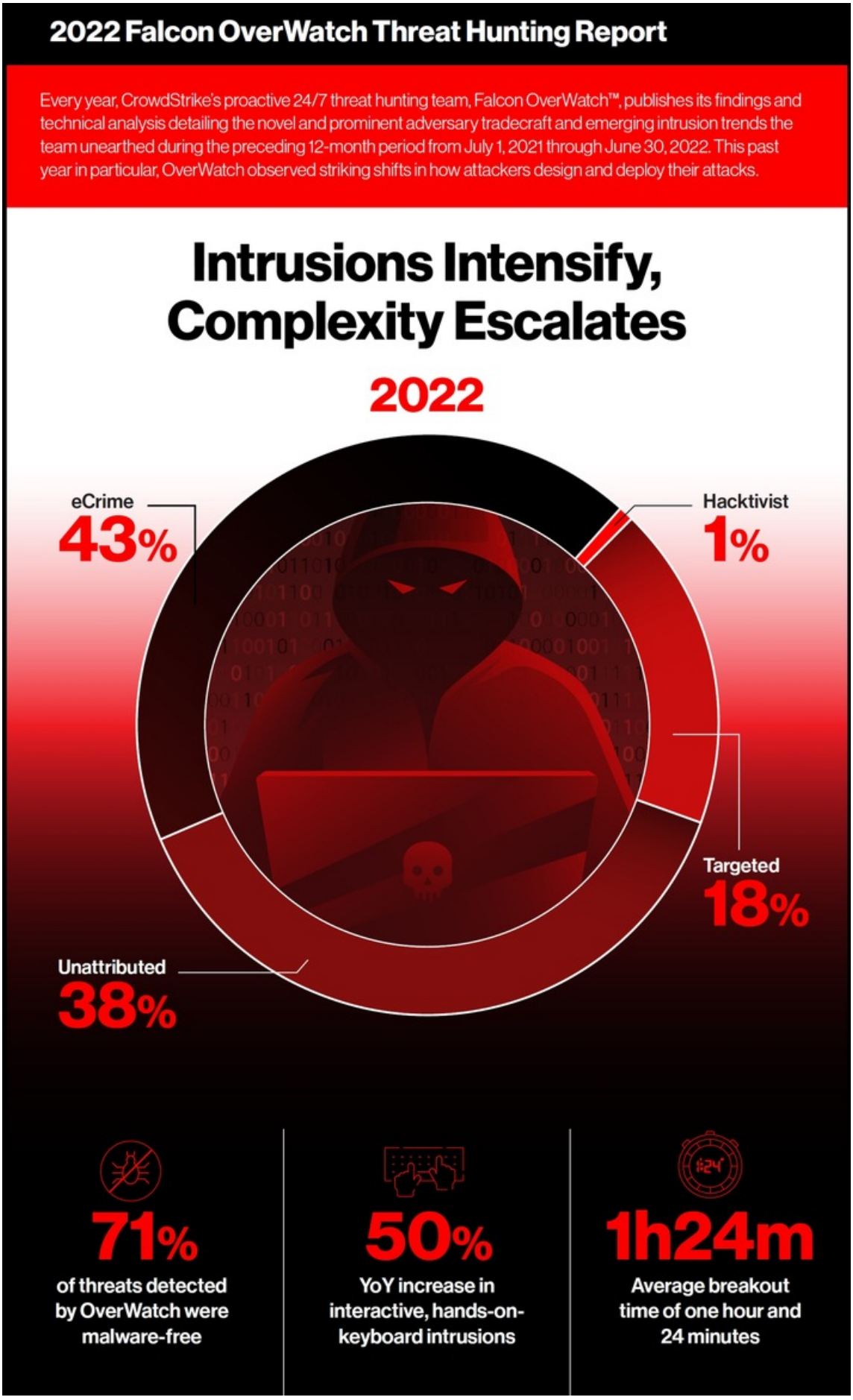
CrowdStrike

13.09.2022 – 10:30 Uhr

Alle sieben Minuten wird ein potenzieller Cyberangriff identifiziert - das zeigt der jährliche Threat Hunting Report von CrowdStrike



