RELATÓRIO ANUAL DE CIBERSEGURANÇA 2025

A leitura estratégica das ameaças, técnicas e impactos que moldaram o cenário de cibersegurança no Brasil.

USM 30 anos | heimdall security research

SUMÁRIO

1. O olhar da Inteligência de Ameaças Pg.04

2. O olhar da Operação de Segurança Pg.05

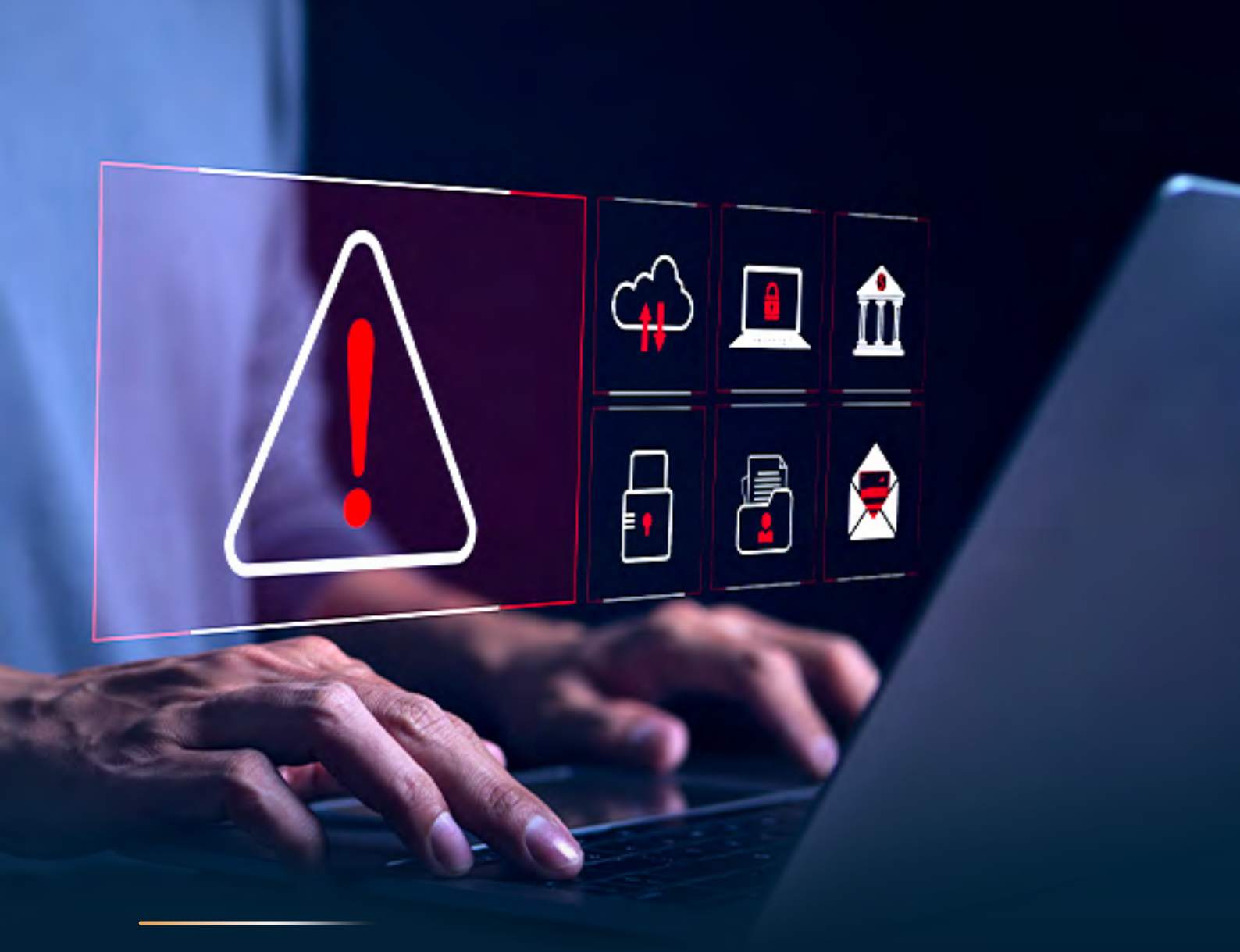
3. Principais ameaças observadas no ambiente corporativo brasileiro Pg.07

