Combatendo Crimes de Alta Tecnologia: Unindo Inteligência (Artificial), Cooperação Internacional e Investigação

WTR PoP-BA 2025

Ministério da Justiça e Segurança Pública

Polícia Federal

PF 80

Ivo de Carvalho Peixinho

Perito Criminal Federal

Coordenador de Repressão a Crimes de Alta Tecnologia

CCAT/CGCIBER/DCIBER/PF

$whoami

Sr Security Analyst
Rede Nacional de Pesquisa
Oct 2004 - Jan 2007 · 2 yrs 4 mos

Worked at CAIS - Centro de Atendimento de Incidentes de Segurança, the Brazilian Academic CSIRT.

Teacher
IBTA
2006 - 2006 · Less than a year

Teacher of Windows Server Security

Infrastructure and Security Administrator
Universidade Federal da Bahia
Dec 1994 - Sep 2004 · 9 yrs 10 mos

Network Administration (Gigabit Ethernet, ATM, PSTN, Routers, L3 Switches)
Routing Protocols (BGP, OSPF, RIP, RIPv2)
Security (Firewalls, VPN, IDS)
Unix Administration (AIX, Linux, Solaris)
Windows Administration (Windows 2000)

Technical Director
Xsite Consultoria e Tecnologia
1996 - 2004 · 8 yrs

Player Card

DCIBER

ESTRUTURA ATUAL

- **Diretoria de Combate a Crimes Cibernéticos**
  - Assessor Técnico Especializado
  - Serviço de Apoio Administrativo
  - Serviço de Gestão Estratégica e Inovação
    - Setor de Sistemas e Dados
    - Setor de Doutrina e Capacitação
    - Setor de Processos, Projetos e Inovação
- Coordenação-Geral de Combate a Crimes Cibernéticos
  - Serviço de Análise de Dados e Inteligência Policial
  - Núcleo de Apoio Administrativo
  - Rede 24x7
  - Unidade de Repressão a Crimes Cibernéticos de Ódio
  - **Coordenação de Repressão a Crimes Cibernéticos Relacionados ao Abuso Sexual Infantojuvenil**
    - Assistente Técnico
  - **Coordenação de Repressão a Crimes de Alta Tecnologia**
    - Serviço de Investigação e Análise de Dados
  - **Coordenação de Repressão a Fraudes Bancárias Eletrônicas**
    - Serviço de Investigação e Análise de Dados
  - **Divisão de Investigação e Operações Especiais**
    - Serviço de Apoio Operacional

Equipe

PCF Peixinho

PCF Maia

PCF Nilson

PCF João Fernando

PCF Flávio

PCF Isabel

PCF Nitto

PCF Marcelo Silva

Ministério da Justiça e Segurança Pública

Polícia Federal

PF 80

Crimes de Alta Tecnologia

Ransomware

Botnets de malware bancário

DDoS

Invasão

Ataque ou violação de Infraestrutura crítica

Eixos de atuação

Repressão

Prevenção

Projetos

Cooperação

Capacitação e Eventos

Repressão

Investigações
Inteligência
Análise
Apoio

Repressão

Op. Data Breach

Hack

USD

III.5. Do concurso material

Somando-se as penas acima aplicadas, a pena definitiva aplicada ao réu é de **10 anos 6 meses e 20 dias de reclusão e 166 dias-multa**, a ser cumprida em **regime fechado**, conforme art. 33, § 2º, alínea "a", do Código Penal, dada a quantidade das penas somadas e também em vista das circunstâncias judiciais apresentadas, as quais indicam a necessidade do regime fechado.

Arbitro o dia-multa em 1/30 do salário mínimo vigente à época do fato, considerando não ter sido possível verificar as condições econômicas do réu. Frise-se que a correção monetária deverá incidir sobre o valor da multa desde a data do fato.

Repressão

Op. Chaes

Malware

Fraude Bancária

OPERAÇÃO PF

PF deflagra operação contra associação criminosa especializada em crimes cibernéticos

Os principais alvos do esquema eram clientes vinculados à Caixa Econômica Federal, mas outras instituições bancárias também foram afetadas

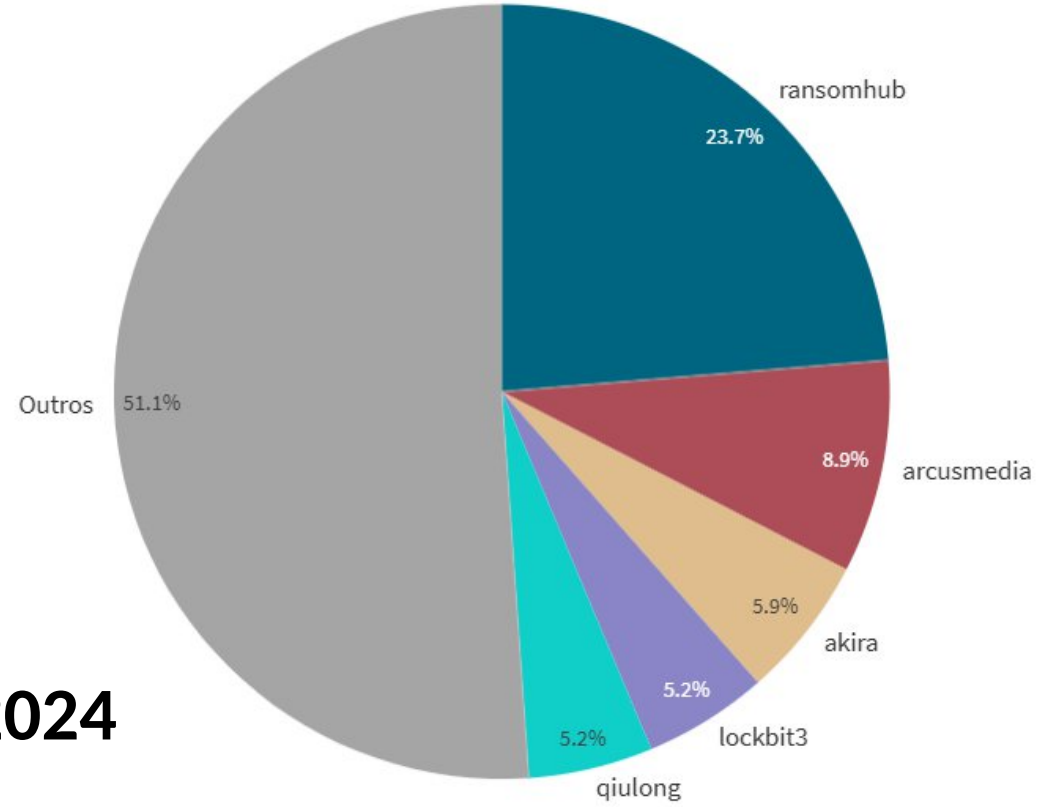
Publicado em 22/01/2025 08h13 Compartilhe:

