CROWDSTRIKE

NOWHERE TO HIDE

Das Problem ist nicht die Malware, sondern der Akteur hinter den Angriffen.

Um Bedrohungsakteure abwehren zu können, müssen Sicherheitsteams wissen, wie die Angreifer vorgehen.

Der CrowdStrike Threat Hunting Report 2023, der vom CrowdStrike Counter Adversary Operations-Team herausgegeben wurde, stellt die neuesten Taktiken der Bedrohungsakteure vor und gibt Einblicke und Hinweise dazu, wie Sie Kompromittierungen stoppen können.

Wichtigste neue Erkenntnisse

IDENTITÄTSBEDROHUNGEN SIND INZWISCHEN STANDARD

Bedrohungsakteure intensivieren ihre Bemühungen bei identitätsbasierten Angriffen, sodass die Folgen von Diebstahl und Missbrauch kompromittierter Identitäten immer schwerwiegender werden.

62 %
aller interaktiven Angriffe nutzten kompromittierte Anmeldedaten

583 %
Zunahme bei Kerberoasting, einer immer häufiger eingesetzten identitätsbasierten Angriffstechnik

CYBERCRIME NIMMT ZU, DA DIE ANGREIFER IMMER SCHNELLER WERDEN

Angreifer können schneller als je zuvor in Umgebungen gelangen und sich dort lateral bewegen.

79 MINUTEN
durchschnittliche Breakout-Time bei Cyberangriffen

7 MINUTEN
betrug die bisher kürzeste erfasste Breakout-Zeit bei einem Cyberangriff

BEDROHUNGSAKTEURE GEHEN IN DER CLOUD GESCHICKTER VOR

Bedrohungsakteure werden immer mehr zu Cloud-Experten und nutzen gängige Konfigurationsfehler sowie integrierte Cloud-Verwaltungstools aus.

160 %
Zunahme bei Anmeldedatendiebstahl über Cloud-Metadaten-APIs

PLATTFORMÜBERGREIFENDE KOMPETENZ STEHT IM MITTELPUNKT

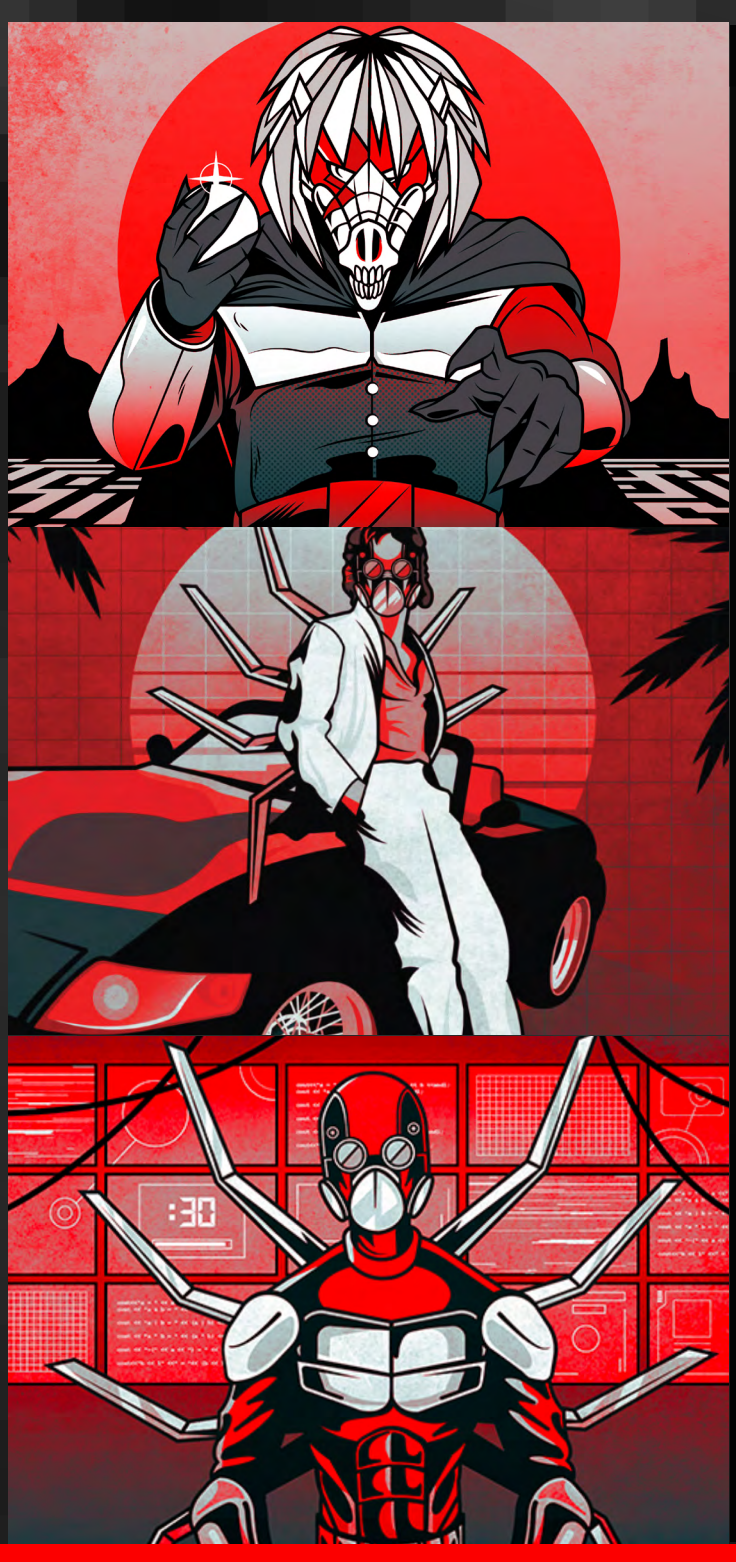
Interaktive Angriffe im Jahr 2023 zeichnen sich durch die Beherrschung aller Betriebssysteme aus.

300 % ZUNAHME
bei Angreifern, die unter Linux PAMs (Pluggable Authentication Modules) durch böswillige Module ersetzen

FINANZDIENSTLEISTER, TECHNOLOGIE- UND SERVICESEKTOR
sind am stärksten betroffen

Erfahren Sie, welche Bedrohungsakteure Ihre Branche angreifen.

CROWDSTRIKE ÜBERWACHT DIESE UND MEHR ALS 200 WEITERE BEDROHUNGSAKTEURE AKTIV. WEITERE INFORMATIONEN ZU DIESEN ANGREIFERN ERHALTEN SIE IM THREAT HUNTING REPORT 2023.



LABYRINTH CHOLLIMA
Für mehrere Betriebssystemangriffe verantwortlich

VICE SPIDER
Für 27 % aller Kerberoasting-Angriffe verantwortlich

INDRIK SPIDER
Ist von opportunistischer Cyberkriminalität zu maßgeschneiderten Angriffen übergegangen

Know them. **Find** them. **Stop** them.

- Von unseren erfahrenen Threat Huntern erhalten Sie einzigartige Einblicke zu besonders erfolgreichen Techniken und Taktiken.
- Erfahren Sie, basierend auf den Erkenntnissen aus realen Angriffen, wie Sie Ihre Sicherheitsstrategie optimieren und dynamische Bedrohungen abwehren können.
- Machen Sie sich mit globalen und regionalen Trends vertraut, damit Sie Bedrohungsakteuren einen Schritt voraus bleiben können.

BERICHT HERUNTERLADEN

CROWDSTRIKE