Unmasking the CoGUI Phishing Kit, the Major Chinese Phishing-as-a-Service Targeting Japan

Shadow Liu, Lime Chen, Albert Song, Strawberry Donut

TeamDonut Contributors

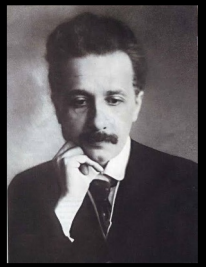
Shadow Liu

Shadow specializes in incident response and threat intelligence.
Her current focus lies in tracking underground markets and phishing campaigns, transforming these findings into actionable intelligence.

Lime Chen

With over 10 years of experience in cybersecurity, Lime specializes in threat intelligence, particularly focusing on East Asia and the underground phishing market.

Albert Song

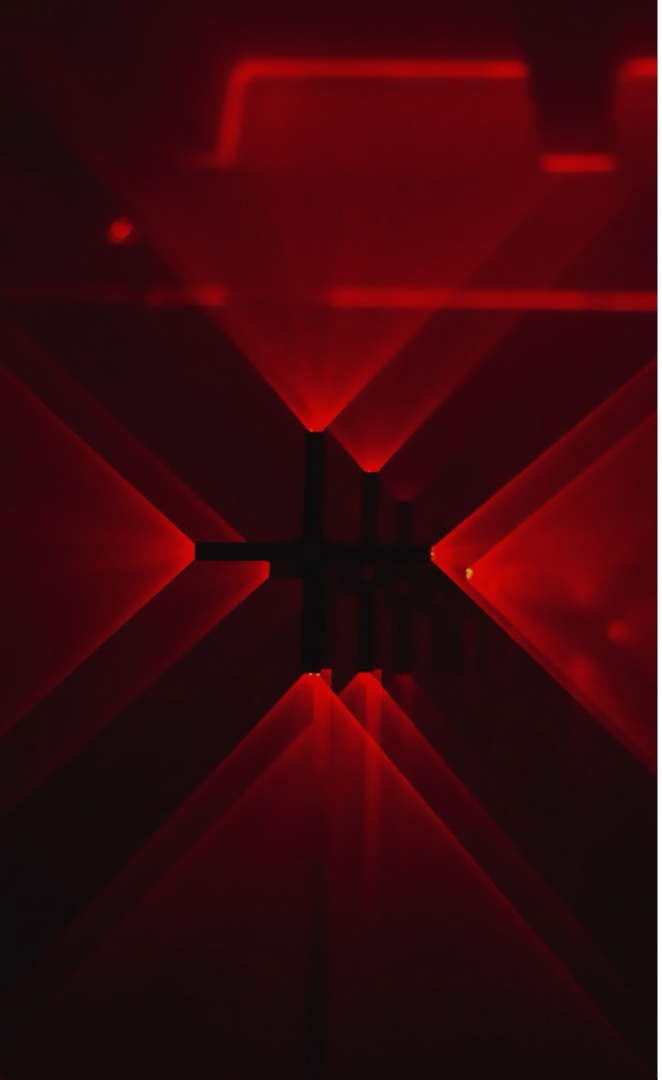


As an architect of threat intelligence platforms, Albert's work emphasizes on designing scalable automated systems for analyzing IoCs, actor infrastructure mapping, and the utilization of threat data to support real-time detection and response.

Strawberry Donut

A data scientist with expertise in fraud detection and Al.

Extensive background in implementing anti-fraud measures within leading banks, securities firms, and internet companies.



Agenda

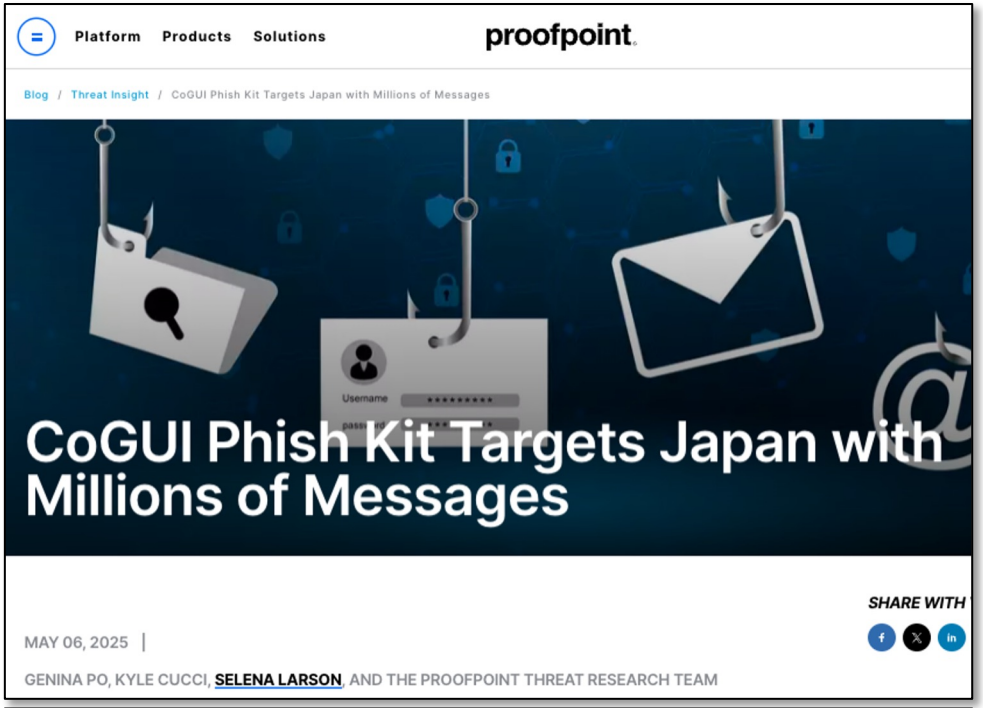
- CoGUI Phishing Attacks Targeting Japan
- Unmasking CoGUI Phishing Kit
- Monitoring Phisher Activities on Telegram
- Threat Actor Profiling
- Key Takeaways

