Les cybercriminels s'emparent des outils de hacking de la NSA

Il fallait s'y attendre : selon un rapport de Recorded Future, une société américaine spécialisée dans l'intelligence sur les menaces, les communautés de pirates chinois et russes ont commencé à étudier les malwares dévoilés en avril par les Shadow Brokers. Rappelons que ce groupe de hackers, inconnu jusqu'alors, a commencé à faire parler de lui en août 2016 en dévoilant des outils de piratage apparemment dérobés à la NSA américaine. Il y a quelques jours, ces mêmes Shadow Brokers ont mis en ligne une nouvelle archive renfermant de nombreux outils, ciblant en particulier les systèmes Solaris et Windows. C'est cet ensemble que les communautés cybercriminelles russes et surtouts chinoise étudient dans l'espoir d'y trouver une souche récupérable pour lancer une attaque à grande échelle.

« *L'underground criminel a vu dans cette publication une importante opportunité de récupérer des exploits avant que l'application des patchs à grande échelle ne soit effective* », résume Levi Gundert, un des dirigeants de Recorded Future, dans les colonnes de *Dark Reading*. Et de comparer la publication des Shadow Brokers à un Noël avant l'heure pour les cybercriminels : « *on parle ici de techniques et outils très sophistiquées, généralement hors de portée de la communauté underground* », dit-il. Basée sur l'étude des forums du Dark Web, l'analyse de Recorded Future montre en particulier l'intérêt du cybercrime pour le framework d'exploits (nom de code FuzzBunch), le malware ciblant le protocole d'échange réseau SMB (EternalBlue) et l'outil d'élévation de privilèges (EternalRomance), tous issus de la dernière publication du mystérieux groupe de hackers et tous ciblant les environnements Windows.

Si Microsoft a déjà patché les vulnérabilités qu'exploitent ces outils – de façon surprenante dès mars 2017, soit un mois avant la divulgation des malwares par les Shadow Brokers -, les pirates chinois ne semblent pas totalement persuadés de la solidité de ces correctifs, selon Recorded Future. « *Beaucoup pensent que les failles sous-jacentes exploitées par ces kits d'outils n'ont pas été totalement comblées par les patchs* », écrit la société dans un billet de blog.

DoublePulsar parti pour durer

Sur les forums russes, la publication des Shadow Brokers a également suscité l'intérêt. Trois jours après la fuite, « *un membre très respecté d'une communauté en vue du Dark Web fournissait un tutoriel détaillé pour transformer en arme l'exploit EternalBlue, ainsi que la charge utile DoublePulsar, ciblant le noyau Windows* », ajoute la société.

Ces signes d'intérêt, combinés au réel savoir-faire des criminels pour transformer en campagne infectieuse à grande échelle une faille zero day, constituent autant de signaux d'alerte pour les RSSI. Les experts pensent même que DoublePulsar devrait s'enkyster dans les systèmes d'information pour plusieurs années. Un peu comme l'a fait le ver Conficker, que les audits de sécurité continuent à déceler. Les exploits EternalBlue, EternalChampion, EternalSynergy et EternalRomance, dévoilés par les Shadow Brokers et faisant partie du kit FuzzBunch, chargent tous DoublePulsar sur les systèmes compromis. Cette charge utile, qui se loge en mémoire, permet à un

assaillant d'exécuter le shellcode de son choix sur le système Windows détourné et de charger d'autres malwares (comme des ransomwares, des botnets). Ce qui rend la frontière entre hacking d'Etat et cybercrime très poreuse.

« *Un bain de sang* »

L'outillage *made in* NSA exploite les failles du serveur SMB de Windows et Windows Server, via des requêtes mal formées (sur le port 445, celui où fonctionne normalement le service SMB). Des failles que Microsoft a patchées – avec espérons-le suffisamment d'efficacité – lors de la publication de son bulletin de sécurité critique MS17-010, du 14 mars. « *La dernière vulnérabilité de ce type était MS08-67 (soit celle qu'exploite Conficker, NDLR) qu'on continue à rencontrer dans nombre d'endroits* », remarque Sean Dillon, un analyste de RiskSense, chez nos confrères de *ThreatPost*. Un scan effectué par la société Phobos tend à montrer que 3,1 % des machines encore vulnérables aux failles SMB sont déjà infectées (soit entre 62 000 et 65 000 systèmes). « *Un bain de sang* », selon son Pdg Dan Tentler.

« *Cela montre que ces outils sont vraiment très bien développés, très dangereux et ne demandent pas un énorme niveau de sophistication technique, ce qui fait que les assaillants les adoptent rapidement dans leurs catalogues et kits d'outils. Et ils réutilisent ces outils tel quel* », note Matthew Hickey, le fondateur du cabinet de conseil Hacker House.

A lire aussi :

Shadow Brokers : et maintenant des exploits visant Swift !

Shadow Brokers : des outils de hack pour Solaris dans la nature

Les Shadow Brokers publient les outils de hacking de serveurs de la NSA