Windows Server 2003 victime d'un cryptomineur Monero

Depuis le 26 mai 2017, et probablement dès le 26 mars, une centaine de machines sous Windows Server 2003 génèrent de la cryptomonnaie Monero (XMR, code utilisé sur les places de marché).

ESET a découvert un botnet de serveurs infectés par un cryptomineur. Baptisé Win32/CoinMiner.AMW par l'éditeur d'antivirus, le malware dérivé d'un mineur Open Source xmrig effectue les calculs informatiques nécessaires pour valider les transactions des monnaies électroniques. Aux dépens des propriétaires des machines, évidemment.

Ces calculs nécessitent d'importantes ressources informatiques et pour lesquels ceux qui fournissent cette ressource sont récompensés en cryptomonnaie. Dans le cas soulevé par ESET, le botnet aurait généré plus de 63□000 dollars en Monero, une monnaie qui se distingue du bitcoin, notamment par des transactions intraçables.

« En nous basant sur les performances des CPU équipant habituellement les serveurs 2003 et les gains réalisés […] nous estimons que le réseau de botnets génère 5,5 XMR par jour, soit 825 dollars américains selon le taux de change actuel », indique Benoît Grunemwald, Cybersecurity Leader chez ESET.

Pour créer leur réseau, les assaillants ont exploité une faille propre au service WebDAV de Microsoft IIS 6.0 dans Windows Server 2003 R2. Si Microsoft a arrêté le support de son OS en juillet 2015, l'éditeur de Redmond avait fait une exception en juin dernier face à la déferlante du ransomware Wannacry en livrant une nouvelle fournée de correctifs de sécurité.

Le calme avant la tempête

En théorie, la faille exploitée par CoinMiner est donc comblée. Mais encore faut-il appliquer les correctifs, ce qui n'est pas toujours le cas des administrateurs qui évitent l'application des mises à jour automatiques. C'est cette négligence que les escrocs ont exploitée en repérant les machines non patchées. Pour cela, ils ont lancé des scans du réseau en force brute, visiblement depuis une machine hébergée chez Amazon Web Services (AWS).

Si la campagne a connu des pics de calculs fin août, avec des pointes à 160 kilohashes par seconde (kH/s) contre 100 kH/s en moyenne auparavant, les assaillants ont ralenti leur activité courant septembre. ESET n'ayant constaté aucune nouvelle infection de machine. *« Parce que le mineur n'a pas de mécanisme de persistance, les attaquants ont lentement commencé à perdre des machines déjà compromises, et le taux de hachage total a diminué jusqu'à 60 kH/s »*, souligne l'éditeur dans son compte rendu.

Un ralentissement qui s'explique probablement par l'application des correctifs de Windows Server au fil des mois par les administrateurs. Mais cette tendance pourrait cacher une prochaine vague d'attaques. *« Ce n'est pas la première fois que les attaquants ont pris une telle pause et il est probable qu'une nouvelle campagne sera lancée dans un proche avenir »*, pense ESET. Le calme avant la tempête□? Dans tous les cas, l'éditeur slovaque conseille, sans plus attendre, d'appliquer la mise à jour de sécurité

KB3197835.

Lire également
WannaCry a été doublé par l'attaque du cryptomineur Adylkuzz
Uiwix, la deuxième couche après WannaCry ?
Pourquoi Windows Server 2003 menace la sécurité du Web