19.02.2019 – 12:39 Uhr

Cyber-Angreifer werden schneller: CrowdStrike gibt Einblicke in Bedrohungslandschaft

USA (ots) -

CrowdStrike, der führende Anbieter von Cloud-basiertem Endpunktschutz, veröffentlicht heute seinen jährlichen Global Threat Report: "Adversary Tradecraft and The Importance of Speed". Die Ergebnisse des Berichts deuten darauf hin, dass die Aktivitäten staatlicher und globaler eCrime-Akteure in allen untersuchten Branchen zunehmen. Außerdem liefert er Erkenntnisse zu realen Angriffen.

Geschwindigkeit ist für eine effektive Cyberabwehr unerlässlich. Das belegt der aktuelle Global Threat Report (GTR). CrowdStrike analysiert darin die "Breakout-Zeit" der Top-Cyber-Angreifer und stellt ein Ranking der schnellsten Akteure vor. Die "Breakout-Zeit" bezeichnet das kritische Zeitfenster zwischen dem Zeitpunkt, zu dem ein Eindringling die erste Maschine kompromittiert und dem Punkt, an dem er beginnt, in andere Systeme des Netzwerks vorzudringen. Das GTR-Ranking bietet Unternehmen einen beispiellosen Einblick in die Geschwindigkeit, mit der sie Einbrüche erkennen, untersuchen und beheben müssen, um Angriffe zu vereiteln. Dieses Vorgehen ist auch als "1-10-60-Regel" bekannt.

Aus diesen Ländern kommen die schnellsten Angreifer (basierend auf den Erkenntnissen von mehr als 30.000 Angriffen, die CrowdStrike 2018 verhindert hat):

- Russische Akteure, die von CrowdStrike als "Bears" bezeichnet werden, sind die schnellsten Angreifer mit einer durchschnittlichen "Breakout-Zeit" von 18:49 Minuten.
- Staatliche Akteure aus Nordkorea, die als "Chollimas" betitelt werden, sind die Zweitschnellsten mit einer durchschnittlichen "Breakout-Zeit" von 2:20:14 Stunden.
- Staatliche Akteure aus China ("Pandas") benötigen durchschnittlich 4:00:26 Stunden.
- Iranische Akteure ("Kittens") benötigen durchschnittlich 5:09:04 Stunden.
- eCrime-Akteure, auch als "Spiders" bezeichnet, haben die längste durchschnittliche "Breakout-Zeit": 9:42:23 Stunden. Allerdings gibt es unter den eCrime-Akteuren einige, die sehr schnell handeln und selbst mit den schnellsten Nationalstaaten konkurrieren können.

"Für unsere Analysen kombinieren wir unseren umfangreichen Cloud-basierten Endpunkt-Sicherheits-Datensatz mit Bedrohungsinformationen und Erkenntnissen aus mehr als 30.000 Verstößen, die unsere OverWatch- und Services-Teams im Jahr 2018 untersucht haben. Damit verfügt CrowdStrike über einen einzigartigen Einblick in die Aktivitäten der Cyber-Angreifer und ist in der Lage, das erste Ranking der Branche zu erstellen", sagt Dmitri Alperovitch, Chief Technology Officer (CTO) und Mitgründer von CrowdStrike. "Der diesjährige Bericht unterstreicht, wie wichtig eine schnelle Reaktion für die Cybersicherheit ist und liefert wertvolle Erkenntnisse darüber, wie einige der zerstörerischsten und leistungsfähigsten Akteure - sowohl staatliche Akteure als auch Angreifer aus dem eCrime-Bereich - besiegt werden können."

Ergebnisse des Global Threat Report:

- Einer der wichtigsten eCrime-Trends 2018 ist der kontinuierliche Aufstieg des "Big Game Hunting". Hierbei werden mehrere Methoden kombiniert, um Ransomware gezielt in großen Unternehmen zu platzieren.
- Ein weiterer Trend, der von CrowdStrike Intelligence erkannt wurde, ist die verstärkte Zusammenarbeit von hoch spezialisierten eCrime-Akteuren. Hier lässt sich auch die zunehmende Verwendung von Geo-Targeting für gezielte Aktionen von eCrime-Gruppierungen beobachten.
- Zu den Branchen, die ganz oben auf der Zielliste der Angriffe ohne Malware stehen, gehören Medien, Technologie und Wissenschaft. Das unterstreicht die Notwendigkeit, dass auch diese Branchen ihren Schutz gegen zunehmend komplexe und moderne Angriffsmethoden verstärken.
- CrowdStrike identifizierte mehrere gezielte Angriffe aus China, den Iran und Russland, die sich auf den Telekommunikationssektor konzentrierten und wahrscheinlich staatliche Spionageaktivitäten unterstützten. Darauffolgende Köder-Aktionen, mit denen

