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 Snow propagé via Microsoft Teams

Contenu

I. Contexte

Les chercheurs en cybersécurité ont découvert une nouvelle menace sophistiquée baptisée **Snow** et activement déployé par le groupe **UNC6692**. Cette panoplie d'outils inclut une extension de navigateur, un outil de tunnelisation et une porte dérobée (backdoor).

L'objectif final de ces attaques est l'exfiltration de données sensibles après une compromission profonde du réseau, facilitée par le vol d'identifiants et la prise de contrôle du domaine.

II. Vecteur d'infiltration

Ingénierie Sociale et Usurpation d'Identité

Pour pénétrer les réseaux ciblés, le groupe UNC6692 privilégie une approche par ingénierie sociale particulièrement agressive. Les utilisateurs malveillants utilisent la tactique de l'« email bombing » (submersion de la boîte mail par des spams) pour créer un sentiment d'urgence chez la victime.

L'attaquant contacte ensuite la cible via Microsoft Teams en se faisant passer pour un agent du support informatique, sous prétexte d'installer un correctif pour bloquer le spam, la victime est incitée à cliquer sur un lien malveillant. Une fois la confiance de l'utilisateur trompée, l'infrastructure technique du malware est déployée silencieusement sur le poste de travail.

III. Analyse technique du malware « Snow »

L'installation initiale exécute des scripts AutoHotkey qui chargent SnowBelt, une extension Chrome malveillante. Cette dernière s'exécute sur une instance "headless" (sans interface graphique) de Microsoft Edge, rendant l'activité totalement invisible pour l'utilisateur.

Pour assurer sa survie et sa communication, la suite s'appuie sur deux composants clés :

SnowGlaze : Un outil de tunnelisation établissant une connexion via WebSocket pour masquer les échanges avec l'infrastructure de commande et contrôle (C2). Il fait également office de proxy SOCKS.

SnowBasin : Une backdoor basée sur Python qui exécute des commandes CMD ou PowerShell envoyées par l'attaquant.

Les capacités de SnowBasin

Endpoint	Function	Description
/stream	Remote Shell	Receives a command and executes it via cmd.exe or powershell.exe. It returns the STDOUT/STDERR results to the attacker.
/buffer	File Exfiltration	If a file path is provided, it reads the file, encodes it in Base64, and sends it back. If a folder is provided, it returns a full directory listing
/flush	File Deletion	Relayed. Signals http://localhost[:]8000/flush to flush buffered data.
/commit	File Ingress	Downloads a file from a provided URL and saves it to a specific path on the local disk. It bypasses SSL certificate verification (CERT_NONE).
/capture	Take Screenshots	Uses the mss and PIL libraries to take a screenshot of all monitors and send the image back as a Base64 string.
/gc	Self-Termination	Shuts down the server instance, effectively ""killing"" the backdoor's connection.

Grâce à cette architecture robuste, l'attaquant dispose d'un contrôle total sur la machine infectée, ouvrant la voie à l'escalade des privilèges.

Exfiltration et impact final

Au stade final, l'acteur malveillant utilise l'outil FTK Imager pour extraire la base de données Active Directory, ainsi que les ruches de registre critiques (SYSTEM, SAM et SECURITY).

De manière surprenante, l'exfiltration des données vers l'extérieur est réalisée via le logiciel LimeWire, permettant aux attaquants de disposer de l'intégralité des identifiants du domaine.

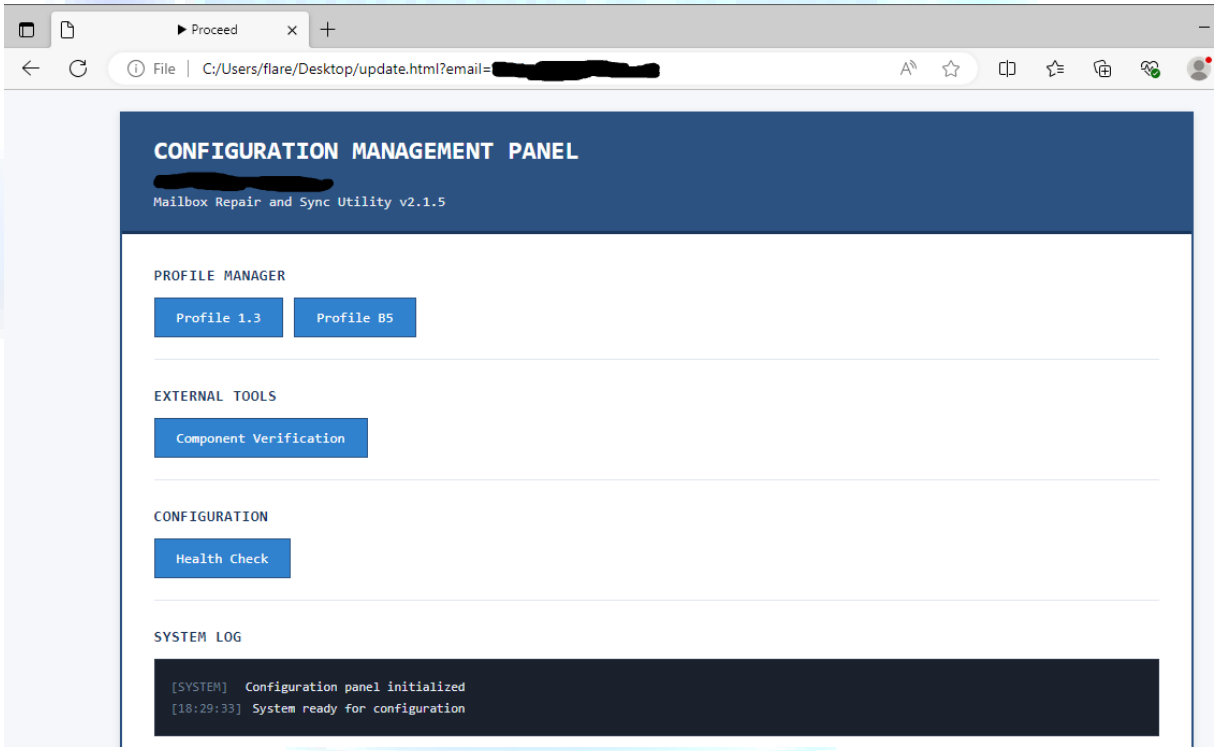
IV. Conclusion

Il est impératif pour les équipes de sécurité de surveiller l'apparition de tâches planifiées inhabituelles et de connexions WebSocket suspectes.

La sensibilisation aux risques de support informatique frauduleux via Microsoft Teams, une tendance croissante dans l'écosystème cybercriminel actuel.

V. Annexes

La page utilisée lors des attaques



Cycle de vie de l'attaque