TLP: CLEAR

RELATÓRIO DE PESQUISAS

Ameaças cibernéticas ao setor de Manufatura no Brasil

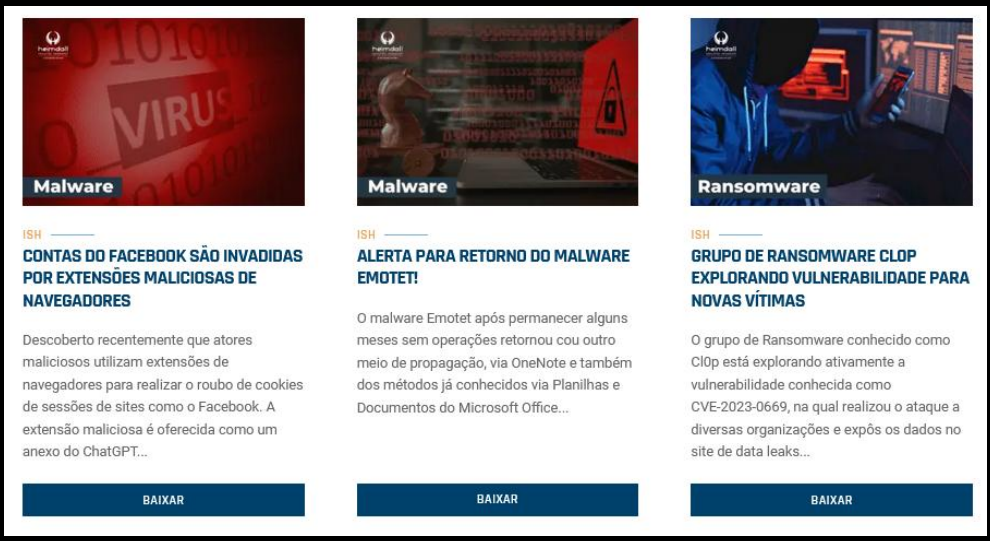
heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Este relatório de segurança, desenvolvido pela equipe de inteligência **Heimdall da ISH Tecnologia**, tem como objetivo proporcionar uma compreensão aprofundada e um dimensionamento preciso das ameaças cibernéticas identificadas. O documento está estruturado em três níveis de abordagem: ***Estratégico***, ***Tático*** e ***Operacional***, garantindo uma visão completa e integrada das ameaças e ações recomendadas.

2 ESTRATÉGICO

2.1 INTRODUÇÃO SOBRE A AMEAÇA

O setor de **manufatura** tornou-se um dos **principais alvos de ameaças cibernéticas no mundo**, ocupando consistentemente as primeiras posições em ataques de ransomware, espionagem industrial e sabotagem digital. Diferente de outros segmentos, os impactos nesse setor vão além da perda de dados: **linhas de produção são interrompidas, cadeias de suprimentos são afetadas e prejuízos financeiros podem atingir dezenas ou centenas de milhões de dólares**.

No **Brasil**, a digitalização acelerada da indústria, combinada com ambientes OT legados, convergência IT/OT e baixa maturidade em segurança industrial, amplia significativamente a superfície de ataque. Este relatório apresenta um panorama **global e nacional** das principais ameaças cibernéticas ao setor de manufatura, conectando dados de inteligência de ameaças, casos reais e tendências observadas em ambientes industriais.

A indústria moderna depende fortemente de **sistemas interconectados**, como:

- *SCADA*
- *PLCs*
- *Sistemas MES*
- *Robôs industriais*
- *Sensores IoT/IIoT*
- *Integrações com ERP e cloud*

Essa conectividade, essencial para eficiência e competitividade, também expõe fábricas a ataques que antes eram restritos a ambientes corporativos. Hoje, um incidente cibernético pode **paralisar uma planta inteira**, gerar riscos físicos a operadores e comprometer contratos globais.

