Multilingual ZIP Phishing Campaigns Targeting Financial and Government Organizations Across Asia

Recent phishing operations across East and Southeast Asia use multilingual ZIP file lures and shared web templates to target government and financial organizations. These operations are characterized by multilingual web templates, region-specific incentives, and adaptive payload delivery mechanisms, demonstrating a clear shift toward scalable and automation-driven infrastructure.

To measure the scope, we pulled fresh data from Hunt.io using AttackCapture™ and the HuntSQL™ datasets, then correlated multilingual phishing pages across regions.

Using HuntSQL-based pivoting, we identified multiple interconnected clusters that reveal how adversaries recycle the same web components (scripts, titles, and file naming conventions) across diverse languages such as Chinese, Japanese, and English.

This research aims to trace these interconnected campaigns, map their thematic overlaps, and uncover how a single infrastructure supports a broad-spectrum phishing ecosystem targeting corporate, governmental, and financial entities throughout Asia.

Before going deeper into each cluster, here are the main findings at a glance.

Key Takeaways

- A total of 28 webpages were identified across three clusters (12 Chinese, 12 English, 4 Japanese) with shared design and functionality.
- Unified backend logic using download.php and visitor_log.php scripts indicates automated deployment.
- Language segmentation shows targeted adaptations for Chinese, English, and Japanese audiences.
- Shift from localized to multinational targeting, expanding from Taiwan, Indonesia, and China to Japan and Southeast Asia.
- Consistent use of ZIP/RAR file lures with bureaucratic, payroll, and tax-related filenames supports phishing-driven malware delivery.
- Evidence of infrastructure reuse, suggesting a single operator or toolkit maintaining multiple campaigns.
- Mapped to ATT&CK across Recon, Resource Development, Initial Access, Execution, C2, Collection, and Defense Evasion.

These overlaps align with earlier research that documented similar phishing waves in the region, providing context for how the current campaign evolved.

Background Reference

In early 2025, FortiGuard Labs documented a coordinated, multi-stage campaign that evolved from the deployment of Winos 4.0 in Taiwan to the distribution of the HoldingHands malware family across East and Southeast Asia.

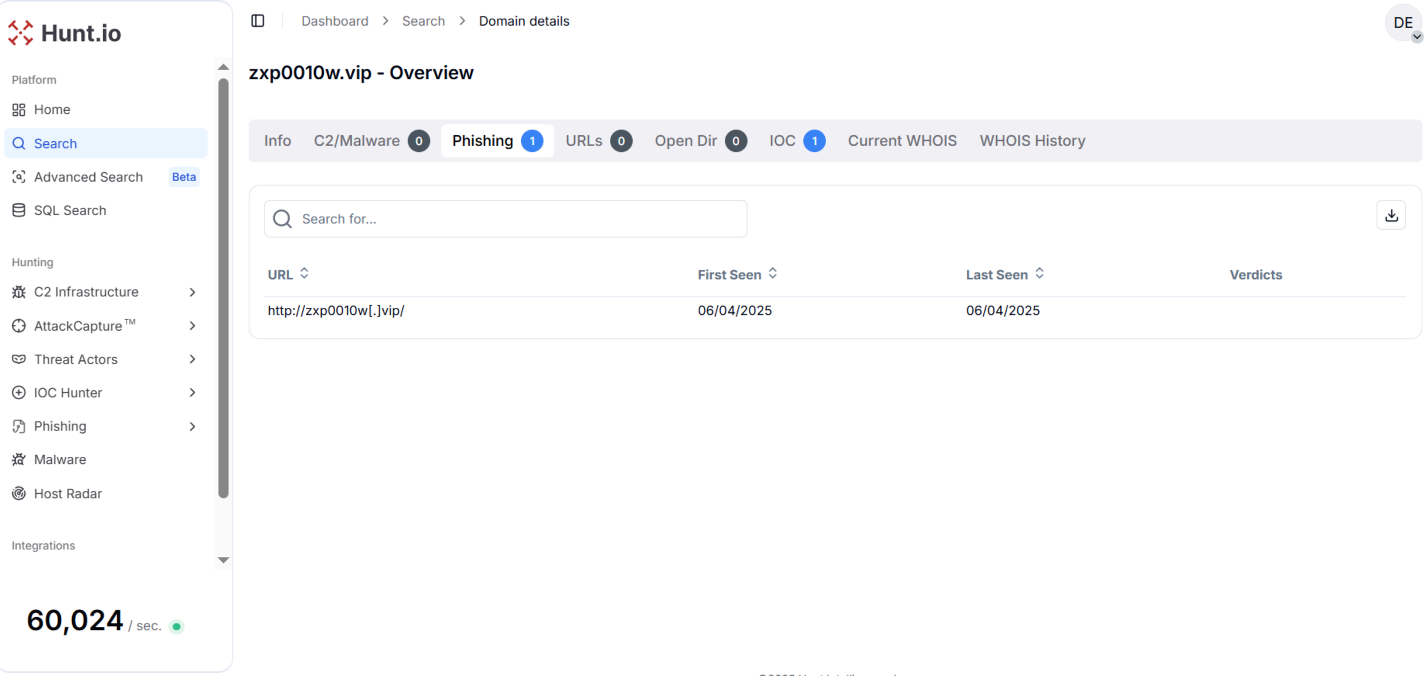
Initially, phishing emails impersonating Taiwan's Ministry of Finance delivered malicious PDFs containing embedded links hosted on Tencent Cloud, using unique IDs to tie multiple payloads to the same operator. Over time, the threat actor abandoned cloud-based hosting in favor of custom domains embedding regional markers such as "tw" (for Taiwan), including twsww[.]xin, which later delivered Japanese-language ZIP payloads.

Another research by FortiGuard Labs traced a continuous lineage of activity extending from Mainland China (March 2024) to Taiwan and Japan (January-March 2025), and most recently, Malaysia. The campaigns relied on fake government or corporate documents such as tax regulations, salary adjustments, or audit notifications to trick users into executing staged malware droppers.

Building on that background, we began the hunt from a known campaign domain and used Hunt.io to pivot across webpage titles, languages, and filename themes, revealing cross-regional links between Chinese, Japanese, and English clusters.

Initial Discovery

Fortinet's blog highlighted multiple domains leveraged by threat actors for distributing malicious content across Asia. To begin with the pivoting, we have selected the domain "zxp0010w[.]vip" as the reference point to fetch the webpage information from hunt.io. The domain "zxp0010w.vip" was first and last observed on June 4, 2025, and is currently flagged for phishing activity on our platform.



zxp0010w.vip - Overview

URL	First Seen	Last Seen	Verdicts
http://zxp0010w[.]vip/	06/04/2025	06/04/2025	

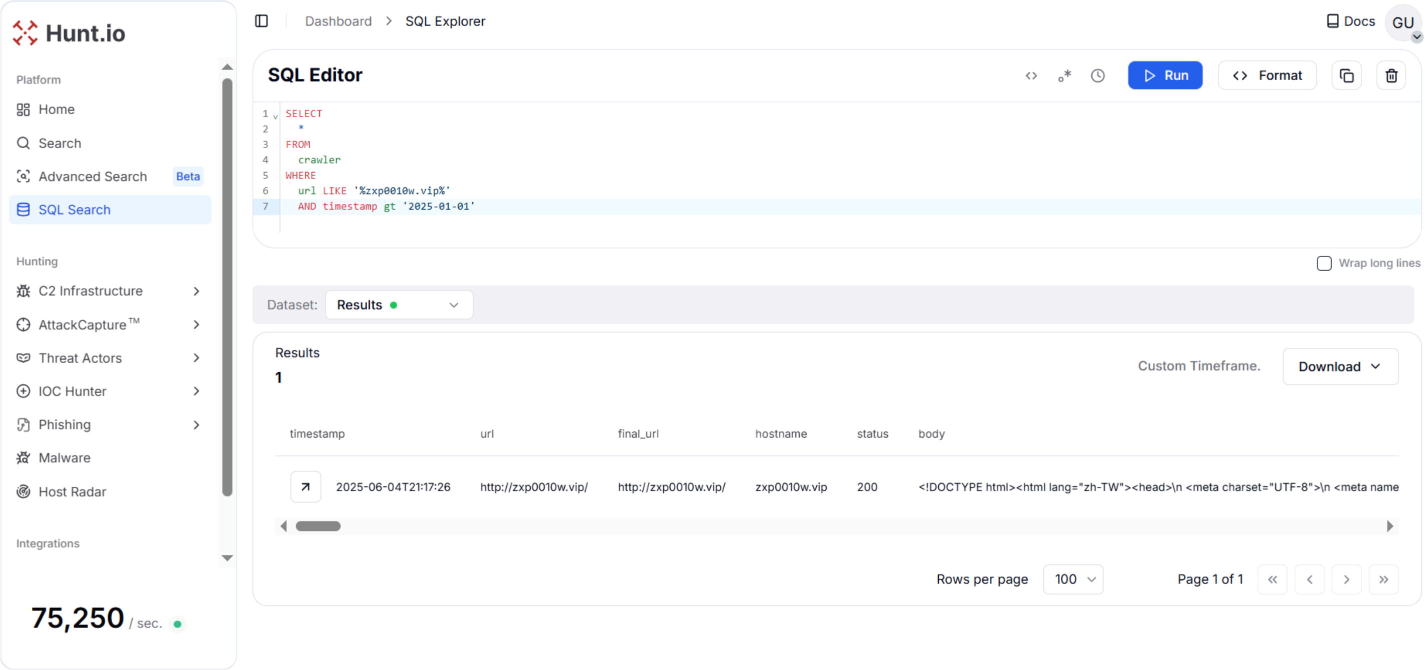
Figure 1. Phishing domain "zxp0010w.vip" observed on June 4, 2025, showing a single-day activity window indicative of short-lived malicious infrastructure.

Using a HuntSQL™ query, we used the crawler dataset to fetch all available fields:

```
SELECT
  *
FROM
  crawler
WHERE
  url LIKE '%zxp0010w.vip%'
  AND timestamp > '2025-01-01';
```

Copy

Output example:



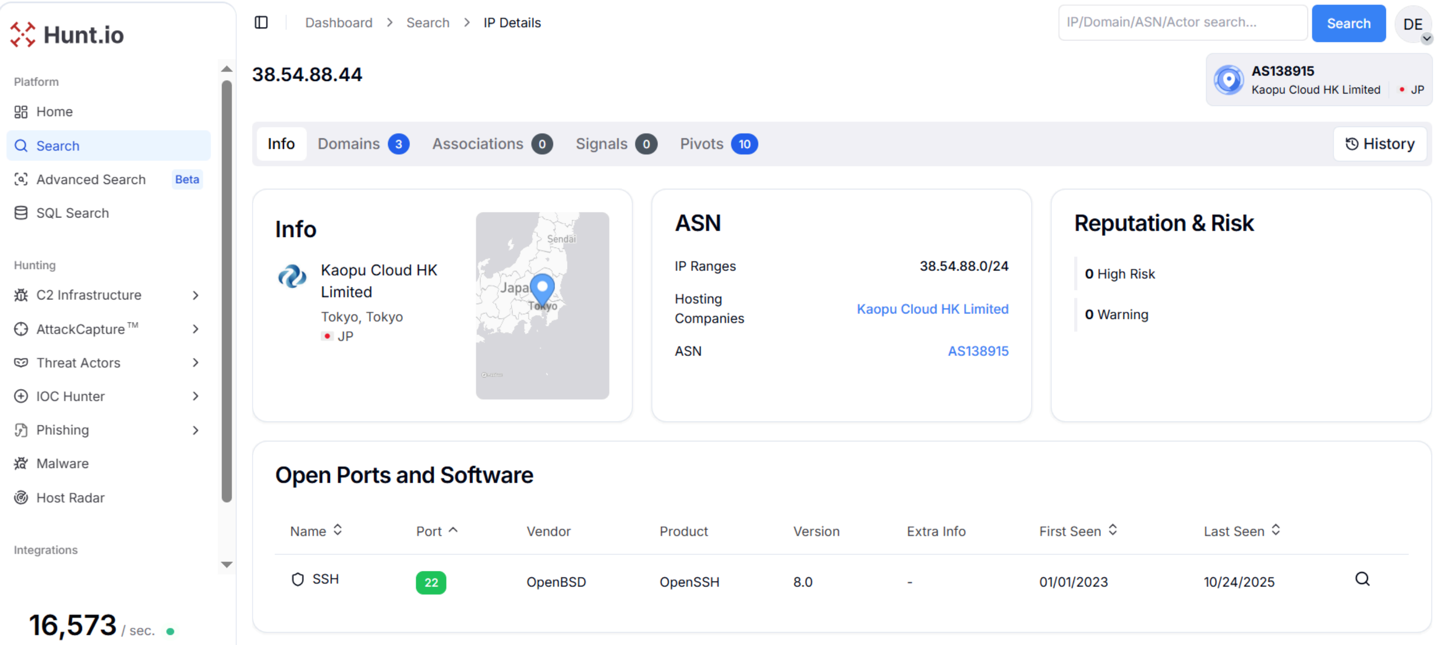
```
SELECT
  *
FROM
  crawler
WHERE
  url LIKE '%zxp0010w.vip%'
  AND timestamp gt '2025-01-01'
```

Results
1

timestamp	url	final_url	hostname	status	body
2025-06-04T21:17:26	http://zxp0010w.vip/	http://zxp0010w.vip/	zxp0010w.vip	200	<!DOCTYPE html><html lang="zh-TW"><head>\n <meta charset="UTF-8">\n <meta name

Figure 2. Initial HuntSQL™ query executed on the crawler dataset to retrieve all webpage records associated with the reference domain zxp0010w[.]vip.

