
INITIATING SYSTEM BOOT..
DECRYPTING ICS LABS ANNUAL REPORT.
ACCESS GRANTED.
ICS LABS
THREAT REPORT 2025

NOVO HORIZONTE DE AMEAÇAS

O cenário digital atual foi marcado por uma evolução constante das ameaças cibernéticas, que se tornam mais sofisticadas e frequentes a cada ano.

Conseguimos observar um aumento expressivo nos ataques, com destaque para o Brasil, onde a superfície de exposição cresceu significativamente.

Esse contexto exige que empresas, governos e usuários adotem práticas cada vez mais rigorosas para garantir a segurança de seus ativos e informações.

O Relatório Anual de Ameaças do ICS Labs apresenta um panorama detalhado das ameaças bloqueadas pelos mecanismos de segurança da organização, os principais vetores de ataque identificados e os desafios enfrentados ao longo do ano, oferecendo insights estratégicos para fortalecer a postura de segurança no próximo ciclo.

01

PANORAMA GLOBAL DE AMEAÇAS

CENÁRIO GLOBAL DE AMEAÇAS CIBERNÉTICAS

Tendências, vetores e impactos observados em escala global

Em 2025, o cenário de ameaças cibernéticas evoluiu de forma significativa, com ataques cada vez mais direcionados, automatizados e orientados à monetização e extorsão.

Megaincidentes de vazamento de dados expuseram bilhões de credenciais globalmente, impulsionados principalmente pelo uso massivo de infostealers, campanhas de ransomware sem criptografia e exploração de falhas críticas em serviços amplamente utilizados.

Além do impacto operacional, esses eventos ampliaram substancialmente os riscos regulatórios, especialmente sob a LGPD, elevaram o custo médio por violação e provocaram danos reputacionais severos. Diante desse contexto, a capacidade de detecção precoce, monitoramento contínuo e resposta coordenada tornou-se fator crítico para a contenção de ameaças antes que causem impactos sistêmicos à infraestrutura e ao negócio.

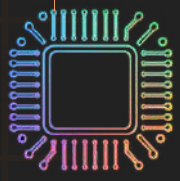
UMA NOVA ECONOMIA DE AMEAÇAS

A consolidação de infostealers e ataques de extorsão redefiniu o custo, a velocidade e a escala dos incidentes cibernéticos, reduzindo o tempo de detecção, ampliando o alcance dos ataques e pressionando organizações a responderem de forma cada vez mais ágil e coordenada.


REC
GOVERNO
13%
SAÚDE
10%
ENSINO
8%
TECH
32%
FINANÇAS
23%
INDÚSTRIA
26%
SYNTH-CORP
SCHOOL
TECH ACADEMY
BIO-MED CENTER
NEO-LIFE
CITY AUTHORITY

SETORES SOB ATAQUE

DISTRIBUIÇÃO DE INCIDENTES . 2025



TECNOLOGIA

32%

INDÚSTRIA

26%

FINANÇAS

23%

Vetor Primário: Exploração de vulnerabilidades em softwares de gestão (ITSM/SaaS)
Impacto: Ataques de Cadeia de Suprimentos (Supply Chain). Os invasores comprometem o fornecedor de tecnologia para usar seus acessos legítimos como "ponte".

Vetor Primário: Ransomware direcionado a ambientes OT (Operacionais).
Impacto: Foco na interrupção de linhas de produção para forçar pagamentos rápidos de resgate.

Vetor Primário: Trojans bancários avançados e Spear Phishing.
Impacto: Tentativas de fraude financeira direta e exfiltração de credenciais de alto privilégio.

ANÁLISE ESTRATÉGICA: O IMPACTO SISTÊMICO

A Crise de Confiança na Tecnologia (32%)

Liderando o ranking de vítimas, empresas de tecnologia e software enfrentam uma ofensiva voltada à exploração de vulnerabilidades zero-day em ferramentas de ITSM e acesso remoto. Criminosos utilizam credenciais roubadas de desenvolvedores e Brokers de Acesso para inserir malwares diretamente em atualizações legítimas ou plataformas de suporte. O objetivo não é apenas o dado da empresa de tech, mas usar sua credibilidade e acessos privilegiados para infiltrar-se silenciosamente em setores críticos como Governo e Saúde.

