MASSIMA FROG

Ransomware:

Números, Tendências e Impactos

O cenário de ransomware no Brasil e no Mundo

Preparado por:
Massima Frog

Apoio:
Bunker CS

Conteúdo:
Consolidado de relatórios de cibersegurança e informações públicas de mercado.

Data:
dez-2025

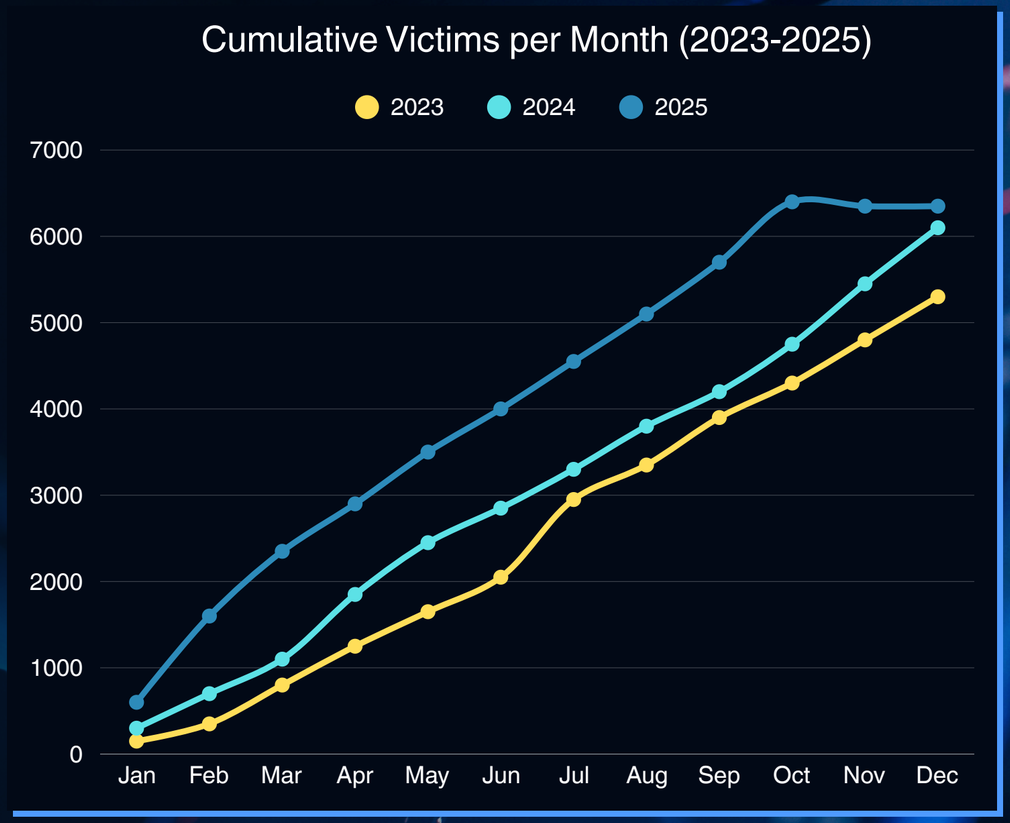
Ransomware

Altamente lucrativo e eficaz para os criminosos

Ransomwares nunca estiveram tão ativos no Brasil.

- Hospitais, indústrias, escritórios de advocacia, redes varejistas — ninguém está fora da mira.
- Atinge empresas de todos os portes, em todas as regiões
- Com conhecimento, IA, tempo e dinheiro, basta um elo fraco: uma credencial exposta já pode ser o suficiente.

Aumento de atividades global, e no Brasil existe a mesma tendência.