Social-Engineering-Kampagnen vorbereitet wurden, trafen vor allem Telekommunikationskunden, aber auch Regierungsstellen.
- CrowdStrike beobachtete ein zunehmendes operatives Tempo der in China ansässigen Akteure, das sich bei anhaltender Belastung der Beziehungen zwischen den USA und China noch weiter beschleunigen dürfte.

Der Global Threat Report von CrowdStrike analysiert umfassende Bedrohungsdaten. Die Daten stammen von CrowdStrike's Teams Falcon Intelligence, Falcon OverWatch, dem branchenführenden Managed Hunting-Team des Unternehmens, sowie CrowdStrike Services. Außerdem kam der CrowdStrike Threat Graph zum Einsatz, eine massiv skalierbare, Cloud-basierte Grafikdatenbanktechnologie, die jede Woche eine Billion Ereignisse in 176 Ländern verarbeitet. Zusammen bieten diese Teams und Tools einen ganzheitlichen Blick auf die im Bericht dargestellte Bedrohungslandschaft.

"Die Bedrohungslandschaft entwickelt sich mit einer beispiellosen Geschwindigkeit und bei jedem Vorstoß kann das Überleben eines Unternehmens auf dem Spiel stehen. Unternehmen können sich keinen passiven Ansatz zum Schutz ihrer Daten und ihres Kapitals leisten", sagt Adam Meyers, Vice President of Intelligence bei CrowdStrike. "Da wir weiterhin sehen, dass hochentwickelte staatliche und eCrime-Akteure das Niveau und die Komplexität der täglichen Bedrohungen erhöhen, sollte dieser Bericht Wirtschaftsführern und Sicherheitsexperten als Quelle dienen, um die Bedrohungslandschaft besser zu verstehen und fundierte Entscheidungen zum Schutz geschäftskritischer Daten zu treffen."

"Während Unternehmen ihr Sicherheitsniveau weiter stärken, wenden Gegner immer ausgefeiltere Techniken an, um ihre Taten zu verbergen und weiter Fuß zu fassen", sagt Jennifer Ayers, Vice President of OverWatch and Security Response bei CrowdStrike. "Es ist notwendig, die Prävention, Identifikation und Reaktion auf Bedrohungen mit einer wachsamen 24/7-Bedrohungssuche in Echtzeit zu ergänzen, um die verborgenen Handlungen dieser Akteure so schnell wie möglich zu identifizieren, da Zeit von entscheidender Bedeutung ist."

Der Global Threat Report von CrowdStrike liefert ein tieferes Verständnis für die Motivationen, Ziele und Aktivitäten von Cyber-Kriminellen, um Unternehmen darüber zu informieren, wie sie sich proaktiv verteidigen können.

Laden Sie den CrowdStrike Global Threat Report 2019 herunter: http://ots.de/DWnNGe

Über CrowdStrike

CrowdStrike ist der führende Anbieter von Cloud-basiertem Schutz von Endgeräten. Die CrowdStrike Falcon Plattform verhindert mithilfe von künstlicher Intelligenz Angriffe auf Endgeräte im oder außerhalb des Netzwerks und bietet sofortigen Schutz und Transparenz im gesamten Unternehmen. Sie ist in wenigen Minuten einsatzbereit. Durch ihre Cloud-Infrastruktur und die Single-Agent-Architektur reduziert die Plattform Komplexität, erleichtert die Verwaltung und erhöht die Skalierbarkeit. CrowdStrike betreut Kunden aus fast allen Industrien und Branchen, darunter führende Finanzinstitutionen, Energieunternehmen und Gesundheitsversorger. Insgesamt werden Lösungen des Unternehmens in 176 Ländern eingesetzt. CrowdStrike wurde 2011 gegründet und hat seinen Hauptsitz in Sunnyvale, Kalifornien. Weitere Informationen finden Sie unter www.crowdstrike.com.

Kontakt:

PIABO PR GmbH
Caroline Jechow | Senior Account Manager
E-Mail: crowdstrike@piabo.net
Telefon: +49 30 2576 205 261