A Convergência TI/OT na Indústria

A liderança da manufatura no ranking de incidentes (26%) não é acidental. Em 2025, testemunhamos a consolidação da convergência entre TI (Tecnologia da Informação) e OT (Tecnologia Operacional). Fábricas que antes eram ilhas isoladas agora estão conectadas à nuvem. Os atacantes exploraram essa nova superfície de ataque, utilizando ransomwares projetados especificamente para paralisar linhas de montagem, sabendo que cada minuto de inatividade custa milhões, forçando pagamentos de resgate recordes.

***ICS Labs Response:** O ICS EDR detectou mais de 1.247 tentativas de intrusão em clientes industriais, evitando paradas que significariam prejuízos inestimáveis.*

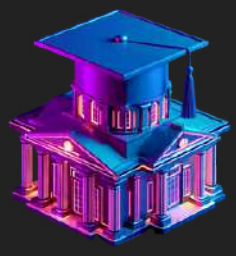
ALVOS DE OPORTUNIDADE

Vulnerabilidade em Infraestrutura Crítica e Acadêmica

A Fragilidade Governamental:
Órgãos governamentais operam, em grande parte, com infraestrutura crítica obsoleta. A falta de segmentação de rede permite que um comprometimento em um departamento administrativo escale para sistemas essenciais ao cidadão.
Vetor Principal:
Exploração de vulnerabilidades não corrigidas (Patch Management falho) e credenciais vazadas na Dark Web.

287 DIAS

TEMPO MÉDIO DE DETECÇÃO SEM UMA PROTEÇÃO ADEQUADA



A Tempestade Perfeita:
O setor de ensino tornou-se o alvo preferencial para grupos de Ransomware em 2025.
Com orçamentos de segurança limitados e uma cultura de 'compartilhamento aberto', escolas e universidades sofrem com o sequestro de dados de pesquisa e informações sensíveis de alunos menores de idade.
Vetor Principal: Phishing direcionado a corpo docente e alunos (Engenharia Social).

+150%

AUMENTO EM ATAQUES DE RANSOMWARE EM 2025.

Fonte: Sophos State of Ransomware Report 2025
Fonte:IBM X-Force Threat Intelligence Index 2025

A ESCALADA

Por que 2025 marcou o ponto de inflexão mais crítico da última década em ameaças cibernéticas

01 // A CAUSA

O GATILHO: COMODITIZAÇÃO DO ACESSO

~~US$ 3.300~~

↓ 61%

$1.3K

PREÇO MÉDIO DE ACESSO INICIAL

O preço para um criminoso comprar credenciais de acesso a uma rede corporativa despencou 61% em 2025. O que antes custava US$ 3.300 agora pode ser adquirido por apenas US$ 1.300 em marketplaces da Dark Web. Atacar ficou muito barato.

02 // A CONSEQUÊNCIA

O VOLUME: EXPLOSÃO DE INCIDENTES

32.576

Incidentes Globais Registrados

Com o acesso barato, o volume de ataques explodiu. Organizações de todos os portes tornaram-se alvos economicamente viáveis para grupos criminosos que antes focavam apenas em grandes corporações.

A barreira de entrada caiu. Qualquer rede conectada à internet agora é um alvo lucrativo. A democratização do acesso transformou o cibercrime em uma indústria de escala massiva.

03 // A ESTRATÉGIA

O ALVO: TECNOLOGIA COMO VETOR

Os atacantes não estão atirando aleatoriamente. Existe um método. O setor de Tecnologia concentra 32% dos ataques porque comprometê-lo significa comprometer toda a cadeia de suprimentos.

32% **Setor de Tecnologia**

Atacar um fornecedor de software significa acesso indireto a **centenas ou milhares de clientes downstream**. É o efeito multiplicador perfeito.

Fonte: IBM X-Force Threat Intelligence Index 2025

O ALVO: LATAM NA MIRA

Adversários globais migraram o foco para a região, com o Brasil liderando o volume de vítimas

01 // O CENÁRIO REGIONAL
AMÉRICA LATINA EM ALERTA

1º LUGAR

🇧🇷	Brasil	Líder Disparado
MX	México	2º Lugar
CO	Colômbia	3º Lugar

Enquanto outras regiões estabilizaram, a LATAM teve um **aumento de 15%** no volume de ataques. O Brasil concentra a maioria desses incidentes devido à sua **maturidade digital desprotegida.**

02 // QUEM SÃO OS ADVERSÁRIOS
A INVASÃO DOS "SPIDERS"

Em 2025, grupos conhecidos como **"Spiders"** intensificaram operações na América Latina. Diferente de atacantes oportunistas, esses são **coletivos organizados e especializados**, operando como empresas criminosas com divisão clara de funções.