Número de vítimas acumulado:

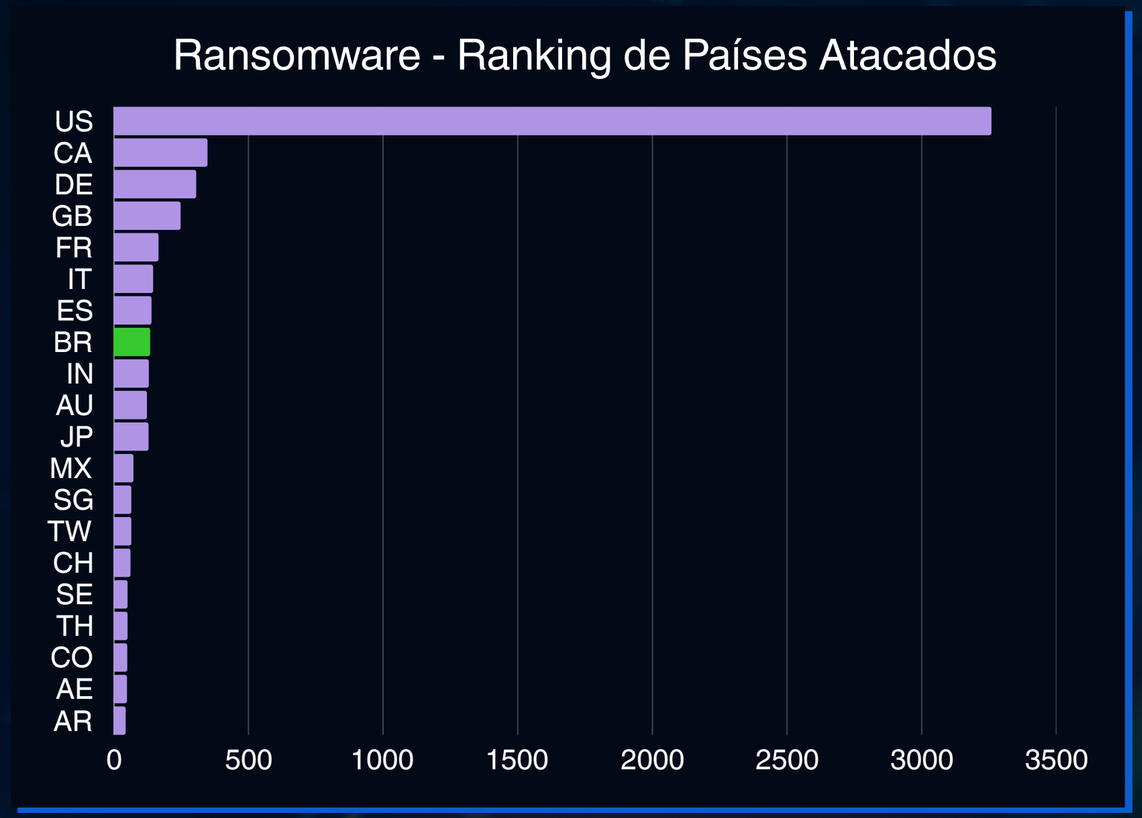
Out/2023	Out/2024	Out/2025
4.297	4.748	6.417

