Die Ökonomie der Erpressung

Das neue Geschäftsmodell mit Ransomware

Cyber Signals
August 2022

Angriffe mit Ransomware unter Ausnutzung von Konfigurationsfehlern

Mehr als 80 Prozent der Ransomware-Attacken lassen sich auf typische Konfigurationsfehler an Software oder Geräten zurückführen.[1]

Einleitung

Die geheim organisierte Ransomware-Ökonomie ermutigt Cyberkriminelle

Auch wenn Ransomware weiterhin für Schlagzeilen sorgt, handelt es sich letztlich doch um ein relativ kleines zusammenhängendes Ökosystem von Akteur*innen, die diesen Bereich der Cybercrime-Wirtschaft antreiben. Die Spezialisierung und Konsolidierung in dieser Cybercrime-Ökonomie haben dazu geführt, dass sich Ransomware-as-a-Service (RaaS) zu einem dominanten Geschäftsmodell entwickelt hat. Es ermöglicht einer größeren Bandbreite von Kriminellen Ransomware einzusetzen – unabhängig von ihren technischen Kenntnissen.

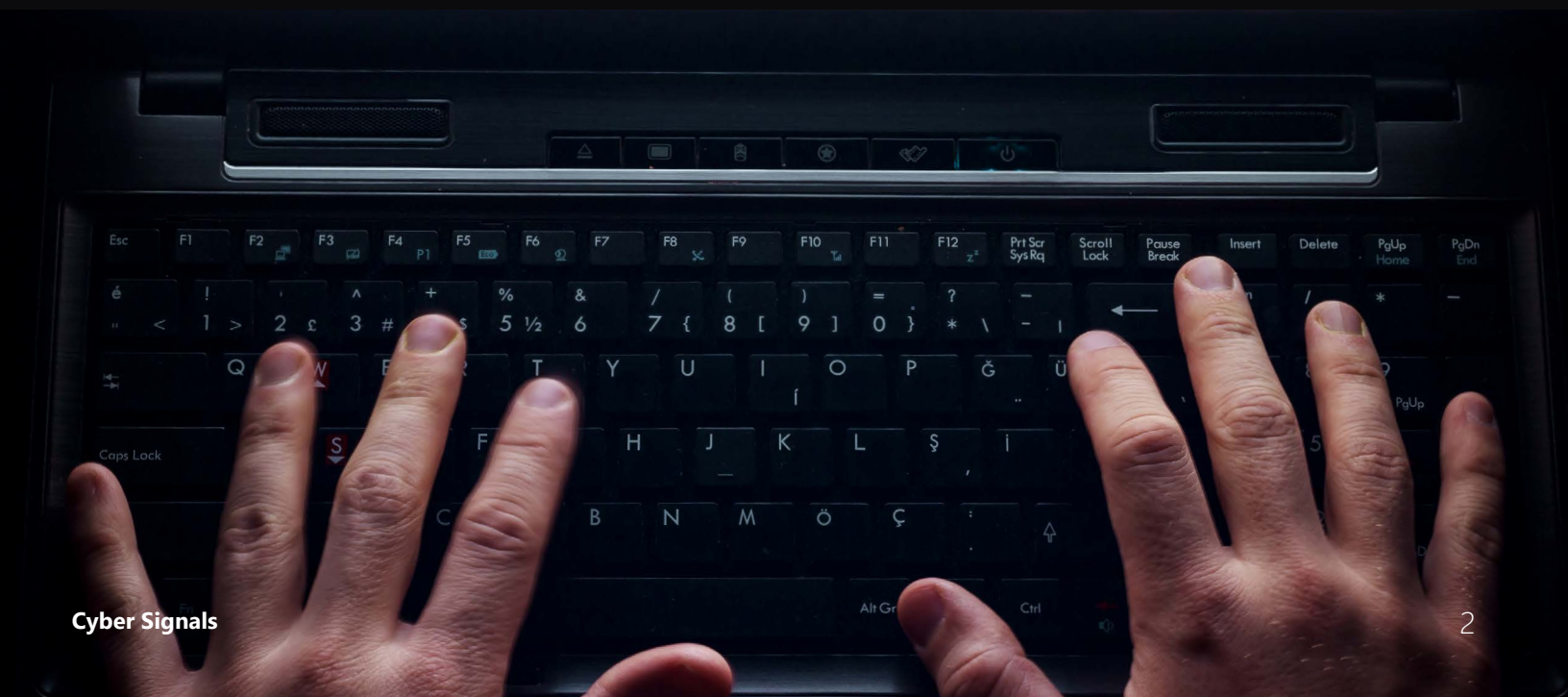
Wir alle sind Verteidiger*innen der Cybersicherheit.