4. Técnicas e táticas mais exploradas pelos atacantes Pg.09

5. Setores impactados, padrões de ataque e onde os controles falham Pg.11

6. Da falha inicial ao impacto operacional: a cadeia de ataque na prática Pg.13

7. 2026 | Esteja pronto para os desafios que vêm pela frente Pg.14



Introdução

Ao longo de 2025, o cenário de ameaças digitais manteve uma trajetória clara de amadurecimento e complexidade. Ataques tornaram-se **mais direcionados, silenciosos e persistentes,** explorando não apenas vulnerabilidades técnicas, mas também falhas de processo, decisões operacionais e limitações estruturais das operações de segurança.

A atuação do **Heimdall, time de Inteligência de Ameaças da ISH**, ao longo do ano, permitiu acompanhar de forma contínua a evolução dessas ofensivas. Grupos criminosos ampliaram o uso de **engenharia social avançada, exploração de cadeias de fornecedores, abuso de credenciais legítimas e ataques de baixa visibilidade,** desenhados para permanecer ativos por longos períodos sem detecção imediata.

Em paralelo, a operação do SOC revelou outro aspecto relevante desse cenário. O **crescimento do volume de alertas, eventos** e **sinais de risco** não foi acompanhado, na mesma proporção, por ganho de clareza operacional.

Em muitos ambientes, equipes passaram a lidar com mais dados, mais ferramentas e mais notificações, mas com maior dificuldade de distinguir o que é ruído do que representa risco real.

O conteúdo a seguir busca apoiar líderes de segurança, tecnologia e risco **na compreensão desse cenário** e **na construção de decisões mais conscientes,** conectadas à realidade operacional e orientadas por inteligência.

1. O olhar da Inteligência de Ameaças

O que mudou no cenário de ameaças em 2025

A análise contínua conduzida pelo Heimdall ao longo de 2025 evidencia uma mudança importante na forma como as ameaças cibernéticas se materializam. Mais do que um aumento de volume, o que se observa é uma **evolução clara na velocidade, no foco e na combinação de técnicas utilizadas pelos atacantes.**

O cenário deixou de ser marcado por campanhas amplas e oportunistas e passou a operar com **precisão**, mirando ativos específicos, setores estratégicos e ambientes com alto impacto operacional.

Três movimentos que definiram o ano

Ao longo do período, três movimentos se destacaram de forma consistente:

• **Exploração acelerada de vulnerabilidades críticas**
Vulnerabilidades classificadas como altas e críticas passaram a ser exploradas em janelas cada vez menores. Em muitos casos, a exploração ocorreu poucos dias após a divulgação pública da falha, antes mesmo que organizações conseguissem aplicar correções ou medidas compensatórias;

• **Ataques mais direcionados e seletivos**
Em vez de campanhas genéricas, os grupos passaram a escolher alvos com maior potencial de impacto, priorizando ambientes críticos, infraestruturas expostas e organizações com dependência operacional elevada de sistemas digitais;

• **Convergência entre diferentes objetivos de ataque**
Espionagem, ransomware e ataques à cadeia de suprimentos deixaram de ser vetores isolados. Em diversos incidentes analisados, essas abordagens apareceram combinadas dentro do mesmo ataque, ampliando danos e dificultando a resposta.

Vulnerabilidade deixou de ser exceção. Passou a ser ponto de partida.

O crescimento no número de vulnerabilidades altas e críticas observadas ao longo de 2025 reforça que o risco não está somente na existência da falha, mas na **velocidade com que ela se transforma em vetor de ataque real.**

Na prática, isso significa que:

• A simples publicação de uma CVE já funciona como um sinal de alerta para grupos criminosos;

• Atrasos em processos de correção ampliam exponencialmente a superfície de ataque;

• Ambientes com visibilidade limitada tornam-se alvos preferenciais, mesmo sem histórico prévio de incidentes.

