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

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Le Malware Electricfish

Contenu

I. Contexte

Des experts en sécurité informatique annoncent avoir découvert un nouveau malware utilisé par les hackers du groupe nord-coréen Lazarus pour exfiltrer les données de leurs victimes. Selon le MAR (malware analysis report) AR19-129A publié sur le site web US-CERT du gouvernement américain, ce malware intitulé ELECTRICFISH a été détecté en suivant les activités malveillantes du groupe de hackers Lazarus, soutenu par le gouvernement de Corée du Nord, et aussi connu sous le nom de HIDDEN COBRA, Guardians of Peace, ZINC ou encore NICKEL ACADEMY.

Ce virus est un outil de tunneling polyvalent qui fonctionne dans l'ombre de votre système d'exploitation et crée un canal de communication entre votre PC et le serveur des attaquants. Il compromet votre sécurité et votre vie privée en rendant votre ordinateur vulnérable à des centaines de menaces en ligne. Si vous soupçonnez que votre ordinateur héberge ElectricFish, prenez immédiatement des mesures pour l'éradiquer.

II. Fonctionnement

Le malware ElectricFish implémente un protocole personnalisé permettant au trafic d'être détourné entre la source et l'adresse IP de destination.… Les hackers peuvent configurer le malware à l'aide d'un serveur ou d'un port proxy et d'identifiants proxy. Ceci permet de connecter à un système situé au sein du serveur proxy, et donc de contourner le système d'authentification du système infecté. Il devient alors possible d'établir une connexion entre l'adresse IP source et l'adresse IP de destination. Les hackers sont alors en mesure de transférer les informations collectées sur les ordinateurs compromis vers les serveurs qu'ils contrôlent…

Le malware est composé d'un fichier exécutable Windows 32 bits illicite, contenant des lignes de commande dont le but principal est de canaliser le trafic entre deux adresses IP. L'application accepte les arguments de ligne de commande lui permettant d'être configurée avec une adresse IP de destination et un port, une adresse IP source et un port, une adresse IP de proxy et un port, ainsi qu'un nom d'utilisateur et un mot de passe, pouvant être utilisés pour s'authentifier auprès d'un proxy serveur. Il tentera d'établir des sessions TCP avec l'adresse IP source et l'adresse IP de destination. Si une connexion est établie à la fois avec les adresses IP source et de destination, cet utilitaire malveillant implémentera un protocole personnalisé, ce qui permettra au trafic d'être « tunnelisé » rapidement et efficacement entre deux ordinateurs. Si nécessaire, le logiciel malveillant peut s'authentifier avec un proxy pour pouvoir atteindre l'adresse IP de destination. Un serveur proxy configuré n'est pas requis pour cet utilitaire.

Une fois le logiciel malveillant authentifié auprès du proxy configuré, il tentera immédiatement d'établir une session avec l'adresse IP de destination, située en dehors du réseau cible et avec l'adresse IP source. L'en-tête du paquet d'authentification initial, envoyé aux systèmes source et cible, sera statique à l'exception de deux octets aléatoires qui changeront à chaque tentative de connexion.

