Linking IoT Attacks to Cybercrime-as-a-Service Offerings Using LLM and DNS Data

Qingxin MAO[†], Yin MINN PA PA[††], Rui TANABE[††,†††], and Katsunari YOSHIOKA[††,††††]

† Yokohama National University 79–1 Tokiwadai, Hodogaya-ku, Yokohama, 2408501 Japan
†† Institute of Advanced Sciences, Yokohama National University
†††† Graduate School of Environment and Information Sciences, Yokohama National University
††† Juntendo University

E-mail: †mao-qingxin-fp@ynu.jp, ††{yinminn-papa-jp,tanabe-rui-xj,yoshioka}@ynu.ac.jp

Abstract Cyberattack monitoring systems, such as honeypots, typically focus on observing the technical aspects of attacks rather than identifying the attackers themselves. However, linking attacks to Cybercrime-as-a-Service (CaaS) offerings is critical for developing more effective countermeasures and understanding their strategies. This study investigates the hypothesis that attackers reuse their IP addresses not only for attacks but also for other cybercrime-related activities, such as offering CaaS. Using over 20,000 IP addresses associated with IoT-related attacks (e.g., command-and-control servers, malware download servers, and malware loaders), we identified related domains through DNSDB queries. Domain names indicative of cybercrime activities were then extracted using a large language model (LLM). This process uncovered over 1,838 domains containing keywords such as "ddos," "stresser," and "bot." Further analysis of these domains revealed their use in offering DDoS-as-a-Service, selling stolen data, and distributing botnet source code. Our findings demonstrate the potential of linking IoT attacks to CaaS through their infrastructure, offering new insights into cybercriminal operations and enhancing the effectiveness of cybersecurity measures.

Key words IoT Botnet, CaaS, Booter, Stresser, DDoS

1. Introduction

The rise of Internet of Things (IoT) botnets conducting cyberattacks, such as Distributed Denial of Service (DDoS) attacks, has created significant cybersecurity challenges[16], [6]. Traditional monitoring systems [8] have primarily focused on observing attack behaviors and infrastructure components, but they often fail to link attacks back to the attack offerings. Establishing this link is crucial for several reasons: it enables better attribution and understanding of attacker strategies, generates actionable threat intelligence for proactive defense, closes gaps in existing countermeasures, and helps disrupt the economic incentives driving cybercrime. Without this connection, countermeasures remain reactive and limited in scope, addressing symptoms of attacks rather than the root causes.

We hypothesize that attackers reuse their infrastructure—particularly IP addresses linked to IoT attacks—for various cybercriminal activities beyond the attacks themselves. To test this hypothesis, we analyzed over 20,000 IP addresses detected by an IoT honeypot system[8], comprising Command and Control (C&C) servers, IoT malware hosting servers, and IoT malware loader servers. Using DNSDB[11], we identified 554,649 domains associated with these IP addresses. To filter domains related to cybercrime, we employed a large language model (LLM)[7], "gpt-4o-2024-08-06" model, with a customized prompt to analyze not only the presence of cybercrime-related keywords like "c2," "C&C," and "ddos" but also the broader context in which these keywords appear. The LLM evaluates domain names by considering keyword combinations, cybercrime slang, and patterns indicative of services such as DDoS-as-a-Service, botnet rentals, and malware distribution. This contextual analysis reduces false positives by distinguishing legitimate domains from those involved in cybercriminal activities.

From this process, we identified 1,838 domains indicative of cybercrime, which were further analyzed through web content inspection. This analysis confirmed 10 cases of cybercriminal activities, including DDoS-as-a-Service offerings, leaked information sales, and botnet script distribution.

Our contributions include:

(1) Introducing a novel methodology integrating DNS data and LLM-based contextual analysis to link IoT botnet activities to attackers
(2) Providing empirical evidence that attackers exploit their infrastructure for multiple cybercrime services
(3) Demonstrating how our approach can enhance the detection and mitigation of organized cybercriminal activities.

This research advances our understanding of how IoT botnets connect to broader cybercrime ecosystems and highlights actionable paths for improved cybersecurity measures.

2. Methodology

The proposed methodology aims to link attack infrastructure (e.g., IP addresses associated with botnets, malware, or other malicious activities) to potential cybercrime as a service offerings by integrating passive DNS discovery, contextual domain filtering, and web content analysis. While the methodology is designed to be broadly applicable, this study focuses on IoT botnet-related infrastructure. The overall process consists of three key stages: identifying associated domains, filtering cybercrime-related domains through contextual analysis, and retrieving and analyzing relevant web content (Fig 1).

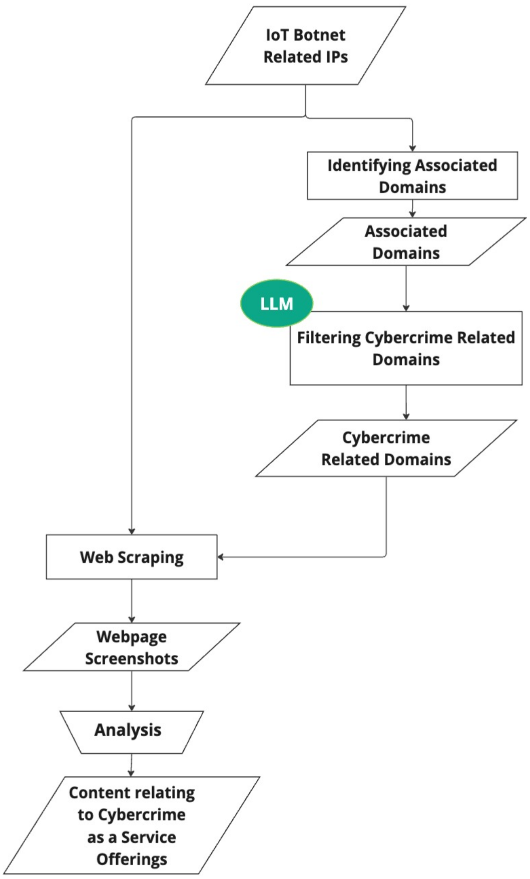

IoT Botnet Related IPs
Identifying Associated Domains
Associated Domains
LLM
Filtering Cybercrime Related Domains
Cybercrime Related Domains
Web Scraping
Webpage Screenshots
Analysis
Content relating to Cybercrime as a Service Offerings

Figure 1 Methodology of Linking IoT Attacks to Cybercrime-as-a-Service Offerings

Step 1 - Identifying Associated Domains: Given our hypothesis that attackers may be using the infrastructure under their control not only for launching attacks but also for other cybercriminal activities—such as offering DDoS attacks as a service—we access the IP addresses related to IoT botnets and retrieve their web content to analyze the nature of their activities. However, while directly accessing these IP addresses is feasible, there is a possibility that the IP addresses of devices under the attackers' control may change, leading to gaps in data collection. Attackers may frequently change the IP addresses of their controlled devices to evade detection, which, while enhancing their concealment, poses the risk of losing customers who purchase their cyberattack services. To mitigate this risk, some attackers may employ fixed domain names, ensuring that customers can locate their web pages even if the underlying IP addresses change. Considering this, our study investigates not only the IP addresses associated with IoT botnets but also the domains linked to them.

