ZCryptor : le ransomware Windows qui progresse comme un ver

Microsoft affirme avoir détecté une nouvelle souche de ransomware, baptisée ZCryptor, qui est capable de se comporter comme un ver, autrement dit de se déplacer d'un ordinateur Windows à l'autre. L'association des capacités de chiffrement de données des rançongiciels et du potentiel de déplacement des vers – via des supports externes ou des disques réseaux – présente évidemment un potentiel dévastateur important. Et comme le note Michael Jay Villanueva, un chercheur de Trend Micro, elle reste peu courante : « *Ce ransomware est un des rares à être en mesure de se diffuser par lui-même. Il laisse une copie de lui-même sur les disques amovibles, rendant l'emploi des supports USB risqué* ». Trend Micro qualifie la menace de critique et estime qu'elle possède un haut potentiel de destruction.

ZCryptor réclame 1,2 bitcoin sous 4 jours

Pour le reste, ZCryptor se diffuse selon des méthodes classiques. Microsoft signale que la souche peut être véhiculée par des spams, des macros Office ou via de faux logiciels d'installation de Flash Player. Une fois en place, ZCryptor s'assure d'être lancé au démarrage de la machine. Le virus va alors chiffrer un grand nombre de fichiers (les .doc, .docx, .txt, .xls, .xlsx, .xml, .jpeg, jpg, .png, .eps…), qui prennent alors l'extension .zcrypt. Pour restaurer l'accès aux données codées, les cybercriminels réclament alors une rançon de 1,2 bitcoin à payer sous 4 jours (soit environ 580 euros). Passé ce délai, la somme est portée à 5 bitcoins.

Dans une étude récente, Palo Alto Networks dénombre 30 familles de ransomwares actifs à ce jour. Si le phénomène n'est pas nouveau – la première souche de ce type serait née en 1989 -, il connaît une importante recrudescence ces derniers mois. Pour l'unité 42, l'équipe de Palo Alto en charge de la veille sur les menaces, la source du regain d'intérêt des cybercriminels pour ce type d'attaques s'explique par l'évolution économique du 'black market' : « *auparavant, les pirates profitaient de leurs actions malveillantes pour dérober des identités, ou des numéros de carte bancaire, et les revendre sur des*

marchés clandestins à vil prix, écrit l'Unité 42. *Ces dernières années, le tarif des données ainsi détournées s'est effondré, passant de 25 dollars en 2011 à seulement 6 dollars l'unité en 2016.1 Il a donc fallu que les cyberpirates trouvent de nouvelles sources de revenus, nombre d'entre eux se tournant vers les ransomwares, ou rançongiciels, séduits par les récents progrès accomplis dans la diffusion des attaques, l'anonymat des transactions et la capacité à crypter et décrypter en toute fiabilité les données* **».**

A lire aussi :

Ransomwares : ingéniosité, perversité et persévérance

Ransomware Locky : la France parmi les deux principaux pays ciblés

Ransomware Locky : l'AFP touchée, son RSSI témoigne

crédit photo : ra2studio-Shutterstock