2.2 Vitimologia e Segmentos afetados

Setores mais visados globalmente:

- *Automotivo*
- *Alimentos e bebidas*
- *Metalurgia e siderurgia*
- *Químico e petroquímico*
- *Energia e manufatura pesada*
- *Farmacêutico*

No Brasil, os alvos mais frequentes incluem:

- *Indústrias de base*
- *Fabricantes com operação 24x7*
- *Empresas integradas a cadeias globais*
- *Organizações com OT legado e baixa segmentação de rede*

2.3 Impacto Estratégico

Vetor de impacto	O que acontece na prática	Consequência para o negócio
Parada de produção (OT/IT)	indisponibilidade de sistemas de chão de fábrica e corporativos	perdas financeiras imediatas + multas contratuais
Extorsão e vazamento	roubo de dados + ameaça de publicação	impacto reputacional + jurídico (LGPD/contratos)
Espionagem industrial	exfiltração silenciosa de projetos/processos	perda de vantagem competitiva
Efeito cascata em supply chain	ataque em fornecedor afeta toda a cadeia	atrasos sistêmicos e falta de insumos
Risco físico	falhas operacionais e incidentes de segurança	impacto em pessoas + compliance

Tabela 1 – Impactos estratégicos para a indústria.

3 TÁTICO

3.1 VISÃO GERAL: MANUFATURA COMO SUPERFÍCIE DE ATAQUE (IT/OT)

Ambientes de manufatura modernos são caracterizados por uma **alta interdependência entre sistemas corporativos (IT) e sistemas operacionais industriais (OT/ICS)**. Essa convergência, embora essencial para eficiência, automação e visibilidade da produção, cria uma superfície de ataque extensa e heterogênea, frequentemente composta por tecnologias legadas e novas plataformas digitais operando em conjunto.

Ambientes típicos na manufatura incluem:

IT (Tecnologia da Informação):

- Active Directory (AD), e-mail corporativo, VPNs, soluções de EDR/XDR, servidores de aplicação, bancos de dados, sistemas ERP, file servers e serviços em nuvem.

OT/ICS (Tecnologia Operacional):

- Controladores Lógicos Programáveis (PLCs), Interfaces Homem-Máquina (HMIs), sistemas SCADA, historianos de processo, estações de engenharia, servidores de automação e redes industriais dedicadas.

Camada de Integração IT/OT:

- Sistemas MES integrados ao ERP, acessos remotos para manutenção e suporte, integradores de sistemas industriais, fornecedores terceirizados e fabricantes de equipamentos (OEMs).

Essa arquitetura integrada faz com que comprometimentos iniciados em ambientes IT possam, direta ou indiretamente, impactar a operação industrial, mesmo sem exploração direta de dispositivos OT.

3.2 EXPOSIÇÃO GLOBAL DE PROTOCOLOS INDUSTRIAIS CRÍTICOS

Análises realizadas por meio de plataformas públicas de indexação de serviços expostos na Internet, como o ***Shodan***, evidenciam uma superfície de ataque significativa associada a protocolos industriais amplamente utilizados no setor de manufatura.

Consultas defensivas focadas em protocolos industriais críticos revelaram os seguintes volumes globais de exposição:

Porta 44818 (EtherNet/IP): aproximadamente 596.197 dispositivos expostos globalmente.

- Este protocolo é amplamente utilizado em ambientes industriais, especialmente em controladores e sistemas Rockwell Automation / Allen-Bradley, comuns em fábricas e plantas de manufatura.

Porta 502 (Modbus/TCP): aproximadamente 638.331 dispositivos expostos globalmente.

- O Modbus/TCP é um dos protocolos industriais mais difundidos no mundo, presente em PLCs, sistemas SCADA, sensores e dispositivos OT legados, frequentemente sem mecanismos nativos de autenticação ou criptografia.

