

kaspersky

GReAT & CTI: O Raio-X das ameaças Nacionais

Como o cibercrime brasileiro evoluiu para ameaça global
E como a **Inteligência de Ameaças da Kaspersky** lidera a defesa.



SPEAKER – Threat Intelligence

Carlos Nascimento

Solutions Manager de Threat Intel.
Une base técnica em operações de
Cibersegurança ao apoio estratégico e
executivo. Foca em maturidade digital,
traduzindo inteligência de ameaças em
resiliência, continuidade de negócios e
proteção contra riscos geopolíticos.

SSM - Threat Intel – Brazil
carlos.nascimento@kaspersky.com



Kaspersky GReAT & CTI

Gerenciando a Superfície de
Ataque e Riscos com
Kaspersky Threat Intelligence



01 Conheça o GReAT



02 Cenários de Ameaças
Brasileiro



03 Como Threat Intel
pode ajudar?

Meet GReAT Kaspersky Global

Research & Analysis Team



Our experts
are globally
renowned

~5,500
highly qualified specialists

50%
of our employees
are R&D

50+
members in our group of
elite world-leading
security experts

5
Unique Centers of
Expertise

Our unique team of experts work together across **5 Centers of Expertise**, applying specialized knowledge and skills to tackle the most sophisticated and dangerous cyberthreats. This approach strengthens our state-of-the-art protection technologies and ensures that the quality of our products and solutions is unsurpassed.

Just look at the numbers!



500,000

unique malicious objects discovered
by Kaspersky every single day

>900

APT groups and operations

>2 billion

attacks launched from online
resources around the world
blocked by us

38.6%

of ICS computers globally have
been attacked

1 billion

Devices protected
by Kaspersky to date

Threat evolution



GReAT in numbers



2008



Established in 2008

900



Monitors over 900
operations and groups

10 years



Providing APT intelligence to
customers and partners for
10 years

90%



90% of monitored activities
relate to cyberespionage

120+



GReAT publishes an average
of 120+ private reports
every year, with over 190
published in 2023

20+



GReAT experts working
globally in 20+ countries —
Europe, Russia, Latin America,
Asia, the Middle East

* Based on the data up to 31.12.2024



GReAT: Who we are and what we do

Rockstar researchers

- We research the most complex, sophisticated threats and attacks
- We discover zero-day vulnerabilities and share our findings with vendors so they can be fixed
- We track the activities of the threat landscape's most dangerous actors

Keen investigators

- We investigate the most complex and impactful incidents on a global scale
- We collaborate with law enforcement agencies around the world, helping make the cyberspace safer



GReAT: Who we are and what we do

Ingenious inventors

- We develop unique tools to support Kaspersky's threat research
- We created and now maintain an infrastructure to keep track of the assets of malicious actors on the internet

Educators and presenters

- We teach security researchers our unique techniques and approaches and help develop training programs
- We prepare and publish groundbreaking reports about high-level cybercrime
- We deliver speeches and share our discoveries with the global community of ITSec specialists

Advanced **persistent threat** landscape in 2025

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the **discovery and analysis** of the most **advanced cyberthreats**. According to their data, in 2025 the top targets for advanced persistent threats (APT) were **governments**, and the most significant threat actor was [Lazarus](#).

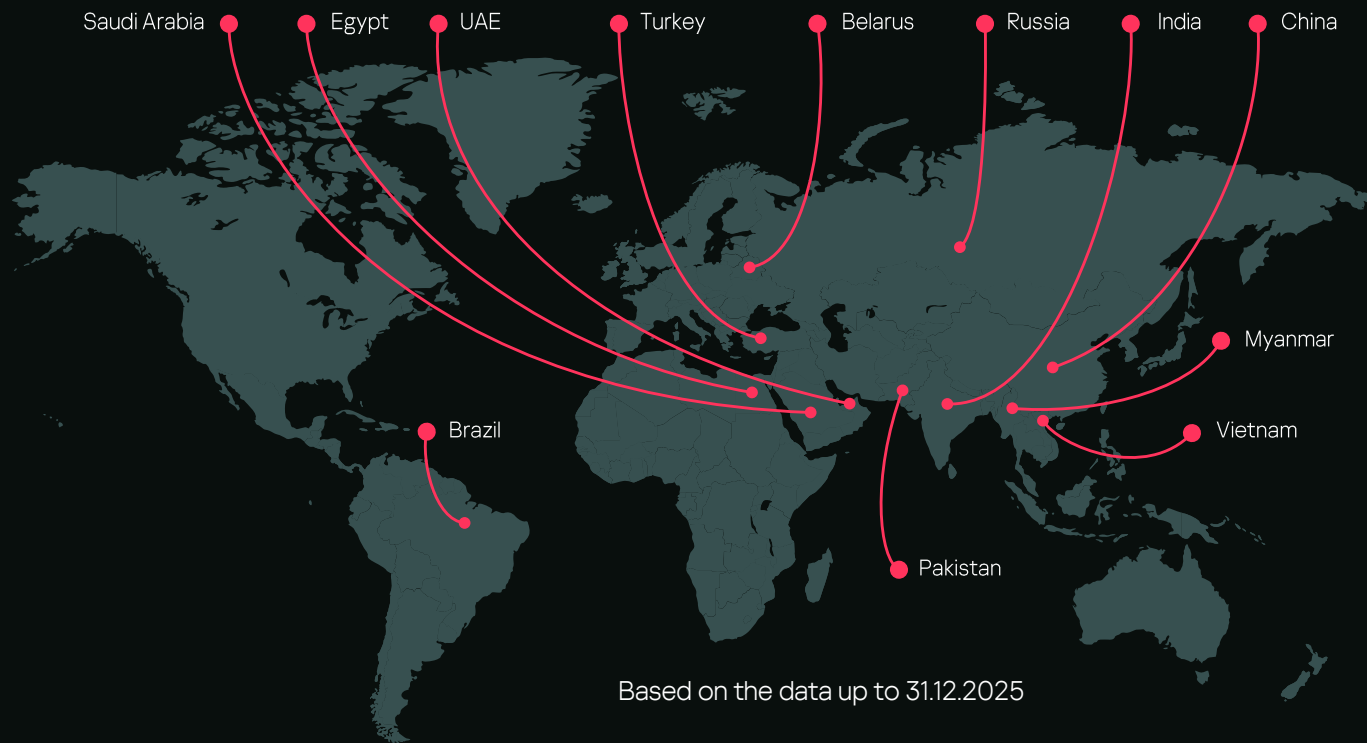
Top 12 targeted countries and territories