Step 2 - Filtering Cybercrime-Related Domains: In the preceding step, we identified domains associated with IoT botnet-related IP addresses for analysis. However, since some IP addresses are shared among many users, it is conceivable that unrelated domains may also be associated with them. For instance, an IP address providing hosting services may typically be associated with over 1,000 domains. To eliminate as many domains unrelated to cybercrime as possible, we employ an LLM in this study to filter them out. The LLM not only checks for the presence of keywords related to cybercrime within the target domains but also analyzes multiple attributes such as the lifespan of the domain, top-level domains (TLDs), and the use of slang, thereby enhancing the reliability of the results.

Step 3 - Web Scraping and Analysis: To understand the activities of attackers, we access the IP addresses and domains under their control and analyze the web content hosted on them. Since each IP address can have over 60,000 ports, accessing all of them is impractical. Therefore, we first investigate which ports are open on the target IP addresses. Based on the investigation results, we access the relevant web ports and proceed with analyzing the content of the web pages obtained.

3. Experiment

In this chapter, we provide a detailed explanation of the specific tools, data, and parameters used in our experiments. All experiments in this study were conducted using Python[9] and Shell Script[10]. The systematic approach and automation facilitated by these tools were essential in handling the large datasets and complex processes involved in our research. The experiment was conducted between October 2024 and January 2025.

Identifying Associated Domains: In this step, we investigate the domains associated with IP addresses related to IoT botnets (Command and Control Servers, Malware Download Servers, and Malware Loaders) observed by IoTPOT[8] using DNSDB[11] . The information stored in DNSDB for each domain includes the timestamps of the first and last observations. Since investigating domains that are too old may not be meaningful, we focus on domains whose last observed timestamp is on or after January 1, 2020, for our analyses.

Filtering Cybercrime-Related Domains: In the previous step, we extracted domains related to IoT botnets using DNSDB. However, these domains are likely to include those unrelated to cybercrime. Therefore, we utilize the OpenAI LLM , ”gpt-4o (gpt-4o-2024-08-06)”[7] model, to extract only the domains associated with cybercrime. To ensure consistency in LLM responses , we set the parameter temperature (which affects the randomness of answers) to 0. Additionally, to have LLM perform accurate extractions, it is necessary to provide precise prompts and examples. We use an LLM prompt to extract domains related to cybercrime, which requires constructing an appropriately designed prompt to ensure accurate extraction.

Initially, we request the LLM to extract domains related to cybercrime. However, ”related to cybercrime” is too broad, so we explicitly specify ”those associated with criminal activities offering DDoS attacks as a service, such as C2 servers and botnets.” To further narrow down the scope of extraction targets, we include a keyword list related to cybercrime in the prompt. This keyword list was also generated by the LLM; using Prompt 1 (Fig 2), we generated approximately 600 keywords, from which we manually extracted 378 that are relevant to this research and included them in Prompt 2 (Fig 3). Finally, to increase the accuracy rate, we present precise examples to the LLM. By extracting three domains that actually provide CaaS and adding them to the prompt, we anticipate that the LLM will extract domains as relevant to actual CaaS as possible. This approach allows LLM to extract domains as accurately as possible.

> Please generate as many keywords related to cybercrime as possible. For example, booter services that offer DDoS attacks, stressers exploited for DDoS attacks, botnet infrastructure (e.g., C&C servers, malware download servers, malware loaders), and types of DDoS attacks such as Layer 4 attacks, Layer 7 attacks, SYN floods, etc.

Figure 2 Prompt 1

Web Scraping & Analysis: We analyze the web content hosted on IP addresses associated with IoT botnets and the domains linked to

> ”Please extract domains from the list below that are likely related to cybercrime activities or businesses. Specifically, look for domains associated with services offering Distributed Denial of Service (DDoS) attacks, botnets, Command and Control (C&C) servers (also referred to as C2 or CNC), malware distribution, and loaders that acquire bot information.
> Common keywords and slang terms that may appear in such domains include:
> ...
> - booter
> - bot
> - c2
> - ddos
>
> ...
> - stresser
>
> ...
> (Omitting the rest, there are over 300 keywords in total.)
> For example:
> - ***stresser.***
> - ***-stresser.***
> - bot.***.***
>
> Please extract domains from the list that contain these keywords or seem to be related to cybercrime activities. Exclude domains that are unlikely to be associated with cybercrime, even if they contain similar patterns.
> Provide the extracted domains, listing one domain per line. If none are found, please respond with ’None’.”

Figure 3 Prompt 2

these IP addresses by accessing them. However, since it is impractical to access all ports of the analysis targets due to the vast number (over 60,000 ports per IP address), we first investigate which ports are open on the IP addresses related to IoT botnets observed by IoTPOT before accessing them. To achieve this, we retrieve information on the IP addresses observed by IoTPOT using Shodan[13] and analyze the port openness status based on that information. Specifically, we retrieve information from Shodan on the IP addresses observed by IoTPOT between October 1, 2024, and November 16, 2024. Furthermore, because the data in Shodan reflects the state at the time of the investigation, we consider the possibility of changes in IP address information. To ensure the accuracy of the information, we retrieve data from Shodan immediately after IoTPOT observes the IP addresses.

