2025
The Botnet &
Malware Ecosystem
Fighting Conference

Angers, France
May 21-23

Unveiling the DVR Ecosystem

A 3-Year Investigation into Global IoT Bot Recruitment Campaigns

UMEMURA Yuki*
MORI Yoshiki
FURUKAWA Hideyuki
OKUGAWA Kanta
KUBO Masaki*

Cybersecurity Research Institute (CSRI), NICT

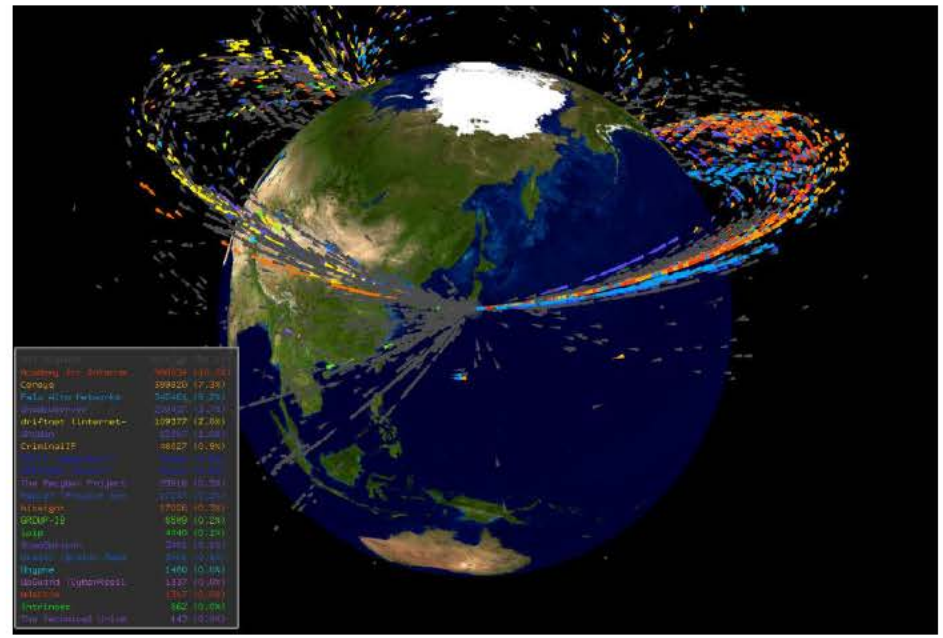
NICT National Institute of Information and Communications Technology

CYBERSECURITY Research Institute

About Us

- **Cybersecurity Research Institute (CSRI), NICT**

- A team of experts dedicated to:
  - Monitoring and analyzing darknet traffic
  - Tracking Internet-wide scanners
  - Discovering and analyzing zero-day vulnerabilities in IoT ecosystem
  - Analyzing malware



Real-time visualization packets arriving at 'NICTER' darknet sensors (300,000 unused IP addresses)

CYBERSECURITY Laboratory

Three Key Challenges in IoT Botnet Research

Challenge 1.
Tracking infected hosts

Challenge 2.
Identifying infection vectors

x ***RapperBot***

Challenge 3.
Analyzing the Evolution and Operation of a Bot Family

Challenge #1: Tracking infected hosts

Methods for Tracking and Profiling Infected Hosts

- How to get the IP address of infected hosts?
  - ✓sinkhole C2 traffic
  - ✓flow data analysis
  - ✓**passive monitoring of scan packets**
- How to identify the infected device?
  - ✓passive scan data (Shodan/Censys)
  - ✓**active scan-back the source**

Our Approach to Tracking Infected Hosts

- **Passive monitoring of scan packets with bot-specific signatures:**

```
iph->id = rand_next();
iph->saddr = LOCAL_ADDR;
iph->daddr = get_random_ip();
iph->check = 0;
iph->check = checksum_generic((uint16_t *)iph, sizeof (struct iphdr));

if (i % 10 == 0)
{
    tcph->dest = htons(2323);
}
else
{
    tcph->dest = htons(23);
}
tcph->seq = iph->daddr;
tcph->check = 0;
tcph->check = checksum_tcpudp(iph, tcph, htons(sizeof (struct tcphdr)), sizeof (struct tcphdr));

paddr.sin_family = AF_INET;
paddr.sin_addr.s_addr = iph->daddr;
paddr.sin_port = tcph->dest;
```

TCP SYN packet patterns

AND/OR

{23 26}
{23 67 70 79 80 81 82 83 84 85 88 90 ...}
{80 81 5555 7574 8080 8081 8181 8443 37215 ...}
{80 81 82 8080}
{80 81 82 83 85}

Characteristic scanning port sets

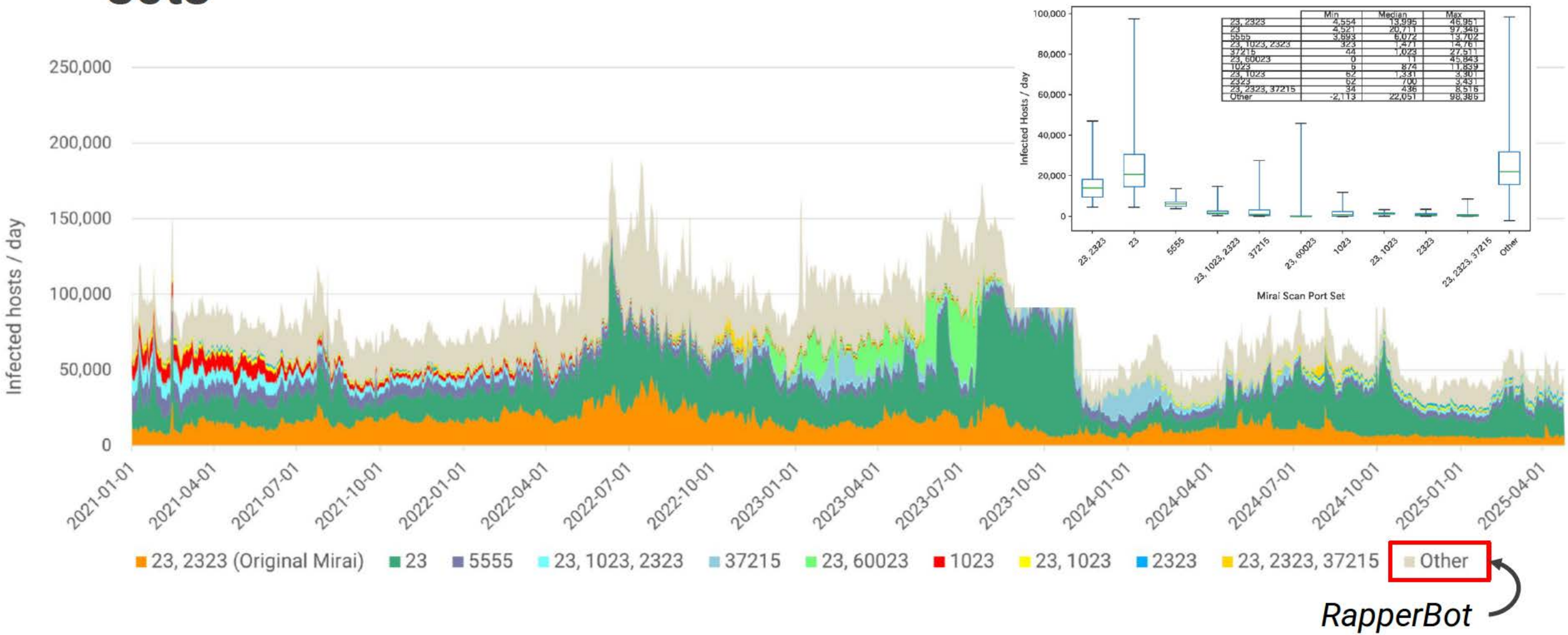
👎 **Non-scanning bots** can't be detected this way