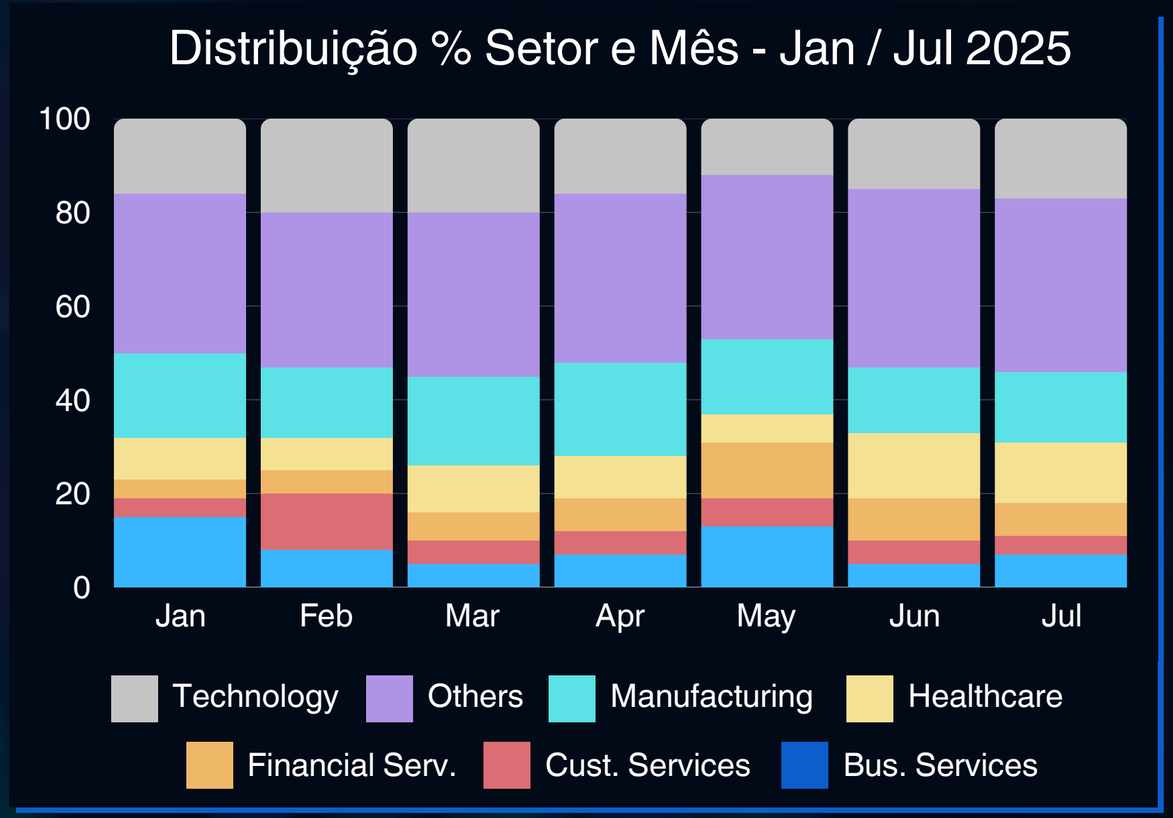
fonte: https://www.cisoadvisor.com.br/akira-amplia-ofensiva-de-ransomware-global/

Brasil como Alvo

Empresas de todos os setores estão na linha de fogo.

MASSIMA FROG





Fonte: Ransomware Statistics for 2025 (Ransomware.Live)

Analisando 195 países...

Geralmente o Brasil oscila entre a quarta e a oitava posição como um dos países mais atacados no mundo...

Nenhum setor está a salvo...

Os criminosos agem organizados como empresas, diversificando seus alvos...

Nem as gigantes são imunes

Se isso acontece com quem investe milhões, o risco para o restante do mercado é exponencial.

CNN BRASIL — Ao vivo | Política | WW | Money | Esportes | Pop | Viagem & Gas

Site da [redacted] sai do ar após ataque hacker – entenda o caso

Uma das empresas de TI que atende a varejista disse que seus sistemas não foram afetados. A suspeita é que o ataque se concentra em servidores de Porto Alegre

Leonardo Guimarães,
20/08/21 às 09:37 | Atualizado 20/08/21 às 09:37

Fonte: caso em grande empresa de varejo (link)

tiinside

Início › Newsletter (TI Inside)

ATAQUES

[redacted] sofre segundo ataque hacker

Por **Redação** - 5 de janeiro de 2025

Fonte: caso em grande empresa de serviços financeiros (link)

exame.

Varejista [redacted] é alvo de ataque cibernético

Empresa foi vítima de um ataque ransomware, mas afirmou que o impacto nas operações foi mínimo e que suas lojas físicas seguem funcionando normalmente

Fonte: caso em grande empresa de varejo (link)

CISO Advisor desde 2019

CIBERCRIME

Grupo alega ter invadido a [redacted] e exibe telas

Paulo Brito 30/12/2021 18:42

Fonte: caso em grande empresa de telecomunicações (link)

