Global Threat Report

Principais ameaças cibernéticas e como proteger sua empresa

O cenário de cibersegurança está passando por uma transformação profunda: os ataques mais eficazes deixaram de depender de invasões técnicas complexas e passaram a explorar acessos legítimos. Credenciais roubadas, sessões sequestradas, tokens válidos e integrações confiáveis tornaram-se as principais portas de entrada para ambientes corporativos. Este guia traduz os pontos críticos do relatório em ações práticas para empresas que buscam reduzir riscos, proteger dados e fortalecer sua maturidade de segurança.

146M+

Credenciais únicas comprometidas identificadas em 2025

2,2M+

Máquinas infectadas por infostealers ao longo do ano

3° lugar

Brasil entre os países mais afetados por infecções globais

61%

Das infecções concentradas na família de malware Lumma

Capítulo 1

Identidades Comprometidas: quando o atacante entra pela porta da frente

Identidades comprometidas são contas, senhas, tokens, cookies de sessão ou acessos legítimos que caem nas mãos de criminosos. Em 2025, o relatório destaca que muitos ataques ocorreram porque os criminosos conseguiram se **autenticar como usuários reais**, em vez de explorar falhas técnicas complexas. Isso torna a detecção significativamente mais difícil — o acesso pode parecer completamente normal para os sistemas de segurança existentes.

Quando uma conta válida é usada por um atacante, a empresa pode demorar para perceber o incidente. O criminoso acessa e-mails, sistemas internos, plataformas em nuvem, ambientes financeiros e dados sensíveis com a mesma aparência de um usuário legítimo. Esse tipo de ataque afeta diretamente a confidencialidade dos dados, a continuidade do negócio e a confiança dos clientes e parceiros.

⚠ Contas legítimas podem ser usadas para movimentação lateral silenciosa — sessões ativas permitem acesso sem necessidade de nova autenticação por senha.

Como se proteger

- Implemente autenticação multifator em todos os acessos críticos
- Revise acessos periodicamente, especialmente contas administrativas
- Monitore logins fora do padrão: horários incomuns, países diferentes e dispositivos desconhecidos
- Use políticas de privilégio mínimo para cada usuário
- Revogue rapidamente acessos de colaboradores desligados e fornecedores inativos

Ganhos esperados

- Redução do risco de invasões com credenciais válidas
- Mais visibilidade sobre quem acessa quais sistemas
- Melhor aderência à ISO 27001, CIS Controls v8 e LGPD

Capítulo 2

Infostealers: a indústria do roubo de credenciais

Infostealers são malwares criados para roubar informações de dispositivos infectados. Eles coletam senhas salvas, cookies de navegador, tokens de autenticação, dados de sessão e credenciais usadas em ferramentas corporativas. Em 2025, foram identificadas mais de **146 milhões de credenciais únicas comprometidas** e mais de **2,2 milhões de máquinas infectadas**. Cada máquina comprometida gerou, em média, cerca de **64 credenciais extraídas** — um número alarmante que demonstra a escala industrial dessas operações criminosas.

Vetor de Entrada Principal

Um único infostealer em um dispositivo pode expor acessos a e-mails, VPNs, plataformas SaaS, sistemas financeiros e ambientes de desenvolvimento simultaneamente — tornando-o a porta de entrada para ataques muito maiores.

Proteção de Endpoint

Use EDR ou antivírus corporativo em todos os dispositivos. Bloqueie o armazenamento de senhas em navegadores. Adote gerenciadores de senha corporativos com controle e auditoria centralizada.

Monitoramento Externo

Monitore vazamentos de credenciais em fontes externas. Aplique MFA resistente a phishing em contas críticas. Treine usuários para evitar downloads suspeitos, cracks, anexos maliciosos e páginas falsas.

Capítulo 3

Brasil entre os países mais impactados

3º

Posição Global

Brasil entre os países mais afetados por infostealers em 2025

137K

Máquinas Infectadas

Dispositivos comprometidos por infostealers no Brasil ao longo do ano

O relatório aponta que o Brasil ficou entre os países mais afetados por infecções relacionadas a infostealers em 2025, ocupando a **3ª posição global**, com mais de **137 mil máquinas infectadas** ao longo do ano. Esse dado mostra que o Brasil não é apenas alvo de ataques isolados — o país se tornou um ambiente relevante para coleta de credenciais que são reutilizadas em fraudes, acessos indevidos e ataques contra empresas.