👍 But **loader's infection activity** reveals which malware is being deployed

CYBERSECURITY Laboratory

Tracking Bots by Destination Ports (Top 10)

- **Daily unique source IPs, grouped by Mirai scan port sets**



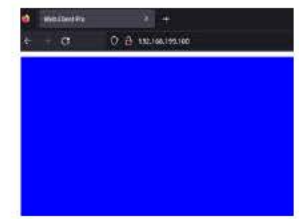
Identifying the Infected Device

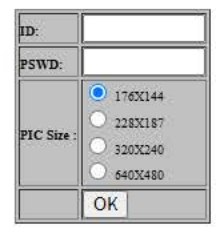
- **Actively scanned-back** bot IPs in **real time** after detecting their scan

No.	Stat	Last Seen[l] v	Src IPaddr[s]	ASNo	ORG	CC	Count[c] v	pps[p]	Proto	Portset
1	Alive	2025/04/27 13:47:57	150	2527	So-net	JP	173	0	S	S:23
2	Alive	2025/04/27 13:47:58	160	2514	NTT PC Communic	JP	139	5	S	S:23
3	Alive	2025/04/27 13:47:55	150	2527	So-net	JP	117	0	S	S:23
4	Alive	2025/04/27 13:47:58	60.1	17676	SoftBank Corp.	JP	82	2	S	S:23,S:2323
5	Alive	2025/04/27 13:47:57	1.3	2514	NTT PC Communic	JP	37	0	S	S:23
6	Alive	2025/04/27 13:47:58	60.3	4713	NTT Communicati	JP	29	2	S	S:23,S:2323
7	Alive	2025/04/27 13:47:58	115	9595	NTT-ME Corporat	JP	27	3	S	S:23
8	Alive	2025/04/27 13:47:34	106	2516	au one net	JP	27	0	S	S:23
9	Alive	2025/04/27 13:47:52	119	17511	K-Opticom Corpo	JP	26	0	S	S:23
10	Alive	2025/04/27 13:47:53	150	4685	Asahi Net	JP	21	0	S	S:23
11	Alive	2025/04/27 13:47:46	126	17676	SoftBank Corp.	JP	19	0	S	S:23
12	Alive	2025/04/27 13:47:58	220	2519	VECTANT	JP	18	1	S	S:23,S:2323
13	Alive	2025/04/27 13:47:58	1.3	2514	NTT PC Communic	JP	15	1	S	S:23
14	Alive	2025/04/27 13:47:58	124	9595	NTT-ME Corporat	JP	15	1	S	S:23
15	Alive	2025/04/27 13:47:52	124	9595	NTT-ME Corporat	JP	14	0	S	S:23,S:60023
16	Alive	2025/04/27 13:47:56	220	2519	VECTANT	JP	13	0	S	S:23
17	Alive	2025/04/27 13:47:52	1.3	2514	NTT PC Communic	JP	11	0	S	S:23
18	Alive	2025/04/27 13:47:56	133	2514	NTT PC Communic	JP	10	0	S	S:23
19	Alive	2025/04/27 13:47:54	219	2514	NTT PC Communic	JP	10	0	S	S:23
20	Alive	2025/04/27 13:47:49	60.1	17676	SoftBank Corp.	JP	10	0	S	S:23
21	Alive	2025/04/27 13:47:47	221	9354	Community Netwo	JP	10	0	S	S:23
22	Alive	2025/04/27 13:47:56	219	2514	NTT PC Communic	JP	9	0	S	S:23
23	Alive	2025/04/27 13:47:52	210	2514	NTT PC Communic	JP	8	0	S	S:23
24	Alive	2025/04/27 13:47:52	117	18081	KCN	JP	8	0	S	S:23
25	Alive	2025/04/27 13:47:40	114	4713	NTT	JP	8	0	S	S:23
26	Alive	2025/04/27 13:47:56	58.1	17511	K-Opticom Corpo	JP	7	0	S	S:23
27	Alive	2025/04/27 13:47:50	58.1	17511	K-Opticom Corpo	JP	7	0	S	S:23,S:2323
28	Alive	2025/04/27 13:47:50	118	4713	NTT	JP	7	0	S	S:9530
29	Alive	2025/04/27 13:47:24	61.1	18081	KCN	JP	7	0	S	S:23
30	Alive	2025/04/27 13:47:58	128	2514	NTT PC Communic	JP	6	1	S	S:23
31	Alive	2025/04/27 13:47:51	124	9595	NTT-ME Corporat	JP	6	0	S	S:23
32	Alive	2025/04/27 13:47:58	125	2518	Biglobe	JP	5	1	S	S:23
33	Alive	2025/04/27 13:47:58	180	4713	NTT	JP	5	1	S	S:23
34	Alive	2025/04/27 13:47:56	153	18013	freebit	JP	5	0	S	S:23
35	Alive	2025/04/27 13:47:55	180	4713	NTT	JP	5	0	S	S:23
36	Alive	2025/04/27 13:47:54	210	2519	VECTANT	JP	5	0	S	S:23
37	Alive	2025/04/27 13:47:48	220	9595	NTT-ME Corporat	JP	5	0	S	S:23
38	Alive	2025/04/27 13:47:46	153	4713	NTT	JP	5	0	S	S:23,S:2323
39	Alive	2025/04/27 13:47:41	210	2514	NTT PC Communic	JP	5	0	S	S:23
40	Alive	2025/04/27 13:47:41	118	18126	Chubu Telecommu	JP	5	0	S	S:23
41	Alive	2025/04/27 13:47:24	36.3	2519	VECTANT	JP	5	0	S	S:23