Security Snapshot

Microsofts Digital Crimes Unit (DCU):
Zwischen Juli 2021 und Juni 2022 wurden mehr als 531.000 Phishing-URLs und 5.400 Phishing-Kits entfernt, wodurch sich über 1.400 gefährliche E-Mail-Konten identifizieren und schließen ließen, die zum Sammeln gestohlener Kundendaten verwendet worden waren.[1]

E-Mail-Bedrohungen:
Die durchschnittliche Zeit, die vergeht, bis Angreifer*innen auf private Daten einer Person zugreifen, wenn diese Opfer einer Phishing-E-Mail geworden ist, beträgt eine Stunde und 12 Minuten.[1]

Endpunkt-Bedrohungen:
Die durchschnittliche Zeit, bis Angreifer*innen damit beginnen sich innerhalb des Unternehmensnetzwerks zu bewegen, nachdem ein Gerät kompromittiert worden ist, beträgt eine Stunde und 42 Minuten.[1]



Neues Geschäftsmodell bietet Verteidiger*innen neue Einblicke

So wie viele Branchen aus Effizienzgründen auf Gig-Arbeiter*innen umgestellt haben, vermieten oder verkaufen auch Cyberkriminelle ihre Ransomware-Tools für einen Anteil am Gewinn, anstatt selbst die Attacken auszuführen.

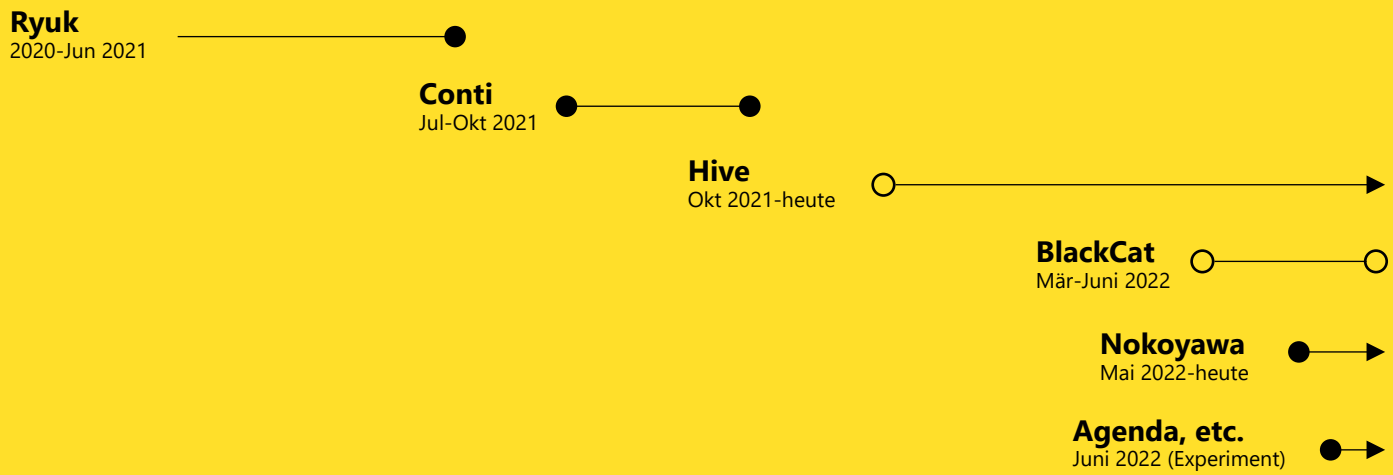
Die Ransomware-as-a-Service-Wirtschaft ermöglicht es Cyberkriminellen, sich Zugang zu den Payloads von Ransomware und Datenlecks sowie zur Zahlungsinfrastruktur zu kaufen. Die Ransomware-"Gangs" sind in Wahrheit RaaS-Programme wie Conti oder REvil, die von vielen verschiedenen Akteur*innen genutzt werden, die zwischen RaaS-Programmen und -Payloads hin und her wechseln.