Top 10 targeted industries

- | | |
|--|--|
|  Government |  Telecom |
|  Technology |  Education |
|  Financial Institutions |  Transportation |
|  Manufacturing |  Construction |
|  Defense |  Energy |

Top 10 significant actors

- | | |
|---|---|
|  Lazarus |  GELSEMIUM |
|  HoneyMyte |  Iron Husky |
|  GOFEE |  Blue Noroff |
|  SideWinder |  BlindEagle |
|  Mysterious Elephant |  Turla |



Based on the data up to 31.12.2025

In-the-wild zero-days caught and reported by Kaspersky

32 zero-days vulnerabilities



CVE-2014-4077	CVE-2019-0859
CVE-2015-2360	CVE-2019-1458
CVE-2016-0034	CVE-2020-0986
CVE-2016-0165	CVE-2020-1380
CVE-2016-3393	CVE-2021-28310
CVE-2018-8174	CVE-2021-31955
CVE-2018-8453	CVE-2021-31956
CVE-2018-8589	CVE-2021-40449
CVE-2018-8611	CVE-2023-28252
CVE-2019-0797	CVE-2024-30051



CVE-2014-0497
CVE-2014-0515
CVE-2014-0546
CVE-2016-4171
CVE-2017-11292



CVE-2023-32434
CVE-2023-32435
CVE-2023-38606
CVE-2023-41990



CVE-2019-13720
CVE-2024-4947

CVE-2025-2783

New

O Brasil e seu cenário de Ameaças!



MALWARE NA AMÉRICA LATINA

726 milhões

ataques bloqueados



408m



108m



43m

- 1.9 milhões por dia
- 1.382 por minuto
- 23 por segundo
- 1.1 malware por pessoa

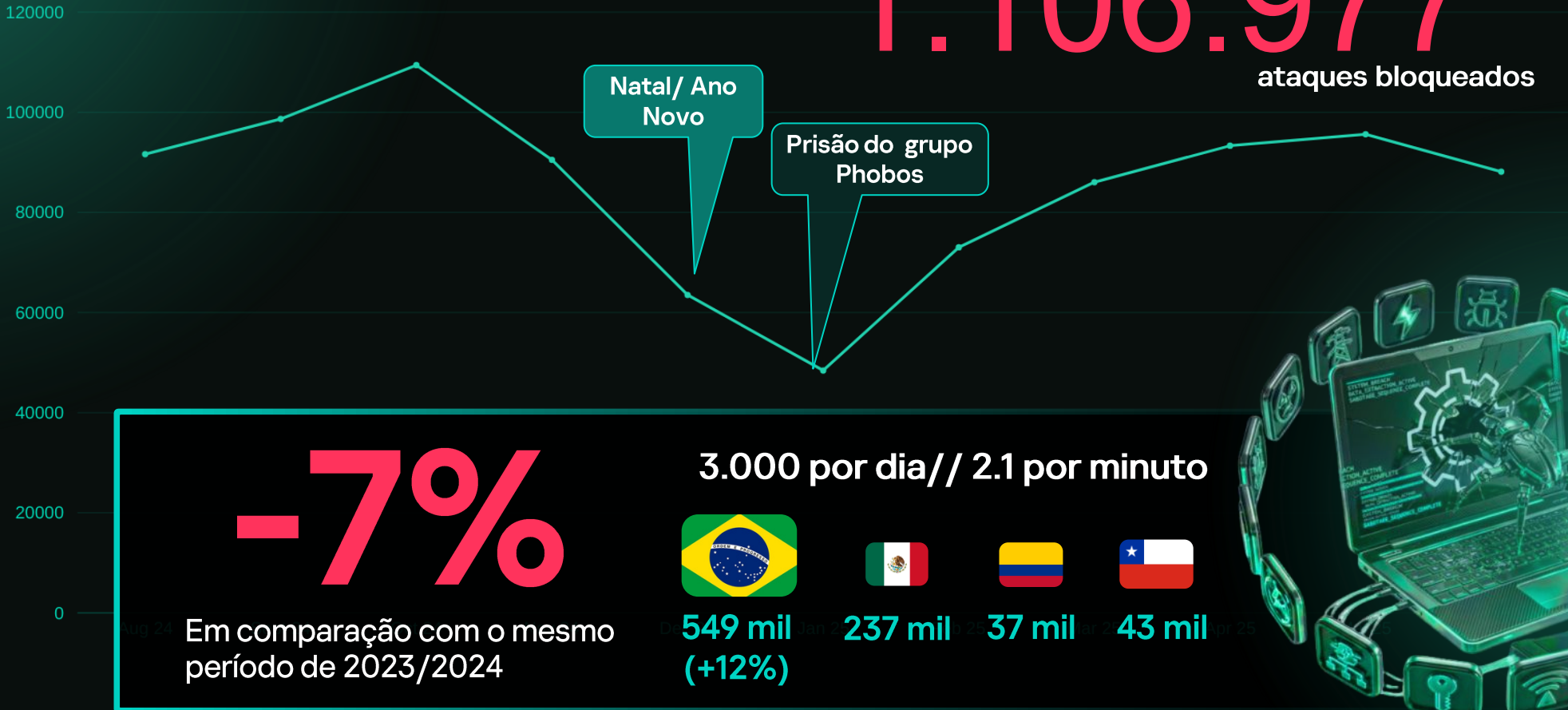
América Latina é a região do mundo com o aumento mais rápido de **ciberincidentes** divulgados, registrando uma taxa de crescimento anual de **25%** entre 2014 e 2025**