20,000 packets/sec

- **Around 70% of hosts were DVRs**
  - 527 out of 602 hosts (87.5%) responded
    - HITRON DVR: 63%
    - Rifatron DVR: 7%
    - Other devices: 17%





CYBERSECURITY Laboratory

What is DVR?

- Digital Video Recorder：A device that records, stores and streams camera recordings

- Linux based OS
- Web UI (HTTP)
- RTSP/ONVIF server
- Telnet/SSH access
- Dynamic DNS
- Internal HDD for recording storage

CPU: HiSilicon 3531
ARM Cortex-A9(Dual-Core)
Memory: 384MB
NAND Flash: 128MB
HDD: 2TB
NIC: 1Gbps

Camera input:
BNC/IP

LAN port

User

- This 1080p 16-channel DVR from 2016 (around $1000) comes with these specs
- Newer models supporting 4K video often include upgraded CPUs, including some with quad-core processors

CYBERSECURITY Laboratory

Challenge #2: Identifying infection vectors

Common Infection Vectors

A) Brute-force login (default credentials)

B) Management interface exploits

- Known CVEs
- Zero-day attacks

A）Brute-force logins

- Original Mirai hard-coded 60 ID/password pairs
- **40%** of them are linked to **DVR**, over **70%** are **surveillance** equipment

Username	Password	Manufacturer (vendor)	Device Model / Type (if known)
666666	**666666**	Dahua Technology	Default user account on Dahua DVRs/IP cams
888888	**888888**	Dahua Technology	Default admin account on Dahua standalone DVR/NVRs
admin	**12345**	Hikvision	IP Cameras/DVRs (older Hikvision models)
(snip)			
root	**1111**	Merit LiLin (Pinetron)	Digital video recorders
root	**juantech**	Guangzhou Juan Optical	DVR device (Juan CCTV DVR/NVR equipment)
root	**jvbzd**	Hangzhou Xiongmai (XM)	IP Camera/DVR (Xiongmai firmware)

A) Brute-force logins

Content redacted – available to in-person attendees only

B) Management Interface Exploits

- **Exploits (zero-day) are sent only if the host returns a valid banner**
  - No banner → No payload
  - Honeypot can't capture the exploit
- **Real hardware is required for observation**
- **But how do we know which device models are being targeted in the first place?**

If infected device spread scans	If infected device doesn't spread scan
✅ Active scan-back	❌ Wait for a incident report
fingerprint device type	From the user or ISP notice

CYBERSECURITY Laboratory

J· 3±u-ғ˟ι

- OEM: ITX Security (Korea)

- Distributed in Japan and overseas
- Vulns reported via JP distributor; patch released
- Patch status via overseas distributors unknown

- Discovered **four previously uknov vulnerabilities**

- **Two were being exploited as zero-days**:
  - ✓Hardcoded backdoor account (CWE-287)
  - ✓OS command injection (CWE-78)

Two Zero-days Exploited by Attackers

Content redacted – available to in-person attendees only

Content redacted – available to in-person attendees only

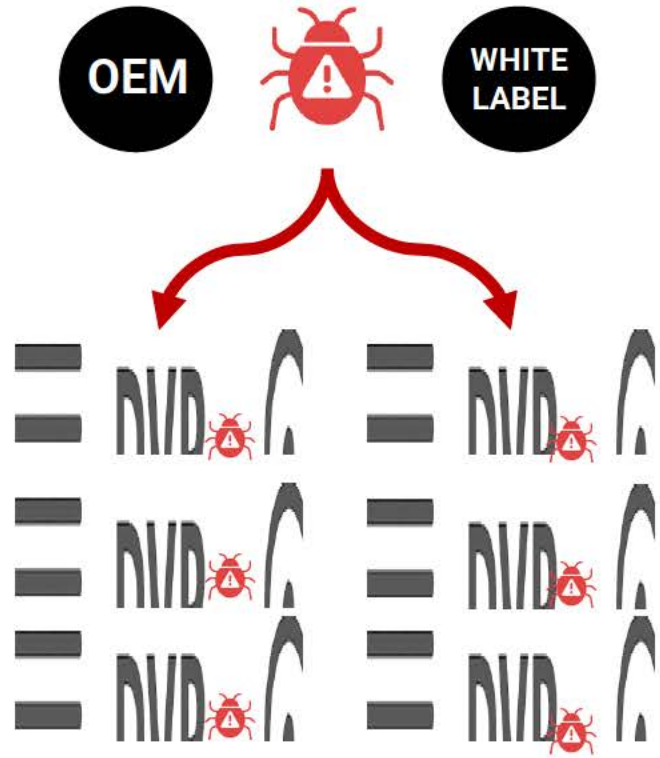
DVRs Keep Getting Targeted: Vulnerable ecosystem

Easy to Hack, Rarely Patched

- **User context**
  - **24/7 online** and **exposed to the internet**
  - Security is often ignored — “if it works, it’s fine”
- **Default Design**
  - **Weak credentials**; **Telnet/HTTP enabled** by default
- **Operational Reality**
  - **Firmware rarely updated**; vulnerabilities left unpatched

Botnets Exploit the Ecosystem

- OEM and white-label DVRs **share common firmware**
- One exploit can impact many vendors across regions
- Patching is fragmented and hard to coordinate