Empresas brasileiras devem considerar que colaboradores, terceiros e prestadores podem ter credenciais expostas em mercados clandestinos sem que tenham qualquer percepção disso. O impacto não fica restrito às vítimas imediatas: credenciais brasileiras podem alimentar campanhas criminosas globais.

- Monitore credenciais corporativas expostas na deep e dark web
- Bloqueie senhas reutilizadas ou já vazadas
- Implemente políticas de troca imediata quando houver suspeita de comprometimento
- Crie campanhas internas sobre segurança em dispositivos pessoais

Capítulo 4

Stealers Predominantes: o domínio de poucas famílias de malware

O ecossistema de infostealers em 2025 foi altamente concentrado. A família **Lumma** foi responsável por mais de **61% das infecções observadas**, seguida por outras famílias como Vidar, Stealc e Redline. Quando poucas famílias dominam o cenário, os criminosos conseguem padronizar operações, distribuir campanhas em larga escala e vender dados roubados com mais eficiência — sinal claro de um cibercrime cada vez mais organizado e industrializado.

🛡️ Proteção de Endpoint

Mantenha ferramentas de proteção atualizadas. Implemente controle de execução de aplicações e restrinja privilégios locais nos dispositivos corporativos.

🔍 Inteligência de Ameaças

Use inteligência de ameaças para acompanhar famílias de malware ativas. Bloqueie indicadores conhecidos de comprometimento assim que identificados.

🚫 Controle de Software

Evite que usuários instalem softwares não autorizados. Softwares piratas, cracks e ferramentas não homologadas são vetores primários de infecção por infostealers.

Capítulo 5

Vulnerabilidades em Tecnologias Amplamente Utilizadas

Mesmo com o crescimento dos ataques baseados em identidade, a exploração de vulnerabilidades continuou altamente relevante em 2025. O relatório cita falhas críticas em tecnologias modernas e populares como **React, Next.js, React Server Components** e componentes do ecossistema **Laravel**. Essas falhas podem permitir execução remota de código, exposição de segredos, roubo de credenciais e comprometimento completo de servidores.

Frameworks populares são amplamente usados por empresas de diferentes portes. Quando uma falha crítica aparece, milhares de aplicações ficam expostas ao mesmo tempo. O problema se agrava quando a empresa não possui inventário de ativos, processo de atualização ou monitoramento contínuo de suas dependências. A janela entre a divulgação de uma vulnerabilidade e sua exploração por criminosos tem se estreitado cada vez mais.

1

Inventário

Mapeie aplicações, bibliotecas e frameworks em uso

2

Priorização

Classifique vulnerabilidades por criticidade e exposição

3

Correção

Aplique patches com prazos definidos, priorizando sistemas públicos

4

Monitoramento

Acompanhe aplicações críticas e proteja segredos e chaves de API

Capítulo 6

Supply Chain: quando a ameaça vem das dependências

Ataques de supply chain acontecem quando criminosos comprometem fornecedores, bibliotecas, pacotes, atualizações ou ferramentas usadas por uma empresa. O relatório destaca o risco em ecossistemas de desenvolvimento como o **NPM**, onde pacotes de terceiros podem executar código malicioso durante processos legítimos de instalação ou build.

Empresas modernas dependem de centenas de bibliotecas, APIs e componentes externos. Isso acelera o desenvolvimento, mas também amplia exponencialmente a superfície de ataque. Um único pacote comprometido pode afetar dezenas ou centenas de empresas ao mesmo tempo, sem que as equipes de desenvolvimento percebam imediatamente. O ataque silencioso pode persistir por semanas antes de ser detectado.

> ⓘ Gere e mantenha um SBOM (Software Bill of Materials) — lista completa de todos os componentes de software utilizados. Essa visibilidade é fundamental para reagir rapidamente a novas vulnerabilidades em dependências.

Controles Essenciais de Supply Chain

1 Análise de dependências no pipeline

Integre ferramentas de análise automática de dependências ao seu processo de CI/CD para detectar componentes maliciosos antes do deploy.

2 Revisão de permissões de tokens

Tokens usados em repositórios e pipelines devem ter escopo mínimo e ser rotacionados periodicamente.

3 Proteção de ambientes CI/CD

Ambientes de build e deploy são alvos críticos. Monitore alterações inesperadas em dependências e configurações.