Inteligência como fator de antecipação

O que diferencia organizações mais resilientes nesse cenário não é apenas a capacidade de resposta, mas a **capacidade de antecipação.**

As pesquisas do Heimdall mostram que ambientes que contam com inteligência de ameaças ativa conseguem:

• Priorizar vulnerabilidades com base em exploração real, não apenas severidade teórica;

• Entender quais setores e tecnologias estão no radar dos atacantes;

• Ajustar controles antes que a ameaça atinja a fase operacional.

Nos últimos anos, a inteligência deixou de ser um apoio pontual à segurança. Ela passou a atuar como **camada estratégica para orientar decisões, priorizar riscos e reduzir o tempo entre exposição e mitigação.**

Esse desequilíbrio cria um cenário recorrente: times ocupados, sistemas ativos, dashboards cheios e, ainda assim, **brechas importantes passam despercebidas.**

O que mais pressiona as operações de SOC

Na prática, os fatores que mais impactaram a eficiência operacional em 2025 foram:

• Crescimento contínuo do volume de alertas provenientes de múltiplas fontes;

• Repetição de eventos similares, originados de um mesmo incidente;

• Baixa contextualização dos alertas no momento da triagem;

• Dependência excessiva de análise manual para priorização;

• Tempo significativo gasto com falsos positivos.

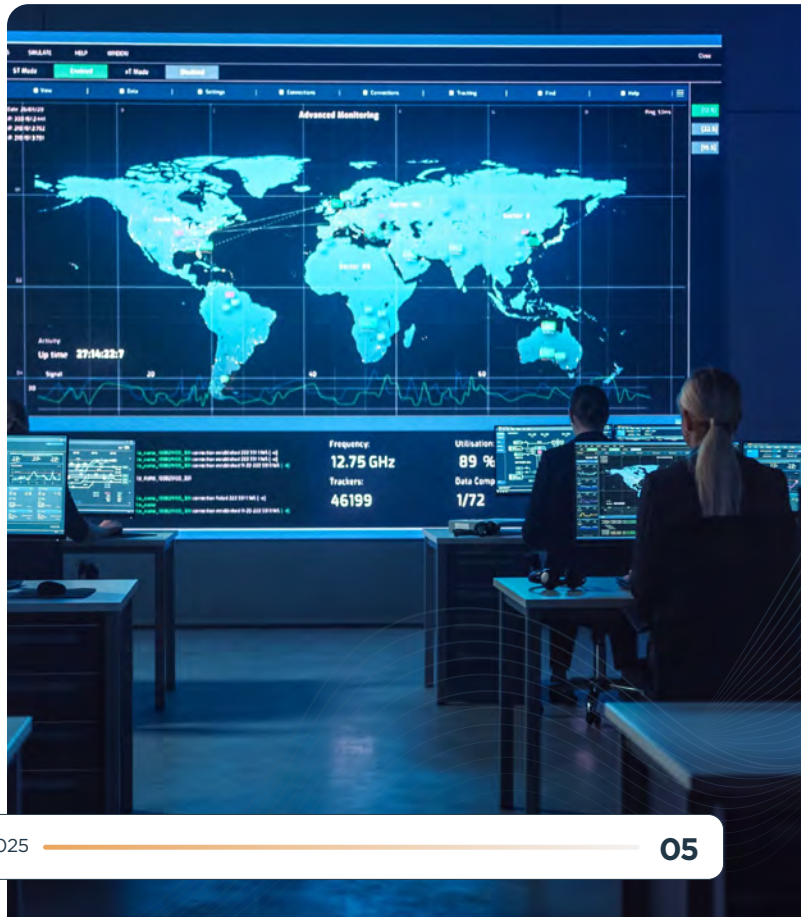
O resultado é perda de foco. Quando tudo parece urgente, decidir o que realmente importa se torna mais difícil.

2. O olhar da Operação de Segurança

Onde o risco se materializa no dia a dia

Ao longo de 2025, o SOC da ISH observou que o principal desafio das operações de segurança deixou de ser a ausência de alertas. O problema passou a ser **o excesso**.

Ambientes monitorados 24x7 operam hoje sob um volume constante de eventos, sinais e notificações. Nem todos representam risco real. Muitos competem pela atenção dos analistas. Poucos exigem ação imediata.