Disclaimer

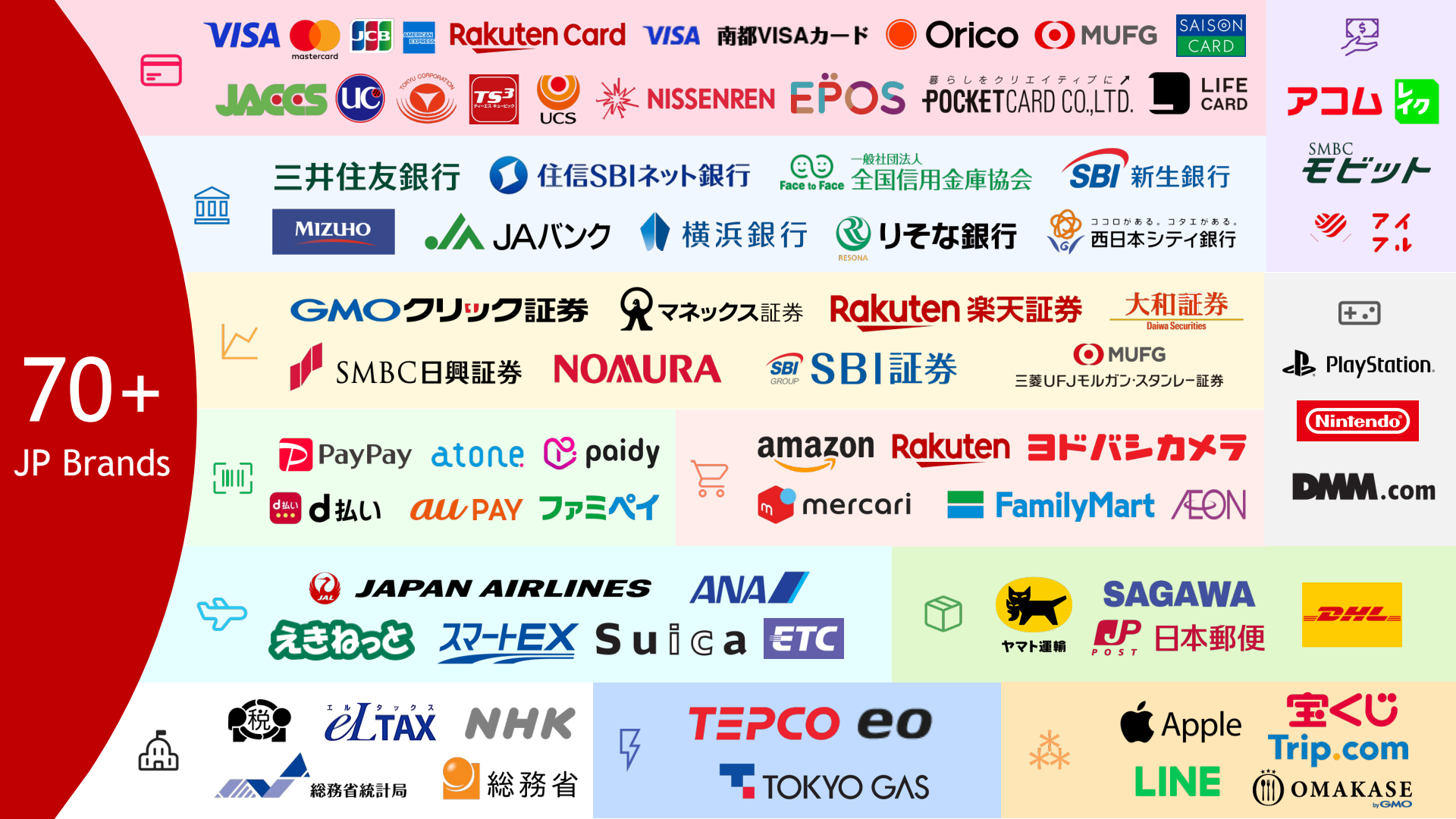
This research is conducted in full compliance with the law, no criminal activity was involved.

