PAYSAGE GÉNÉRAL DES MENACES

TÉLÉCHARGEZ LE RAPPORT COMPLET EN ANGLAIS

Talos a observé plusieurs tendances majeures dans le paysage des menaces en 2022. En nous fondant sur des données télémétriques et des études de cas réalisées dans le cadre des missions Cisco Talos Incident Response (CTIR), nous avons remarqué que des hackers intégraient des versions piratées/fuitées d'outils de Read Teaming populaires en utilisant des fichiers binaires « living-off-the-land » (LoLBins), tels que PowerShell et Microsoft PS Exec. Nous avons également noté une augmentation des attaques par clé USB.

OUTILS À DOUBLE USAGE

Le développement d'outils malveillants est gourmand en ressources et permet potentiellement de suivre un hacker. Pour éviter ces coûts élevés et renforcer leur anonymat, de nombreux cybercriminels se tournent vers des frameworks offensifs et de Red Teaming afin de prendre en charge un large éventail d'actions tout au long du cycle de vie des attaques.

Cobalt Strike reste une option populaire auprès des acteurs de la cybercriminalité (Figure 1). Prisé des hackers, cet outil légitime de protection du réseau et d'émulation des menaces offre un large éventail de fonctionnalités, notamment la reconnaissance, les activités de post-exploitation et diverses simulations d'attaque.

Talos et la communauté de la cybersécurité font face à Cobalt Strike depuis des années, concevant en permanence des systèmes de détection plus robustes et plus performants. Tout au long de l'année, nous avons également vu des hackers s'adapter à ces développements en ayant recours à d'autres frameworks offensifs comme Sliver et Brute Ratel (Figure 2).

Talos a par ailleurs découvert deux modèles offensifs distincts développés par les hackers à leurs propres fins. Il s'agit de « Manjusaka » et d'« Alchimist ». Ce dernier est déjà largement exploité, et bien que nous n'ayons pas observé d'utilisation généralisée de Manjusaka au moment de la rédaction de ce document, les hackers du monde entier peuvent potentiellement l'adopter.

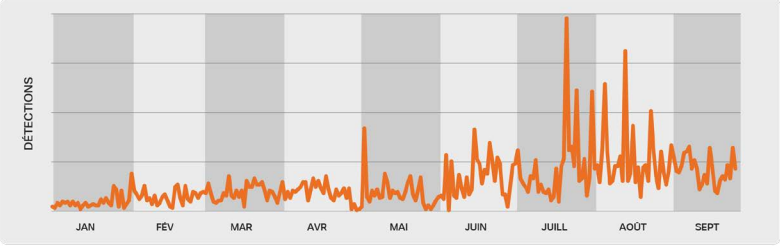

Figure 1. *Détections Cisco Secure Endpoint de l'utilisation de Cobalt Strike.*

Cobalt Strike

- Prisé des hackers, cet outil légitime de protection du réseau et d'émulation des menaces offre un large éventail de fonctionnalités, notamment la reconnaissance, les activités de post-exploitation et divers packages d'attaque.
- La balise est la charge utile de Cobalt Strike qui permet de générer des attaques et du trafic sortant via HTTP, HTTPS ou DNS. Les balises Cobalt Strike peuvent être comparées au produit de sécurité Meterpreter (qui fait partie du framework de Metasploit) et sont utilisées par les testeurs d'intrusion ainsi que les chercheurs en sécurité offensive lors de la fourniture de leurs services.

Brute Ratel

- Un outil de Red Teaming à la fois sophistiqué et légitime publié en 2020 en tant qu'outil de simulation d'attaque. Depuis, les hackers l'utilisent dans le but de faciliter les différentes étapes du cycle de vie des attaques.
- Brute Ratel est spécialement conçu pour éviter la détection par les solutions de détection et de réponse sur les terminaux (EDR, Endpoint Detection and Response) ou autres antivirus (AV).

Sliver

- Un framework de Red Teaming open source et un outil de simulation d'attaque pouvant être utilisés pour effectuer des tests de sécurité. Les implants Sliver sont compilés dynamiquement avec des clés de chiffrement asymétriques par binaire et prennent en charge C2 sur un certain nombre de protocoles (mTLS, HTTP, DNS).
- Les implants Sliver sont pris en charge sous MacOS, Windows et Linux. Sliver propose de nombreuses fonctionnalités, dont des charges utiles avec ou sans déploiement, la génération de code dynamique, des pivots sur les canaux (ou « pipes ») nommés, l'exécution d'assembly .NET en mémoire et bien plus encore.