Alertas demais, visibilidade de menos

Um dos pontos mais sensíveis observados pelo SOC foi a diferença entre **quantidade de alertas e qualidade da visibilidade**. Em muitos ambientes, os analistas enxergam fragmentos do problema, mas não o contexto completo. Isso gera:

• Investigações paralelas sobre o mesmo evento;

• Dificuldade de correlacionar ações isoladas em um ataque contínuo;

• Respostas tardias a incidentes que evoluem silenciosamente.

O risco não está apenas no ataque sofisticado. Está no ruído que impede sua identificação a tempo.

O custo invisível dos falsos positivos

Entre os desafios operacionais observados pelo SOC ao longo do ano, um se destacou pelo impacto direto na eficiência das equipes: o volume de falsos positivos.

Entre janeiro e outubro, o SOC da ISH registrou **mais de 41 mil falsos positivos**. Convertido em esforço operacional, esse volume representou **mais de 35 mil horas dedicadas à investigação de alertas sem risco real**, o equivalente a aproximadamente **R$ 7 milhões em recursos humanos e tecnológicos.**

O problema não está apenas na ameaça externa, mas também na eficiência interna da detecção.

O setor financeiro liderou o volume de ocorrências, com cerca de **16 mil alertas indevidos no período**, refletindo o alto nível de monitoramento exigido em ambientes altamente transacionais e regulados, onde qualquer comportamento fora do padrão pode gerar sinalização automática.

Mas o fenômeno não se restringe a um único segmento. Falsos positivos surgem em diferentes camadas da defesa:

• Atualizações legítimas confundidas com comunicação maliciosa;

• Scripts internos identificados como comportamento suspeito;

• Acessos fora do horário comercial classificados como anomalias;

• Movimentações intensas de dados tratadas como possível exfiltração.

Isoladamente, cada evento parece pequeno. Somados, criam um ruído constante que compromete a precisão das detecções críticas.

O impacto humano da operação sob pressão

A operação de segurança é, antes de tudo, feita por pessoas. Em 2025, ficou evidente que a sobrecarga operacional afeta diretamente:

• A qualidade das análises;

• A consistência das decisões;

• A capacidade de resposta em incidentes críticos.

Esse cenário, conhecido como **fadiga de alertas**, não é falha individual nem falta de comprometimento. É consequência de modelos operacionais que não acompanharam a complexidade atual dos ambientes digitais.

Quando o SOC reage, em vez de conduzir

Outro padrão recorrente observado foi a atuação reativa. Em ambientes onde a operação vive apagando incêndios:

• O tempo de resposta aumenta;

• A priorização acontece tarde demais;

• A segurança passa a responder ao ataque, não a antecipá-lo.

Sem contexto, sem correlação e sem critérios claros de risco, o SOC deixa de ser um centro de decisão e passa a ser apenas um ponto de contenção.

O sinal de alerta para as organizações

A leitura da operação em 2025 deixa uma mensagem clara:

• Um SOC pode estar funcionando tecnicamente e ainda assim falhar estrategicamente;

• Quando a operação perde a capacidade de distinguir ruído de ameaça real, o risco deixa de ser hipotético e passa a ser operacional;

• Essa é a fronteira onde a segurança começa a impactar diretamente a continuidade do negócio.

3. Principais ameaças observadas no ambiente corporativo brasileiro

A análise dos incidentes monitorados pelo Heimdall mostra que o cenário de ameaças deixou de ser fragmentado. As ofensivas passaram a combinar múltiplas técnicas em uma mesma campanha, com foco claro em acesso inicial rápido, persistência e monetização.

