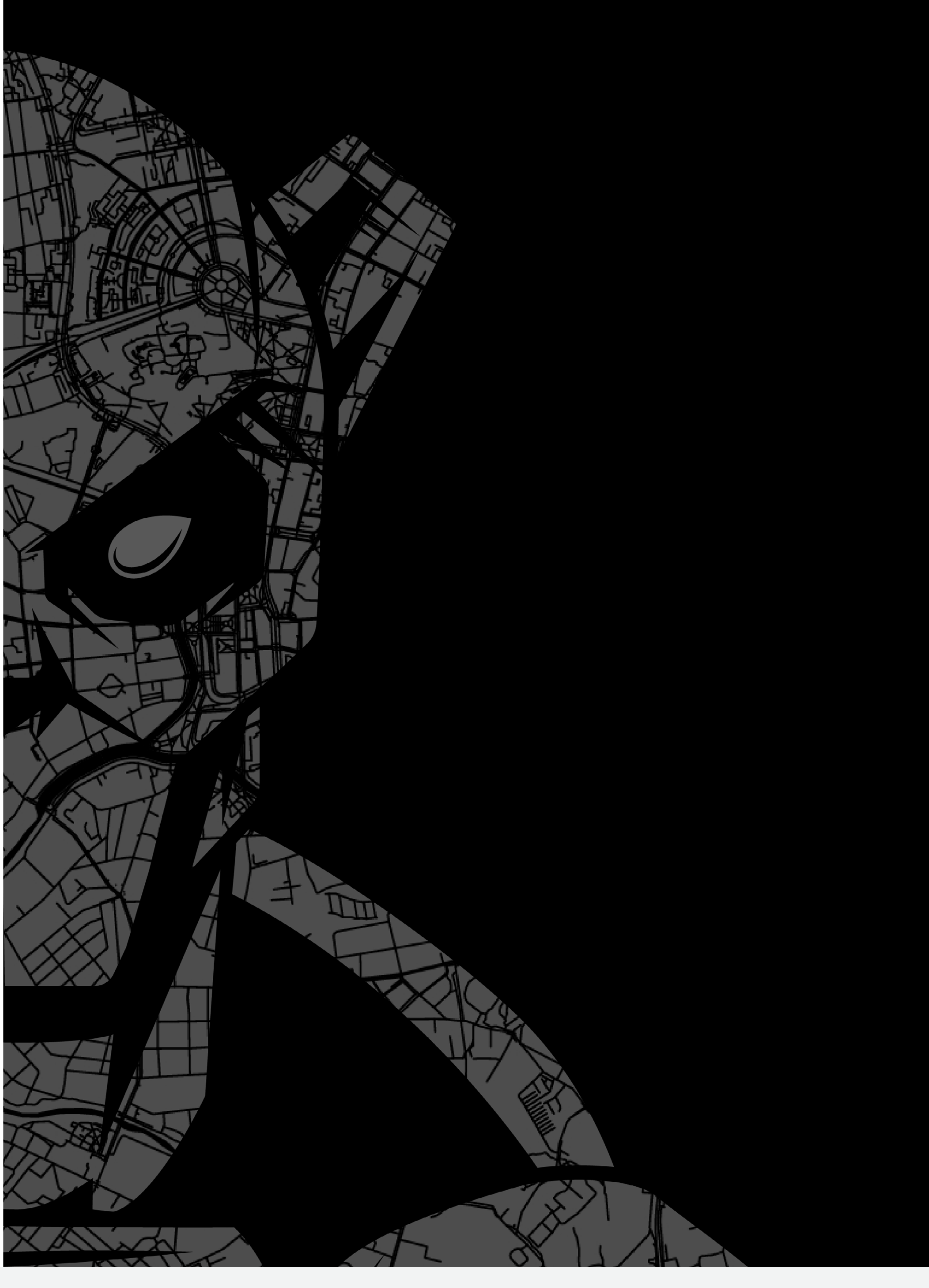
CROWDSTRIKE



2023 GLOBAL THREAT REPORT

Agressieve cybercriminelen gingen in 2022 nog sneller en geavanceerder te werk:
Wat u weten moet

Het 2023 Global Threat Report van CrowdStrike, een van de meest vertrouwde en uitgebreide analyses van het moderne dreigingslandschap en de ontwikkelingen in de manieren waarop cybercriminelen te werk gaan, geeft een overzicht van de belangrijkste trends in 2022 en de aanvallers die hierachter zitten.

