Un malware multi compétences est né. Proteus

Un malware multi compétences est né. Proteus

Les experts de sécurité de Fortinet ont découvert un malware multifonction nommé Proteus. Il vérifie notamment les comptes e-commerce piratés.

Imaginer un malware capable de transformer les ordinateurs en serveur proxy, de miner différentes monnaies virtuelles, d'enregistrer les frappes au clavier et de vérifier la validité des comptes victimes d'un vol de données. Et bien cela existe. Les experts de Fortinet ont déniché ce couteau suisse du logiciel malveillant.
Baptisé Proteus, le malware est écrit en .Net et se diffuse à travers le botnet Andromeda. Les spécialistes de Fortinet constatent que ce malware peut éliminer d'autres logiciels malveillants sur les PC compromis. Tout comme Andromeda, il communique via un chiffrement symétrique avec des serveurs C&C pour contrôler les actions du malware sur les PC. De plus, il est capable d'ajouter des modules additionnels, les télécharger et les exécuter à la demande. Proteus s'épanouit dans le minage de crypto-monnaies. Il supporte les outils, HA256 miner, CPUMiner et ZCashMiner utilisés pour les monnaies virtuelles comme Bitcoin, Litecoin, Zcash.

Un vérificateur de comptes e-commerce piratés

Pour les spécialistes de la sécurité, la grande spécificité de Proteus réside dans sa capacité à vérifier la validité des comptes volés sur certains sites. Dans les cas présent, le code source du malware a montré que la vérification est réclamée par le serveur de C&C qui fournit des identifiants et des mots de passe. Le PC infecté va donc envoyer une requête sur certains sites de e-commerce comme Amazon, eBay, Spotify, Netflix et plusieurs sites allemands…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Proteus, le couteau suisse du logiciel malveillant