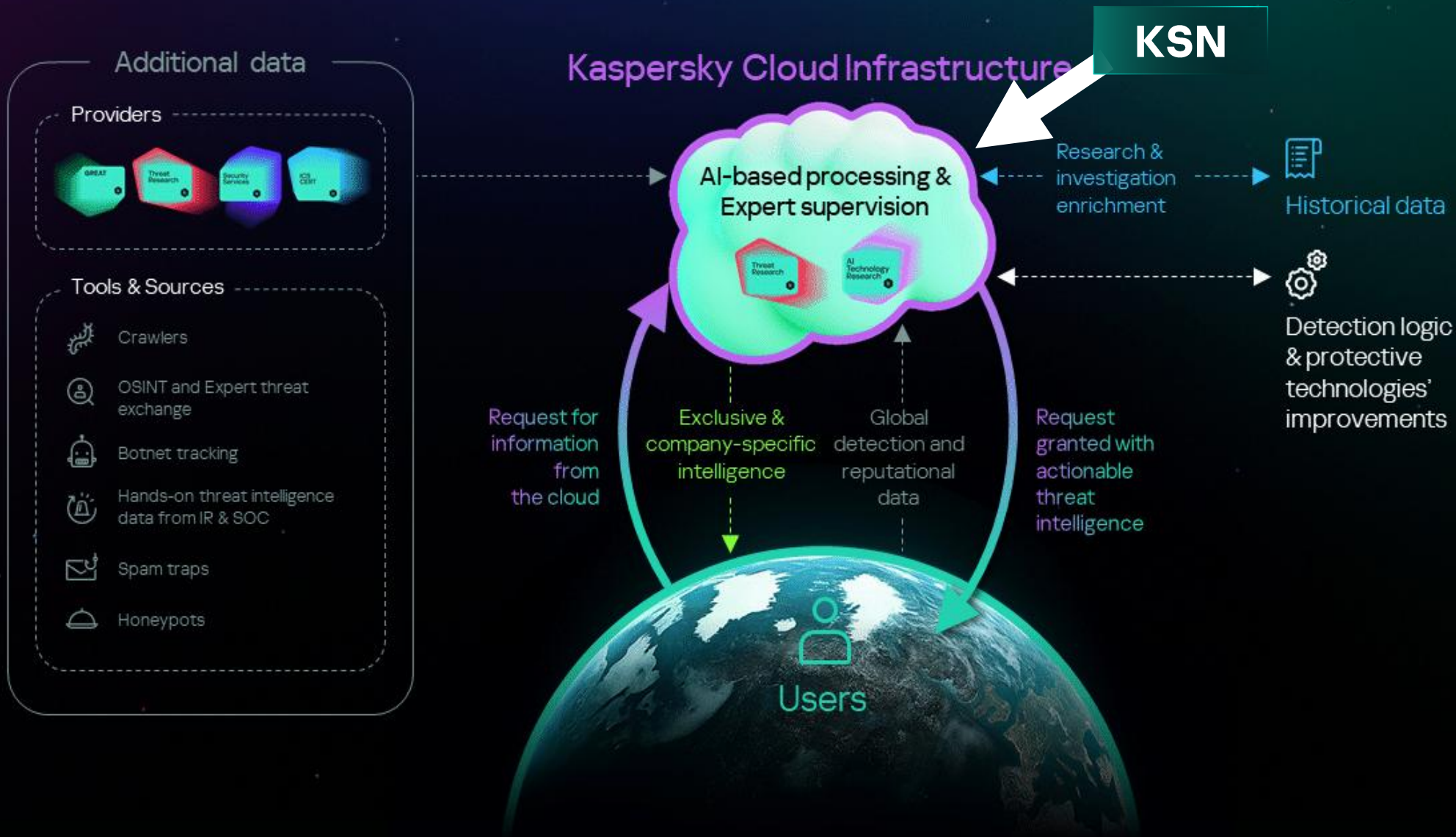
* Dados: CEPAL.org
** Dados Banco Mundial