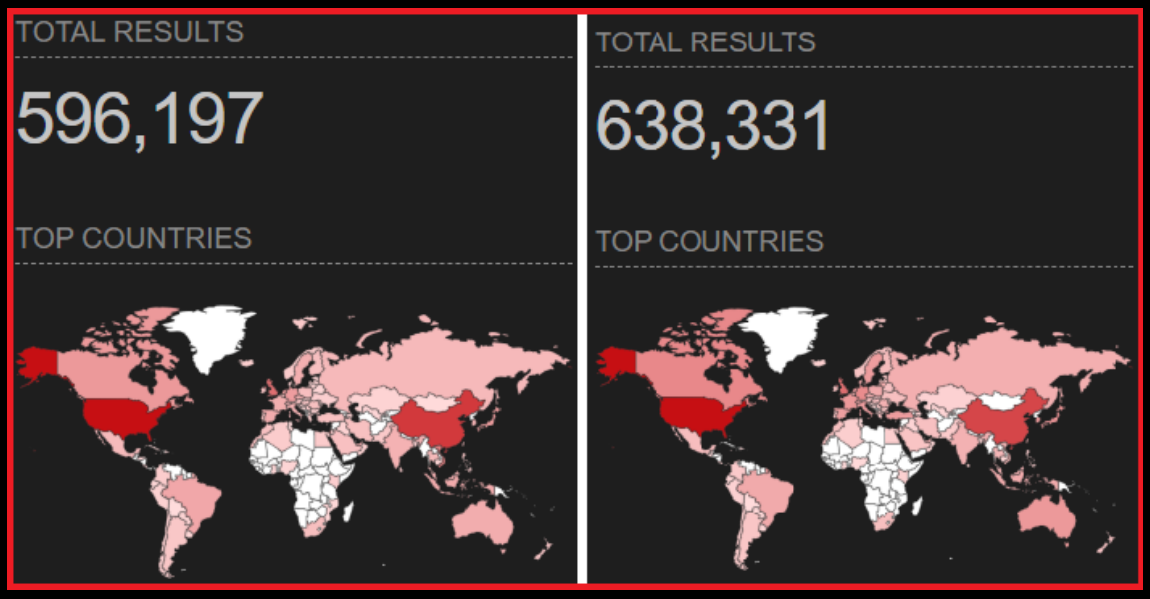


Figura 1 – Superfície de ataque Global em ambientes industriais (Protocolos OT Expostos).

Esses números indicam que centenas de milhares de dispositivos industriais permanecem potencialmente acessíveis pela Internet, muitas vezes fora de zonas desmilitarizadas (DMZs) ou sem controles robustos de acesso. Embora a exposição não implique, por si só, comprometimento, ela amplia significativamente o risco de exploração, especialmente quando combinada com:

- *Credenciais fracas ou reutilizadas;*
- *Ausência de autenticação forte (ex.: MFA);*
- *Vulnerabilidades conhecidas em firmware ou gateways industriais;*
- *Integrações diretas entre ambientes IT e OT.*

Do ponto de vista de ameaças cibernéticas à manufatura, essa exposição é particularmente relevante, pois grupos de ransomware e atores de espionagem industrial têm demonstrado preferência por vetores de acesso inicial que envolvem serviços remotos e protocolos industriais expostos, permitindo comprometer rapidamente sistemas que sustentam a operação. Em cenários reais, mesmo quando os atacantes não interagem diretamente com PLCs ou dispositivos de

controle, o simples comprometimento de sistemas industriais de suporte, como servidores de automação, historianos ou interfaces de supervisão, pode resultar em interrupção da produção, perda de visibilidade operacional e impactos financeiros relevantes.

3.3 PRINCIPAIS AMEAÇAS CONTRA O SEGMENTO DE MANUFATURA

As ameaças cibernéticas que mais impactam o setor de manufatura apresentam motivações distintas, mas frequentemente se sobrepõem dentro de um mesmo incidente. A seguir, destacam-se as três categorias predominantes observadas globalmente e no Brasil.

A) Ransomware e "extorsão industrial"

- O ransomware permanece como a principal ameaça ao setor de manufatura por representar o caminho mais rápido e eficaz para monetizar a interrupção da produção e o vazamento de dados sensíveis. Diferentemente de outros setores, a manufatura possui baixa tolerância a downtime, o que aumenta a pressão para pagamento.

Dados recentes indicam que:

  - Em incidentes no setor de manufatura, malware está presente em aproximadamente 66% das violações, e 71% desse malware corresponde a ransomware.
  - Ambientes industriais mostram crescimento sustentado do número de incidentes, com centenas de casos reportados por trimestre, indicando que o fenômeno não é pontual, mas estrutural.

Além da criptografia, observa-se a consolidação do modelo de dupla extorsão, no qual dados corporativos, projetos industriais, contratos e informações de fornecedores são exfiltrados antes do impacto final, ampliando os riscos legais e reputacionais.

