Le crypto-ver

Les cybercriminels ont trouvé une nouvelle manière de se faire de l'argent en 2017. Cela faisait longtemps qu'ils tentaient de prendre en otage des disques durs, mais les gens sont devenus plus vigilants et n'ouvrent plus n'importe quelle pièce jointe à un mail. Voilà pourquoi les cybercriminels se sont vu contraints d'inventer une nouvelle façon d'installer leur rançongiciel (#ransomware). Leur solution : le ver.

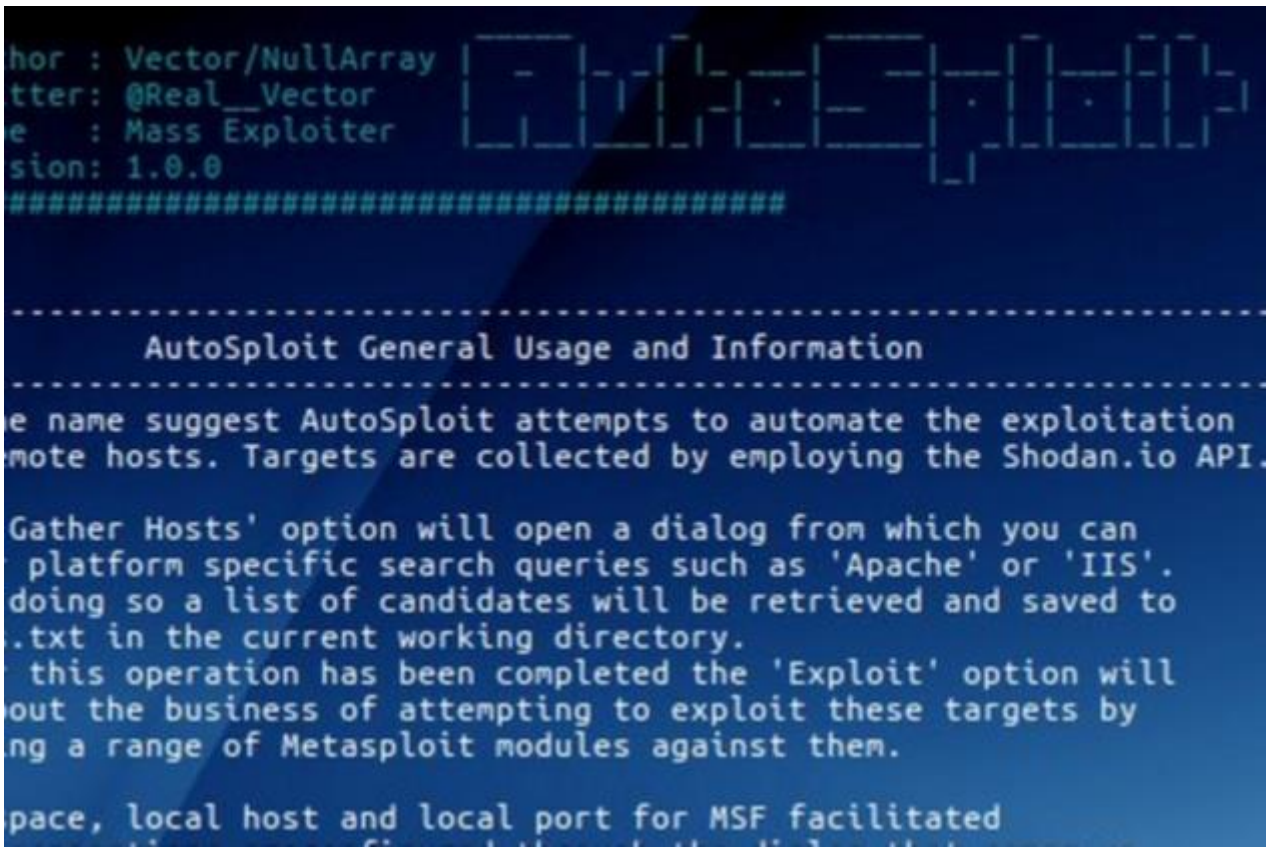
Le spécialiste de la sécurité Kaspersky lance donc une mise en garde. **Le 'crypto-ver' est « une forme mixte dangereuse de maliciel (malware) et de rançongiciel qui se répand d'elle-même ».** Elle peut se propager d'ordinateur à ordinateur, sans spam (pourriel) ou autre infection. Le malware se duplique simplement dans les appareils interconnectés.