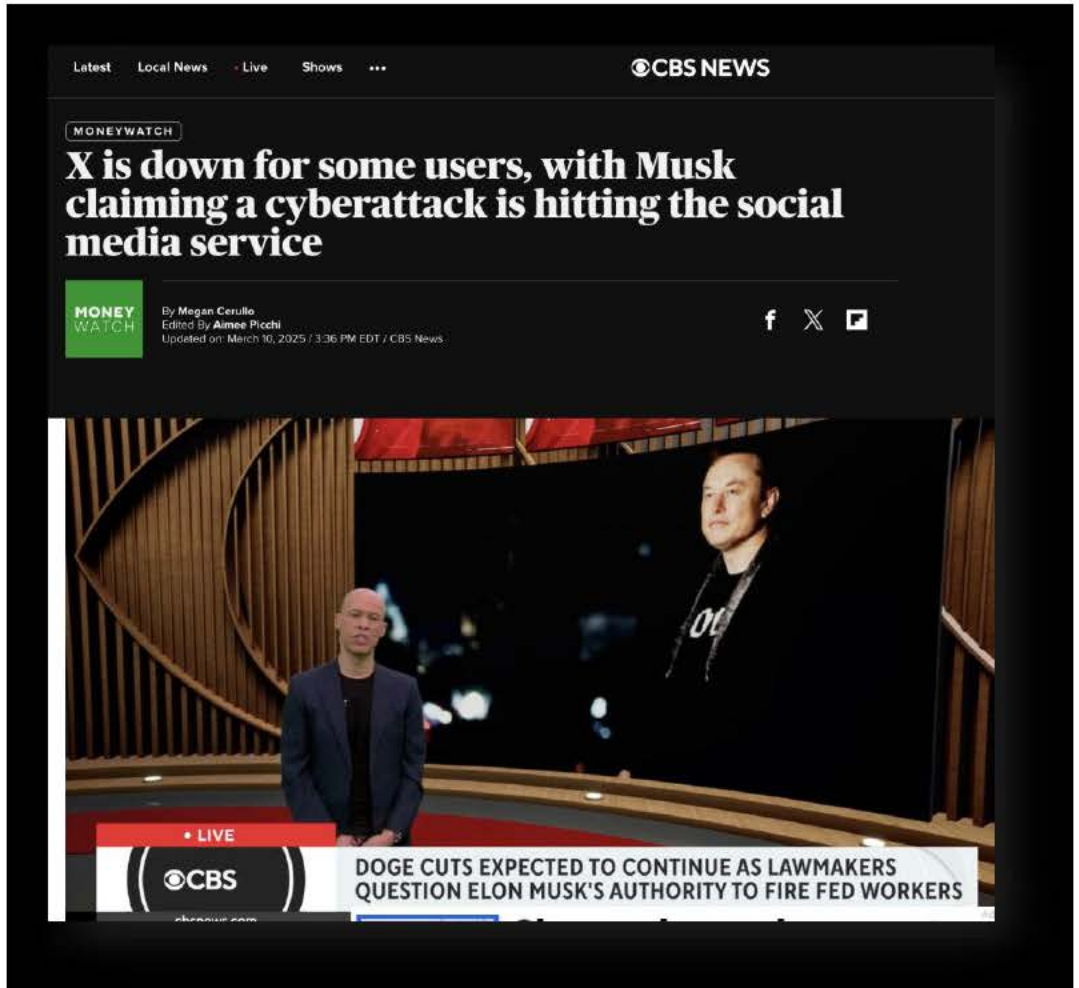
Challenge #3： Analyzing the Evolution and Operation of a Bot Family

Why We Focused on RappeBot

- **Exclusive Targeting Strategy**
  - Only RapperBot exploits ITX/CTRing DVRs
- **Detection-Avoidant Behavior**
  - Avoid spraying payloads; target confirmed devices only
- **Variant-Based Functional Evolution**
  - Multiple variants for different targets and infection vector
- **Infection Trends and Abuse**
  - Persistent infections in Japan, with active use in DDoS campaigns

RapperBot in a Confirmed Attack

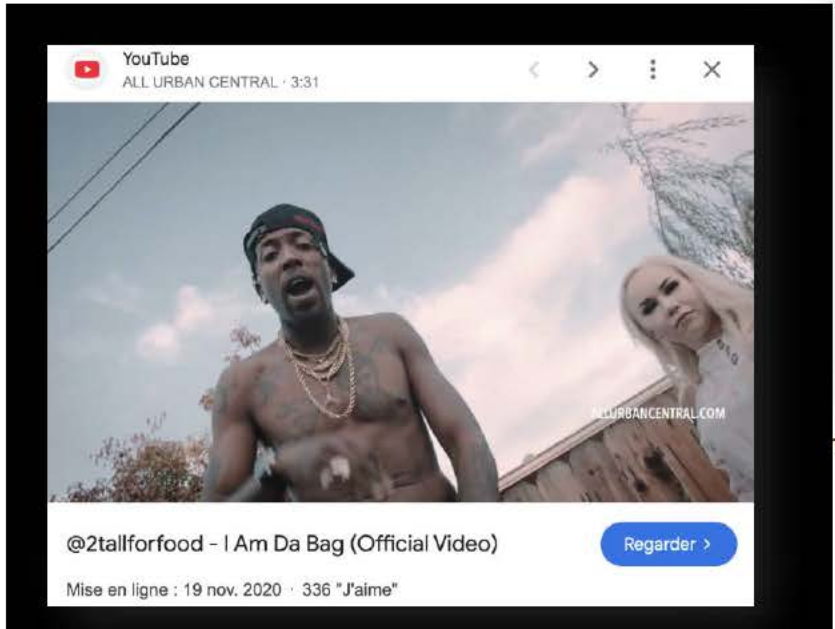
- **RapperBot was used in the March 10 DDoS attack on X, confirmed through our C2 monitoring**



CYBERSECURITY Laboratory

Emergence of RapperBot

- Discovered in June 2022 by CNCERT
- Named derived from a **YouTube video of rappers**
- Based on Mirai source code
- Targets Linux-based IoT devices
- Propagates via SSH brute-force (not Telnet)
- C2 infrastructure overlaps with Fbot, linked to Rippr group



原创 | 预警：新僵尸网络家族正在利用IoT设备构建攻击网络

来源：网络安全应急技术国家工程实验室　时间：2022-07-05　阅读次数：1

作者 | 本报告由CNCERT物联网威胁研究团队与绿盟科技伏影实验室共同发布

一. 概述

1.1 新僵尸网络家族预警

2022年6月22日，我们监测发现一个新的僵尸网络正在利用IoT设备的弱口令构建僵尸网络。根据僵尸网络恶意代码中的url、youtube视频内容以及通信命令特征，我们将这个僵尸网络家族分别命名为RapperBot。截止目前，已发现失陷主机已经超过5000台，但是未监测到攻击者下发任何攻击指令，这说明该僵尸网络仍在持续构建中。

