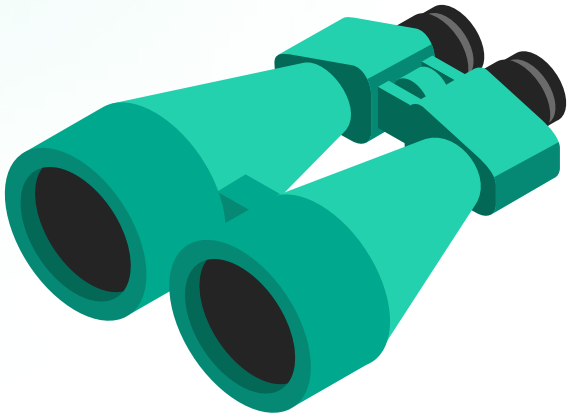
Deteção e Resposta Gerida: Relatório de Análise



kaspersky

Resumo

* Grave – incidentes muito graves relacionados com ataques iniciados por humanos, que representam 9% de todos os incidentes identificados

Recomendações

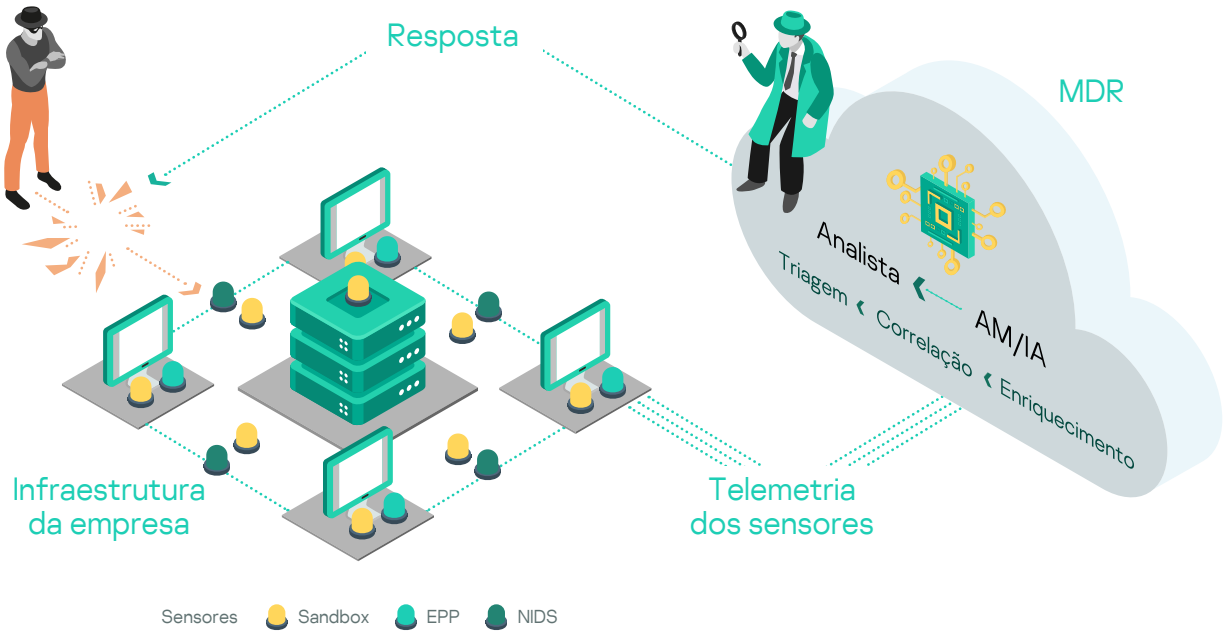
- Um terço de todos os incidentes graves foram ataques direcionados iniciados por humanos. Para os detetar na totalidade, não bastam as ferramentas automáticas, e deve ser implementada a caça manual à ameaça, em combinação com a monitorização clássica acionada por alertas[1].
- Os exercícios profissionais de equipa vermelha[2] são muito semelhantes aos ataques avançados e, por este motivo, são uma boa abordagem para avaliar a eficácia operacional de uma organização.
- Nove por cento dos incidentes muito graves reportados foram ataques de engenharia social bem-sucedidos, o que ilustra a necessidade de consciencialização da segurança dos trabalhadores[3].
- Esteja pronto para detetar ameaças em todas as táticas (fases da kill chain do ataque). Até os ataques mais complexos são compostos por etapas simples, designadas técnicas, e a deteção de uma técnica específica pode revelar o ataque completo.
- Tecnologias de deteção distintas são eficazes para técnicas de ataque distintas. Disponha de diversas tecnologias de segurança[4] para aumentar as possibilidades de deteção.

[1] www.kaspersky.com/enterprise-security/managed-detection-and-response
[2] www.kaspersky.com/enterprise-security/security-assessment
[3] www.kaspersky.com/enterprise-security/security-awareness
[4] www.kaspersky.com/enterprise-security/wiki-section/products/multi-layered-approach-to-security