MAAK KENNIS MET JE TEGENSTANDERS

eCRIME | DOOR EEN STAAT GESPONSORD | HACKTIVISTEN

33 nieuwe namen van aanvallers in 2022

200+ gevolgde tegenstanders

WAAR ZE ACTIEF ZIJN

- Technologie
- Financiële dienstverlening
- Gezondheidszorg
- Telecommunicatie
- Productie
- Academische wereld
- Overheid

HOE ZE TE WERK GAAN

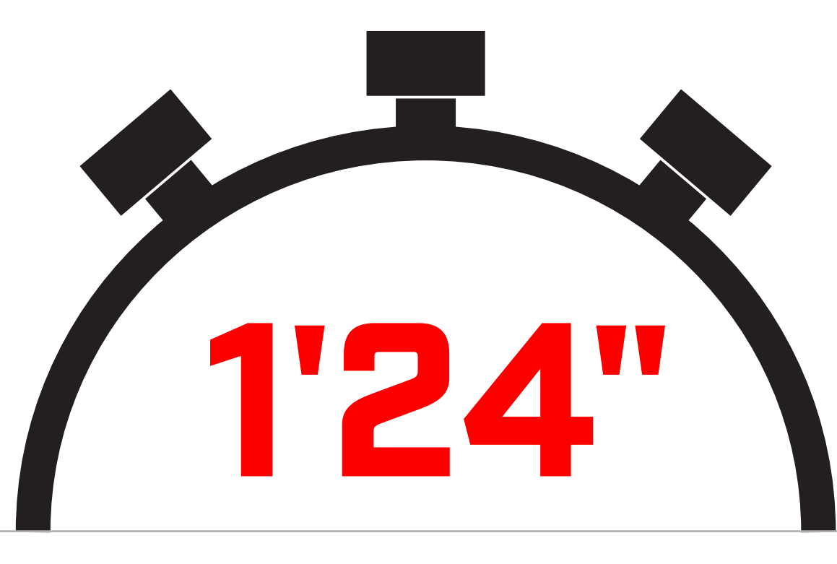
Het dreigingslandschap bleef in 2022 volop in beweging en vijandige activiteiten maakten het steeds moeilijker voor organisaties om zichzelf te beschermen.

98 MINUTEN

84 MINUTEN

BREAKOUT-TIJD BLIJFT ONDER DE 2 UR

Cybercriminelen hebben gemiddeld 1 uur en 24 minuten nodig om lateraal te bewegen, 14 minuten minder dan in 2021.



71%

VAN DE AANVALLEN WAS ZONDER MALWARE

Aanvallers maken steeds minder gebruik van malware en passen 'hands-on-keyboard'-technieken toe. Deze trend is deels gerelateerd aan het grootschalige misbruik van geldige inloggegevens om toegang te krijgen en persistentie mogelijk te maken, evenals het vermogen van aanvallers om snel misbruik te kunnen maken van zwakke plekken.

50%

TOENAME VAN INTERACTIEVE INBREUKEN

CrowdStrike zag een significante toename van interactieve inbreuken, met een opvallende stijging in het vierde kwartaal van 2022.

ADVERTENTIES VAN ACCESS BROKERS LIETEN EEN FORSE TOENAME VAN 112% ZIEN

Diensten van access brokers werden populairder in 2022. Er werden meer dan 2500 advertenties voor toegang geïdentificeerd. Dit is een aanzienlijke stijging ten opzichte van 2021, die duidelijk aangeeft dat de vraag naar diensten van access brokers groeit.

