ALLGEMEINE BEDROHUNGSLANDSCHAFT

LADEN SIE HIER DEN VOLLSTÄNDIGEN ENGLISCHEN BERICHT HERUNTER

Talos beobachtete 2022 mehrere wichtige Trends in der gesamten Bedrohungslandschaft. Basierend auf Telemetriedaten und Case Studys bei Cisco Talos Incident Response-Projekten haben wir beobachtet, dass Angreifer gecrackte/geleakte Versionen gängiger Red Team-Tools integrieren, Living-off-the-Land-Binärdateien (LoLBins) wie PowerShell und Microsoft PS Exec verwenden sowie zunehmend USB-Angriffe durchführen.

TOOLS MIT MEHREREN EINSATZBEREICHEN

Die Entwicklung schädlicher Tools ist ressourcenintensiv und ermöglicht unter Umständen die Nachverfolgung eines Angreifers. Um diese hohen Kosten zu umgehen und eine zusätzliche Anonymitätsebene zu schaffen, greifen viele Angreifer zu offensiven und Team-basierten Frameworks, um während eines Angriffs unterschiedliche Aktionen zu unterstützen.

Cobalt Strike bleibt weiterhin eine beliebte Option für Cyber-Bedrohungsakteure **(Abbildung 1)**. Es handelt sich um ein legitimes Netzwerkverteidigungstool mit Fähigkeiten zur Bedrohungsemulation und einer Reihe weiterer Funktionen, darunter Aufklärung, Maßnahmen nach einem Angriff und verschiedene Angriffssimulationen, was es zu einem hochfunktionellen Tool für Angreifer macht.

Talos und die Security-Community beschäftigen sich seit Jahren mit Cobalt Strike und entwickeln kontinuierlich bessere und robustere Erkennungsmöglichkeiten. Im Laufe des Jahres erlebten wir auch, wie sich Bedrohungsakteure an diese Entwicklungen anpassten, indem sie sich zusätzlichen offensiven Frameworks wie Sliver und Brute Ratel zuwandten **(Abbildung 2)**.

Darüber hinaus entdeckte Talos zwei separate Angriffs-Frameworks, die von Angreifern für ihre eigenen Zwecke entwickelt wurden: „Manjusaka“ und „Alchimist“. Alchimist ist bereits in Umlauf, und obwohl wir bis zur Erstellung dieses Dokuments noch keine weit verbreitete Nutzung von Manjusaka beobachtet haben, hat es das Potenzial, von Bedrohungsakteuren weltweit übernommen zu werden.

LIVING-OFF-THE-LAND-BINÄRDATEIEN

Living-off-the-Land-Binärdateien (LoLBins) sind legitime Dienstprogramme und Tools, die auf einem Betriebssystem vorinstalliert sind und

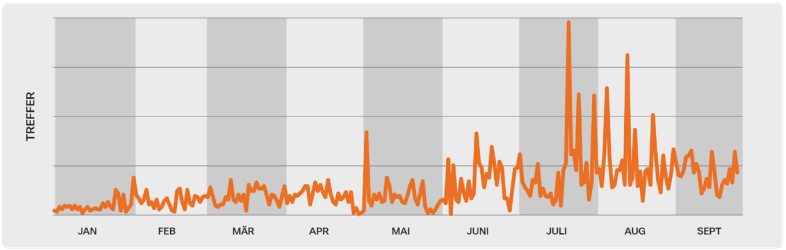

***Abbildung 1.** Cisco Secure Endpoint-Erkennungen bei Verwendung von mit Cobalt Strike benannten Pipes.*

Cobalt Strike

- Ein legitimes Netzwerkverteidigungstool mit Fähigkeiten zur Bedrohungsemulation und einer Reihe weiterer Funktionen, darunter Aufklärung, Maßnahmen nach einem Angriff und verschiedene Angriffspakete, was es zu einem hochfunktionellen Tool für Angreifer macht.
- Beacon ist die Payload von Cobalt Strike für die Generierung von Angriffen und die Erstellung von ausgehendem Traffic über HTTP, HTTPS oder DNS. Cobalt Strike-Beacons können mit Meterpreter verglichen werden, das Teil des Metasploit-Frameworks ist, und für Penetrationstests und offensive Sicherheitsforschung bei der Bereitstellung der Services verwendet werden.