B) Espionagem industrial e roubo de propriedade intelectual

- A espionagem industrial voltou a ganhar relevância no setor de manufatura, impulsionada por disputas econômicas, tecnológicas e geopolíticas. Relatórios recentes destacam um aumento significativo da motivação de espionagem, especialmente quando comparado ao ano anterior.

Nesse contexto, os atacantes buscam:

- *Projetos de engenharia e design de produtos;*
- *Fórmulas, processos industriais e segredos de fabricação;*
- *Dados de fornecedores estratégicos e cadeias de suprimentos;*
- *Informações comerciais sensíveis (custos, contratos, estratégias).*

Diferentemente do ransomware, essas operações tendem a ser mais silenciosas e prolongadas, com foco em persistência e exfiltração contínua, dificultando a detecção e aumentando o impacto de longo prazo para a competitividade da organização.

C) Ameaças OT específicas (interrupção e manipulação)

- Ameaças direcionadas a ambientes OT/ICS exploram, em geral, fragilidades estruturais, como:
  - *Acesso remoto inseguro a sistemas industriais;*
  - *Segmentação insuficiente entre IT e OT;*
  - *Uso de credenciais reutilizadas ou padrões;*
  - *Dependência de protocolos industriais legados sem autenticação ou criptografia*.

Embora nem todos os ataques envolvam manipulação direta de PLCs ou SCADA, a indisponibilidade de sistemas de suporte à operação (como historianos, estações de engenharia ou servidores MES) já é suficiente para causar interrupções significativas na produção.

Síntese analítica

Em muitos incidentes reais, essas três categorias não atuam isoladamente. Um ataque pode iniciar com credenciais válidas (TI), evoluir para espionagem silenciosa e culminar em ransomware como mecanismo de monetização ou distração. Essa convergência reforça a necessidade de uma abordagem integrada de segurança IT/OT, apoiada por inteligência de ameaças e monitoramento contínuo.

4 TENDÊNCIAS GLOBAIS COM NÚMEROS

Indicador	Dado	Fonte
Manufatura como #1 alvo	4 anos consecutivos como indústria nº 1 visada	IBM X-Force 2025
Objetivo dos ataques (manufatura)	Extorsão 29%/ roubo de dados 24%	IBM X-Force 2025
Malware em violações de manufatura	66% das violações	Verizon 2025 DBIR
Entre o malware, ransomware	71% do malware	Verizon 2025 DBIR
Intensidade de ataques	1.585 ataques semanais por org./ +30%	Check Point CPR 2025
Root cause em manufatura	Vulnerabilidades exploradas = 32% (2025)	Sophos (2025)
Custo médio recuperação	US$ 1,3M	Sophos (2025)

Tabela 2 – Indicadores globais recentes (manufatura).

4.1 VETORES DE ENTRADA MAIS COMUNS (O QUE MAIS "ABRE A PORTA")

Vetor	Por que funciona na manufatura	Sinal de alerta
Exploração de edge/VPN	acesso remoto é essencial para operação e terceiros	picos de login, falhas repetidas, CVEs recentes
Credenciais válidas	equipes e fornecedores compartilham acessos	login fora de horário/local, "impossible travel"
Phishing/ anexos	processos com PDFs, notas, pedidos, RH, logística	anexos compactados, links cloud, urgência
Supply chain	um fornecedor comprometido impacta muitos	atualizações suspeitas, integrações quebradas
Pivot IT-OT	segmentação fraca + AD/ERP integrados ao chão	tráfego incomum, ferramentas remotas, jump hosts

Tabela 3 – Vetores típicos

5 PANORAMA NO BRASIL

5.1 O QUE MUDA NO BRASIL

O cenário brasileiro apresenta **características específicas** que influenciam diretamente o risco cibernético no setor de manufatura. Um dos principais fatores é a **alta presença de ambientes OT legados**, muitas vezes operando há anos com atualizações limitadas devido a restrições operacionais, custos de parada e dependência de fornecedores especializados. Além disso, é comum a **forte dependência de terceiros**, integradores e prestadores de serviço para manutenção de sistemas industriais e suporte remoto. Esses acessos, quando não adequadamente governados, ampliam a superfície de ataque e reduzem a visibilidade sobre atividades potencialmente maliciosas.

