L’effaceur de disques durs StoneDrill s’intéresse à l’Europe

Les chercheurs de l’équipe GReAT (Global Research & Analysis) de Kaspesky Lab viennent de mettre la main sur un nouveau malware : StoneDrill. A l’instar du précédent Shamoon (ou Disttrack), StoneDrill ambitionne de détruire toutes les données des disques durs des machines qu’il infecte.

Difficile à détecter

Le mode de propagation de cet « effaceur » (wiper) reste inconnu des équipes de l’éditeur de sécurité russe. Mais son mode opératoire ne manque pas d’ingéniosité. Dès qu’il est installé sur la machine attaquée, le malware s’implante dans la mémoire du navigateur par défaut de l’utilisateur. Ce qui complique sa détection d’autant que, lors de cette opération, il utilise des techniques anti-détection visant à leurrer les antivirus. Une fois bien en place, StoneDrill déclenche alors son processus de destruction des fichiers du disque, que les médias soient physiques ou logiques (partitions), en réécrivant les données à l’aide de nombre aléatoires. Ce qui rend la récupération des données quasi impossible.

Ce n’est pas tout. Les chercheurs ont également découvert la présence d’une backdoor. Laquelle a visiblement pour but de permettre aux attaquants l’espionnage de l’activité de leurs victimes. Pas moins de quatre panneaux de commandes et contrôle (CC) ont ainsi été détectés.

Une version aboutie de plusieurs wiper

StoneDrill apparaît comme une version évoluée, si ce n’est aboutie, de plusieurs wiper. Dont Shamoon, qui semble avoir inspiré les développeurs de StoneDrill par son style de programmation, rapporte Kaspersky. Mais aussi de la menace persistante (APT) NewsBeef (également connu sous Charming Kitten) active depuis plusieurs années en Arabie Saoudite et qui s’attaque au Browser Exploitation Framework (BeEF), un outil de test de pénétration dédié aux navigateurs.

« Nous avons été très intrigués par les similitudes et les comparaisons entre ces trois opérations malveillantes, déclare Mohamad Amin Hasbini, chercheur senior en sécurité chez Kaspersky Lab. *StoneDrill était-il un autre avatar de l'effaceur Shamoon ? Ou bien StoneDrill et Shamoon sont-ils le fait de deux groupes différents et sans liens dont ils se trouvent qu'ils ont ciblé des entreprises saoudiennes au même moment ? Ou encore deux groupes distincts mais poursuivant les mêmes objectifs ? La dernière hypothèse est la plus probable. »* La présence de ressources linguistiques en arabe yéménite et de persan chez StoneDrill pourrait laisser penser à une extrapolation numérique du conflit irano-saoudien dans lequel le Yemen est impliqué par « procuration ».

StoneDrill arrive en Europe

« Mais, bien entendu, nous n'écartons pas la possibilité que ces éléments soient des fausses pistes », précise le chercheur. D'autant que, au-delà du Moyen-Orient, son terrain de jeu favori, StoneDrill a également été identifiée en Europe. Mais Kaspersky se garde d'en préciser la seule cible, constatée pour le moment, et le pays concerné.

Shamoon s'était illustré en 2012 en affectant quelque 35 000 ordinateurs d'une compagnie pétrolière et gazière du Moyen-Orient. Ce qui avait fait peser un risque sur 10% de l'approvisionnement mondial en pétrole. Jusqu'alors relativement isolé, le malware a ressurgi en 2016 avec une version 2.0 plus évoluée, et une campagne de propagation plus large touchant 11 organisations. Des évolutions qui ont visiblement inspiré les concepteurs de StoneDrill. Si le malware a lancé ses premières attaques dès 2016, Kaspersky dit en ignorer les conséquences pour l'heure.

Lire également
Anatomie du malware super furtif, caché dans la mémoire des serveurs
Le malware bancaire Dridex devient hyper furtif, grâce au AtomBombing
Ransomware : les cybercriminels font maintenant la tournée des hôtels