1. Ransomware segue como vetor dominante

Os ataques de ransomware continuam sendo a principal ameaça operacional, mas com mudanças relevantes no modo de atuação:

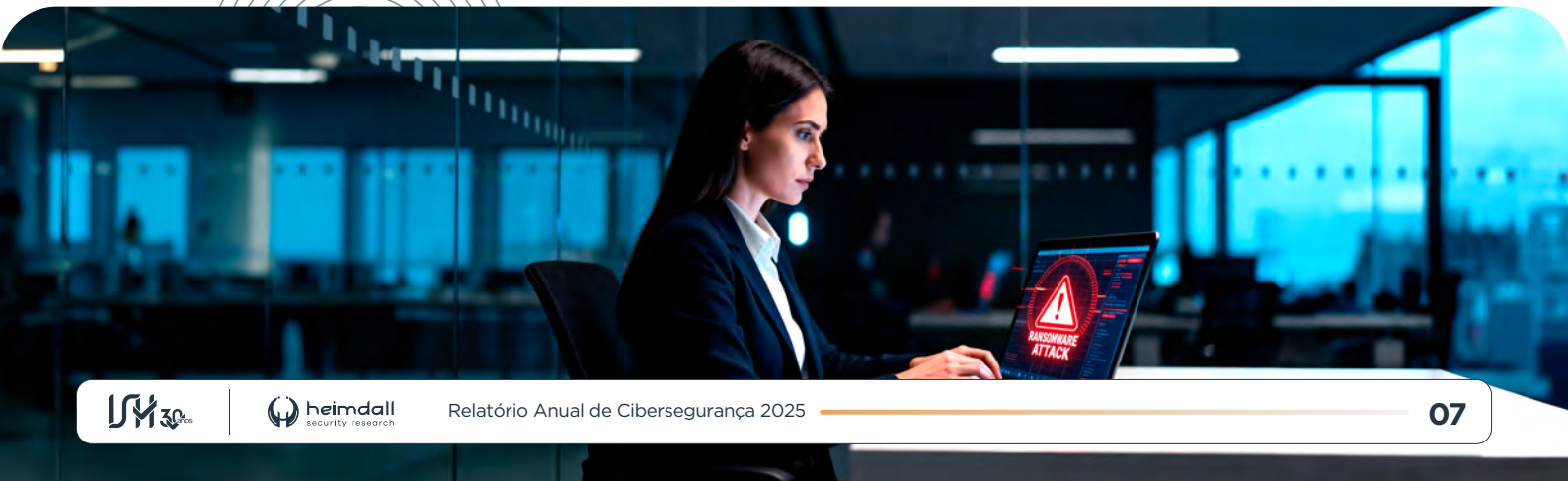
• Campanhas mais seletivas, priorizando ambientes com alto impacto operacional;

• Uso recorrente de credenciais válidas para acesso inicial;

• Execução mais rápida entre a intrusão e a criptografia;

• Adoção consistente de dupla extorsão, com exfiltração prévia de dados.

Grupos como **Akira, Rhysida, INC e Arcusmedia** mantiveram atuação constante, explorando falhas conhecidas e ambientes com baixa maturidade de segmentação e controle de acesso.



2. Exploração de vulnerabilidades como porta de entrada

A exploração de vulnerabilidades críticas permaneceu entre os principais vetores de acesso inicial, especialmente em:

• Gateways de acesso remoto;

• Serviços expostos à internet;

• Infraestruturas legadas sem patching regular.

Falhas amplamente divulgadas continuaram sendo exploradas mesmo semanas após sua publicação, indicando lacunas recorrentes em gestão de vulnerabilidades e priorização de correções.

O padrão observado indica que **não é a existência da vulnerabilidade que determina o risco, mas a falta de resposta no tempo certo.**

3. Credenciais válidas como ativo estratégico do atacante

Grande parte dos ataques analisados envolveu o uso de credenciais legítimas em algum momento da cadeia de comprometimento. Essas credenciais foram obtidas por meio de:

• Phishing direcionado;

• Vazamentos anteriores reutilizados;

• Comprometimento de dispositivos pessoais;

• Falhas em políticas de autenticação e privilégio.

Uma vez dentro do ambiente, o atacante passa a operar com baixo ruído, dificultando a detecção e ampliando o tempo de permanência.

4. Expansão lateral e persistência silenciosa

Após o acesso inicial, os ataques tendem a evoluir rapidamente para:

• Movimentação lateral entre sistemas;

• Elevação de privilégios;

• Criação de persistência por serviços, tarefas agendadas ou contas adicionais.

Em muitos casos, o ambiente permanece comprometido por longos períodos antes da identificação do incidente, aumentando o impacto final.

