WannaCry : des millions de machines infectées ?

Si WannaCry a pu infecter plus de 200 000 PC dans le monde, c'est notamment en exploitant une vulnérabilité zero-day du serveur SMB (Server Message Block) de partage d'imprimantes et fichiers sur le réseau des entreprises. Une faille exploitée par des outils de la NSA (qui ont de toute évidence été mis en ligne en avril par le groupe de hackers les Shadow Brokers) et qui touchait toutes les versions de Windows. Y compris Windows XP alors que le système n'est plus supporté par son éditeur mais toujours exploité par des organisations (devant la gravité de la situation, Microsoft a néanmoins déployé un patch de sécurité pour son vieil OS).

Face à cette capacité de propagation du ransomworm qui a défrayé la chronique à partir du 12 mai en Espagne, on pourrait considérer comme raisonnables les dégâts limités à ces quelques centaines de milliers de machines infectées. Sauf que leur nombre pourrait être beaucoup plus important et s'élever dans les faits à plusieurs millions d'unités.

Le chaos évité

« Nous soutenons que, selon nos données de recherche, le nombre réel de systèmes affectés s'élève en millions, avance la société de cybersécurité Kryptos Logic dans un billet de blog daté du 29 mai. *Et nous estimons que entre 14 à 16 millions d'infections et de réinfections ont été atténuées évitant ainsi ce qui aurait créé le chaos depuis le 12 mai. »* Et de rapporter que *« quelques centaines de milliers de systèmes ont été perturbés par l'attaque du ransomware jusqu'à ce que le kill-switch (un interrupteur de propagation découvert dans le code, NDLR) soit activé, suivi de 2 à 3 millions de systèmes affectés qui n'ont pas été perturbés par l'attaque. Sans l'effet atténuant du kill-switch, le nombre de systèmes vulnérables infectés aurait pu s'élever de manière plausible en dizaines de millions ou plus »*. On a frôlé la catastrophe.

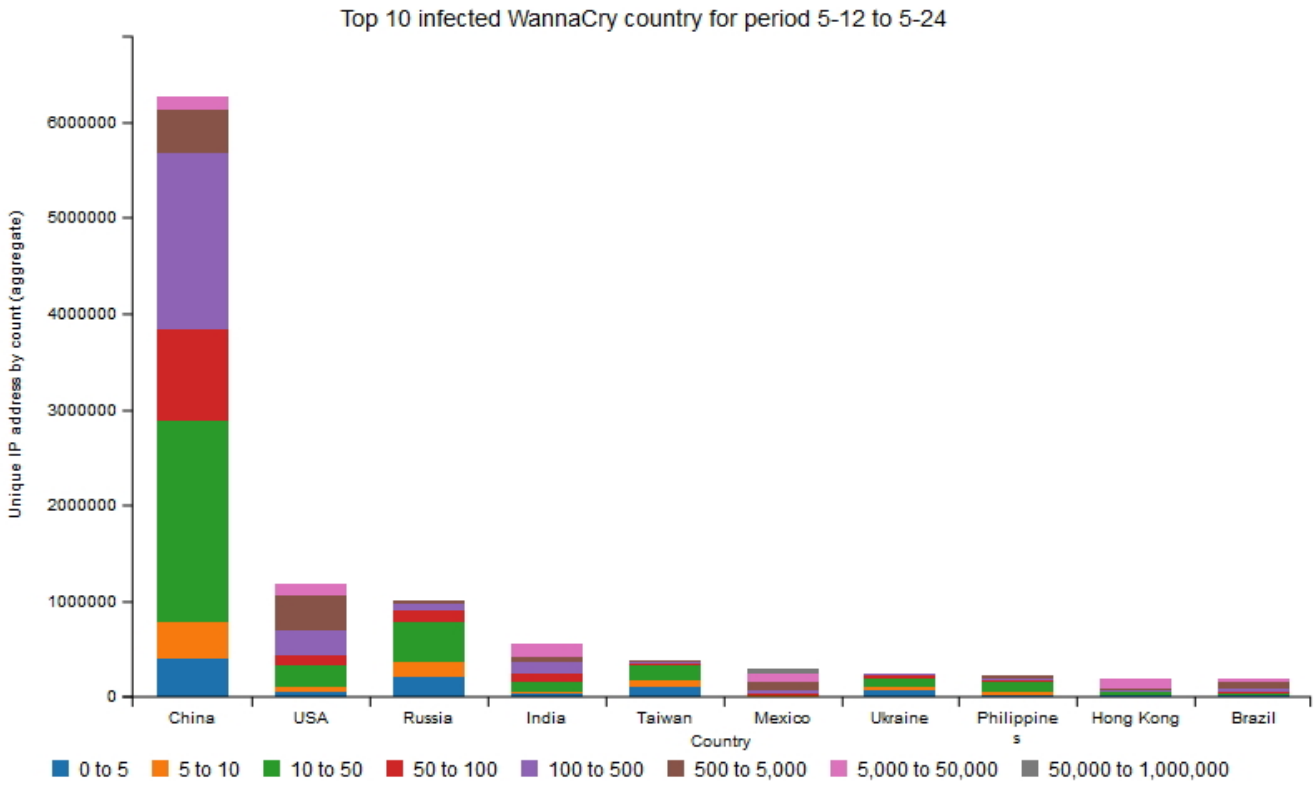
Comment Kryptos Logic en arrive à cette conclusion ? Au-delà de son expertise qui l'amène à surveiller des centaines de botnets par an et quelque 100 million de menaces potentielles quotidiennement, les experts justifient leurs estimations en considérant que *« les adresses IP hautement touchées peuvent être corrélées avec un nombre élevé de machines infectées partageant une adresse IP publique »*. Celles-ci peuvent en effet être utilisées par des routeurs de NAT (traduction d'adresses réseau) ou VPN (notamment) pour adresser plusieurs systèmes derrière. Autrement dit, derrière une adresse IP touchée, des dizaines ou centaines de machines peuvent être affectées.

Des infections sans conséquence

La société de sécurité tient néanmoins à préciser qu'elle considère les « infections évitées » comme des exploitations réussies du ransomware. Ce qui ne manque pas de gonfler les chiffres. *« Les systèmes exploités et comptabilisés par [notre] plate-forme Vantage après le kill-switch n'ont pas été totalement perturbés. Par conséquent, nous qualifions une infection en tant que système qui a été exploité par WannaCry, peu importe si elle a été perturbée de manière bénigne ou activée par l'attaque du ransomware »*, justifient les experts en cyber-sécurité. Autrement dit, si WannaCry a réussi à infecter un grand

nombre de machines, sa charge n'a été efficace que sur une minorité d'entre elles. Soit le nombre de 200□000 à 300□000 communément admis aujourd'hui.

Selon Kryptos, WannaCry s'est propagé sur plus de 9□500 réseaux IP de FAI et/ou d'entreprise dans plus de 8□900 villes de 90 pays. *« Certaines traces d'infection atteignent pratiquement tous les pays du monde »*, précise la société. La Chine arrive largement en tête des pays les plus touchés avec plus de 6 millions d'infections WannaCry devant les Etats-Unis et la Russie (autour de 1 million chacun). Une analyse différente de celle de Malewarebytes.



Lire également

WannaCry : le ransomware qui n'a plus besoin du phishing

Alain Bouillé, Cesin : « WannaCry doit pousser les entreprises à patcher plus vite »

EternalRocks, un ver mieux outillé que WannaCry