veja Negócios

[redacted] vai pagar R$ 1,5 milhão por vazamento de dados de clientes

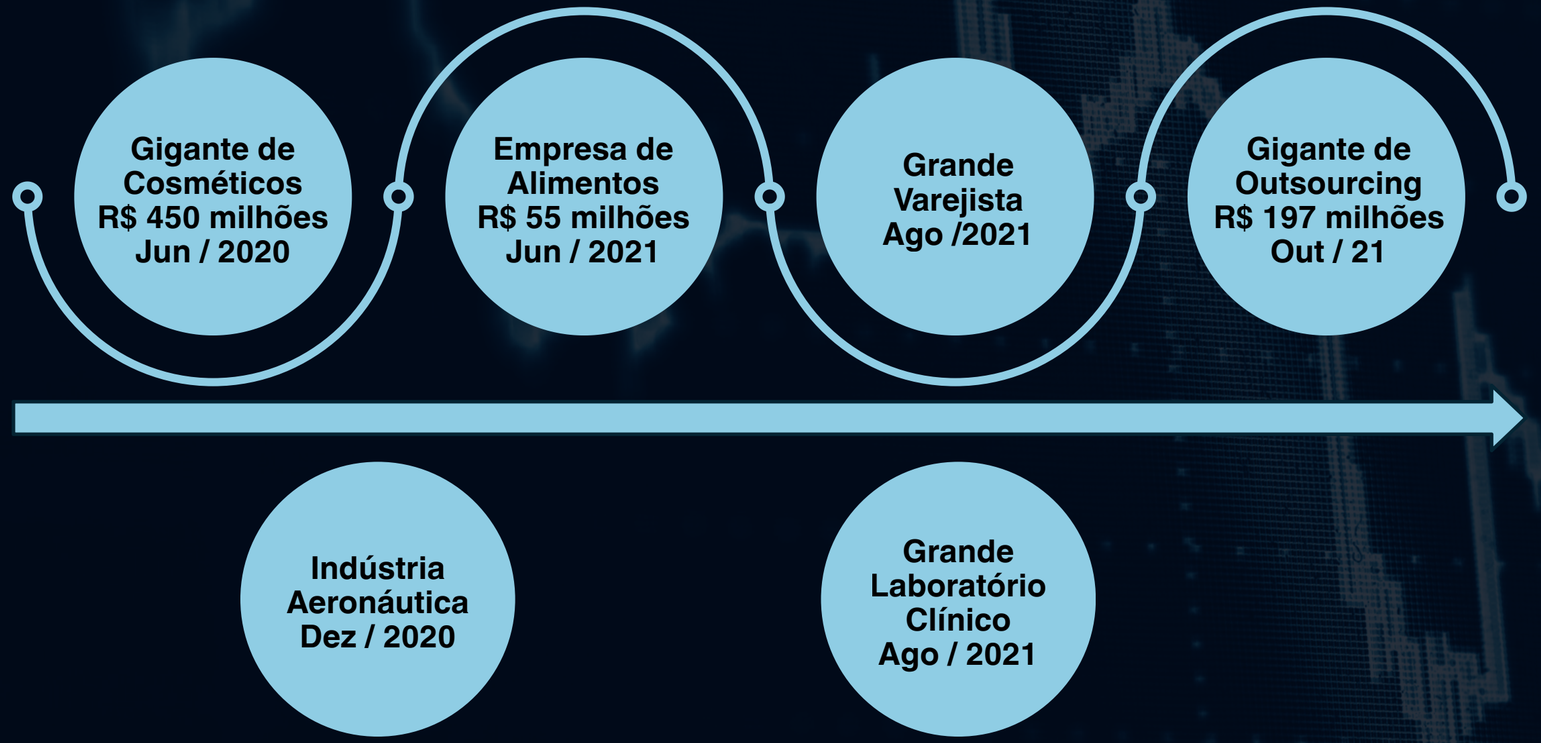
Investigação constatou o comprometimento dos dados cadastrais de 19.961 correntistas – 13.207 continham informações bancárias

Por Redação
| 19 dez 2018, 07h31 • Atualizado em 19 dez 2018, 08h21

Fonte: caso em grande empresa de serviços financeiros (link)

Muito além das manchetes...

A maioria dos ataques nunca é divulgada. PMEs caem em silêncio — e, muitas vezes, são a porta de entrada para grandes empresas



2021 – apresentou aumento de 92% em relação a 2020[1]

2022 – numero de tentativas de intrusão no Brasil 31 Bilhões[2]

2023 – 44% das empresas no Brasil sofreram ataques de Ransomware[3]

Kaspersky registrou 483 mil detecções de Ransomware em 2023[4].
Jun/23 a Jul/24 média de 1.334 ataques por dia[5].

Fontes:
1 – Estudo apontado por Varonis
2 - Estudo da Sonicwall mencionado
3 – Matéria Infomoney
4 – Estudo Karspersky
5 – Informação Karspersky

EDR não é estratégia de resiliência

Detectar comportamento não é o mesmo que impedir a criptografia.