RaaS senkt die Einstiegshürde und verschleiert die Identität der Angreifer*innen, die hinter den Lösegeldforderungen stehen. Einige der Programme haben mehr als 50 „Affiliates" also Partner, wie sie die Nutzer*innen nennen, die mit unterschiedlichen Tools, Techniken und Zielen an dem Service partizipieren. So wie jede Person, die ein Auto hat, für einen Mitfahrdienst unterwegs sein kann, ist auch jede Person in der Lage, die über einen Laptop und eine Kreditkarte verfügt und bereit ist, im Dark Web nach Penetrationstest-Tools oder gebrauchsfertiger Malware zu suchen, sich dieser Wirtschaft anzuschließen.

Diese Industrialisierung der Internetkriminalität hat spezialisierte Rollen hervorgebracht, wie z. B. die des Access-Brokers, der den Zugang zu Netzwerken verkauft. An einer einzigen Kompromittierung sind während der verschiedenen Phasen des Eindringens oft mehrere Cyberkriminelle beteiligt.

RaaS-Kits lassen sich leicht im Dark Web finden und werden genauso beworben wie sonstige Waren im Internet.

Zeitverlauf der DEV-0237 Payloads von Ransomware



Quelle: Microsoft 365 Defender Threat Intelligence Team und Microsoft Threat Intelligence Center (MSTIC)

Briefing zur Bedrohungslage

RaaS-Kits können Kundenservice-Support, Angebotspakete, Bewertungen von Nutzer*innen, Foren und andere Funktionen umfassen.

Cyberkriminelle können einen festen Preis für ein RaaS-Kit zahlen. Andere Gruppen, die RaaS im Rahmen eines Partnerschaftsmodells vertreiben, streichen wiederum einen Prozentsatz des Profits ein.

Bei Ransomware-Angriffen werden Entscheidungen auf der Grundlage von Netzwerkkonfigurationen getroffen, die sich bei jedem Opfer unterscheiden, auch wenn die Payload der Ransomware dieselbe ist. Ransomware bildet den Höhepunkt eines Angriffs, der auch die Exfiltration von Daten und andere Folgen nach sich ziehen kann. Da die Wirtschaft der Cyberkriminellen sehr stark vernetzt ist, können scheinbar nicht miteinander in Verbindung stehende Angriffe aufeinander aufbauen. Infostealer-Malware, die Passwörter und Cookies entwendet, wird mit weniger Strenge behandelt, aber Cyberkriminelle verkaufen diese Passwörter, um andere Angriffe zu ermöglichen.

Diese Attacken folgen einem Schema, bei dem der erste Zugriff über eine Malware-Infektion oder das Ausnutzen einer Schwachstelle erfolgt und anschließend Anmeldedaten gestohlen werden, um die Zugriffsrechte zu erhöhen und sich weiter auszubreiten. Durch die Industrialisierung können auch Angreifer*innen ohne besondere Kenntnisse oder spezielle Fähigkeiten Ransomware-Angriffe durchführen, die eine große Wirkung haben.

Seit der Abschaltung von Conti haben wir Verschiebungen in der Szene der Ransomware beobachtet. Einige Partner, die Conti einsetzten, wechselten zu Payloads aus etablierten RaaS-Ökosystemen wie LockBit und Hive, während andere gleichzeitig Payloads aus mehreren RaaS-Ökosystemen einsetzen.

Neue RaaS wie QuantumLocker und Black Basta füllen das Vakuum, das durch die Abschaltung von Conti entstanden ist. Da sich die meisten Berichte über Ransomware auf die Payloads und nicht auf die Akteur*innen konzentrieren, führt dieser Wechsel der Payloads bei Regierungen, Strafverfolgungsbehörden, Medien, Sicherheitsforscher*innen und Verteidiger*innen wahrscheinlich zu Verwirrung darüber, wer hinter den Angriffen steckt.

In der Berichterstattung über Ransomware mag es wie ein endlos wachsendes Problem erscheinen; in Wirklichkeit gibt es jedoch nur eine begrenzte Anzahl von Akteur*innen, die eine Reihe von Techniken einsetzen.

