Après WannaCry : les Shadow Brokers promettent de nouvelles révélations

A peine la crise créée par le ransomworm (combinaison d'un rançongiciel et d'un ver informatique) en passe de se résorber, les Shadow Brokers signent leur retour sur la Toile. Alors qu'il avait expliqué mettre fin à ses activités en janvier, le groupe de hackers, inconnu jusqu'en août 2016, date à laquelle il a commencé à dévoiler des outils de hacking dérobés à la NSA (plus exactement à son bras armé en matière de cyberattaques, le groupe Equation), publie un nouveau message ce 16 mai. Il y annonce la création prochaine d'un nouveau service, sur abonnement, donnant accès à de nouveaux outils de piratage dérobés et autres données confidentielles. Les Shadow Brokers ne détaillent toutefois pas réellement les données encore en leur possession, ni leur provenance (même si leur discours semble indiquer qu'elles émanent une fois de plus de The Equation Group)

Cet espèce de club du hack ouvrirait en juin et serait accessible contre un abonnement mensuel (dont le tarif n'est pas précisé). Les Shadow Brokers indiquent que les futures archives offertes aux membres du « Monthly Data Dump » pourraient renfermer des outils et exploits pour navigateurs, routeurs et téléphones, des exploits inédits exfiltrés d'un nouveau kit d'opérations de la NSA (dont des outils ciblant Windows 10), des données sur les réseaux de fournisseurs Swift (le réseau de virements interbancaires) et ceux des banques centrales ainsi que des informations sur les programmes nucléaires et balistiques de la Russie, de la Chine, de l'Iran et de la Corée du Nord. Une menace qu'il faut évidemment prendre au sérieux, étant donné la validité des précédentes révélations des Shadow Brokers, qui renfermaient notamment des exploits pour Windows, Linux ou Solaris, pour les firewalls Cisco, Juniper ou Fortinet ou encore des informations précises sur les prestataires Swift. Sans surprise, en marge de leur volonté annoncée de créer un club, les Shadow Brokers laissent la porte ouverte à un achat en une fois de l'ensemble des données encore en leur possession. Sans toutefois fixer un prix pour le lot.

Proximité entre la NSA et l'industrie US ?

Dans son anglais assez inimitable, le groupe de hackers étale en effet sa déception de n'avoir vu ni les services de renseignements des grands pays actifs sur la Toile, ni les grands noms de l'industrie acheter les outils qu'il a dérobés à The Equation Group, depuis les premières révélations en août 2016. Les Shadow Brokers expliquent, en substance, ne pas être responsables de la pagaille créée par WannaCry. Et de mettre en avant le fait qu'ils avaient dévoilés, en janvier 2017, des captures d'écran montrant qu'ils étaient en possession des outils de hacking de Windows issus de la NSA. Une façon de signaler clairement à cette dernière que les exploits ciblant la faille zero day affectant le protocole SMB, une vulnérabilité critique exploitée par les outils de la famille Eternal (en particulier EternalBlue qu'embarque WannaCry), avaient fuité.

Selon les Shadow Brokers, c'est cette démarche qui a permis à Microsoft de patcher la faille SMB avant la divulgation des outils issus de The Equation Group en avril. « *La bonne terminologie est une vulnérabilité 30 jours parce que le patch Microsoft était disponible 30 jours avant la publication de l'archive* », écrivent les hackers. Au passage, pour les Shadow Brokers, cet épisode dévoile les relations entre

l'industrie US et les services de renseignement de l'Oncle Sam : « *The Equation Group paie les entreprises de technologie américaines pour ne pas patcher les vulnérabilités avant leur découverte publique* », accusent les hackers, qui pointent également la responsabilité de la Corée du Nord dans l'attaque WannaCry. Pour le groupe de hackers, que certains soupçonnent d'être lié à la Russie, les critiques de Microsoft à l'encontre des gouvernements « *amassant des vulnérabilités* », selon les mots de Brad Smith, le directeur des affaires juridiques de Redmond, ne seraient donc que de la poudre aux yeux.

A lire aussi :

Shadow Brokers : et maintenant des exploits visant Swift !

WannaCry : autopsie du ransomware 2.0, boosté par les exploits de la NSA

10 questions pour comprendre l'affaire Shadow Brokers

Crédit Photo : produktionsbuero TINUS-Shutterstock