



RELATÓRIO DE PESQUISAS

Ameaças Cibernéticas ao setor de **Saúde no Brasil**

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

 Malware	 Malware	 Ransomware
ISH CONTAS DO FACEBOOK SÃO INVADIDAS POR EXTENSÕES MALICIOSAS DE NAVEGADORES Descoberto recentemente que atores maliciosos utilizam extensões de navegadores para realizar o roubo de cookies de sessões de sites como o Facebook. A extensão maliciosa é oferecida como um anexo do ChatGPT... BAIXAR	ISH ALERTA PARA RETORNO DO MALWARE EMOTET! O malware Emotet após permanecer alguns meses sem operações retornou com outro meio de propagação, via OneNote e também dos métodos já conhecidos via Planilhas e Documentos do Microsoft Office... BAIXAR	ISH GRUPO DE RANSOMWARE CLOP EXPLORANDO VULNERABILIDADE PARA NOVAS VÍTIMAS O grupo de Ransomware conhecido como Clop está explorando ativamente a vulnerabilidade conhecida como CVE-2023-0669, na qual realizou o ataque a diversas organizações e expôs os dados no site de data leaks... BAIXAR

SUMÁRIO

1	Introdução executiva.....	6
2	Estratégico.....	6
2.1	Introdução sobre a ameaça	6
2.2	Vitimologia e Segmentos afetados	6
3	Tático	7
3.1	Tendências globais relevantes	7
3.2	Ransomware.....	7
3.3	Tendência global de ameaças ao setor	7
3.4	Atividades em fóruns clandestinos	8
3.5	Ameaças a nível Brasil.....	8
4	Estatísticas de ataques de ransomware	9
4.1	Impactos dos ataques no Setor e no Brasil	10
4.2	Grupos de ransomware que realizaram ataques neste período	10
5	A conexão que expõe a riscos	12
6	Casos reais de ataques no brasil e no mundo	14
7	Panorama das violações no setor de Saúde	15
7.1	Distribuição das Táticas MITRE ATT&CK.....	15
8	Conclusão	17
9	MITRE ATT&CK.....	18
9.1	Akira ransomware	18
9.2	Rhysida ransomware	20
9.3	Inc ransomware.....	21
10	Recomendações.....	22
10.1	Controle de Acesso Inicial	22
10.2	Gestão de Identidades e Privilégios	22
10.3	Proteção de Endpoints e Servidores	22
10.4	Segurança de Rede	22
10.5	Proteção de Dados e Backups.....	23
10.6	Deteção e Monitoramento	23
10.7	Resposta e Preparação	23

10.8	Ambientes de Saúde	23
11	Operacional.....	25
11.1	Indicadores de Comprometimento (IoC).....	25
12	Referências	27
13	Autores.....	27

LISTA DE TABELAS

Tabela 1 – Tabela MITRE ATT&CK – Akira ransomware.....	19
Tabela 2 – Tabela MITRE ATT&CK – Rhysida ransomware.	21
Tabela 3 – Tabela MITRE ATT&CK – Inc ransomware.	21
Tabela 4 – Indicadores de Comprometimento.	26

LISTA DE FIGURAS

Figura 1 – Comparativos Global de ataques de ransomware 2024-2025.	7
Figura 2 – Comparativo de ataques de ransomware no Brasil até o momento.	9
Figura 3 – Dispositivos DICOM expostos online.....	12
Figura 4 – Top 10 cidades Brasileiras com servidores PACS expostos online.	13
Figura 5 – Distribuição de Táticas MITRE ATT&CK em violações observadas.	15

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 saúde no Brasil está cada vez mais exposto a **ameaças cibernéticas**, em especial aos **ataques de ransomware**. Apesar de representarem uma porcentagem menor em relação a outros setores, os impactos são **altamente desproporcionais**, atingindo a continuidade dos serviços médicos, a privacidade de pacientes e a confiança da sociedade nas instituições de saúde.

Um único ataque pode provocar *paralisação de atendimentos*, *vazamento de dados clínicos sensíveis e prejuízos financeiros e reputacionais significativos*. Isso reforça a necessidade de tratar a cibersegurança na saúde como **prioridade estratégica**.

Este relatório apresenta um **panorama das principais ameaças recentes**, conectando dados nacionais com as tendências globais destacadas pelo [Health-ISAC – 2025 Q2 Health Sector Heartbeat](#).

2.2 VITIMOLOGIA E SEGMENTOS AFETADOS

- Organizações do setor de saúde, incluindo hospitais, clínicas, laboratórios e operadoras de planos de saúde.

3 TÁTICO

3.1 TENDÊNCIAS GLOBAIS RELEVANTES

De acordo com o relatório **Health-ISAC – 2025 Q2 Health Sector Heartbeat**, algumas tendências têm se destacado e afetam diretamente o setor de saúde em todo o mundo, trazendo riscos que também refletem no cenário brasileiro.

