La Corée du Nord de plus en plus soupçonnée d'être le berceau de WannaCry

Les soupçons connexion entre le ransomware Wannacry, qui a infecté plus de 300□000 PC d'entreprises dans 150 pays depuis le 12 mai dernier, et le groupe de cyber-pirates Lazarus se renforcent. Ce dernier est déjà suspecté d'avoir détourné quelque 81 millions de dollars à la banque centrale du Bengladesh après avoir réussi à pénétrer son système puis en accédant au réseau interbancaire de transactions internationales Swift. Il serait aussi à l'origine de l'attaque du studio Sony Pictures en 2014.

Les chercheurs en sécurité et autorités américaines accusent la Corée du Nord de soutenir Lazarus, voire d'en être à l'origine. Même si à ce jour aucune preuve formelle de ce lien n'a pu être apportée. Et Pyongyang a toujours réfuté ces allégations. Mais les indices se multiplient. *Reuters* rapporte que, selon Kim Heung-Kwang, un professeur d'informatique Nord-coréen passé en Corée du Sud en 2004, les cyber-attaques visant à enrichir ses auteurs sont organisées par l'Unité 180, une cellule dédiée issue du Reconnaissance General Bureau (RGB), l'agence du renseignement de ce pays considéré comme l'un des plus fermé au monde, y compris au niveau du réseau Internet (ce qui complexifie les possibilités de représailles). Plusieurs des anciens élèves de Kim Heung-Kwang auraient rejoint la cyber-armée nord-coréenne, a-indiqué l'ancien professeur qui a conservé des sources à l'intérieur du pays dirigé par Kim Jong-Un.

Le code de Lazarus dans WannaCry

L'ancien professeur n'est pas le seul à accuser Pyongyang d'être à l'origine de WannaCry. Symantec aussi. *« Les outils et l'infrastructure utilisés dans les attaques du ransomware WannaCry ont des liens étroits avec Lazarus »*, indique la firme de sécurité dans un nouveau rapport publié hier, lundi 22 mai. Selon l'éditeur, des versions antérieures à WannaCry (ou WCry) ont été exploitées dès février 2017. Puis de nouveau en mars et en avril. Elles ne se différenciaient que par leur mode de propagation (par le vol d'identifiants et non l'exploitation de la vulnérabilité zero-day EternalBlue). *« L'analyse de ces premières attaques de WannaCry [...] a révélé des points communs importants dans les outils, les techniques et l'infrastructure utilisés par les agresseurs et ceux vus lors d'attaques antérieures de Lazarus, ce qui rend très probable le fait que Lazarus soit derrière la propagation de WannaCry »*, explique Symantec.

La firme justifie ses soupçons en s'appuyant sur les agents malveillants retrouvés lors des attaques antérieures à celles constatées à partir du 12 mai. En février, Trojan.Volgmer et deux variantes de Backdoor.Destover, l'outil de nettoyage de disque retrouvé après l'attaque de Sony Pictures, ont été récupérés sur le réseau d'une des victimes (qui a vu une centaine de PC infectés en deux minutes). En mars et avril, c'est Trojan.Alphanc et Trojan.Bravonc qui sont à l'œuvre. Le premier est une version modifiée de Backdoor.Duuzer, le second utilise la même adresse IP de serveur de commande et contrôle (C&C) que Backdoor.Duuzer et Backdoor.Destover. L'ensemble de ces outils de pénétration sont tous liés à Lazarus, selon Symantec. Tout comme les codes de Infostealer.Fakepude et Backdoor.Contopee, dont s'inspire WannaCry.

Une campagne de cybercriminalité

Si Symantec ne semble manifester aucun doute quant aux liens qui unissent WannaCry et le groupe Lazarus, l'éditeur se garde néanmoins d'accuser directement le gouvernement nord-coréen. *« Malgré les liens avec Lazarus, les attaques de WannaCry ne comportent pas les caractéristiques d'une campagne menée par un Etat-nation, mais sont plus typiques d'une campagne de cybercriminalité »*, remarque la firme dans sa publication. Sans pour autant réfuter la possibilité d'une manœuvre gouvernementale. D'autant que, si l'attaque contre Sony Pictures visait à empêcher la sortie d'une fiction tournant autour du dictateur nord-coréen, celle de la banque bangladaise affichait clairement la volonté de détourner des fonds.

Symantec n'est pas seul à soupçonner Lazarus d'être à l'origine de WannaCry. Expert en sécurité chez Google, Neel Mehta a également annoncé, la semaine dernière, avoir retrouvé des traces des outils du groupe de cyber-hackers dans le code du ransomware. A ce jour, WannaCry aurait rapporté moins de 109□000 dollars (49,32 bitcoins) à ses auteurs, rapporte le tweet dédié @actual_ransom, qui suit l'activité sur les 3 portefeuilles associés au ransomware.

[Article mis à jour le 24/05]

Lire également :

EternalRocks, un ver mieux outillé que WannaCry

WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue

Uiwix, la deuxième couche après WannaCry ?

crédit photo : Astrelok / Shutterstock.com