Introdução

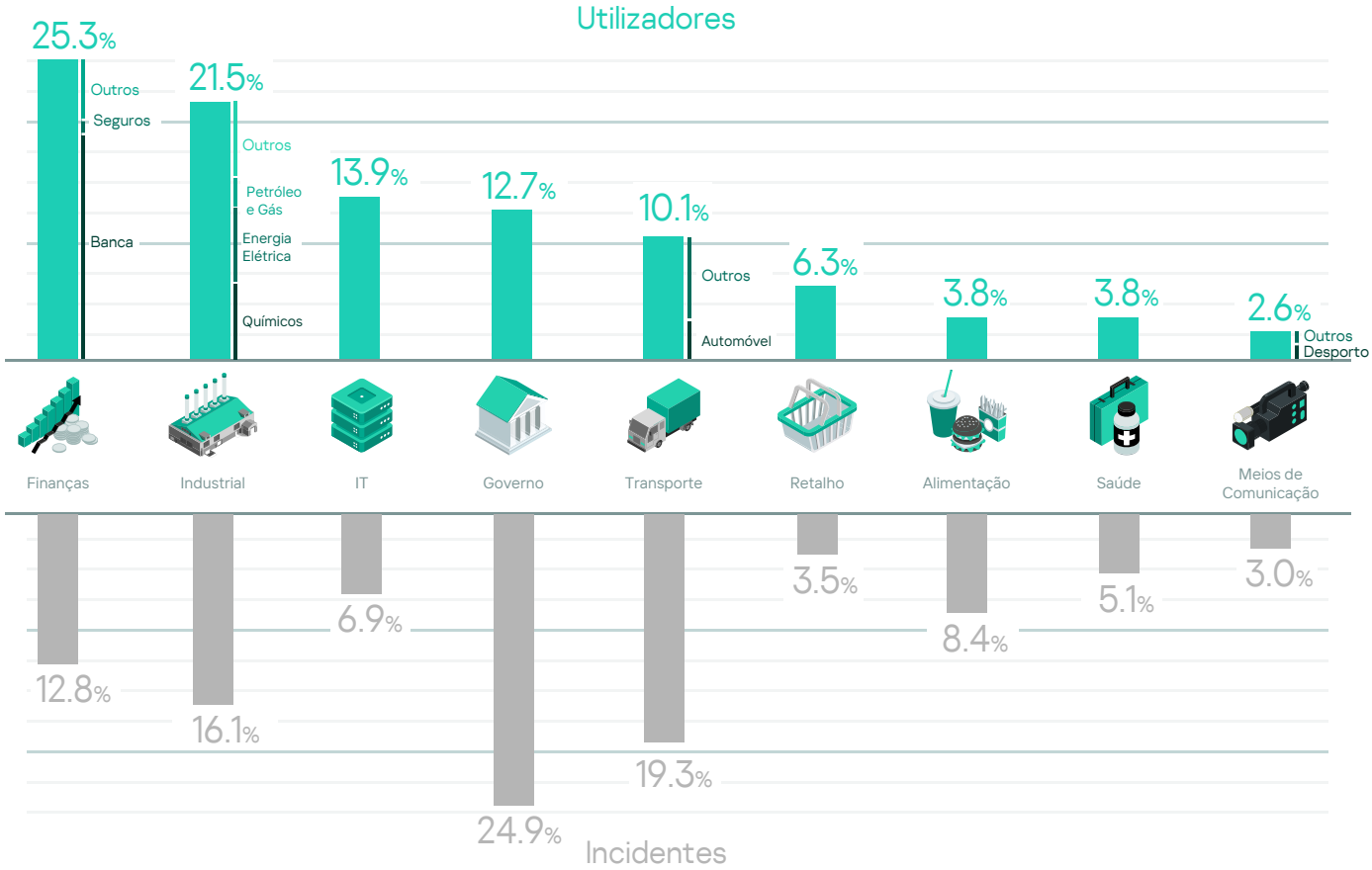
À medida que os ciberataques se tornam mais sofisticados e que as soluções de segurança requerem mais recursos para analisar a enorme quantidade de dados recolhidos todos os dias, muitas organizações sentem a necessidade de obter serviços de segurança avançados que se possam ocupar desta complexidade crescente em tempo real, 24 horas por dia, sete dias por semana.

Segundo uma estimativa feita em 2020, no Guia de Mercado dos Serviços de MDR da Gartner, «em 2025, 50 % das organizações utilizará serviços de Deteção e Resposta Gerida para as funções de monitorização, deteção e resposta a ameaças, que oferecerão recursos de contenção das ameaças».



Cobertura de serviços de MDR: indústrias e verticais

O nosso serviço de MDR é utilizado em todos os segmentos da indústria, como demonstraremos mais à frente com o número de incidentes detetados. Todos os dados apresentados no relatório são relativos ao quarto trimestre de 2020.[1]



[1] O relatório baseia-se em metadados anónimos fornecidos pelos clientes de forma voluntária desde o quarto trimestre de 2020, altura em que o serviço ficou disponível em mercados selecionados. Foi lançado globalmente no primeiro trimestre de 2021.

Rotina Diária de MDR

O serviço de MDR retira uma grande quantidade de telemetria bruta dos sensores, filtra e enriquece estes eventos, tornando-os alertas para que os caçadores de ameaças produzam incidentes que possam contribuir para tempos de resposta mais rápidos por parte dos humanos e que possam ser reutilizados noutras ferramentas de segurança.