3.2 RANSOMWARE

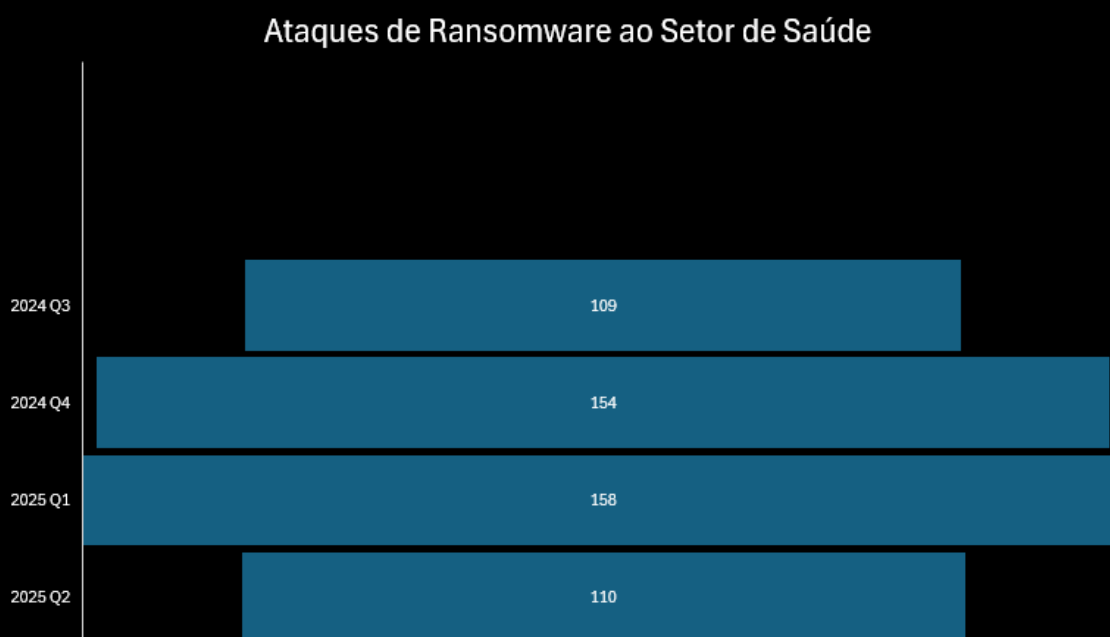


Figura 1 – Comparativos Global de ataques de ransomware 2024-2025.

O ransomware continua sendo a principal ameaça para organizações de saúde. No segundo trimestre de 2025 foram registrados **93 ataques direcionados ao setor (5,8% do total global)**. Embora os números mostrem uma redução em relação a trimestres anteriores, observa-se a atuação de **novos grupos emergentes**, como o **BERT Ransomware**, que amplia a sofisticação dos ataques e mantém o setor em constante risco.

3.3 TENDÊNCIA GLOBAL DE AMEAÇAS AO SETOR

As fragilidades tecnológicas do setor têm sido exploradas de diferentes formas:

- **Dangling DNS:** registros DNS mal configurados permitem que criminosos redirecionem tráfego legítimo para sites maliciosos, criando riscos de fraude e perda de confiança.

- **Bases de dados expostas:** muitos hospitais e clínicas ainda possuem informações acessíveis na internet sem a devida proteção, abrindo espaço para vazamentos em larga escala.
- **Exposição de executivos (CEO doxxing):** informações pessoais e profissionais de líderes do setor têm sido utilizadas em ataques direcionados, elevando o risco de engenharia social e extorsão.

3.4 ATIVIDADES EM FÓRUNS CLANDESTINOS

O mercado negro digital continua ativo e voltado para explorar brechas do setor de saúde. Os principais movimentos identificados incluem:

- **Venda de dados médicos roubados,** como exames e históricos de pacientes, extraídos de clínicas e prestadores de diagnóstico. Esses dados possuem alto valor devido à sua sensibilidade e potencial de uso em fraudes.
- **Comercialização de acessos remotos a redes hospitalares,** com preços variando entre **US\$ 1.200** e **US\$ 20.000**, dependendo do porte e da criticidade da instituição comprometida.

Contexto: Esses fatores demonstram que, mesmo com oscilações nos números absolutos de ataques, o setor de saúde permanece altamente atrativo para criminosos. A combinação de dados sensíveis, sistemas críticos e baixa tolerância a interrupções torna as organizações de saúde alvos estratégicos em escala global.

3.5 AMEAÇAS A NÍVEL BRASIL

O setor de saúde no Brasil enfrenta um cenário de risco crescente diante da sofisticação e diversidade das ameaças cibernéticas. Os ataques de **ransomware** continuam sendo a principal ameaça, com potencial de paralisar hospitais e clínicas, impedir atendimentos e comprometer a continuidade dos serviços. Além disso, o **vazamento de dados médicos sensíveis**, que possuem alto valor no mercado ilegal, agrava a exposição das instituições e aumenta os riscos legais e reputacionais. Somam-se a isso as campanhas de **phishing e engenharia social**, ainda o vetor mais comum de intrusão, explorando a vulnerabilidade de colaboradores para roubo de credenciais ou instalação de malwares.

Outro ponto crítico é a vulnerabilidade de **dispositivos médicos conectados (IoT)**, como monitores e bombas de infusão, que ampliam a superfície de ataque e podem até comprometer tratamentos. O comércio clandestino de acessos a redes hospitalares e bases de dados, aliado à fragmentação na defesa e à falta de colaboração entre instituições, reforça a atratividade do setor para cibercriminosos. Esse conjunto de fatores demonstra que, mesmo sem representar o maior volume de incidentes, o impacto dos ataques na saúde é

altamente desproporcional, exigindo que a **cibersegurança seja tratada como prioridade estratégica** para proteger pacientes, operações e a confiança pública.

