

NESSUN POSTO DOVE
NASCONDERSICROWDSTRIKE
2023
THREAT
HUNTING
REPORT

Il tuo problema
non è il malware,
il tuo problema
sono gli avversari.

È fondamentale che i team di sicurezza sappiano
come operano i cybercriminali per essere
posizionati al meglio per fermarli.

Il Report sul threat hunting 2023 di CrowdStrike,
sviluppato dal team Counter Adversary
Operations di CrowdStrike, mette a nudo le
più recenti tecniche degli avversari e fornisce
conoscenze e approfondimenti per aiutare
a bloccare le compromissioni.

Nuove intuizioni sbalorditive

LE MINACCE ALL'IDENTITÀ SONO DIVENTATE MAINSTREAM

Gli avversari raddoppiano le intrusioni basate
sull'identità, mentre il furto e l'abuso di identità
compromesse hanno un impatto ancora più pesante.

62%

di intrusioni interattive che hanno
coinvolto identità compromesse

583%

di aumento del Kerberoasting, una tecnica
di attacco in ascesa basata sull'identità

L'ECRIME CRESCE MAN MANO CHE GLI AVVERSARI DIVENTANO PIÙ VELOCI

Gli avversari entrano ed escono dagli
ambienti più velocemente che mai.

79 MINUTI

era il tempo di breakout medio
dell'eCrime osservato

7 MINUTI

era il tempo di breakout più rapido
dell'eCrime osservato

GLI AVVERSARI SI FANNO PIÙ SCALTRI NEL CLOUD

I cybercriminali stanno diventando esperti di cloud:
sfruttano le comuni configurazioni errate e abusano
degli strumenti di gestione del cloud integrati.

160%

di aumento del furto di credenziali attraverso
le API dei metadati delle istanze cloud

RIFLETTORI PUNTATI SULLE COMPETENZE MULTIPIATTAFORMA

Le competenze su più sistemi operativi sono un tratto
distintivo delle intrusioni interattive nel 2023.

3X INCREMENTO

nella sostituzione da parte degli avversari
di Pluggable Authentication Modules (PAM)
con moduli dannosi in Linux

FINANZA, TECNOLOGIA E SERVIZI

i settori più colpiti

Scopri gli
avversari che ti
prendono di mira

CROWDSTRIKE MONITORA
ATTIVAMENTE QUESTI AVVERSARI
E PIÙ DI ALTRI 200. SCOPRI
DI PIÙ SU DI LORO NEL REPORT
SUL THREAT HUNTING 2023.



LABYRINTH CHOLLIMA

Ha guidato la carica in diversi
attacchi ai sistemi operativi

VICE SPIDER

Responsabile del 27% di tutti
gli attacchi di Kerberoasting

INDRIK SPIDER

È passato dall'eCrime opportunistico
agli attacchi personalizzati

Conoscolo.
Trovalo.
Fermalo.

- Ottieni conoscenze senza pari dai nostri esperti di threat hunting mentre parlano delle principali intrusioni e tecniche.
- Fai esperienze reali per potenziare la tua strategia di sicurezza e superare le minacce in rapida evoluzione.
- Resta un passo avanti agli avversari grazie alla comprensione delle tendenze globali e locali.

SCARICA IL REPORT