5. Ataques à cadeia de suprimentos e terceiros

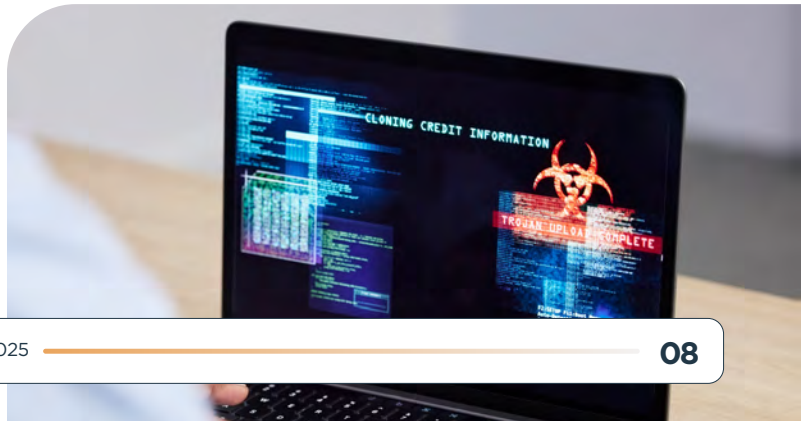
Outro movimento relevante foi o aumento de ataques indiretos, explorando:

• Fornecedores de tecnologia;

• Prestadores de serviço;

• Integrações entre sistemas.

A dependência de terceiros ampliou a superfície de ataque e criou cenários de efeito dominó, onde uma única falha compromete múltiplas organizações.



Síntese da ameaça

O que se observa é um cenário onde:

• Os ataques são mais planejados;

• A exploração é mais rápida;

• A permanência no ambiente é maior;

• O impacto final é mais amplo.

As ameaças deixaram de ser episódicas e passaram a operar **como processos contínuos**, explorando falhas técnicas, operacionais e de governança.

4. Técnicas e táticas mais exploradas pelos atacantes

A análise das campanhas monitoradas revela que os ataques seguem **padrões técnicos bem definidos**, com combinações recorrentes de técnicas que priorizam velocidade, baixo ruído e alto impacto.

Essas técnicas não são novas isoladamente, mas passaram a ser usadas de forma **mais coordenada e eficiente.**

Acesso inicial: o ponto mais explorado da cadeia

O início da maioria dos ataques continua concentrado em poucos vetores principais:

• Exploração de serviços expostos à internet;

• Uso de credenciais válidas comprometidas;

• Phishing direcionado a usuários com acesso privilegiado;

• Vulnerabilidades conhecidas sem correção aplicada.

A preferência por acessos legítimos ou falhas já documentadas reduz a necessidade de exploits complexos e dificulta a detecção inicial.

Execução rápida após a intrusão

Uma vez obtido o acesso, a execução de código malicioso ocorre de forma quase imediata. Os atacantes priorizam:

• Uso de ferramentas nativas do sistema operacional;

• Scripts simples para download e execução de payloads;

• Técnicas que evitam arquivos maliciosos tradicionais.

Esse comportamento reduz alertas baseados em assinatura e aumenta a taxa de sucesso da intrusão.

Persistência: permanecer sem ser visto

Garantir acesso contínuo ao ambiente é parte central da estratégia. As técnicas mais observadas incluem:

• Criação de tarefas agendadas;

• Modificação de serviços existentes;

• Uso de contas válidas para manter acesso recorrente;

• Backdoors discretos em sistemas pouco monitorados.

A persistência é construída para resistir a reinicializações e ações pontuais de contenção.

Elevação de privilégios e credenciais

Após estabelecer presença no ambiente, os atacantes buscam rapidamente ampliar seu nível de acesso. As táticas mais comuns envolvem:

• Dump de credenciais em memória;

• Exploração de permissões excessivas;

• Reutilização de senhas entre sistemas;

• Abuso de contas administrativas mal protegidas.

Esse estágio é decisivo para permitir movimentação lateral e acesso a ativos críticos.

