CROWDSTRIKE

2023 GLOBAL THREAT REPORT

Avversari implacabili incrementano velocità e sofisticazione nel 2022:
Cosa è necessario sapere

Il Global Threat Report 2023 di CrowdStrike, una delle analisi più affidabili e complete del settore relativa all'attuale panorama delle minacce informatiche e all'abilità operativa in continua evoluzione degli avversari, esplora le tendenze più significative del 2022 e gli attaccanti che le sostengono.

CONOSCI I TUOI AVVERSARI

HACTIVISTI | CRIMINALI | SPONSORIZZATI DAGLI STATI-NAZIONE

33 nuovi avversari identificati nel 2022

200+ avversari monitorati

DOVE SONO ATTIVI

- Tecnologia
- Financial Service
- Sanità
- Telecomunicazioni
- Manifatturiero
- Settore accademico
- Pubblica amministrazione

COME OPERANO

Il panorama delle minacce ha continuato ad evolversi nel 2022, con le operazioni degli avversari che hanno reso sempre più difficile alle organizzazioni garantirsi la protezione.

98' ⇣ 84'

IL TEMPO DI BREAKOUT RESTA INFERIORE ALLE 2 ORE

Ai criminali informatici servono in media 1 ora e 24 minuti per spostarsi lateralmente, 14 minuti in meno rispetto al 2021.

1'24"

71%

DEGLI ATTACCHI ERA PRIVO DI MALWARE

Gli avversari continuano a muoversi oltre il malware, impiegando tecniche di "hands-on-keyboard", una tendenza in parte connessa al loro prolifico abuso di credenziali valide per consentire l'accesso e la persistenza, nonché alla loro capacità di implementare rapidamente exploit delle vulnerabilità.

50%

INCREMENTO DELLE TATTICHE DI INTRUSIONE INTERATTIVE

CrowdStrike ha rilevato un aumento significativo delle intrusioni interattive, con un'impennata dell'attività nel quarto trimestre del 2022.

GLI ANNUNCI DI ACCESS BROKER HANNO ACCELERATO IL PASSO CON UN AUMENTO DEL 112%

La popolarità dei servizi di access broker è aumentata nel 2022 con oltre 2.500 annunci di accesso identificati, in netta salita rispetto al 2021, a sottolineare la crescente domanda dei servizi di access broker.

COSA CERCANO

Gli avversari si sono dimostrati implacabili nel prendere di mira i dati e le infrastrutture delle vittime nel 2022.

LO SFRUTTAMENTO DEL CLOUD È CRESCIUTO DEL **95%**

Nel corso del 2022, i casi che hanno coinvolto autori di minacce cloud-conscious sono quasi triplicati rispetto al 2021, a testimonianza di una tendenza sempre più ampia verso l'adozione di conoscenze e tecniche da parte dei protagonisti dell'eCrime e degli Stati-Nazione per colpire gli ambienti cloud.

IL FURTO DI DATI E LE CAMPAGNE DI ESTORSIONE SONO CONTINUATE, MA SENZA RANSOMWARE

Il team di CrowdStrike Intelligence ha osservato un aumento del 20% nel numero di avversari che operano mediante furto di dati ed estorsione, senza effettuare il deploy di ransomware. Questo modello di "doppia estorsione" è la tattica più comune tra gli avversari del big game hunting (BGH).

IL RIUTILIZZO DELLE VULNERABILITÀ METTE A RISCHIO I COMPONENTI ESPOSTI

Le vulnerabilità zero-day e N-day osservate nel 2022 hanno dimostrato la capacità degli avversari di utilizzare conoscenze specialistiche per aggirare le patch precedenti e prendere di mira a ripetizione gli stessi componenti vulnerabili.

GLI AVVERSARI DEL CHINA-NEXUS SONO STATI I GRUPPI DI INTRUSIONE MIRATA PIÙ ATTIVI

Gli avversari del China-nexus, e i criminali che adottano tattiche, tecniche e procedure (TTP) affini, nel 2022 hanno preso di mira quasi tutti i 39 settori industriali globali e le 20 regioni geografiche che CrowdStrike Intelligence monitora.

GLI AVVERSARI DEL RUSSIA-NEXUS HANNO CONTINUATO GLI ATTACCHI MILITARI, PSICOLOGICI E DI HACTIVISTI INFORMATICI CONTRO L'UCRAINA

Nel corso del 2022, è stato osservato un uso senza precedenti delle capacità informatiche, con l'obiettivo di raccogliere informazioni, distruggere infrastrutture o seminare divisioni e influenzare il sentimento pubblico che si riversa in Europa.

WHAT'S NEXT?

Tutto e niente. Per essere pronto, devi:

- Conoscere i tuoi avversari
- Dare la priorità alla protezione dell'identità e del cloud
- Applicare le patch ai componenti vulnerabili
- Esercitarti nella strategia di difesa:
  devi essere pronto a scattare quando non c'è nemmeno un secondo da perdere

Scarica il report completo

Capire il loro gioco è l'unico modo per batterli.

Informazioni su CrowdStrike

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), leader della sicurezza informatica a livello globale, sta ridefinendo la sicurezza nell'era del cloud grazie alla sua piattaforma di protezione degli endpoint creata appositamente per bloccare le compromissioni. L'architettura basata su un unico agent a basso impatto della piattaforma CrowdStrike Falcon® applica l'intelligenza artificiale a livello del cloud per offrire protezione e visibilità istantanee sull'intera azienda e prevenire gli attacchi agli endpoint ed ai workload sia all'interno che all'esterno della rete aziendale. Sfruttando la tecnologia proprietaria di CrowdStrike Threat Graph®, ogni settimana CrowdStrike Falcon crea correlazioni in tempo reale tra oltre 4 miglaia di miliardi di eventi legati agli endpoint provenienti da tutto il mondo, alimentando una delle piattaforme di sicurezza più avanzate mai esistite. Con CrowdStrike, i clienti ottengono una protezione migliore, prestazioni più elevate e un time-to-value immediato grazie alla piattaforma Falcon nativa del cloud.Ciò solo una cosa da ricordare di CrowdStrike: noi blocchiamo le compromissioni.

CrowdStrike: **We stop breaches**.

Ulteriori informazioni: **https://www.crowdstrike.com/it/**

Seguici

Avvia oggi stesso la prova gratuita: **https://www.crowdstrike.com/free-trial-guide/**

CROWDSTRIKE
Protection that powers you