The domain "zxp0010w[.]vip" was found; this host resolved to IP address 38.54.88[.]44, which is associated with Kaopu Cloud HK Limited, a hosting provider operating under AS138915 and located in Tokyo, Japan. Open port analysis reveals SSH (port 22) running OpenBSD OpenSSH 8.0, first observed in January 2023 and still active as of October 2025, indicating a long-lived server potentially used for persistent infrastructure or remote administration.



38.54.88.44

AS138915
Kaopu Cloud HK Limited • JP

Info

Kaopu Cloud HK Limited
Tokyo, Tokyo
JP

ASN

IP Ranges	38.54.88.0/24
Hosting Companies	Kaopu Cloud HK Limited
ASN	AS138915

Reputation & Risk

0 High Risk

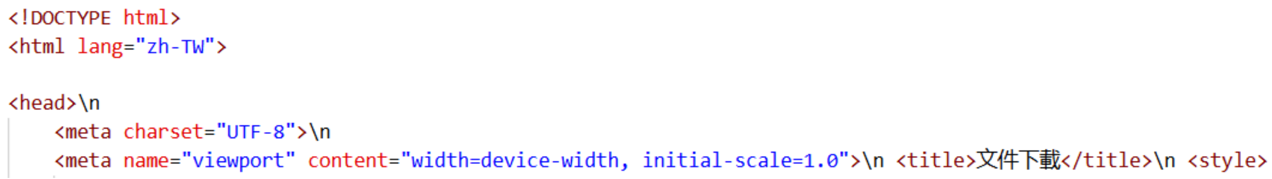
0 Warning

Open Ports and Software

Name	Port	Vendor	Product	Version	Extra Info	First Seen	Last Seen
SSH	22	OpenBSD	OpenSSH	8.0	-	01/01/2023	10/24/2025

Figure 3. The domain "zxp0010w[.]vip" resolves to IP address 38.54.88[.]44, hosted by Kaopu Cloud HK Limited (AS138915) in Tokyo, Japan

The code analysis of website shows an HTML page titled "**文件下載**" (File Download) hosted on IP address 38.54.88[.]44. The webpage is written in Traditional Chinese (lang="zh-TW"), used in Taiwan.

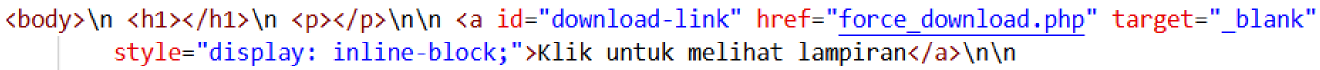


```
<!DOCTYPE html>
<html lang="zh-TW">

<head>\n
    <meta charset="UTF-8">\n
    <meta name="viewport" content="width=device-width, initial-scale=1.0">\n <title>文件下載</title>\n <style>
```

Figure 4. HuntSQL™ query results reveal a "文件下載" (File Download) page written in Traditional Chinese, suggesting Taiwan-focused lure content.

The download button reads "Klik untuk melihat lampiran" in Indonesian, which translates to "Click to view attachment". This linguistic inconsistency suggests that the page may have been designed to target users from Taiwan and Indonesia.

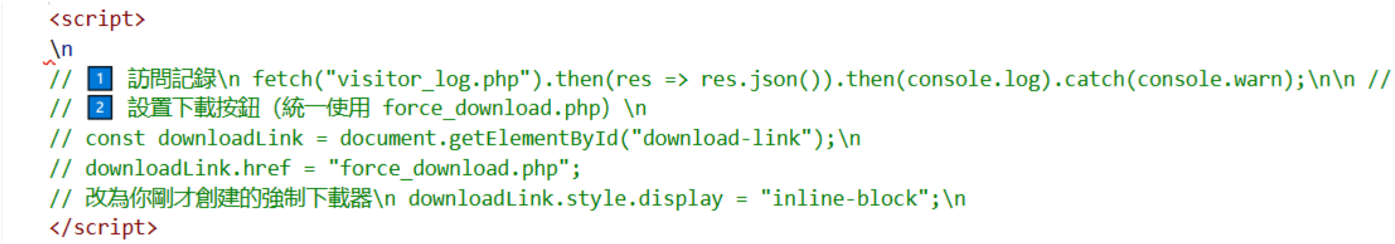


```
<body>\n <h1></h1>\n <p></p>\n\n <a id="download-link" href="force_download.php" target="_blank"
        style="display: inline-block;">Klik untuk melihat lampiran</a>\n\n
```

Figure 5. The presence of the Indonesian text "Klik untuk melihat lampiran" ("Click to view attachment") on a page otherwise using Traditional Chinese suggests cross-regional targeting between Taiwan and Indonesia.

The embedded script first sends a background request to visitor_log.php each time the page loads, as indicated by the comment "訪問記錄" ("visit record"), likely to log visitor information such as IP address or user agent. Secondly, it dynamically reveals the previously hidden download button and assigns its target to force_download.php, described in the comment as a "forced downloader". This setup suggests the page is designed to both track visitor activity and deliver a downloadable payload upon interaction.

That first discovery became the pivot point for a broader search, beginning with the Chinese-language cluster.



```
<script>
\n
// 1️⃣ 訪問記錄\n fetch("visitor_log.php").then(res => res.json()).then(console.log).catch(console.warn);\n\n //
// 2️⃣ 設置下載按鈕 (統一使用 force_download.php) \n
// const downloadLink = document.getElementById("download-link");\n
// downloadLink.href = "force_download.php";
// 改為你剛才創建的強制下載器\n downloadLink.style.display = "inline-block";\n
</script>
```

Figure 6. Embedded JavaScript logic logs visitor activity via "visitor_log.php" ("訪問記錄") and dynamically exposes a hidden download button linked to "force_download.php," functioning as a forced payload delivery mechanism.

Pivoting and Cluster Analysis

Chinese Cluster

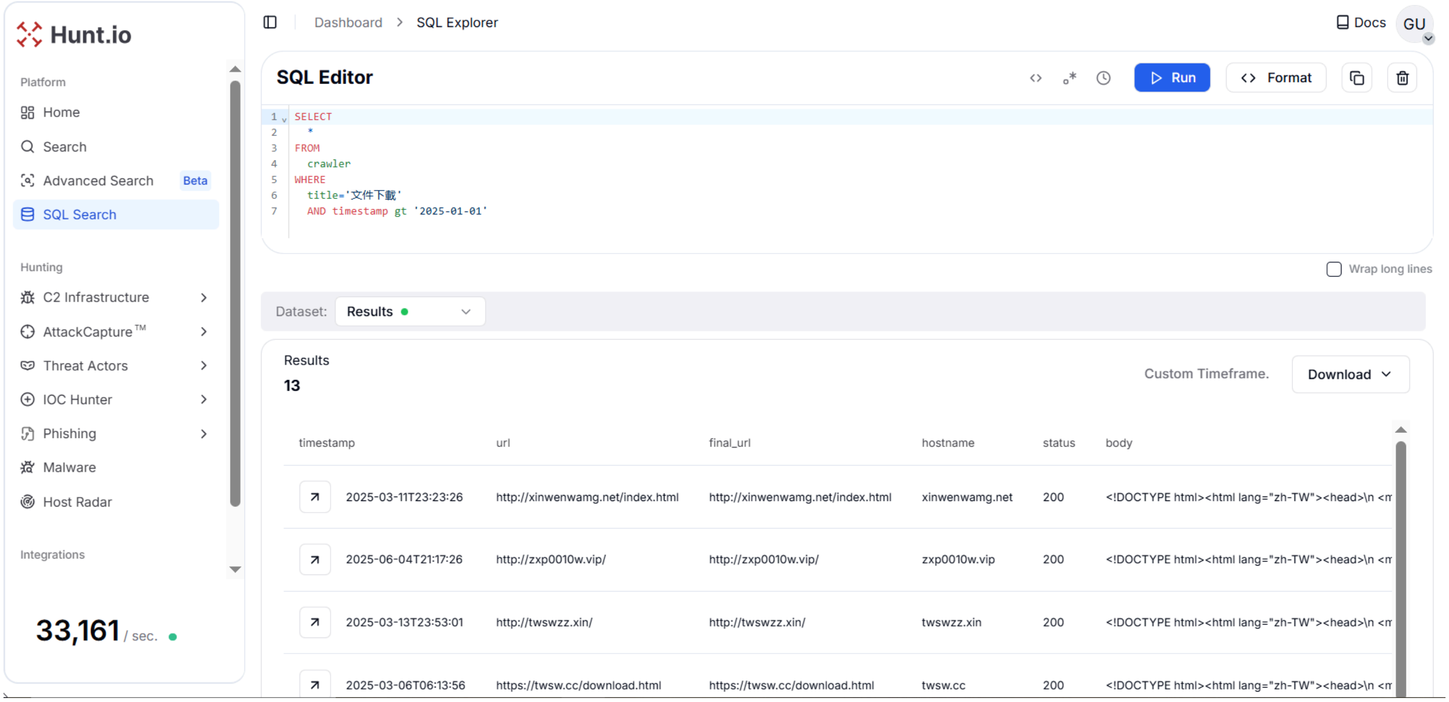
After identifying that the domain zxp0010w[.]vip hosted a webpage titled "文件下載" (**File Download**), we used the title as a pivot point to uncover other potentially related sites sharing the same characteristics.

A HuntSQL™ query was designed to extract all crawler records containing pages with the same title captured after January 1, 2025. The query returned **11 unique results** that are related to the same phishing campaign.

```
SELECT
  *
FROM
   crawler
WHERE
  title = '文件下載'
  AND timestamp > '2025-01-01';
```

Copy

Output example:



```
SELECT
  *
FROM
  crawler
WHERE
  title='文件下載'
  AND timestamp gt '2025-01-01'
```

Results
13

timestamp	url	final_url	hostname	status	body
2025-03-11T23:23:26	http://xinwenwamg.net/index.html	http://xinwenwamg.net/index.html	xinwenwamg.net	200	<!DOCTYPE html><html lang="zh-TW"><head>\n <m
2025-06-04T21:17:26	http://zxp0010w.vip/	http://zxp0010w.vip/	zxp0010w.vip	200	<!DOCTYPE html><html lang="zh-TW"><head>\n <m
2025-03-13T23:53:01	http://twswzz.xin/	http://twswzz.xin/	twswzz.xin	200	<!DOCTYPE html><html lang="zh-TW"><head>\n <m
2025-03-06T06:13:56	https://twsw.cc/download.html	https://twsw.cc/download.html	twsw.cc	200	<!DOCTYPE html><html lang="zh-TW"><head>\n <m

Figure 7. Pivoting on the title "文件下載" enabled the identification of 11 additional domains exhibiting similar characteristics linked with the same campaign.

The eleven webpages are part of a **coordinated campaign** delivering staged ZIP/RAR payloads under the guise of legitimate documents. The most used language was Traditional Chinese, followed by Japanese, which strongly suggests an **organized operation targeting users across Taiwan, Hong Kong, and Japan**.

Moreover, the theme of filenames spotted on webpages was bureaucratic and financial, targeting East Asian organizations such as Chinese and Japanese users. The filenames include "稅務電子發票名單.rar" (Tax Invoice List), "進出口申報.zip" (Import-Export Declaration), "財務負責人核對後回傳（電腦版）1.zip" (Finance Confirmation Form), "條例檔案.zip" (Regulatory Document), "通知函.rar" (Notification Letter), "《商業登記條例修改通知書》Bilingual.PCVersion.zip" (Business Registration Amendment Notice), "香港金融管理局企業相關條例（電腦版）.zip" (Hong Kong Monetary Authority Regulations), "添付資料一覧.zip" (Attached Documents List, Japanese), and "申請平台.zip" (Application Platform).