WAT ZE WILLEN

Aanvallers richtten zich in 2022 niet-aflatend op de data en infrastructuur van hun slachtoffers.

HET AANTAL INCIDENTEN MET CLOUDMISBRUIK NAM TOE MET 95%

In de loop van 2022 is het aantal zaken waarbij cloudbewuste actoren betrokken waren, bijna verdrievoudigd ten opzichte van 2021. Dit wijst erop dat cybercriminelen en natiestaten steeds meer over de benodigde kennis en technieken beschikken om cloudomgevingen aan te vallen.

GEGEVENSDIEFSTAL EN AFPERSING GINGEN DOOR – ZONDER RANSOMWARE

CrowdStrike Intelligence zag een toename van 20% in het aantal cybercriminelen die geen gebruik maakten van ransomware voor gegevensdiefstal en afpersing. Deze 'dubbele afpersing' is de meestgebruikte methode bij big game hunting (BGH).

HERGEBRUIK VAN KWETSBAARHEDEN VORMT EEN RISICO VOOR BLOOTGESTELDE COMPONENTEN

Uit Zero-day- en N-day-kwetsbaarheden in 2022 blijkt dat cybercriminelen in staat zijn om gespecialiseerde kennis te gebruiken om maatregelen uit eerdere patches te omzeilen en zich meerdere keren op dezelfde kwetsbare componenten te richten.

CHINA-NEXUS AANVALLERS WAREN DE ACTIEFSTE DOELGERICHTE GROEPEN BIJ INBREUKEN

China-nexus aanvallers, en actoren die vergelijkbare tactieken, technieken en procedures (TTP's) gebruiken, richtten zich in 2022 op bijna alle 39 industriesectoren wereldwijd en 20 geografische regio's die door CrowdStrike Intelligence worden gevolgd.

RUSLAND-NEXUS TEGENSTANDERS GINGEN DOOR MET MILITAIRE, PSYCHOLOGISCHE EN HACKTIVIST-AANVALLEN OP OEKRAÏNE

In heel 2022 werd een ongekend gebruik van cybermogelijkheden waargenomen, met als doel inlichtingen te verzamelen, infrastructuur te vernietigen of verdeeldheid te zaaien en het publieke sentiment in Europa te beïnvloeden.

WAT NU?

Wees op alles voorbereid. In het kort:

- Ken uw tegenstanders
- Geef identiteits- en cloudbeveiliging een hoge prioriteit
- Patch kwetsbare componenten
- Oefen je verdediging:
  Wees er klaar voor als elke seconde telt

Download het volledige rapport

U kunt ze alleen verslaan als u weet hoe ze te werk gaan.

Over CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), een wereldwijde leider op het gebied van cybersecurity, heeft een nieuwe invulling gegeven aan moderne beveiliging met 's werelds meest geavanceerde cloud-native platform voor het beschermen van cruciale bedrijfsrisico's: endpoints en cloudworkloads, identiteit en gegevens. Het CrowdStrike Falcon®-platform is gebaseerd op de CrowdStrike Security Cloud en AI van wereldklasse. Dit platform gebruikt realtime aanvalsindicatoren, informatie over bedreigingen, ontwikkelingen in de mogelijkheden van aanvallers en verrijkte telemetrie vanuit de hele onderneming om het volgende te bieden: hypernauwkeurige detecties, geautomatiseerde bescherming en herstel, geavanceerde opsporing van bedreigingen en waarneembaarheid van kwetsbaarheden op basis van prioriteit. Het Falcon-platform, dat speciaal voor de cloud is gebouwd met een architectuur met één lichtgewicht agent, biedt snelle en schaalbare implementatie, superieure bescherming en prestaties, minder complexiteit en onmiddellijke time-to-value.

CrowdStrike: **We stop breaches**.

Meer informatie: **https://www.crowdstrike.com/**

Volg ons:

Start vandaag nog met een gratis proefversie: **https://www.crowdstrike.com/free-trial-guide/**

CROWDSTRIKE
Protection that powers you