Repressão

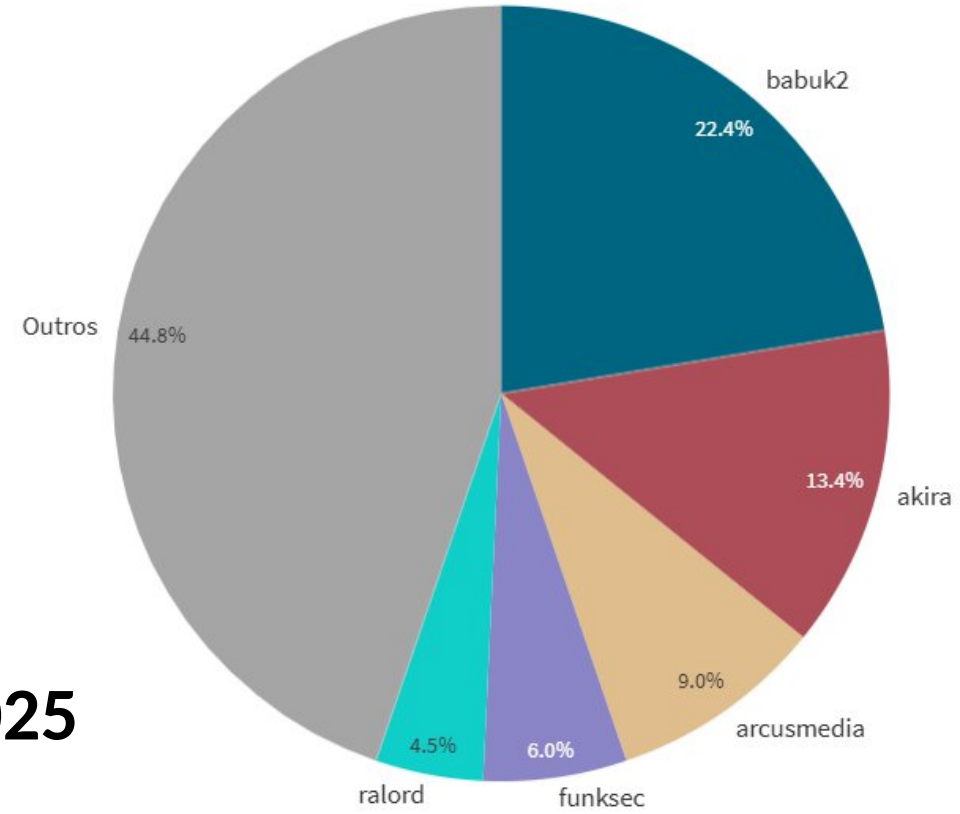
Op. Databrokers

Hacker	Vítimas
EL84	Governo de Alberta (Canadá)
XHINZ	University of Alaska (EUA)
	PRF (BR)