WIZARD SPIDER

Operador por trás do RansomHub, um dos ransomwares mais ativos de 2025. Seu modelo de negócio é baseado em extorsão rápida: criptografa sistemas críticos e exige pagamento em janelas de 48-72 horas, maximizando pressão operacional sobre as vítimas.

PROPHET SPIDER

Especialista em Initial Access Brokerage — ele não executa ataques, ele os viabiliza. Invade redes corporativas explorando vulnerabilidades ou credenciais vazadas e vende o acesso inicial para grupos de ransomware em marketplaces da Dark Web, funcionando como intermediário na cadeia de ataque.

CARBON SPIDER

Historicamente focado em Europa e Ásia, começou a atacar a América Latina pela primeira vez em 2024. Essa mudança geográfica sinaliza que grupos APT globais identificaram a região como alvo de alta viabilidade — infraestrutura digital em expansão com defesas ainda em maturação.

Fonte: ICS Labs Threat Intelligence / CTI Research

MODUS OPERANDI: A CRISE DE IDENTIDADE

A mudança de paradigma: Adversários deixaram de "invadir" para simplesmente "fazer login"

ATAQUES SEM MALWARE (MALWARE-FREE)

Eles não quebram a porta. Eles usam a chave.

Cerca de **75%** das detecções atuais não envolvem uso de malware na fase inicial. Os atacantes utilizam credenciais válidas (compradas na Dark Web por US$ 1.300 em média) para acessar o ambiente como se fossem funcionários legítimos, tornando-se invisíveis para antivírus tradicionais.

O FIM DO MFA COMO BARREIRA

BYPASS DE AUTENTICAÇÃO

A Autenticação de Múltiplos Fatores não é mais infalível. O uso de Infostealers para roubar "Cookies de Sessão" permite que criminosos sequestrem sessões ativas, contornando a necessidade do código ou token de aprovação.

Ao importar esses cookies, os criminosos executam a técnica de 'Pass-the-Cookie', conseguindo personificar o usuário legítimo e acessar aplicações corporativas (como Office 365, e-mails e CRMs) instantaneamente.

OPERAÇÃO "HANDS-ON-KEYBOARD"

ATAQUE HUMANO INTERATIVO

O ataque não é automatizado. É um humano operando o teclado em tempo real. Eles usam ferramentas nativas do próprio sistema (como PowerShell e RDP) para se moverem lateralmente ("Living Off The Land"), misturando-se ao tráfego normal da TI.

Essa camuflagem permite evadir detecções comportamentais de EDRs, garantindo persistência silenciosa na rede. O atacante permanece invisível por semanas, mapeando a infraestrutura e exfiltrando dados críticos antes de ser detectado.

ICS SIEM detecta logins anômalos por análise comportamental, identificando credenciais comprometidas em <60 segundos.

A VELOCIDADE DO ADVERSÁRIO

A janela de oportunidade para defesa está fechando

TEMPO MÉDIO DE MOVIMENTAÇÃO LATERAL

62 MIN

MÉDIA DE BREAKOUT TIME

Tempo médio que um adversário leva para se mover lateralmente da máquina inicial para outro host na rede. Uma vez dentro, eles se espalham rapidamente.

01 // EVOLUÇÃO

CADA VEZ MAIS RÁPIDO

2023 **84 MIN**

2025 **62 MIN**

A automação dos grupos de eCrime reduziu drasticamente o tempo de movimentação lateral.
Frameworks como Cobalt Strike e ferramentas automatizadas aceleram o processo de comprometimento.

02 // RESPOSTA

A REGRA 1-10-60

Para vencer essa corrida contra o tempo, os times de SOC precisam operar em velocidades de elite, seguindo o padrão da indústria:

1 — **MINUTO PARA DETECTAR**
Identificar atividade suspeita em tempo real

10 — **MINUTOS PARA INVESTIGAR**
Analisar contexto, correlacionar eventos e determinar severidade

60 — **MINUTOS PARA REMEDIAR**
Conter, isolar e eliminar a ameaça completamente

ICS Labs atinge essa métrica com:
- 1min: SIEM detecção automática
- 10min: SOAR investigação orquestrada
- 60min: EDR remediação coordenada

Análise manual não é mais viável nesse cenário. Automação e orquestração (SOAR) são essenciais para atingir esses tempos de resposta e vencer adversários que operam em 62 minutos.