Empfehlungen:

Aufbau einer sorgfältigen Berechtigungsverwaltung: Entwickeln Sie eine logische Netzwerksegmentierung auf der Grundlage von Berechtigungen, die gemeinsam mit der Netzwerksegmentierung implementiert wird, um die Bewegungen von Angreifer*innen innerhalb eines Netzwerks einzuschränken.

Überprüfen Sie die Exposition von Anmeldeinformationen: Zu überprüfen, wie gefährdet die Anmeldeinformationen sind, ist entscheidend für das Verhindern von Ransomware-Angriffen und Cyberkriminalität im Allgemeinen. IT-Sicherheitsteams und Security Operations Centers (SOCs) können zusammenarbeiten, um administrative Berechtigungen einzuschränken und zu ermitteln, inwieweit Anmeldeinformationen gefährdet sind.

Verringern der Angriffsfläche: Indem bestimmte Regeln festgelegt werden, lässt sich die Angriffsfläche verkleinern und der erfolgreiche Einsatz gängiger Angriffstechniken bei Ransomware-Attacken lässt sich verhindern. Bei den beobachteten Attacken verschiedener mit Ransomware in Verbindung stehender Gruppierungen waren Unternehmen mit klar definierten Regeln in der Lage, Angriffe bereits im Anfangsstadium zu unterbinden und gleichzeitig Hands-on-Keyboard-Aktivitäten zu verhindern.

Doppelte Erpressung: Cyberkriminelle erweitern ihre Angriffsstrategie aus

Ransomware dient dazu, von einem Opfer eine Zahlung zu erpressen. Die meisten der aktuellen RaaS-Programme verbreiten auch gestohlene Daten, man spricht in diesem Falle von doppelter Erpressung. Da die Systemausfälle bei einer Attacke zu Gegenreaktionen führen und die Regierung die Betreiber von Ransomware zunehmend bei ihrem Tun stört, verzichten einige Gruppen auf Ransomware und widmen sich der Datenerpressung.

Zwei dieser Gruppen, die sich auf Erpressung spezialisiert haben, sind DEV-0537 (auch bekannt als LAPSUS$) und DEV-0390 (eine ehemalige Conti-Tochtergesellschaft). Die Eindringlinge von DEV-0390 starten ihre Angriffe mit Malware, verwenden aber legale Tools, um Daten zu exfiltrieren und Zahlungen zu erpressen. Sie setzen Penetrationstest-Tools wie Cobalt Strike, Brute Ratel C4 und das legale Fernverwaltungsprogramm Atera ein, um sich Zugang zu einem Opfer zu verschaffen. DEV-0390 verschafft sich durch den Diebstahl von Anmeldeinformationen erweiterte Zugriffsrechte, macht sensible Daten ausfindig (häufig auf Backup- und Dateiservern des Unternehmens) und sendet die Daten mithilfe eines Dateisicherungsprogramms an eine Cloud-Filesharing-Website.

Abwehr von Angriffen

Herausforderungen

1 Gestohlene Kennwörter und ungeschützte Identitäten

Mehr als die Schadsoftware benötigen die Angreifer*innen Anmeldeinformationen, um erfolgreich zu sein. Bei fast allen erfolgreichen Ransomware-Einsätzen verschaffen sich Hacker*innen Zugang zu privilegierten Konten auf der Ebene von Administrator*innen, die ihnen einen umfassenden Zugriff auf das Netzwerk eines Unternehmens gewähren.

2 Fehlende oder deaktivierte Sicherheitsprodukte

Bei fast allen beobachteten Ransomware-Vorfällen auf mindestens einem System, das für den Angriff ausgenutzt wurde, fehlten Sicherheitsprodukte oder diese wurden falsch konfiguriert, so dass Eindringlinge bestimmte Schutzmechanismen manipulieren oder deaktivieren konnten.

3 Falsch konfigurierte oder missbräuchlich genutzte Anwendungen

Auch wenn Sie gerne eine bestimmte Anwendung für einen bestimmten Zweck verwenden, heißt das nicht, dass Kriminelle sie nicht für andere Zwecke missbrauchen können. Allzu oft bedeuten „veraltete" Konfigurationen, dass eine Anwendung in ihrem Standardzustand ist und allen Benutzer*innen einen umfassenden Zugriff auf die gesamte Organisation ermöglicht. Übersehen Sie dieses Risiko nicht und zögern Sie nicht, App-Einstellungen aus Angst vor Störungen zu ändern.

