Threat Intelligence à partir des rapports

Ilias Bettayeb - 2092408

Type : Travail individuel

Dépôt : Moodle via le lien « Quiz – Analyse des rapports Threat Intelligence » sous la section « Semaine 9 – Rapports Threat Intelligence » avant 21h30.

Énoncé : En tant qu'équipe Threat Intelligence, vous êtes invité à analyser les deux rapports « Tropic Trooper's Back: USBferry Attack Targets Air gapped Environments » et « Tropic Trooper's New Strategy » pour extraire des informations sur les menaces afin d'aider votre organisation à mieux comprendre le paysage des attaques et à se préparer à se défendre. A cet effet, vous êtes demandé de répondre aux questions suivantes :

USBferry malware

Modus Operandi :

1. Comment le malware USBferry se propage-t-il et s'exécute-t-il sur les systèmes cibles ? Quelle est sa principale méthode d'infection ? **(1 point)**

Copie les logiciels malveillants sur un support amovible et infecte d'autres machines.

Ils emploient la stratégie d'infection par le port USB en utilisant le périphérique USB pour transporter des logiciels malveillants dans l'ordinateur de la cible et facilitent une brèche dans l'environnement réseau sécurisé. (p.6)

2. Comment USBferry surmonte-t-il l'isolement de l'entrefer (*Air Gap*) et quelles techniques ou méthodes innovantes utilise-t-il pour faciliter la communication avec les réseaux externes ? **(1 point)**

En transportant le programme d'installation vers une machine hôte isolée via USB. Data Enrypted T1022 et Exfiltration Over Command and Control Channel T1041

Cibles et victimes :

3. Quels secteurs ou types d'organisations ont été ciblés par USBferry ? Existe-t-il des régions spécifiques avec des taux d'infection plus élevés ? **(1 point)**

Hôpital militaire, les banques nationales, Agences Militaires ou d'Armée de mer, Institution gouvernementales. Asie, mais plus récemment Asie du Sud-Est (Taiwan et philippines).

Impact collatéral :

4. Au-delà des objectifs principaux, quel impact collatéral USBferry a-t-il sur les systèmes *Air Gap*, et existe-t-il des conséquences secondaires dont les organisations devraient être conscientes ? **(1 point)**

Mitigation et prévention :

5. Quelles stratégies de mitigations recommandez-vous pour se défendre contre les attaques USBferry ? **(1 point)**

Éviter d'insérer des clés USB inconnues, utilisez un antivirus, surveillez l'actvité du réseau, éduquez les membres de l'équipe

<u>Tropic Trooper Threat Actor Group</u>

Concentration géographique :

6. Quelles régions/pays sont généralement ciblés par le groupe de menace Tropic Trooper ? Y a-t-il des motivations géopolitiques derrière leurs activités ? **(1 point)**

Asie du Sud-Est : Taiwanese, Philippine, and Hong Kong targets. Après une recherche rapide sur Google, j'ai pu voir que c'est un groupe Chinois. Il y a évidemment des conflits socio-politiques entre Taiwan et la Chine par rapport à qui appartient Taiwan. Aussi, il peut y avoir quelques tensions entre la Chine et Hong Kong, qui est advantage occidentalisé et a une importante influence américaine. Pour les Philippines, je ne connais pas la situation des 2 pays. Donc, il se peut qu'il y ait des motivations géopolitiques.

Évolution des tactiques :

7. Comment les tactiques et techniques employées par Tropic Trooper ont-elles évolué au fil du temps ? Y a-t-il des changements notables dans leur mode de fonctionnement ? **(1 point)**

Le groupe utilise des attaques plus complexes et s'adapte aux systèmes de défense pour être efficace et éviter la détection. Le groupe fait du hijacking ce qui est assez notable. On peut voir que le groupe exploiter des vulnérabilités sur Microsoft Office, puis l'injection de backdoor dans le système. Le groupe fait aussi de l'encodage pour dissimuler les activités malveillantes. Bref, une bonne évolution.

Web Shell:

8. Quelle commande Web Shell est utilisée pour afficher les informations du répertoire actuel ? **(1 point)**

La question me semble assez bizarre, mais on peut print le current directory avec pwd ou afficher les différents éléments du répertoire avec la commande ls -la par exemple

Communications Command & Control :

9. Quel numéro de port est utilisé par Tropic Trooper pour établir les communications de Command & Control ? **(1 point)**

Le numéro de port 443.

MITRE ATT&CK :

10. Quel est le nom du fichier utilisé par Tropic Trooper dans la phase d'exécution ? **(1 point)**

Le system configuration file (in.sys).

11. Quelles techniques d'évasion Tropic Trooper utilise-t-il pour contourner les contrôles de sécurité et les mécanismes de détection ? **(1 point)**

Le chiffrement, par exemple. Le groupe chiffre ses configurations et utile SSL pour se connecter à des serveurs, cela permet de dissimuler les communications. Utilise des fichiers MSI, qui seront exécutés avec des commandes donc l'Activité est moins visible. Exploitation de vulnérabilité sans être détecté aussi.

12. Quel est l'identifiant de la technique utilisée pour inciter la victime à double-cliquer sur des fichiers leurres ? **(1 point)**

T1204

13. En observant les différentes MITRE techniques de la tactique Command & Control, quelle est, selon vous, la stratégie de haut niveau de Tropic Trooper pour établir et maintenir le Command & Control ? **(1 point)**

T1102 – Web Service

L'utilisation de services communs, tels que ceux proposés par Google ou Twitter, permet aux adversaires de se cacher plus facilement dans le bruit attendu. Ces sites agissement comme un mécanisme qui peuvent offrir une couverture importante en raison de la probabilité que les hôtes d'un réseau communiquent déjà avec eux avant une compromission Les fournisseurs de services Web utilisent généralement le cryptage SSL/TLS, offrant ainsi aux adversaires un niveau de protection supplémentaire. Le groupe peut donc se cacher derrière un site populaire pour maintenir Command and Control.

https://attack.mitre.org/tactics/TA0011/

Indicators of Compromise (IoCs):

14. Quel est le SHA-256 de la version modifiée du malware TSPY64_UFINSTAL.ZCHD-A ? **(1 point)**

6395f8bc082b319159ef0418e90578351 511de07992280e0f400bc5cf1aa829f

15. Décrivez le comportement du fichier malveillant BKDR_YAHAMAM dans la phase de commande et de contrôle **(1 point)**

BKDR_YAHAMAM est généralement crypté alors intégré dans un fichier image. Une fois déchiffré, il est chargé et exécuté en mémoire par un fichier .DLL qui est enregistré en tant que service (TROJ_YAHAMAM). Il exfiltre les données des systèmes infectés, télécharge et télécharge des fichiers et dispose d'un shell distant. Il supprime également un composant rootkit nommé « usb.sys », détecté comme RTKT_HIDEPORT.ZTCA-XO. Le rootkit crée le service usb30 et cache les preuves de communication du port pour échapper à la détection et rester persistant.

BKDR_YAHAMAM crypte la communication C&C en utilisant la multiplication avec une clé de 1 octet. Les attaquants peuvent utilisez le "?" et les commandes « Aide » pour voir les différentes options proposées par la porte dérobée, comme indiqué dans son code. BKDR_YAHAMAM peut voler presque tout type de fichier sauvegardé dans un système infecté. Peut aussi tuer les processeurs, effaces fichiers et répertoires, etc…

https://documents.trendmicro.com/assets/wp/wp-operation-tropic-trooper.pdf