After ascertaining the status of the ports opened by the IP addresses associated with the IoT botnet, we proceed to access these addresses to retrieve and analyze their web content. Since web pages may not persist for extended periods due to various reasons—such as attackers’ intentions or takedowns by security agencies—we aim to capture screenshots and web contents of the web pages while they are still current. Accordingly, similar to how we use Shodan to investigate information on IP addresses, we employ headless Chrome with Selenium[12] to automatically access the IoT botnet-related IP addresses observed by IoTPOT daily, obtaining screenshots and web contents. Conversely, for the domains extracted from DNSDB, we access them only once due to time constraints. Furthermore, when acquiring these data, to retrieve all web pages present on the same device while preventing infinite loops, we ensure that external link information is fetched only once.

Then we manually analyze the web contents to investigate the activities in which the attackers are engaged. For example, for attackers who are selling cyberattacks as a service, we specifically investigate what kinds of services they are offering, at what prices they are selling them, and what contact methods they use. By examining these details, we aim to gain a comprehensive understanding of the attackers’ operational behaviors and the scope of their services.

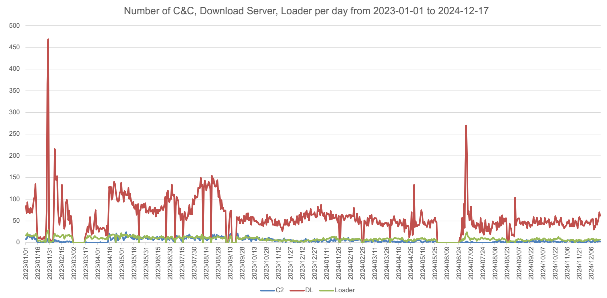


Figure 4 Number of C2 server, Malware Download Server, and Loader observed per day from 2023-01-01 to 2024-12-17

4. Results

In this chapter, we present a detailed analysis of the experimental results.

4.1 Domain Identification via DNSDB

Fig 4 shows the observation results of IoT botnet related IP addresses from January 1, 2023, to December 17, 2024. The horizontal axis represents dates, and the vertical axis represents the number of IP addresses. The blue line indicates the number of C&C server IP addresses, the red line represents the number of Download Server IP addresses, and the green line shows the number of Loader IP addresses. Over these approximately two years, we observed a total of 23,387 IP addresses across these three categories. From Fig 4, it can be seen that the number of Download Servers is overwhelmingly large, and that on average, fewer than 20 C&C servers and Loaders are observed per day. Additionally, observations were halted around March 2023 and June 2024 due to server downtime caused by power outages. By investigating domains associated with 23,387 IP addresses collected by IoTPOT between January 1, 2023, and December 17, 2024, using DNSDB, we identified a total of 554,649 domains.

4.2 Extraction of Cybercrime-Related Domains Using LLM

We utilized DNSDB to obtain 554,649 domains associated with IoT botnets. However, since it is highly probable that these domains include ones unrelated to cybercrime, we employed a Large Language Model (LLM) to extract only the domains pertinent to cybercrime. As a result, we extracted 1,838 domains. Table 1 illustrates the keywords contained within these domains. One important point to note is that the domain count results partially overlap. For example, the 102 domains containing ”botnet” are subsumed within the 321 domains containing ”bot.” Furthermore, given the large number of keywords and the fact that the domain count results for keywords not listed in Table 1 (such as ”CaaS,” ”C&C,” etc.) are mostly zero or near zero, we present only the top 10 keywords in Table 1.

Furthermore, we examined the status of the domains using VirusTotal[15]. The VirusTotal assessment results are presented in Tables 2. In Table 2, the numbers in the first column represent the number of vendors that judged a domain as ”malicious.” Similarly, the third column indicates the number of vendors that judged a domain as ”suspicious.” The second and fourth columns denote the corresponding numbers of domains. For example, in Table 2, there are 43 domains that were judged as ”malicious” by 3 vendors. From Table 2, we observe that the total number of domains classified as ”malicious” is 569, and those classified as ”suspicious” amount to 377.

Notably, multiple domains were flagged by more than one security vendor, indicating the reliability of the LLM's extraction process in identifying potentially harmful domains linked to cybercriminal activities.

Table 1 Keywords contained within domains

Cyber Related Keyword	Domain Count	Example
c2	359	c2***.***
bot	321	*bot**.**
botnet	102	botnet**.**
cnc	88	**cnc.**
dos	42	dos**.**
stress	42	stress**.**
card	42	**card.**
ddos	27	**ddos.**
fullz	18	**-fullz.**
mirai	14	mirai-**.**

Table 2 Results of Investigation by Virustotal

Malicious	Count	Suspicious	Count
1	99	1	196
2	57	2	124
3	43	3	45
11	41	4	12
12	40		
4	35		
9	32		
10	31		
5	29		
13	26		
6	25		
7	25		
15	24		
8	21		
16	15		
14	14		
17	7		
18	4		
19	1		
Total	**569**	**Total**	**377**

Table 3 Type of Ports

C&C Server		Download Server		Loader	
Port Number	Count	Port Number	Count	Port Number	Count
22(SSH)	38	80	168	22	33
80(HTTP)	33	21	167	80	24
3306	20	22	141	111	9
111	18	53(DNS)	127	21	9
21(FTP)	16	2000	83	3306	9
443(HTTPS)	13	5060	64	443	7
3389	10	443	52	53	7
1337	6	23(Telnet)	44	3389	5
8080	6	8291	38	1337	4
445	5	111	35	161	4
5985	5	1701	35	2000	4
135	4	3306	35	8080	4
3128	4	1723	34	2222	3
53	4	7547	27	2323	3
993	4	8080	27	3128	3
110	3	8728	27	33060	3
1234	3	161	24	5000	3
143	3	3389	21	81	3

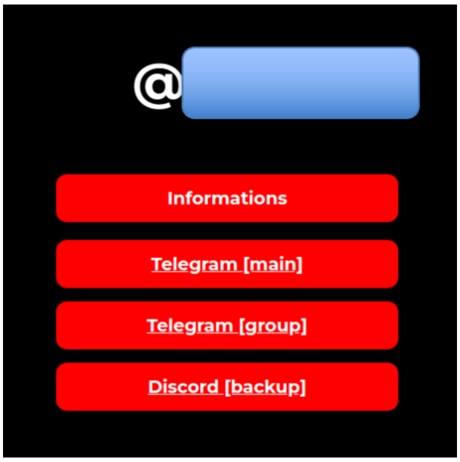


Figure 5 Case 1 - Before

4.3 Web Scraping & Web Contents of Cybercrime Related Domains&IPs

In this study, we accessed the web service ports of IP addresses associated with IoT botnets and the domains linked to these IP addresses to analyze their content. Prior to this analysis, it was necessary to investigate which ports these infrastructures had open. Therefore, we obtained information on the IP addresses observed by IoTPOT using Shodan and analyzed the status of open ports based on this data.