4 ESTATÍSTICAS DE ATAQUES DE RANSOMWARE

No período analisado, foram registrados **90 ataques de ransomware no Brasil**, sendo que **6 deles tiveram como alvo organizações do setor de saúde**. Esse número representa aproximadamente **6,7% do total de incidentes**. Embora o percentual possa parecer relativamente baixo quando comparado a outros setores, os impactos no segmento da saúde são **muito mais críticos**.

Hospitais, clínicas e laboratórios lidam com **informações altamente sensíveis** e dependem da **continuidade operacional** para garantir atendimentos, diagnósticos e procedimentos médicos. Assim, cada ataque direcionado ao setor de saúde tem potencial de gerar **interrupções severas nos serviços, vazamento de dados de pacientes e prejuízos financeiros e reputacionais significativos**. Esse dado reforça que, mesmo representando uma fração dos incidentes, a saúde deve ser considerada um **alvo estratégico prioritário** nas políticas de cibersegurança.

Distribuição de Ataques de Ransomware no Brasil

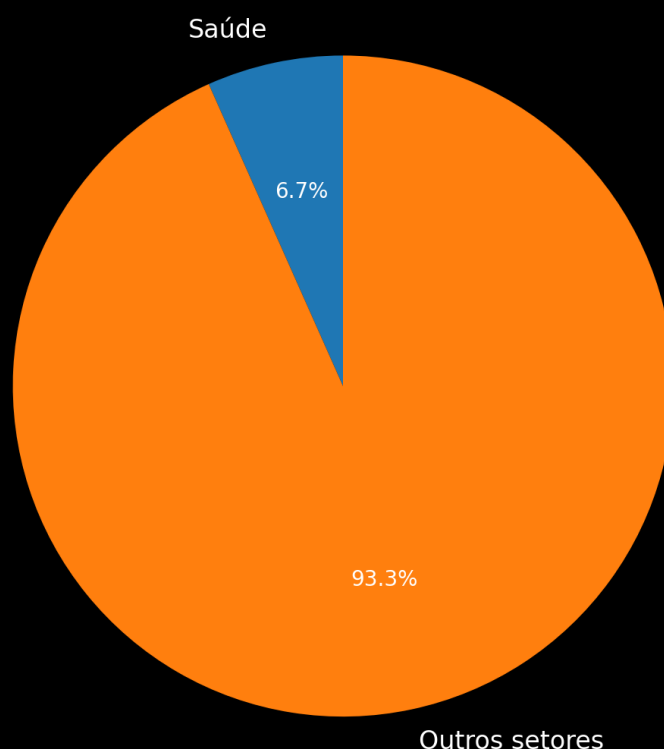


Figura 2 – Comparativo de ataques de ransomware no Brasil até o momento.

4.1 IMPACTOS DOS ATAQUES NO SETOR E NO BRASIL

No período analisado, foram registrados **90 ataques de ransomware no Brasil**, sendo que **6 deles tiveram como alvo organizações do setor de saúde**. Esse número corresponde a **6,7% do total de incidentes**, percentual que supera a média global apontada no relatório **Health-ISAC – 2025 Q2 Health Sector Heartbeat**, de **5,8%**. Essa diferença mostra que o setor de saúde brasileiro encontra-se **mais exposto do que a média mundial**, ainda que enfrente desafios semelhantes. A combinação de **infraestruturas críticas, dados altamente sensíveis e baixa tolerância a interrupções** torna cada ataque potencialmente devastador, com impactos desproporcionais que podem comprometer tanto a vida dos pacientes quanto a reputação e a sustentabilidade das instituições de saúde no país.

As consequências vão muito além da interrupção operacional. **Prontuários médicos e dados sensíveis de pacientes** têm sido **vazados e comercializados na dark web**, servindo de combustível para fraudes e extorsões. Para as instituições, os danos são múltiplos: **perdas financeiras milionárias**, multas por descumprimento da **LGPD** e, talvez o mais grave, a **quebra de confiança de pacientes e parceiros**, uma ferida difícil de recuperar. Esses ataques não revelam apenas falhas tecnológicas, mas também fragilidades éticas e sociais, reforçando que a cibersegurança na saúde deve ser encarada como uma questão de segurança pública e de preservação de vidas.

4.2 GRUPOS DE RANSOMWARE QUE REALIZARAM ATAQUES NESTE PERÍODO

- *Arcusmedia*
- *Akira*
- *incransom*
- *rhysida e outros grupos.*

No cenário **brasileiro**, grupos como Arcusmedia, Akira, Incransom e Rhysida foram identificados como os responsáveis por ataques de ransomware contra organizações de saúde neste período. Cada um deles atua de forma independente, empregando suas próprias técnicas e estratégias, mas todos têm em comum a exploração de vulnerabilidades críticas e a escolha de alvos altamente sensíveis. A presença desses grupos no país confirma que o setor de saúde brasileiro está dentro do **radar de coletivos** cibercriminosos já conhecidos internacionalmente pela sua agressividade e capacidade de causar graves interrupções operacionais.