Eventos diários de um hospedeiro

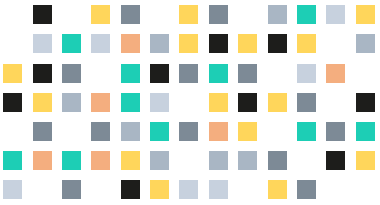
~15MIL

Este valor pode flutuar de forma significativa, dependendo da atividade do hospedeiro

Dos quais

65MIL alertas foram processados

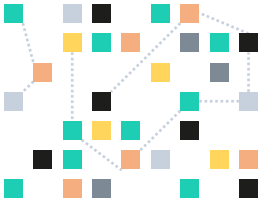
durante três meses a partir de todos os sensores



43 mil alertas enriquecidos triados manualmente e 22 mil com a ajuda da AI/ML

Resultando em

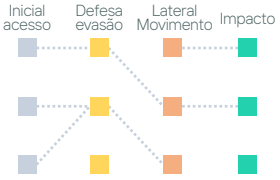
1,506 incidentes reportados aos clientes



- Alertas relacionados com os incidentes reportados: 2566
- A conversão de alertas em incidentes é de 5,9 %, ou seja, 94,1 % foram falsos positivos

92.9%

enriquecidos com ATT&CK



- 1,400 incidentes podem ser mapeados no MITRE ATT&CK
- Outros incidentes podem incluir incidentes de visibilidade ou incidentes pouco graves sem necessidade de enquadramento

Eficácia na resolução do incidente

Quantos alertas foram necessários para resolver o incidente?

1 alerta

para 80.1% dos incidentes

Comprova a eficácia geral da deteção e resolução de incidentes

2 a 4 alertas

para 15.3% dos incidentes

Mostra onde são necessários ajustes no processo de deteção e resolução de incidentes. Todos estes casos são sujeitos à criação de uma nova lógica de deteção, que permite colocá-los depois na estatística de deteção com um alerta

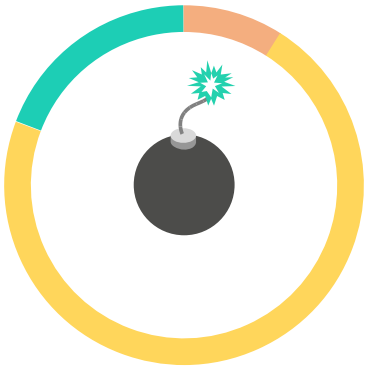
5 alertas ou mais

para 4.6% dos incidentes

Os incidentes com um grande número de alertas estão associados a casos em que não é possível uma resolução rápida ou em que esta não é eficaz:

- Descoberto um novo ataque direcionado ou uma APT (Ameaça Persistente Avançada)
- Monitorização de ataque solicitada pelo cliente, sem resposta
- Avaliações de segurança sem resposta (p. ex.: teste de penetração)

Gravidade dos incidentes



9% incidentes muito graves

Causam grande disrupção ou acesso não autorizado aos ativos do cliente abrangidos pela MDR.

Indícios identificados de um ataque direcionado ou de uma ameaça desconhecida, exigindo investigação forense digital adicional

72% incidentes de gravidade média

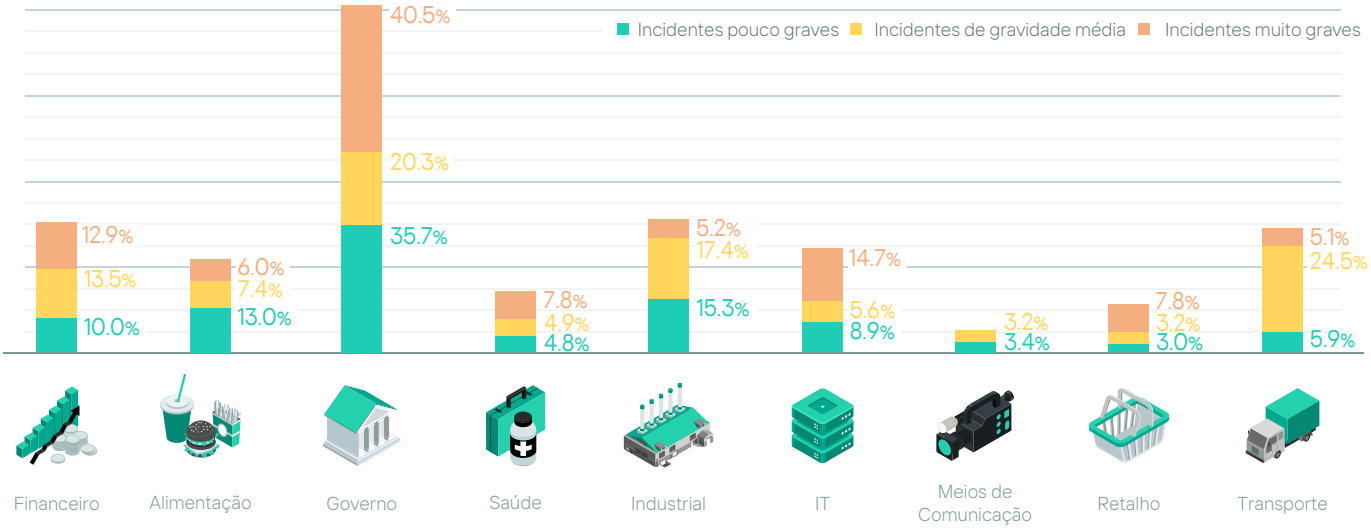
Afetam a eficácia ou o desempenho dos ativos do cliente abrangidos pela MDR ou levam a casos isolados de corrupção de dados.

19% incidentes pouco graves

Não afetam significativamente a eficácia nem o desempenho dos ativos do cliente abrangidos pela MDR, e é improvável que levem à corrupção de dados.

Software potencialmente não desejado identificado – adware, riskware, «não é vírus», etc.