此外，我们注意到RapperBot僵尸网络连接过C2地址2.58.149.116，曾经有一个历史解析域名：dota.lwishiwashappy.eu，该域名在Rippr团伙运营的僵尸网络Fbot中也曾使用过。根据相关威胁情报，Rippr团伙运营着Fbot在内多个僵尸网络家族，该团伙拥有极其丰富的0DAY/NDAY武器库，且参与过针对"北京健康宝攻击事件"以及针对"乌克兰DDoS攻击"在内的多起攻击活动。

以上迹象表明，由RapperBot家族构建的僵尸网络已经成为一个重要的潜在威胁源。

1.2 IoT僵尸网络总体情况

根据CNCERT的监控数据，最近一个月内共监测发现了超过3000个活跃的IoT类僵尸网络C2控制地址，其中有161个级度活跃的C&C地址，控制了大量的失陷主机。其中控制数超过5000台控制主机的C&C占6%，控制数在1000至5000台主机的C&C占21%少于1000台主机的C&C占73%。

https://www.ics-cert.org.cn/portal/page/112/1208496c5e164aceb8dadd08ab993dd2.html

CYBERSECURITY Laboratory

RapperBot – 3-Year Attack Campaign Details

Content redacted – available to in-person attendees only

RapperBot and Mirai: Similarities and Differences

Identical to Mirai

```
void attack_udp_generic(uint8_t targs_len,attack_target *targs,uint8_t opts_len,attack_option *opts)
```

1. Attack function arguments are identical to Mirai

```
#define ATK_OPT_PAYLOAD_SIZE    0   // What should the size of the packet data be?
#define ATK_OPT_PAYLOAD_RAND    1   // Should we randomize the packet data contents?
#define ATK_OPT_IP_TOS          2   // tos field in IP header
#define ATK_OPT_IP_IDENT        3   // ident field in IP header
#define ATK_OPT_IP_TTL          4   // ttl field in IP header
#define ATK_OPT_IP_DF           5   // Dont-Fragment bit set
#define ATK_OPT_SPORT           6   // Should we force a source port? (0 = random)
#define ATK_OPT_DPORT           7   // Should we force a dest port? (0 = random)
```

2. Same option structure as Mirai

- Option 0 = packet data size
- Option 1 = data content
- Option 7 = destination port number

Modified from Mirai

Obfuscated string struct with per-string keys

```
struct table_value {
    char *val;
    uint16_t val_len;
    BOOL locked;
};
```

```
struct table_value {
    uint32_t key;
    char *val;
    uint16_t val_len;
    BOOL locked;
};
```

Password list struct nested by banner

```
struct scanner_auth {
    char *username;
    char *password;
    uint16_t weight_min;
    uint16_t weight_max;
    uint8_t username_len;
    uint8_t password_len;
};
```

```
struct scanner_auth {
    bool_t regular_expression;
    char *banner;
    struct {
        char *username;
        char *password;
    } credentials[100];
    uint32_t entry_count;
};
```

CYBERSECURITY Laboratory

Functional Comparison: RapperBot vs Original Mirai

Function	**RapperBot (ver.2025.02.recon)**	Original Mirai
Scan Target Ports	**36 ports, scan result reporting**	2 ports, scan result reporting
String Obfuscation Method	Per-string single-byte XOR keys	Single global XOR key
Collected Host Data	**Global IP Address*, Hostname, Current directory, Network interface name, MAC address, etc**	N/A
C2 Resolution Method	**TXT record via OpenNIC DNS**	Standard DNS (A record)
C2 Protocol	Structured, XOR-encoded payload	Fixed-format binary, unencrypted
Supported DDoS Methods	11	10

*: RapperBot uses **STUN/3478** to obtain a global ip address

RapperBot Variants by Scanning Behavior

Variant Type	Scanning Behavior	Infection Method	Scan Ports	ID/Password Combos	Target Devices
No-scan	None	external loader	N/A	None	• **ITX DVR** • **CTRing DVR**
Telnet Scanner	Brute-force	Malware installed after successful login	32 (1 random port)	895	• **Huawei HG659 Router** • **Nokia G-010S-A GPON SFP**
SSH Scanner	Brute-force		5	508	• **Hikvison DVR** • **WiMAX Router**
Recon Scanner	Scans for device types only	Sends device info to loader for exploitation	36	N/A	• **Rifatron DVR** • **Shenzhen TVT DVR NVMS-9000**

RapperBot Exploit Arsenal

Content redacted – available to in-person attendees only

Tracking DVRs via Predictable DDNS Hostname

- If the DDNS hostname is derived from the MAC address, attackers can brute-force valid hostnames and track active devices

