Talos

REVUE DE L'ANNÉE 2022

MENACES PERSISTANTES AVANCÉES

TÉLÉCHARGEZ LE RAPPORT COMPLET EN ANGLAIS

Les menaces persistantes avancées (APT, Advanced Persistent Threats) associées à un État se sont adaptées à l'évolution du contexte géopolitique en 2022. Cisco Talos a observé plusieurs campagnes offensives liées à différents groupes en provenance de Russie, d'Iran, de Chine, de Corée du Nord et d'autres pays du sous-continent indien. Ces groupes se sont livrés à diverses activités nuisibles, notamment l'espionnage, le vol de propriété intellectuelle ainsi que le déploiement de programmes malveillants aux effets dévastateurs. Voici les principales tendances qui se sont dégagées :

- Diffusion de nouveaux programmes malveillants personnalisés et de nouvelles variantes de menaces déjà connues.
- Exploitation des vulnérabilités connues du public, telles que les utilitaires Log4j.
- Mise en place de nouveaux outils et comportements pour échapper à la détection.
- Augmentation de l'activité des APT dans le cadre de nos missions Cisco Talos Incident Response (CTIR), dont le groupe de l'État iranien MuddyWater et plusieurs menaces affiliées à la Chine.

Russie

Il s'agit là des groupes d'État les plus actifs observés par Talos en 2022, avant que la Russie n'envahisse l'Ukraine en février.

Fancy Bear

Ce groupe de hackers est suspecté d'entretenir des liens avec le renseignement militaire russe (GRU).

- A utilisé des tactiques, techniques et procédures (TTP) similaires à celles identifiées dans « WhisperGate », un virus à l'origine d'une attaque destructrice par wiper perpétrée plusieurs semaines avant l'invasion.

Gamaredon

Ce groupe de cyberespionnage est lourdement soupçonné d'être soutenu par le gouvernement russe en Crimée.

- A lancé une vaste campagne de spear phishing (hameçonnage ciblé) visant à infecter les administrations ukrainiennes via des programmes malveillants qui dérobent des données pour exfiltrer les éléments sensibles.

Turla

Certains attribuent l'activité de ce groupe russe au FSB, le Service fédéral de sécurité de la Fédération de Russie.

- Reste engagé dans le cadre d'opérations très ciblées contre des entités publiques et privées de pays de l'OTAN et de l'ex-URSS en utilisant des points d'eau, des campagnes de spear phishing, des techniques d'ingénierie sociale, l'exploitation de vulnérabilités connues ainsi que des portes dérobées personnalisées, comme Crutch et Gazer.

Iran

Ces groupes mènent des cyberattaques à l'échelle mondiale avec pour objectif principal de voler la propriété intellectuelle et de collecter des informations. Ils conservent probablement les moyens techniques de déployer des ransomwares et autres programmes malveillants destructeurs.

MuddyWater

En nous fondant sur un examen complet, nous pensons que MuddyWater se compose de plusieurs sous-groupes chargés de s'attaquer à un pays ou une à région spécifique.

- Bien qu'ils aient recours à des TTP uniques afin de compromettre les cibles désignées, ces sous-groupes partagent également des programmes malveillants, des outils et des procédures jugés efficaces dans d'autres campagnes.
- Cette année, MuddyWater a tenté de compromettre des entités gouvernementales turques et déployé un nouvel implant nommé SloughRAT au Moyen-Orient.
- Nos interventions CTIR ont révélé l'utilisation d'un large éventail d'outils de post-exploitation et de porte dérobée. Même après la remédiation, nous avons constaté la présence de portes dérobées supplémentaires dans l'infrastructure serveur ainsi que le recours à Impacket pour exécuter des services à distance et des outils d'attaque.

MENACES PERSISTANTES AVANCÉES

Chine

Les acteurs d'APT en lien avec la Chine ont ciblé des entités dans un grand nombre de secteurs d'activité, volant la propriété intellectuelle et les données sensibles des industries clés et autres infrastructures essentielles qui s'alignent sur les objectifs stratégiques du pays.

Mustang Panda

Ce groupe est connu pour exploiter les événements liés à l'actualité en vue de compromettre les victimes, en particulier aux États-Unis et en Asie.

- A tiré parti du conflit entre la Russie et l'Ukraine pour cibler des entreprises européennes (y compris des entités russes) dans le cadre d'une vaste campagne d'espionnage.

Deep Panda

Ce groupe de cyberespionnage d'État cible les gouvernements, l'armée, les services publics et les organismes financiers.

- A exploité les vulnérabilités de Log4j pour compromettre un établissement de santé, puis installé une porte dérobée personnalisée afin d'établir une menace persistante.

Corée du Nord

Talos a observé une activité prolifique des hackers liés au gouvernement nord-coréen, en particulier le Lazarus Group, lequel soutient des objectifs politiques et de sécurité nationale par le biais de l'espionnage, du vol de données ou encore d'attaques perturbatrices.

Lazarus Group

Ce groupe est connu pour utiliser des programmes malveillants personnalisés et se livrer à des vols d'argent à grande échelle.

- A exploité les vulnérabilités de Log4j sur les serveurs publics VMware Horizon afin de cibler les entreprises du secteur de l'énergie opérant aux États-Unis, au Canada et au Japon.
- Talos a découvert un nouveau cheval de Troie d'accès à distance (que nous avons nommé MagicRAT) ainsi que d'autres implants personnalisés utilisés pour la reconnaissance interne et le vol de données.

Asie du Sud

Talos a suivi de nombreuses campagnes qui ciblaient principalement des entités en Inde. La majorité d'entre elles semble provenir d'acteurs liés à l'État pakistanais, un ennemi de longue date.

Transparent Tribe

- Ce groupe cible essentiellement les entités gouvernementales et militaires, ainsi que les organisations affiliées en Afghanistan et en Inde. Dans ce qui semble être une expansion de son modèle de victimologie standard, il a commencé à s'attaquer aux étudiants et aux établissements d'enseignement en Inde.

Bitter APT

- Le principal objectif de ce groupe est axé autour de l'espionnage. Il a ciblé des gouvernements ainsi que des entités d'Asie du Sud et de l'Est à travers une longue campagne déployée dans les secteurs de l'énergie et de l'ingénierie.

Autres APTs

- Plus tôt cette année, Talos a publié une étude qui laisse croire que des acteurs d'APT opérant en Asie du Sud auraient réutilisé involontairement du code VBA écrit par différents groupes malveillants.