Repressão
RANSOMWARE 2024/2025

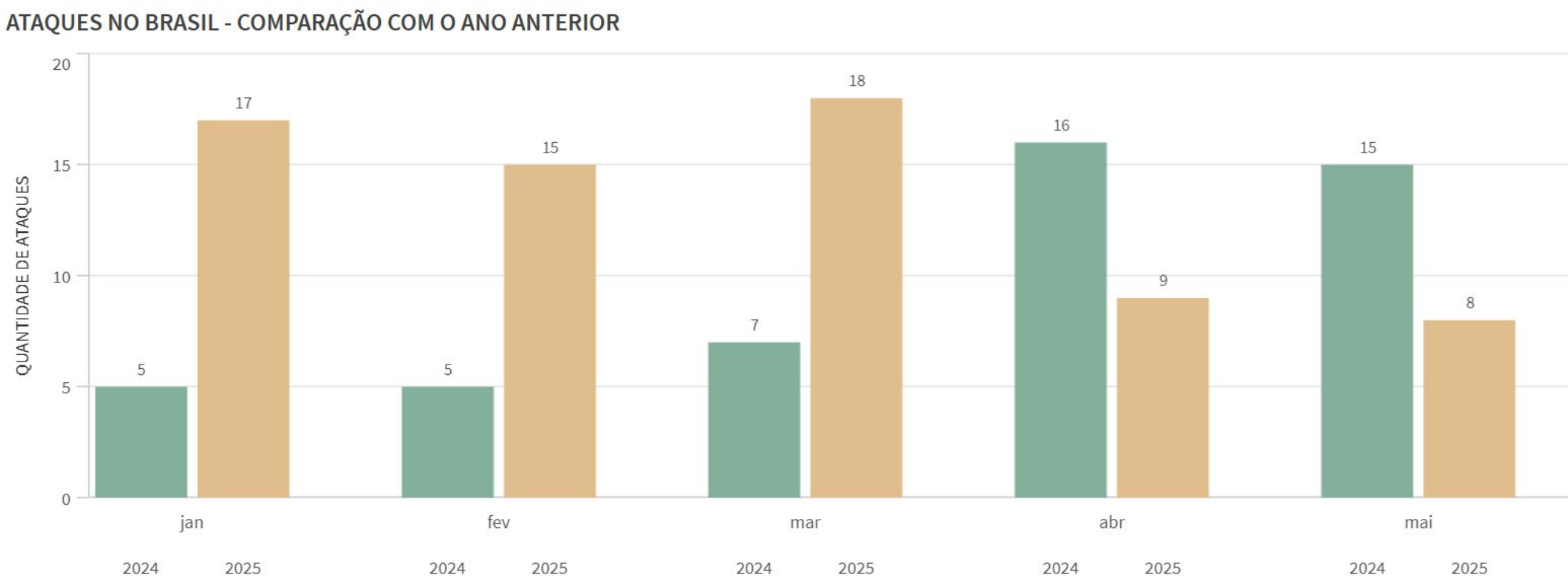


2024



2025

Repressão
RANSOMWARE 2024/2025



Repressão

ANÁLISE DE CASOS 2024/2025

16/20

IPJ-RAAT
CCAT
2024/2025

130/70

Informações
Comuns
2024/2025

Repressão 2024/2025

1416/	492	Casos	132/	73	IPLs inst.
878/	267	RDF	68/	37	IPL relat.

9/	5	Autoria
3/	4	Presos

Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Repressão Malware Bancário

- Operação Código Reverso (2018)
  - Operador William
- Operação Creeper (2021)
  - Dev Picker
- Operação Iceberg (2023)
  - Dev Picker e Gothie
- Operação Grandoreiro (2024)
  - Operador Cavenagui
- Operação Chaes (2025)

Made in Brazil: como o país se tornou um fabricante e exportador de ameaças bancárias

Vírus da família grandoreiro atingiu 40 países pelo mundo e mais de 900 instituições financeiros — foram 150 mil vítimas

Ingrid Oliveira

26 ago 2024 - 05h00 Compartilhar Exibir comentários

Ouvir texto 0:00

Resumo

O Brasil liderou ataques bancários na América Latina, exportando ameaças cibernéticas através do malware Grandoreiro, desmantelado em ação conjunta da Kaspersky, Interpol e autoridades brasileiras.

Repressão Malware Bancário

Os relatórios e laudos de análise técnica, produzidos pelo SETEC/SR/PF/TO, referentes ao material apreendido por ocasião da deflagração da operação "Código Reverso", foram juntados aos autos conforme segue:

a) Laudo Pericial n. 180/2018 — Informática (ID 1418499778 - Págs. 183/191);

b) Laudo Pericial n. 266/2018 — Merceológico (ID 1418499778 - Págs. 192/206);

c) Laudo Pericial n. 268/2018 — Merceológico (ID 1418499778 - Págs. 207/211):

d) Laudo Pericial n. 269/2018 — Merceológico (ID 1418499778 - Págs. 212/213 e ID 1418499776 - Págs. 1/3);

Unificação das Penas

Promovo a unificação das penas, para o montante total de **11 anos, 3 meses e 10 dias de reclusão e 256 dias-multa**.

Em seu interrogatório, o acusado declarou possuir renda formal de um salário mínimo. Dessa forma, fixo o valor do dia-multa no patamar de 1/30 do salário mínimo vigente à época da conduta, incidindo a devida correção monetária.

Deixo de realizar a detração, pois não haverá alteração no regime inicial de cumprimento de pena, competindo ao Juízo da Execução realizar eventuais ajustes após o trânsito em julgado.

A pena privativa de liberdade será cumprida em **regime inicial fechado** (art. 33, § 2º, "a", do CP).

O condenado não atende aos requisitos para a substituição da pena privativa de liberdade (art. 44 do Código Penal), ou mesmo para a suspensão condicional da pena (art. 77 do Código Penal), ante o patamar da pena fixada.

Condeno o acusado a ressarcir solidariamente com os demais acusados, os danos acarretados à União Federal, no total de R$ 16.359.067,50 (atualizado até 09/2018).

fixada de acordo com o número de delitos cometidos, aplicando-se 1/6 pela prática de 2 infrações; 1/5 para 3 infrações; 1/4 para 4 infrações; 1/3 para 5 infrações;1/2 para 6 infrações; **e 2/3 para 7 ou mais infrações**" (STJ, HC nº 442.316 / SP 2018/0067542-1 autuado em 25/03/2018).

o) Laudo Pericial n. 212/2018 — Merceológico (ID 1418499780 - Pág. 106/112):

p) Laudo Pericial n. 191/2018 — Documentoscópico (ID 1418499780 - Pág. 113/121);

q) Laudo Pericial n. 162/2018 — Documentoscópico (ID 1418499780 - Pág. 135/142);

r) Laudo Pericial n. 163/2018 —Merceológico (ID 1418499780 - Pág. 143/146);

s) Laudo Pericial n. 165/2018 — Merceológico (ID 1418499780 - Pág. 147/150); e

t) Laudo Pericial n. 167/2018 — Informática (ID 1418499780 - Pág. 151/160).

Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Invasão

Brasil | Invasão hacker

Ataque à C&M é financ

Há estimativa

Gabriel Garcia
04/07/2025 16h19

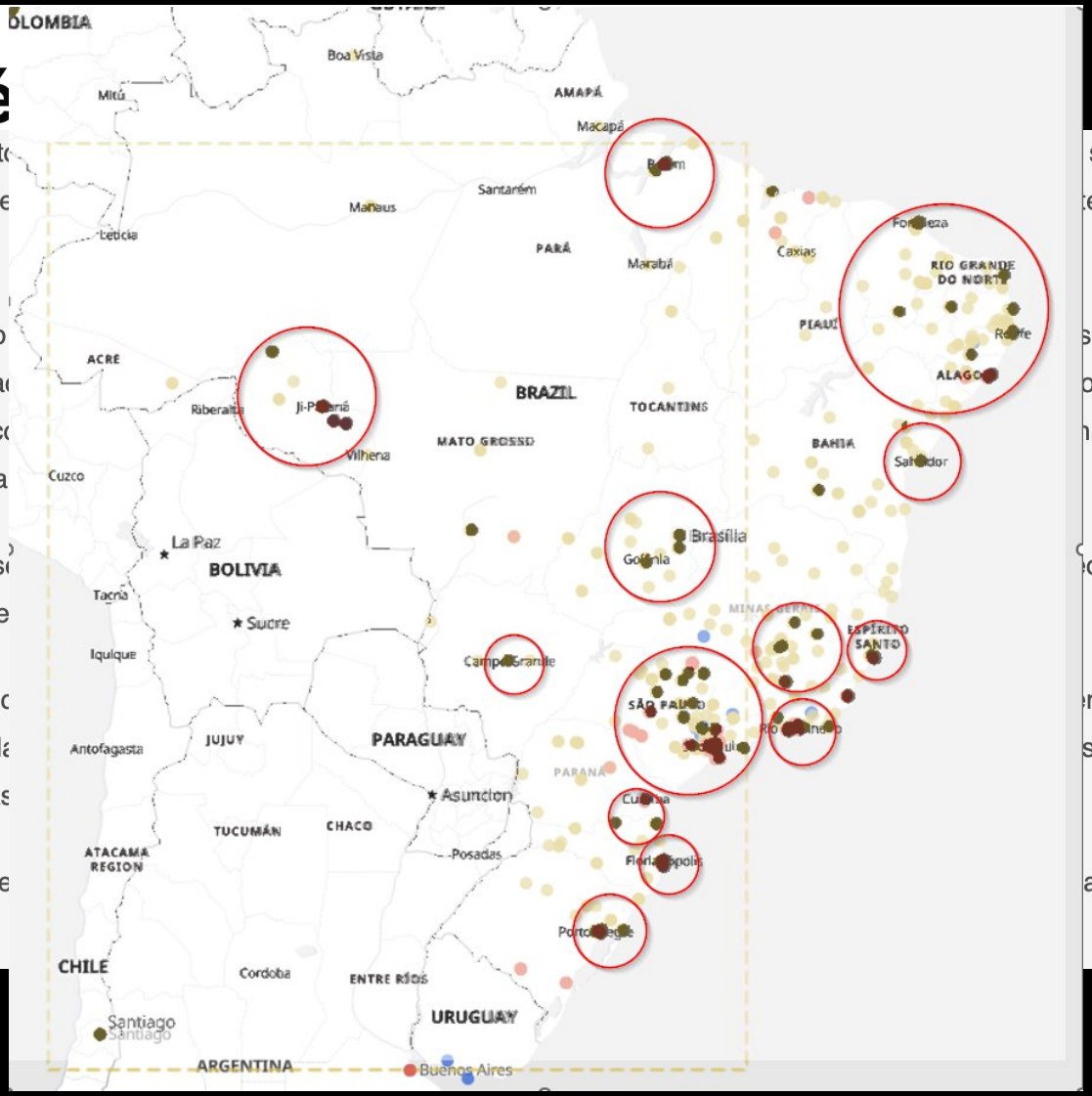
Em atenção ao disposto
no sistema de busca de
operar normalmente.

O incidente provocou o
oito) pessoas. Foram a
agência e número da c
extratos, nem acesso a

Todas as medidas de s
Autoridade Nacional de

É importante ressaltar
contas bancárias. Ainda
razão, o CNJ reforça as

O CNJ não se utiliza de
telefônicas.



segurança
tema voltou a

s e noventa e
o, número da
nas ou

deral e a

m acessar
s. Por essa

as

Ministério da Justiça e Segurança Pública
Polícia Federal
PF 80

Inteligência

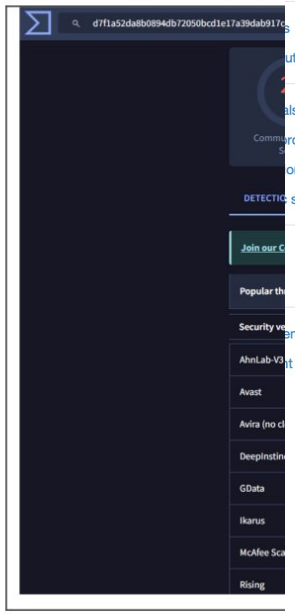


Figura 1 – Análise do Virusto

Não seguro https://cape.pf.gov.br/analysis/209/

capePF Dashboard Recentes Pendentes Buscar API Submeter Estatísticas Usuário

Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API Bookmarks MISP Peixinho Icp Log out