CoGUI Phishing Attacks Targeting Japan

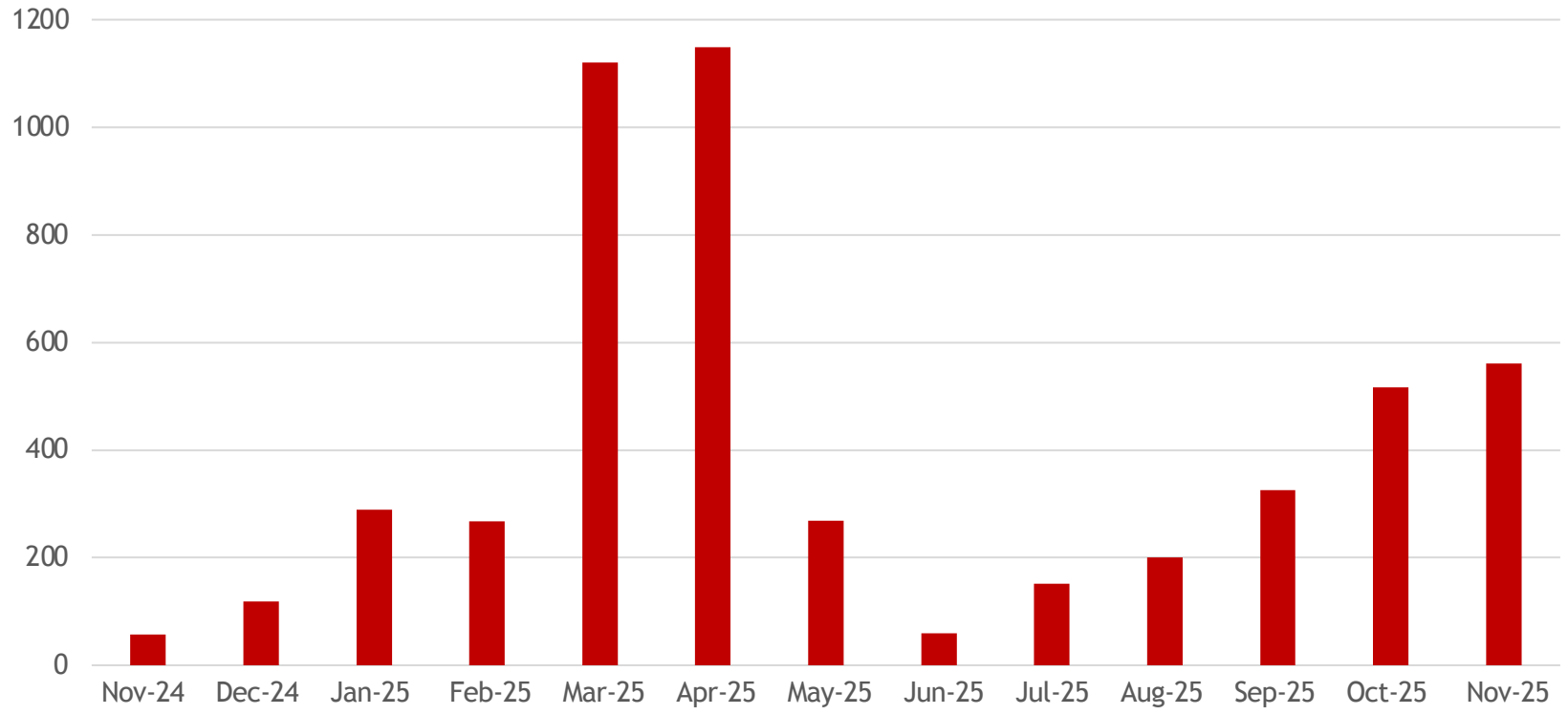
In May 2025, vendors named the phishing kit used in the massive Japanese campaigns as “CoGUI”