ANATOMIA DE UM ATAQUE

Da invasão inicial à extorsão: a jornada completa de um adversário em 6 etapas

01 // O PLAYBOOK UNIVERSAL

A JORNADA DO ATACANTE

1 INITIAL ACCESS
Phishing, credenciais vazadas ou exploração de vulnerabilidades públicas

2 EXECUTION & PERSISTENCE
Malware executado, backdoors instalados, acesso mantido após reinicializações

3 PRIVILEGE ESCALATION
Elevação de usuário comum para Domain Admin — controle total da rede

4 LATERAL MOVEMENT
Espalhamento: de 1 máquina comprometida para dezenas de servidores

5 COLLECTION & EXFILTRATION
Dados sensíveis coletados e enviados para servidores C2 (Command & Control)

6 IMPACT
Criptografia massiva (ransomware) ou extorsão com ameaça de vazamento

CENÁRIO CATASTRÓFICO: MANUFATURA BRASILEIRA

Cronologia de um incidente ransomware — Março 2025

DIA 0 Funcionária clica em e-mail de Phishing. **Credenciais Capturadas**

DIA 2 Escalada bem-sucedida. Atacante obtém **privilégios de Domain Admin.**

DIA 4 Lateral movement: **47 servidores comprometidos.** Backups corrompidos.

DIA 5 Criptografia massiva iniciada. **Nota de resgate: US$ 2.3M**

IMPACTO FINAL

8 DIAS
PARADA TOTAL

US$ 12M
PREJUÍZO

340
FUNCIONÁRIOS OCIOSOS

02

QUANDO O ADVERSÁRIO É INVISÍVEL

OS ADVERSÁRIOS MAIS PERIGOSOS

Grupos APT com capacidade, recursos e motivação para executar ataques em escala global

ICS INSIGHTS:

Os "Spiders" vistos anteriormente são grupos criminosos (eCrime). Os APTs desta seção são patrocinados por governos, recursos ilimitados, objetivos geopolíticos com possibilidade de persistência de anos. Daí vem o nome Ameaças Persistentes.

APT 29

RUSSIA (SVR)

Cozy Bear . Midnight Blizzard

ALVOS PRINCIPAIS

Governos . Tecnologia . Defesa . Think Tanks

ATAQUES 2024-2025

SOLAR WINDS Follow-up campaigns
Campanhas contra OTAN e aliados

APT 28

RUSSIA (GRU)

Fancy Bear . Forest Blizzard

ALVOS PRINCIPAIS

Militar . Política . Infraestrutura

ATAQUES 2024-2025

Interferência em eleições europeias
DDoS Massivo em infraestrutura

APT 41

CHINA (MSS)

Double Dragon · Winnti

ALVOS PRINCIPAIS

Tecnologia · Saúde · Manufatura · Finanças

ATAQUES 2024-2025

Espionagem industrial massiva
Roubo de propriedade intelectual

LAZARUS

NORTH KOREA (RGB)

Hidden Cobra . Zinc

ALVOS PRINCIPAIS

Finanças . Criptomoedas . Exchanges . Bancos

ATAQUES 2024-2025

Roubo de US$ 2 Bilhões em cripto
Ataques a Exchanges e fintechs

APT 40

CHINA (PLA NAVY)

Leviathan · Kryptonite Panda

ALVOS PRINCIPAIS

Marítimo · Naval · Engenharia · Portos

ATAQUES 2024-2025

Espionagem de tecnologia naval
Comprometimento de portos LATAM

KIMSUKY

NORTH KOREA (RGB)

Velvet Chollima · Black Banshee

ALVOS PRINCIPAIS

Governo · Think Tanks · Pesquisa · Academia

ATAQUES 2024-2025

Campanhas de spear-phishing massivas
Roubo de inteligência geopolítica

APT 33

IRÃ (IRGC)

Elfin · Holmium

ALVOS PRINCIPAIS

Petróleo & Gás · Aviação · Energia · Militar

ATAQUES 2024-2025

Sabotagem em infraestrutura energética
Wiper attacks contra adversários regionais

SANDWORM

RUSSIA (GRU)

Voodoo Bear . Seashell Blizzard

ALVOS PRINCIPAIS

Energia · Telecoms · Governo · Infraestrutura

ATAQUES 2024-2025

Sabotagem telecoms e sistemas SCADA
Blackouts em redes elétricas europeias

ICS INSIGHTS // A GUERRA NO NOSSO QUINTAL

A convergência IT/OT nas indústrias brasileiras abriu portas para sabotadores. Enquanto o varejo e saúde sofrem com a extorsão do APT41, setores estratégicos como Energia e Naval enfrentam o monitoramento silencioso de atores estatais. Não somos mais espectadores: o Brasil tornou-se um campo de batalha ativo.