Outro aspecto relevante é a **grande diversidade de maturidade em controles de segurança**, variando desde plantas industriais com práticas avançadas de segmentação e monitoramento até fábricas com **baixa governança em segurança da informação e OT**, especialmente fora de grandes centros industriais.

Por fim, a **exposição de serviços à Internet** e os **incidentes reportados ao CERT.br** fornecem uma visão importante sobre tendências gerais da "internet brasileira". Embora esses dados não sejam segmentados por setor, eles funcionam como um **termômetro de risco**, indicando padrões de exploração e comportamento adversário que também afetam ambientes industriais.

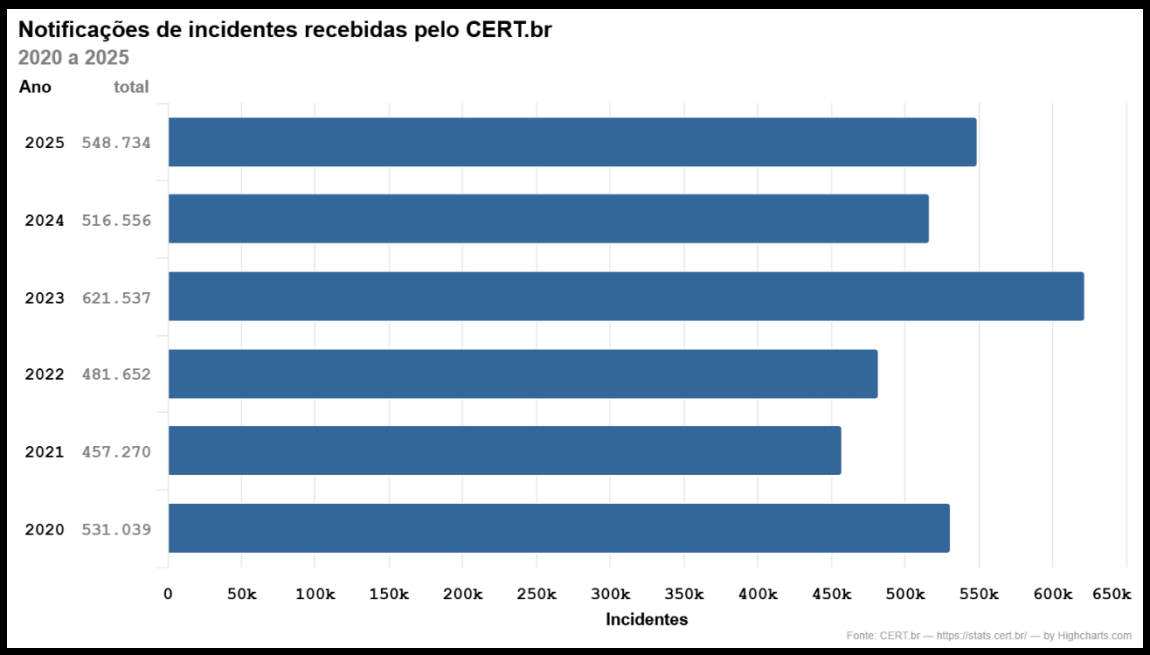


Figura 2 – Incidentes reportados ao CERT.br 2020 - 2025.

5.2 EVIDÊNCIA OSINT DE PRESSÃO DE RANSOMWARE NO PAÍS

Análises baseadas em **OSINT**, especialmente em plataformas que monitoram claims públicos de grupos de ransomware, indicam que o Brasil figura de forma recorrente entre o top 10 países com maior número de **organizações alegadamente vitimadas.** Esse cenário sugere uma pressão contínua de grupos de extorsão sobre empresas brasileiras, incluindo organizações do setor de manufatura. Embora esse tipo de evidência possua limitações metodológicas, como dependência de autodeclarações de grupos criminosos e ausência de validação independente, ela é amplamente utilizada por equipes de inteligência de ameaças como indicador de tendência. Em conjunto com dados de incidentes reportados e análises globais, essas informações reforçam a percepção de que o Brasil permanece como um alvo relevante para operações de ransomware, impulsionado por fatores econômicos, operacionais e estruturais. Abaixo segue tabela com dados de **janeiro a começo de dezembro de 2025**.

