cisco | Talos

JAHRESRÜCKBLICK 2022

ADVANCED PERSISTENT THREATS

LADEN SIE HIER DEN VOLLSTÄNDIGEN ENGLISCHEN BERICHT HERUNTER

Staatlich geförderte oder durch Staaten in Auftrag gegebene Advanced Persistent Threats (APTs) haben sich 2022 an die sich verändernde geopolitische Landschaft angepasst. Cisco Talos beobachtete mehrere offensive Cyberkampagnen in Verbindung mit unterschiedlichen Gruppen aus Russland, dem Iran, China, Nordkorea und Ländern des indischen Subkontinents. Diese Gruppen waren an einer Vielzahl schädlicher Aktivitäten beteiligt, darunter Spionage, Diebstahl von geistigem Eigentum und Verbreitung gefährlicher Malware. Zu den wichtigsten beobachteten Trends zählen:

- Verbreitung neuer, speziell entwickelter Malware und aktualisierter Varianten bereits bekannter Malware
- Ausnutzung öffentlich bekannter Schwachstellen wie Log4j-Dienstprogramme
- Aktualisierung von Tools und Verhaltensmustern, um die Erkennung zu umgehen
- Zunehmende APT-Aktivität in unseren CTIR-Projekten (Cisco Talos Incident Response), darunter die vom Iran gesponserte MuddyWater-Gruppe und mehrere mit China im Zusammenhang stehende APTs.

Russland

Die aktivsten staatlich geförderten Gruppen, die Talos 2022 beobachtete, insbesondere im Vorfeld des russischen Überfalls auf die Ukraine im Februar.

Fancy Bear

Eine mutmaßliche Einheit des russischen Militärgeheimdienstes GRU (Glawnoje Raswedywatelnoje Uprawlenije, Hauptverwaltung für Aufklärung).

- Anwendung von Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTPs), die denen von WhisperGate ähneln, einem zerstörerischen Wiper-Angriff mehrere Wochen vor der Invasion.

Gamaredon

Allgemein wird vermutet, dass es sich um eine Gruppe von durch die Regierung unterstützten Akteuren auf der Krim handelt.

- Start einer massiven Spear-Phishing-Kampagne zur Infizierung von Usern der ukrainischen Regierung mit Malware, die Informationen stiehlt, um an vertrauliche Daten zu gelangen.

Turla

Russischer Herkunft, wird teilweise dem russischen Inlandsgeheimdienst FSB zugeschrieben.

- Ist weiterhin sehr gezielt gegen Einrichtungen des öffentlichen und privaten Sektors in NATO-Ländern und Nachfolgestaaten der Sowjetunion tätig und nutzt dabei Watering Holes, Spear-Phishing-Kampagnen, Social-Engineering-Techniken, bekannte Schwachstellen und benutzerdefinierte Backdoors wie Crutch und Gazer.

Iran

Diese Gruppen führen Cyberangriffe weltweit durch, mit dem Hauptziel, geistiges Eigentum zu stehlen und Informationen zu sammeln. Sie verfügen wahrscheinlich über die technischen Mittel, um Ransomware und andere schädliche Malware bereitzustellen.

MuddyWater

Basierend auf einer umfassenden Überprüfung gehen wir davon aus, dass MuddyWater aus mehreren Untergruppen besteht, die mit der Ausrichtung auf ein bestimmtes Land oder eine bestimmte Region beauftragt sind.

- Jede MuddyWater-Untergruppe verwendet einzigartige TTPs, um ihre designierten Ziele zu kompromittieren, allerdings nutzen sie Malware, Tools und Verfahren, die in anderen regionalen Kampagnen als effektiv gelten, auch übergreifend.
- In diesem Jahr versuchte MuddyWater, die türkische Regierung zu kompromittieren, und setzte im Nahen Osten ein neues Implantat namens SloughRAT ein.
- Basierend auf CTIR-Interaktionen haben wir die Verwendung zahlreicher Backdoor- und Post-Exploit-Tools beobachtet. Sogar nach der Behebung fanden wir zusätzliche Backdoors in der Serverinfrastruktur sowie Hinweise auf die Verwendung von Impacket für die Ausführung von Remote-Services und Angriffstools.

ADVANCED PERSISTENT THREATS

China

Die mit China im Zusammenhang stehenden APT-Akteure zielten auf Unternehmen aus den verschiedensten Branchen ab und stahlen geistiges Eigentum und vertrauliche Daten aus wichtigen Branchen und kritischen Infrastruktursektoren, die mit den strategischen Zielen Chinas in Einklang stehen.

Mustang Panda

Nutzt aktuelle Ereignisse aus, um Opfer zu kompromittieren, insbesondere in den USA und Asien.

- Nutzte den russischen Krieg gegen die Ukraine, um in einer groß angelegten Spionagekampagne europäische Organisationen ins Visier zu nehmen, darunter auch russische.

Deep Panda

Eine separate staatlich geförderte Cyberspionagegruppe, die auf Regierungen, Militärs, Versorgungsunternehmen und Finanzorganisationen abzielt.

- Nutzte die Log4j-Schwachstelle, um eine Organisation des Gesundheitswesens zu kompromittieren, und stellte später eine benutzerdefinierte Backdoor bereit, um Persistenz herzustellen.

Nordkorea

Talos hat umfangreiche Aktivitäten von Bedrohungsakteuren beobachtet, die mit der nordkoreanischen Regierung, insbesondere der Lazarus Group, in Verbindung stehen und politische und nationale Sicherheitsziele durch Spionage, Datendiebstahl und disruptive Angriffe unterstützen.

Lazarus Group

Verwendet benutzerdefinierte Malware und ist an groß angelegtem Gelddiebstahl beteiligt.

- Nutzte Log4j-Schwachstellen in öffentlich zugänglichen VMware Horizon-Servern für Energieunternehmen aus den USA, Kanada und Japan.
- Talos entdeckte einen neuen Remote-Access-Trojaner, den wir MagicRAT, nannten, sowie andere benutzerdefinierte Implantate, die für interne Aufklärung und Datendiebstahl verwendet wurden.

Südasien

Talos verfolgte zahlreiche Kampagnen, die in erster Linie auf Unternehmen in Indien abzielten. Die meisten scheinen von mit dem Staat zusammenhängenden Akteuren in Pakistan zu stammen, einem langjährigen Gegner in der Region.

Transparent Tribe

- Zielt vorwiegend auf Regierungs- und Militärunternehmen sowie angeschlossene Organisationen in Afghanistan und Indien ab. Die Gruppe begann, sich auf Studierende und Bildungseinrichtungen in Indien zu konzentrieren, was auf eine Erweiterung ihres bisherigen Opferkreises hinweist.

Bitter APT

- Das Hauptziel dieser Gruppe scheint Spionage zu sein. In einer langfristig angelegten Kampagne zielte sie auf süd- und ostasiatische Regierungen und Unternehmen aus den Bereichen Energie und Technik ab.

Andere APTs

- Zu Beginn des Jahres veröffentlichte Talos eine Studie, welche die Vermutung nahelegte, dass mehrere in Südasien tätige APT-Akteure VBA-Code, der von verschiedenen Bedrohungsgruppen geschrieben wurde, möglicherweise unbeabsichtigt wiederverwendet hatten.