If your DVR's host name

is Y559469, Your DVR's remote address

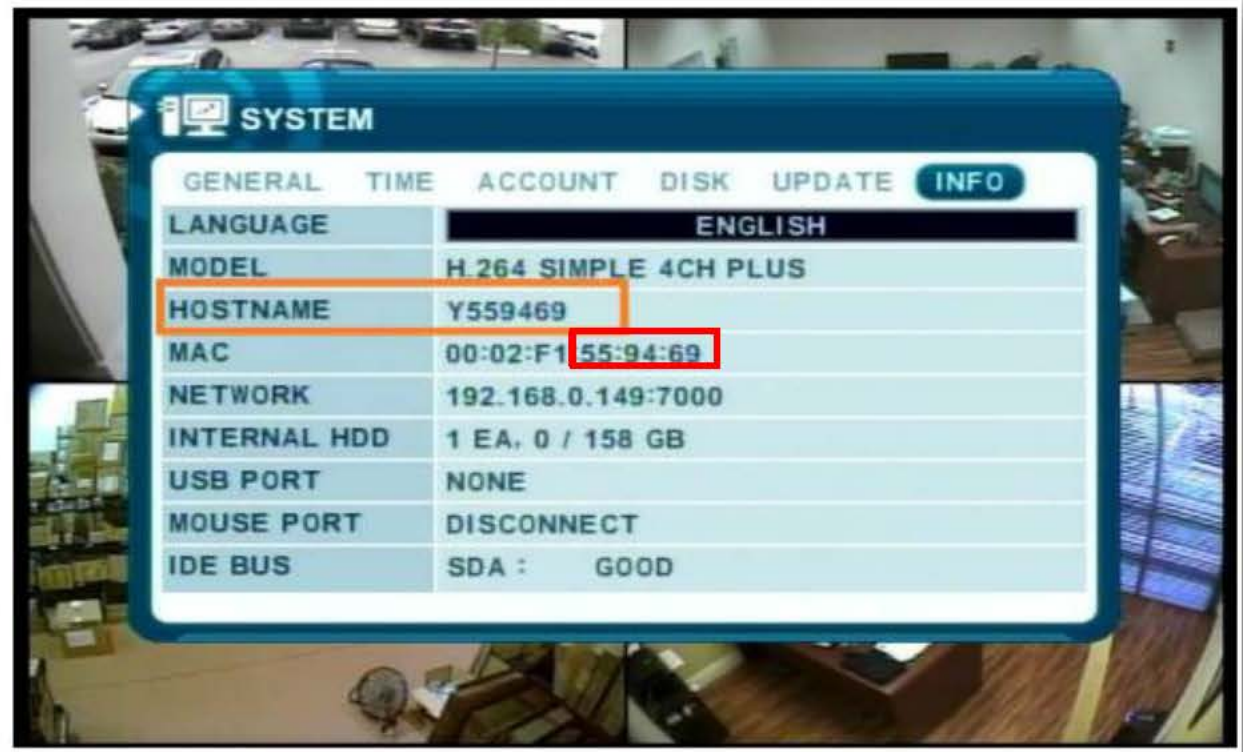
address is **http://Y559469.dvrhost.com:7000**

MAC address **DDNS domain**

BE SURE TO SUBSTITUTE YOUR HOSTNAME FOR THE ADDRESS USED IN THIS EXAMPLE

The remote address will be used in place of **"Host/IP"** in your mobile app and /or web browser.

Port 7000 is the **DEFAULT** port for the iDVR-E series, if you have changed the port to ***any other number***, please use that instead



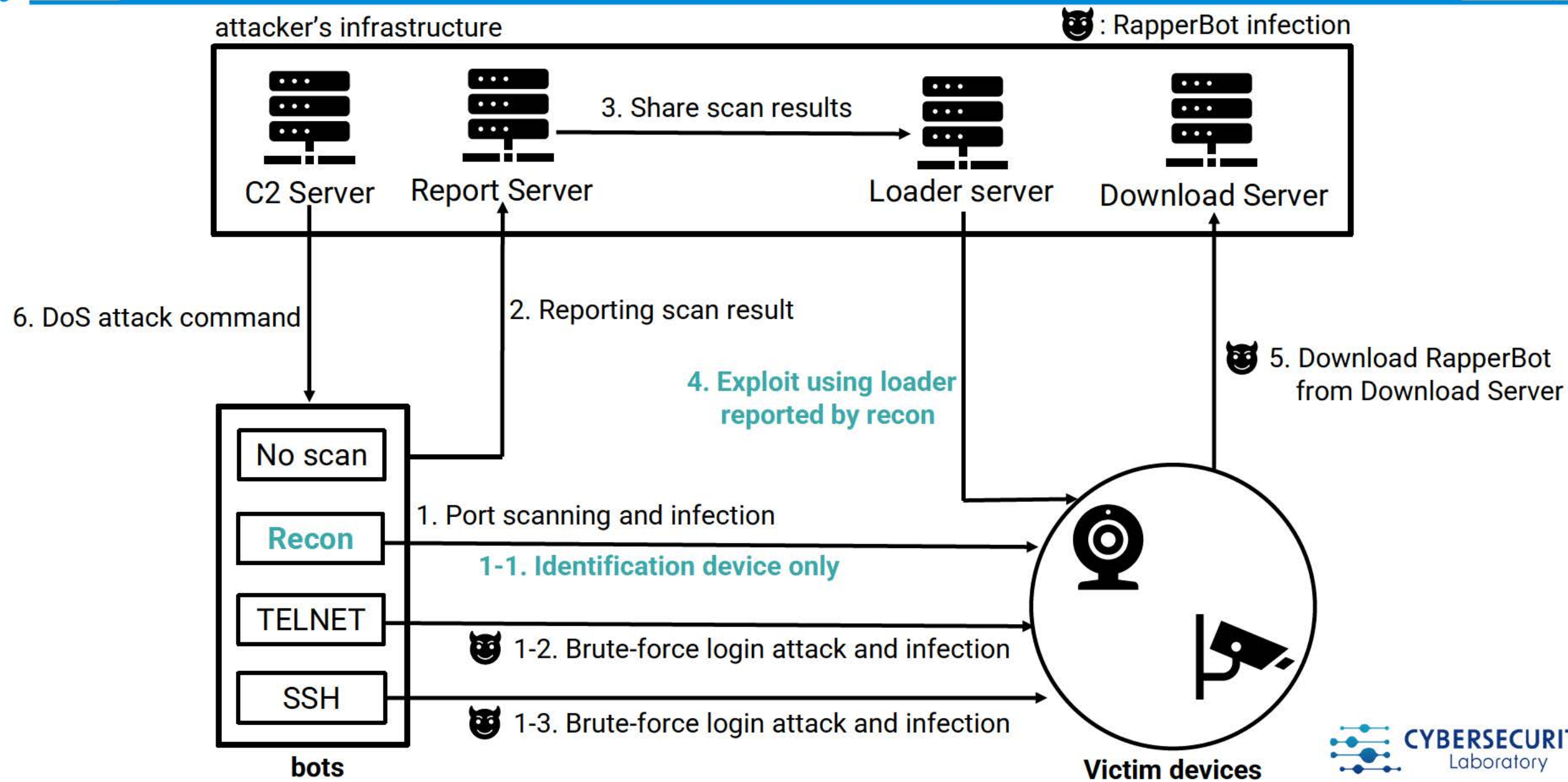
DVR manual (https://videos.cctvcamerapros.com/pdf/surveillance-dvrs/iDVR/iDVR-DDNS-Setup.pdf)

