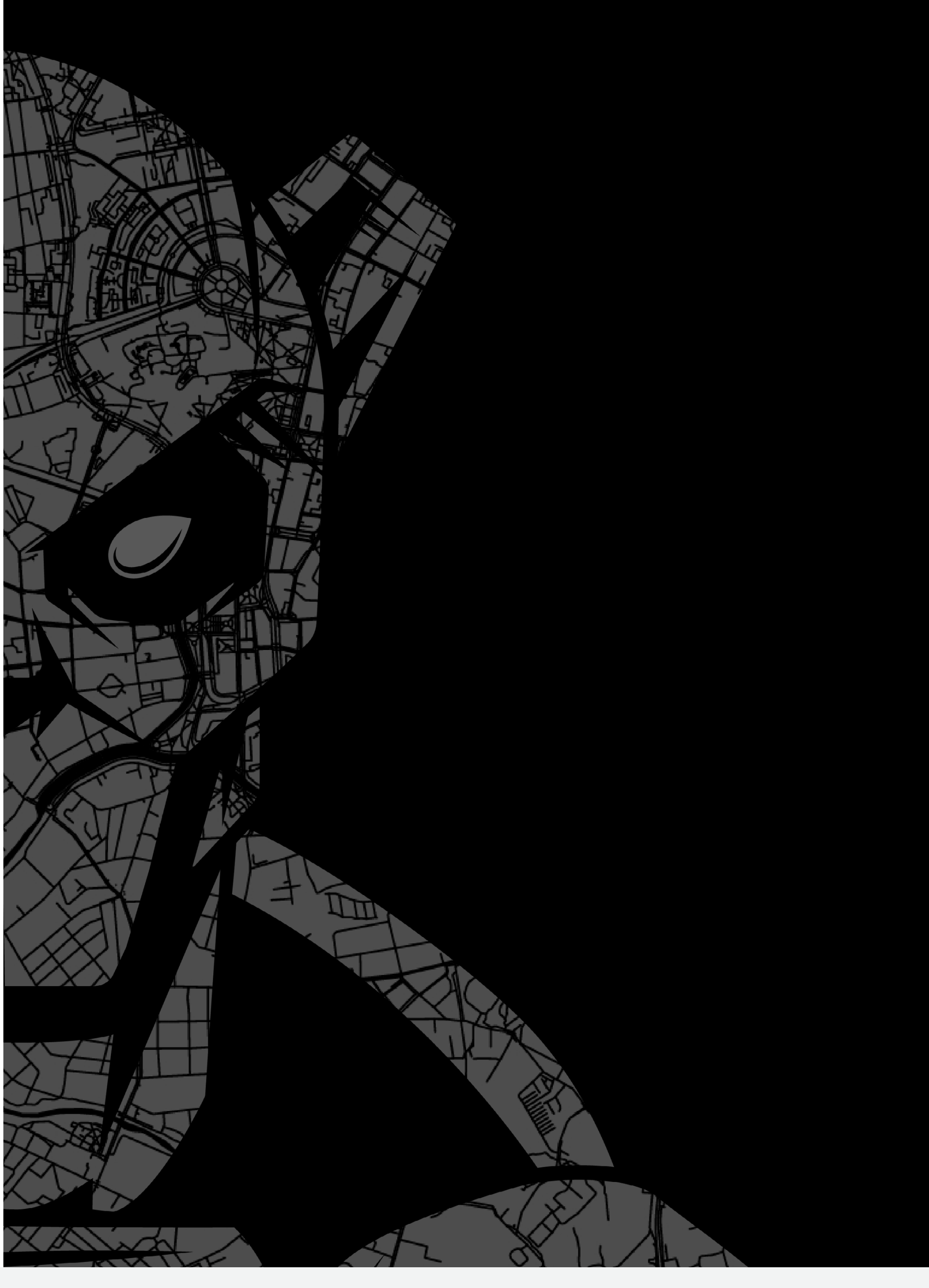
CROWDSTRIKE



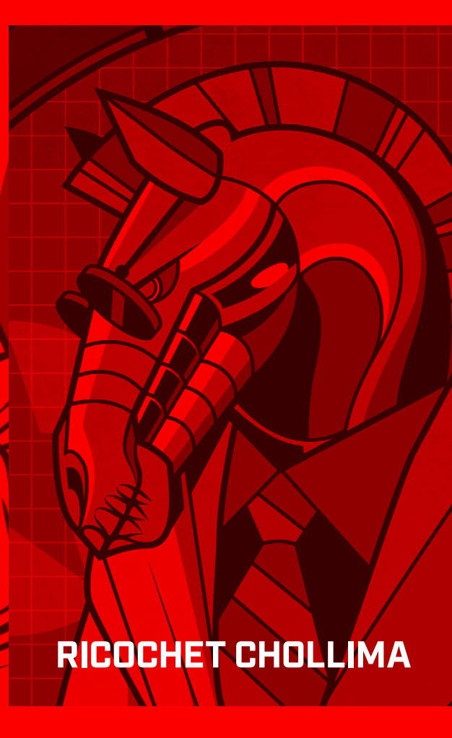
GLOBAL THREAT REPORT 2023

Unerbittliche Angreifer
noch schneller und raffinierter:
Das Wichtigste aus 2022 im Überblick

Der CrowdStrike Global Threat Report 2023
liefert umfassende Analysen der heutigen Bedrohungslandschaft
und beleuchtet die wichtigsten Trends des Jahres 2022, die dafür
verantwortlichen Akteure, sowie deren Entwicklung.

