Ransomware : Bad Rabbit avec des bouts de code de hacking de la NSA à l'intérieur

Les enquêtes sur le mode opératoire de Bad Rabbit, le ransomware qui a frappé l'Europe de l'Est en début de semaine, se poursuivent. Notamment sur son mode de propagation.

Si, initialement, les chercheurs en sécurité ont pensé que le malware se propageait de PC en PC par l'intermédiaire du protocole de partage de ressources SMB (Server Message Block) de Microsoft (en exploitant Mimikatz pour forcer les mots de passe réseau), Bad Rabbit aurait aussi utilisé un *exploit* de la NSA pour renforcer le processus de diffusion.

C'est du moins la thèse de Talos. Dans une mise à jour de son alerte, le bras armé de Cisco dans la cybersurveillance déclare avoir trouvé des traces de EternalRomance dans le code.

Cet outil a été développé, parmi d'autres, par l'agence américaine de renseignement pour exploiter les failles de SMB… avant de se les faire dérober par le mystérieux groupe de hackers Shadow Brokers.

Talos précise que les auteurs de Bad Rabbit n'ont pas implémenté EternelRomance tel quel et y ont apporté des modifications. Ce qui expliquerait pourquoi le nouveau rançongiciel n'a pas été détecté de manière précoce.

L'*exploit « est très similaire à l'implémentation Python accessible publiquement de l'exploit EternalRomance qui est également exploité par Nyetya (NotPetya, NDLR)*, souligne les chercheurs.

« *Cependant, l'implémentation [d'EternelRomance] dans Bad Rabbit est différente de celle de Nyetya, bien qu'elle soit encore largement basée sur l'exploit EternalRomance publié par les Shadow Brokers.* »

Troisième exploitation des outils de la NSA

Une analyse qu'a également confirmée F-Secure. *« Nous avons vérifié les mêmes observations que Cisco Talos Security sur EternalRomance exploité par Bad Rabbit »*, écrit la firme de sécurité dans une mise à jour de sa publication.

Ce qui confirmerait l'idée, partagée par Kaspersky, que les auteurs de Bad Rabbit et ceux de Petya/NotPetya sont probablement les mêmes (des précisions dans ce télégramme).

Bad Rabbit est le troisième malware/ransomware à exploiter les outils de la NSA depuis le début de l'année. Une série commencée avec Wannacry en mai, qui s'est appuyé sur EternaBlue, et poursuivie en juin avec NotPetya qui y a ajouté l'exploit de EternalRomance.

A quand le prochain épisode ?

Lire également

Ransomwares : enfin une protection générique pour Windows ?
Petya : 5 questions pour comprendre le ransomware qui terrorise les entreprises
Jean-Louis Lanet, Inria : « si le ransomware parfait existait… »