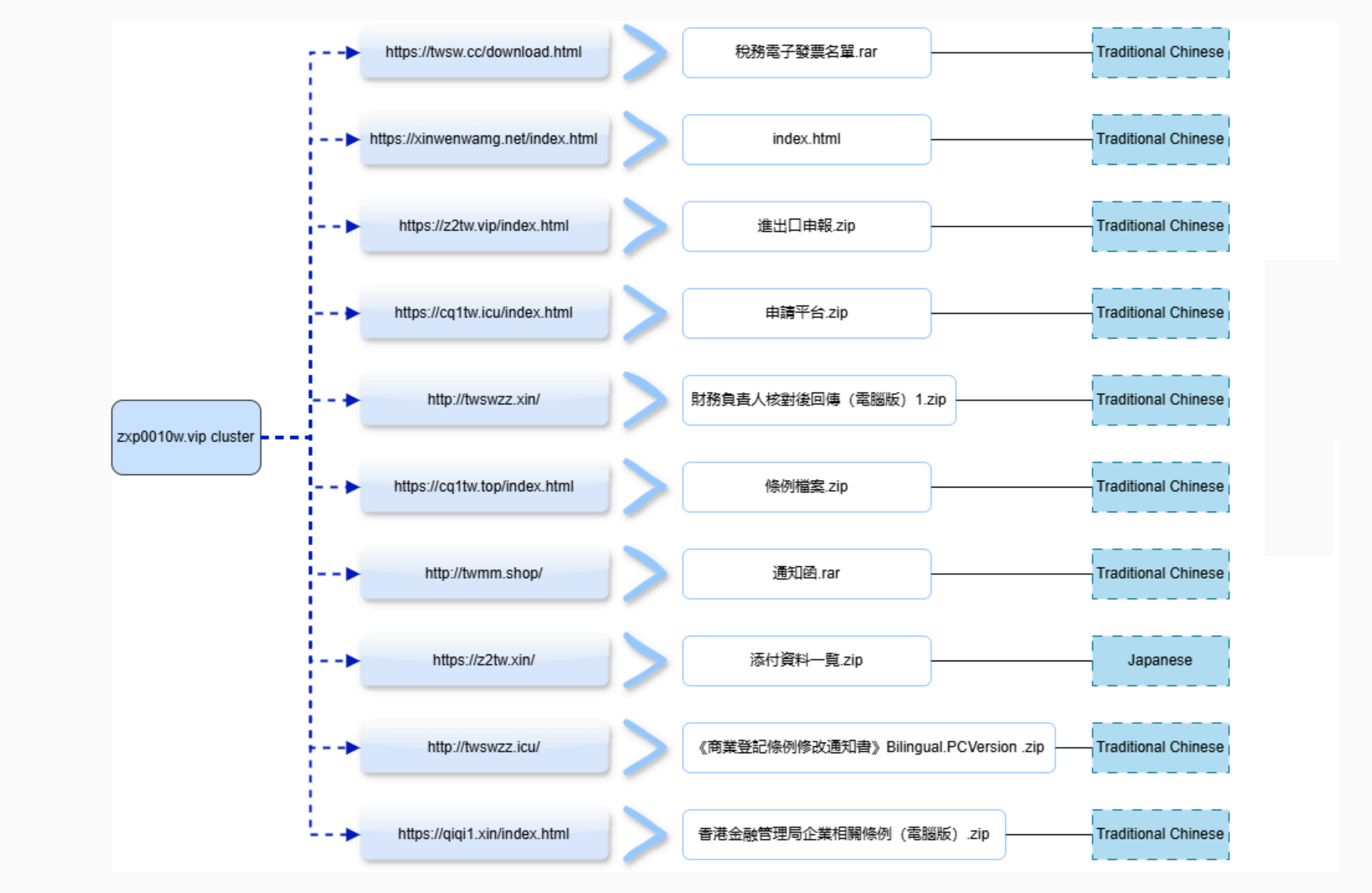


Figure 8. A mindmap of eleven interconnected webpages with the title "文件下載", showcasing bureaucratic and financial-themed ZIP/RAR archives written in Traditional Chinese and Japanese, likely designed to target organizations in Taiwan, Hong Kong, and Japan.

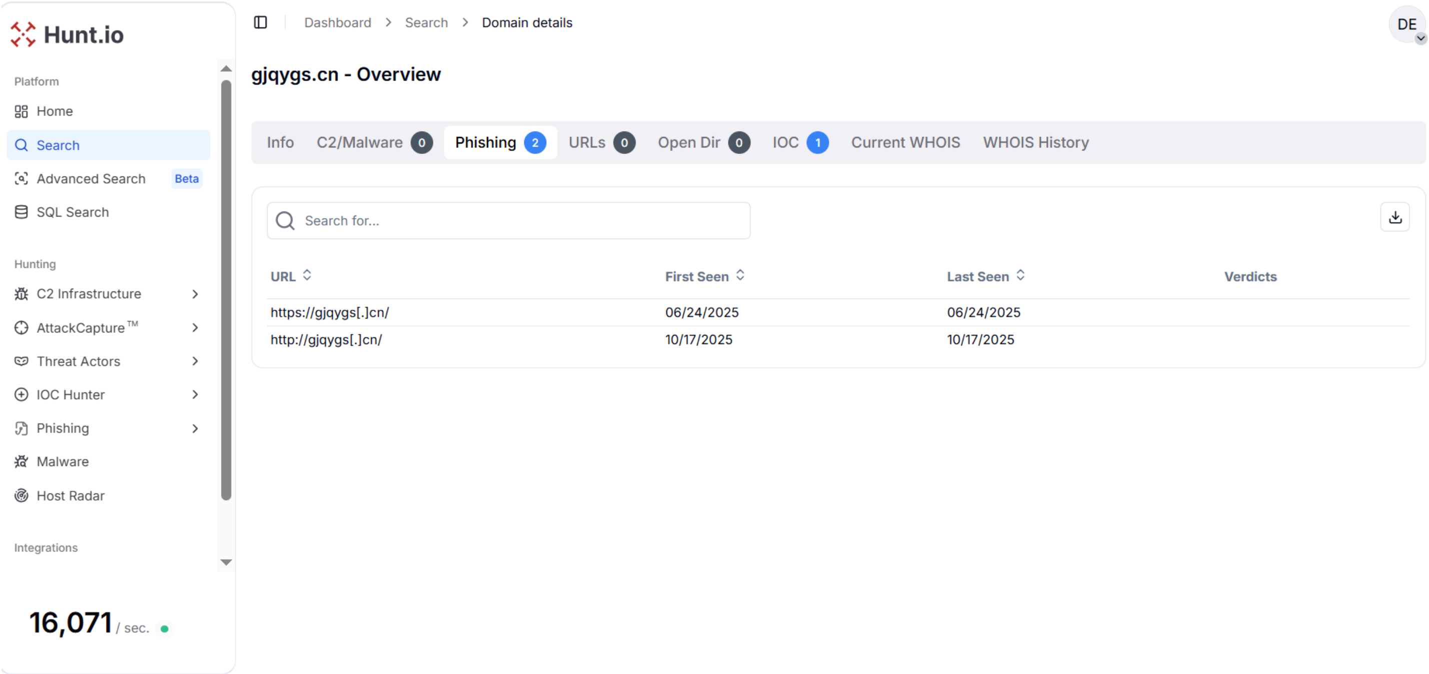
The Chinese-language pages all use the same ZIP/RAR delivery setup and web scripts, pointing to a single kit operating across Taiwan, Hong Kong, and Japan.

After mapping the Chinese-language sites, we moved to English-language pages to check if the same web kit was reused.

English Cluster

For the second pivot, we selected the domain "gjqygs[.]cn" as the reference point to fetch the webpage information from hunt.io. The domain "gjqygs[.]cn" has been observed engaging in phishing activity, with two distinct detections recorded on June 24, 2025, and October 17, 2025, respectively.

The host was accessed over both HTTP and HTTPS, suggesting a minimal setup aimed at credential harvesting or impersonation campaigns.



gjqygs.cn - Overview

URL	First Seen	Last Seen	Verdicts
https://gjqygs[.]cn/	06/24/2025	06/24/2025	
http://gjqygs[.]cn/	10/17/2025	10/17/2025	

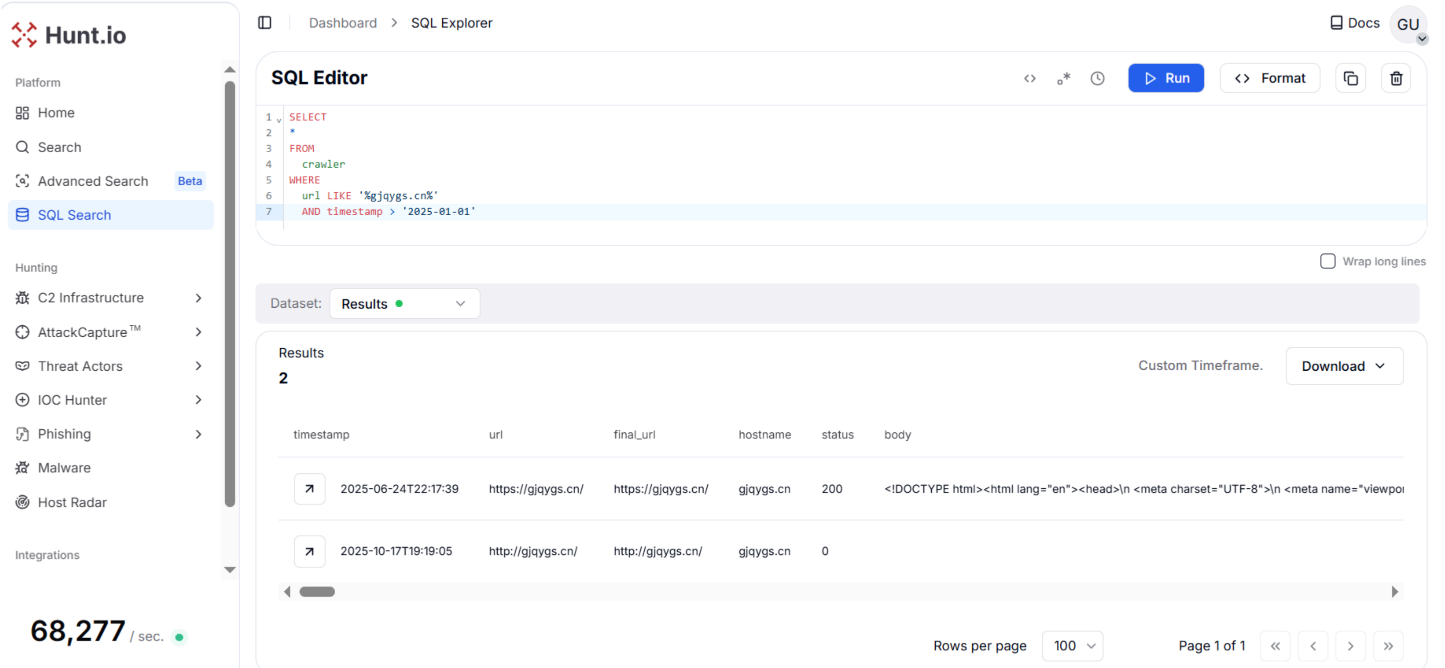
Figure 9. Phishing domain "gjqygs[.]cn" observed on June 24 and October 17, 2025, active over HTTP and HTTPS services.

Using a HuntSQL™ query, we used the crawler dataset to fetch all available fields and expand the information:

```
SELECT
  *
FROM
  crawler
WHERE
  url LIKE '%gjqygs.cn%'
  AND timestamp > '2025-01-01'
```

Copy

Output example:



```
SELECT
*
FROM
  crawler
WHERE
  url LIKE '%gjqygs.cn%'
  AND timestamp > '2025-01-01'
```

Dataset: Results

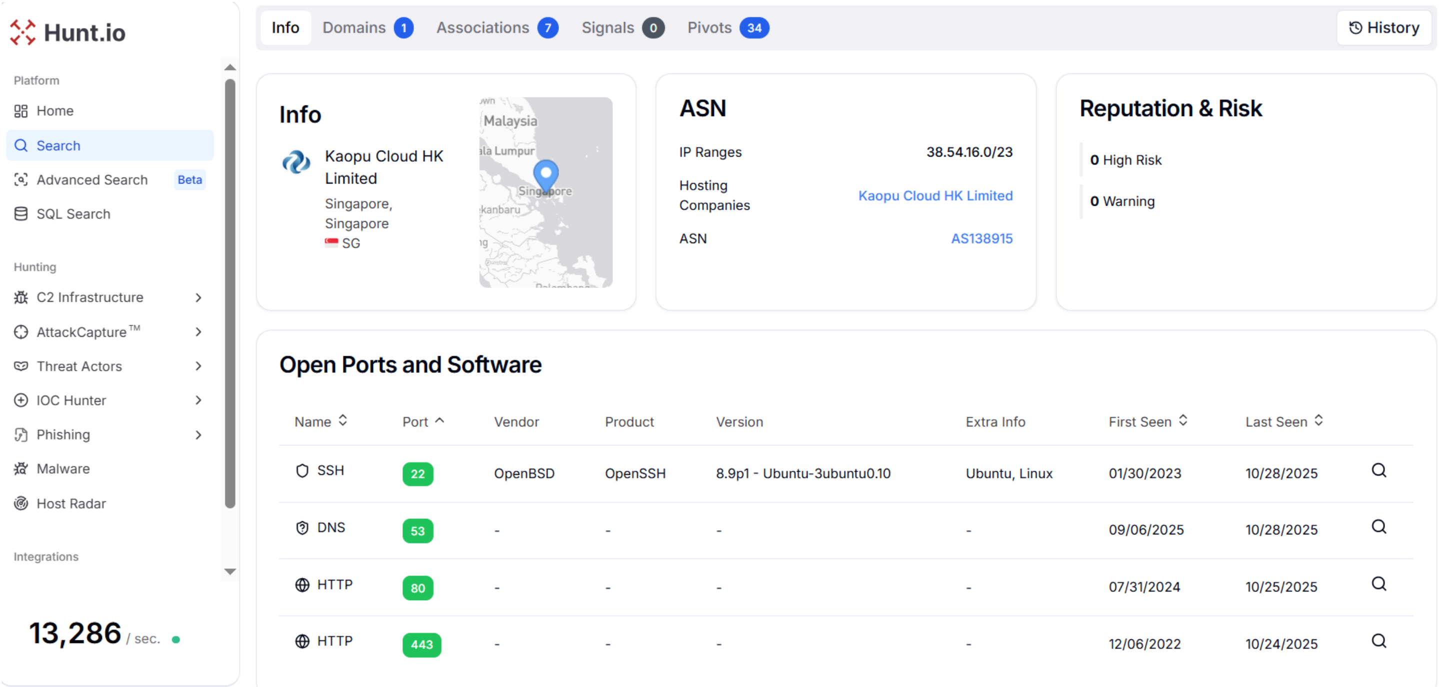
Results
2

	timestamp	url	final_url	hostname	status	body
↗	2025-06-24T22:17:39	https://gjqygs.cn/	https://gjqygs.cn/	gjqygs.cn	200	<!DOCTYPE html><html lang="en"><head>\n <meta charset="UTF-8">\n <meta name="viewpor
↗	2025-10-17T19:19:05	http://gjqygs.cn/	http://gjqygs.cn/	gjqygs.cn	0	

Rows per page 100 Page 1 of 1

Figure 10. A HuntSQL™ query executed on the crawler dataset to retrieve all webpage records associated with the reference domain gjqygs[.]cn.