My Events Org Events

Enter value to search Event info Filter

Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Last modified at	Published at	Info	Distribution	Actions
DIP	82124		intel_dip	4		2025-08-18	2025-08-25 15:00:05		Documento de Inteligência 202520030596 SADIP/CGCIBER/DCIBER/PF	All	
DIP	82123		intel_dip	7		2025-08-15	2025-08-25 15:00:04		Documento de Inteligência 202520030516 DAE/DIP/PF	All	
DIP	82122		intel_dip	5		2025-08-15	2025-08-25 15:00:03		Documento de Inteligência 202520030515 DAE/DIP/PF	All	
CCAT-CGCIBER	82121		common-taxonomy:information-gathering="phishing" common-taxonomy:intrusion="vulnerability-exploitation" manual	2		2025-08-25	2025-08-25 10:18:24		Página de prefeitura na Paraíba sendo usada para cometimento de phishing na China.	Community	
CCAT-CGCIBER	82120		Fraud phishing manual	2		2025-08-19	2025-08-19 10:38:26		Atores de ameaça estrangeiros contactando autoridades brasileiras para obter informações sensíveis.	Community	
DIP	82119		intel_dip	8	1	2025-08-08	2025-08-18 19:37:57		Documento de Inteligência 202520030223 UADIP/DRCC/SR/PF/RS	All	
CCAT-CGCIBER	82117		Inteligência manual phishing	2		2025-08-18	2025-08-18 14:50:28		Site fraudulento Receita Federal - DELECIBER/SP	Organisation	
CCAT-CGCIBER	82116		ddos Inteligência manual origem:FBI	20	2	2024-09-24	2025-08-18 14:24:59		PowerOFF Security Hide - Inteligência FBI do Coinbase	Community	

riminosa

rtefato

nforma

Ainda de acordo com o Virustotal, o art
para a ferramenta em **2025-08-18 07:**
partir de análise realizada nesta CCAT
obter o endereço Internet (URL)
https://dns.google/resolve?name=bugattimotorssystem.point2this.com, aparentemente usado para comunicação com a infraestrutura criminosa (C2 – Comando e Controle).

[4] https://cape.pf.gov.br/analysis/209/
[5] https://www.ibm.com/think/x-force/grandoreiro-banking-trojan-unleashed

Prevenção

Campanhas
Comunicações
Apresentações
Folder

Prevenção
CAMPANHAS

Prevenção

CAMPANHA InterCOP

Ministério da Justiça e Segurança Pública

Polícia Federal

PF 80

Prevenção
CAMPANHA InterCOP

Tema	Rede Social	Link	Estatistica		
			Alcance	Impressões	Total Interações
The No More Ransom Project	X	https://x.com/policiafederal/status/1816899412251070870	6384	6384	151
Weekly post regarding cyber security month	X	https://x.com/policiafederal/status/1848430651495878790	5331	5331	227
International Computer Security Day	Facebook	https://www.facebook.com/share/1Y6hDhhSdT/	4541	8149	386
	Instagram	https://www.instagram.com/p/DC_sr3pumL1/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==	27535	35716	766
	X	https://x.com/policiafederal/status/1862887565122019800	5032	5032	175
Data Privacy Week	X	https://x.com/policiafederal/status/1882801011942703347	4005	4005	81
Safer Internet Day	X	https://x.com/policiafederal/status/1889350340962644086	4254	4254	165
International girls in ICT Day	Facebook	https://www.facebook.com/share/1EpLS46XEC/	6709	10189	297
	Instagram	https://www.instagram.com/p/DI1ZcpRMAOm/?utm_source=ig_web_copy_link&igsh=MzRlODBiNWFlZA==	63980	87230	2184
	X	https://x.com/policiafederal/status/1915428169282130007	4327	4327	127

