ESET attribue la cyberattaque Petya au groupe TeleBots

	ESET attribue la cyberattaque Petya au groupe TeleBots

Selon les experts ESET®, la cyberattaque dite « Petya » pourrait être attribuée au groupe TeleBots. Il existe des similitudes entre les nombreuses campagnes menées contre l'Ukraine, l'amélioration des outils utilisés par le cyber-groupe entre décembre 2016 et mars 2017 et la menace Diskoder.C (Petya).

« La cyberattaque de 2016 menée contre les institutions financières ainsi que le développement d'une version Linux du malware KillDisk par TeleBots, ont attiré l'attention des chercheurs ESET. En parallèle, le nombre croissant d'attaques contre les systèmes informatiques que connaît l'Ukraine **nous ont fait pointer du doigt le groupe TeleBots,** » déclare Anton Cherepanov, Senior malware researcher chez ESET.

Le mode opératoire du groupe TeleBots est l'utilisation systématique du malware KillDisk qui réécrit les extensions de fichiers des victimes. L'obtention d'une rançon n'est donc pas leur objectif principal, car les fichiers cibles ne sont pas chiffrés, mais réécrit. Si l'évolution du malware contient de nouvelles fonctions, comme le chiffrement ou l'ajout de leurs coordonnées, l'objectif de KillDisk n'est toujours pas de récolter de l'argent.

Entre janvier et mars 2017, TeleBots a compromis une société d'édition de logiciels en Ukraine, utilisant alors des tunnels VPN pour accéder aux réseaux internes de plusieurs institutions financières. Au cours de cette campagne, l**es cybercriminels ont utilisé tout un arsenal d'outils en Python, SysInternals PsExec et des logins de session Windows volés pour déployer un nouveau ransomware.** Il fut détecté par ESET comme Win32/Filecoder.NKH et fut suivi par une version pour Linux, détecté comme Python/Filecoder.R.

TeleBots a ensuite lancé un nouveau malware le 18 mai 2017 : Win32/Filecoder.AESNI.C (également appelée XData). C**e ransomware s'est principalement diffusé en Ukraine via une mise à jour du logiciel financier M.E.Doc, largement utilisé en Ukraine.** Selon le LiveGrid® d'ESET, le malware se déploie juste après l'exécution du logiciel, **ce qui lui permet de se répandre automatiquement à l'intérieur d'un réseau compromis.** Bien qu'ESET ait mis à la disposition un outil de déchiffrement pour la plateforme Windows®, cette attaque ne fut pas très médiatisée.

Le 27 juin 2017, l'épidémie de ransomwares de type Petya (Diskoder.C) ayant compromis de nombreux systèmes notamment en Ukraine, a permis de montrer **la capacité du malware à remplacer le MBR par son propre code malveillant, code qui a été emprunté au ransomware Win32/Diskoder.Petya :** c'est pourquoi certains chercheurs ont nommé cette menace ExPetr, PetrWrap, Petya ou NotPetya.

Cependant, contrairement au ransomware original Petya, **les auteurs de Diskcoder.C ont modifié le code MBR de telle sorte que la récupération de fichiers ne soit pas possible, malgré l'affichage des instructions de paiement.** Une fois le malware exécuté, **il tente de se propager à l'aide de l'exploit Eternablue, en s'aidant de la backdoor DoublePulsar.** Il s'agit de la même méthode utilisée par le ransomware WannaCry.

Le malware est également capable de se diffuser de la même manière que le ransomware Win32/Filecoder.AESNI.C (XData), en utilisant Mimikatz, pour obtenir des mots de passe, puis en exécutant SysInternals PsExec. En outre, les attaquants ont mis en place une troisième méthode de diffusion à l'aide d'un mécanisme WMI.

Ces trois méthodes ont été utilisées pour diffuser les ransomwares, cependant et contrairement à WannaCry, l'exploit EternalBlue utilisé par le malware Diskoder.C cible uniquement des ordinateurs ayant un adressage interne.

Lier TeleBots à cette activité permet de comprendre pourquoi les infections se sont étendues à d'autres pays que l'Ukraine. ESET a analysé les connexions VPN entre les employés, les clients et les partenaires mondiaux de l'éditeur ainsi que le système interne de messagerie et d'échange de documents. Tout cela a permis aux cybercriminels d'envoyer des messages aux victimes (spearphishing). Les pirates ayant eu accès au serveur légitime de mise à jour ont diffusé des mises à jour malveillantes automatiquement (aucune interaction avec l'utilisateur ne fut nécessaire).

« Avec une infiltration si poussée dans l'infrastructure de l'éditeur du logiciel M.E.Doc et de sa clientèle, les pirates disposaient des ressources nécessaires pour diffuser Diskoder.C. Bien qu'il y eut des dommages collatéraux, cette attaque a permis de démontrer la connaissance approfondie de leur cible par les pirates. D'autre part, **l'amélioration du kit d'exploit EternalBlue le rend encore plus sophistiqué, ce à quoi devront faire face les acteurs de la cybersécurité dans les prochaines années,** » conclut Anton Cherepanov.

Réagissez à cet article

Source : *ESET*