Between October 1, 2024, and November 16, 2024, IoTPOT observed 71 IP addresses associated with Command and Control (C&C) servers, 1,257 IP addresses associated with Download Servers, and 88 IP addresses associated with Loaders. Subsequently, by examining these IP addresses with Shodan, we acquired information on 56 C&C servers, 578 Download Servers, and 54 Loaders. Table 3 presents the port-opening statuses. From Table 3, it became apparent that many devices had ports 80 and 443 open, which are typically used for HTTP and HTTPS services, respectively.

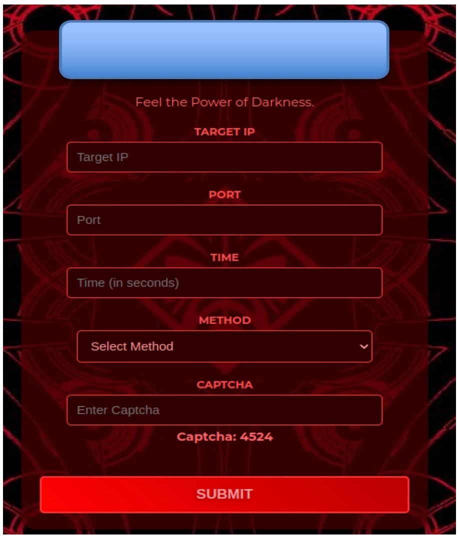
Based on these findings, we accessed ports 80 and 443 of the domains and IoT botnet-related IP addresses. Analyzing the retrieved web content, we discovered a total of ten Cases:

- Eight cases where DDoS attacks were being offered as a service.
- One case involving the sale of leaked information.
- One case of sharing botnet and DDoS attack scripts.

Below, we provide detailed explanations of some of these cases, starting with those offering DDoS attacks as a service.

Case 1: The first case (Fig 5, 6) we identified was obtained when accessing a domain (contained keyword "stresser") presumed to be associated with cybercrime . We initially discovered this case on January 9, 2025. The homepage displayed contact information for Telegram and Discord; however, the invitation links had expired, preventing us from joining the Telegram and Discord channels. When we revisited the site a week later, the content of the webpage had been updated. Upon examining the "Method" section, we found entries listed as "UDP, TCP, DNS," which are presumed to be attack methods. It is inferred that by inputting the attack target and the parameters used for the attack into the blank fields on this web page, an attack can be initiated.

Case 2: The second case was also found through domain access (didn't contain any cybercrime related keywords) . As shown in Fig 7 , the interface included sections labeled "Layer 7 Servers" and "Layer 4 Servers," with status information for servers in various regions listed beneath. This layout closely resembles management dashboards used by other DoS service providers to manage their infrastructure, suggesting a high likelihood that it serves as a demonstration of attack capabilities or a control panel for orchestrating attacks.



[redacted]

Feel the Power of Darkness.

TARGET IP

Target IP

PORT

Port

TIME

Time (in seconds)

METHOD

Select Method

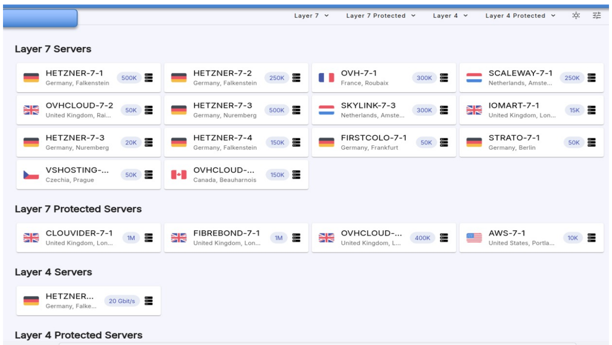
CAPTCHA

Enter Captcha

Captcha: 4524

SUBMIT

Figure 6 Case 1 - After



[redacted]

Layer 7 Servers

HETZNER-7-1 Germany, Falkenstein 500K
HETZNER-7-2 Germany, Falkenstein 250K
OVH-7-1 France, Roubaix 300K
SCALEWAY-7-1 Netherlands, Amste... 250K
OVHCLOUD-7-2 United Kingdom, Rai... 50K
HETZNER-7-3 Germany, Nuremberg 500K
SKYLINK-7-3 Netherlands, Amste... 300K
IOMART-7-1 United Kingdom, Lon... 15K
HETZNER-7-3 Germany, Nuremberg 20K
HETZNER-7-4 Germany, Falkenstein 150K
FIRSTCOLO-7-1 Germany, Frankfurt 50K
STRATO-7-1 Germany, Berlin 50K
VSHOSTING-... Czechia, Prague 50K
OVHCLOUD-... Canada, Beauharnois 150K

Layer 7 Protected Servers

CLOUVIDER-7-1 United Kingdom, Lon... 1M
FIBREBOND-7-1 United Kingdom, Lon... 1M
OVHCLOUD-... United Kingdom, L... 400K
AWS-7-1 United States, Portla... 10K

Layer 4 Servers

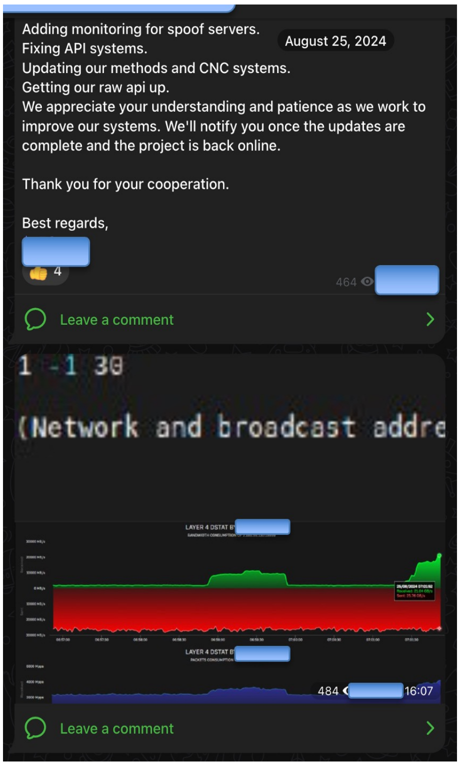
HETZNER... Germany, Falke... 20 Gbit/s

Layer 4 Protected Servers

Figure 7 Case 2

Case 3: The third case (Fig 8), also obtained via domain access, differed from the others in that service information was not displayed on the homepage. The domain name contained the keyword "stress," and the web page included what appeared to be a message from the attacker. This message contained the name of a service, which, upon searching in Google, led us to articles discussing the service. These articles provided information about a Telegram channel operated by the attackers. By joining this Telegram channel, we observed that the attackers were announcing information regarding the potency of their attacks and their targets. For instance, the channel included a post by the administrator from August 2024 showcasing the capabilities of their DDoS attacks. Additionally, this channel has 224 subscribers, the channel's information listed three account names of the operators, through which one could contact them to purchase attacks.