Brute Ratel

- Ein legitimes, hochentwickeltes Red-Teaming-Tool, das 2020 als Tool zur Angriffssimulation veröffentlicht wurde. Es wird seitdem von Bedrohungsakteuren genutzt, um verschiedene Phasen des Angriffslebenszyklus zu vereinfachen.
- Brute Ratel wurde speziell entwickelt, um die Erkennung durch Endpoint Detection and Response- (EDR) und Antivirus- (AV)-Lösungen zu vermeiden.

Sliver

- Ein Open-Source-Red-Teaming-Framework und Tool zur Angriffssimulation, das für Sicherheitstests verwendet werden kann. Die Implantate von Sliver werden dynamisch mit asymetrischen Verschlüsselungsschlüsseln pro Binärdatei kompiliert und unterstützen C2 über eine Reihe von Protokollen (mTLS, HTTP, DNS).
- Implantate von Sliver werden unter MacOS, Windows und Linux unterstützt. Sliver hat zahlreiche Funktionen, darunter gestufte und stufenlose Payloads, dynamische Codegenerierung, benannte Pipe-Pivots, Ausführung von InMemory.NET-Assemblies und vieles mehr.

***Abbildung 2.** Vergleich gängiger Tools mit mehreren Einsatzbereichen.*

ALLGEMEINE BEDROHUNGSLANDSCHAFT

häufig von Angreifern missbraucht werden. Da es sich dabei um von Natur aus vertrauenswürdige Tools für Routineaufgaben handelt, könnten Netzwerkverteidigern bei der Überwachung auf schädliches Verhalten Angriffe mit LoLBins entgehen. Wir beobachten weiterhin, dass Angreifer in allen Phasen eines Angriffs legitime Tools und Dienstprogramme nutzen, um ihre Tätigkeiten zu unterstützen.

Laut unserer Telemetrie hängen 4 der 25 aktivsten Cisco Secure Endpoint Behavioral Protection-Signaturen mit PowerShell zusammen, wodurch umso deutlicher wird, wie stark Angreifer für ihre schädlichen Zwecke von diesem nativen Windows-Dienstprogramm abhängig sind **(Abbildung 3)**. Angreifer nutzen PowerShell häufig, um eine Vielzahl von Aktivitäten zu unterstützen, darunter die Installation von Adware wie ChromeLoader, das Herunterladen von Kryptowährungs-Minern oder die Ausnutzung von Schwachstellen in Software wie Elasticsearch.

