AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Le malware Trigona qui personnalise ses outils d'exfiltration de données

Contenu

I. Contexte

Les récentes vagues d'attaques liées au ransomware Trigona marquent un tournant dans le mode opératoire des exfiltrations des données. Contrairement aux campagnes précédentes, les cybercriminels utilisent désormais un outil d'exfiltration de données personnalisé, conçu pour opérer plus rapidement et avec une discrétion accrue au sein des environnements compromis.

Cette évolution témoigne d'une volonté manifeste de s'affranchir des outils publics tels que Rclone ou MegaSync, qui sont aujourd'hui systématiquement détectés par les solutions de sécurité (EDR/AV). Selon les experts, cet investissement dans un malware propriétaire vise à maintenir un profil bas durant la phase la plus critique de l'intrusion : le vol de données.

II. Analyse technique du malware

Le cœur de cette nouvelle menace repose sur un utilitaire en ligne de commande nommé *uploader_client.exe*. Ce programme se connecte à une adresse de serveur codée en dur et présente des fonctionnalités avancées optimisant à la fois la vitesse et l'évasion :

- Le support de cinq connexions simultanées par fichier permet un transfert massif et rapide des données ;
- Le logiciel effectue une rotation des connexions TCP tous les 2 Go de trafic pour contourner la surveillance réseau et l'analyse de flux ;
- Une option permet d'exclure les fichiers volumineux à faible valeur (comme les fichiers médias) pour se concentrer sur les documents critiques (factures, PDF) ;
- L'utilisation d'une clé d'authentification garantit que seuls les attaquants peuvent accéder aux données dérobées sur leur serveur.

En complément de cet outil d'exfiltration, les acteurs malveillants préparent minutieusement le terrain en neutralisant les défenses locales de la victime.

III. Vecteurs d'attaque et neutralisation des défenses

Pour assurer le succès de l'opération, les opérateurs de Trigona déploient un arsenal d'outils destinés à paralyser la sécurité des systèmes. L'attaque débute souvent par l'installation de la suite **Huorong Network Security (HRSword)** en tant que service de pilote noyau.

Une fois cette base établie, les attaquants utilisent des utilitaires spécialisés (tels que **PCHunter, Gmer, YDark ou DumpGuard**) pour désactiver les produits de protection des

Endpoint. Nombre de ces outils exploitent des vulnérabilités au niveau du noyau pour forcer l'arrêt des processus de sécurité.

Pour amplifier leur contrôle, les cybercriminels s'appuient sur :

PowerRun : Pour exécuter des scripts avec des privilèges élevés, contournant ainsi les protections du mode utilisateur.

AnyDesk : Pour maintenir un accès à distance direct sur les machines compromises.

Mimikatz et Nirsoft : Pour le vol d'identifiants et la récupération de mots de passe.

IV. Recommandations de sécurité

Apparu en octobre 2022, Trigona fonctionne sur un modèle de double extorsion, exigeant des rançons en cryptomonnaie Monero. Bien que l'infrastructure du groupe ait été sévèrement perturbée en octobre 2023 par des hacktivistes ukrainiens entraînant le vol de leur code source et de leurs bases de données, les observations récentes confirment une reprise totale de leurs activités. Cette résilience souligne la capacité des acteurs malveillants à se réorganiser rapidement après un démantèlement partiel.

La vigilance est de mise face à cette recrudescence. Les actions recommandées sont les suivantes :

1. Surveiller l'exécution de processus inhabituels comme uploader_client.exe.
2. Auditer l'utilisation d'outils d'administration à distance (AnyDesk) non autorisés.
3. Renforcer la surveillance des connexions TCP sortantes volumineuses vers des adresses IP inconnues.