Capítulo 7

Terceiros e Integrações: o risco que vem do ecossistema

Terceiros são fornecedores, parceiros, integradores, plataformas SaaS e prestadores que possuem algum tipo de acesso, conexão ou integração com a empresa. Em 2025, atacantes exploraram os elos mais frágeis da cadeia para alcançar ambientes mais protegidos. Em muitos casos, o acesso ocorreu por **chaves de API, tokens de integração, credenciais de suporte ou contas de fornecedores** com permissões excessivas.

Uma empresa pode ter excelentes controles internos e ainda assim ser significativamente impactada por um fornecedor com baixa maturidade de segurança. Quando terceiros possuem acessos críticos, eles deixam de ser apenas parceiros externos e passam a funcionar como extensão direta do ambiente corporativo — com todos os riscos que isso implica para dados, sistemas e clientes.

Mapeamento e Classificação

Mapeie todos os fornecedores com acesso a sistemas, dados ou integrações. Classifique terceiros por criticidade e revise os acessos concedidos periodicamente, garantindo que permissões reflitam a necessidade real de cada parceiro.

Requisitos Contratuais

Exija requisitos mínimos de segurança em contratos com fornecedores. A conformidade com LGPD, ISO 27001 e SOC 2 deve ser parte dos critérios de seleção e manutenção de parceiros de negócios.

Monitoramento Contínuo

Monitore credenciais de fornecedores expostas em vazamentos. Use segregação de ambientes e limitação de permissões. Implemente avaliação contínua de risco de terceiros como processo recorrente, não apenas na contratação.

Capítulo 8

Setor Financeiro Brasileiro: abuso de acessos confiáveis

Casos Relevantes em 2025

O relatório apresenta incidentes com características em comum no setor financeiro brasileiro envolvendo empresas como **C&M Software, Sinqia e FictorPay**:

- Exploração de terceiros com acesso privilegiado
- Abuso de credenciais legítimas de parceiros
- Comprometimento de integrações críticas
- Valores desviados em alguns casos chegando a centenas de milhões de reais

⊗ O setor financeiro depende de alta disponibilidade e integração entre múltiplas instituições — quando um elo é comprometido, o impacto pode atingir toda a cadeia.

Esses casos mostram que segurança financeira não depende apenas de proteger sistemas internos. Também exige governança forte sobre parceiros, credenciais, integrações e monitoramento de movimentações anômalas em tempo real. A velocidade de detecção é determinante para limitar o impacto.

Como se proteger no setor financeiro

- Monitore transações fora do padrão com alertas em tempo real
- Use segregação de funções em operações críticas
- Implemente aprovação em múltiplas etapas para movimentações sensíveis
- Revise acessos privilegiados de terceiros regularmente
- Monitore integrações financeiras continuamente
- Crie planos de resposta específicos para fraude e comprometimento de fornecedores
- Teste cenários de crise com TI, segurança, jurídico, comunicação e negócios

Capítulo 9

Ransomware e Extorsão: o valor dos dados como pressão

Ransomware é um tipo de ataque em que criminosos extorquem empresas por meio de bloqueio de sistemas, roubo de dados ou ameaça de exposição pública. Em 2025, o relatório destaca uma mudança importante: a **criptografia de arquivos deixou de ser o único foco**. Em muitos casos, os criminosos passaram a usar dados roubados, reputação e pressão operacional como instrumentos de extorsão — mesmo sem necessariamente criptografar sistemas.

Isso muda a equação da defesa. Mesmo que a empresa consiga restaurar sistemas por backup, ainda pode sofrer com exposição de dados, impacto jurídico, danos à imagem e pressão de clientes ou reguladores. A defesa contra ransomware precisa combinar prevenção, detecção, resposta e continuidade de negócios de forma integrada.

Backups Protegidos

Mantenha backups regulares, protegidos e testados com periodicidade. Isolamento dos backups é essencial.

Segmentação de Rede

Segmente redes e ambientes críticos. Monitore movimentação lateral que pode preceder um ataque de ransomware.

Resposta a Incidentes

Tenha um plano de continuidade de negócios atualizado e realize simulações periódicas de crise com todas as áreas envolvidas.

Contas Administrativas

Proteja contas administrativas com MFA forte, PAM e monitoramento de uso — elas são o principal alvo em ataques de ransomware.