Esses ataques não apenas interrompem serviços essenciais, mas também têm potencial para **expor dados clínicos sigilosos, utilizados em fraudes ou vendidos em fóruns clandestinos**. A escolha de hospitais, clínicas e laboratórios como alvos demonstra a natureza estratégica do ransomware, pois a impossibilidade de suspender atividades médicas críticas aumenta a pressão para que as vítimas considerem o pagamento do resgate. O fato de grupos dessa

relevância terem atuado no Brasil reforça a percepção de que o país se tornou um **terreno fértil** para ataques cibernéticos contra a saúde. Esse cenário exige que as organizações fortaleçam sua postura de defesa, invistam em medidas preventivas e tratem a cibersegurança como um pilar fundamental para a proteção de vidas, dados e reputação institucional.

5 A CONEXÃO QUE EXPÕE A RISCOS

Após entender que a conectividade pode colocar vidas em risco, é fundamental compreender **como essa exposição acontece na prática** e porque ela representa um problema tão crítico para a segurança hospitalar. Muitos dispositivos médicos modernos, como **bombas de infusão, monitores de sinais vitais, respiradores, servidores de imagem (PACS)** e até sistemas de prontuário eletrônico, foram projetados para operar em redes locais. No entanto, por conveniência ou má configuração, eles acabam sendo **conectados diretamente à internet** para facilitar atualizações, permitir suporte remoto ou integrar com sistemas hospitalares e laboratórios.

O problema é que essa conectividade, quando feita sem os devidos cuidados, **abre portas para invasores**. Falhas comuns incluem:

- **Interfaces web acessíveis sem autenticação;**
- **Senhas padrão ou fracas deixadas ativas;**
- **Protocolos desatualizados ou sem criptografia (como HTTP, VNC e Telnet);**
- **Integrações mal configuradas com PACS, HIS e RIS;**
- **Portas críticas expostas (como 104, 5800, 5900, 3389 etc.).**

Ferramentas como o **Shodan**, que funcionam como "Google para dispositivos conectados", permitem que qualquer pessoa com conhecimento básico encontre esses equipamentos usando termos simples como "PACS", "DICOM" ou outros ligados a este setor.



Figura 3 – Dispositivos DICOM expostos online.

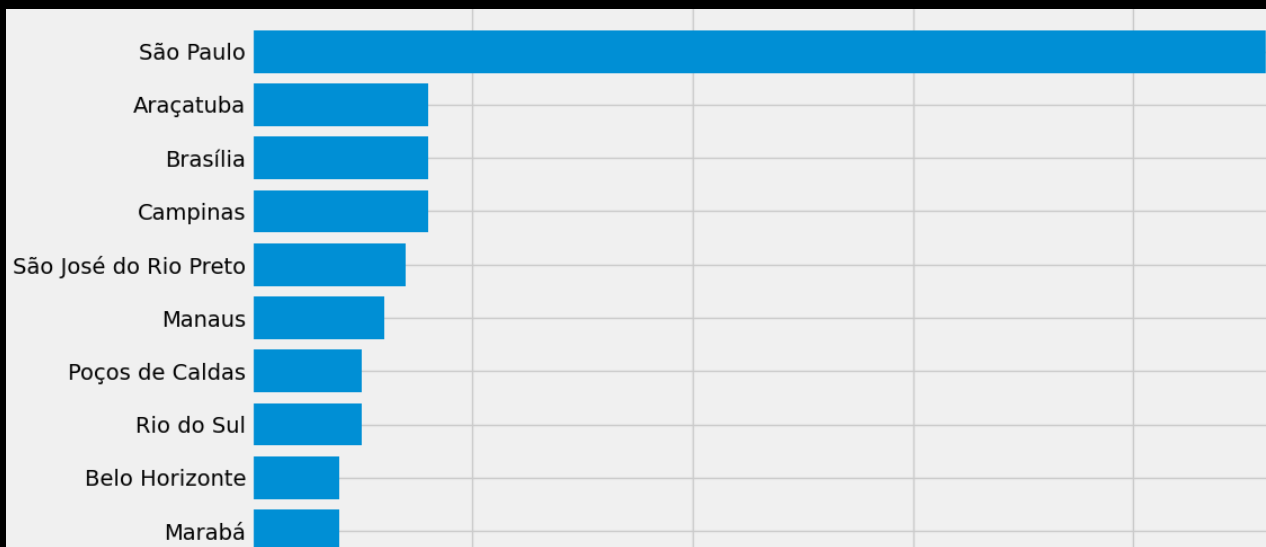


Figura 4 – Top 10 cidades Brasileiras com servidores PACS expostos online.

6 CASOS REAIS DE ATAQUES NO BRASIL E NO MUNDO

Ataques cibernéticos a dispositivos médicos e sistemas hospitalares não são hipotéticos, eles já estão acontecendo ao redor do mundo, inclusive no Brasil. Abaixo estão alguns exemplos concretos que demonstram a gravidade da exposição de equipamentos médicos conectados:

- **Agosto de 2024 – Brasil:** um ataque cibernético paralisou por vários dias o acesso a exames e prontuários médicos em uma das maiores instituições de saúde da região.
- **Setembro de 2024 – Brasil:** hospitais públicos e privados foram alvos de uma onda de ataques de ransomware, interrompendo atendimentos de emergência e afetando sistemas de suporte à vida.
- **Setembro de 2020 – Alemanha:** um ataque a sistemas hospitalares resultou na indisponibilidade de serviços críticos, contribuindo indiretamente para a morte de uma paciente que não pôde ser atendida a tempo.