The domain gjqygs[.]cn resolves to the IP address 38.54.17[.]167, which, according to Hunt.io, is hosted by Kaopu Cloud HK Limited under ASN AS138915, and is located in Singapore. The host exposes multiple open services, including SSH (port 22) running OpenBSD OpenSSH 8.9p1 on Ubuntu, DNS (port 53), and HTTP/HTTPS (ports 80 and 443), all of which remained active as recently as October 2025.



Info

Kaopu Cloud HK Limited
Singapore, Singapore
SG

ASN

IP Ranges	38.54.16.0/23
Hosting Companies	Kaopu Cloud HK Limited
ASN	AS138915

Reputation & Risk

0 High Risk

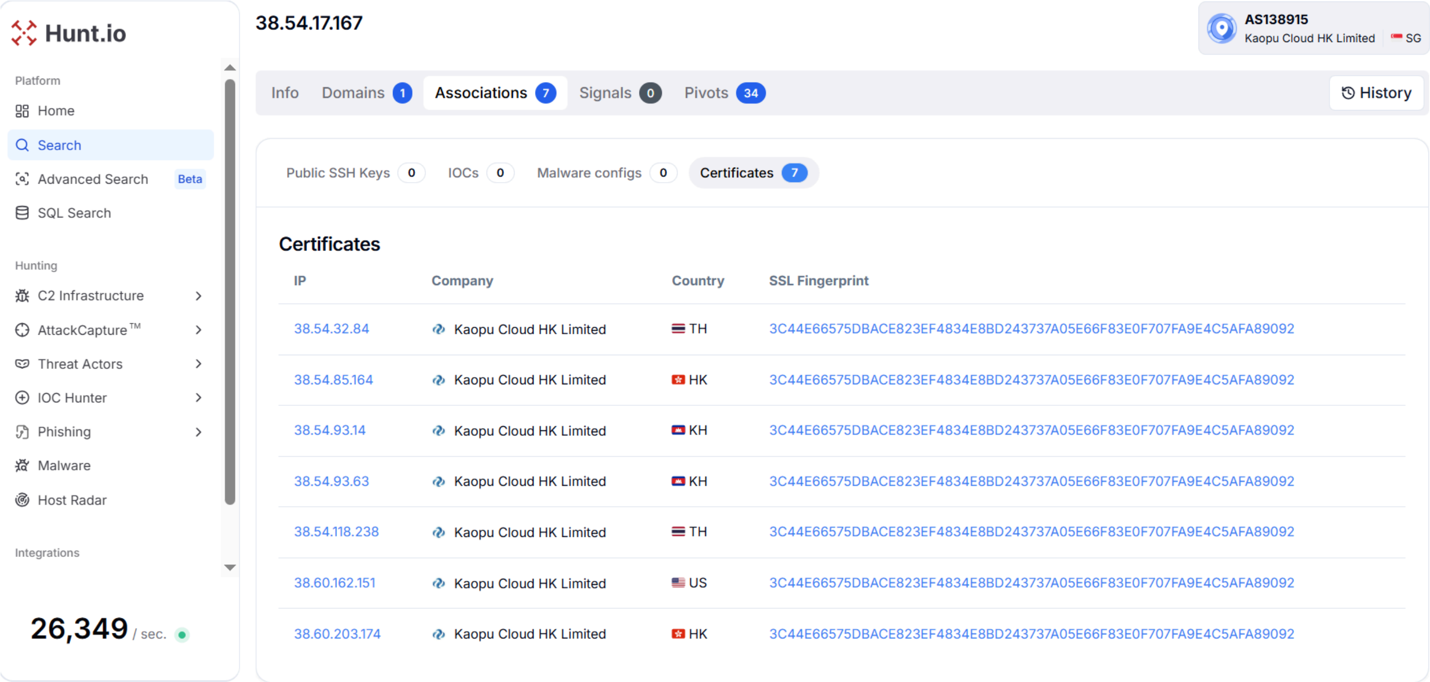
0 Warning

Open Ports and Software

Name	Port	Vendor	Product	Version	Extra Info	First Seen	Last Seen
SSH	22	OpenBSD	OpenSSH	8.9p1 - Ubuntu-3ubuntu0.10	Ubuntu, Linux	01/30/2023	10/28/2025
DNS	53	-	-	-	-	09/06/2025	10/28/2025
HTTP	80	-	-	-	-	07/31/2024	10/25/2025
HTTP	443	-	-	-	-	12/06/2022	10/24/2025

Figure 11. Hunt.io analysis shows the domain "gjqygs[.]cn" resolves to IP 38.54.17[.]167 hosted by Kaopu Cloud HK Limited (AS138915) in Singapore, with multiple active services as of October 2025.

The IP address "38.54.17[.]167" shows connections to seven other IPs across multiple regions sharing the same SSL fingerprint (3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092). These related IPs are distributed across Thailand (38.54.32[.]84, 38.54.118[.]238), Hong Kong (38.54.85[.]164, 38.60.203[.]174), Cambodia (38.54.93[.]14, 38.54.93[.]63), and the United States (38.60.162[.]151).



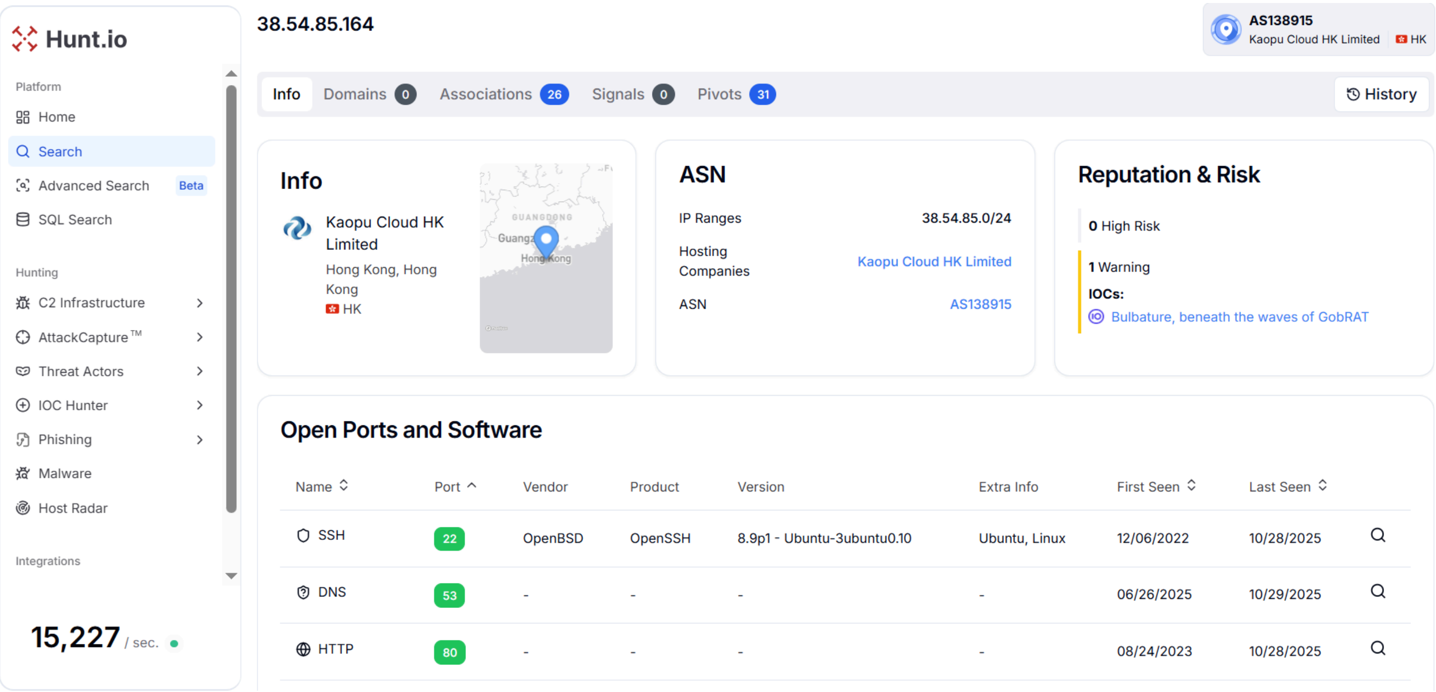
Certificates

IP	Company	Country	SSL Fingerprint
38.54.32.84	Kaopu Cloud HK Limited	TH	3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092
38.54.85.164	Kaopu Cloud HK Limited	HK	3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092
38.54.93.14	Kaopu Cloud HK Limited	KH	3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092
38.54.93.63	Kaopu Cloud HK Limited	KH	3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092
38.54.118.238	Kaopu Cloud HK Limited	TH	3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092
38.60.162.151	Kaopu Cloud HK Limited	US	3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092
38.60.203.174	Kaopu Cloud HK Limited	HK	3C44E66575DBACE823EF4834E8BD243737A05E66F83E0F707FA9E4C5AFA89092

Figure 12. Hunt.io revealed 7 similar hosts sharing the same SSL certificate fingerprint across the (Kaopu Cloud HK Limited, Singapore) infrastructure.

One of the IP addresses, 38.54.85[.]164, operated by Kaopu Cloud HK Limited under ASN AS138915 and located in Hong Kong, has been flagged in threat intelligence sources with one warning linked to the "Bulbature, beneath the waves of GobRAT" campaign.

This association suggests possible involvement in GobRAT-related activity, known for targeting Linux-based systems through remote administration tools. However, the previous Fortinet report, which served as the primary focus of our hunt, was related to Windows-based malware, and therefore does not appear to be linked to GobRAT at this stage.



38.54.85.164

AS138915
Kaopu Cloud HK Limited HK

Info

Kaopu Cloud HK Limited
Hong Kong, Hong Kong
HK

ASN

IP Ranges	38.54.85.0/24
Hosting Companies	Kaopu Cloud HK Limited
ASN	AS138915

Reputation & Risk

0 High Risk

1 Warning

IOCs:

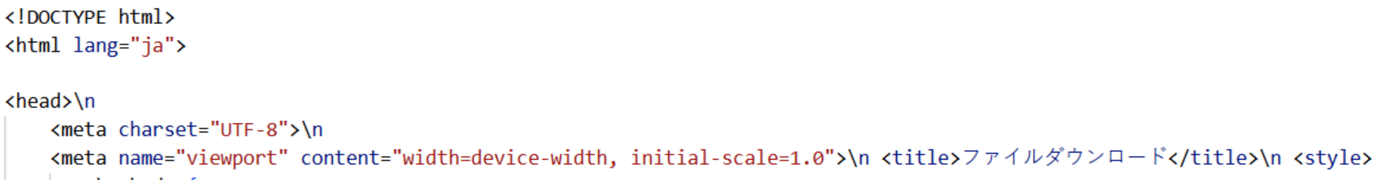
Bulbature, beneath the waves of GobRAT

Open Ports and Software

Name	Port	Vendor	Product	Version	Extra Info	First Seen	Last Seen
SSH	22	OpenBSD	OpenSSH	8.9p1 - Ubuntu-3ubuntu0.10	Ubuntu, Linux	12/06/2022	10/28/2025
DNS	53	-	-	-	-	06/26/2025	10/29/2025
HTTP	80	-	-	-	-	08/24/2023	10/28/2025

Figure 13. Hunt.io shows an IP address 38.54.85[.]164 (Kaopu Cloud HK Limited, Hong Kong) has a connection to GobRAT-related activity with multiple active services.

The code analysis of the website shows an HTML page titled "File Download" and the language used in the webpage is English (lang="en").