Prevenção
COMUNICAÇÕES

8/11

Comunicações
CCAT
2024/2025

Ministério da Justiça e Segurança Pública
Polícia Federal
PF 80

Projetos

Sistemas
Ferramentas

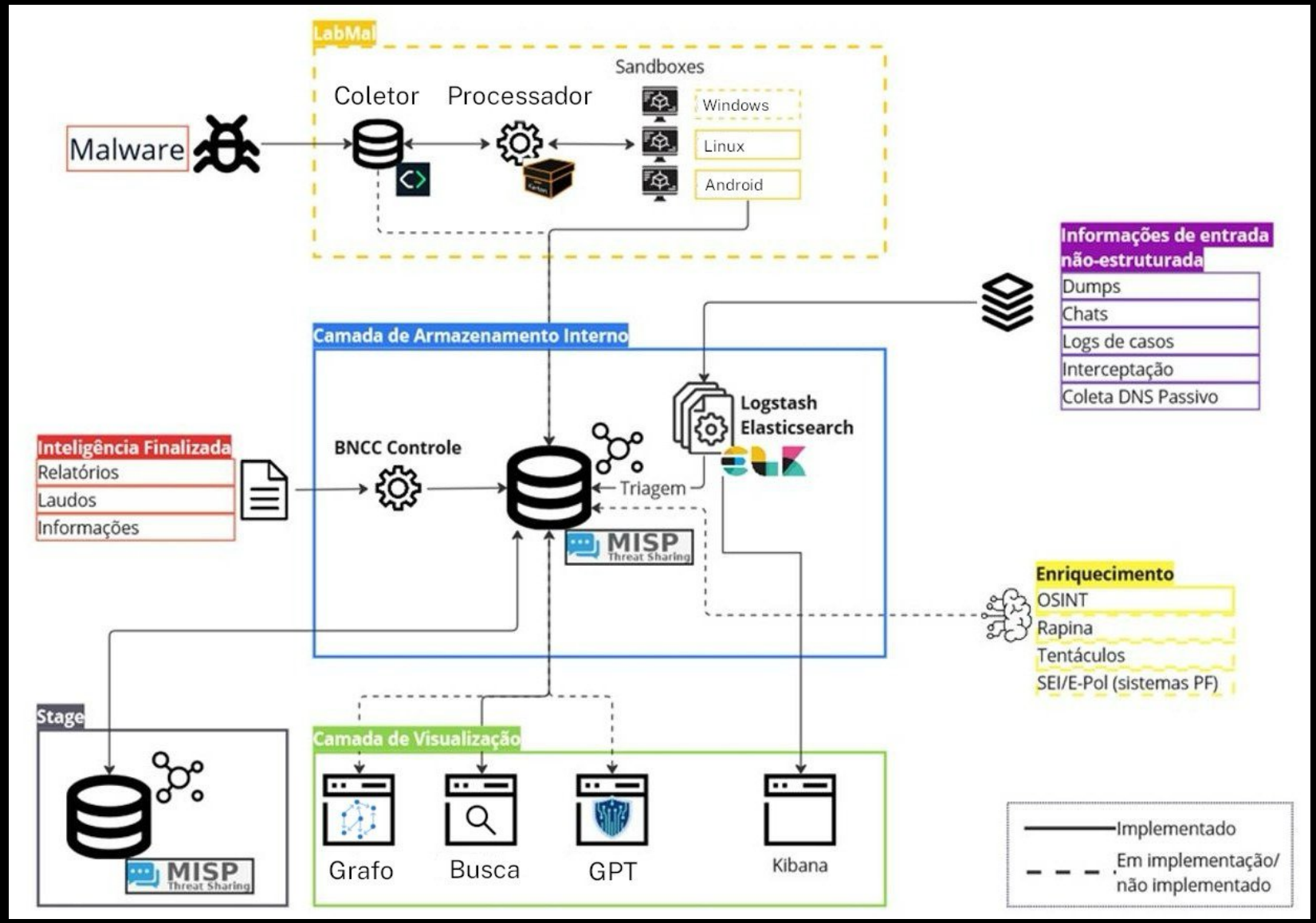
Projetos

- Projeto Capivara – BNCC 2.0
  - Consulta
    - Interface de grafo, busca e GPT (LLM)
  - Malware
    - Coleta e armazenamento
    - Analise (sandboxes): Windows, Linux, Android
    - Extração de configuração (IA e regras)
  - Gov.br
    - Base de investigações

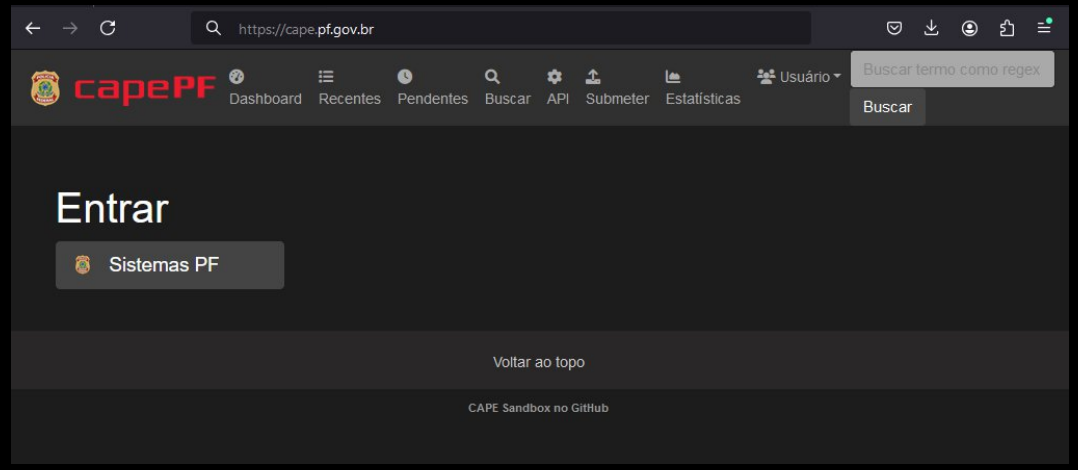
Projeto Capivara – BNCC 2.0

- Inteligência finalizada
  - Documentos (laudos, relatórios, inquéritos)
  - Extração de entidades/indicadores (regex, NLP, LLM)
- Dados não estruturados / triagem
  - DNS Passivo, Netflow (Interceptação), Chats, Dumps, Logs, Forense (IPED / SARD-web)
- Enriquecimento
  - OSINT (Telegram)
  - Sistemas Cyber (Rapina, Tentáculos)
  - Outros sistemas PF