Esses exemplos não apenas confirmam que os riscos são concretos, mas também mostram que **as consequências podem ser severas, imediatas e até fatais.**

7 PANORAMA DAS VIOLAÇÕES NO SETOR DE SAÚDE

Entre janeiro e junho de 2025, identificamos no setor de saúde no Brasil **11.426 registros de violações de segurança**, evidenciando sua alta exposição a riscos cibernéticos. Deste total, **97% destas violações foram confirmadas**, representando impactos diretos às organizações. Ainda mais preocupante, vários destes casos foram classificados como de alta severidade, indicando situações capazes de comprometer a continuidade do atendimento médico, expor informações sensíveis de pacientes e gerar prejuízos financeiros e reputacionais significativos.

Esses dados reforçam que o setor de saúde não deve ser analisado apenas pelo volume absoluto de incidentes, mas principalmente pela **gravidade dos ataques sofridos**. O cenário atual mostra que, mesmo representando uma fração do total nacional, os impactos no segmento de saúde são **desproporcionais e críticos**, exigindo atenção imediata e medidas robustas de mitigação.

7.1 DISTRIBUIÇÃO DAS TÁTICAS MITRE ATT&CK

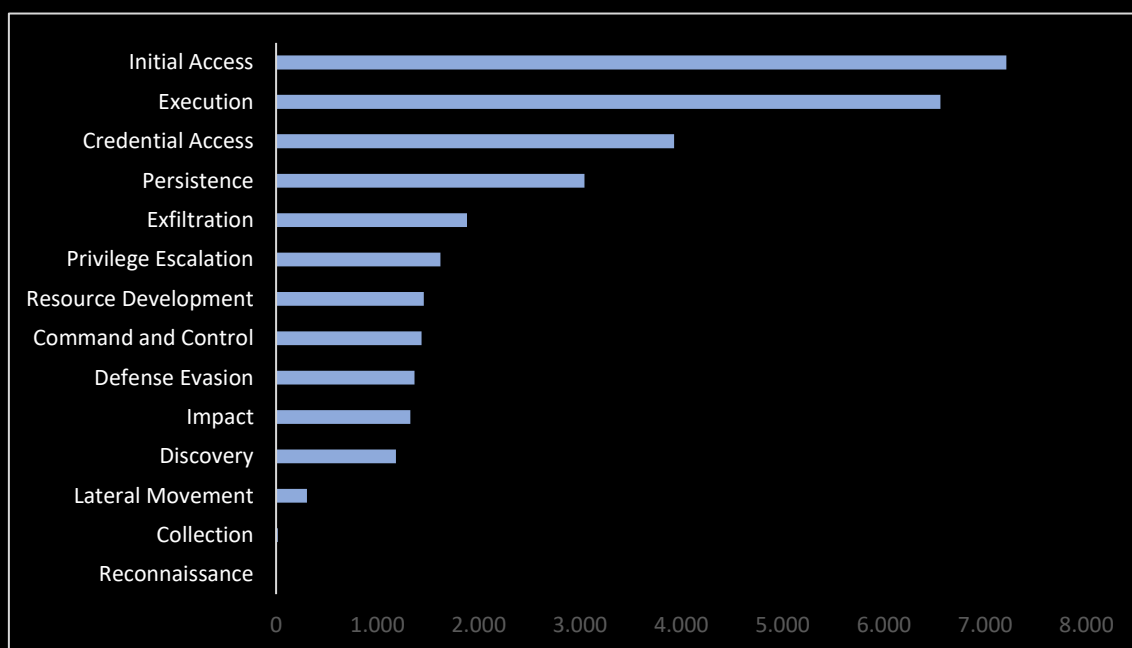


Figura 5 – Distribuição de Táticas MITRE ATT&CK em violações observadas.

A análise revela que os cibercriminosos priorizam fortemente três vetores no setor de saúde: **Initial Access** (27,9%), **Execution** (25,4%) e **Credential Access** (13,9%). Somados, esses três representam mais de **67% de todas as ocorrências**, deixando claro que a maior parte dos ataques tem como foco entrar nos sistemas, executar cargas maliciosas e capturar credenciais para movimentação posterior. Táticas como Persistence (11,8%) e Exfiltration (7,3%) reforçam a estratégia de manter presença prolongada e extrair dados sensíveis, ampliando o impacto do ataque. Embora outras técnicas apareçam em menor volume, o quadro evidencia

uma clara priorização por acesso inicial rápido e escalada de privilégios,
aumentando a pressão sobre hospitais e clínicas

8 CONCLUSÃO

Os dados evidenciam que, embora apenas **6,7% dos ataques de ransomware no Brasil** tenham atingido o setor de saúde, o **impacto é desproporcional e crítico**. Diferente de outros segmentos, cada incidente neste setor compromete diretamente a **continuidade do atendimento médico**, expõe **informações sensíveis de pacientes** e gera **prejuízos financeiros e reputacionais severos**. Na prática, o ransomware em hospitais e clínicas não é apenas uma ameaça tecnológica: é um risco concreto à vida humana e à confiança da sociedade no sistema de saúde.

A convergência entre vulnerabilidades conhecidas (sistemas legados, falta de segmentação de rede, falhas em DNS e exposição de acessos), a ascensão de **grupos criminosos especializados** e o comércio ilegal de dados médicos demonstra que o setor de saúde brasileiro precisa adotar a **cibersegurança como prioridade estratégica**. Investir em prevenção, resposta a incidentes, inteligência de ameaças e colaboração entre instituições não é mais opcional, é uma condição indispensável para proteger pacientes, garantir a resiliência operacional e preservar a credibilidade das organizações de saúde no país.