País	Ataques
EUA	3.597
Canadá	359
Alemanha	263
Reino Unido	261
França	154
Itália	150
Espanha	130
Australia	117
Brasil	116
Japão	103

Tabela 4 – Indicadores relacionados a atividades de ransomware por países em 2025.

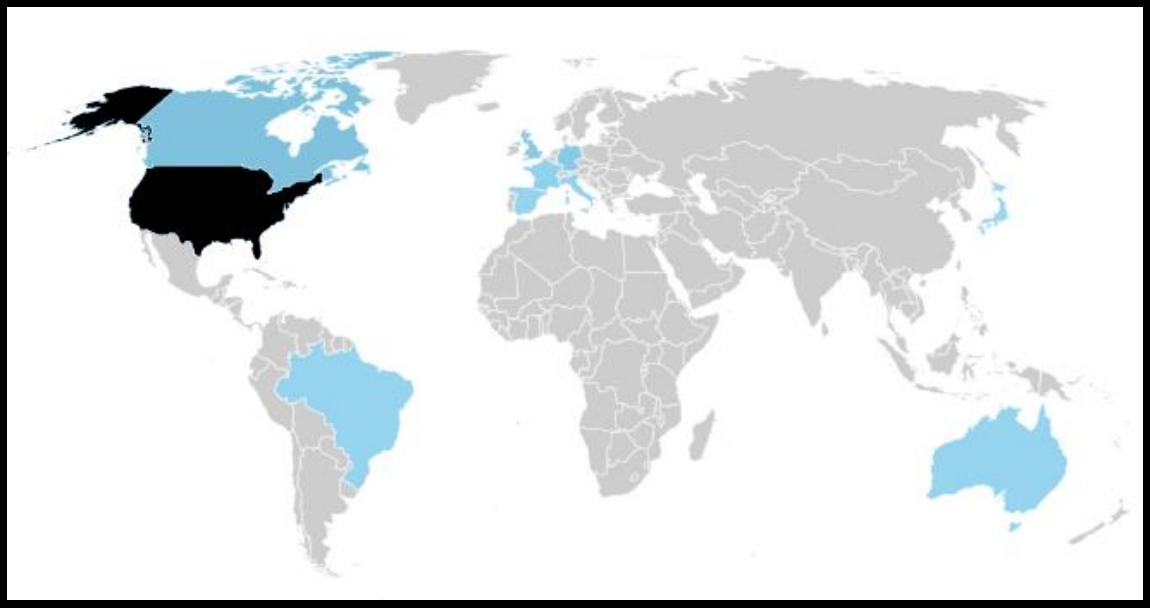


Figura 3 – Mapa de calor de países afetados por ransomware em 2025.

5.3 Casos e Cenários típicos no segmento

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada

Cenário 1 - Ransomware interrompe operação (IT e OT)

- O comprometimento inicial ocorre, em geral, **por exploração de VPNs, dispositivos de borda (edge) vulneráveis ou uso de credenciais** previamente vazadas, muitas vezes associadas a acessos remotos legítimos.
- Após obter acesso, o atacante expande privilégios e realiza **criptografia de servidores críticos**, como Active Directory, file servers e sistemas ERP, resultando em impacto direto em sistemas de suporte à produção, incluindo MES e aplicações industriais integradas.
- A **interrupção operacional** leva à paralisação parcial ou total da produção, criando **pressão imediata para negociação**, uma vez que o custo do downtime cresce rapidamente a cada hora de inatividade.

É observado que, ransomware e extorsão continuam sendo o principal vetor de impacto no setor de manufatura, explorando a baixa tolerância a indisponibilidade operacional.

Cenário 2 - "Extorsão sem criptografia"

- Nesse cenário, o atacante prioriza a exfiltração de dados sensíveis, como projetos de engenharia, listas de fornecedores, contratos comerciais e informações de recursos humanos.

- Mesmo sem criptografar sistemas ou interromper diretamente a produção, o grupo ameaça publicar ou comercializar os dados roubados (modelo de dupla extorsão), gerando riscos legais, regulatórios e reputacionais significativos.
- Esse modelo tem sido adotado com maior frequência à medida que organizações fortalecem backups e capacidades de recuperação, reduzindo a eficácia do ransomware tradicional.