ANGREIFER-STECKBRIEFE

eCRIME | NATIONAL-STAATLICHE AKTEURE | HACKTIVISTEN



33 neu identifizierte Angreifer in 2022

200+ verfolgte Angreifer

WO SIND SIE AKTIV

- Technologie
- Finanzsektor
- Gesundheitswesen
- Telekommunikation
- Fertigungsindustrie
- Bildungswesen
- Behörden/Regierungen

WIE GEHEN SIE VOR

Für Unternehmen wird es immer schwieriger, sich vor Angriffen zu schützen, da sich die Bedrohungslandschaft weiterentwickelt und Cyberangriffe zunehmen.

98' → 84'

BREAKOUT TIME WEITERHIN UNTER 2 STUNDEN

eCrime-Akteure benötigen im Durchschnitt 1 Stunde und 24 Minuten, um sich lateral zu bewegen – 14 Minuten weniger als in 2021.

1'24"

71% DER ANGRIFFE WAREN MALWARE-FREI

Angreifer nutzen immer weniger Malware, sondern setzen zunehmend auf „Hands-on-Keyboard"-Techniken. Ein Trend, der unter anderem darauf zurückzuführen ist, dass sie verstärkt gültige Anmeldedaten missbrauchen, um sich Zugang zu verschaffen, sowie auf ihre Fähigkeit, Sicherheitslücken schnell auszunutzen.

50% SPRUNGHAFTER ANSTIEG INTERAKTIVER ANGRIFFSKAMPAGNEN

Die Anzahl der interaktiven Angriffe ist 2022 um 50 % gestiegen und nahm im vierten Quartal besonders stark zu.

ZAHL DER ACCESS BROKER-INSERATE UM 112 % GESTIEGEN

Die Dienstleistungen von Access Brokern erfreuten sich im Jahr 2022 zunehmender Beliebtheit. Es wurden mehr als 2.500 Inserate mit Zugangsdaten geschaltet, ein deutlicher Anstieg im Vergleich zu 2021, was die wachsende Nachfrage nach diesen Services unterstreicht.

WAS WOLLEN SIE

Auch 2022 hatten Angreifer es auf die Daten
und die Infrastruktur der Opfer abgesehen.

CLOUD-EXPLOIT-VORFÄLLE UM 95 % GESTIEGEN

Die Zahl der Fälle, in denen Cloud-Angreifer involviert waren, hat sich 2022 im Vergleich zum Vorjahr fast verdreifacht. Dies verdeutlicht einen weiteren, größeren Trend: eCrime und nationalstaatliche Akteure eignen sich zunehmend Wissen und Techniken an, um Cloud-Umgebungen anzugreifen.