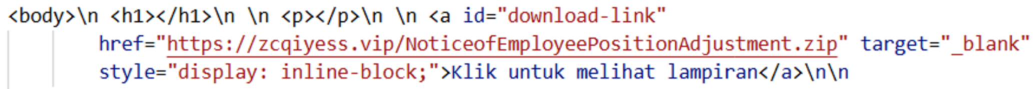


```
<!DOCTYPE html>
<html lang="ja">

<head>\n
    <meta charset="UTF-8">\n
    <meta name="viewport" content="width=device-width, initial-scale=1.0">\n <title>ファイルダウンロード</title>\n <style>
```

Figure 14. HuntSQL™ query results reveal a "File Download" HTML title written in the English language

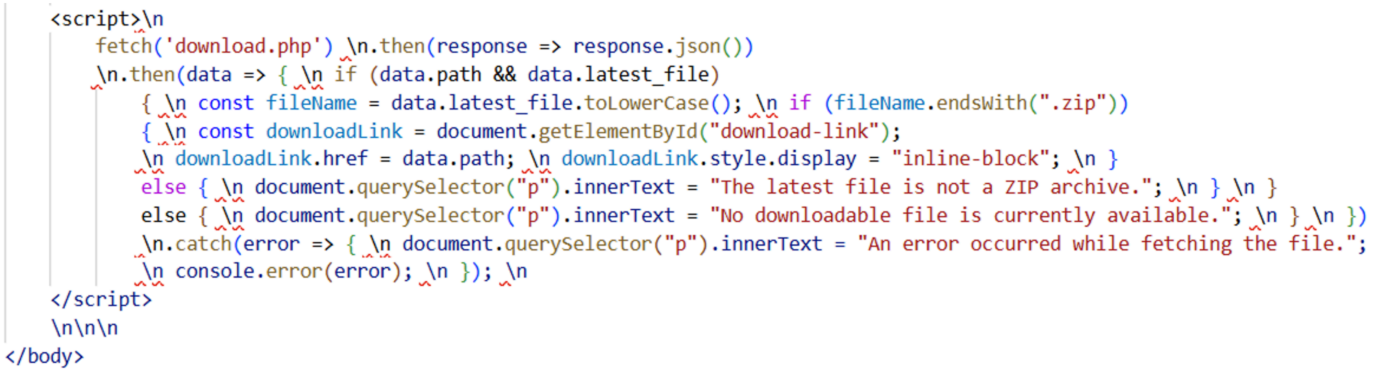
Similar to the previous campaign, this webpage also contains the same "Klik untuk melihat lampiran" download button, which triggers the download of NoticeofEmployeePositionAdjustment.zip (not seen in the previous campaign).



```
<body>\n <h1></h1>\n \n <p></p>\n \n <a id="download-link"
        href="https://zcqiyess.vip/NoticeofEmployeePositionAdjustment.zip" target="_blank"
        style="display: inline-block;">Klik untuk melihat lampiran</a>\n\n
```

Figure 15. A ZIP file is downloaded whenever a user clicks on the download button, having a similar Indonesian button "Klik untuk melihat lampiran" (Click to view attachment).

The script dynamically fetches file information from download.php and only displays the download link if a valid .zip file is available. It checks the server's JSON response for path and latest_file, and if conditions match, it updates the link's URL and makes it visible. Otherwise, it shows messages like "No downloadable file is currently available" or "The latest file is not a ZIP archive."



```
    <script>\n
        fetch('download.php') \n.then(response => response.json())
        \n.then(data => { \n if (data.path && data.latest_file)
            { \n const fileName = data.latest_file.toLowerCase(); \n if (fileName.endsWith(".zip"))
            { \n const downloadLink = document.getElementById("download-link");
            \n downloadLink.href = data.path; \n downloadLink.style.display = "inline-block"; \n }
            else { \n document.querySelector("p").innerText = "The latest file is not a ZIP archive."; \n } \n }
            else { \n document.querySelector("p").innerText = "No downloadable file is currently available."; \n } \n })
            \n.catch(error => { \n document.querySelector("p").innerText = "An error occurred while fetching the file.";
            \n console.error(error); \n }); \n
    </script>
    \n\n\n
</body>
```

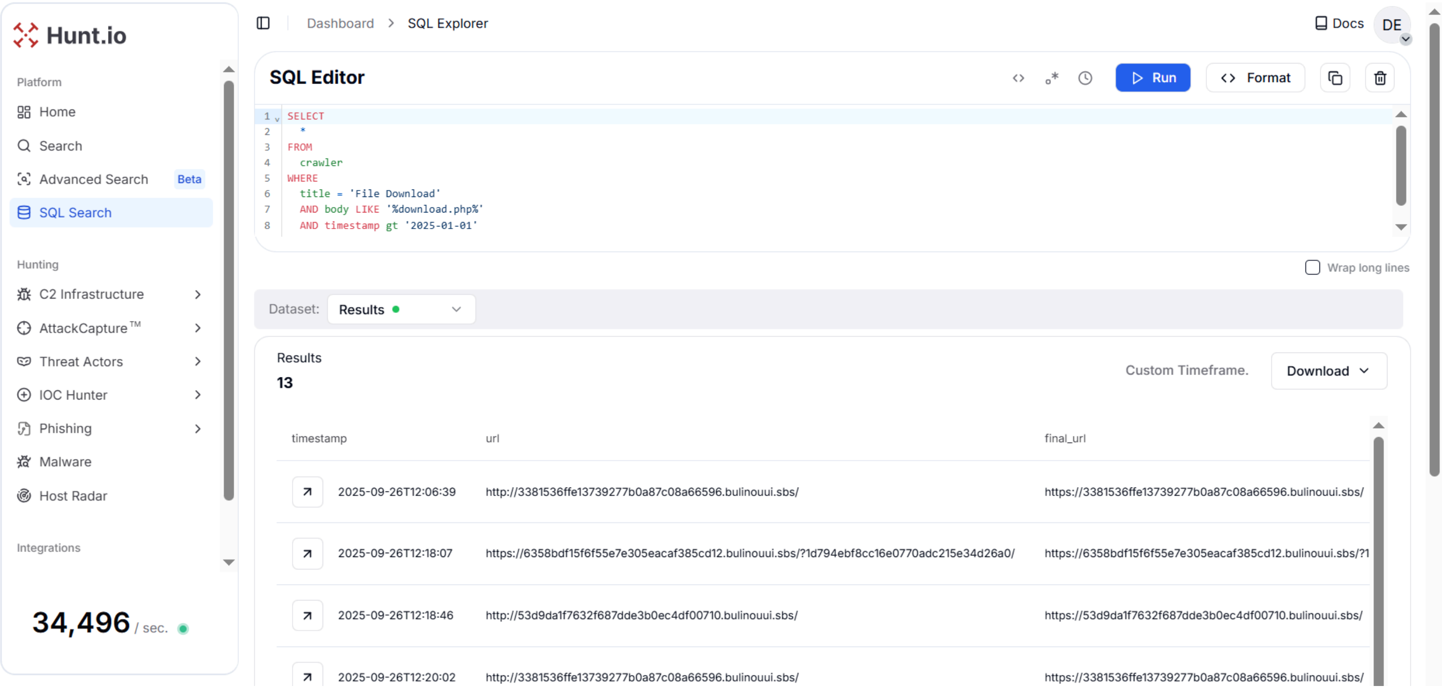
Figure 16. Dynamic script logic that displays the ZIP download link only when a valid payload is available from download.php.

To proceed further, a HuntSQL™ query is designed to extract all crawler records containing pages with the same title "File Download" captured after January 1, 2025. The query returned **11 unique results** that are related to this campaign.

```
SELECT
  *
FROM
  crawler
WHERE
  title = 'File Download'
  AND body LIKE '%download.php%'
  AND timestamp gt '2025-01-01'
```

Copy

Output example:



```sql
SELECT
  *
FROM
  crawler
WHERE
  title = 'File Download'
  AND body LIKE '%download.php%'
  AND timestamp gt '2025-01-01'
```

Results
13

timestamp	url	final_url
2025-09-26T12:06:39	http://3381536ffe13739277b0a87c08a66596.bulinouui.sbs/	https://3381536ffe13739277b0a87c08a66596.bulinouui.sbs/
2025-09-26T12:18:07	https://6358bdf15f6f55e7e305eacaf385cd12.bulinouui.sbs/?1d794ebf8cc16e0770adc215e34d26a0/	https://6358bdf15f6f55e7e305eacaf385cd12.bulinouui.sbs/?1
2025-09-26T12:18:46	http://53d9da1f7632f687dde3b0ec4df00710.bulinouui.sbs/	https://53d9da1f7632f687dde3b0ec4df00710.bulinouui.sbs/
2025-09-26T12:20:02	http://3381536ffe13739277b0a87c08a66596.bulinouui.sbs/	https://3381536ffe13739277b0a87c08a66596.bulinouui.sbs/

Figure 17. Pivoting on the title "File Download" enabled the identification of 11 additional domains exhibiting similar characteristics linked with the same campaign.

The newly uncovered cluster shows consistent characteristics with previously identified campaigns delivering staged ZIP and archive payloads disguised as legitimate financial or document-related files. The webpages, primarily hosted on .vip and .sbs domains such as zcqiyess[.]vip and multiple subdomains of bulinouui[.]sbs, follow an identical structure that dynamically fetches payload details from download.php.

All the webpages used the English language in the HTML, followed by filenames including Tax Filing Documents.zip, दाखिल करने के दस्तावेज़.zip (Documents for Filing, Hindi), and Tax Return Documents.tar.gz, suggesting a thematic focus on taxation and compliance, indicating an expansion of targeting toward **Southeast Asian regions**.

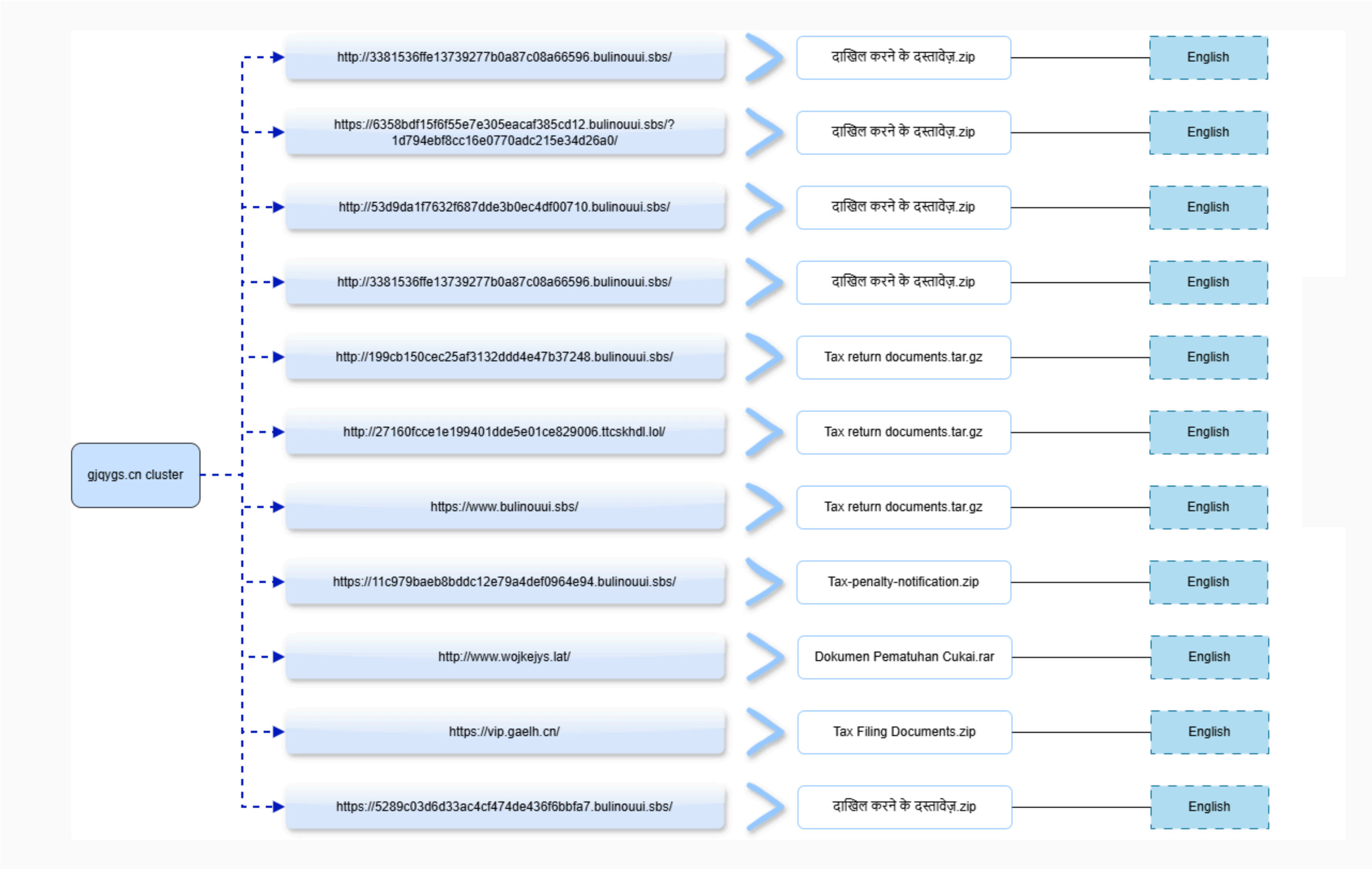
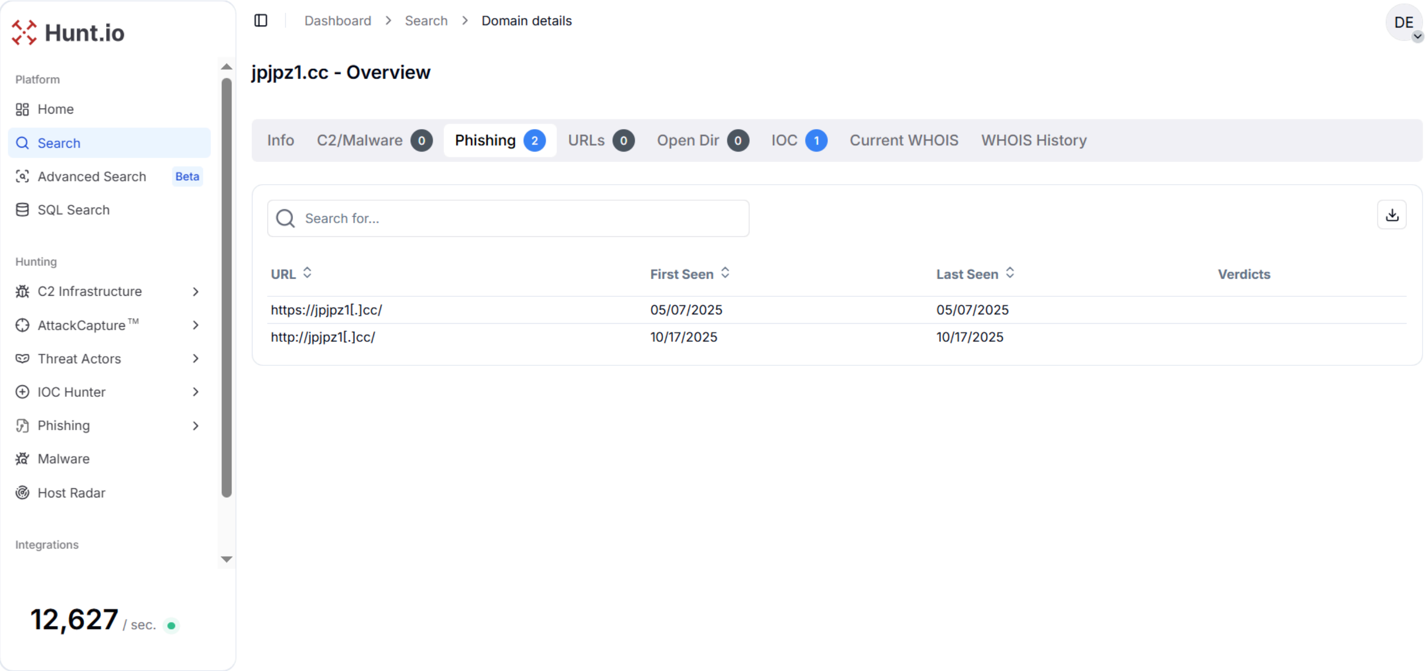