EDR / XDR são plataformas generalistas

- Monitoram todo o ciclo de ataque e analisam comportamento, mas dependem fortemente de contexto.
- Utilizam IA, machine learning e análise comportamental, porém nem sempre detectam ransomware no estágio inicial.

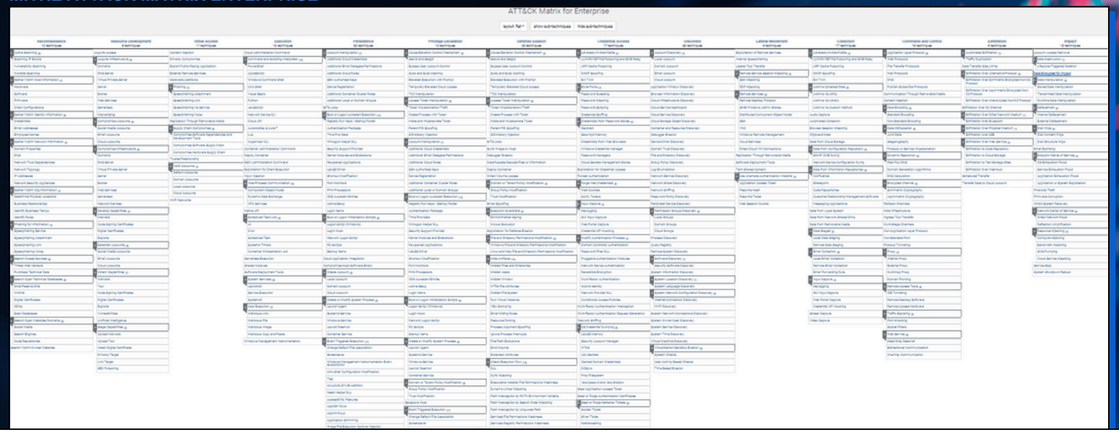
Ransomware não é um vetor único

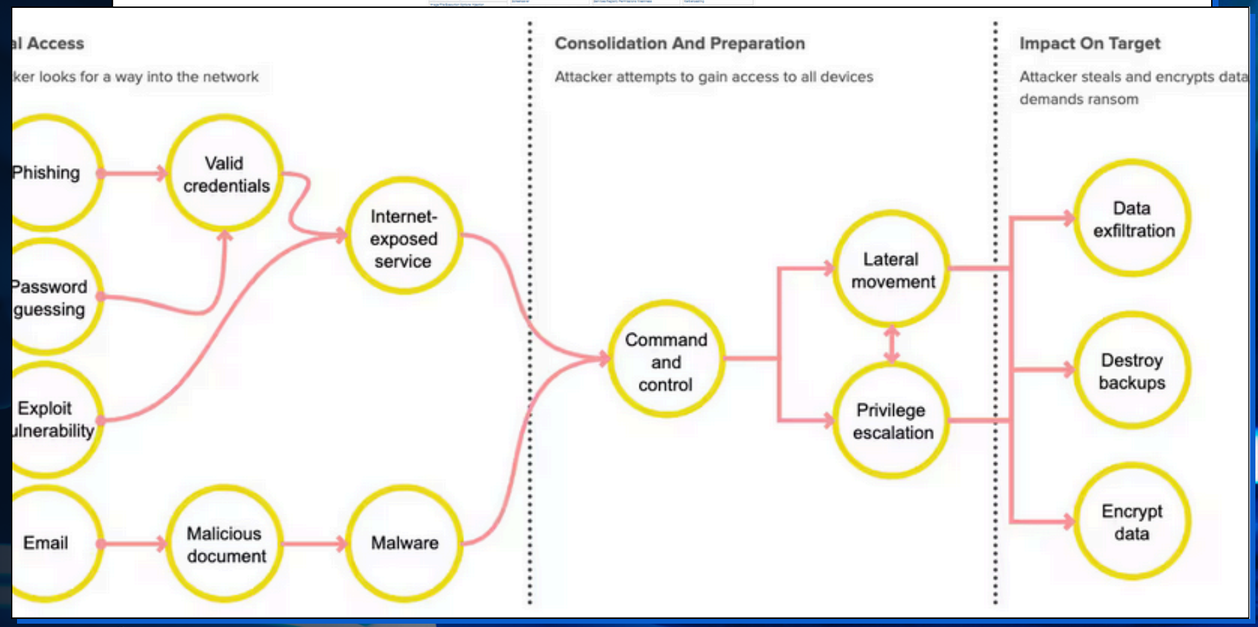
- Explora múltiplas táticas simultâneas e pontos cegos operacionais.