Tendência observada: Diante da melhoria das defesas, grupos criminosos têm migrado para estratégias de roubo de dados e chantagem, mantendo o potencial de impacto financeiro sem necessariamente causar indisponibilidade operacional imediata.

Cenário 3 - Comprometimento via fornecedor ou integrador

- Acesso remoto concedido a fornecedores, integradores ou prestadores de manutenção passa a funcionar como uma "ponte" para o ambiente corporativo e, potencialmente, para sistemas industriais.
- Os atacantes exploram esse acesso utilizando ferramentas legítimas do próprio ambiente (técnicas de living-off-the-land), o que reduz a geração de alertas e dificulta a diferenciação entre atividades normais e maliciosas.
- A baixa visibilidade e governança sobre acessos de terceiros prolonga o tempo de permanência do atacante, aumentando o risco de impacto sistêmico.

Incidentes envolvendo cadeias de suprimento e terceiros tornaram-se uma **preocupação crescente para executivos**, uma vez que um único fornecedor comprometido pode afetar múltiplas organizações e interromper operações em escala.

5.4 TABELA MITRE ATT&CK

Este tópico apresenta as Táticas, Técnicas e Procedimentos (TTPs) identificados nesta ameaça, conforme o framework MITRE ATT&CK, oferecendo uma visão tática detalhada sobre o comportamento do adversário. O objetivo é permitir o mapeamento das técnicas utilizadas pelos atacantes, facilitando a implementação de contramedidas eficazes e o aprimoramento das defesas de segurança.

5.5 RANSOMWARE QILIN (AGENDA)

Tática	Técnica	Detalhes
Initial Access	T1078 - Valid Accounts T1133 - External Remote Services T1190 - Exploit Public-Facing App	abuso de credenciais e acesso remoto; exploração de serviços expostos (perímetro)
Execution	T1059 - Command and Scripting Interpreter	execução via PowerShell/cmd e LOLBins para reduzir detecção
Persistence	T1053 - Scheduled Task/Job T1543 - Create/Modify System Process	tarefas/serviços para manter presença antes do impacto
Privilege Escalation	T1068 - Exploitation for Privilege Escalation	elevação local para atingir servidores críticos
Defense Evasion	T1218 - System Binary Proxy Execution T1027 Obfuscated/Encrypted Files T1070 - Indicator Removal T1112 - Modify Registry	ocultação, limpeza de rastros e ajustes de registro
Discovery	T1082 - System Information Discovery T1087 - Account Discovery	inventário do ambiente para escolher “crown jewels”
Lateral Movement	T1021 - Remote Services (RDP/SMB/SSH) T1570 - Lateral Tool Transfer	pivot rápido para servidores e infraestrutura (AD/VMware/file servers)
Impact	T1486 - Data Encrypted for Impact T1490 - Inhibit System Recovery T1489 - Service Stop	criptografia + impedir recuperação + parar serviços

Tabela 5 – Tabela MITRE ATT&CK Ransomware Qilin.

5.6 RANSOMWARE AKIRA

Tática	Técnica	Detalhes
Initial Access	T1078 - Valid Accounts T1133 - External Remote Services T1190 - Exploit Public-Facing App	credenciais comprometidas; VPN/RDP; exploração de serviços expostos

Execution	T1059 - Command and Scripting Interpreter	execução via PowerShell/cmd durante expansão e preparo
Persistence	T1053 - Scheduled Task/Job T1543 - Create/Modify System Process	manter acesso para finalizar exfiltração/cripto
Defense Evasion	T1562.001 - Impair Defenses T1027 - Obfuscated/Encrypted Files	contorno de EDR/AV antes do impacto
Credential Access	T1003 - OS Credential Dumping	coleta de credenciais para ampliar alcance
Discovery	T1087 - Account Discovery T1018 - Remote System Discovery	mapeamento de hosts e contas privilegiadas
Lateral Movement	T1021.001 - RDP T1021.002 - SMB/Windows Admin Shares	deslocamento para servidores críticos e infraestrutura
Exfiltration	T1041 - Exfiltration Over C2 Channel	roubo de dados para double extortion
Impact	T1486 - Data Encrypted for Impact	criptografia e interrupção operacional

Tabela 6 – Tabela MITRE ATT&CK Ransomware Akira.