gjqygs.cn cluster
http://3381536ffe13739277b0a87c08a66596.bulinouui.sbs/
दाखिल करने के दस्तावेज़.zip
English
https://6358bdf15f6f55e7e305eacaf385cd12.bulinouui.sbs/?1d794ebf8cc16e0770adc215e34d26a0/
दाखिल करने के दस्तावेज़.zip
English
http://53d9da1f7632f687dde3b0ec4df00710.bulinouui.sbs/
दाखिल करने के दस्तावेज़.zip
English
http://3381536ffe13739277b0a87c08a66596.bulinouui.sbs/
दाखिल करने के दस्तावेज़.zip
English
http://199cb150cec25af3132ddd4e47b37248.bulinouui.sbs/
Tax return documents.tar.gz
English
http://27160fcce1e199401dde5e01ce829006.ttcskhdl.lol/
Tax return documents.tar.gz
English
https://www.bulinouui.sbs/
Tax return documents.tar.gz
English
https://11c979baeb8bddc12e79a4def0964e94.bulinouui.sbs/
Tax-penalty-notification.zip
English
http://www.wojkejys.lat/
Dokumen Pematuhan Cukai.rar
English
https://vip.gaelh.cn/
Tax Filing Documents.zip
English
https://5289c03d6d33ac4cf474de436f6bbfa7.bulinouui.sbs/
दाखिल करने के दस्तावेज़.zip
English

Figure 18. A mindmap of 11 webpages interconnected with the same title "File Download", showcasing English-language pages delivering staged ZIP / GZ lures with evidence of campaign expansion toward Southeast Asian business targets.

The English-language versions reuse the same templates but switch filenames and copy to fit corporate and government themes in Southeast Asia. The final step was to confirm whether the same infrastructure produced Japanese-language versions of the campaign.

Japanese Cluster

For the third pivot, we selected the domain "jpjpz1[.]cc" as the reference point to fetch the webpage information from hunt.io. The domain jpjpz1[.]cc has been observed in two phishing detections, first on May 7, 2025, and again on October 17, 2025, indicating possible reuse of infrastructure over time.



jpjpz1.cc - Overview

URL	First Seen	Last Seen	Verdicts
https://jpjpz1[.]cc/	05/07/2025	05/07/2025	
http://jpjpz1[.]cc/	10/17/2025	10/17/2025	

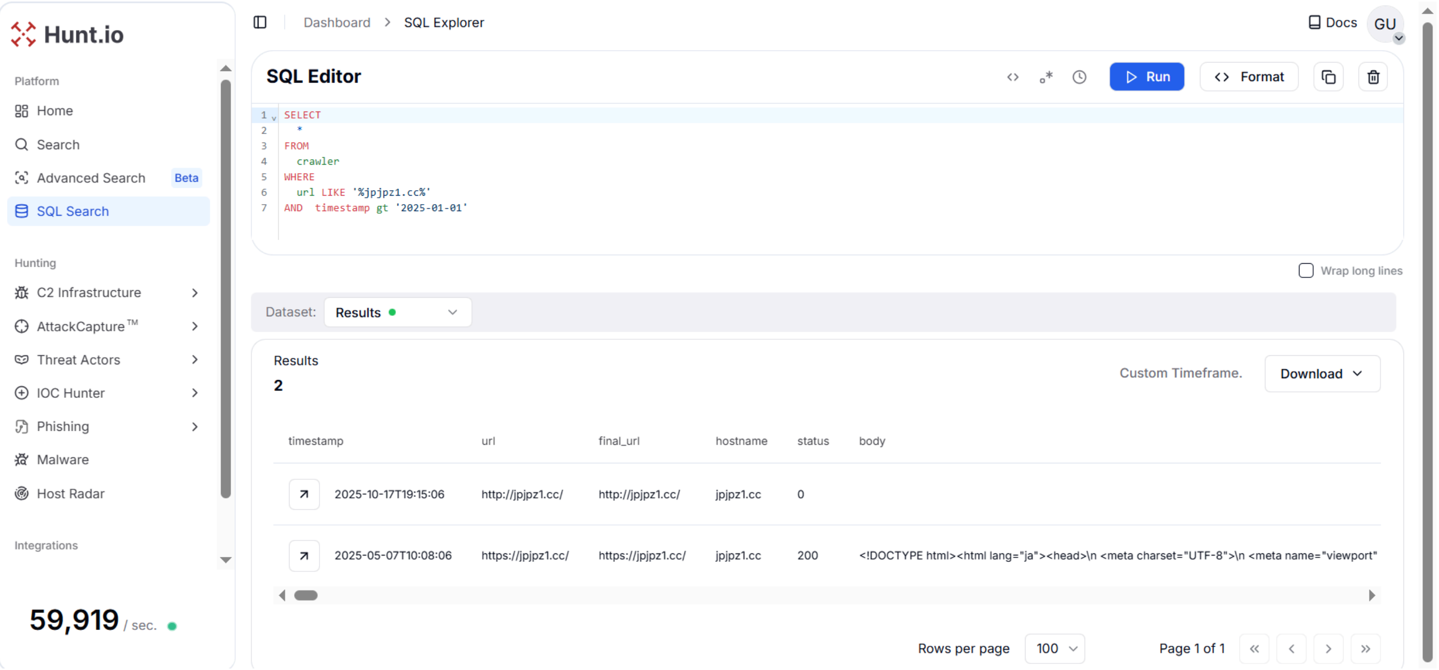
Figure 19. The analysis shows "jpjpz1[.]cc" observed on May 7 and October 17, 2025, indicating reused infrastructure over HTTP and HTTPS.

A HuntSQL™ query is used to identify all records containing references to the domain "jpjpz1[.]cc" collected after January 1, 2025. It searches within the crawler dataset to locate any URLs where the domain appears, allowing analysts to uncover recent sightings or related infrastructure:

```
SELECT
  *
FROM
  crawler
WHERE
  url LIKE '%jpjpz1.cc%'
AND  timestamp gt '2025-01-01'


Copy
```

Output example:



```
SELECT
  *
FROM
  crawler
WHERE
  url LIKE '%jpjpz1.cc%'
AND  timestamp gt '2025-01-01'
```

Results
2

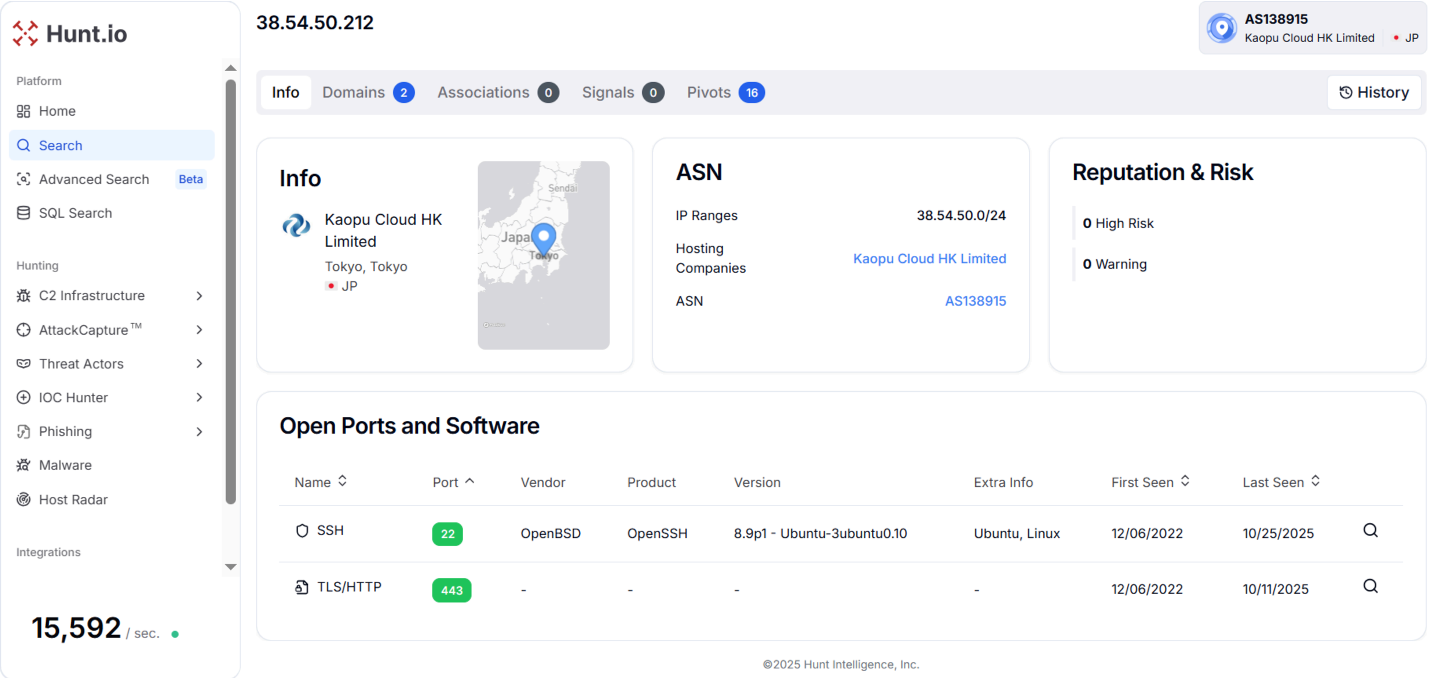
Custom Timeframe. Download

	timestamp	url	final_url	hostname	status	body
↗	2025-10-17T19:15:06	http://jpjpz1.cc/	http://jpjpz1.cc/	jpjpz1.cc	0	
↗	2025-05-07T10:08:06	https://jpjpz1.cc/	https://jpjpz1.cc/	jpjpz1.cc	200	<!DOCTYPE html><html lang="ja"><head>\n <meta charset="UTF-8">\n <meta name="viewport"

Rows per page 100 Page 1 of 1

Figure 20. A HuntSQL™ query executed on the crawler dataset to retrieve all webpage records associated with the reference domain jpjpz1[.]cc.

The domain jpjpz1[.]cc resolved to IP address 38.54.50[.]212, which is operated by Kaopu Cloud HK Limited under ASN AS138915, located in Tokyo, Japan. The host exposes key services such as SSH (port 22) running OpenBSD OpenSSH 8.9p1 on Ubuntu Linux and TLS/HTTP (port 443), both active since December 2022 and observed as recently as October 2025.



38.54.50.212

AS138915
Kaopu Cloud HK Limited • JP

Info

Kaopu Cloud HK Limited
Tokyo, Tokyo
JP

ASN

IP Ranges: 38.54.50.0/24
Hosting Companies: Kaopu Cloud HK Limited
ASN: AS138915

Reputation & Risk

0 High Risk
0 Warning

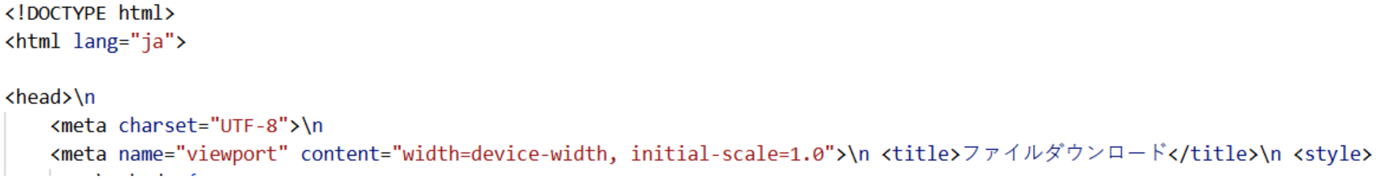
Open Ports and Software

Name	Port	Vendor	Product	Version	Extra Info	First Seen	Last Seen
SSH	22	OpenBSD	OpenSSH	8.9p1 - Ubuntu-3ubuntu0.10	Ubuntu, Linux	12/06/2022	10/25/2025
TLS/HTTP	443	-	-	-	-	12/06/2022	10/11/2025

©2025 Hunt Intelligence, Inc.