Confiar em uma defesa genérica não é uma estratégia

- A complexidade atual exige camadas especializadas e complementares.

MITRE ATTACK MATRIX ENTERPRISE





CORRELAÇÃO DE EVENTOS

O limite das defesas tradicionais

Visibilidade não é o mesmo que contenção

NGAV e EDR são essenciais...

... mas **não resolvem** sozinhos o problema do ransomware.

- NGAV - previne ameaças conhecidas e desconhecidas, mas depende de padrões, modelos e contexto.
- EDR / XDR - monitora o ciclo completo do ataque, correlaciona eventos e apoia investigação e resposta.
- O ponto crítico - ransomware moderno age rápido, silencioso e antes da correlação comportamental completa.

Resultado:

- Mesmo ambientes maduros de NGAV e EDR, o ransomware pode passar desapercebido ou ser detectado apenas depois que a criptografia já começou.

Resiliência exige defesa em camadas

Ameaças especializadas exigem respostas especializadas

Ransomware não é apenas malware...

... é uma técnica de impacto.

- **Camada 1 – Prevenção (NGAV / EDR)**
  Bloqueia parte dos ataques iniciais.
- **Camada 2 – Detecção e resposta (EDR / XDR)**
  Analisa comportamento, contexto e movimentação lateral.
- **Camada 3 – Contenção especializada anti-ransomware**
  *Atua no momento da criptografia, baseado em **lógica matemática**, detectando e bloqueando o processo antes do impacto.*

Resultado:

- Mesmo quando algo passa pela defesa das camadas de prevenção, detecção e resposta, o dano não acontece.

Onde o ransomware realmente causa dano

Quando a criptografia começa, o tempo de resposta é zero

Security Snares - age no exato momento do impacto!

- atua exatamente onde as defesas tradicionais não conseguem reagir a tempo.
- focado exclusivamente no momento crítico do ataque: a tentativa de criptografia maliciosa.
- Atua independente de contexto, IA, machine learning ou correlação comportamental.
- Bloqueia o processo de criptografia no primeiro arquivo, antes que o impacto se espalhe.

Resultado:

- Mesmo que o ataque passe pelas camadas anteriores, **o dano não acontece.**

Uma abordagem focada exatamente onde o problema acontece

Especializada onde a defesa genérica falha

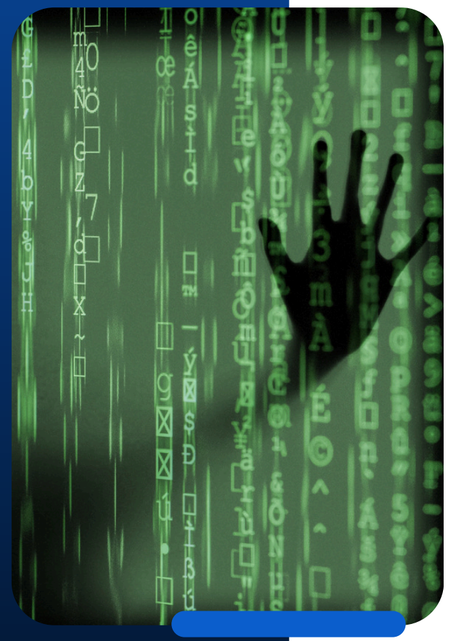
O Security Snares não tenta prever o ataque

Ele impede o impacto!

- Agente leve, sem reboot e com consumo mínimo de recursos.
- Aprende os processos criptográficos legítimos do ambiente.
- Qualquer tentativa de criptografia desconhecida é automaticamente bloqueada — inclusive em cenários Zero Day, Zero Hour ou Zero Second.
- Ao bloquear, notifica o ecossistema de segurança (EDR, XDR, SIEM) para investigação e resposta coordenada.