Aachen (ots) -

CrowdStrike, ein führender Anbieter von Cloud-basiertem Schutz von Endgeräten, Cloud-Workloads, Identitäten und Daten, veröffentlichte heute seinen vierten jährlichen Threat Hunting Report *Nowhere to Hide: 2022 Falcon OverWatch Threat Hunting Report*. Der globale Bericht zeigt einen rekordverdächtigen Anstieg von Hands-On-Angriffsversuchen um 50 Prozent im Vergleich

zum Vorjahr sowie deutliche Veränderungen bei den Angriffstrends und den Vorgehensweisen der Angreifer. Die Falcon OverWatch Threat Hunter haben mehr als 77.000 potenzielle Angriffsversuche identifiziert, was ungefähr einem Angriffsversuch alle sieben Minuten entspricht. Dabei handelt es sich um Fälle, bei denen durch eine proaktive, von Menschen geleitete, Bedrohungsjagd Angreifer aufgedeckt wurden, die in verschiedenen Phasen der Angriffskette aktiv bösartige Techniken angewendet haben. Dabei setzen sie alles daran, sich den autonomen Erkennungsmethoden zu entziehen.

Falcon OverWatch hat errechnet, dass die Breakout Time (also die Zeit, die ein Angreifer im Durchschnitt benötigt, um von der anfänglichen Kompromittierung zu anderen Hosts innerhalb der Opferumgebung überzugehen) für eCrime-Angreifer auf 1 Stunde und 24 Minuten gesunken ist - im Vergleich zu 1 Stunde und 38 Minuten, die Falcon OverWatch noch für den CrowdStrike Global Threat Report 2022 ermittelte. Darüber hinaus stellte das OverWatch-Team fest, dass bei etwa einem Drittel (30 %) dieser eCrime-Attacken der Angreifer in der Lage war, sich in weniger als 30 Minuten lateral zu bewegen. Diese Ergebnisse unterstreichen die Geschwindigkeit und das Ausmaß, in dem Bedrohungsakteure ihre Taktiken, Techniken und Verfahren (TTPs) weiterentwickeln und in der Lage sind, selbst die fortschrittlichsten technologiebasierten Abwehrsysteme zu umgehen, um ihre Ziele erfolgreich zu erreichen.

"In den letzten 12 Monaten sah sich die Welt mit neuen Herausforderungen konfrontiert, die durch wirtschaftlichen Druck und geopolitische Spannungen ausgelöst wurden und eine Bedrohungslandschaft entstehen ließen, die so kompliziert wie nie zuvor ist", sagt Param Singh, Vice President, Falcon OverWatch bei CrowdStrike. "Um dreiste Bedrohungsakteure auszubremsen, müssen Sicherheitsteams Lösungen implementieren, die zu jeder Tages- und Nachtzeit proaktiv nach versteckten und fortschrittlichen Angriffen suchen. Die Kombination der CrowdStrike Falcon-Plattform mit der Telemetrie, den Werkzeugen, der Threat Intelligence und dem menschlichen Einfallsreichtum der Falcon OverWatch Threat Hunter schützt Unternehmen weltweit vor den raffiniertesten und am schwersten zu erkennenden Bedrohungen."

Weitere wichtige Erkenntnisse aus dem Bericht sind:

- **eCrime ist hauptverantwortlich für interaktive Einbruchskampagnen.** eCrime war für 43 Prozent der interaktiven Einbrüche verantwortlich, während staatliche Akteure 18 Prozent der Aktivitäten ausmachten. Auf Hacktivisten entfielen nur ein Prozent der interaktiven Einbruchskampagnen, während die übrigen Einbrüche nicht zugeordnet werden konnten.
- **Die Angreifer verlassen sich immer weniger auf Malware.** Auf Malware-freie Angriffe entfielen 71 Prozent aller vom CrowdStrike Threat Graph indizierten Entdeckungen. Die Vorherrschaft von Malware-freien Angriffen hängt zum Teil damit zusammen, dass die Angreifer in großem Umfang gültige Anmeldeinformationen missbrauchen, um den Zugang zu und das Verbleiben in den Opferumgebungen zu erleichtern. Ein weiterer Faktor ist die Geschwindigkeit, mit der neue Schwachstellen aufgedeckt werden sowie die Geschwindigkeit, mit der Angreifer in der Lage sind, Exploits zu implementieren.
- **Die Technologiebranche ist die wichtigste Zielbranche für interaktive Angriffe.** Die fünf wichtigsten Zielbranchen sind Technologie (19 %), Telekommunikation (10 %), Fertigung (7 %), Hochschulen (7 %) und das Gesundheitswesen (7 %). Bemerkenswert ist, dass die Technologiebranche beinahe doppelt so oft zum Ziel interaktiver Eindringlinge wurde wie die am zweithäufigsten betroffene Branche.
- **Der Telekommunikationssektor ist die wichtigste Branche für gezielte Angriffe durch staatliche Akteure.** Die fünf wichtigsten Zielbranchen sind Telekommunikation (37 %), Technologie (14 %), Behörden (9 %), Hochschulen (5 %) und Medien (4,5 %). Die Telekommunikationsbranche ist nach wie vor das Ziel staatlich geförderter Überwachungs-, Nachrichten- und Spionageabwehrmaßnahmen. Dabei erfuhr die Telekommunikationsbranche 163 Prozent mehr gezielte Eingriffe durch staatliche Akteure, als die Branche, die am zweithäufigsten ins Visier genommen wurde.
- **Das Gesundheitswesen befindet sich im Fadenkreuz von Ransomware-as-a-Service (RaaS).** Das Volumen der versuchten interaktiven Angriffe auf das Gesundheitswesen hat sich im Vergleich zum Vorjahr verdoppelt. Die überwiegende Mehrheit dieser Einbrüche wird eCrime zugeschrieben.