6 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

- **Reduzir a exposição de serviços externos críticos,** especialmente VPNs, dispositivos de borda e acessos remotos, garantindo atualização contínua, hardening adequado e autenticação multifator obrigatória, inclusive para terceiros.
- **Fortalecer a segurança de identidade e acesso,** adotando o princípio do menor privilégio, eliminando contas compartilhadas, revisando acessos administrativos e monitorando o uso anômalo de credenciais válidas.
- **Implementar segmentação efetiva entre ambientes IT e OT,** com controle rigoroso de tráfego, zonas de segurança bem definidas e limitação de acessos diretos a sistemas industriais críticos.
- **Proteger os "ativos que sustentam a operação",** como Active Directory, servidores de arquivos, virtualização, ERP e MES, priorizando esses sistemas em estratégias de monitoramento, hardening e resposta a incidentes.
- **Controlar e monitorar acessos de terceiros**, integradores e fornecedores, utilizando acessos temporários (just-in-time), registro completo de sessões e governança clara sobre quem acessa o ambiente industrial.
- **Adotar backups resilientes e testados regularmente,** preferencialmente offline ou imutáveis, garantindo capacidade real de recuperação sem depender de pagamento de resgate.
- **Implantar detecções comportamentais focadas em ransomware e movimentação lateral,** com atenção especial a SMB, RDP, PsExec, WMI e tentativas de desativação de soluções de segurança.
- **Estabelecer uma capacidade contínua de Cyber Threat Intelligence (CTI),** para acompanhar campanhas ativas, vetores emergentes e TTPs relevantes ao setor de manufatura, orientando decisões de patching, detecção e mitigação.

7 OPERACIONAL

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Comprometimento (IoCs) relacionadas a análise do(s) artefato(s) deste relatório.

7.1 INDICADORES DE COMPROMETIMENTO (IOC)

7.2 QILIN (AGENDA) RANSOMWARE

Indicadores do artefato	
md5:	6a93e618e467ed13f98819172e24fffa
sha1:	d34550ebc2bee47c708c8e048eb78881468e6bca
sha256:	e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527
File name:	qilin.exe

Indicadores do artefato	
md5:	334fd98ab462edc1274fecdb89fb0791
sha1:	e3496a341c96d77c0ef9bdeec333dd98e2215527
sha256:	55e070a86b3ef2488d0e58f945f432aca494bfe65c9c4363d739649225efbbd1
File name:	AgendaRansomware.exe

Indicadores do artefato	
md5:	14dec91fdcaab96f51382a43adb84016
sha1:	a85d9d2a3913011cd282abc7d9711b2346c23899
sha256:	37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6
File name:	1.exe

7.3 AKIRA RANSOMWARE

Indicadores do artefato	
md5:	e57340a208ac9d95a1f015a5d6d98b94
sha1:	4549f715bfeab0477c816dc7629b3d50963c4d23
sha256:	87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d
File name:	rans.exe

Indicadores do artefato	
md5:	e8139b0bc60a930586cf3af6fa5ea573
sha1:	86f46189ea993c35fd029ca2308870c069f921e0
sha256:	0c662d28268514fabc7129fd14d6e3e9d7df29261a861bcf8aab1f318bb8e7d0
File name:	ntdll.dll

Indicadores do artefato	
md5:	a1f4931992bf05e9bff4b173c15cab15

sha1:	c4627fe0fd45541f84b3050acb56e73efb5095e1
sha256:	1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218
File name:	1ec34305e593c27bb95d538d45b6a17433e71fa1c1877ce78bf2dbda6839f218.exe

Tabela 7 – Indicadores de Comprometimento.

8 REFERÊNCIAS

- ***Heimdall by ISH Tecnologia***
- ***CTI Purple Team by ISH Tecnologia***
- ***CERT.BR***
- ***MITRE ATT&CK***
- ***CISA***
- ***Dragos***
- ***Sophos***
- ***Checkpoint***
- ***Data Breach Report***

9 AUTORES

- ***Ismael Rocha – Threat Intelligence Specialist***

heimdall
security research
A DIVISION OF ISH