9 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.

9.1 AKIRA RANSOMWARE

Tática	Técnica	Detalhes
Initial Access	T1078 Valid Accounts T1190 Exploit Public Facing Application T1133 External Remote Services T1566.001 Phishing: Spearphishing Attachment T1566.002 Phishing: Spearphishing Link	O grupo Akira adota diferentes técnicas para obter acesso inicial aos ambientes de suas vítimas. Entre as principais estratégias estão o uso e abuso de credenciais de contas existentes, explorando acessos válidos já comprometidos, bem como a exploração de vulnerabilidades em sistemas expostos à internet. Além disso, seus operadores recorrem frequentemente a serviços de acesso remoto, como conexões via RDP ou VPN, para invadir redes corporativas. Outro vetor bastante utilizado envolve campanhas de phishing, nas quais são enviados e-mails maliciosos contendo anexos infectados ou links nocivos, ambos projetados para enganar usuários e permitir a infiltração em sistemas.
Credential Access	T1003 OS Credential Dumping T1003.001 OS Credential Dumping: LSASS Memory	O grupo Akira também faz uso de ferramentas conhecidas, como Mimikatz e LaZagne, para realizar o dumping de credenciais e obter informações de autenticação armazenadas nos sistemas. Além disso, seus operadores procuram acessar materiais de credenciais diretamente na memória do processo LSASS (Local Security Authority Subsystem Service), técnica que lhes permite capturar senhas e tokens de autenticação e, assim, ampliar seu controle sobre a rede comprometida.
Discovery	T1016 System Network Configuration Discovery T1082 System Information Discovery T1482 Domain Trust Discovery	O grupo Akira faz uso de diferentes ferramentas e comandos do Windows para reconhecimento e mapeamento de redes comprometidas. Utiliza scanners e o PCHunter64 para obter informações detalhadas de processos e sistemas, além de comandos como net e nltest para enumerar domínios,

	T1057 Process Discovery T1069.001 Permission Groups Discovery: Local Groups T1069.002 Permission Groups Discovery: Domain Group T1018 Remote System Discovery	grupos, permissões e listar outros sistemas da rede. Também emprega a Tasklist via PowerShell para visualizar processos em execução. Essas técnicas fornecem aos atacantes a visibilidade necessária para realizar movimento lateral e escalonamento de privilégios de forma estruturada.
Persistence	T1136.002 Create Account: Domain Account	Os agentes da ameaça Akira tentam abusar das funções dos controladores de domínio criando novas contas de domínio para estabelecer persistência.
Defense Evasion	T1562.001 Impair Defenses: Disable or Modify Tools	Os agentes da ameaça Akira usam ataques BYOVD para desabilitar software antivírus.
Command and Control	T1219 Remote Access Software T1090 Proxy	O grupo Akira utiliza ferramentas legítimas para manter acesso e exfiltrar dados. Entre elas, o AnyDesk , usado para garantir acesso remoto contínuo aos sistemas das vítimas, e o Ngrok , empregado para criar túneis seguros que facilitam o envio de informações para servidores externos durante os ataques.
Collection	T1560.001 Archive Collected Data: Archive via Utility	Os agentes da ameaça Akira usam ferramentas como o WinRAR para compactar arquivos.
Exfiltration	T1048 Exfiltration Over Alternative Protocol T1537 Transfer Data to Cloud Account T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	O grupo Akira emprega diferentes ferramentas para exfiltração de dados durante suas operações. Utiliza o WinSCP para realizar transferências de arquivos, o CloudZilla para enviar informações a contas em nuvem e conectar-se a servidores sob seu controle, e o RClone para sincronizar arquivos com serviços de armazenamento em nuvem. Essas técnicas permitem que os atacantes movimentem grandes volumes de dados roubados de forma eficiente e menos perceptível.
Impact	T1486 Date Encrypted for Impact T1490 Inhibit System Recovery T1657 Financial Theft	O grupo Akira realiza a criptografia de dados para interromper serviços, remove cópias de sombra do Windows para dificultar a recuperação e adota o modelo de dupla extorsão , combinando bloqueio de sistemas e ameaça de vazamento de informações para obter ganhos financeiros.

Tabela 1 – Tabela MITRE ATT&CK – Akira ransomware.