Todos os dias identificámos 1 a 2 incidentes considerados importantes. Os clientes dos setores dos Meios de Comunicação e dos Transportes foram os únicos que não sofreram incidentes muito graves no 4T de 2020.
Os setores do Governo, das Finanças e de IT enfrentaram constantemente os maiores desafios neste trimestre.



Quanto tempo demora a identificar um incidente?

A vida de um alerta relacionado com um evento suspeito começa na fila de espera para uma triagem realizada por um analista humano (os alertas com base em IA / AM – 33 % – são processados em segundos e não são aqui apresentados).

Todos os alertas triados são convertidos em casos de incidentes, depois investigados por um analista e, por fim, é criado um cartão de incidente e reportado ao cliente. Partilhamos os intervalos de tempo para o processamento completo dos alertas (incluindo a espera na fila) até ao relatório de incidente.

52.6 min muito graves

Os incidentes mais delicados, que requerem um maior enriquecimento e mais tempo de caça

21.1 min de gravidade média

No que respeita ao volume, este é o tipo de gravidade dos incidentes mais comum. O tempo mais rápido mostra a eficácia da criação de modelos para os cartões dos incidentes mais comuns

30.2 min pouco graves

A prioridade mais baixa destes incidentes significa que passam a maior parte do tempo na fila para serem processados pelo analista

A natureza dos incidentes muito graves

Quais são as causas dos incidentes muito graves?

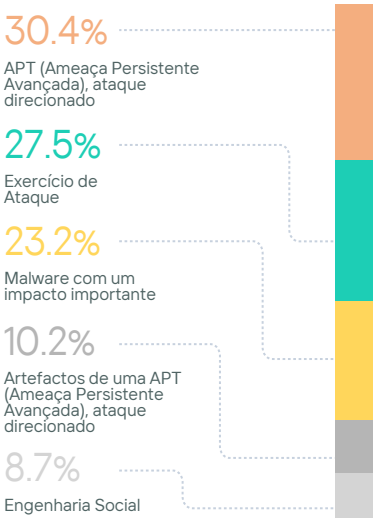
Um terço (30.4%) de todos os incidentes muito graves foram ataques direcionados ou APTs (Ameaças Persistentes Avançadas)

Cada 4º incidente muito grave estava relacionado com um exercício de ataque iniciado por um humano (teste de penetração, equipa vermelha, emulação de adversário, etc.)

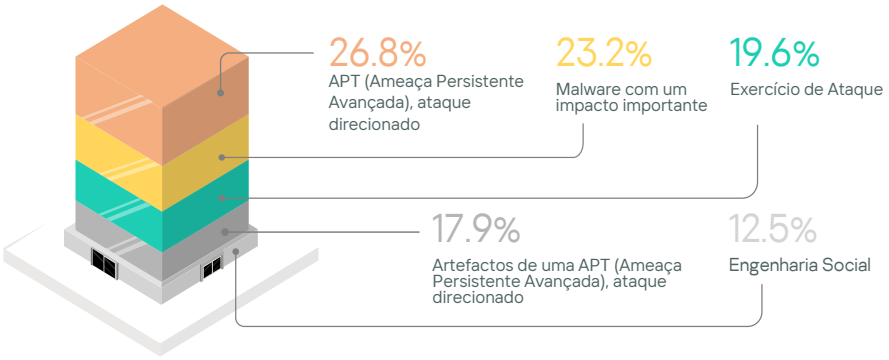
Cada 5º incidente foi um surto de malware, tal como um ransomware (p. ex. WannaCry) com um impacto significativo, mas não iniciado por um humano

10%foram incidentes não classificados com sinais claros de ataques anteriores ou de exercícios de ataque
(p. ex. dump Lsass, ficheiros kirbi, sinais de SO persistente, etc.)
Isto aconteceu principalmente com clientes novos ou com a adição de um novo hospedeiro ao campo de monitorização

9% foram acessos iniciais de engenharia social bem-sucedidos, mas com ataques evitados antes de que pudessem ser devidamente classificados



Quantas organizações experienciaram incidentes muito graves?



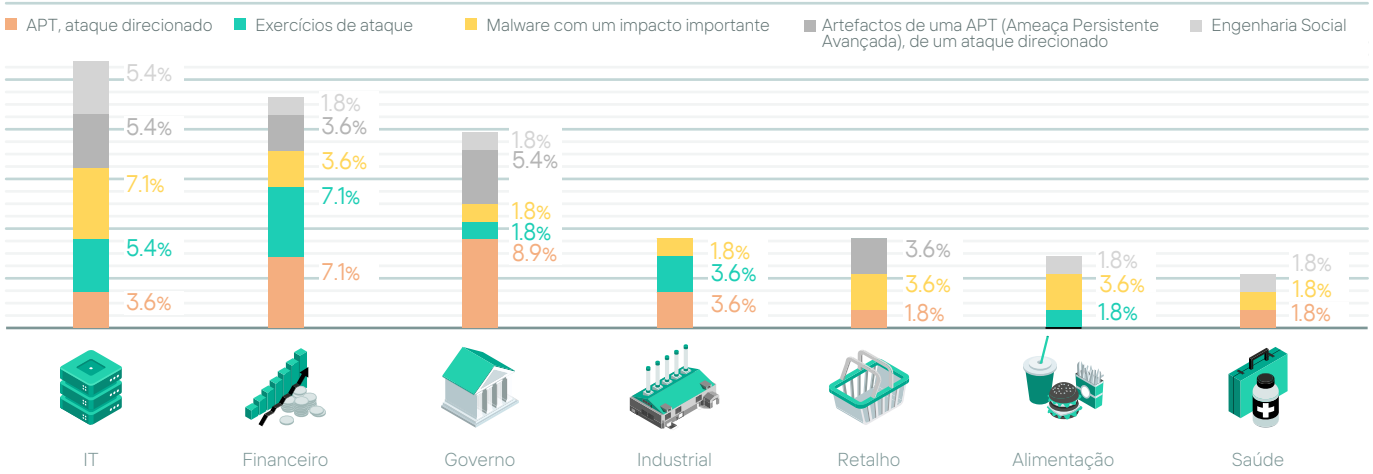
27% das organizações sofreram um ataque direcionado ou uma APT (Ameaça Persistente Avançada)