RANSOMWARE NA AMÉRICA LATINA

1.106.977

ataques bloqueados

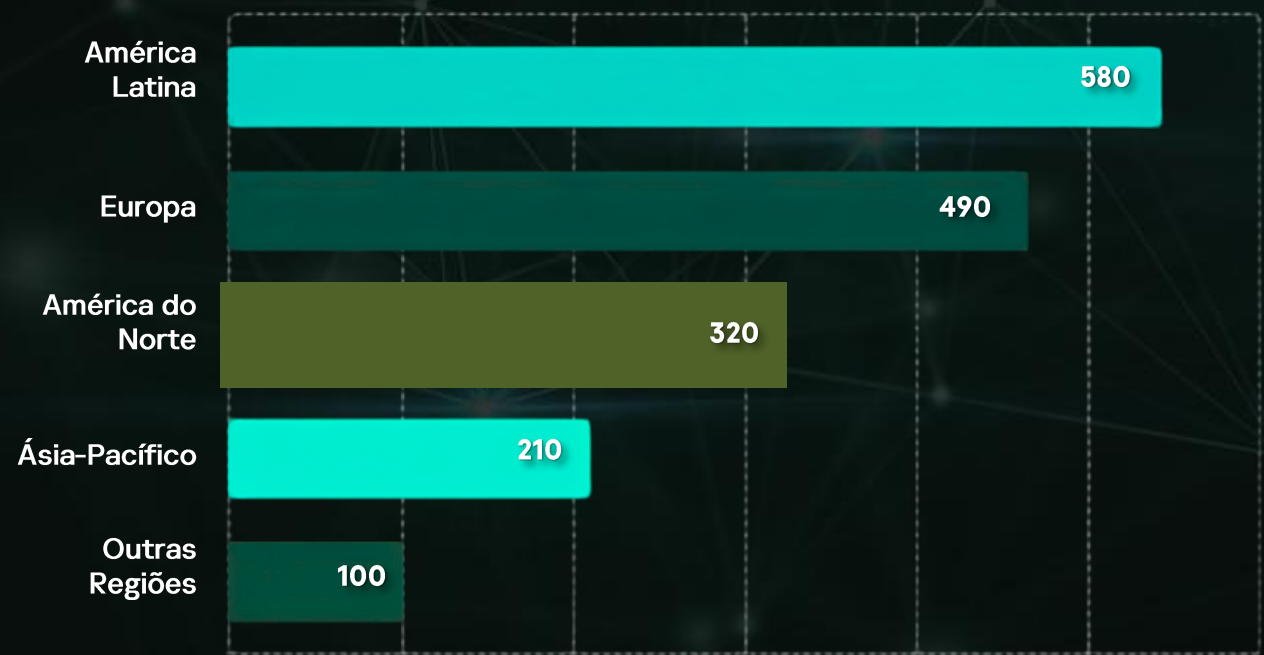




O Brasil como Exportador Global de Ameaças

O underground criminoso brasileiro abriga alguns dos perpetradores de cibercrime mais ativos e criativos do mundo.

REGIÃO



Bancos Atacados



1.700

Bancos Atacados
Pelo Grandoreiro em 2024



45

Países Afetados
Em todos os continentes



276

Carteiras Crypto
Comprometidas globalmente

BeatBanker: um trojan de dupla função para Android



The image shows a screenshot of an Android emulator. On the left, there's a sidebar with a character icon and some stats. The main area displays a post titled "[BTMOB RAT] Full Collection" with a thread URL and forum name. Below this, there's a section titled "Persistência" (Persistence) which explains the functionality of the `KeepAliveServiceMediaPlayer` component. It states that this component ensures continuous operation by using `MediaPlayer` to play a small, continuous audio file, preventing the system from suspending or closing the process. A code snippet is provided, showing the `RunPlayBack()` method. The audio file is identified as `output8.mp3`, which is 5 seconds long and contains some Chinese words. At the bottom, there's a status bar showing "BTMOB Servers" and a message: "Proof: BTMOB Collection Size - 8.3GB I'll be active again soon!".

Persistência

O componente `KeepAliveServiceMediaPlayer` garante operação contínua iniciando reprodução ininterrupta por meio do `MediaPlayer`. Ele usa uma notificação para manter o serviço ativo em primeiro plano e carrega um arquivo de áudio pequeno e contínuo. Essa atividade constante impede que o sistema suspenda ou encerre o processo por inatividade.

```
public final void RunPlayBack() throws IllegalStateException {
    Log.d("KeepAliveServiceMediaPlayer", "music begins looping...");
    MediaPlayer mediaPlayerCreate = MediaPlayer.create(this, Uri.fromFile(EZFuH5PjyhYuKSHhR2.iMtl1wscbbkK4QUI32(this, "output8.mp3")));
    EZFuH5PjyhYuKSHhR2 = mediaPlayerCreate;
    mediaPlayerCreate.setLooping(true);
    EZFuH5PjyhYuKSHhR2.start();
}
```

O áudio identificado `output8.mp3` tem 5 segundos de duração, é reproduzido de forma contínua e contém algumas palavras em chinês.

Proof: BTMOB Collection
Size - 8.3GB
I'll be active again soon!

Como o BeatBanker se infiltra

<https://SecureList.com.br>

A Anatomia da Invasão

Do Infostealer ao Acesso Inicial

● Infostealer

Coleta credenciais
(Lumma, Stealc)



● Broker

Vende acesso comprometido
no underground



● Atacante

Penetra rede corporativa
ou cadeia de suprimentos



O ataque de hoje começou muito antes, quando uma credencial de VPN foi vendida por alguns dólares no underground.

Fornecedores comprometidos tornam-se porta de entrada para toda a cadeia de suprimentos. Um único elo fraco basta para derrubar operações inteiras.