9.2 RHYSIDA RANSOMWARE

Tática	Técnica	Detalhes
Resource Development	T1587 Develop Capabilities	Criação de ferramentas personalizadas, como executáveis nomeados "Rhysida-0.1".
Initial Access	T1078 Valid Accounts	Acesso via serviços VPN/RDP externos com credenciais comprometidas.
Execution	T1059.009 Command and Scripting Interpreter: Cloud API T1059.001 Command and Scripting Interpreter: PowerShell T1059.003 Command and Scripting Interpreter: Windows Command Shell	Os operadores do Rhysida utilizam o AZCopy para movimentar dados em ambientes de nuvem, além de comandos PowerShell como ipconfig, nltest e net para executar ações maliciosas. Também recorrem a scripts em lote (ex.: 1.ps1) para automatizar a execução do ransomware.
Privilege Escalation	T1055.002 Process Injection: Portable Executable Injection	Os operadores do Rhysida injetam o aplicativo de ransomware, um executável PE de 64 bits para Windows em processos em execução nos sistemas comprometidos.
Defense Evasion	T1070.001 Indicator Removal: Clear Windows Event Logs T1070.004 Indicator Removal: File Deletion T1564.003 Hide Artifacts: Hidden Window	Os operadores do Rhysida utilizam o wevtutil.exe para limpar logs do Windows, empregam PowerShell para excluir arquivos binários e executam janelas PowerShell ocultas para dificultar a detecção.
Credential Access	T1003.003 OS Credential Dumping: NTDS T1112 Modify Registry	Os operadores do Rhysida utilizam o secretsdump para extrair credenciais, incluindo NTDS, e executam modificações no registro do Windows por meio do cmd.exe para reforçar o controle sobre os sistemas comprometidos.
Discovery	T1016 System Network Configuration Discovery T1018 Remote System Discovery T1033 System Owner/User Discovery T1069.001 Permission Groups Discovery: Local Groups T1069.002 Permission Groups Discovery: Domain Groups	Os operadores do Rhysida realizam extensa enumeração de rede e contas para mapear o ambiente. Utilizam comandos como ipconfig para configurações de rede, whoami e net para identificar usuários logados, além de net localgroup administrators e net group "domain admins" para descobrir privilégios locais e de domínio. Também recorrem ao comando net user [username] /domain para informações de contas e ao nltest para identificar relações de confiança entre domínios.

	T1087.002 Account Discovery: Domain Account T1482 Domain Trust Discovery	
Lateral Movement	T1021.001 Remote Services: Remote Desktop Protocol T1021.004 Remote Services: SSH	Os operadores do Rhysida utilizam o RDP para movimento lateral e exploram credenciais comprometidas em conjunto com o PuTTY , conectando-se a sistemas das vítimas por meio de SSH .
Command and Control	T1219 Remote Access Software	Atores do Rhysida foram observados usando o software AnyDesk para obter acesso remoto aos sistemas das vítimas.
Impact	T1486 Data Encrypted for Impact T1657 Financial Theft	O Rhysida utiliza criptografia de arquivos com RSA-4096 combinado ao algoritmo ChaCha20 , tornando a recuperação sem chave quase impossível. Além disso, adota a dupla extorsão , exigindo pagamento tanto para a descriptografia quanto para impedir a divulgação dos dados exfiltrados.

Tabela 2 – Tabela MITRE ATT&CK – Rhysida ransomware.

9.3 INC RANSOMWARE

Tática	Técnica	Detalhes
Initial Access	T1078 Valid Accounts T1190 Exploit Public-Facing Application	Credenciais adquiridas de access brokers e campanhas de phishing ; exploração da vulnerabilidade CVE-2023-3519 (Citrix/NetScaler).
Credencial Access	T1003 OS Credential Dumping	Uso do HackTool.PS1.VeeamCreds para roubo de credenciais do Veeam Backup & Replication.
Discovery	T1046 Network Scanning T1083 File and Directory Discovery	Uso de NetScan e Advanced IP Scanner para mapear redes; inspeção de arquivos com Notepad, Wordpad e Paint; download e uso de Mimikatz .
Lateral Movement	T1021.002 Remote Services	Propagação via PsExec, além de ferramentas legítimas como AnyDesk e TightVNC.
Collection	T1560 Archive Collected Data	Compressão de arquivos.
Exfiltration	T1567 Exfiltration Over Web Service: Exfiltration to Cloud Storage	Exfiltração de dados e envio para nuvem usando MegaSync .
Impact	T1490 Inhibit System Recovery T1486 Data Encrypted for Impact	Exclusão de cópias de sombra com vssadmin ; criptografia via AES , com modos rápido, médio e lento.

Tabela 3 – Tabela MITRE ATT&CK – Inc ransomware.

10 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:

10.1 CONTROLE DE ACESSO INICIAL

- Ative **MFA (autenticação multifator)** em VPN, RDP e sistemas críticos.
- Nunca deixe **RDP exposto diretamente à internet**; use VPN com regras de acesso restritas.
- Mantenha **sistemas atualizados** (especialmente Citrix, NetScaler, VPNs e gateways).
- Reforce a segurança de e-mails: bloqueio de anexos perigosos, proteção contra links maliciosos e uso de políticas DMARC/SPF/DKIM.

10.2 GESTÃO DE IDENTIDADES E PRIVILÉGIOS

- Use o princípio de **menor privilégio**: cada usuário só deve ter o acesso realmente necessário.
- Troque senhas locais padrão e utilize soluções como **LAPS** para senhas únicas.
- Proteja credenciais de administradores com **contas separadas** e monitoradas.
- Ative proteções do Windows como Credential Guard e LSA Protection para evitar roubo de senhas.

10.3 PROTEÇÃO DE ENDPOINTS E SERVIDORES

- Utilize um **EDR (antivírus avançado)** configurado em modo de bloqueio, não apenas de monitoramento.
- Implemente **controle de aplicações** (AppLocker/WDAC) para bloquear ferramentas de ataque comuns (ex: PsExec, Mimikatz, AnyDesk, TightVNC, Ngrok, RClone).
- Restrinja o uso de **PowerShell**: habilite logging, bloqueie execução de scripts desconhecidos e use modo restrito.