Case 4: In the fourth case, the domain name also contained the keyword "stress," but upon accessing it, we were redirected to another domain. The redirect destination included a Discord invitation link; however, the link had expired, preventing access. The homepage featured a field for entering a key, which presumably would need to be obtained from the attackers through specific means. However, the term "stress" is related to DDoS attacks because it is commonly used to describe tools and services (stressers) that are designed to generate high levels of network traffic for the purpose of stress testing. While legitimate in controlled and authorized environments, these tools are frequently misused by cybercriminals to conduct unauthorized DDoS attacks against targets.



[redacted]

Adding monitoring for spoof servers.
Fixing API systems.
Updating our methods and CNC systems.
Getting our raw api up.
We appreciate your understanding and patience as we work to improve our systems. We'll notify you once the updates are complete and the project is back online.

Thank you for your cooperation.

Best regards,
[redacted]

August 25, 2024

👏 4 464 👁 [redacted]

Leave a comment

1 -1 30

(Network and broadcast addre

LAYER 4 DSTAT BY [redacted]

LAYER 4 DSTAT BY [redacted]

484 👁 [redacted] 16:07

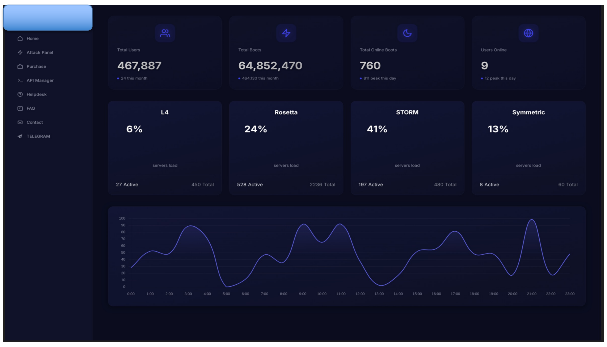
Leave a comment

Figure 8 Case 3 - Telegram Channel

Case 5: The fifth case was discovered by directly accessing an IP address. This case involved the offering of DDoS attacks as a service, with detailed information such as types of attacks and pricing clearly stated on the homepage. This case not only offers five types of attacks—SynAck, DNS, UDP, NTP, and ZSYN—but distinctively also provides the "OVH Method," and furthermore, it is capable of bypassing Cloudflare. The pricing was as follows: Standard plan - $7 per month, Enterprise plan - $50 per month, Commercial plan - $180 per month. However, in order to investigate the payment methods facilitated by the attackers, we attempted to click on the "Purchase" button, but there was no response. Contact information was provided at the bottom of the page. However, when attempting to access the contact links, we could only reach an account on platform X (formerly Twitter), which appeared inactive, with the last post dating back to March 2021. Revisiting the website a few days later, we found that it was no longer accessible.

Case 6: The sixth case (Fig 9), also found by direct IP address access, similarly offered DDoS attack services with explicit details on attack types, pricing, and operational status displayed on the homepage. In this case, three types of attacks—TCP, UDP, and DNS—are offered, with attack services priced at approximately 20 dollars. However, details such as the service duration are not specified, and the three available plans provided are all identical. Furthermore, clicking on them elicited no response. Contact information included a Telegram handle and an email address. Upon joining the Telegram channel, we found only five members and no posts. Notably, we first observed this case in October 2024, and upon revisiting in January 2025, the web page was still operational, making it a rare instance with a prolonged active period.

Case 7: The seventh case (Fig 10), discovered through direct IP address access, explicitly provided information related to attack services. In this case, two plans are offered: the "Discord Bot Plan" at $15 per month and the "API Plan" at $20 per month. However, similar to Cases 5 and 6, there was no response when we pressed the purchase button. While contact links were provided, attempting to click them yielded no response. We first observed this case on November 16, 2024. However, when we accessed it again a week later, the web page had been taken down.


[redacted]

- Home
- Attack Panel
- Purchase
- API Manager
- Helpdesk
- FAQ
- Contact
- TELEGRAM

Total Users 467,887 • 24 this month

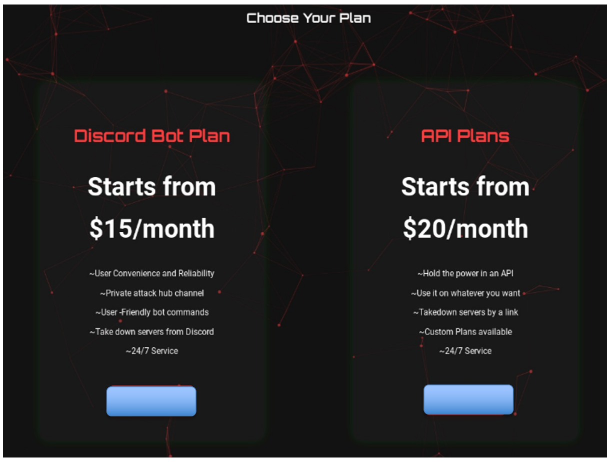
Total Boots 64,852,470 • 464,130 this month

Total Online Boots 760 • 811 peak this day

Users Online 9 • 12 peak this day

L4	Rosetta	STORM	Symmetric
6%	24%	41%	13%
servers load	servers load	servers load	servers load
27 Active 450 Total	528 Active 2236 Total	197 Active 480 Total	8 Active 60 Total

Figure 9 Case 6


Choose Your Plan

Discord Bot Plan

Starts from $15/month

~User Convenience and Reliability
~Private attack hub channel
~User -Friendly bot commands
~Take down servers from Discord
~24/7 Service

[redacted]

