RANSOMWARE UND COMMODITY LOADER

LADEN SIE HIER DEN VOLLSTÄNDIGEN ENGLISCHEN BERICHT HERUNTER

RANSOMWARE-BEDROHUNGSLANDSCHAFT

Der Bereich Ransomware ist dynamisch und passt sich kontinuierlich an Veränderungen im geopolitischen Umfeld, Aktionen von Verteidigern und Bemühungen der Strafverfolgungsbehörden an, die 2022 an Umfang und Intensität zunahmen. Dies führt dazu, dass Gruppen sich umbenannten, den Betrieb einstellten oder neue strategische Partnerschaften schlossen. Cisco Talos beobachtete 2022 unterschiedliche damit zusammenhängende Trends.

Talos verfolgt mehr als ein Dutzend RaaS-Gruppen (Ransomware-as-a-Service) **(Abbildung 1)**. Basierend auf unseren Erkenntnissen war LockBit 2022 die aktivste Gruppe mit einem Anteil von über 20 Prozent an der Gesamtzahl der Opferbeiträge im Dark Web, dicht gefolgt von Hive und Black Basta. Diese Erkenntnisse deuten auf eine stärkere Demokratisierung von Ransomware-Angreifern hin, eine allgemeine Veränderung gegenüber den Vorjahren, in denen einige ausgewählte Gruppen die Landschaft monopolisiert hatten. Ransomware-Partner sind auch nicht mehr in Silos strukturiert, sondern arbeiten über mehrere Gruppen hinweg, in denen Akteure mit einzigartigen Fähigkeiten mehr Möglichkeiten haben, unterschiedliche Kampagnen und Organisationen zu unterstützen.

In der gesamten Community kam es zu stärkeren Spannungen, da der Krieg in der Ukraine viele Bedrohungsakteure dazu zwang, sich auf eine Seite des Konflikts zu stellen und ihre Operationen gegen pro-russische oder pro-ukrainische Ziele zu richten. Die RaaS-Gruppe Conti gehörte zu den lautesten und warnte, sie würde jeden angreifen, der versuchte, sich in die Invasion Russlands einzumischen. Eine Person mit Verbindungen zu Conti rächte sich an der Ransomware-Gruppe, indem sie Informationen preisgab, einschließlich des Quellcodes der Malware und interner Chats zwischen den Partnern. In einem anderen Fall wurde Talos auf die Offenlegung eines geleakten Builders für den Ransomware-Verschlüsseler LockBit 3.0 aufmerksam, der als „LockBitBlack“ bezeichnet wurde. Die verantwortliche Person ist ein mutmaßlicher LockBit-Entwickler, der laut LockBit behauptete, er sei mit der Zahlungsstruktur der Gruppe unzufrieden.

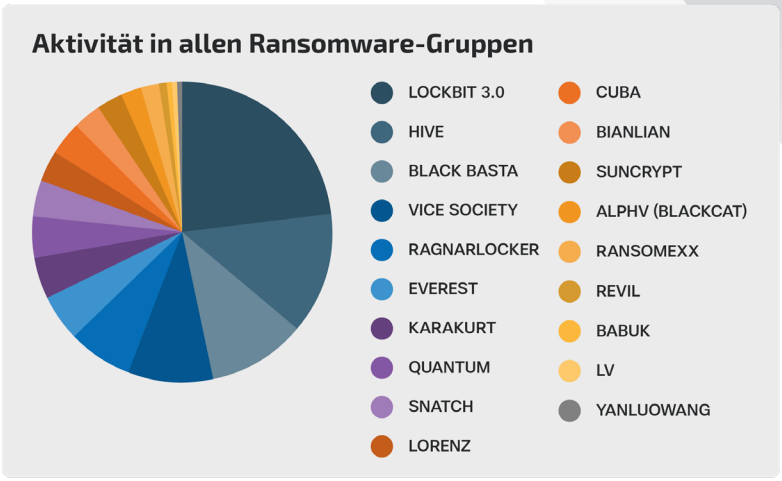

Abbildung 1. *Anzahl der Beiträge auf von Talos überwachten Ransomware-Datenleak-Websites, Januar–Oktober.*

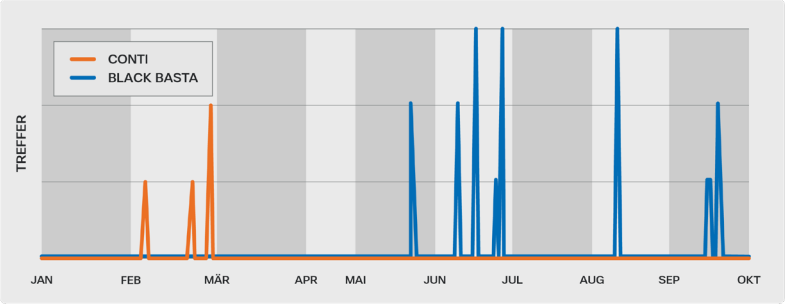

Abbildung 2. *Erkennung von Verhaltensindikatoren in Secure Malware Analytics für die Ransomware Conti und Registrierungsänderungen durch Black Basta.*

Diese Art von Spannungen führt häufig dazu, dass sich Ransomware-Gruppen neue Namen geben oder dass neue entstehen. Als Conti inaktiv wurde und seine Infrastruktur offline nahm, verzeichneten wir einen allgemeinen Rückgang der Erkennungsraten in unseren Telemetriedaten, aber kurz danach tauchte eine Conti-Gruppe mit dem neuen Namen „Black Basta“ auf. ForscherInnen gehen davon aus, dass die beiden Gruppen ähnliche Zahlungs- und Leaking-Websites und Kommunikationsstile haben **(Abbildung 2)**.