Figure 21. The domain "jpjpz1[.]cc" resolves to IP 38.54.50[.]212 hosted by Kaopu Cloud HK Limited (AS138915) in Tokyo, Japan, with active SSH and HTTPS services since December 2022.

The code analysis of the webpage shows an HTML page titled "ファイルダウンロード" and the webpage is written in the Japanese language (lang="ja").

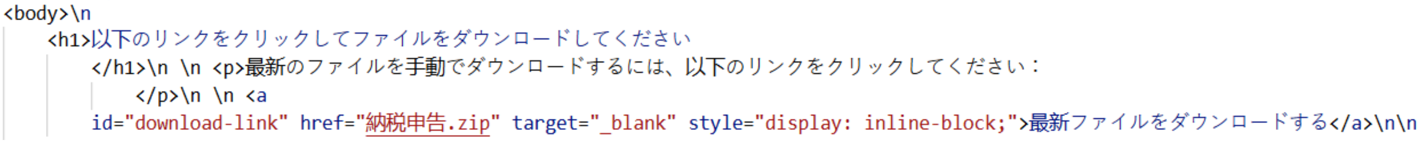


```
<!DOCTYPE html>
<html lang="ja">

<head>\n
    <meta charset="UTF-8">\n
    <meta name="viewport" content="width=device-width, initial-scale=1.0">\n <title>ファイルダウンロード</title>\n <style>
```

Figure 22. HuntSQL™ query results reveal a "ファイルダウンロード" HTML title written in the Japanese language.

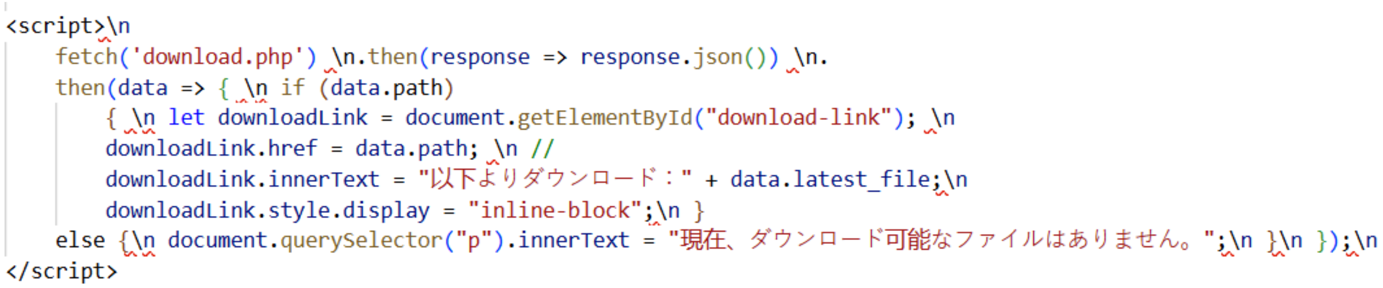
The webpage contains a Japanese-language download button that lures users to "click the link below to download the file," and it initially contains a static anchor pointing to 納税申告**.zip** ("Tax Filing.zip") that is hidden until the page's JavaScript runs.



```
<body>\n
    <h1>以下のリンクをクリックしてファイルをダウンロードしてください
        </h1>\n \n <p>最新のファイルを手動でダウンロードするには、以下のリンクをクリックしてください：
            </p>\n \n <a
        id="download-link" href="納税申告.zip" target="_blank" style="display: inline-block;">最新ファイルをダウンロードする</a>\n\n
```

Figure 23. A ZIP file is downloaded whenever a user clicks the Japanese-language download button, "click the link below to download the file".

Similar to the previous campaign, this script uses Japanese words to handle the download and display error in case of a failed download.



```
<script>\n
    fetch('download.php') \n.then(response => response.json()) \n.
    then(data => { \n if (data.path)
        { \n let downloadLink = document.getElementById("download-link"); \n
        downloadLink.href = data.path; \n //
        downloadLink.innerText = "以下よりダウンロード：" + data.latest_file;\n
        downloadLink.style.display = "inline-block";\n }
    else {\n document.querySelector("p").innerText = "現在、ダウンロード可能なファイルはありません。";\n }\n });\n
</script>
```

Figure 24. Dynamic script logic that displays the ZIP download link only when a valid payload is available from download.php.

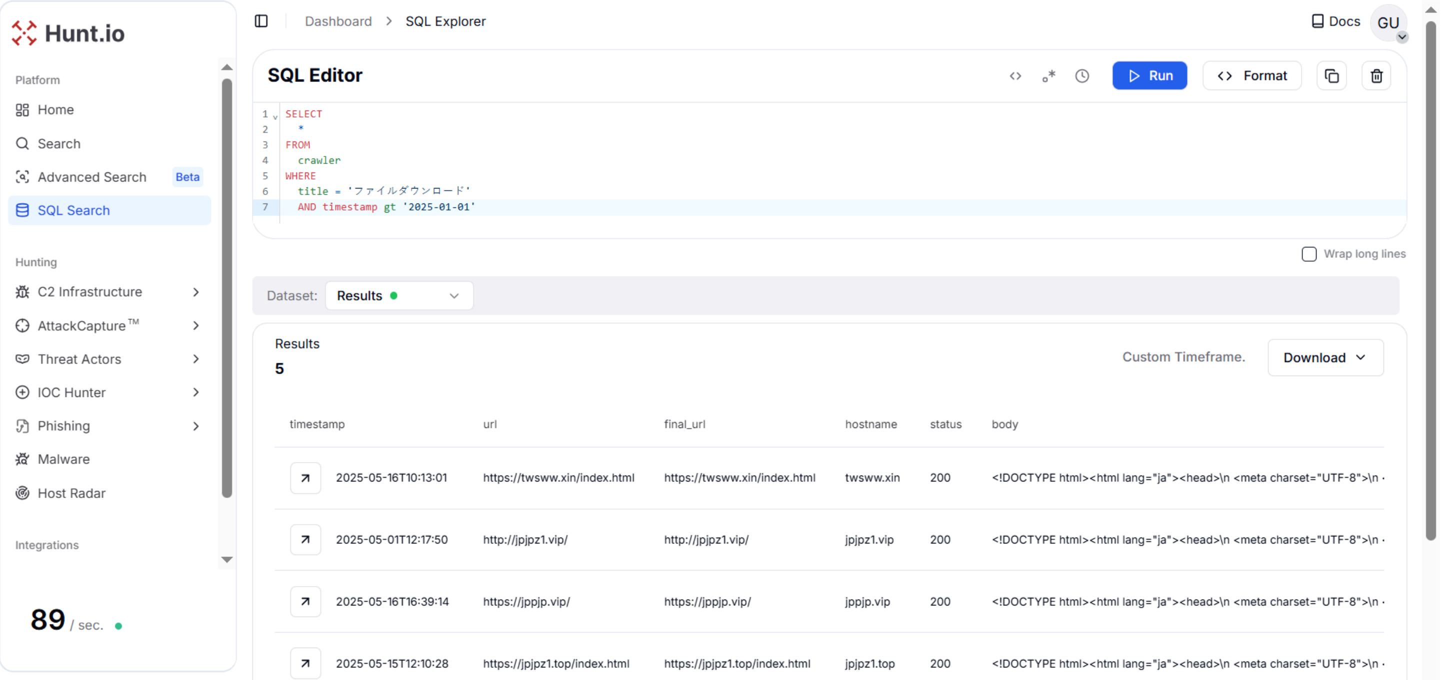
From there, a HuntSQL™ query is designed to extract all crawler records containing pages with the same title "ファイルダウンロード" captured after January 1, 2025. The query returned **3 unique results** that are related to this campaign.

```
SELECT
  *
FROM
  crawler
WHERE
```

```
    title = 'ファイルダウンロード'
    AND timestamp gt '2025-01-01'
```

Copy

Output example:



```
SELECT
  *
FROM
  crawler
WHERE
  title = 'ファイルダウンロード'
  AND timestamp gt '2025-01-01'
```

Results
5

	timestamp	url	final_url	hostname	status	body
↗	2025-05-16T10:13:01	https://twsww.xin/index.html	https://twsww.xin/index.html	twsww.xin	200	<!DOCTYPE html><html lang="ja"><head>\n <meta charset="UTF-8">\n ·
↗	2025-05-01T12:17:50	http://jpjpz1.vip/	http://jpjpz1.vip/	jpjpz1.vip	200	<!DOCTYPE html><html lang="ja"><head>\n <meta charset="UTF-8">\n ·
↗	2025-05-16T16:39:14	https://jppjp.vip/	https://jppjp.vip/	jppjp.vip	200	<!DOCTYPE html><html lang="ja"><head>\n <meta charset="UTF-8">\n ·
↗	2025-05-15T12:10:28	https://jpjpz1.top/index.html	https://jpjpz1.top/index.html	jpjpz1.top	200	<!DOCTYPE html><html lang="ja"><head>\n <meta charset="UTF-8">\n ·

Figure 25. Pivoting on the title "ファイルダウンロード" enabled the identification of 3 additional domains exhibiting similar characteristics linked with the same campaign.

All three webpages follow an identical Japanese-language template, indicating they are part of the same **Japanese-themed lure cluster** tied to the broader **previous campaign**.

The theme of ZIP files shows bureaucratic and financial connotations crafted to deceive Japanese corporate or tax-related targets. The filenames include 給与制度見直しのご案内**.zip** (Notice of Salary System Review), 国税庁の審査により**.zip** (According to the National Tax Agency Review), and 給与制度改定のお知らせ**.zip** (Salary System Revision Notice).

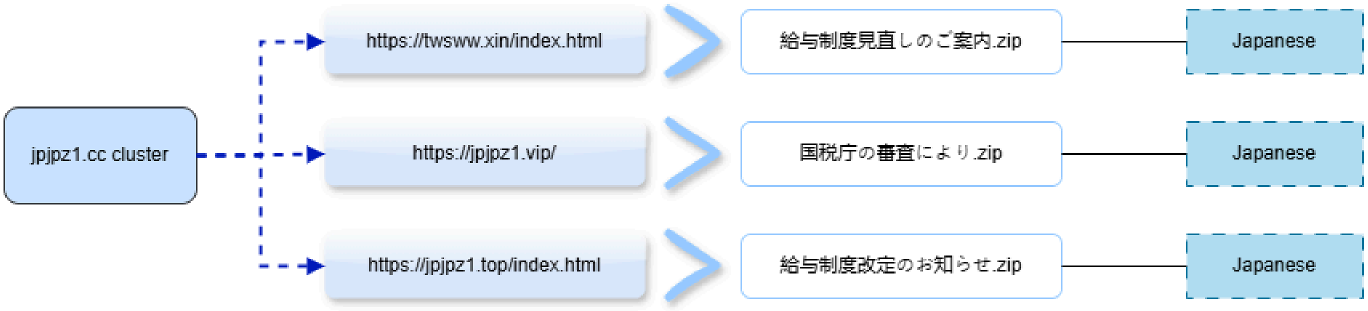

jpjpz1.cc cluster
https://twsww.xin/index.html
https://jpjpz1.vip/
https://jpjpz1.top/index.html
給与制度見直しのご案内.zip
国税庁の審査により.zip
給与制度改定のお知らせ.zip
Japanese
Japanese
Japanese

Figure 26. A mindmap of 3 webpages interconnected with the same title "ファイルダウンロード", showcasing Japanese language pages delivering staged ZIP with tax/finance theme, evidence of campaign targeting Japan.

The uniformity of structure, function, and similar naming conventions points toward a **centralized infrastructure or kit** deployed by an attacker that automatically generates these webpages for tricking users into downloading initial payloads.

The Japanese pages follow the same pattern, showing the kit's final adaptation for local targets and language.

Together, the three clusters reveal a single, automated phishing framework tailored for multiple Asian regions. The next section outlines how to defend against it.

Mitigation Strategies

- Proactively block all discovered domains and monitor for future domains following similar naming conventions (e.g., *.vip, *.xin, *.top, *.site).
- Researchers and security teams can use Hunt.io's datasets (like AttackCapture™ and HuntSQL™) to continuously query for newly observed phishing pages containing download.php or visitor_log.php, helping to identify early-stage infrastructure reuse.
- Detect and flag outbound HTTP requests to suspicious download.php or visitor_log.php endpoints.
- Configure mail gateways to detect ZIP/RAR attachments with HR, tax, or finance-themed filenames in phishing messages.
- Automatically sanitize downloaded or emailed archives before user access to prevent payload execution.
- Conduct awareness campaigns on phishing and fake "official" document downloads, particularly those referencing HR, finance, or government notices.
- Limit users' ability to execute scripts or compressed files from email attachments or browsers.

