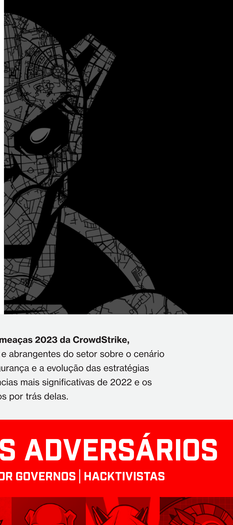
CROWDSTRIKE



RELATÓRIO GLOBAL DE AMEAÇAS 2023

Adversários implacáveis aumentam sua velocidade e sofisticação em 2022: **o que você precisa saber**

O Relatório Global de Ameaças 2023 da CrowdStrike, uma das análises mais confiáveis e abrangentes do setor sobre o cenário atual das ameaças à cibersegurança e a evolução das estratégias adversárias, explora as tendências mais significativas de 2022 e os adversários por trás delas.

CONHEÇA SEUS ADVERSÁRIOS

eCRIME | PATROCINADO POR GOVERNOS | HACKTIVISTAS

33 adversários recém-nomeados apareceram em 2022

+200 adversários rastreados

ONDE ELES ATUAM

- Tecnologia
- Finanças
- Saúde
- Telecomunicações
- Manufatura
- Ensino
- Governo

COMO ELES OPERAM

O cenário de ameaças seguiu evoluindo em 2022, com as operações adversárias tornando cada vez mais difícil para as organizações se protegerem.

98' ⇟ 84'

O TEMPO DE COMPROMETIMENTO PERMANECE ABAIXO DE 2 HORAS

Os adversários do eCrime precisam em média de 1 hora e 24 minutos para se mover lateralmente - uma redução de 14 minutos em relação a 2021.

71%

DOS ATAQUES FORAM LIVRES DE MALWARE

Os adversários continuam indo além do malware e empregando técnicas interativas "hands-on-keyboard", uma tendência parcialmente relacionada ao abuso prolífico de credenciais válidas para acesso e persistência, além de sua capacidade de operacionalizar rapidamente explorações de vulnerabilidade.

50%

SALTO DE 50% NAS CAMPANHAS DE INTRUSÃO INTERATIVA

A CrowdStrike observou um aumento *significativo* nas intrusões interativas, com pico de atividade no quarto trimestre de 2022.

ANÚNCIOS DE BROKERS DE ACESSO À TODA, COM UM AUMENTO DE 112%

A popularidade dos serviços de brokers de acesso aumentou em 2022, com mais de 2.500 anúncios identificados, um aumento acentuado em relação a 2021 – ressaltando a crescente demanda por serviços de brokers de acesso.

O QUE ELES BUSCAM

Os adversários foram implacáveis ao atacar os dados e infraestrutura das vítimas em 2022.

INCIDENTES DE EXPLORAÇÃO EM NUVEM CRESCERAM 95%

Ao longo de 2022, os casos envolvendo agentes de ameaças "cloud-conscious" quase triplicaram em relação a 2021, uma manifestação da tendência ampla de atores do eCrime e associados a governos adotarem técnicas e conhecimentos para atingir ambientes em nuvem.

AS CAMPANHAS DE ROUBO DE DADOS E EXTORSÃO CONTINUARAM — SEM RANSOMWARE

A CrowdStrike Intelligence observou um aumento de 20% no número de adversários executando roubo de dados e extorsão sem implantar ransomware. Esse modelo de "extorsão dupla" é a tática mais comum entre os adversários de Big Game Hunting (BGH).

A REUTILIZAÇÃO DE VULNERABILIDADES COLOCA OS COMPONENTES EXPOSTOS EM RISCO

Vulnerabilidades de Dia zero e Dia N observadas em 2022 demonstram a capacidade dos adversários de usar seu conhecimento especializado para contornar as mitigações de correções anteriores e atingir os mesmos componentes vulneráveis várias vezes.

ADVERSÁRIOS ASSOCIADOS À CHINA FORAM OS GRUPOS DE INTRUSÃO DIRECIONADA MAIS ATIVOS

Os adversários ligados à China - e atores que usam táticas, técnicas e procedimentos (TTPs) que se identificam com eles - foram vistos atacando quase todos os 39 setores da indústria global e as 20 regiões geográficas rastreadas pela CrowdStrike Intelligence em 2022.

ADVERSÁRIOS ASSOCIADOS À RÚSSIA SEGUIRAM SEUS ATAQUES MILITARES, PSICOLÓGICOS E HACKTIVISTAS CONTRA A UCRÂNIA

Ao longo de 2022, foi observado um uso sem precedentes de capacidades cibernéticas para coletar inteligência, destruir infraestrutura ou semear divisão e influenciar o sentimento público que se espalha pela Europa.

O QUE VEM A

Tudo e qualquer coisa. Para estar preparado, você precisa:

- Conhecer seus adversários
- Priorizar a proteção de identidade e nuvem
- Corrigir componentes vulneráveis
- Treinar como se fosse valendo: **esteja pronto para quando cada segundo contar**

Baixe o relatório

Entender o jogo deles é a única maneira de vencê-los.

Sobre a CrowdStrike

A CrowdStrike Holdings, Inc. (Nasdaq: CRWD), líder global em segurança cibernética, redefiniu a segurança moderna com a plataforma nativa de nuvem mais avançada do mundo para proteger áreas críticas de risco corporativo — endpoints e cargas de trabalho, identidade e dados em nuvem. Alimentada pela CrowdStrike Security Cloud e IA de classe mundial, a plataforma CrowdStrike Falcon® utiliza indicadores de ataque, inteligência de ameaças, evolução de tática adversária e telemetria enriquecida de toda a empresa, em tempo real, para fornecer detecções hiperprecisas, proteção e remediação automatizadas, investigação de ameaças de elite e observabilidade priorizada de vulnerabilidades. Construída especificamente na nuvem com uma única arquitetura de agente leve, a plataforma Falcon oferece implementação rápida e escalável, proteção e desempenho superiores, complexidade reduzida e retorno imediato do valor.

CrowdStrike: **Nós interrompemos ataques**.

Saiba mais https://www.crowdstrike.com.br

Nos siga:

Comece uma avaliação gratuita hoje: https://www.crowdstrike.com/free-trial-guide/

CROWDSTRIKE
Protection that powers you