Engenharia Social com Sotaque Brasileiro

Os atacantes conhecem a rotina financeira do seu departamento fiscal **melhor** que muitos sistemas de auditoria. Filtros globais de e-mail simplesmente não reconhecem o contexto local.



PIX

Transferências urgentes falsificadas



Imposto de Renda

Intimações e restituições falsas



Nota Fiscal Eletrônica

Documentos tributários adulterados



Intimações Judiciais

Urgência fabricada para clicar

Caso GReAT — Desmascarando a Tetrade

✓ Guildma

C2 oculto em páginas do Facebook e YouTube com comunicação criptografada



✓ Grandoreiro

Trojan bancário com alcance global – 45 países, 1.700 bancos em 2024

✓ Melcoz

Derivado do Alina RAT, especializado em interceptar sessões bancárias

✓ Jora

Família mais recente com recursos avançados de bypass de autenticação

O Kaspersky GReAT foi o **primeiro a identificar** que essas quatro famílias operavam sob a mesma arquitetura de C2. Uma descoberta original que **reconfigurou o entendimento global da ameaça**.

O Modelo de Exportação da Fraude

Da Fraude Local ao Crime Organizado

Global

Os bancos nacionais incorporaram overlay, bypass de MFA e criptografia complexa, transformando operações artesanais em franquias criminosas internacionais.



Fase 1 -

Desenvolvimento local

(trojans bancários nacionais com overlay e bypass de MFA)



Fase 2 -

Infraestrutura oculta

(C2 em Facebook e YouTube com comunicação criptografada, desde 2015 pelo Guildma)



Fase 3 -

Exportação global

(abertura de filiais no exterior, adaptação para atacar bancos europeus e latino-americanos)



O Guildma (ativo desde 2015) esconde comunicação com seu servidor de controle em formato criptografado dentro de páginas do Facebook e YouTube. Isso torna a detecção por ferramentas convencionais quase impossível.

Bastidores da Investigação

Como o GReAT Opera



Engenharia Reversa

Dissecação de amostras de malware para mapear TTPs, infraestrutura e autoria dos grupos criminosos.



Inteligência OSINT & Dark Web

Monitoramento de fóruns fechados, marketplaces do underground e canais Telegram criminosos.

Telemetria KSN

Rede global Kaspersky Security Network detecta padrões de ataque em tempo real em milhões de endpoints.



Cooperação Global

Parceria com INTERPOL e agências de lei enforcement compartilhando TTPs e IoCs — resultando em prisões em múltiplos países.



MAVERICK

Ataques à cadeia de suprimentos e ao sistema financeiro!

Maverick: Novo Troian bancário distribuído via WhatsApp

The image shows a Windows File Explorer window displaying the resources of the file `meshiwupezho.exe` (version 1.0.0.0). The left pane shows the file structure, with the `Resources` folder expanded. The right pane shows the list of resources, including various Costura (Costura) files and the `meshiwupezho.packages.Selenium.WebDriver_4_35_0.runtime` file, which is highlighted with a red box. Below the list, the `Zap` resource is also highlighted with a red box and a red circle containing the number 1.

On the right side of the image, a code snippet is shown, likely from a C# source file, illustrating a method `IsInBrazil()` that checks for Brazilian locale, region, and date format using `AntiAnalysisBrazil` classes. The code is as follows:

```
151 // Token: 0x06000041 RID: 65 RVA: 0x00003B80 File Offset: 0x00001D80
152 private static void CausalityTraceLevelDefaultLevel(ref int A_0, ref int A_1, ref int A_2,
153
public static bool IsInBrazil()
{
    int num = 0;
    if (AntiAnalysisBrazil.IsValidBrazilianTimezone())
    {
        num++;
    }
    if (AntiAnalysisBrazil.IsBrazilianLocale())
    {
        num++;
    }
    if (AntiAnalysisBrazil.IsBrazilianRegion())
    {
        num++;
    }
    if (AntiAnalysisBrazil.IsBrazilianDateFormat())
    {
        num++;
    }
    return num >= 2;
}
```

<https://SecureList.com.br>

Malware Sofisticado que vive na memória!

Um ataque de man-in-the-middle

LNK / EXI

```

$cs = Get-WmiObject -Class Win32_Computer
$os = Get-WmiObject -Class Win32_Operating
$sav = Get-WmiObject -Namespace "root\Security"
$antivirusName = if ($sav) { $sav.DisplayNa
$info = @{
    "1" = "kslp4ic5hc7jr8q46g6vt26amt"
    "2" = $os.OSArchitecture.Substring(0
    "10" = [Convert]::ToBase64String(
        [Text.Encoding]::Default.Get
        "$($cs.UserName):" +
        "$($cs.Sys if ($byteCou
        "$($cs.Capt {
        "$($os.v6 = CreateProcessA
        "$ant if ( v6 )
        {
            if ( NtAllocateVi
            && NtWriteVirtu
    )
}

```

```
v6 = CreateProcessA
if ( v6 )
{
    if ( NtAllocateVirtualMemory(
        && NtWriteVirtualMemory(
            {
                memset(v11, 0,
                v11[0] = 1;
                v11[1] = GetCurrentProcessId();
                if ( NtWriteVirtualMemory(
                    v5 = (int)NtCreateProcess(
                }
            }
        )
    )
}
if ( Handle )
    NtClose(Handle);
```

```
$shellcode += "\x00", "\x00"
$shellcode += 0xB8
$shellcode += ConvertToByteArray $exitThreadPtr
$shellcode += 0xFF, 0xD0
```

<https://SecureList.com.br>



CTI – Threat Intel

O Ponto Cego das Defesas Tradicionais



CTI – Threat Intel

O Ponto Cego das Defesas Tradicionais

Ter ferramenta de segurança sem inteligência local é como colocar um guarda que não fala a língua do invasor.