Capítulo 10

Monitoramento Contínuo e Resposta Rápida

Monitoramento contínuo é a prática de acompanhar acessos, ativos, vulnerabilidades, credenciais, integrações e sinais de ataque de forma permanente. O relatório reforça que as ameaças atuais são dinâmicas: ataques podem começar por uma credencial vazada, passar por um fornecedor comprometido e terminar em fraude, vazamento ou extorsão — às vezes em questão de horas.

Empresas que dependem apenas de auditorias pontuais ou ações reativas tendem a descobrir incidentes tarde demais. A segurança moderna exige **visibilidade contínua, priorização por risco e resposta rápida**. Cada hora de detecção tardia amplia o raio de impacto de um incidente de forma exponencial. A integração entre times de TI, desenvolvimento, jurídico e negócios é fundamental para uma resposta eficaz.

- Defina e acompanhe métricas objetivas: **MTTD** (tempo médio de detecção), **MTTR** (tempo médio de resposta) e percentual de riscos críticos corrigidos dentro do SLA definido.

O que monitorar continuamente

- **Logs de autenticação e sistemas críticos**
- **Exposição de credenciais em vazamentos externos**
- **Vulnerabilidades em ativos expostos à internet**
- **Comportamentos anômalos de usuários e sistemas**
- **Integrações e tokens de terceiros ativos**

Matriz de Maturidade em Cibersegurança

Com base nos riscos identificados no relatório, avalie em qual nível sua empresa se encontra e defina prioridades claras para evoluir. Uma empresa que possui controles tradicionais mas ainda não monitora credenciais, terceiros e integrações de forma contínua estaria em torno do **Nível 2,6 de 5** — exposta a ataques modernos baseados em identidade, supply chain e abuso de terceiros.

1

Nível 1 – Inicial

Controles básicos sem padronização. Resposta reativa. Pouca visibilidade sobre acessos, terceiros e vulnerabilidades.

2

Nível 2 – Básico

Políticas de senha, antivírus, backups e alguns controles de acesso. Falhas em MFA, monitoramento contínuo e gestão de terceiros.

3

Nível 3 – Intermediário

MFA em sistemas críticos, inventário de ativos, gestão de vulnerabilidades e processos de resposta a incidentes definidos.

4

Nível 4 – Avançado

Monitoramento contínuo de identidades, endpoints, aplicações e fornecedores. Processos integrados com TI, jurídico e negócios.

5

Nível 5 – Otimizado

Segurança orientada por risco, automação e inteligência de ameaças. Antecipação de cenários. Segurança como diferencial competitivo.

Resumo Executivo e Próximos Passos

O Global Threat Report 2025 demonstra que a cibersegurança entrou em uma fase em que **identidade, contexto e confiança** tornaram-se os pontos centrais de proteção. Os ataques mais relevantes não dependem de falhas técnicas sofisticadas — eles exploram credenciais válidas, sessões roubadas, tokens, fornecedores, integrações e ambientes de desenvolvimento. Para empresas brasileiras, o alerta é ainda mais urgente: o Brasil figura entre os países mais impactados, e os incidentes no setor financeiro demonstram como terceiros e acessos confiáveis podem gerar impactos expressivos.

A principal lição é clara: proteger a empresa hoje exige entender **quais acessos existem, quem pode usá-los, quais fornecedores estão conectados, quais dados são críticos e como responder rapidamente** quando algo foge do padrão. A segurança mais eficiente combina tecnologia, processo e consciência — reduzindo riscos sem travar o negócio e ajudando a empresa a crescer com mais confiança.

01

Proteja identidades críticas

Implemente MFA em e-mails, VPNs, sistemas financeiros e painéis administrativos. Este é o passo de maior impacto imediato.

02

Monitore credenciais expostas

Ative monitoramento de vazamentos na deep e dark web. Reaja imediatamente quando uma credencial corporativa aparecer em listas comprometidas.

03

Revise acessos de terceiros

Mapeie fornecedores com acesso a sistemas, revise permissões e exija requisitos mínimos de segurança em contratos.

04

Atualize aplicações vulneráveis

Mantenha inventário de ativos e implemente gestão de patches com prazos definidos, priorizando sistemas expostos à internet.

05

Fortaleça a resposta a incidentes

Documente, teste e refine seu plano de resposta. Realize simulações com TI, segurança, jurídico, comunicação e liderança.