23% tornaram-se vítimas de surtos de malware com um grande impacto (tais como o ransomware)

20% dos nossos clientes realizaram exercícios de ataque

Número de organizações com incidentes graves por segmento vertical

Quase todos os setores da indústria enfrentaram todos os tipos de incidentes ao longo dos três meses do período analisado.

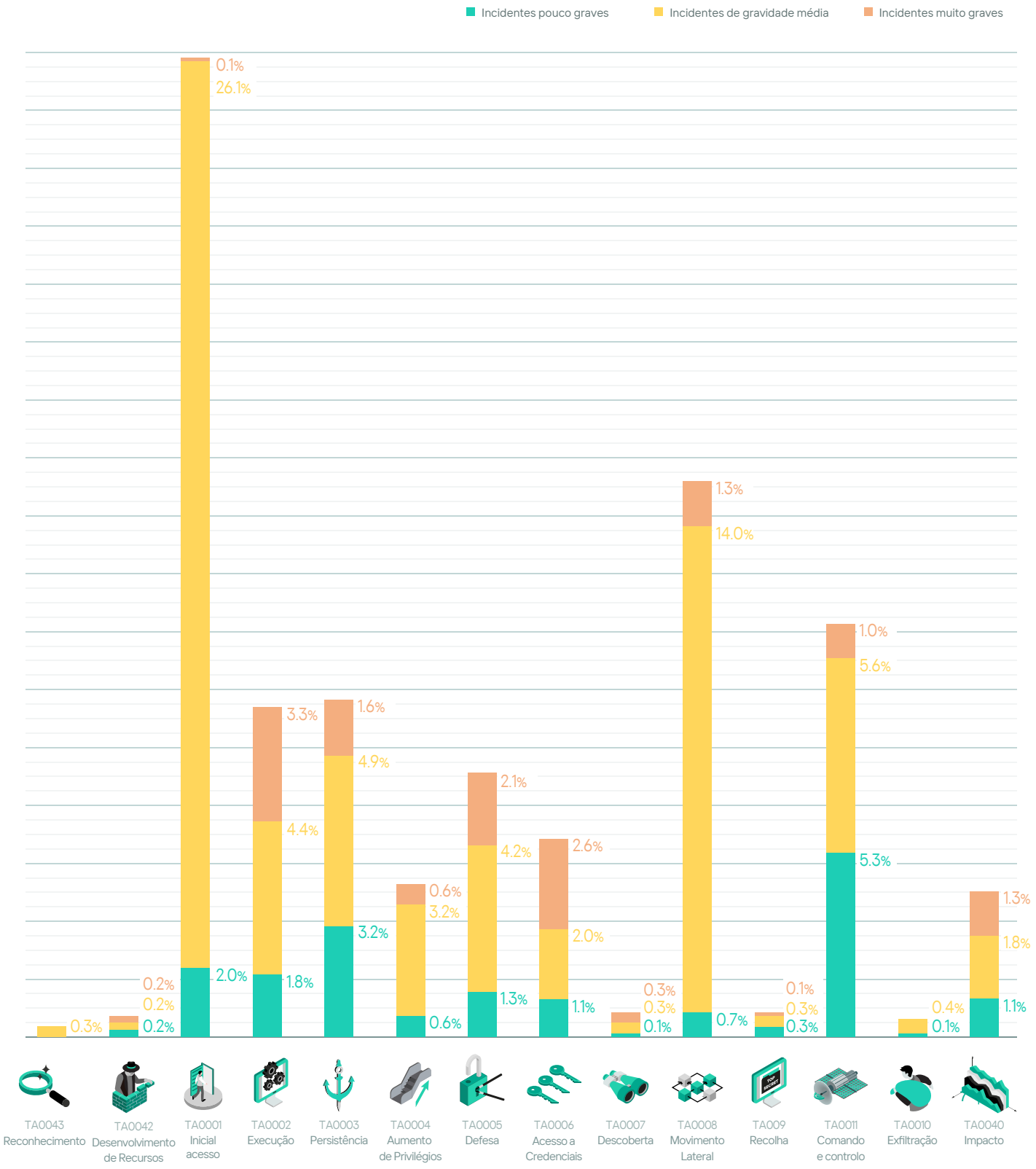


Os artefactos de uma APT (Ameaça Persistente Avançada) - sinais de ataques anteriores iniciados por humanos - são quase sempre encontrados juntamente com APT ativas. Isto prova que se uma organização recuperou de uma APT, ela é geralmente atacada de novo e, em princípio, pelo mesmo autor. Os setores alvo das APT normalmente também fazem equipas vermelhas, o que demonstra que fazem uma avaliação de risco correta.