CYBERSECURITY Laboratory

C2 Resolution via OpenNIC and TXT Records

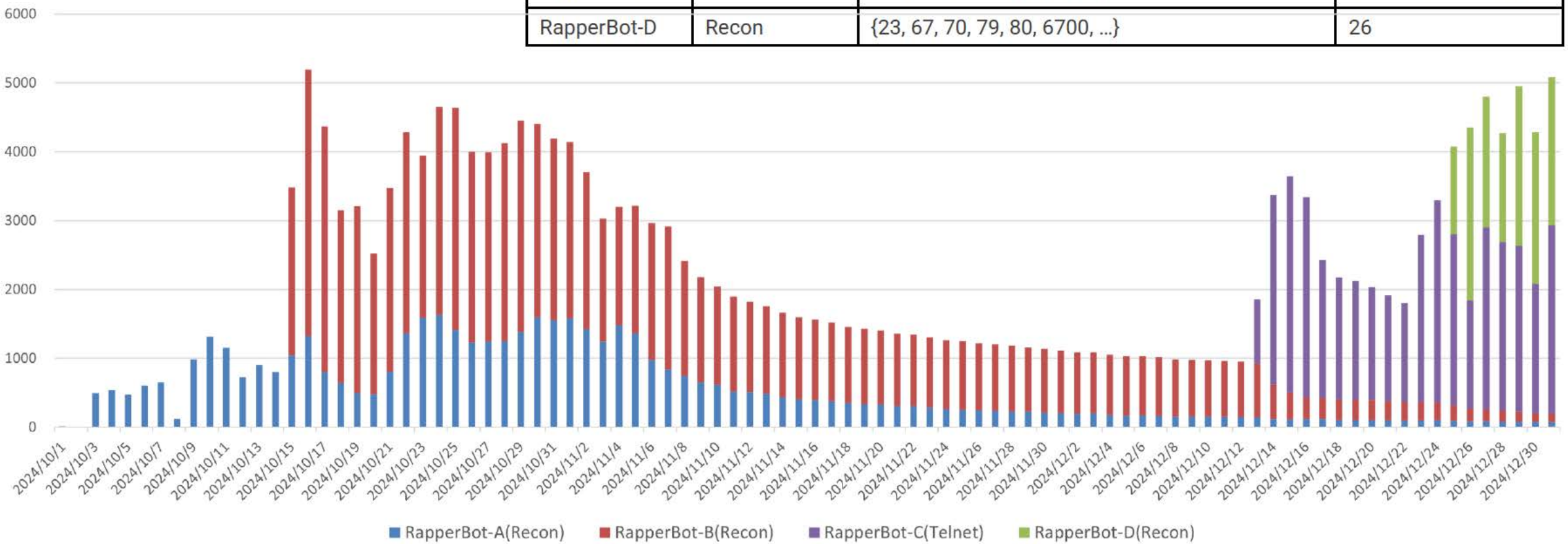
Content redacted – available to in-person attendees only

RapperBot infection strategy



RapperBot Botnet: Infection Timeline

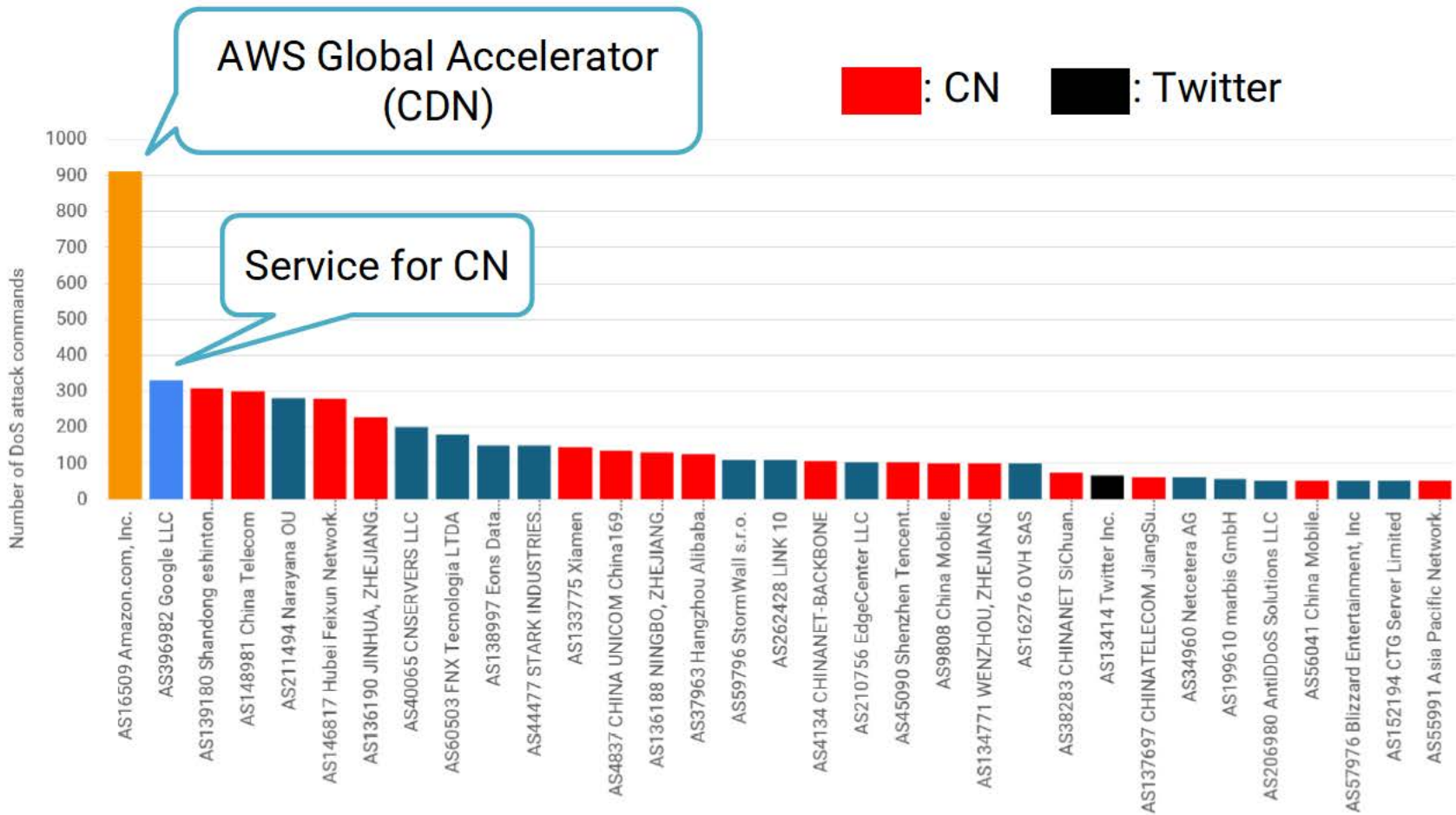
Lable	Variant Type	Scan Ports	Ports
RapperBot-A	Recon	{67, 80, 6700, 8291, 501000, ...}	14
RapperBot-B	Recon	{23, 80, 2051, 34567, 345678, ...}	16
RapperBot-C	Telnet	{23, 26, 254, 523, 1023, ...}	31 + 1 random port
RapperBot-D	Recon	{23, 67, 70, 79, 80, 6700, ...}	26



NOTE: Hosts infected with the No-scan variant are not reflected in this count.