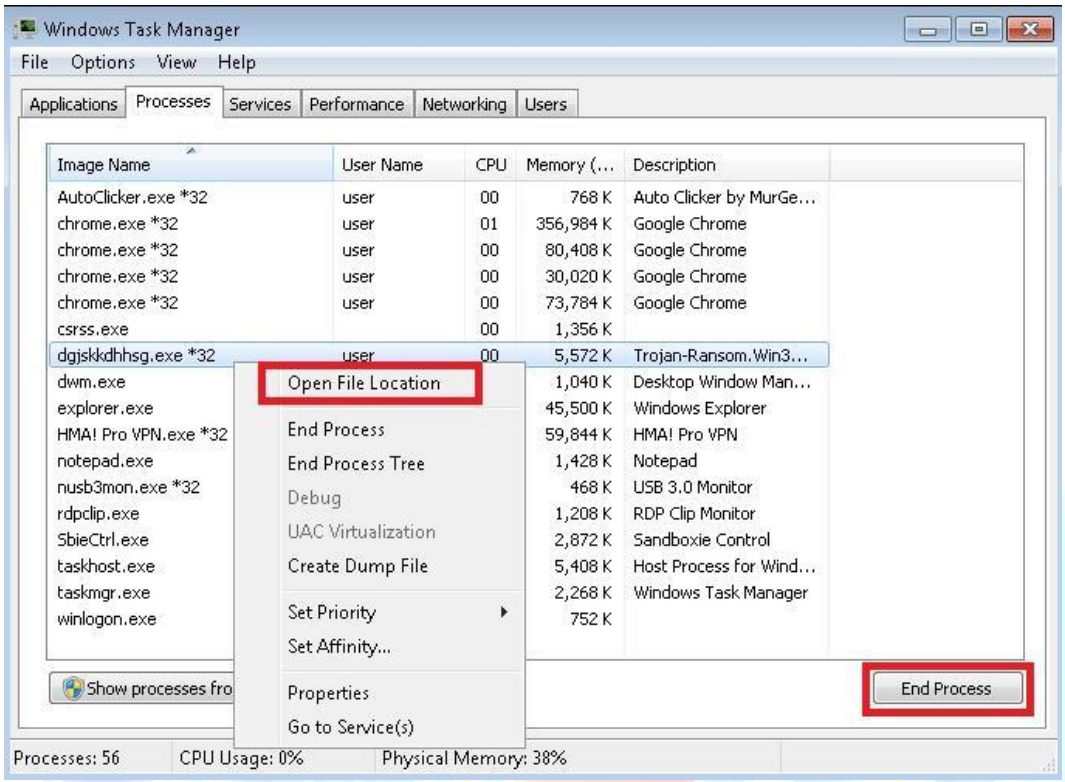
III. Comment se protéger

Pour vous éviter d'être victime d'une attaque ciblée provenant d'un acteur malveillant connu ou non, il est recommandé de prendre les précautions suivantes :

- Maintenir à jour les signatures et les moteurs d'antivirus ;
- Désactiver les services de partage de fichiers et d'imprimantes. Si ces services sont requis, utilisez des mots de passe forts ou l'authentification Active Directory ;
- Utilisez des outils de sécurité authentiques de pointe à jour, et assurez-vous que votre équipe de sécurité a accès aux plus récentes données de veille sur les cybermenaces ;
- Veillez à mettre à jour régulièrement tous les logiciels employés dans votre entreprise, en particulier en installant chaque nouveau correctif de sécurité dès sa publication. Des produits de sécurité offrant des fonctions d'analyse des vulnérabilités et de gestion des correctifs peuvent vous aider à automatiser ces processus ;
- Choisissez une solution de sécurité éprouvée dotée de capacités de détection comportementale pour une protection efficace contre les menaces connues et inconnues, notamment les exploitations de vulnérabilités ;
- Faites-en sorte que votre personnel connaisse les règles élémentaires de cyber-hygiène, sachant que de nombreuses attaques ciblées commencent par des techniques d'ingénierie sociale (phishing ou autres) ;
- Limitez la capacité des utilisateurs (autorisations) à installer et exécuter des applications logicielles non désirées. N'ajoutez pas d'utilisateurs au groupe des administrateurs locaux, sauf si cela est requis ;
- Appliquez une stratégie de mot de passe fort et implémentez des changements de mot de passe réguliers ;
- Soyez prudent lorsque vous ouvrez des pièces jointes à un courrier électronique, même si la pièce jointe est attendue et que l'expéditeur semble être connu ;
- Activez un pare-feu personnel sur les postes de travail de votre structure, configuré pour refuser les demandes de connexion non sollicitées ;
- Désactivez les services inutiles sur les postes de travail et les serveurs d'agence ;
- Rechercher et supprimer les pièces jointes suspectes; s'assurer que la pièce jointe numérisée correspond à son "type de fichier" (c'est-à-dire que l'extension correspond à l'en-tête du fichier) ;
- Surveiller les habitudes de navigation des utilisateurs sur le Web; restreindre l'accès aux sites à contenus douteux.
- Faites preuve de prudence lorsque vous utilisez un support amovible (p. Ex. Clés USB, lecteurs externes, CD, etc.) ;
- Analysez tous les logiciels téléchargés sur Internet avant leur exécution ;

IV. Annexes

Annexes 1: identification de processus suspect



Annexes 2: identification d'adresses de redirection