A ERA DA EXTORSÃO

Não é mais sobre travar computadores. É sobre destruir reputações.

01 PASSADO
O VELHO RANSOMWARE

FOCO: **Criptografia de Dados**

> ***"Seus arquivos foram criptografados. Solicite resgate em Bitcoin para tê-los de volta."***

O modelo tradicional de ransomware focava exclusivamente em criptografar arquivos e sistemas. O criminoso exigia pagamento para fornecer a chave de descriptografia.

Por que se tornou obsoleto: As organizações melhoraram suas estratégias de backup e disaster recovery. Com backups imutáveis e offsite, muitas vítimas simplesmente restauravam os dados sem pagar. Os criminosos pararam de lucrar apenas com criptografia.

02 PADRÃO ATUAL
A DUPLA EXTORSÃO

FOCO: **Exfiltração de Dados (Data Leak)**

> ***“Antes de criptografar, copiamos tudo.”***

A evolução crítica: os atacantes agora exfiltram dados sensíveis ANTES de criptografar. Se a vítima possui backups e recusa o pagamento, os criminosos publicam os dados roubados em "Leak Sites" (Wall of Shame) na Dark Web.

Dados financeiros, contratos confidenciais, informações de clientes, segredos comerciais e prontuários médicos são expostos publicamente, causando danos irreversíveis à reputação e violações graves de compliance (LGPD, HIPAA, GDPR).

03

CENÁRIO CATASTRÓFICO

A TRIPLA EXTORSÃO

FOCO: **Assédio Psicológico**

> ***"Vamos garantir que ninguém confie em você novamente."***

O estágio mais agressivo da extorsão cibernética. Além de criptografar e vazar dados, os atacantes aplicam pressão psicológica máxima sobre a vítima através de múltiplas frentes:

TÁTICAS DE PRESSÃO:

- Contato direto com stakeholders: Ligam para clientes, parceiros comerciais e fornecedores informando sobre o ataque e vazamento.
- Notificação à imprensa: Enviam comunicados a veículos de mídia para amplificar o dano reputacional.
- Ataques DDoS coordenados: Derrubam o site institucional e serviços online da empresa até que o pagamento seja efetuado.
- Ameaças aos executivos: Em casos extremos, grupos chegam a ameaçar diretamente C-levels e suas famílias.

ICS REPORT: O objetivo é tornar a continuidade do negócio impossível sem o pagamento do resgate. Neste cenário, backup não é suficiente. Apenas detecção precoce, contenção rápida e resposta coordenada 24/7 podem prevenir o dano sistêmico.

03

NOSSO ECOSSISTEMA DE PROTEÇÃO

ICS ANALYZER

ADVANCED THREAT ANALYSIS

Análise forense digital e threat intelligence. Processa URLs maliciosas, hashes e anomalias, gerando relatórios técnicos com IOCs e recomendações de remediação.

- Centralização de Logs
- Análise Avançada e Correlação
- Relatórios e Dashboards Personalizados
- Automação e Integração

ICS ANTISPAM

EMAIL THREAT PROTECTION

Camada de proteção que executa a filtragem de e-mails recebidos antes que o e-mail malicioso chegue até o usuário. Servindo como primeira barreira para que o usuário não seja vítima de phishing e/ou spam.

- Inteligência contra ameaças de e-mail em tempo real
- Proteção total contra ameaças de e-mail como phishing, BEC
- Detecção de ameaças por meio do reconhecimento de padrões
- Dashboards em tempo real

ICS EDR

ENDPOINT DETECTION & RESPONSE

Proteção contínua de endpoints com prevenção automatizada, detecção comportamental e resposta orquestrada. Análise heurística e machine learning identificam ameaças em tempo real.

- Detecção comportamental com IA
- Isolamento automático de ameaças
- Resposta em segundos
- Análise forense pós-incidente

ICS SIEM

SECURITY INFORMATION & EVENT MANAGEMENT

Inteligência centralizada que coleta, normaliza e correlaciona logs em tempo real. Algoritmos avançados identificam padrões anômalos e priorizam incidentes por criticidade.

- Correlação inteligente de eventos
- Dashboards em tempo real
- Alertas priorizados por severidade
- Compliance (LGPD, ISO 27001)

ECOSSISTEMA EXPANDIDO

Ferramentas complementares de defesa em profundidade

Além dos 4 pilares estratégicos (EDR, SIEM, Analyzer e AntiSpam), o ICS Labs oferece um ecossistema completo de ferramentas especializadas que ampliam a cobertura de segurança e fortalecem a postura defensiva em camadas críticas da infraestrutura.
Cada componente foi projetado para integrar-se perfeitamente aos pilares principais, criando uma defesa multicamadas sem gaps de visibilidade.

