elastic security labs

Relatório Global de Ameaças de 2022

Infográfico

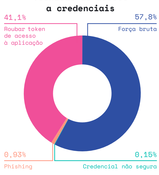
De onde estão vindo as ameaças?

Com base na telemetria da solução, o Relatório Global de Ameaças de 2022 do Elastic Security Labs revela fenômenos, tendências e recomendações sobre ameaças para ajudar as organizações a se preparar para o futuro. As descobertas incluem...

No mundo real, as nuvens ficam mais seguras quando se implementam controles acima do padrão

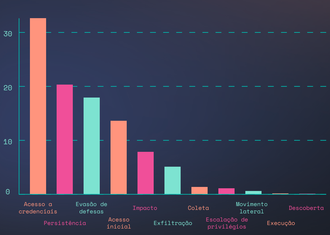
Quase 41% dos alertas de acesso a credenciais foram de tentativas de roubar tokens de acesso a aplicações em comparação com outros elementos com credenciais.

Técnicas de acesso a credenciais



Porcentagens de técnicas do MITRE ATT&CK para tática de acesso a credenciais

Uma vez dentro, a prioridade nº 1 dos invasores é conseguir acesso a credenciais



Porcentagens do total de nomes de táticas do MITRE ATT&CK para alertas de detecção baseados na nuvem

O software comercial está sendo usado como arma

Malware projetado para red teams está sendo usado contra as organizações.

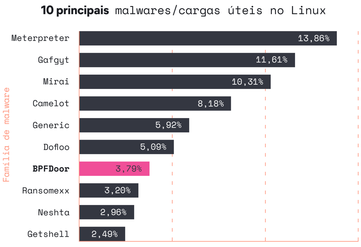
O CobaltStrike foi o binário ou carga útil malicioso mais popular para endpoints do Windows, seguido pelo AgentTesla e pelo RedLineStealer.

Todas as detecções

- CobaltStrike..... 35%
- AgentTesla..... 25%
- RedLineStealer..... 10%

O software aberto não é tão seguro quanto você pensa

10 principais malwares/cargas úteis no Linux



10 principais malwares e cargas úteis do Linux, mostrando o aumento da atividade do BPFDoor

Os trojans continuam a ser uma das maneiras preferidas de usar entregáveis como arma

Malware por categoria

- Trojan..... 80,5%
- Criptominerador... 11,3%
- Ransomware..... 3,7%
- Packer..... 2,4%
- Backdoor..... 0,9%
- Proxy..... 0,7%
- Outros..... 0,5%

Boas notícias – a segurança do endpoint está funcionando

Os ataques a endpoints estão se tornando mais diversificados nos esforços para contornar as defesas. Este ano, observamos 50 técnicas diferentes de infiltração em endpoints que não funcionaram.

Técnica	Porcentagem do sinal
Mascaramento	44,29%
Execução de proxy binário do sistema	30,00%
Manipulação de token de acesso	12,32%
Injeção de processo	7,02%
Trabalhos de BITS	4,74%
Execução de proxy de utilitários de desenvolvedores confiáveis	0,90%
Processamento de script XSL	0,66%
Enfraquecimento de defesas	0,65%
Exploração para evasão de defesas	0,64%
Execução de proxy de script do sistema	0,13%
Modificação do Registro	0,03%
Remoção do indicador no host	0,01%

Obtenha informações completas sobre as descobertas dos pesquisadores do Elastic Security Labs no Relatório Global de Ameaças de 2022