4 Langsames Patching

Die beste Art, Software zu schützen, ist, sie ständig zu aktualisieren. Während einige Cloud-basierte Anwendungen ohne Zutun der Benutzer*innen aktualisiert werden, müssen Unternehmen die Patches anderer Hersteller sofort installieren. Im Jahr 2022 stellte Microsoft fest, dass ältere Schwachstellen immer noch eine der Hauptursachen für Angriffe sind.

Maßnahmen

1 Identitäten authentisieren

Setzen Sie die Multifaktor-Authentisierung (MFA) für alle Konten voraus, priorisieren Sie Administrations- und andere sensible Rollen. Bei einer hybriden Belegschaft sollten Sie MFA auf allen Geräten, an allen Standorten und zu jeder Zeit verlangen. Aktivieren Sie passwortlose Authentisierung wie FIDO-Schlüssel oder Microsoft Authenticator für Anwendungen, die dies unterstützen.

2 Blinde Flecken in der Sicherheit beseitigen

Wie Rauchmelder müssen auch Sicherheitsprodukte an den richtigen Stellen installiert und regelmäßig getestet werden. Vergewissern Sie sich, dass die Sicherheitstools in ihrer sichersten Konfiguration betrieben werden und dass kein Teil des Netzwerks ungeschützt ist.

3 Sichern Sie internetfähige Ressourcen

Ziehen Sie in Erwägung, doppelte oder ungenutzte Anwendungen zu löschen, um riskante, ungenutzte Dienste zu eliminieren. Achten Sie darauf, wo Sie Remote-Helpdesk-Anwendungen wie TeamViewer zulassen. Diese werden bekanntermaßen von Bedrohungsakteur*innen eingesetzt, um sich Zugang zu Laptops zu verschaffen.

4 Systeme auf dem neuesten Stand halten

Machen Sie die Software-Inventarisierung zu einem kontinuierlichen Prozess. Verfolgen Sie, welche Produkte Sie einsetzen, und setzen Sie Prioritäten beim Support für diese Produkte. Nutzen Sie Ihre Fähigkeit, schnell und schlüssig zu patchen, um festzustellen, wo der Übergang zu Cloud-basierten Diensten von Vorteil ist.

Abwehr von Angriffen

DEV-0537 verfolgt eine ganz andere Strategie und Arbeitsweise. Der erste Zugang erfolgt über den Erwerb von Zugangsdaten aus dem kriminellen Untergrund oder von Beschäftigten der Organisationen, die als Ziel ausgemacht worden sind.

Da Cyberkriminelle die Verflechtung von Identitäten und Vertrauensbeziehungen in modernen Technologie-Ökosystemen verstehen, zielen sie auf Telekommunikations-, Technologie-, IT-Dienstleistungs- sowie Support-Unternehmen ab, um sich von einem Unternehmen ausgehend Zugang zu Partner- oder Lieferantennetzwerken zu verschaffen. Reine Erpressungsangriffe zeigen, dass Verteidiger*innen von Netzwerken nicht nur auf Ransomware achten müssen, sondern auch auf die Exfiltration von Daten und laterale Bewegungen.

Wenn Angreifer*innen planen, ein Unternehmen damit zu erpressen, dass sie Daten veröffentlichen, ist die Ransomware-Payload der unbedeutendste und am wenigsten relevante Teil der Angriffsstrategie. Letztendlich liegt es im Ermessen der Betreiber*innen, was eingesetzt wird, und Ransomware bedeutet nicht immer die große Beute, auf die es die Bedrohungsakteur*innen abgesehen haben.

Während Ransomware oder doppelte Erpressung ein unvermeidliches Ergebnis eines Angriffs durch raffinierte Angreifer*innen zu sein scheint, ist Ransomware eine vermeidbare Katastrophe. Da sich die Angreifer*innen auf Sicherheitslücken verlassen, sind Investitionen in die Cyberhygiene von großer Bedeutung, um Hacker*innen abzuwehren.

Microsofts einzigartige Sicht gibt uns einen Einblick in die Aktivitäten von Bedrohungsakteur*innen. Anstatt sich auf Forenbeiträge oder Chat-Leaks zu verlassen, untersucht unser Team von Sicherheitsexpert*innen neue Ransomware-Taktiken und entwickelt Threat Intelligence, die in unsere Sicherheitslösungen einfließen.