ICS CTI

Cyber Threat Intelligence

Inteligência de ameaças em tempo real correlacionada com indicadores de comprometimento (IOCs) globais. Fornece contexto estratégico sobre adversários, campanhas ativas e TTPs (Tactics, Techniques, and Procedures) para detecção proativa e antecipação de ataques direcionados.

ICS DECEPTOR

Deception Technology

Armadilhas digitais (honeypots e honeynets) que detectam movimentação lateral de atacantes antes que comprometam sistemas críticos. Gera alertas de alta fidelidade ao identificar interações suspeitas com ativos falsos, reduzindo falsos positivos e acelerando resposta.

ICS FEEDS

Threat Intelligence Feeds

Feeds de assinaturas de ameaças atualizados 24/7 com IOCs de fontes globais confiáveis. Integra-se automaticamente ao SIEM, IPS e Firewall para bloqueio imediato de IPs, domínios e hashes maliciosos identificados em campanhas emergentes ao redor do mundo.

ICS GAV

Gestão de Ativos e Vulnerabilidades

Inventário automatizado de ativos TI e OT com varredura contínua de vulnerabilidades. Prioriza correções (patch management) com base em risco real ao negócio, exploração ativa na wild e criticidade CVSS, reduzindo a superfície de ataque de forma inteligente.

ICS SOAR
Security Orchestration & Response

Orquestração e resposta automatizada de incidentes via playbooks predefinidos. Executa ações coordenadas (isolamento de endpoint, bloqueio de IP, quarentena de usuário) em segundos, permitindo que analistas atinjam a Regra 1-10-60 de forma consistente.

ICS WAF
Web Application Firewall

Proteção de aplicações web contra OWASP Top 10 (SQL Injection, XSS, CSRF, etc.), ataques DDoS de camada 7 e bots maliciosos. Utiliza machine learning para identificar padrões anômalos e bloquear exploits zero-day antes que alcancem a aplicação.

INTEGRAÇÃO NATIVA

Cada ferramenta deste ecossistema expandido foi projetada para integrar-se perfeitamente aos 4 pilares principais, compartilhando telemetria, IOCs e contexto de ameaças em tempo real. O resultado é uma defesa multicamadas coordenada, onde gaps de visibilidade são eliminados e a velocidade de resposta é maximizada.

IMPACTO NA POSTURA DE SEGURANÇA

Como o ICS Labs transforma a defesa cibernética em profundidade

DEFESA INTEGRADA EM CAMADAS

Juntas, essas ferramentas compõem nossa defesa em profundidade, reduzindo a superfície de ataque e garantindo a integridade dos dados.

→ O ICS ANTISPAM é a Primeira linha de defesa contra phishing (vetor #1 de Initial Access). Adiciona inteligência ao processo, detalhando vulnerabilidades e relacionando-as a ameaças observadas no mundo todo. Com isso, é possível antecipar riscos e permitir que o IPS bloqueie ataques antes de qualquer impacto.

→ O ICS SIEM reúne alertas de várias fontes em um só lugar, dando à equipe do NGSOC clareza para identificar, priorizar e tratar incidentes com rapidez. Suas correlações e regras permitem uma resposta coordenada diante de ameaças em andamento.

→ O ICS ANALYZER amplia essa visão, trazendo uma leitura mais profunda do ambiente. Ele identifica padrões, tendências e possíveis caminhos de ataque que poderiam passar despercebidos. Detecta exfiltração de dados ANTES da Dupla/Tripla Extorsão, Traz visibilidade profunda sobre Supply Chain

→ O ICS EDR atua direto nos endpoints onde 75% dos ataques começam sem malware. Ele também fornece dados técnicos para entender o executável envolvido e fortalecer as defesas para o futuro.