10.4 SEGURANÇA DE REDE

- Separe a rede em segmentos: usuários, servidores e equipamentos médicos não devem se comunicar livremente.
- Restrinja o uso de SMB e Admin\$ apenas a administradores.
- Monitore e bloqueie conexões de saída para serviços suspeitos como MegaSync, Ngrok, RClone e storage em nuvem não autorizado.

- Use filtros de DNS e proxy para impedir acesso a sites maliciosos.

10.5 PROTEÇÃO DE DADOS E BACKUPS

- Mantenha backups no modelo 3-2-1: várias cópias, em locais diferentes, com pelo menos uma cópia offline ou imutável.
- Teste regularmente a restauração dos backups para garantir que funcionam.
- Proteja sistemas de backup (como Veeam) com MFA e acesso restrito.
- Monitore comandos suspeitos como vssadmin delete ou wbadmin que apagam cópias de segurança.

10.6 DETECÇÃO E MONITORAMENTO

- Crie alertas para comandos maliciosos comuns:
- wevtutil cl (apagar logs)
- vssadmin delete (apagar backups)
- nltest, net group, whoami (enumeração de rede e privilégios).
- Detecte execuções de ferramentas como PsExec, AnyDesk, TightVNC, Ngrok, RClone.
- Monitore tentativas de acesso ao processo lsass.exe (típico de roubo de credenciais).

10.7 RESPOSTA E PREPARAÇÃO

- Desenvolva um playbook de resposta a ransomware, incluindo contatos de emergência, comunicação pública e critérios para decisão de pagamento.
- Realize simulações e exercícios periódicos de ataque cibernético com times técnicos e clínicos.
- Treine funcionários para reconhecer e reportar phishing e comportamentos suspeitos.

10.8 AMBIENTES DE SAÚDE

- Faça inventário completo de **equipamentos médicos conectados**.
- Coloque esses dispositivos em uma **rede separada e isolada**.
- Troque **senhas padrão** em dispositivos médicos e sistemas de suporte.
- Tenha **planos de contingência** para operar manualmente (em papel) em caso de indisponibilidade dos sistemas.
- **Implemente monitoramento contínuo** em dispositivos médicos, com alertas para tráfego anômalo ou conexões externas suspeitas. Isso ajuda a identificar quando um equipamento pode estar sendo explorado como porta de entrada.

- **Estabeleça políticas de atualização e manutenção seguras** para dispositivos médicos, garantindo que patches críticos sejam aplicados sempre que o fabricante disponibilizar, reduzindo a exposição a vulnerabilidades conhecidas.

11 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.

11.1 INDICADORES DE COMPROMETIMENTO (IoC)

Indicadores do artefato	
md5:	2a74a11a5815ccd8e70dacd0a12b7b05
sha1:	5f2d4b7799d68fede72d04612c9d0791b7c1d49d
sha256:	bd925297784089ce7ff2b548a6a8eaf1c8207ba05dc3192facbb54128dbaed2c
File name:	bd925297784089ce7ff2b548a6a8eaf1c8207ba05dc3192facbb54128dbaed2c.exe

Indicadores do artefato	
md5:	0c8e88877383ccd23a755f429006b437
sha1:	69b3d913a3967153d1e91ba1a31ebd839b297ed
sha256:	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6
File name:	0c8e88877383ccd23a755f429006b437

Indicadores do artefato	
md5:	1e256229b58061860be8dbf0dc4fe67e
sha1:	338d4f4ec714359d589918cee1adad12ef231907
sha256:	d5c2f87033a5baeeb1b5b681f2c4a156ff1c05ccd1bfdaf6eae019fc4d5320ee
File name:	chileconhostexe.exe.dat

Indicadores do artefato	
md5:	1fb412212359a970be06b9a4578c1e68
sha1:	efa771d6f699c7240c80260d50925ed8baae3cdc
sha256:	fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced
File name:	Inc_Ransomware

Indicadores do artefato	
md5:	1922a47e467e4185eea0bb003e813dde
sha1:	cd0228e52de03fc2423e22df9840ba5dc707c4b4
sha256:	1754c9973bac8260412e5ec34bf5156f5bb157aa797f95ff4fc905439b74357a
File name:	ais.exe.vir

Indicadores do artefato	
md5:	eefcd1ab5b3638c870730e459d3545ed
sha1:	efb651a5c755a9a5a96b08ddda736efd0bc03315
sha256:	3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75
File name:	akira_v2-CapturedBy-DrPwner

Indicadores do artefato	
-------------------------	--

md5:	205589629ead5d3c1d9e914b49c08589
sha1:	3c1d57a054f3bee458754c24de73af6450ffdfb4
sha256:	ae455890e2123a9d011e47065828b0a03c08fd66570fab9d0340d2f5d5eb40c3
File name:	aki.exe

Indicadores do artefato	
md5:	7d827558e7841cc2887fc99537c1c97e
sha1:	94ed0a9c9c9fe568dc814218edeb17b951fc78a8
sha256:	0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c
File name:	akira_v2-CapturedBy-DrPwner

Tabela 4 – Indicadores de Comprometimento.

12 REFERÊNCIAS

- Heimdall by ISH Tecnologia
- [MITRE ATT&CK](#)
- [Health-ISAC](#)
- [CISA](#)
- [NVD](#)

13 AUTORES

- Ismael Rocha – Threat Intelligence Specialist
- Thiago Cesar Maciel da Paixão – Threat Intelligence Analyst



heimdall
security research

A DIVISION OF ISH