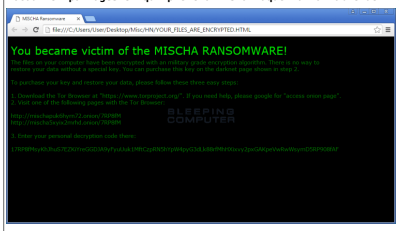
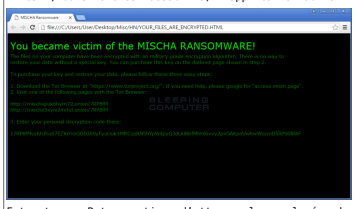
Mischa, le ransomware successeur de Petya

Mischa, le ransomware successeur de Petya

Apparu au mois de mars, le ransomware Petya a ouvert une nouvelle voie dans le développement des ransomwares. Il s'agissait du premier cas d'un malware qui allait au-delà du chiffrement des fichiers sur les disques locaux et partagés et qui préférait s'attaquer à la table de fichiers principale



Ceci étant dit, Petya n'était pas infaillible et les chercheurs ont été rapidement en mesure de créer un outil de restauration de certains des fichiers chiffrés par ce malware. Les individus malintentionnés n'ont pas perdu leur temps et ils ont trouvé le moyen de contourner une autre lacune de Petya : sa dépendance vis-à-vis de la volonté de la victime qui doit octroyer au malware les autorisations d'administrateur pour accéder à la table de fichiers principale (MFT).
Un nouveau programme d'installation de Petya a été détecté la semaine dernière. Celui-ci utilise un scénario de réserve. Si le malware n'obtient pas les autorisations d'administrateur au lancement, c'est un autre ransomware qui sera installé sur la machine infectée, en l'occurrence Mischa.
D'après les explications de Lawrence Abrams, de chez Bleeping Computer, les autorisations d'administrateur indispensables au fonctionnement de Petya figurent dans le manifeste de la version originale. Dans les commentaires envoyés à Threatpost, Lawrence Abrams explique « qu'avant l'exécution du code, Windows affiche la boîte de dialogue UAC qui sollicite ces autorisations. Si le service UAC est désactivé, l'application est exécutée automatiquement avec [les autorisations d'administrateur]. Si l'utilisateur clique sur « No » dans la fenêtre UAC, l'application n'est pas exécutée et, par conséquent, l'installation de Petya n'a pas lieu ».
Pour les exploitants de Petya, ces échecs représentent un gaspillage de ressources d'après Lawrence Abrams. Pour rectifier le tir, ils ont empaqueté un autre ransomware avec le programme d'installation. Il s'agit de Mischa qui sera exécuté si l'option « Petya » n'a pas pu être mise en œuvre.
Le manifeste de la nouvelle version indique que le fonctionnement requiert les données du compte utilisateur. Dans ce cas, Windows autorise le lancement de l'application sans afficher d'avertissement UAC. Comme l'explique Lawrence Abrams, « au lancement du programme d'installation, il sollicite les autorisations d'administrateur conformément à ses paramètres. La boîte de dialogue UAC s'affiche et si l'utilisateur choisit « Yes », ou si UAC est désactivé, l'application obtient les autorisations d'administrateur et installe Petya. Dans le cas contraire, c'est Mischa qui sera installé. Cette méthode est très intelligente ».



Entre temps, Petya continue d'attaquer les employées des services des ressources humaines allemands à l'aide de messages non sollicités qui contiennent des liens vers un fichier malveillant dans le cloud. Au début, les individus malintentionnés utilisaient Dropbox, mais depuis le blocage des liens Dropbox malveillants, ils se sont rabattus sur le service allemand TelekomCloud. Le fichier exécutable se dissimule sous les traits d'un fichier PDF qui serait un prétendu CV d'un candidat à un poste libre. Il contient même une photo.
« Lorsque l'utilisateur télécharge le fichier exécutable, l'icône PDF s'affiche, ce qui laisse penser qu'il s'agit bien d'un CV au format PDF » explique Lawrence Abrams. Toutefois, lorsque ce fichier est ouvert, il tente d'installer Petya. Et si cela ne marche pas, il installe le ransomware Mischa.
Le comportement de Mischa est identique à celui des autres ransomwares standard. Il analyse le disque local à la recherche de fichiers portant certaines extensions. Il chiffre les fichiers à l'aide d'une clé AES et ajoute à leur nom une extension de 4 caractères, par exemple 7GP3. Lawrence Abrams explique que « lorsque Mischa chiffre le fichier, il conserve la clé de chiffrement à la fin du fichier obtenu. Il convient de noter qu'il ne chiffre pas uniquement les fichiers traditionnels dans ce genre d'attaque (PNG, JPG, DOCX, etc.), mais également les fichiers EXE. »
Une fois qu'il a chiffré les fichiers, Mischa exige le versement d'une rançon de 1,93 bitcoins (environ 875 dollars américains) pour le déchiffrement. La somme doit être payée via le site Tor. Il n'existe pas encore d'outil de déchiffrement pour ce ransomware. « Nous conseillons aux victimes de vérifier avant tout la conservation des clichés instantanés à l'aide de Shadow Explorer. Ils pourraient être utile pour restaurer une ancienne version des fichiers chiffrés » conclut Lawrence Abrams.

Article du Kaspersky Lab

Source : *Petya possède un suppléant : Mischa – Securelist*