Assinaturas Genéricas

Não reconhecem variantes de Grandoreiro ou Guildma customizadas para contexto brasileiro.



SIEM Sem Contexto Local

Alertas sem correlação com gatilhos culturais como PIX e NF-e passam despercebidos.



Resposta Reativa

Investigar após o incidente custa dez vezes mais do que bloquear com CTI antecipada.

CTI em Ação — Do Relatório à Defesa Ativa



Kaspersky Digital Footprint (DFI) & Reporting

Resposta especializada a incidentes com profissionais que conhecem as TTPs do **cibercrime brasileiro** — reduzindo tempo de contenção e impacto operacional.

Threat Data Feeds

Feeds de IoCs **integráveis** diretamente ao seu stack de segurança. CTI não é para gerar PDFs para o CISO ler — é para injetar **bloqueios automáticos** antes do primeiro disparo.

Resiliência Estratégica contra Ameaças Nacionais



Visibilidade

Mapeamento completo da superfície de ataque com contexto local



Inteligência

CTI global e local do GReAT integrada ao seu stack



Resposta

Contenção acelerada com DFI e automação via Threat Data Feeds



Antecipar-se à ameaça local não é mais diferencial competitivo — é garantia de **continuidade do negócio** no Brasil.

Integre a **CTI Kaspersky** na sua estratégia de defesa
hoje!

RELATÓRIOS DE CTI

O time GReAT produz cerca de **150 a 200 relatórios/ano!**



[Back to Reporting](#)

GoPIX: architecture analysis and features

General

Report

TTPs

IOCs

Rules

 YARA

 Suricata

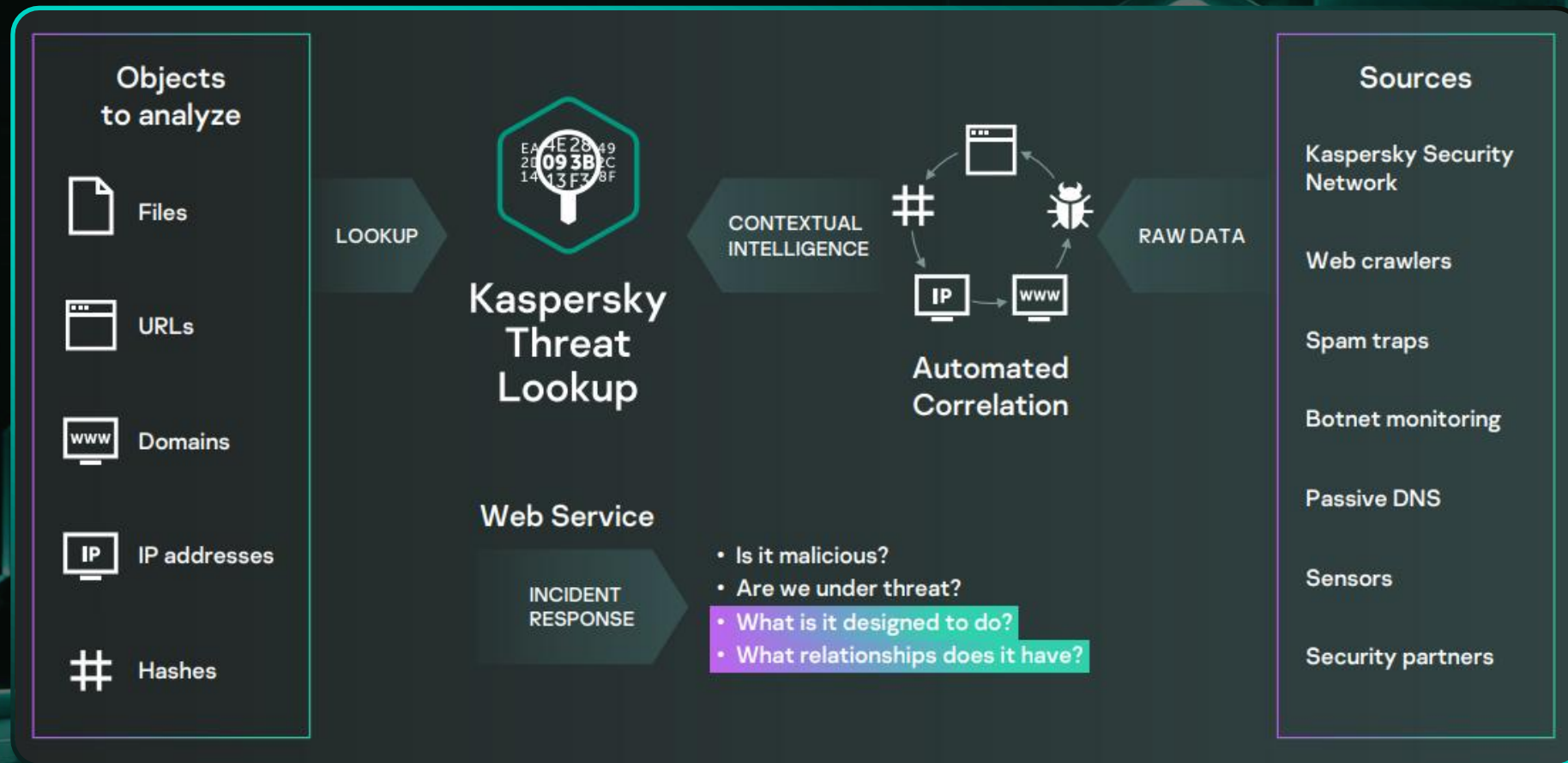
 Download

```
1 rule crimeware_BR_GoPIX_mem_payload {
2   meta:
3     description = "Detects GoPIX payload and scripts"
4     author = "Kaspersky"
5     copyright = "Kaspersky"
6     distribution = "DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY M
7     version = "1.0"
```