Le premier ver, baptisé SamSam, s'est manifesté en avril. Et au cours des dernières semaines, des experts en sécurité ont découvert le ver ZCryptor. Ce dernier se présente sous la forme d'une simple mise à jour d'un programme largement utilisé tel Flash. Une fois en place, le ver commence à se propager, puis il crypte des dizaines d'extensions. Les victimes voient ensuite apparaître leur écran habituel, qui les informe que leurs fichiers ont été pris en otage et qu'ils doivent verser une rançon pour pouvoir y accéder de nouveau.

Les spécialistes de la sécurité n'ont pas encore trouvé une parade contre ZCryptor. Voilà pourquoi Kaspersky prodigue le conseil suivant : soyez sur vos gardes, veillez à disposer d'une bonne protection et effectuez régulièrement des sauvegardes (backups).

(source : https://www.lenetexpert.fr/tag/dsi/page/10/?print=print-search)

Pirater les objets connectés devient simple comme un jeu d'enfant



Avec le logiciel AutoSploit, quelques mots-clés suffisent pour pirater en masse des systèmes accessibles par Internet. Le logiciel provoque une vive polémique parmi les chercheurs en sécurité.

Mauvaise nouvelle pour les utilisateurs d'objets connectés. Un hacker dénommé « VectorSEC » vient de créer un outil diabolique qui permet de pirater en masse ces appareils, et de façon totalement automatique. Baptisé « AutoSploit », ce logiciel combine en effet deux outils bien connus des chercheurs en sécurité : Shodan.io, un moteur de recherche qui permet de détecter des objets connectés vulnérables ; et Metasploit, une plateforme de piratage modulaire utilisée notamment pour faire des audits de sécurité.

L'utilisation d'AutoSploit est ultrasimple. Il suffit d'indiquer un mot-clé qui fasse référence à un système particulier (« IIS », « Apache », « Western Digital », etc.). Le logiciel va alors récupérer auprès de Shodan.io une liste d'appareils accessibles, puis sélectionner dans les modules de Metasploit une séries d'attaques permettant d'obtenir un accès direct au système. Emballé c'est pesé.

Dans la communauté des hackers, cette publication a créé une vive polémique. Certains estiment, en effet, que ce logiciel ne respecte pas le code éthique des chercheurs en sécurité. *« Il n'y a aucune raison valable de mettre le piratage de masse de systèmes publiques à la portée des script-kiddies. Ce n'est pas parce qu'il est possible de faire quelque chose qu'il est sage de le faire. Tout*

ceci se terminera en larmes », explique Richard Bejtlich, fondateur de TaoSecurity, une filiale orientée sécurité de Cisco.

L'un de ses collègues, Craig Williams, va même plus loin, en cataloguant l'outil comme du malware. Car selon lui, il permet *« de cibler des systèmes sur Internet que [l'utilisateur] ne contrôle pas et n'a pas la permission d'attaquer »*. Le fait que le piratage soit totalement arbitraire ne permettrait pas d'utiliser AutoSploit de manière légale, comme dans le cadre d'un audit de sécurité.

De son côté, Rob Graham, PDG d'Errata Security, pense que la publication de ce logiciel est une bonne chose car, au final, cela va contribuer à l'amélioration du niveau de sécurité général. *« Tous ce qui facilite le travail des script-kiddies est une bonne chose car ces systèmes vont être piratés, puis patchés sans grand dommage. Ils seront donc moins vulnérables pour les pirates des acteurs gouvernementaux ou de la criminalité organisée »*, estime-t-il. En d'autres termes, AutoSploit serait un mal nécessaire pour faire avancer le schmilblick. Et vous, qu'en pensez-vous ?

https://www.lenetexpert.fr/cyber-securite-des-menaces-de-plus-en-plus-presentes-mais-des-collaborateurs-pas-assez-formes-le-net-expert-informatique/