COMMODITY LOADER

Commodity Loader – kommerzielle Trojaner, die Malware der zweiten Stufe verbreiten – sind eine ständige Bedrohung, die weiterhin globale Auswirkungen hat. Ursprünglich als Banking-Trojaner entwickelt, der darauf abzielte, sich an den Unternehmen zu bereichern, haben sie sich im Laufe der Zeit an umfassendere Sicherheitskontrollen angepasst und sich zu viel raffinierteren Bedrohungen entwickelt.

© 2023 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

RANSOMWARE UND COMMODITY LOADER

Sie fungieren heute in erster Linie als Loader mit modularen Funktionen, mit deren Hilfe Cyberkriminelle mit einer Reihe von Open-Source-Tools und neu entwickelter Malware arbeiten können. Die vier aktivsten Standard-Loader 2022 waren laut unserer Analyse mehrerer Netzwerk- und Endpunkt-Telemetriesätze Qakbot, Emotet, IcedID und Trickbot **(Abbildung 3)**.

Unsere Telemetrie hat Aktivitäten im Zusammenhang mit Trickbot erkannt, allerdings gehen wir davon aus, dass ein Großteil davon wahrscheinlich alte, infizierte Endpunkte erkannt hat, da die Malware-Betreiber seit Anfang 2022 inaktiv sind. Auf ähnliche Weise bleibt Emotet, obwohl es weiterhin verwendet wird, deutlich weniger aktiv als vor der Beseitigung des Botnets Anfang Januar 2021 durch die Strafverfolgungsbehörden. Andere Malware, wie Qakbot und IcedID, hat diese Lücke geschlossen und wird immer beliebter.

Ein übergreifender Trend, den wir 2022 beobachteten, ist, dass Betreiber häufiger Qakbot, Emotet und IcedID mit ISO-, ZIP- und LNK-Dateitypen einsetzen, was wahrscheinlich die Bemühungen von Microsoft zur Blockierung von Dokumenten mit Makros umgehen würde. Außerdem beobachtete Talos, dass Qakbot-, Emotet- und IcedID-Betreiber schädliche Payloads mithilfe von Living-off-the-Land-Binärdateien (LoLBins) in Opferumgebungen herunterladen und starten. In einigen Fällen verfeinerten die User von Qakbot und Emotet ihre Angriffssequenz, indem sie mit verschiedenen LoLBins experimentierten, um ihre Chancen zu verbessern, innerhalb eines Unternehmens unentdeckt zu bleiben.

Unsere Telemetrie hat Aktivitäten im Zusammenhang mit Trickbot erkannt, allerdings gehen wir davon aus, dass ein Großteil davon wahrscheinlich alte, infizierte Endpunkte erkannt hat, da die Malware-Betreiber seit Anfang 2022 inaktiv sind. Auf ähnliche Weise bleibt Emotet, obwohl es weiterhin verwendet wird, deutlich weniger aktiv als vor der Beseitigung des Botnets Anfang Januar 2021 durch die Strafverfolgungsbehörden. Andere Malware, wie Qakbot und IcedID, hat diese Lücke geschlossen und wird immer beliebter.

Eine detaillierte Überprüfung der einzelnen Commodity Loader ist im vollständigen Bericht verfügbar.

Commodity Loader

	Qakbot	IcedID	Emotet	Trickbot
Aliase	Quackbot, Qbot, Pinkslipbot	BokBot	Geodo, Heodo	---
Verbindungen	Standard-Malware, die wahrscheinlich von eurasischen Cyberkriminellen entwickelt wurde	Unbekannt	Standard-Malware, die von Mummy Spider entwickelt wurde, einer mit Russland in Verbindung stehender Gruppe von Cyberkriminellen	Standard-Malware, die von Wizard Spider entwickelt wurde, einer mit Russland in Verbindung stehender Gruppe von Cyberkriminellen
Aktiv seit	2007	2014	2017	2016

Ziele

- Erstmaliger Zugriff und Herstellung von Persistenz, um weitere Eindringversuche zu erleichtern.
- Verbreitung von Malware der nächsten Stufe, einschließlich Ransomware.

Opferkreis

- Zielgruppe sind alle Branchen weltweit.
- Seit dem Russland-Ukraine-Krieg drohte Trickbot mit Vergeltungsmaßnahmen für vermeintliche Angriffe gegen das russische Volk.

Nennenswerte TTPs

- Phishing, Malspam, Social Engineering, Ausnutzung von Schwachstellen, Datendiebstahl, z. B. Finanzdaten und Anmeldeinformationen, und Verbreitung von Würmern.
- Hochgradig modular, sodass Betreiber eine Vielzahl von Angriffen durchführen können.

Malware und Tools

- Die Malware-Varianten stellen verschiedene andere Malware-Familien, einschließlich einander gegenseitig, bereit und werden von diesen bereitgestellt.
- In verschiedenen Phasen des Angriffslebenszyklus werden kommerzielle Tools wie Cobalt Strike sowie LoLBins verwendet.

Abbildung 3. *Bedrohungsmatrix für Commodity Loader.*

© 2023 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. | talosintelligence.com