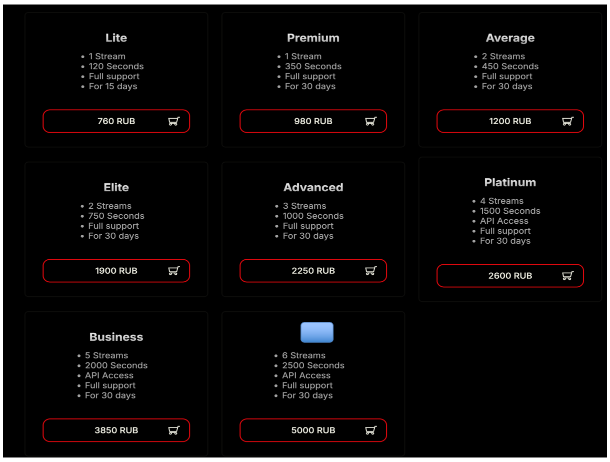
API Plans

Starts from $20/month

~Hold the power in an API
~Use it on whatever you want
~Takedown servers by a link
~Custom Plans available
~24/7 Service

[redacted]

Figure 10 Case 7


Lite
- 1 Stream
- 120 Seconds
- Full support
- For 15 days

760 RUB

Premium
- 1 Stream
- 350 Seconds
- Full support
- For 30 days

980 RUB

Average
- 2 Streams
- 450 Seconds
- Full support
- For 30 days

1200 RUB

Elite
- 2 Streams
- 750 Seconds
- Full support
- For 30 days

1900 RUB

Advanced
- 3 Streams
- 1000 Seconds
- Full support
- For 30 days

2250 RUB

Platinum
- 4 Streams
- 1500 Seconds
- API Access
- Full support
- For 30 days

2600 RUB

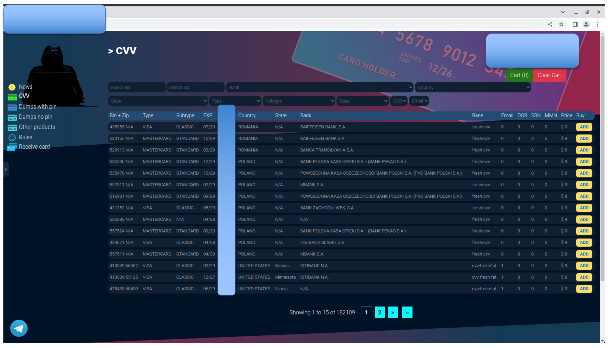
Business
- 5 Streams
- 2000 Seconds
- API Access
- Full support
- For 30 days

3850 RUB

[redacted]
- 6 Streams
- 2500 Seconds
- API Access
- Full support
- For 30 days

5000 RUB

Figure 11 Case 8 - Price


[redacted]

> CVV

[redacted]

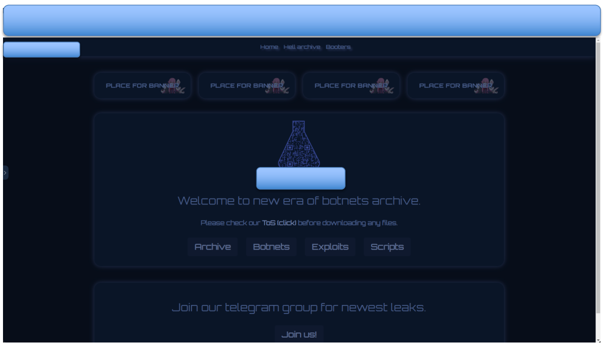
Cart (0) Clear Cart

- News
- CVV
- Dumps with pin
- Dumps no pin
- Other products
- Rules
- Receive card

Bin + Zip	Type	Subtype	EXP	[redacted]	Country	State	Bank	Base	Email	DOB	SSN	MMN	Price	Buy
438955 N/A	VISA	CLASSIC	07/29	[redacted]	ROMANIA	N/A	RAIFFEISEN BANK, S.A.	fresh-cvv	0	0	0	0	$ 9	ADD
533155 N/A	MASTERCARD	STANDARD	10/29	[redacted]	ROMANIA	N/A	RAIFFEISEN BANK S.A.	fresh-cvv	0	0	0	0	$ 9	ADD
529913 N/A	MASTERCARD	STANDARD	03/29	[redacted]	ROMANIA	N/A	BANCA TRANSILVANIA S.A.	fresh-cvv	0	0	0	0	$ 9	ADD
535230 N/A	MASTERCARD	STANDARD	12/29	[redacted]	POLAND	N/A	BANK POLSKA KASA OPIEKI S.A. - (BANK PEKAO S.A.)	fresh-cvv	0	0	0	0	$ 9	ADD
535470 N/A	MASTERCARD	STANDARD	10/29	[redacted]	POLAND	N/A	POWSZECHNA KASA OSZCZEDNOSCI BANK POLSKI S.A. (PKO BANK POLSKI S.A.)	fresh-cvv	0	0	0	0	$ 9	ADD
557511 N/A	MASTERCARD	STANDARD	02/29	[redacted]	POLAND	N/A	MBANK S.A.	fresh-cvv	0	0	0	0	$ 9	ADD
516931 N/A	MASTERCARD	STANDARD	09/29	[redacted]	POLAND	N/A	POWSZECHNA KASA OSZCZEDNOSCI BANK POLSKI S.A. (PKO BANK POLSKI S.A.)	fresh-cvv	0	0	0	0	$ 9	ADD
421352 N/A	VISA	CLASSIC	05/29	[redacted]	POLAND	N/A	BANK ZACHODNI WBK, S.A.	fresh-cvv	0	0	0	0	$ 9	ADD
535693 N/A	MASTERCARD	N/A	04/28	[redacted]	POLAND	N/A	N/A	fresh-cvv	0	0	0	0	$ 9	ADD
557524 N/A	MASTERCARD	STANDARD	09/28	[redacted]	POLAND	N/A	BANK POLSKA KASA OPIEKI S.A. - (BANK PEKAO S.A.)	fresh-cvv	0	0	0	0	$ 9	ADD
424671 N/A	VISA	CLASSIC	04/28	[redacted]	POLAND	N/A	ING BANK SLASKI, S.A.	fresh-cvv	0	0	0	0	$ 9	ADD
557511 N/A	MASTERCARD	STANDARD	04/30	[redacted]	POLAND	N/A	MBANK S.A.	fresh-cvv	0	0	0	0	$ 9	ADD
410039 66062	VISA	CLASSIC	02/29	[redacted]	UNITED STATES	Kansas	CITIBANK N.A.	cvv-fresh-fat	1	0	0	0	$ 9	ADD
410039 55125	VISA	CLASSIC	12/27	[redacted]	UNITED STATES	Minnesota	CITIBANK N.A.	cvv-fresh-fat	1	0	0	0	$ 9	ADD
478433 60430	VISA	CLASSIC	06/29	[redacted]	UNITED STATES	Illinois	N/A	cvv-fresh-fat	1	0	0	0	$ 9	ADD

Showing 1 to 15 of 182109 | 1 2 > »

Figure 12 Case 9


[redacted]

[redacted] Home Hell archive Booters

PLACE FOR BANNER PLACE FOR BANNER PLACE FOR BANNER PLACE FOR BANNER

[redacted]

Welcome to new era of botnets archive.