ALCANCE
OPERACIONAL

+ 8 MIL
ACCESS POINTS MONITORADOS

+3.000
FIREWALLS PROTEGIDOS

+5 MIL
SWITCHES GERENCIADOS

+2.500
VPN'S SEGURAS

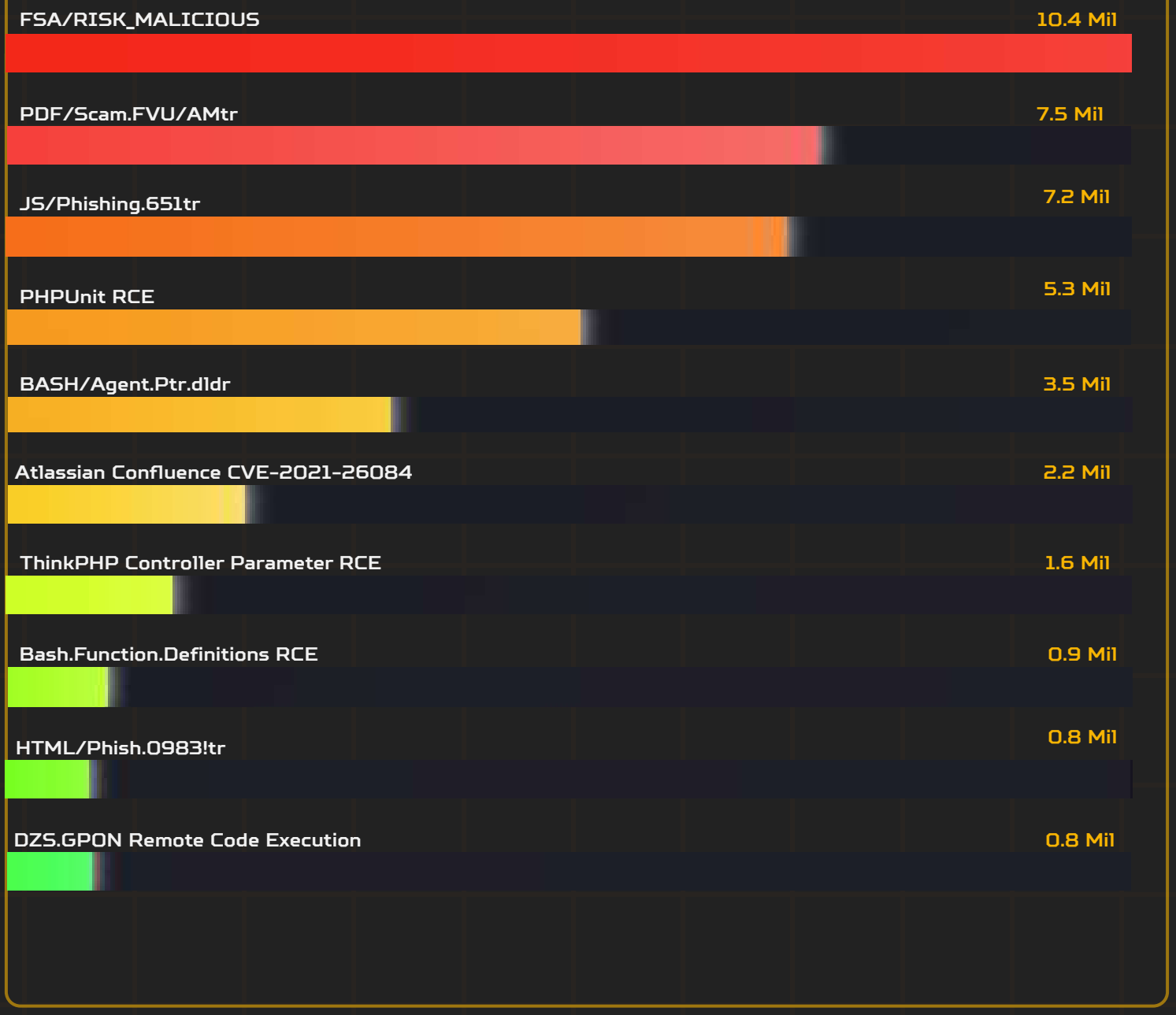
100M+
EVENTOS / MES

+1 MILHÃO
DEVICES SOB PROTEÇÃO

TOP 10 AMEAÇAS NEUTRALIZADAS

Volume de detecções e ROI de Prevenção - 2025

DETECÇÕES (MILHARES)



ANÁLISE DE SEVERIDADE

Embora o phishing domine o volume (7.2 Mil detecções), vulnerabilidades de Execução Remota (RCE) em servidores representam o maior risco financeiro.