95%

DATENDIEBSTAHL UND ERPRESSUNGS-KAMPAGNEN DAUERN AN - AUCH OHNE RANSOMWARE

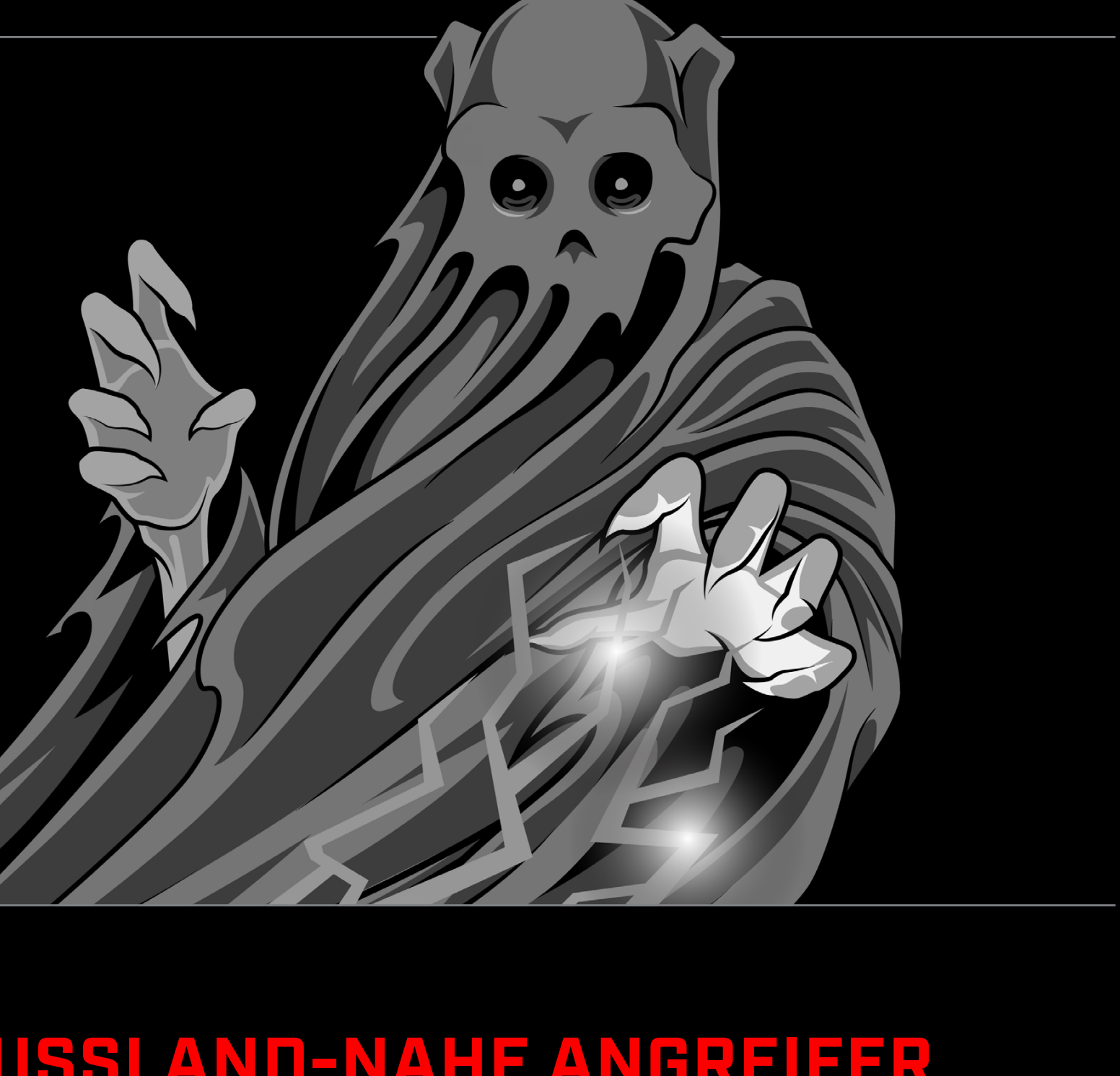
CrowdStrike Intelligence beobachtete einen 20%igen Anstieg bei der Zahl der Angreifer, die Datendiebstahl und Erpressung betreiben, ohne Ransomware einzusetzen. Dieses Modell der „doppelten Erpressung" ist die gängigste Taktik von Big Game Hunting-Angreifern.

WIEDERVERWENDETE SCHWACHSTELLEN GEFÄHRDEN EXPONIERTE KOMPONENTEN

Die im Jahr 2022 beobachteten Zero-Day- und N-Day-Schwachstellen belegen, dass die Angreifer in der Lage sind, ihr Spezialwissen zu nutzen, um die Schutzmaßnahmen vorheriger Patches zu umgehen und dieselben anfälligen Komponenten mehrfach anzugreifen.

CHINA-NAHE ANGREIFER BILDETEN DIE AKTIVSTE ANGREIFERGRUPPE

China-nahe Angreifer – sowie Akteure mit den gleichen Taktiken, Techniken und Verfahren (TTPs) – wurden 2022 in nahezu allen 39 globalen Industriesektoren und 20 geografischen Regionen beobachtet, die CrowdStrike Intelligence überwacht.



RUSSLAND-NAHE ANGREIFER SETZTEN IHRE MILITÄRISCHEN, PSYCHOLOGISCHEN UND HACKTIVISTISCHEN ANGRIFFE GEGEN DIE UKRAINE FORT

Über das komplette Jahr 2022 hinweg beobachtete CrowdStrike Intelligence zahlreiche Cyber-Taktiken, die darauf abzielten, nachrichtendienstliche Informationen zu sammeln, Infrastrukturen zu zerstören und Zwietracht zu säen, sowie die Stimmung in der Öffentlichkeit in Europa zu beeinflussen.

WAS IST ZU ERWARTEN

Alles. Deswegen muss man:

> Seine Gegner kennen
> Den Identitäts- und Cloud-Schutz priorisieren
> Anfällige Komponenten patchen
> Den Ernstfall trainieren:
Seien Sie vorbereitet, wenn jede Sekunde zählt

Vollständigen Bericht lesen

Nur wer das Spiel der Angreifer versteht, kann gewinnen.

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.com/**
Folgen Sie uns:

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

CROWDSTRIKE
Protection that powers you