Figure 2. *Comparatif des outils courants à double usage.*

PAYSAGE GÉNÉRAL DES MENACES

FICHIERS BINAIRES LIVING-OFF-THE-LAND

Couramment employés par les agresseurs, les LoLBins sont des utilitaires et des outils légitimes préinstallés dans un système d'exploitation. Étant donné qu'il s'agit d'outils intrinsèquement fiables exécutés pour les activités de routine, les responsables de la protection du réseau peuvent passer à côté d'attaques tirant profit des LoLBins lors de la surveillance des comportements malveillants. Nous continuons de voir des hackers faire appel à des outils et à des utilitaires légitimes à toutes les étapes d'une attaque afin de mener à bien leurs opérations.

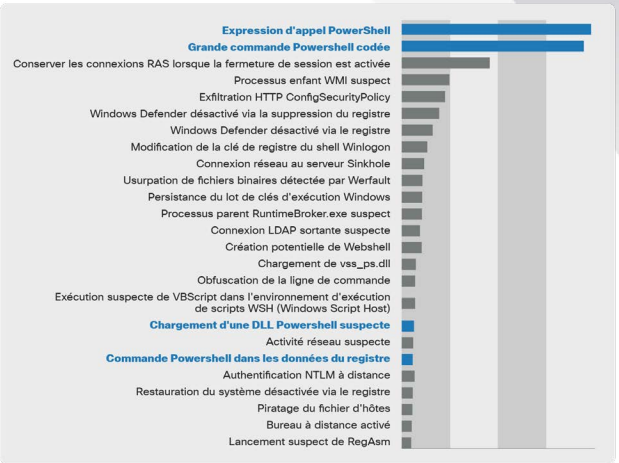

Figure 3. *Top 25 des signatures de protection comportementale les plus actives de Cisco Secure Endpoint.*

Selon nos données télémétriques, 4 des 25 signatures de protection comportementale les plus actives de Cisco Secure Endpoint sont liées à PowerShell. Cela illustre que les hackers utilisent constamment cet utilitaire Windows natif à des fins malveillantes (Figure 3). Les cybercriminels s'appuient couramment sur PowerShell pour prendre en charge un large éventail d'activités, notamment l'installation de logiciels publicitaires comme ChromeLoader, le téléchargement de mineurs de cryptomonnaie ou encore l'exploitation des vulnérabilités de logiciels tels qu'Elasticsearch.

commonly use PowerShell to support a broad range of activities, including installing adware like ChromeLoader, downloading cryptocurrency miners, or exploiting vulnerabilities in software such as Elasticsearch.

ATTAQUES PAR CLÉ USB

La propagation des programmes malveillants via les périphériques de stockage amovibles remonte à l'époque des lecteurs de disquettes. Tout au long de 2022, Talos a observé une légère augmentation des détections dans Cisco Secure Malware Analytics pour divers comportements associés aux clés USB et aux disques externes, mettant ainsi en évidence l'utilisation continue par les hackers de cette tactique ancienne, mais efficace. Ces comportements incluent l'écriture d'exécutables ou la définition d'attributs de fichier masqués sur une clé USB afin qu'ils ne soient pas détectés (Figures 4 et 5).

La hausse des détections s'explique en partie par le programme malveillant Raspberry Robin, qui se propage entre les périphériques via des clés USB partagées. Cependant, des groupes d'APT ont également montré la capacité d'utiliser l'accès aux clés USB dans le cadre de leurs attaques.

2022 nous a appris que les attaques par clé USB étaient de retour et que les hackers s'adaptaient au fait que les entreprises détournent leur attention des anciens vecteurs de menaces.

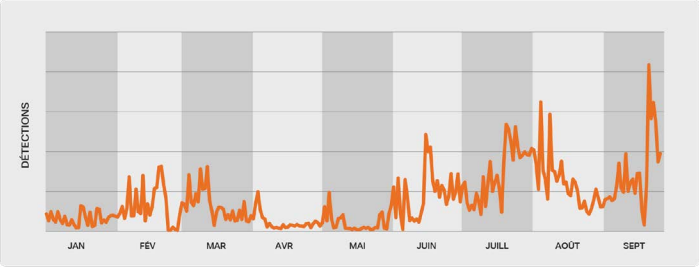

Figure 4. *Détections Cisco Secure Malware Analytics des exécutables écrits sur une clé USB.*

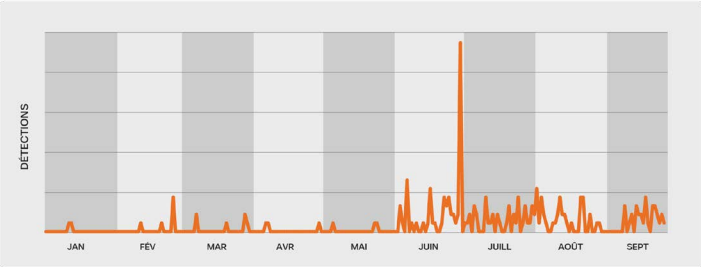

Figure 5. *Détections Cisco Secure Malware Analytics de la définition d'attributs de fichier masqués sur une clé USB.*