PHPUnit e ThinkPHP sozinhas causariam prejuízos estimados em R$ 1,8 milhão.
FSA/RISK_MALICIOUS: R$ 540Mi
PDF/Scam: R$ 338Mi
JS/Phishing:R$ 867Mi
PHPUnit RCE:R$ 1.1Mi
ThinkPHP RCE:R$ 706Mi

*Valores estimados de acordo com a tendência global

A BARREIRA INVISÍVEL

Proteção em tempo real contra a ameaça #1: Phishing e Spam

O CENÁRIO DE SPAM & PHISHING EM 2025

O email continua sendo o vetor de ataque mais explorado globalmente. Em 2025, campanhas de phishing evoluíram para engenharia social assistida por IA, tornando-se indistinguíveis de comunicações legítimas.

Segundo o FBI, as perdas totais relatadas em 2024 chegaram a US$16,6 bilhões, sendo que fraudes do tipo Business Email Compromise (BEC) representaram aproximadamente US$2,77 bilhões. No Brasil, também houve um aumento expressivo nas tentativas de BEC, acompanhando a tendência global.

Com base na tendência de crescimento observada nos últimos anos, estima-se que as perdas globais por crimes cibernéticos possam ultrapassar US$22 bilhões em 2025.

Diante desse cenário crítico, a primeira linha de defesa é impedir que a ameaça chegue ao usuário. É aqui que o ICS AntiSpam opera 24/7.

Emails Processados

69M

Em 12 meses de operação contínua

Detecções de Spam

52.8M

Ameaças bloqueadas antes do usuário

Taxa de spam

76.4%

Spams Detectados / Dia

145K

≈ 6.000 ameaças por hora

Emails Processados / Minuto

133

Análises em tempo real

FLUXO DE FILTRAGEM · 12 MESES

69M

Emails Recebidos

52.8M

Spams Bloqueados

76.4%

16.3M

E-mails Legítimos

23.6%

Fonte: FBI Internet Crime Complaint Center (IC3) Report 2024

O ANO QUE A DEFESA EVOLUIU

Uma análise completa do cenário global de ameaças cibernéticas e a resposta do ICS Labs às adversidades de 2025

Em 2025, não enfrentamos apenas ataques. Enfrentamos adversários organizados, táticas sofisticadas e velocidade sem precedentes. O custo de acesso a uma rede caiu para US$ 1.3K, o tempo de breakout diminuiu para 62 minutos, e 75% dos ataques ocorreram sem malware. Mas também evoluímos. O ICS Labs provou que defesa inteligente, automatizada e integrada não é apenas possível, é essencial.

PERSPECTIVA 2026

AS AMEAÇAS VÃO PIORAR

Grupos APT estão incorporando IA generativa em campanhas de phishing.

Breakout time deve cair para menos de 30 minutos. Ransomware-as-a-Service continuará democratizando ataques sofisticados. A superfície de ataque global expandirá 20% com IoT e OT.

A DEFESA DEVE EVOLUIR

Detecção manual não é mais viável. A Regra 1-10-60 (detectar em 1min, investigar em 10min, remediar em 60min) será o padrão mínimo. Organizações que não automatizarem defesa, threat intelligence e resposta se tornarão estatísticas.

ESTAMOS PREPARADOS

Nosso ecossistema de proteção construído sobre 4 pilares estratégicos opera 24/7/365 monitorando, detectando e neutralizando ameaças em tempo real.
Cada ferramenta foi projetada para bloquear uma etapa específica do Kill Chain, criando uma defesa em profundidade que adversários não conseguem superar.

Essa arquitetura é sustentada pelo nosso NGSOC (Next-Generation SOC), o centro nervoso da operação.

Atuando em regime de monitoramento contínuo, nossa equipe de analistas realiza a correlação avançada de eventos e a triagem de incidentes em tempo real, assegurando que a detecção automatizada seja validada por uma resposta humana especializada, garantindo que nenhuma anomalia passe despercebida.

Dados de telemetria: Janeiro a Dezembro 2025

ICS LABS

ICS LABS

Sua melhor estratégia de defesa

SUA JORNADA DE IMPLEMENTAÇÃO DA CIBERSEGURANÇA NÃO PRECISA SER COMPLEXA.

A Inorpel Cybersecurity atua como parceira estratégica do diagnóstico à operação contínua, simplificando decisões, integrando tecnologias e garantindo proteção real ao negócio.

Com especialistas e um ecossistema completo de segurança, ajudamos sua empresa a evoluir a maturidade cibernética de forma constante, reduzindo riscos e aumentando a resiliência.

FALE CONOSCO

Avance com segurança em toda a sua jornada digital

ICS LABS

www.icslabs.com.br

WEBSITE

www.inorpelcybersecurity.com.br

E-MAIL

contato@icslabs.com.br

LIGUE AGORA

0800 623 0031