Tecnologia de deteção e TTP adversários

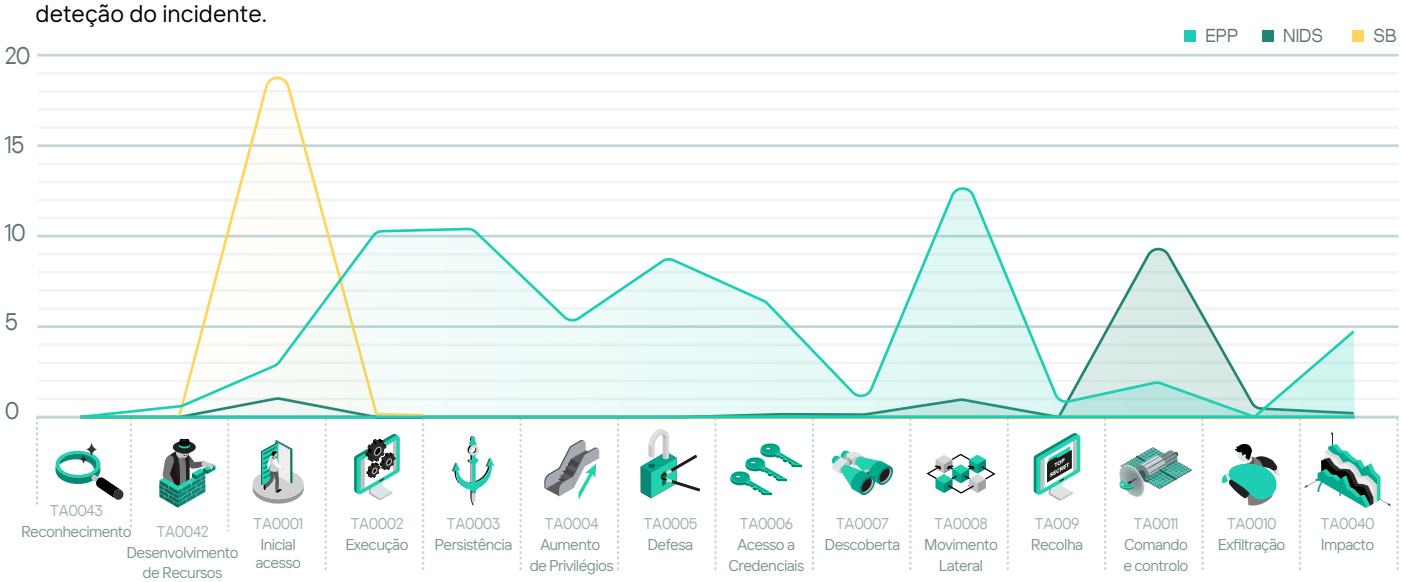
Táticas adversárias

A maioria dos incidentes foi detetada na fase de acesso inicial. As táticas de Execução, Persistência, Evasão de Defesas, Acesso a Credencial, Movimento Lateral, Comando e Controlo são as fontes de um número significativo de deteções de ataques. Foram detetados menos incidentes nas fases de Exfiltração e de Recolha por terem sido classificados e solucionados corretamente em fases precoces. Todos os casos detetados nestas últimas fases são sujeitos a uma análise minuciosa e à melhoria da lógica de deteção, de modo a aumentar as possibilidades de deteção da ameaça tão cedo quanto possível.



Táticas e tecnologia de deteção

Na MDR, recebemos telemetria de diferentes tipos de sensores (tecnologias de deteção): Plataformas de Proteção de Endpoint (EPP), Sandbox (SB) e Sistema de Deteção de Intrusões em Rede (NIDS). Os NIDS e os SB fazem parte da Plataforma Contra Ataques Direcionados da Kaspersky[1]. Os NIDS com base no hospedeiro fazem parte de uma EPP abrangente, a Kaspersky Endpoint Security for Business (Segurança Endpoint para Negócios da Kaspersky)[2]. De seguida, apresentamos as técnicas MITRE ATT&CK com melhores resultados na nossa MDR de cada sensor. O gráfico mostra a tática adversária no momento da deteção do incidente.



De seguida, apresentamos as técnicas MITRE ATT&CK com melhores resultados (as que mais contribuíram para a técnica do número de incidentes) na nossa MDR de cada sensor.