CYBERSECURITY Laboratory

Target Distribution of DDoS Commands (Mar-Apr 2025)



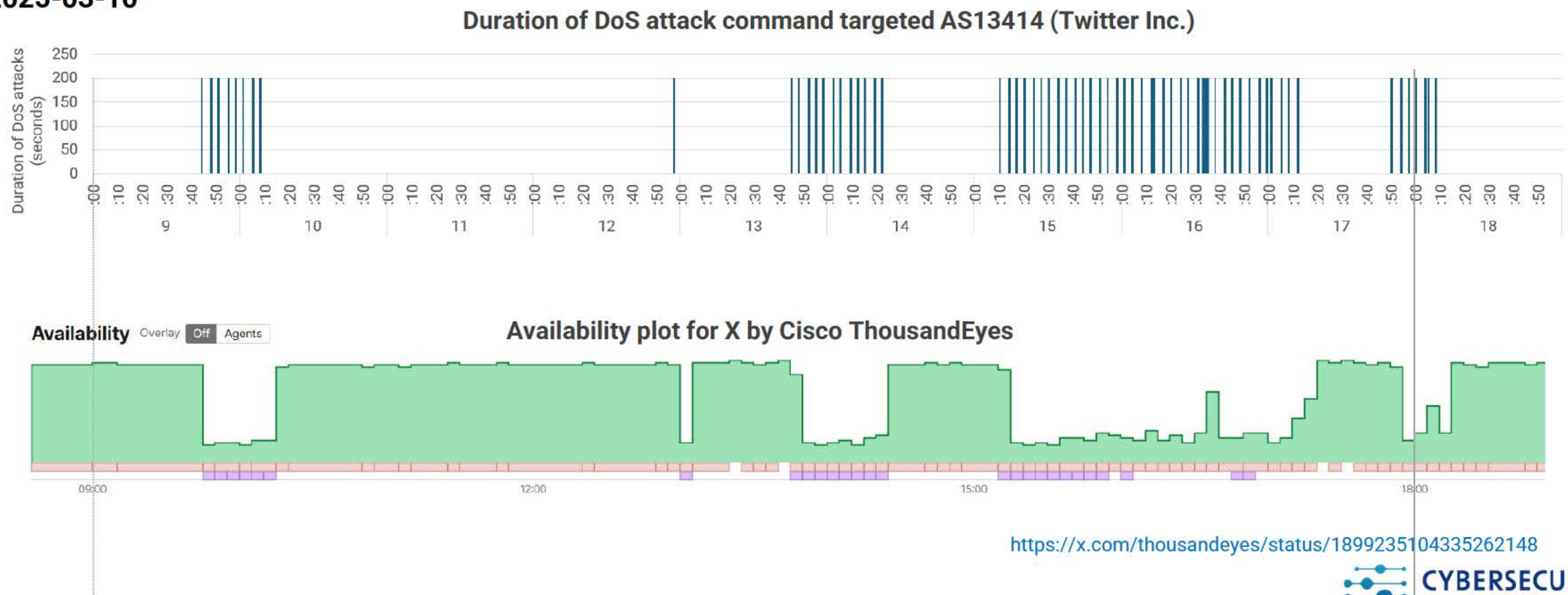
- **Majority of targets were Chinese ASNs**
- **Includes AWS Global Accelerator (Amazon ASN)**
- **GCP infrastructure serving China (confirmed via TLS certs)**
- **Targets run diverse services with no consistent pattern**
  - ✓ e.g., CDN, web, mail, SSH-only

CYBERSECURITY Laboratory

Correlating RapperBot C2 Commands with X Downtime

- RapperBot C2 attack timing exactly aligns with observed outage in ThousandEyes

2025-03-10



https://x.com/thousandeyes/status/1899235104335262148

CYBERSECURITY Laboratory

Conclusion

Vulnerable DVR ecosystem	Vulnerability impacts 28+ vendors
	No fix for distributors, end users
RapperBot's Changing TTPs	C2, recon targets, new zero-days
Toward Mitigation	**Track and analyze RapperBot's new target**
	Global coordinator to reach distributors

Thank you!

Questions?

NICT
Cybersecurity Research Institute

NICTER Blog
blog.nicter.jp

NICTER Analysis Team
@nicter_jp

REFERENCES

Partial IOCs

- Download servers :
  - 95[.]214[.]27[.]202
  - 194[.]180[.]48[.]105
  - zyb[.]ac
  - rppr[.]cc
  - vzxv[.]me
  - 4v[.]wtf
  - o0s[.]cc
  - 6sz[.]ru
- Command and Control servers:
  - ozxxb[.]eu
  - h[.]vzxv[.]me
  - qiap[.]cc
  - helloworld[.]libre
  - dbovmix[.]xyz txt
  - tvoewev[.]link txt
  - keipyeb[.]africa txt
  - dfubdf[.]click txt
  - 194[.]180[.]48[.]105
  - 193[.]32[.]162[.]174
  - nexuszeta[.]lib txt
  - iranistrash[.]libre txt
  - iguessimhere[.]libre txt
  - churchofhollywood[.]libre txt
  - 167[.]99[.]0.202

OpenNIC

- Scan report servers:
  - 158[.]255[.]213[.]225
  - 193[.]31[.]6[.]57
  - 80[.]66[.]77[.]235
  - pool[.]rentcheapcars[.]sbs
  - pool3[.]rentcheapcars[.]sbs
- Monero wallets:
  - 48SFiWgbAaFf75KsRSEEr4i DcxrevFzVmhgfb6Qudss52J K8cCR8bwmUxNBPN2Vmq DTucJL3eabiZc5XRYVGkbh 6BH58Ytk
- Email address:
  - horse@riseup[.]net