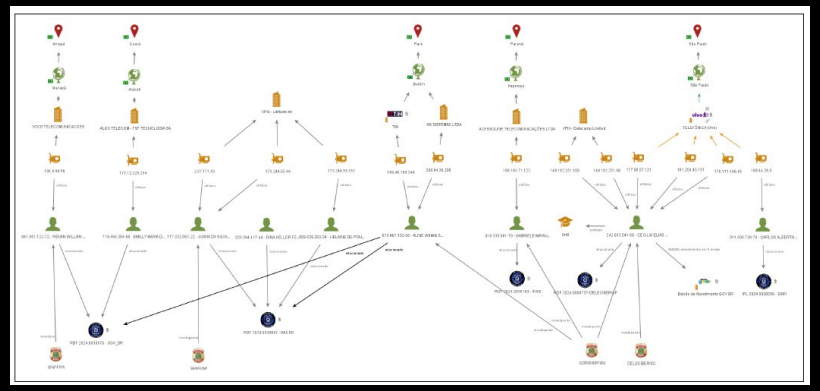
Projeto Capivara – BNCC 2.0

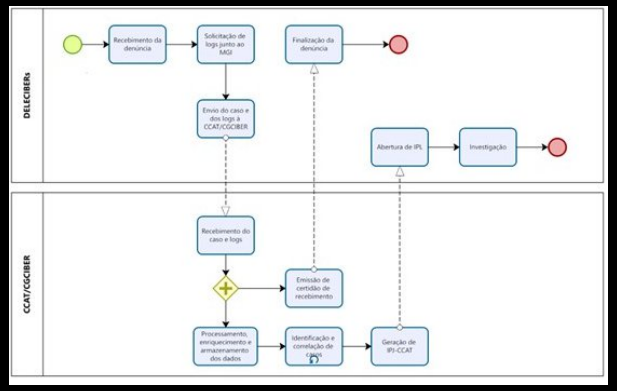


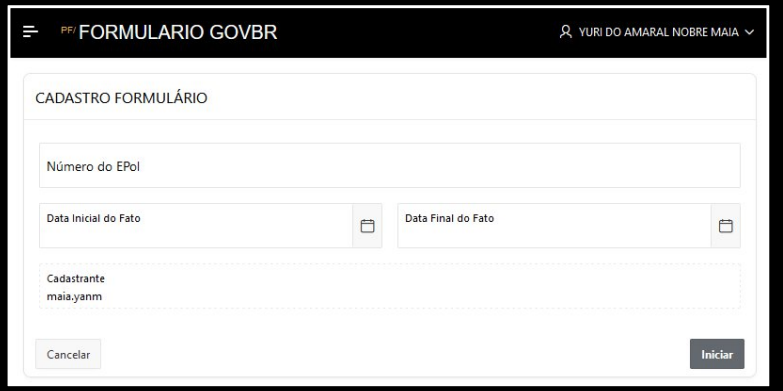
Projetos
EVOLUÇÕES

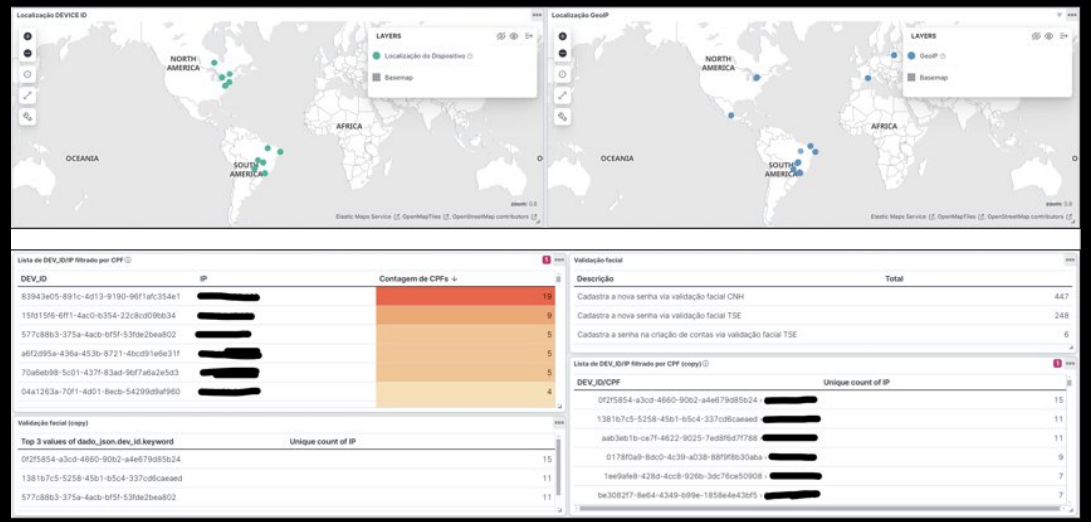


Projetos Gov.br









Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Cooperação Internacional

24/7

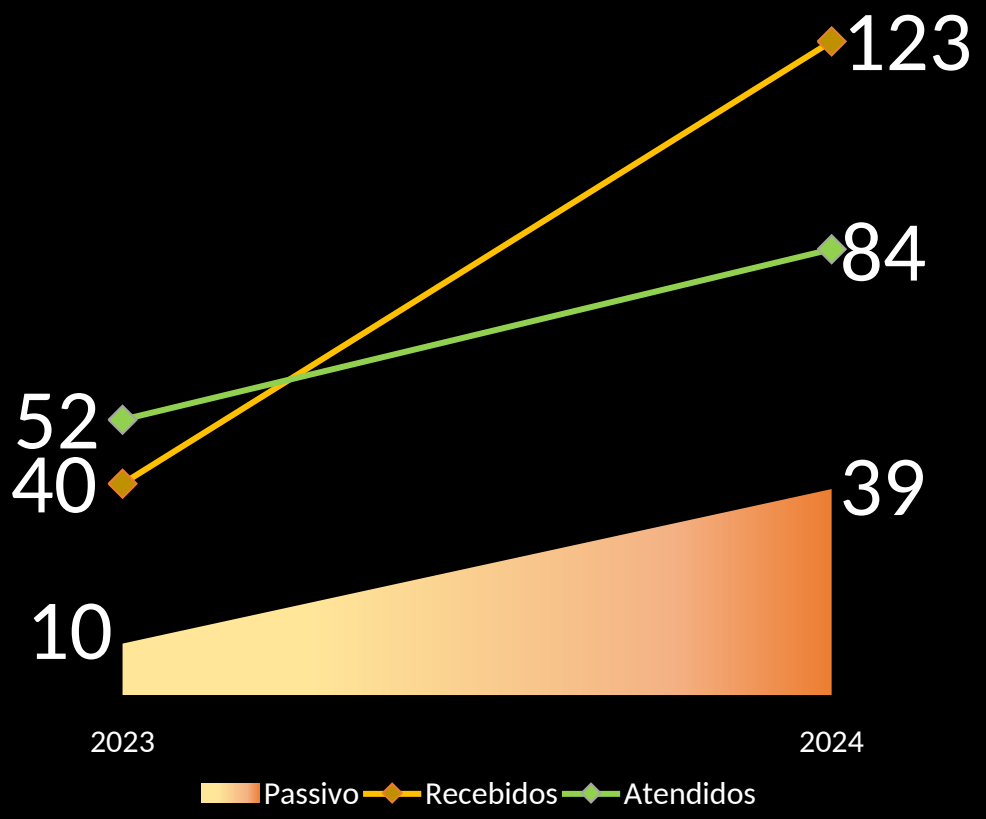
CRI

PowerOFF

Relacionamento

Cooperação Internacional

24/7



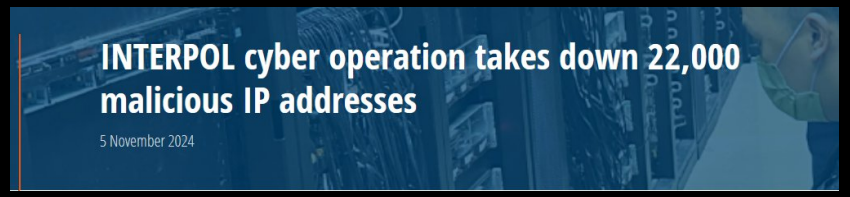
+60%
Atendimento

+200%
Demanda

Ministério da Justiça e Segurança Pública
Polícia Federal
PF 80

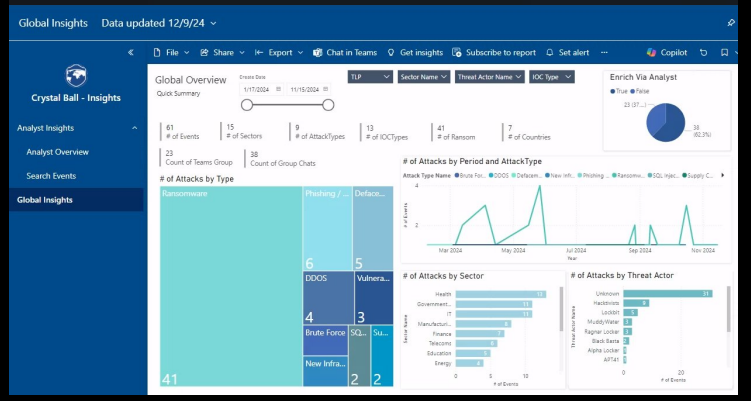
Cooperação Internacional

ALCEDO / CRI / POWEROFF / SYNERGIA



EMPACT

CRI
INTERNATIONAL COUNTER RANSOMWARE INITIATIVE



Ministério da Justiça e Segurança Pública

Polícia Federal
PF 80

Cooperação Internacional

INTERPOL Americas WG on Cybercrime 2024

100+ participantes

35 países

15 parceiros privados

Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Cooperação Internacional

Apresentação
Underground
Economy
Op Grandoreiro

Reunião
Ameripol
AC3

1° Lugar
CyberLeague
Espanha

Cooperação Nacional

9H30

Assinatura do Acordo de Cooperação Técnica da Fiesp com a Polícia Federal para a troca de informações visando a prevenção de crimes de alta tecnologia

Josué Gomes da Silva,
presidente da Fiesp

Andrei Rodrigues,
diretor geral da Polícia Federal

CONTEXTUALIZAÇÃO

Otavio Margonari Russo,
diretor de Combate a Crimes Cibernéticos da Polícia Federal

Rony Vainzof,
diretor adjunto do departamento de Defesa e Segurança (Deseg) da Fiesp

MJSP e Febraban firmam acordo para combate a fraudes, golpes e crimes cibernéticos

Composto por representantes de setores públicos e privados, grupo de trabalho visa discutir ações de prevenção e combate a fraudes, golpes e crimes cibernéticos