Integrierter Bedrohungsschutz für Geräte, Identitäten, Anwendungen, E-Mails, Daten und die Cloud hilft uns, Angriffe zu erkennen, die sich mehreren Akteur*innen zuordnen ließen, hinter denen in Wirklichkeit aber nur einzige Gruppe von Cyberkriminellen steckt. Unsere Digital Crimes Unit, die sich aus technischen, rechtlichen und wirtschaftlichen Expert*innen zusammensetzt, arbeitet weiterhin mit den Strafverfolgungsbehörden zusammen, um Cyberkriminalität zu unterbinden.

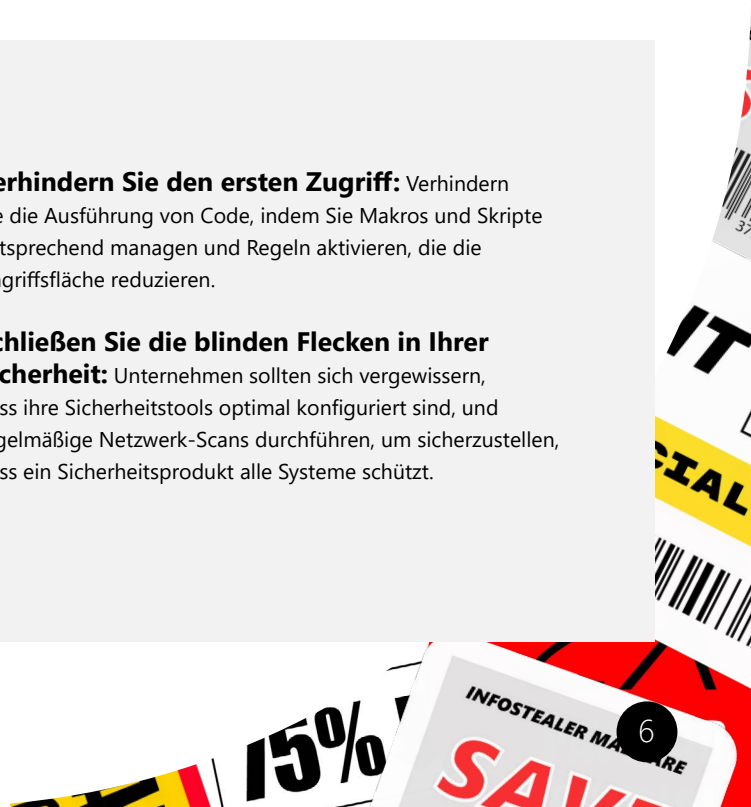
Empfehlungen:

Die Cloud absichern: Da sich Angreifer*innen in Richtung Cloud-Ressourcen bewegen, ist es wichtig, Cloud-Ressourcen und -Identitäten sowie lokale Konten zu sichern. Sicherheitsteams sollten sich darauf konzentrieren, die Infrastruktur für Sicherheitsidentitäten zu stärken, die Multifaktor-Authentisierung (MFA) für alle Konten einzusetzen und Cloud-Administrator*innen bzw. Tenant-Administrator*innen mit demselben Maß an Sicherheit und Sorgfalt bei den Anmeldeinformationen zu behandeln wie Domain-Administrator*innen.

Ausführliche Empfehlungen von Microsoft finden Sie unter https://aka.ms/ransomware-as-a-service.

Verhindern Sie den ersten Zugriff: Verhindern Sie die Ausführung von Code, indem Sie Makros und Skripte entsprechend managen und Regeln aktivieren, die die Angriffsfläche reduzieren.

Schließen Sie die blinden Flecken in Ihrer Sicherheit: Unternehmen sollten sich vergewissern, dass ihre Sicherheitstools optimal konfiguriert sind, und regelmäßige Netzwerk-Scans durchführen, um sicherzustellen, dass ein Sicherheitsprodukt alle Systeme schützt.