Implementing these actions reduces exposure to this multilingual campaign and provides a clearer view of its overall structure.

Conclusion

The multilingual phishing and document-themed campaigns uncovered through Hunt.io pivoting reveal a sophisticated, evolving infrastructure that adapts its lures and delivery mechanisms across regions and languages. From China and Taiwan to Japan and Southeast Asia, the adversaries have continuously repurposed templates, filenames, and hosting patterns to sustain their operations while evading conventional detection.

The strong overlap in domain structures, webpage titles, and scripting logic indicates a shared toolkit or centralized builder designed to automate payload delivery at scale. This investigation links multiple clusters to a unified phishing toolkit used across Asia and demonstrates how Hunt.io's HuntSQL™ pivots reveal infrastructure reuse at scale.

The following indicators summarize the infrastructure tied to this campaign and can be used for immediate blocking or enrichment. To explore similar phishing infrastructure and datasets in real time, open a free Hunt.io account or book a demo.

Indicators of Compromise (IOCs)

Root Clusters - Domains

Cluster	Root Domain	Role / Function
English Cluster	gjqygs[.]cn	Command & Control / Central Hosting Node
Chinese Cluster	zxp0010w[.]vip	Hosting Infrastructure for Chinese-language lures
Japanese Cluster	jpjpz1[.]cc	Hosting Infrastructure for Japanese-language lures

Root Clusters - IP

Type	Indicator	Description / Notes
IP Address	38.54.88[.]44	Hosting IP associated with Chinese cluster domain zxp0010w[.]vip
IP Address	38.54.17[.]167	Hosting IP associated with English cluster domain gjqygs[.]cn
IP Address	38.54.50[.]212	Hosting IP associated with Japanese cluster domain jpjpz1[.]cc

Campaign Root: zxp0010w[.]vip Cluster (Traditional Chinese)

Domain / URL	Payload File	Language / Theme
https://twsw[.]cc/download.html	稅務電子發票名單.rar	Traditional Chinese - Tax Invoice List
https://xinwenwamg[.]net/index.html	index.html	Traditional Chinese - Generic Landing Page

Domain / URL	Payload File	Language / Theme
https://z2tw[.]vip/index.html	進出口申報.zip	Traditional Chinese - Import/Export Declaration
https://cq1tw[.]icu/index.html	申請平台.zip	Traditional Chinese - Application Platform
http://twswzz[.]xin	財務負責人核對後回傳（電腦版）1.zip	Traditional Chinese - Financial Confirmation Form
https://cq1tw[.]top/index.html	條例檔案.zip	Traditional Chinese - Regulatory Document
http://twmm[.]shop	通知函.rar	Traditional Chinese - Notification Letter
https://z2tw[.]xin	添付資料一覧.zip	Japanese - Attached Documents List
http://twswzz[.]icu	《商業登記條例修改通知書》Bilingual.PCVersion.zip	Traditional Chinese - Business Registration Amendment Notice
https://qiqi1[.]xin/index.html	香港金融管理局企業相關條例（電腦版）.zip	Traditional Chinese - HK Monetary Authority Regulations

Campaign Root: gjqygs[.]cn Cluster (English / Indonesian)

URL	Payload File	Language
http://3381536ffe13739277b0a87c08a66596.bulinouui[.]sbs	दाखिल करने के दस्तावेज़.zip	English
https://6358bdf15f655e7e305eacaf385cd12.bulinouui[.]sbs/?1d794ebf8cc16e0770adc215e34d26a0	दाखिल करने के दस्तावेज़.zip	English
http://53d9da1f7632f687dde3b0ec4df00710.bulinouui[.]sbs	दाखिल करने के दस्तावेज़.zip	English
http://3381536ffe13739277b0a87c08a66596.bulinouui[.]sbs	दाखिल करने के दस्तावेज़.zip	English
http://199cb150cec25af3132ddd4e47b37248.bulinouui[.]sbs	Tax return documents.tar.gz	English
http://27160fcce1e199401dde5e01ce829006.ttcskhdl[.]lol	Tax return documents.tar.gz	English
https://www.bulinouui[.]sbs	Tax return documents.tar.gz	English
https://11c979baeb8bddc12e79ad4def0964e94.bulinouui[.]sbs	Tax-penalty-notification.zip	English
http://www.wojkejys[.]lat	Dokumen Pematuhan Cukai.rar	English
https://vip.gaelh[.]cn	Tax Filing Documents.zip	English
https://5289c03d6d33ac4cf474de436f6bbf47.bulinouui[.]sbs	दाखिल करने के दस्तावेज़.zip	English

Campaign Root: jpjpz1[.]cc Cluster (Japanese)

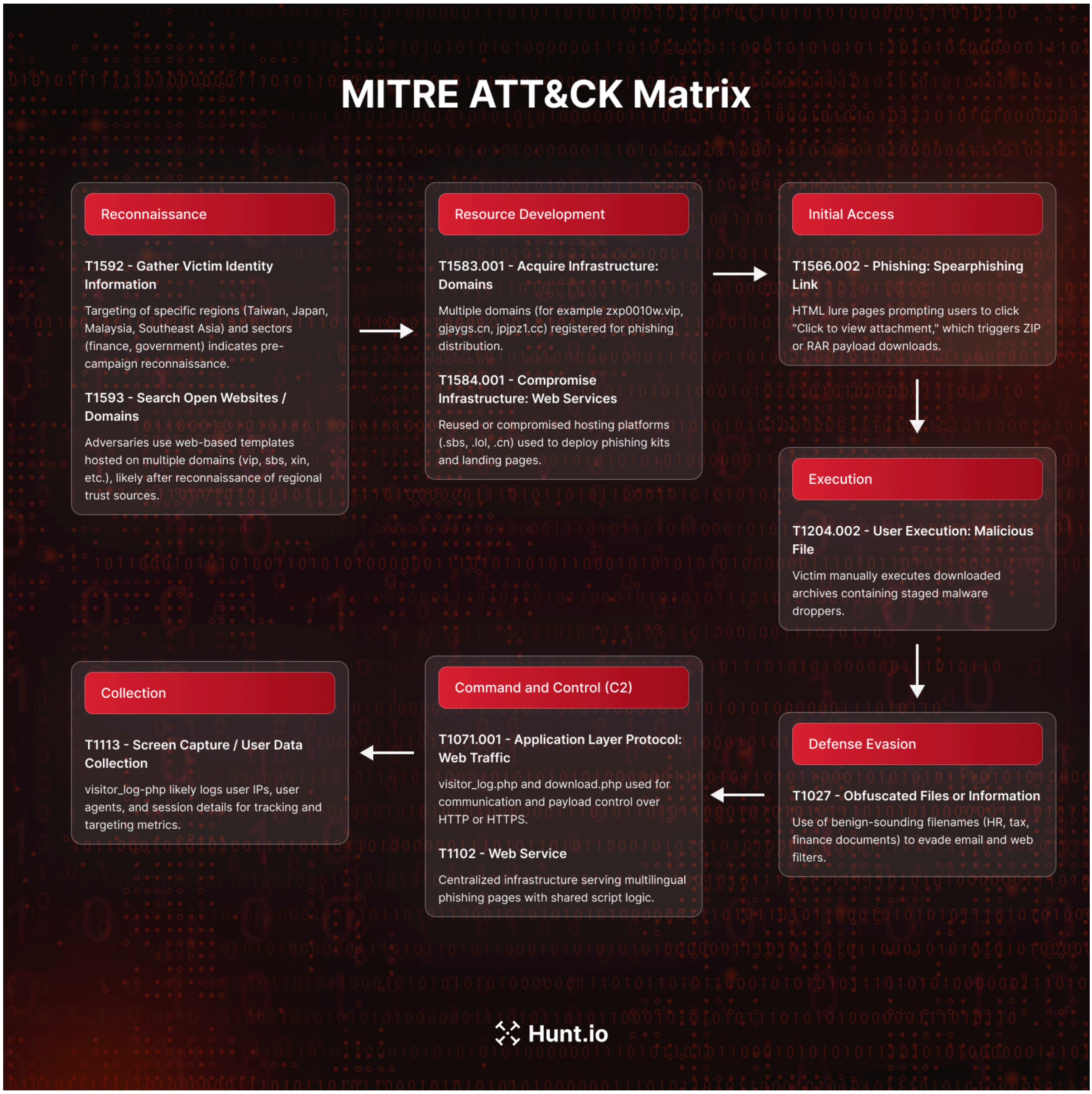
Domain / URL	Payload File	Language / Theme
https://twsww[.]xin/index.html	給与制度見直しのご案内.zip	Japanese - Salary System Review Notice
https://jpjpz1[.]vip	国税庁の審査により.zip	Japanese - National Tax Agency Review
https://jpjpz1[.]top/index.html	給与制度改定のお知らせ.zip	Japanese -- Salary System Revision Notice

Domains and IPs - All Clusters

Domain	IP Address
z2tw[.]vip	38.54.16[.]25
cq1tw[.]icu	38.54.1[.]105
cq1tw[.]top	38.54.17[.]174
qiqi1[.]xin	38.54.119[.]194
xinwenwamg[.]net	38.54.16[.]25
twswzz[.]xin	38.54.107[.]195
twsw[.]cc	103.127.219[.]148
zxp0010w[.]vip	38.54.88[.]44
z2tw[.]xin	38.54.16[.]254
twmm[.]shop	38.54.1[.]23
twswzz[.]icu	38.60.199[.]26
qiqi1[.]xin	38.54.119[.]194
jpjpz1[.]top	38.54.88[.]103
twsww[.]xin	38.54.107[.]103
jpjpz1[.]vip	154.205.139[.]195
jppjp[.]vip	154.205.139[.]223
zcqiyess[.]vip	38.54.17[.]132
vip.gaelh[.]cn	38.54.17[.]132

MITRE ATT&CK Matrix

Below is a visual map of the techniques we observed across the campaign clusters.



MITRE ATT&CK Matrix

Reconnaissance

T1592 - Gather Victim Identity Information

Targeting of specific regions (Taiwan, Japan, Malaysia, Southeast Asia) and sectors (finance, government) indicates pre-campaign reconnaissance.

T1593 - Search Open Websites / Domains

Adversaries use web-based templates hosted on multiple domains (vip, sbs, xin, etc.), likely after reconnaissance of regional trust sources.

Resource Development

T1583.001 - Acquire Infrastructure: Domains

Multiple domains (for example zxp0010w.vip, gjaygs.cn, jpjpz1.cc) registered for phishing distribution.

T1584.001 - Compromise Infrastructure: Web Services

Reused or compromised hosting platforms (.sbs, .lol, .cn) used to deploy phishing kits and landing pages.

Initial Access

T1566.002 - Phishing: Spearphishing Link

HTML lure pages prompting users to click "Click to view attachment," which triggers ZIP or RAR payload downloads.

Execution

T1204.002 - User Execution: Malicious File

Victim manually executes downloaded archives containing staged malware droppers.

Defense Evasion

T1027 - Obfuscated Files or Information

Use of benign-sounding filenames (HR, tax, finance documents) to evade email and web filters.

Command and Control (C2)

T1071.001 - Application Layer Protocol: Web Traffic

visitor_log.php and download.php used for communication and payload control over HTTP or HTTPS.

T1102 - Web Service

Centralized infrastructure serving multilingual phishing pages with shared script logic.

Collection

T1113 - Screen Capture / User Data Collection

visitor_log-php likely logs user IPs, user agents, and session details for tracking and targeting metrics.

Hunt.io

Fig 27. MITRE ATT&CK techniques observed across Chinese, English, and Japanese clusters

Tactic	Technique ID	Technique Name	Observed in Campaign / Description
Reconnaissance	T1592	Gather Victim Identity Information	Targeting of specific regions (Taiwan, Japan, Malaysia, Southeast Asia) and sectors (finance, government) indicates pre-campaign reconnaissance.
Reconnaissance	T1593	Search Open Websites/Domains	Adversaries use web-based templates hosted on multiple domains (.vip, .sbs, .xin, etc.) likely after reconnaissance of regional trust sources.
Resource Development	T1583.001	Acquire Infrastructure: Domains	Multiple domains (e.g., zxp0010w.vip, gjqygs.cn, jpjpz1.cc) registered for phishing distribution.
Resource Development	T1584.001	Compromise Infrastructure: Web Services	Reused or compromised hosting platforms (.sbs, .lol, .cn) to deploy phishing kits.

Tactic	Technique ID	Technique Name	Observed in Campaign / Description
Initial Access	T1566.002	Phishing: Spearphishing Link	HTML pages luring victims to click "Click to view attachment" button, triggering ZIP/RAR payload download.
Execution	T1204.002	User Execution: Malicious File	Victim manually executes downloaded archives containing staged malware droppers.
Defense Evasion	T1027	Obfuscated Files or Information	Use of benign-sounding filenames (HR, tax, finance documents) to evade email and web filters.
Command and Control (C2)	T1071.001	Application Layer Protocol: Web Traffic	Use of visitor_log.php and download.php for communication and payload control over HTTP(S).
Command and Control (C2)	T1102	Web Service	Centralized infrastructure serving multilingual phishing pages with shared script logic.
Collection	T1113	Screen Capture / User Data Collection	visitor_log.php likely logs user IPs, user-agents, and session details for tracking and targeting metrics.