Resultado:

- A criptografia maliciosa é interrompida **antes que o dano aconteça**.



Casos com Security Snares

UNISYS (WHITE LABEL)

(Unisys Ransomware Protection Service)

A Unisys gerencia tecnologias EDR para seus clientes. Após enfrentar diversos ataques de ransomware, testou o SecuritySnares e outras soluções e optou pela SecuritySnares como componente central de seu serviço de proteção. Atualmente, também está implementando o RansomSnare internamente, após um incidente que não foi detectado.

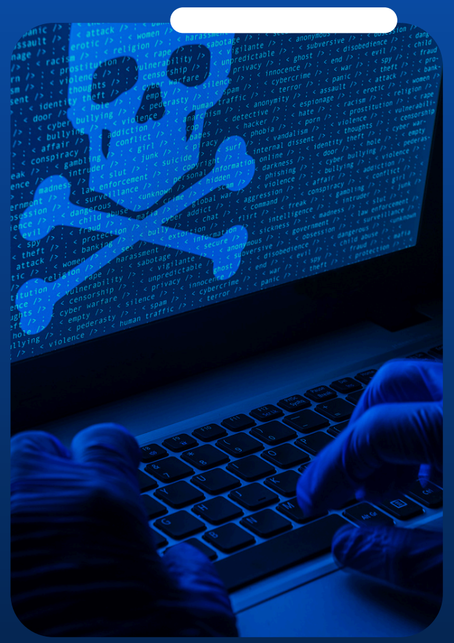
Casos com Security Snares

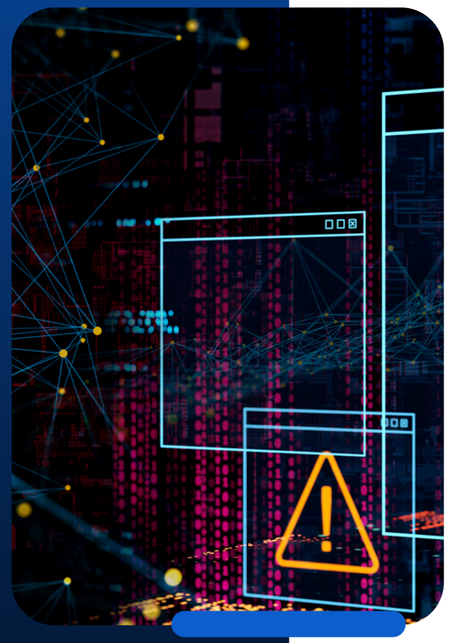
SHELBY COUNTY SCHOOL DISTRICT (MEMPHIS, TN)

Cliente atual de um EDR líder de mercado, sofreu uma paralisação em todo o distrito por conta de um ataque de ransomware não detectado. Estão em processo de expansão do uso da SecuritySnares para todo o condado e, possivelmente, para o Estado do Tennessee.

FLYNN GROUP (CONSTRUTORA DO CANADÁ)

Preocupada com as limitações dos EDRs contra Ransomwares, testou a eficácia da solução com amostras de ransomware do VirusTotal e identificou diversas brechas. Isso motivou a adoção do RansomSnare.





Casos com Security Snares

TRIARQ HEALTH (BLUE CROSS/BLUE SHIELD OF MICHIGAN)

Anteriormente cliente de um EDR líder de mercado, a Triarq migrou para um EDR concorrente após aquisição pela BCBS. Mesmo assim, continuou enfrentando falhas na detecção de ransomware com ambas as soluções. Como provedor de serviços em nuvem para o setor de saúde, o caso evidenciou as limitações dos líderes tradicionais em ambientes críticos.

BIRMINGHAM PUBLIC SCHOOL DISTRICT

Iniciou com um EDR líder, depois migrou para outro EDR através de um subsídio do governo estadual de Michigan, mas também sofreu um incidente com ransomware. Após testes, decidiram implantar o RansomSnare em todo o distrito escolar.

MASSIMA FROG

Obrigado

fale conosco:

contact-us@massimafrog.com

www.linkedin.com/company/massimafrog/

www.massimafrog.com

baixe o folder:

*- A **Massima Frog** é parceira oficial da Security Snares e a **Bunker CS** é distribuidora exclusiva da Security Snares no Brasil -*