Publicado em 23/08/2024 16h33 | Atualizado em 14/10/2024 13h39 Compartilhe:

Foto: Divulgação/Febraban

Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Capacitação e Eventos

Cursos Presenciais

Cursos EAD

Eventos

Apresentações

Capacitações e Eventos
I CICAT (AGO/2024)

Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Capacitações e Eventos
CBAM 2024.01 – EAD (OUT/2024)

Curso Básico de Análise de Malware - 2024.01

Curso Básico de Análise de Malware

Informações sobre o evento

Carga horária: **40 horas**
Formato: **Com acompanhamento docente**
Público alvo: **Apenas Policiais Federais**
Área responsável: **CCAT/CGCIBER/DCIBER**
Contato: **ccat.cgciber.dciber@pf.gov.br**

Apresentação

Ministério da Justiça e Segurança Pública
Polícia Federal
PF 80

Capacitações e Eventos
I CADM (MAR/2025)

Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Capacitações e Eventos
II CICAT (ABR/2025)

Ministério da Justiça e Segurança Pública

Polícia Federal PF 80

Capacitações e Eventos

Capacitação	Formato	Data	Participantes
I CICAT	*Presencial*	*Ago/2024*	*20*
CBAM – 2024.01	*EaD*	*Out/2024*	*32*
I CADM	*Presencial*	*Mar/2025*	*15*
CBAM – 2025.01	*EaD*	*Mar/2025*	*15*
II CICAT	*Presencial*	*Abr/2025*	*18*
CBAM – 2025.02	*EaD*	*Mai/2025*	*15*
CBAM – 2025.03	EaD	**Ago/2025**	15
II CADM	Presencial	**Ago/2025**	15
CBAM – 2025.04	EaD	**Out/2025**	15
III CICAT	Presencial	**Nov/2025**	30
		TOTAL	**190**

Polícia Federal
PF 80

2025/2026

- Investigação botnets de distribuição de malware
- Especialização de atendimento
- Novas ações de prevenção
- Capacitação em técnicas ofensivas
- Evolução das soluções e infraestrutura
- Projeto Capivara

Obrigado!

Ivo de Carvalho Peixinho

Perito Criminal Federal

peixinho.icp@pf.gov.br