CROWDSTRIKE

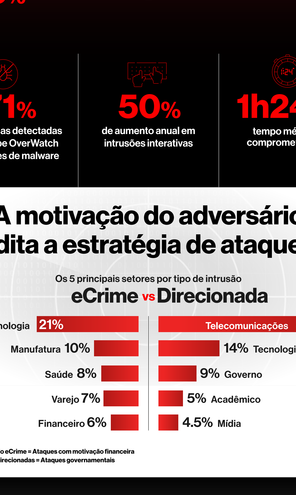
NÃO HÁ ONDE SE ESCONDER

Relatório de Investigação de Ameaças Falcon OverWatch 2022

A cada ano, a Falcon OverWatch™, equipe de investigação de ameaças proativa 24x7 da CrowdStrike, publica suas descobertas e análises técnicas detalhando as novas e proeminentes estratégias adversárias e as tendências emergentes do intrusões que a equipe descobriu nos 12 meses anteriores, nessa edição, de 1º de julho de 2021 a 30 de junho de 2022. Neste último ano em particular, a OverWatch observou mudanças impressionantes na forma como os invasores projetam e executam seus ataques.

As intrusões se intensificam, a complexidade escala

2022



71%
das ameaças detectadas pela equipe OverWatch foram livres de malware

50%
de aumento anual em intrusões interativas

1h24m
tempo médio de comprometimento

A motivação do adversário dita a estratégia de ataque

Os 5 principais setores por tipo de intrusão

eCrime vs Direcionada

Intrusões do eCrime = Ataques com motivação financeira
Intrusões direcionadas = Ataques governamentais

Estratégias novas e em destaque

IceApple

Objetivos
Evasão de defesa, acesso a credenciais, exfiltração

Alvos
Servidores IIS

Características
- Framework de pós-exploração sofisticado baseado em .NET
- Explora assemblies .NET carregados através de reflexão
- Baixa pegada forense, residindo na memória

fscan

Objetivos
Descoberta

Alvos
Host interno, mapeamento de ambiente

Características
- Ferramenta adversária em alta no final de 2021/início de 2022
- Scanner de vulnerabilidade adaptado para fingerprinting avançado
- Exploração por meio de modificação de chave pública, comandos SSH

Sweet Potato

Objetivos
Elevação de privilégios

Alvos
Credenciais do sistema operacional Windows, Tokens de segurança

Características
- Força a autenticação do sistema para capturar credenciais em trânsito
- Primeira variação, "Hot Potato", descoberta em 2016
- O script automatizado tenta múltiplas variações (por exemplo, Juicy Potato, Lonely Potato, etc.)

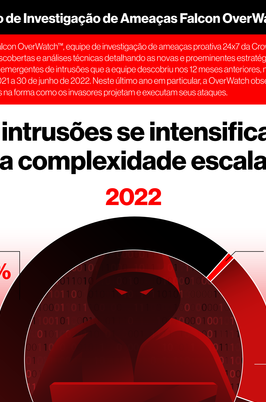
Web Server Zero-Day

Objetivos
Persistência (via web shell), reconhecimento interativo, coleta de credenciais, exfiltração

Alvos
Instâncias de data center e servidor Confluence

Características
- Vulnerabilidade que habilita a execução remota de código não autenticado
- Observado no eCrime e intrusões direcionadas
- Ataque em fases envolvendo implantação de web shell, reconhecimento interativo, coleta de credenciais, recuperação remota de ferramentas

A investigação proativa de ameaças não é uma ferramenta, é uma missão



Conheça a estratégia. Conheça o adversário.
Investigue implacavelmente.

Relatório de Investigação de Ameaças Falcon OverWatch 2022

Faça o download do relatório completo

Saiba mais: https://www.crowdstrike.com/services/
Notícias

CROWDSTRIKE

Nós interrompemos ataques