Movimentação lateral: expansão do impacto

A movimentação lateral ocorre de forma gradual e estratégica, com foco em:

• Servidores centrais;

• Ambientes de virtualização;

• Sistemas de backup;

• Bases de dados sensíveis.

Em muitos casos, o atacante evita movimentos agressivos para não gerar ruído, priorizando alcance silencioso.

Exfiltração e impacto final

Nos ataques mais maduros, a fase final envolve:

• Exfiltração seletiva de dados;

• Preparação do ambiente para criptografia;

• Desativação de mecanismos de segurança;

• Execução coordenada do impacto.

A exfiltração passou a ser parte padrão da operação, reforçando a lógica de dupla extorsão.

O padrão técnico observado

As táticas analisadas indicam um cenário onde:

• A cadeia de ataque é curta e objetiva;

• O tempo entre acesso inicial e impacto é cada vez menor;

• Técnicas legítimas são usadas contra o próprio ambiente;

• A detecção depende menos de ferramentas isoladas e mais de contexto.

O atacante moderno não depende de uma única técnica. Ele combina **acesso, execução, persistência e movimento** de forma integrada, explorando lacunas operacionais e de visibilidade.

5. Setores impactados, padrões de ataque e onde os controles falham

A análise dos incidentes observados ao longo do período revela que, embora os ataques tenham características técnicas distintas, **os padrões de impacto entre setores se repetem**. O que muda não é tanto o alvo, mas **o efeito operacional quando controles básicos falham.**

Mais do que setores "preferidos", os atacantes buscam **ambientes previsíveis, expostos e com baixa maturidade de resposta.**

Setores mais impactados

Os dados mostram concentração de ataques em setores que combinam **alta dependência digital, operações críticas e ambientes heterogêneos.**

Saúde

• Ambientes legados convivendo com novas tecnologias;

• Exposição recorrente de PACS, DICOM e sistemas clínicos;

• Impacto direto na continuidade de atendimento e na integridade de dados sensíveis.

Governo e setor público

• Infraestruturas extensas, descentralizadas e com múltiplos fornecedores;

• Dificuldade de padronização de controles e aplicação de patches;

• Alto volume de ataques oportunistas e campanhas de ransomware.

Indústria e manufatura

• Integração entre ambientes IT e OT;

• Sistemas industriais expostos ou mal segmentados;

• Ataques que visam interrupção operacional e extorsão.

Serviços financeiros e seguros

• Ambientes mais maduros em proteção perimetral;

• Aumento de ataques focados em identidade, APIs e cadeias de fornecedores;

• Tentativas recorrentes de movimentação lateral após acesso inicial.

Padrões recorrentes entre os setores

Independentemente do segmento, os ataques seguem **roteiros semelhantes**, explorando lacunas conhecidas:

Exposição de serviços críticos à internet sem controles adequados

Uso de credenciais válidas como principal vetor de acesso

Falta de visibilidade sobre ativos, usuários e integrações

Dependência excessiva de controles preventivos, com pouca capacidade de detecção

Na prática, **o ataque raramente começa com algo sofisticado**. Ele começa onde ninguém está olhando.

Onde os controles falham com mais frequência

A recorrência dos incidentes aponta falhas estruturais que atravessam setores:

Gestão de vulnerabilidades

• Patches aplicados de forma tardia ou inexistente;

• Falta de priorização baseada em exploração real;

• Ambientes críticos tratados com a mesma régua de sistemas secundários.

Identidade e acesso

• Credenciais sem MFA em sistemas sensíveis;

• Privilégios excessivos e falta de revisão periódica;

• Ausência de correlação entre comportamento e contexto de acesso.

Segmentação e arquitetura

• Ambientes planos que facilitam movimentação lateral;

• Integrações expostas entre sistemas internos e terceiros;

• Falta de separação entre produção, testes e ambientes administrativos.

Monitoramento e resposta

• Alertas em excesso e baixa capacidade de priorização;

• Falta de correlação entre eventos técnicos e impacto real;

• Incidentes detectados tardiamente, quando o dano já ocorreu.

O ponto comum: risco conhecido, resposta insuficiente

Os incidentes analisados não revelam desconhecimento técnico. Revelam **dificuldade de execução**.

