique du Vermont, Burlington Electric, faisant craindre une attaque russe contre une infrastructure vitale aux Etats-Unis. Sauf que le malware en question n'a été identifié que sur un PC portable de l'entreprise, machine qui n'était par ailleurs pas reliée aux installations électriques, a précisé par la suite Burlington Electric.

Trump toujours sceptique

Rappelons que si Barack Obama a endossé les conclusions de ses services de sécurité, pointant la responsabilité directe de Moscou dans le piratage du parti démocrate, son successeur Donald Trump a lui réitéré ses doutes. Le 31 décembre, il a expliqué que cette « *accusation plutôt sérieuse* » contre la Russie de Vladimir Poutine devait être étayée par des certitudes. Sous-entendant par-là, que les éléments produits jusqu'à présent ne lui suffisent pas. Donald Trump prendra officiellement ses fonctions à la Maison Blanche le 20 janvier.

A lire aussi :

Obama engage la cyberguerre froide contre la Russie

L'élection de Trump brouillée par le piratage

Les CEO américains ne sont pas préparés aux cyberattaques

Crédit photo : Ivelin Radkov / Shutterstock