Der Bericht umfasst die Erkenntnisse der globalen Threat Hunting-Aktivitäten von Falcon OverWatch im Zeitraum vom 1. Juli 2021 bis zum 30. Juni 2022 und enthält detaillierte Angriffsdaten und -analysen, Fallstudien und umsetzbare Empfehlungen.

Zusätzliche Informationen

- Laden Sie den vollständigen Bericht *Nowhere to Hide: 2022 Falcon OverWatch Threat Hunting Report* auf der CrowdStrike-Website herunter.
- Seien Sie am 19. September um 20:30 Uhr auf Twitter Spaces live dabei, wenn die Experten die wichtigsten Erkenntnisse aus dem Falcon OverWatch Threat Hunting Report 2022 vorstellen https://twitter.com/i/spaces/1YpJkgOPADrJj
- Nehmen Sie am 6. Oktober an einem Live-CrowdCast des CrowdStrike Falcon OverWatch Threat Hunting-Teams teil und erfahren Sie mehr über neue Angriffstrends und Handelspraktiken aus dem Falcon OverWatch Threat Hunting Report 2022. Registrieren Sie sich hier: https://www.crowdstrike.com/resources/crowdcasts/nowhere-to-hide-2022-falcon-overwatch-threat-hunting-report/

Über CrowdStrike

CrowdStrike Holdings Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Plattform zum Schutz von Workloads, Endgeräten, Identitäten und Daten die Sicherheit im Cloud-Zeitalter neu.

Dank der CrowdStrike Security Cloud und erstklassiger künstlicher Intelligenz kann die CrowdStrike Falcon®-Plattform Echtzeit-Angriffsindikatoren, Bedrohungsdaten, sich ständig weiterentwickelnde Methoden der Angreifer sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen nutzen, um hochpräzise Detektionen, automatisierte Schutz- und Abhilfemaßnahmen, erstklassiges Threat Hunting und eine nach Prioritäten geordnete Beobachtung von Schwachstellen zu ermöglichen.

Die speziell für die Cloud entwickelte Falcon-Plattform verfügt über einen einzigen, schlanken Agenten und bietet eine schnelle und skalierbare Implementierung, ausgezeichneten Schutz und Leistung bei geringerer Komplexität und schneller Wertschöpfung.

Das Motto von CrowdStrike lautet: We stop breaches.

Mehr Informationen finden Sie unter:https://www.crowdstrike.de

Folgen Sie uns: Blog | Twitter | LinkedIn | Facebook | Instagram

Jetzt kostenlos testen: https://www.crowdstrike.com/free-trial-guide/

Pressekontakt:

HARVARD ENGAGE! COMMUNICATIONS GMBH
Oliver Salzberger / Ava Duehring
Tel: +49 89 53 29 57 23
E-Mail: crowdstrike@harvard.de

Medieninhalte

CrowdStrike veröffentlicht OverWatch Threat Hunting Report 2022 / Weiterer Text über ots und www.presseportal.de/nr/132391 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke unter Beachtung ggf. genannter Nutzungsbedingungen honorarfrei. Veröffentlichung bitte mit Bildrechte-Hinweis.