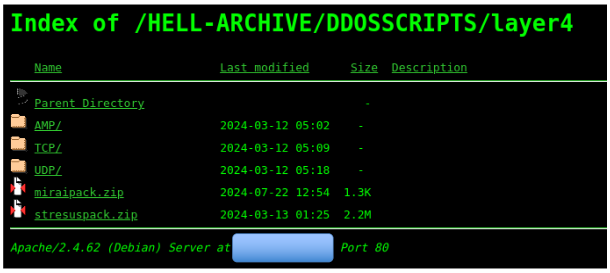
Please check our ToS (click) before downloading any files.

Archive Botnets Exploits Scripts

Join our telegram group for newest leaks.

Join us!

Figure 13 Case 10 - Webpage


```
Index of /HELL-ARCHIVE/DDOSSCRIPTS/layer4

  Name                       Last modified      Size  Description

  Parent Directory                                -
  AMP/                       2024-03-12 05:02     -
  TCP/                       2024-03-12 05:09     -
  UDP/                       2024-03-12 05:18     -
  miraipack.zip              2024-07-22 12:54   1.3K
  stresuspack.zip            2024-03-13 01:25   2.2M

Apache/2.4.62 (Debian) Server at [redacted] Port 80
```

Figure 14 Case 10 - DDoS Script

Case 8: The eighth case (Fig 11) was initially discovered in 2023 by another researcher within our team. As of the current study, the web page remains operational using our access methods. Similar to other cases offering DDoS attack services, the site provided information about the attacks and contact details. Joining the Telegram channel listed as the contact point, we found that the channel had 210 members. Furthermore, this case offers 8 plans, providing 3 Layer 7 methods and 15 Layer 4 methods [For example: TCP-ACK(Tcp ACK Flag flood), UDP-PPS(UDP Flood with high PPS etc.)]. Additionally, it provides an API along with an API manual. Upon proceeding to the purchase phase, a total of five payment methods (Cryptocurrenty(BTC,LTC,etc.), CryptoBot(Any), Card(RUB), Card(UAH), Other) are offered, and it is possible to advance to the actual payment stage.

Case 9: The ninth case (Fig. 12) was identified when accessing a domain containing the keyword "fullz". The site specifically offered credit card details and bank account information for sale and used cryptocurrency for transactions, displaying the attacker's Bitcoin address. Analysis of the screenshots obtained via Selenium revealed that this website is associated with over 200 domains out of the 1,838 domains we discovered through DNSDB, indicating that the sellers were investing significant resources in extensive advertising. These 200 domains included keywords such as "card" and "fullz," referring to a complete set of an individual's personally identifiable information (PII) and all are active at the time is our scraping. Additionally, the web page featured a Telegram contact, which, upon clicking, was found to lead to an automated sales bot rather than a standard communication channel.

Case 10: The final case (Fig 13, 14) was discovered via domain access, where botnet scripts and DDoS attack scripts were being shared freely. The content included code related to the Mirai botnet, Layer 4 and Layer 7 DDoS attack scripts, and various other malicious codes. Upon joining the Telegram channel listed on the homepage, we found 1,253 members actively engaged. The channel was announcing new domains approximately every half month, indicating ongoing activity and updates.

From these cases, we deduced that attackers are utilizing the infrastructure under their control not only to launch attacks but also to engage in various cybercriminal activities. This includes offering attack services, selling stolen information, and distributing malicious tools.

It is important to note that due to ethical considerations and safety protocols, our research strictly avoided any actions that could negatively impact society. We did not engage in executing or purchasing attacks, nor did we interact in ways that would support or facilitate cybercriminal activities. All interactions were limited to passive observations and data collection necessary for the analysis. All activities conducted in this research adhered to ethical guidelines and legal regulations, ensuring that no harm was caused to any systems or individuals.

5. Discussion

5.1 Key Findings and Contributions

This study demonstrates the feasibility of linking IoT botnet infrastructures to broader cybercrime operations through a novel combination of DNS data analysis and LLM-based contextual domain filtering. By uncovering 10 significant cases, including DDoS-as-a-Service offerings, stolen data sales, and botnet script distributions, we provide actionable insights into how attackers exploit their existing infrastructures. These findings highlight that IoT-based attack infrastructures are multipurpose, supporting both direct attacks and monetization through Cybercrime-as-a-Service (CaaS) offerings. Our methodology addresses limitations in traditional approaches that rely on static keyword matching or manual inspection by introducing LLM-based contextual filtering. This enables detection of not only obvious cybercrime-related terms but also evolving slang and domain patterns.

5.2 Practical and Strategic Implications

The domains identified in this study offer immediate applications for threat intelligence, aiding security practitioners in developing blocklists or signatures for intrusion detection systems. Additionally, law enforcement agencies can use these findings to map out attacker networks and disrupt key infrastructure. Understanding how attackers coordinate services like DDoS campaigns through domains and Telegram channels allows defenders to better predict and thwart malicious operations.

5.3 Limitations and Opportunities for Improvement

Several limitations are inherent to this study. The domain extraction depends on the accuracy of the LLM's prompt design and the chosen keyword list.Additionally, web scraping was limited to ports 80 and 443, which may have excluded domains or services hosted on non-standard ports. Expanding the scope of port analysis could reveal hidden services. Lastly, the transient nature of CaaS services poses a challenge, as some identified domains or services may become inaccessible before further analysis is possible. Continuous monitoring is crucial to address this limitation.