Kaspersky Threat Lookup



THREAT LOOKUP



THREAT LOOKUP

84.38.129.44

Threat Lookup

Lookup 1

Dark web 0

Surface web 0

KIRA OSINT IOCs 0

Reporting 0

Actors 0

Software 0

Digital Footpri

More

Daily request quota for your group: 85 of 100 left

Report for IP address

84.38.129.44

Dangerous

Open in research graph

Copy request

Export results

Overview

Hits	≈ 100	Owner name	—	Created	Jun 1, 2016
First seen	Jan 26, 2026 10:46	Owner ID	None	Updated	Dec 10, 2024
Threat score	100				
Categories	Botnet C&C Malware				

spersky

Overview

Hits ≈ 100

First seen Jan 26, 2026 10:46

Threat score 100

Owner name

—

Created

Jun 1, 2016

Owner ID

None

Updated

Dec 10, 2024

Categories

Botnet C&C

Malware

Data Feeds ⓘ

Botnet C&C URL Data Feed

IP Reputation Data Feed

Malicious URL Data Stream

[Go to Data Feeds](#) ↗

Industries

—

Actors ⓘ

—

Software ⓘ

—

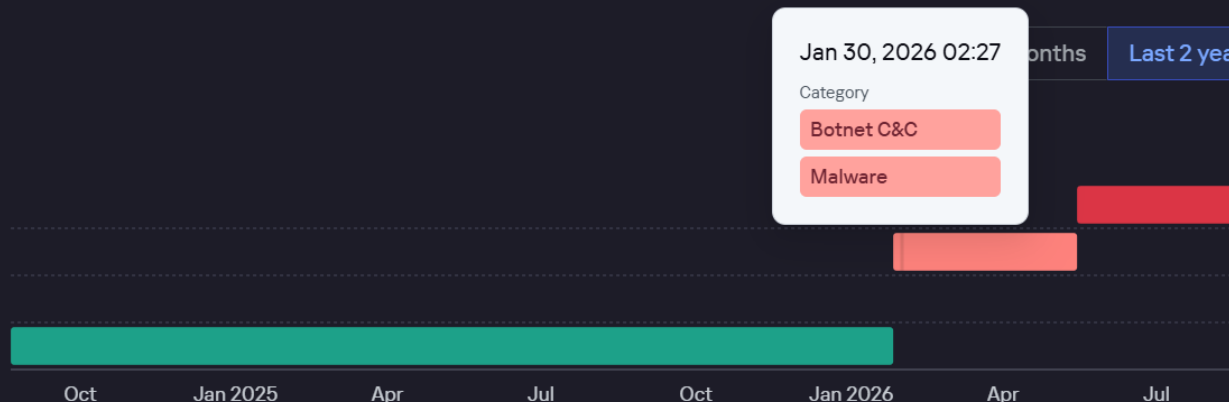
Timeline

Dangerous

Not trusted

Adware and other

No threats detected



Oct

Jan 2025

Apr

Jul

Oct

Jan 2026

Apr

Jul

Files related to IP address ⓘ

[Download data](#)

Status	Hits (≈)	File MD5	Detection name	Web address
Malware	100	443ba48fdb0af716b332051a720cb...	HEUR:Trojan-Downloader.MSOffice....	84.38.129.44/226/ec/32jhjh...
Malware	10	3fad0738fe0a33974c87aa5025d44...	Trojan.JS.SAgent.sb	84.38.129.44/232/ds78s7d8...
Malware	10	07294c2118317c91918631ac2f601a42	Trojan.MSOffice.Agent.sb	84.38.129.44/232/ce/be.doc...
Malware	10	fbf5f3177e4914db452055ffd8814349	HEUR:Trojan-Downloader.MSOffice....	84.38.129.44/232/ce/be.doc...
Malware	10	8000583ce76d063131ab55971ae1c...	HEUR:Trojan-Downloader.MSOffice....	84.38.129.44/231/buh/nc.do...
Malware	10	442c4e4f0102941552e03b1e55a18...	Trojan.JS.SAgent.sb	84.38.129.44/231/ds78s7d8...
Malware	10	ca59d4eee89c784ac3a59db8c73e1...	HEUR:Exploit.MSOffice.CVE-2018-...	84.38.129.44/231/buh/nc.do...
Malware	10	49f9fc4ffa6fc5c39983e1c9bb4e3d...	HEUR:Exploit.MSOffice.Generic	84.38.129.44/400/unh/ce.d...
Malware	10	fa7d9b87122b51017e205a37bb862...	Trojan.JS.SAgent.sb	84.38.129.44/400/as866sd7...
Malware	10	c47f04735758f167e2774f8b4a9925...	HEUR:Trojan.Script.Generic	84.38.129.44/400/unh...

kaspersky



Kaspersky Digital Footprint Intelligence (DFI)