Profil unserer Expertin

Emily Hacker:
Threat Intelligence Analystin

Emily Hacker hatte nicht damit gerechnet, dass sie als Analystin für die Threat Intelligence bei Microsoft arbeiten würde, nachdem sie Journalismus am College studiert hatte. Ihr erster Job im Bereich der Cybersicherheit war als technische Redakteurin bei einem Öl- und Gasunternehmen. „Ich habe Intelligence-Berichte bearbeitet, Präsentationen erstellt und half bei den Statistiken über Vorfälle. Im Laufe dieses ersten Jahres war ich absolut begeistert von der Arbeit als Intelligence Analystin."

Emilys Weg bei Microsoft begann im Jahr 2020 als Analystin für Microsoft Defender for Endpoint und Microsoft Defender for Office. Eines der Schwerpunktthemen dieser Teams ist der Schutz der Kund*innen vor Bedrohungen durch Ransomware. Emily war von vorneherein an vielen der Untersuchungen beteiligt, auf denen Microsofts Wissen über die RaaS-Ökonomie und die Beziehung zwischen Access Broker/Betreiber*innen und Partner*innen. Dafür suchte sie aktiv nach Beweisen für Pre-Ransomware-Signale.

„Das Verfolgen von Trends und Techniken, die von RaaS-Betreiber*innen und ihren Partner*innen in der Pre-Ransomware Phase eines Vorfalls genutzt werden, ist entscheidend, um Kund*innen vor dieser Art von Bedrohungen zu schützen", sagt sie. „Meine Aufgabe ist es, diese Pre-Ransomware-Akteur*innen so früh wie möglich zu erkennen. Wenn Sie nur nach der Payload der Ransomware selbst suchen, sind Sie zu spät dran."

Um in der sich verändernden RaaS-Landschaft den Überblick zu behalten, nutzen Emily und ihr Team eine Kombination aus automatisierten Systemen und menschlicher Analyse, um Protokolle, Warnungen und andere Aktivitäten in Echtzeit zu analysieren, zu eskalieren und darauf zu reagieren. Emilys Team hilft dabei, verschiedene Vorfälle an der vordersten Front der Kundennetzwerke zu antizipieren, ihnen zuvorzukommen und auf sie zu reagieren. Gleichzeitig trägt es zu MSTICs ständig wachsender Bewertung von Tools, Motiven und Strategien von Ransomware-Akteur*innen bei.

Bei einem Ransomware-Vorfall kann unglaublich viel auf dem Spiel stehen. Die Betreiber*innen von Ransomware sind dafür bekannt, dass sie es auf wichtige Netzwerke in den Bereichen Bildung, Transport, Gesundheitswesen oder Telekommunikation abgesehen haben. Wenn diese Netzwerke betroffen sind, können die Folgen katastrophal sein.

„Die Arbeit, die wir bei Microsoft leisten, um Ransomware-Vorfälle zu verfolgen und zu verhindern, ist wichtig, weil wir damit nicht nur unsere, sondern auch deren Kund*innen schützen", so Hacker. „Die Tools und Techniken im Zusammenhang mit Ransomware und Vorfällen im Vorfeld von Ransomware so früh wie möglich zu erkennen, ist entscheidend, wenn diese Vorfälle potenziell weitreichende Folgen für Unternehmen, ihre Beschäftigten und ihre Kund*innen haben."

> **" Meine Aufgabe ist es, diese Pre-Ransomware-Akteur*innen so früh wie möglich zu erkennen. Wenn Sie nur nach der Payload der Ransomware selbst suchen, sind Sie zu spät dran."**
>
> Threat Intelligence Analystin
> **Emily Hacker**

Microsoft

[1] **Methodik:** Für die Snapshot-Daten haben Microsoft-Plattformen, einschließlich Defender und Azure Active Directory, und unsere Digital Crimes Unit anonymisierte Daten zu Bedrohungsaktivitäten wie bösartige E-Mail-Konten, Phishing-E-Mails und Angreiferbewegungen in Netzwerken bereitgestellt. Weitere Erkenntnisse stammen aus den 43 Billionen Sicherheitssignalen, die täglich bei Microsoft gewonnen werden, einschließlich der Cloud, der Endpunkte, des Intelligent Edge und unserer Compromise Security Recovery Practice und Detection and Response Teams. Das Titelbild ist repräsentativ für das Geschäftsmodell der Partner. Die Prozentsätze stellen keine tatsächlichen Rabatte dar.

© 2022 Microsoft Corporation. All rights reserved. Cyber Signals is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. This document is provided "as is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product.