6. Related Work

In recent years, IoT botnets conducting cyberattacks such as DDoS attacks have become a significant threat, making it an urgent issue to understand their operational realities. Antonakakis *et al.* [1] presented the growth, composition and evolution of Mirai botnet. They identified 33 C&C clusters that shared no infrastructure and estimated their relative size using different datasets. Bastos *et al.* [2] analyzed Bashlite and Mirai's C&C servers, showing that most of them were seen only for a few days, and that 84% of them were hosted in cloud providers. Tanabe *et al.* [14] investigated how binaries, download servers and C&C servers are related to each other, revealing how they evolve over time and how attackers source their IP addresses. Davanian *et al.* [3] developed a milker tool to connect to C&C servers and disclose their activities in live.

In our previous research, we analyzed IoT botnet attack activities by grouping attack infrastructures based on observations from honeypots, dynamic malware analysis, and pseudo-bot scripts [4]. We then expanded our approach to include loaders—specialized systems that infiltrate vulnerable devices and convert them into bots [5]. Additionally, we refined the grouping method by restricting the use of C&C server data to only those host groups that had actively issued attack commands. By feeding observed attack commands (gathered via pseudo-bot scripts) into bot specimens in an analysis environment, we explored the DoS attack capabilities of these bots. Correlating these results with the grouping data, we revealed the actual DoS attack potential of IoT botnets.

While these works show interesting findings on the IoT botnet, primarily works focused on the attacks and the devices involved, without addressing the relationship between the attacks and the attackers themselves. Therefore, it remains unclear if the attackers are utilizing their infrastructure for other cybercriminal activities beyond executing attacks. This study focuses on linking attacks to their attackers. We targeted over 20,000 IP addresses associated with IoT botnet-related attacks, including C&C servers, malware download servers, and loaders. Using DNSDB, we gathered domains linked to these IP addresses and employed a Large Language Model (LLM) to identify domains associated with cybercrime. Additionally, we analyzed the web content hosted on these domains IP addresses to gain insight into the attackers' activities. Although this study only investigated a portion of Cybercrime-as-a-Service (CaaS) available on the Internet, it demonstrates the possibility of linking attacks to CaaS offerings starting by analyzing the devices under the attackers' control. This work represents a first step in analyzing cybercrime from a new perspective and is expected to contribute to proposing effective countermeasures against cybercrime.

7. Conclusion

This study presents a novel methodology to link IoT botnet-related infrastructures to broader cybercrime activities by integrating DNS data with LLM-based contextual analysis. We successfully identified 1,838 domains related to cybercrime and uncovered 10 cases involving CaaS operations. The results demonstrate that IoT botnet infrastructures are not limited to launching attacks but serve as part of a broader ecosystem supporting various cybercriminal enterprises. Our work highlights the importance of leveraging large-scale DNS data and contextual analysis to reveal previously hidden cybercrime operations. This research provides a foundation for improving cyber defense strategies by linking attack infrastructures directly to their operational outcome.

Acknowledgments: This research was achieved through commissioned research (JPJ012368C05201) by the National Institute of Information and Communications Technology (NICT), Japan. This study includes outcomes obtained from the commissioned research (JPJ012368C08101) by the National Institute of Information and Communications Technology (NICT), Japan. Additionally, this research incorporates results from the commissioned project "Research and Development on IoT Malware Neutralization/Inactivation Technologies for Effective Utilization of Radio Waves," conducted under the Ministry of Internal Affairs and Communications' "Research and Development for Expansion of Radio Wave Resources (JPJ000254)."

References

[1] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)*, pages 1093–1110, 2017.

[2] Gabriel Bastos, Artur Marzano, Osvaldo Fonseca, Elverton Fazzion, Cristine Hoepers, Klaus Steding-Jessen, Marcelo H.P.C. Chaves, Italo Cunha, Dorgival Guedes, and Wagner Meira Jr. Identifying and characterizing bashlite and mirai c2c servers. In *ISCC 2019*, Barcelona, Spain, 2019.

[3] Ali Davanian, Michail Faloutsos, and Martina Lindorfer. C2miner: Tricking iot malware into revealing live command & control servers. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security*, pages 112–127, 2024.

[4] Yuki Endo, Kaichi Sameshima, Rui Tanabe, Katsunari Yoshioka, and Tsutomu Matsumoto. Analysis of iot botnet activities based on attack commands collected via botnet milker scripts. *Computer Security Symposium 2023*, pages 909–915, 2023.

[5] Yuki Endo, Rui Tanabe, Katsunari Yoshioka, and Tsutomu Matsumoto. Enhanced analysis of iot botnet activity by fusing honeypots, malware dynamic analysis, and cc observation. *ICSS*, 2024(12):1–6, 2024.

[6] NTTEAST. What are the damage cases of ddos attacks? an introduction to risks posed by attacks and countermeasures against damage. `https://business.ntt-east.co.jp/service/securitypackage/column/cybermimamori_ddos_none/index.html`, 2024. Accessed: 2025-01-15.

[7] OpenAI. `https://openai.com/`, 2025.

[8] YIN MINN PA PA, SHOGO SUZUKI, KATSUNARI YOSHIOKA, TSUTOMU MATSUMOTO, and CHRISTIAN ROSSOW TAKAHIRO KASAMA. Iotpot: A novel honeypot for revealing current iot threats. *Journal of Information Processing*, 24(3):522–533, 2016.

[9] Python. `https://www.python.org/`, 2025.

[10] Shell Script. `https://www.shellscript.sh/`, 2025.

[11] Farsight Security. DNSDB. `https://www.domaintools.com/products/farsight-dnsdb/`, 2025.

[12] Selenium. `https://www.selenium.dev/`, 2025.

[13] SHODAN. `https://www.shodan.io/dashboard`, 2025.

[14] Rui Tanabe, Tatsuya Tamai, Akira Fujita, Ryoichi Isawa, Katsunari Yoshioka, Tsutomu Matsumoto, Carlos Gañán, and Michel Van Eeten. Disposable botnets: examining the anatomy of iot botnet infrastructure. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–10, 2020.

[15] VirusTotal. `https://www.virustotal.com/gui/home/search`, 2025.

[16] LAC WATCH. Distributed denial-of-service (ddos) attacks: A comprehensive analysis of incident cases, mitigation methods, attack objectives, and typologies. `https://www.lac.co.jp/lacwatch/service/20230619_003412.html`, 2023. Accessed: 2025-01-15.