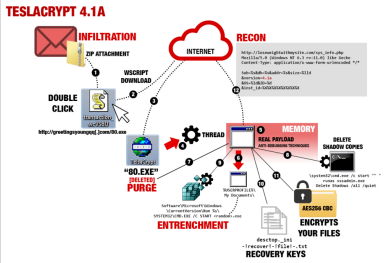
Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

	Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

Ces nouveaux exemplaires de TeslaCrypt sont diffusés massivement en tant que pièce jointe dans des spams qui imitent les avis de réception de colis des courriers express. D'après Endgame, la version 4.1A est apparue il y a environ une semaine ; outre les extensions déjà ciblées, elle attaque également les fichiers suivants .7z, .apk, .asset, .avi, .bak, .bik, .bsa, .csv, .d3dbsp, .das, .forge, .iwi, .lbf, .litemod, .litesql, .ltx, .m4a, .mp4, .rar, .re4, .sav, .slm, .sql,

La diffusion de TeslaCryp via le spam constitue également un changement : lors des campagnes récentes de TeslaCrypt, le ransomware avait été propagé via des kits d'exploitation et des redirections depuis des sites WordPress et Joomla. Dans ce cas, la victime doit ouvrir le fichier ZIP en pièce jointe afin d'activer un downloader JavaScript qui utilise Wscript (un composant de Windows) pour télécharger le fichier binaire de TeslaCrypt depuis le domaine greetingsyoungqq[.]com.
D'après notre interlocutrice, l'analyse de la version actualisée du ransomware fut complexe car elle lance de nombreux flux d'application et d'opérations de débogage afin de compliquer la tâche des outils de protection. Comme l'explique Amanda Rousseau, « il semblerait qu'il essaie de dissimuler les lignes dans la mémoire. Il est plus difficile pour l'Antivirus de les détecter s'il n'analyse pas la mémoire. »



Le recours à Wscript rend également la détection plus compliquée car le trafic ressemble à des communications légitimes de Windows. Selon Amanda Rousseau, il aura fallu quatre jours aux outils de détection pour identifier la technique et l'ajouter aux signatures. La durée de service des serveurs de commande sur lesquels se trouve TeslaCrypt a été limitée. A l'issue de celle-ci, les individus malintentionnés changent d'hébergement.
La version actualisée du ransomware utilise également un objet COM pour dissimuler les lignes de code extraites et élimine les identifiants de zone afin qu'ils ne soient pas découverts. De plus, pour éviter la surveillance, le malware arrête plusieurs processus Windows : Task Manager, Registry Editor, SysInternals Process Explorer, System Configuration et Command Shell. Pour garantir sa présence permanente, il se copie sur le disque et crée le paramètre correspondant dans la base de registres.
Vous trouverez une description technique détaillée de TeslaCrypt, y compris de ses méthodes de chiffrement et de ses techniques de lutte contre le débogage sur le blog d'Endgame.
Amanda Rousseau a indiqué dans ses commentaires que lors des essais, les nouveaux échantillons ont atteint les disques réseau connectés et ont tenté de chiffrer les fichiers qui s'y trouvaient. Ils tentent également de supprimer le cliché instantané du volume afin de priver la victime de toute chance de récupération.
Mais il y a malgré tout une bonne nouvelle : la version actualisée de TeslaCrypt chiffre les fichiers à l'aide d'une clé AES 256 et non pas à l'aide d'une clé RSA de 4 096 bits comme indiqué dans la demande de rançon et qui plus est, les informations indispensables au déchiffrement restent sur la machine infectée. « Nous avons trouvé l'algorithme de chiffrement : il fonctionne correctement, mais laisse le fichier de restauration dans le système » a confirmé Amanda Rousseau. « Si l'on part du programme de déchiffrement antérieur de TeslaCrypt et que son code est actualisé conformément aux [découvertes], il sera possible de réaliser le déchiffrement. » Il y a un an environ, Cisco a diffusé un utilitaire de ligne de commande capable de déchiffrer les fichiers touchés par TeslaCrypt.
Amanda Rousseau a également signalé que les auteurs de la version actualisée du ransomware avait emprunté beaucoup de code aux versions antérieures, notamment l'utilisation des objets COM et certaines techniques de débogage. « On dirait que les individus malintentionnés suivent les chercheurs à la trace en surveillant le code [de déchiffrement] publié sur Github en open source » explique le président d'Endgame en montrant les modifications introduites au cours du dernier mois depuis la version 4.0 jusqu'à la version 4 1A. – De petites modifications sont introduites dans chaque version et à la sortie de chaque nouveau décrypteur. Il prenne le meilleur de ce qui était utilisé il y a deux mois et l'appliquent aujourd'hui. »… [Lire la suite]

Source : *TeslaCrypt s'attaque à de nouveaux fichiers et améliore sa protection – Securelist*