Acesso Inicial

EPP SB — T1566.001
Anexo spear phishing

SB NIDS — T1566.002
Ligação spear phishing

NIDS — T1190
Explorar uma Aplicação Aberta ao Público

NIDS — T1133
Serviços Remotos Externos

Execução

EPP SB — T1053
Tarefa / Trabalho Programados

EPP SB — T1204
Execução pelo Utilizador

EPP — T1059.001
PowerShell

EPP — T1059
Intérprete de Comandos e de Scripts

SB — T1204.001
Ligação maliciosa

Persistência

EPP SB — T1053
Tarefa / Trabalho Programados

EPP — T1547.001
Chaves de Registo do Programa / Pasta de Arranque

EPP — T1546.008
Funcionalidades de Acessibilidade

NIDS — T1133
Serviços Remotos Externos

Aumento de privilégios

EPP SB — T1053
Tarefa / Trabalho Programados

EPP — T1547.001
Chaves de Registo do Programa / Pasta de Arranque

EPP — T1546.008
Funcionalidades de Acessibilidade

EPP — T1055
Injeção de Processos

Evasão de defesas

EPP — T1036
Disfarce

EPP — T1055
Injeção de Processos

Acesso a credencial

EPP — T1003
Dumping de credencial de SO

Descoberta

NIDS — T1083
Descoberta de Ficheiros e de Diretórios

Movimento Lateral

EPP NIDS — T1210
Exploração de Serviços Remotos

EPP — T1021
Serviços Remotos

Comando e Controlo

NIDS — T1071
Protocolo de Camada de Aplicação

NIDS — T1095
Protocolo de Camada de Não Aplicação

NIDS — T1102
Serviço Web

Exfiltração

NIDS — T1048
Exfiltração sobre um Protocolo Alternativo

Impacto

EPP — T1496
Sequestro de recursos

EPP

- Evidentemente, a maior cobertura em todas as táticas
- Vocacionada para as fases de ataque mais ruidosas: entre o acesso inicial e o compromisso estabelecido que conduz ao impacto

Sandbox

- Ajuda a acelerar a triagem e fornece aos analistas um contexto adicional
- Resultados focados no prólogo e no epílogo da kill chain

NIDS

- Foco específico nas táticas de pré-impacto
- Uma adição útil para cobrir as táticas de acesso inicial

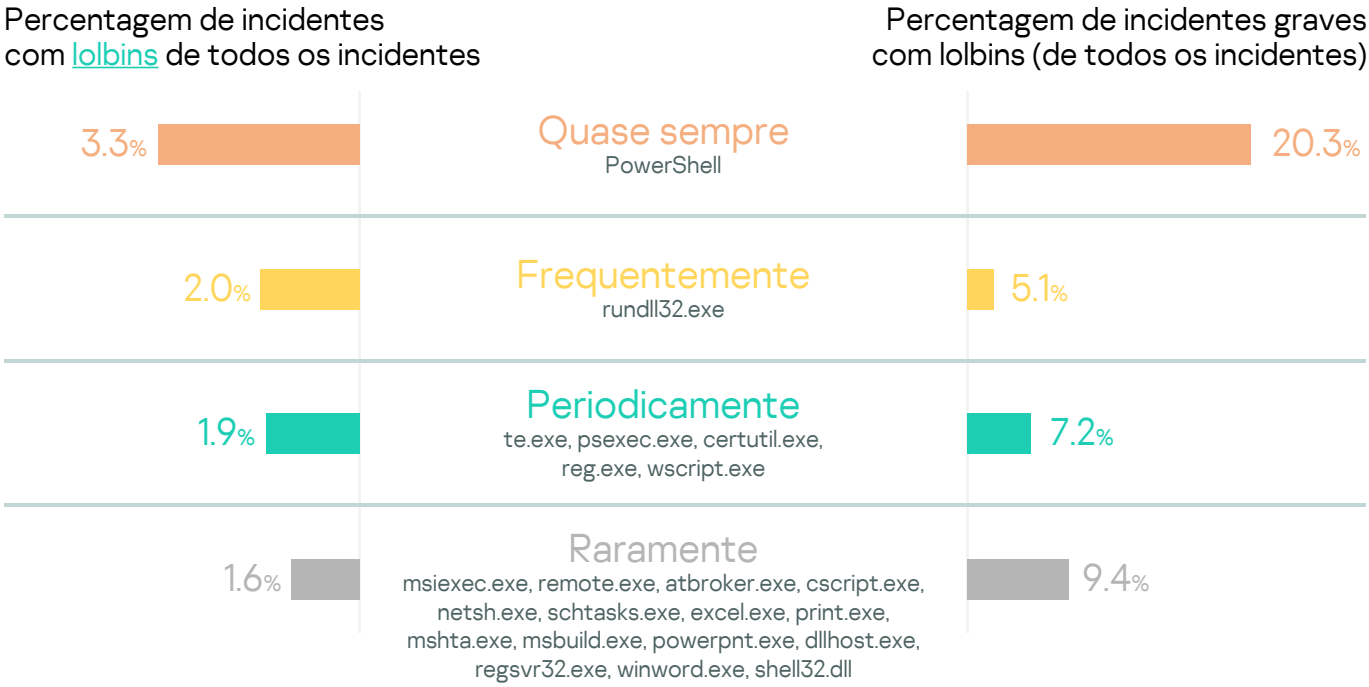
[1] KATA – www.kaspersky.com/enterprise-security/anti-targeted-attack-platform
[2] KESB – www.kaspersky.com/enterprise-security/endpoint

Técnicas adversárias

Ferramentas utilizadas em incidentes

Os criminosos tendem a usar ferramentas integradas nos SO para diminuírem o rasto do envio de instrumentos, para reduzirem os custos do desenvolvimento de conjuntos de ferramentas e, principalmente, para diluírem o próprio trabalho nas atividades legítimas, o que torna o trabalho de quem defende muito mais difícil.

Estas ferramentas denominam-se "living-off-the-land binaries" e podem ser analisadas no site do projeto "lolbins". A principal conclusão não surpreende. Apesar de a Microsoft ter feito esforços impressionantes para melhorar a segurança e o controlo do PowerShell, continua claramente a ser a ferramenta mais utilizada pelos atores adversários.



Mapeamento de incidentes com o MITRE ATT&CK

Uma boa forma de avaliar a lógica de deteção da MITRE é através da sua eficácia. Apresenta a percentagem de todos os incidentes reportados que foi detetada pelas regras de caça à ameaça baseadas em técnicas específicas.