DIGITAL FOOTPRINT INTELLIGENCE

MISCONFIGURATION

Date

Threat name

Risk

Category

VAZAMENTO DE CREDENCIAIS

Date

Threat name

Risk

Category

EXTERNAL ATTACK SURFACE

High 260

Medium 1K

Low 118

Info 292

FAKE APP/SOCIAL MEDIA

Date

Threat name

Risk

Category

> ...DF7636740

Jan 12, 2026 13:14

Cross Site Scripting
vulnerability

High

Web vulnerability

> ...F10641895

Apr 22, 2026 06:17

Fake X (Twitter) account
entity detected

Medium

Fake social media ent

> ...DF10641894

Apr 22, 2026 06:17

Fake Telegram account
entity detected

Medium

Fake social media ent

> ...DF10641893

Apr 22, 2026 06:17

Fake Facebook account
entity detected

Medium

Fake social media ent

> ...F10641892

Apr 22, 2026 06:17

Fake Facebook post entity
detected

Medium

Fake social media ent

> ...DF10641891

Apr 22, 2026 06:17

Fake Instagram account

Medium

Fake social media ent

Prática

HANDS ON!



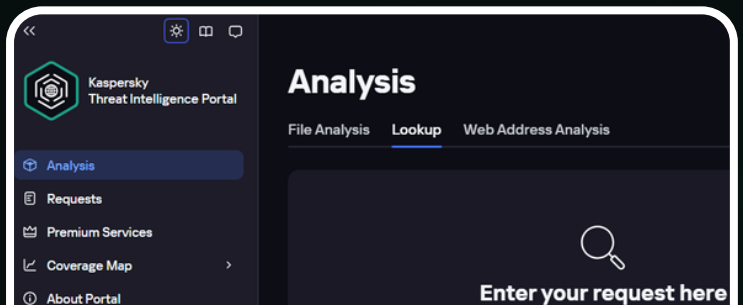
 [ps://OpenTIP.Kaspersky.com](https://OpenTIP.Kaspersky.com)

google-images.ml

84.38.129.44

```
"threat_score": 100,  
"category": "botnet_cnc",  
"first_seen": "26.01.2026 13:46",  
"last_seen": "12.02.2026 10:45",  
"popularity": 3,  
"ip_geo": "nl",  
"users_geo": "br, mx, es",
```

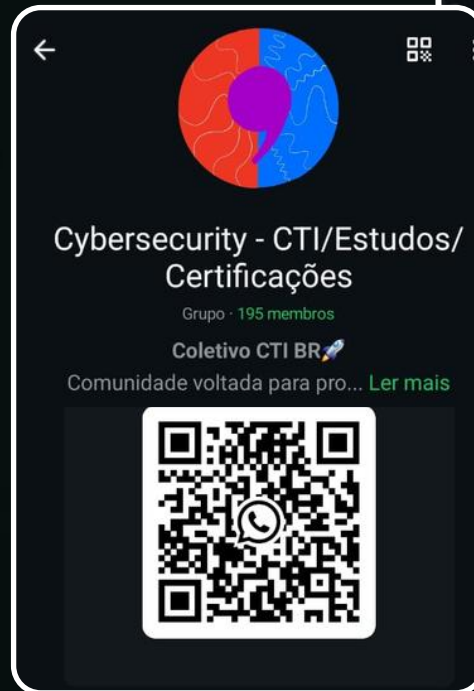
Recursos da para a Comunidade



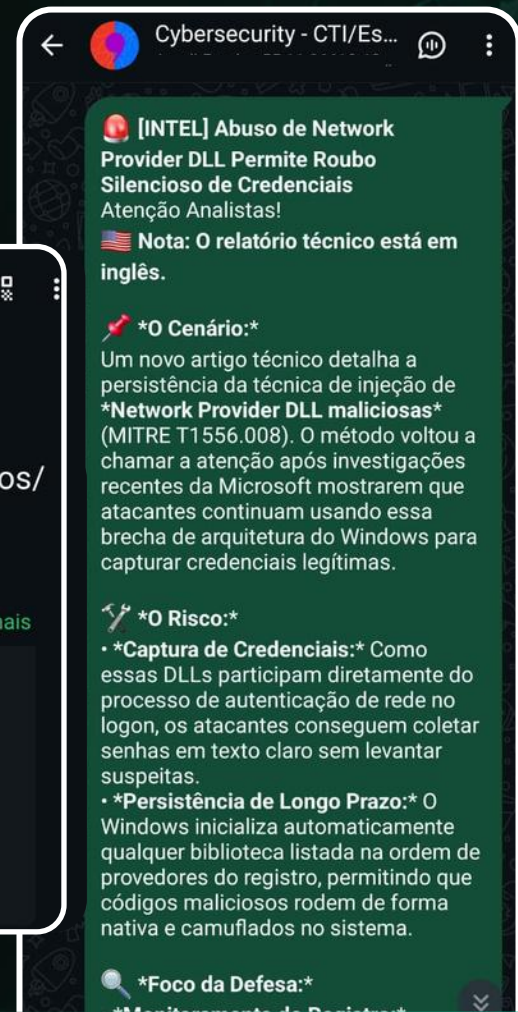
<https://OpenTIP.Kaspersky.com>
(Sandbox)



<https://SecureList.com.br>
(Relatórios)



Cybersecurity - CTI/Estudos/Certificações
Coletivo CTI BR (WhatsApp)



THANK YOU
THANK YOU
THANK YOU



Faça o seu **relatório de exposição!** É **gratuito!**