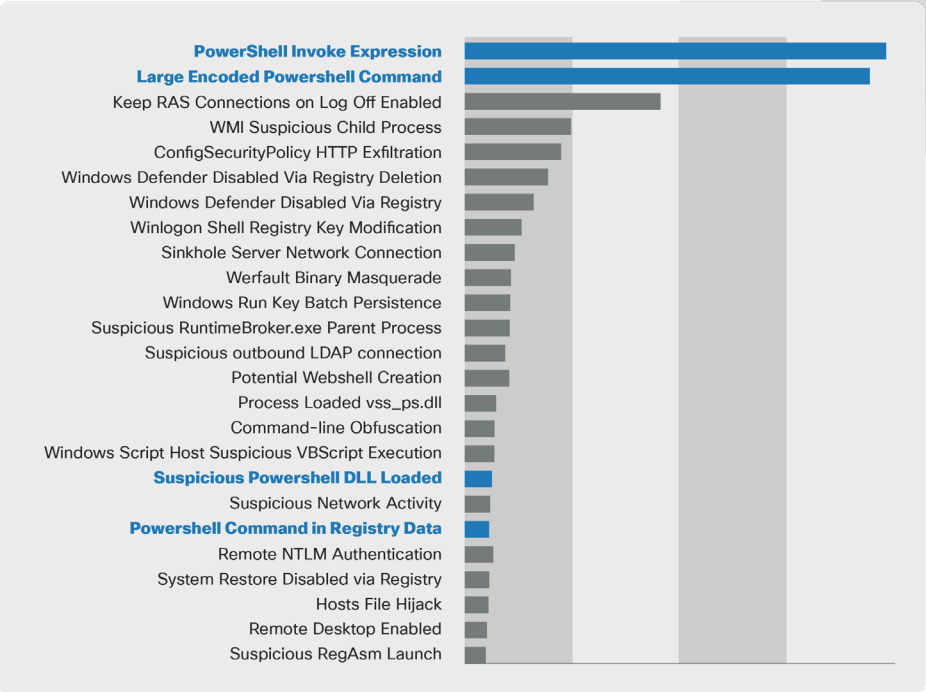

Abbildung 3. *Die 25 aktivsten Cisco Secure Endpoint Behavioral Protection-Signaturen.*

USB-BEDROHUNGEN

Die Verbreitung von Malware über Wechseldatenträger geht auf Diskettenlaufwerke zurück. Im Laufe des Jahres 2022 beobachtete Talos eine Zunahme der Erkennungen in Cisco Secure Malware Analytics für verschiedene Verhaltensweisen im Zusammenhang mit USB-Sticks und externen Laufwerken, was die anhaltende Nutzung dieser alten, aber effektiven Taktik durch Angreifer hervorhebt. Zu diesen Verhaltensweisen zählen ausführbare Dateien, die auf ein USB-Laufwerk geschrieben werden, oder das Festlegen versteckter Attribute für Dateien auf einem USB-Laufwerk, damit diese nicht erkannt werden **(Abbildungen 4 und 5)**.

Der Anstieg ist teilweise auf die Malware Raspberry Robin zurückzuführen, die sich über Geräte mit gemeinsam genutzten USB-Laufwerken ausbreitet. Allerdings wurde auch beobachtet, dass APT-Gruppen den Zugriff auf USB-Laufwerke als Teil ihrer Angriffe nutzten.

2022 hat uns gezeigt, dass USB-Angriffe zurückgekehrt sind und dass Angreifer ihre Taktik anpassen werden, um auszunutzen, dass Unternehmen ihre Aufmerksamkeit von älteren Angriffsvektoren abwenden.

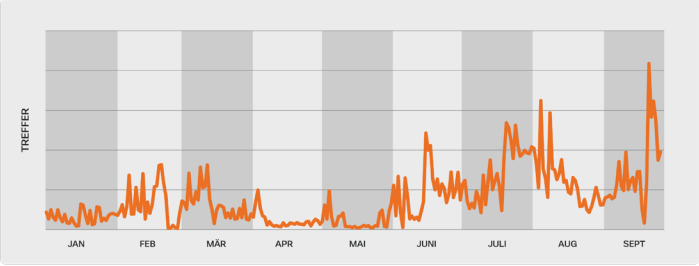

Abbildung 4. *Cisco Secure Malware Analytics-Erkennungen ausführbarer Dateien, die auf USB geschrieben wurden.*

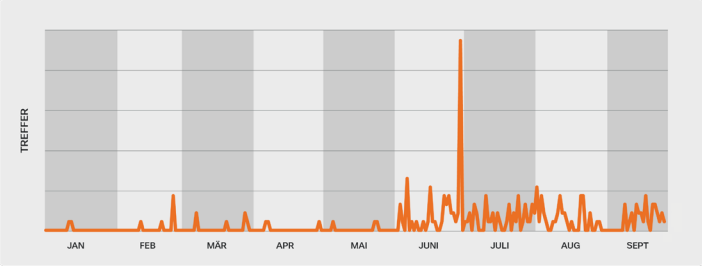

Abbildung 5. *Cisco Secure Malware Analytics-Erkennungen der Festlegung versteckter Attribute für Dateien auf einem USB-Gerät.*