33%

T1566: Phishing

Demonstra tanto a eficácia da MDR relativamente a esta técnica desde a fase de Acesso inicial, quanto a popularidade da técnica entre os atacantes.

16.5%

T1210: Exploração de Serviços Remotos

Está associada a tentativas de exploração remota (p. ex. «EternalBlue»).

10.6%

T1071: Protocolo de Camada de Aplicação

Protocolos de escolha de comunicações com uma infraestrutura C&C. Para comparação, T1095: o Protocolo de Camada de Não Aplicação foi encontrado apenas em 3,79 % dos incidentes.

5.3%

T1021: Serviços Remotos

É amplamente utilizado por atacantes para movimento lateral (T1021.002: SMB/Windows Admin Shares e T1021.001: Remote Desktop Protocol).

4.4%

T1036: Disfarce

Frequentemente, a utilização de Funcionalidades de Acessibilidade ocultas, quando ações como sethc.exe, narrator.exe, magnify.exe, utilman.exe etc. são substituídas por cmd.exe e, segundo as estatísticas, muito raramente relacionadas com incidentes muito graves. Menos casos estão associados à renomeação de ficheiros maliciosos para parecerem ferramentas do sistema ou à criação de tarefas programadas que pareçam legítimas – estas normalmente estão associadas a incidentes muito graves ou de gravidade média.

3.3%

T1204: Execução pelo Utilizador

Engenharia social bem-sucedida relacionada com anexos de phishing ou com tentativas de execução de software descarregado da Internet.

6.6%

T1059: Intérprete de Comandos e de Scripts

Acima de tudo, consiste em T1059.001: PowerShell e T1059.004: Unix Shell.

>0% >5% >10% >20%

TA0043: Reconhecimento	TA0042: Desenvolvimento de Recursos	TA0001: Acesso Inicial	TA0002: Execução	TA0003: Persistência	TA0004: Aumento de Privilégios	TA0005: Evasão de Defesas
T1595: Varredura Ativa	T1587: Desenvolver Capacidades	T1190: Explorar uma Aplicação Aberta ao Público	T1059: Intérprete de Comandos e de Scripts	T1098: Manipulação de Contas	T1548: Abusar do Mecanismo de Controlo dos Aumentos	T1140: Desofuscar / Descodificar Ficheiros ou Informação
	T1588: Obter Capacidades	T1133: Serviços Remotos Externos	T1203: Exploração para Execução pelo Cliente	T1547: Execução Automática de Atualizações ou de Logon	T1134: Manipulação dos Códigos de Acesso	T1564: Esconder Artefactos
		T1566: Phishing	T1559: Comunicação Interprocesso	T1037: Scripts de Iniciação de Atualizações ou de Logon	T1546: Execução Acionada por um Evento	T1562: Comprometer as Defesas
		T1091: Reprodução por Meios Removíveis	T1053: Tarefa / Trabalho Programados	T1554: Comprometer o Binário do Software do Cliente	T1068: Exploração para Aumento dos Privilégios	T1070: Remoção de Indicador no Hospedeiro
		T1078: Contas Válidas	T1569: Serviços do Sistema	T1136: Criar Conta	T1574: Sequestrar o Fluxo de Execução	T1036: Disfarce
			T1204: Execução pelo Utilizador	T1505: Componente de Software do Servidor	T1055: Injeção de Processo	T1112: Alterar o Registo
			T1047: Instrumentação da Gestão do Windows			T1027: Ficheiros ou Informação Ofuscados
						T1542: Atualização Pré-SO
						T1218: Execução de Proxy ! Binário Assinado

TA0006: Acesso a Credencial	TA0007: Descoberta	TA0008: Movimento Lateral	TA0009: Recolha	TA0011: Comando e Controlo	TA0010: Exfiltração	TA0040: Impacto
T1110: Força Bruta	T1087: Descoberta de Conta	T1210: Exploração de Serviços Remotos	T1123: Captação de Áudio	T1071: Protocolo de Camada de Aplicação	T1048: Exfiltração sobre um Protocolo Alternativo	T1485: Destruição de Dados
T1555: Credenciais de Armazéns de Palavras-Passe	T1482: Descoberta de Domínios de Confiança	T1570: Transferência de Movimento Lateral	T1005: Dados do Sistema Local	T1001: Ofuscação de Dados		T1486: Dados Encriptados para Impacto
T1556: Alterar o Processo de Autenticação	T1083: Descoberta de Ficheiros e de Diretórios	T1021: Serviços Remotos	T1056: Captação de Input	T1105: Transferência de Ferramentas de Entrada		T1565: Manipulação de Dados
T1003: Dumping de credencial de SO	T1046: Varredura de Serviços da Rede	T1550: Utilizar Material de Autenticação Alternativo		T1095: Protocolo de Camada de Não Aplicação		T1561: Limpar o Disco
T1552: Credenciais Não Seguras	T1135: Descoberta de Partilha de Rede			T1090: Proxy		T1496: Sequestro de Recursos
	T1069: Descoberta de Grupos de Permissões			T1219: Software de Acesso Remoto		
	T1012: Registo de Pesquisa			T1102: Serviço Web		
	T1018: Descoberta de Sistema Remoto					
	T1033: Descoberta de Proprietário / Utilizador do Sistema					
	T1497: Virtualização / Evasão do Sandbox					