As organizações sabem onde estão os riscos, mas esbarram em:

• Falta de visibilidade consolidada;

• Processos fragmentados;

• Decisões reativas em vez de orientadas por inteligência.

É nesse espaço entre o risco conhecido e a resposta efetiva que os ataques se consolidam.

6. Da falha inicial ao impacto operacional: a cadeia de ataque na prática

Os incidentes analisados mostram que os ataques mais bem-sucedidos não começam com ações sofisticadas, mas com **falhas previsíveis que permanecem abertas por tempo demais.**

A cadeia de ataque se repete com pequenas variações, independentemente do setor ou do porte da organização.

Na maioria dos casos, o ponto inicial está associado a **exposição indevida de serviços, credenciais comprometidas ou vulnerabilidades conhecidas sem correção aplicada.**

Portas administrativas abertas, serviços de acesso remoto mal configurados, falhas em dispositivos de borda e aplicações legadas seguem sendo portas de entrada recorrentes.

Uma vez dentro do ambiente, o atacante raramente age de forma ruidosa.
O movimento inicial costuma ser discreto, com validação de acessos, enumeração do ambiente e coleta de informações que permitam entender a topologia da rede, os ativos críticos e os caminhos de privilégio.

Essa etapa passa despercebida quando não há visibilidade adequada sobre comportamento, identidade e movimentação lateral.

Na sequência, surgem padrões claros:

• Reutilização de credenciais legítimas para evitar detecção;

• Escalonamento progressivo de privilégios;

• Exploração de relações de confiança entre sistemas e fornecedores;

• Uso de ferramentas nativas do próprio ambiente para manter persistência.

Quando o ataque evolui para ransomware, vazamento de dados ou sabotagem operacional, a organização já perdeu o fator tempo.

O impacto passa a ser consequência de decisões tomadas muito antes do incidente: ausência de priorização de risco, dependência excessiva de alertas isolados e falta de correlação entre eventos.

Um ponto recorrente observado é que **o controle falha menos por ausência de tecnologia e mais por falta de contexto**. Ambientes contam com múltiplas ferramentas, mas operam sem uma visão integrada do que é crítico, do que mudou e do que realmente representa risco.

O resultado é uma defesa reativa, focada em apagar alertas, não em interromper cadeias de ataque.

O que essa cadeia revela para líderes de segurança

Para a liderança, os dados reforçam algumas lições centrais:

1. A primeira é que **segurança não pode ser tratada como um conjunto de controles estáticos**. O atacante se adapta mais rápido do que ciclos tradicionais de revisão, e ambientes que não evoluem continuamente se tornam alvos previsíveis;

2. A segunda é que **visibilidade antecede proteção**. Sem entender superfície de ataque, fluxos de acesso e dependências entre ativos, decisões estratégicas são tomadas no escuro;

3. Por fim, fica evidente que **resposta a incidentes começa antes do incidente**. A maturidade está menos na capacidade de reagir sob crise e mais na habilidade de reduzir caminhos de exploração antes que eles sejam utilizados.

Os ataques analisados mostram que não há um único ponto de falha, mas uma sucessão de pequenas lacunas não tratadas. É nessa soma de decisões, omissões e atrasos que o risco se materializa.

7. 2026 | Esteja pronto para os desafios que vêm pela frente

Os desafios enfrentados pelas organizações hoje **não desaparecem com a virada do calendário.** A complexidade dos ambientes digitais, a velocidade de exploração de vulnerabilidades e a profissionalização dos grupos de ameaça seguem avançando, independentemente do setor ou do porte da empresa.

É nesse cenário que a ISH atua.

Com três décadas de experiência, a ISH é referência nacional em cibersegurança, atuando lado a lado com empresas que não podem parar. Combinando inteligência de ameaças, operação de SOC, resposta a incidentes e visão estratégica, levamos organizações a reduzir riscos reais, proteger ativos críticos e sustentar a continuidade dos negócios.

Os desafios continuam evoluindo. **A segurança também precisa evoluir.**

USM 30 anos | heimdall security research

Fale com nossos especialistas

para tornar sua organização capaz de transformar risco em controle, visibilidade em ação e segurança em continuidade operacional.