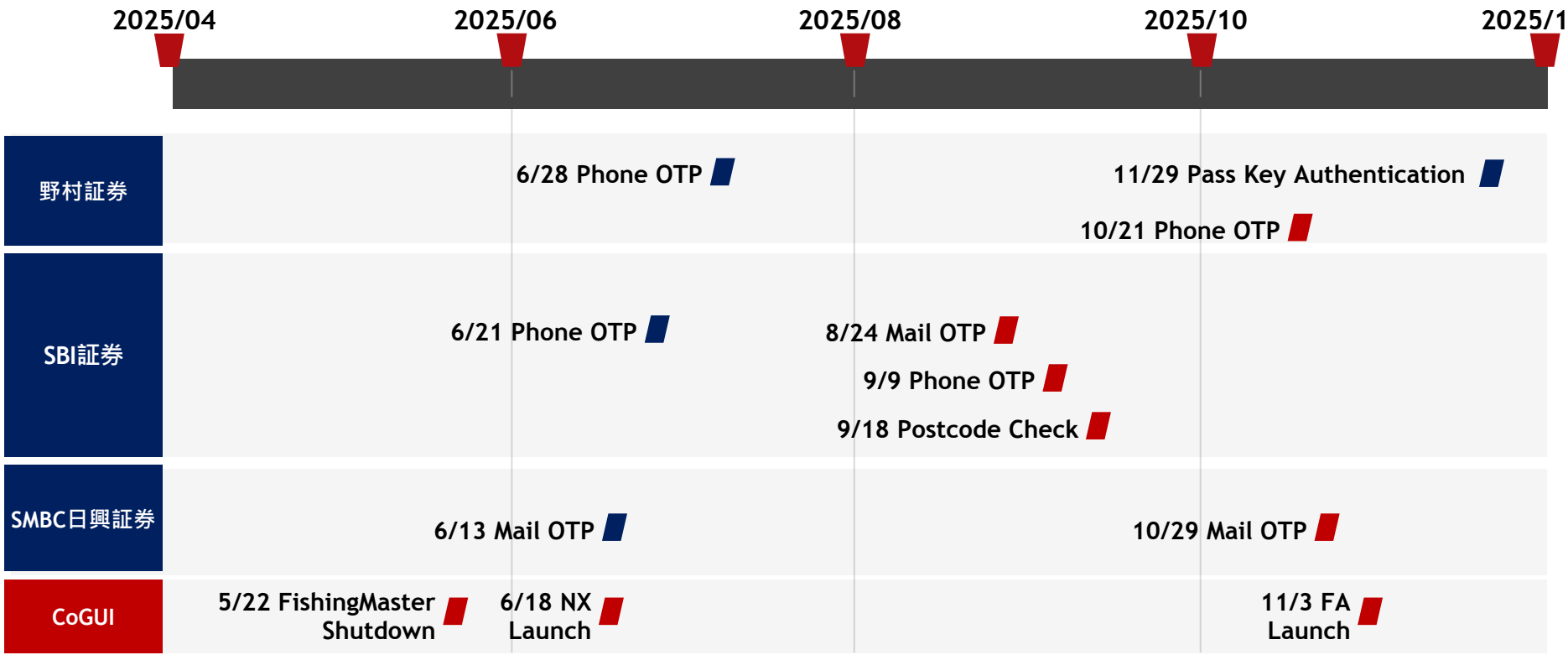
Sources:
1. Proofpoint: CoGUI Phish Kit Targets Japan with Millions of Messages
2. URLScan: Rise of Oriental Gudgeon


70+
JP Brands
VISA
mastercard
JCB
AMERICAN EXPRESS
Rakuten Card
VISA
南都VISAカード
Orico
MUFG
SAISON CARD
JACCS
UC
TOKYU CORPORATION
TS3
UCS
NISSENREN
EPOS
暮らしをクリエイティブに
POCKETCARD CO.,LTD.
LIFE CARD
アコム
レイク
三井住友銀行
住信SBIネット銀行
Face to Face
一般社団法人
全国信用金庫協会
SBI 新生銀行
SMBC
モビット
MIZUHO
JAバンク
横浜銀行
りそな銀行
RESONA
ココロがある。コタエがある。
西日本シティ銀行
アイフル
GMOクリック証券
マネックス証券
Rakuten 楽天証券
大和証券
Daiwa Securities
SMBC日興証券
NOMURA
SBI GROUP
SBI証券
MUFG
三菱UFJモルガン・スタンレー証券
PlayStation
Nintendo
DMM.com
PayPay
atone
paidy
d払い
au PAY
ファミペイ
amazon
Rakuten
ヨドバシカメラ
mercari
FamilyMart
AEON
JAPAN AIRLINES
ANA
えきねっと
スマートEX
Suica
ETC
ヤマト運輸
SAGAWA
JP POST
日本郵便
DHL
税
eLTAX
NHK
総務省統計局
総務省
TEPCO
eo
TOKYO GAS
Apple
宝くじ
Trip.com
LINE
OMAKASE
by GMO

CoGUI Phishing Domains Stats cross 24/25



CoGUI’s Fraud Prevention Arms Race



Unmasking CoGUI Phishing Kit

Meet the CoGUI Phishing Family

FishingMaster

Period: 2024-09 ~ 2025-05
TG Channel: @userfm920666
TG User: @userfm920

NX

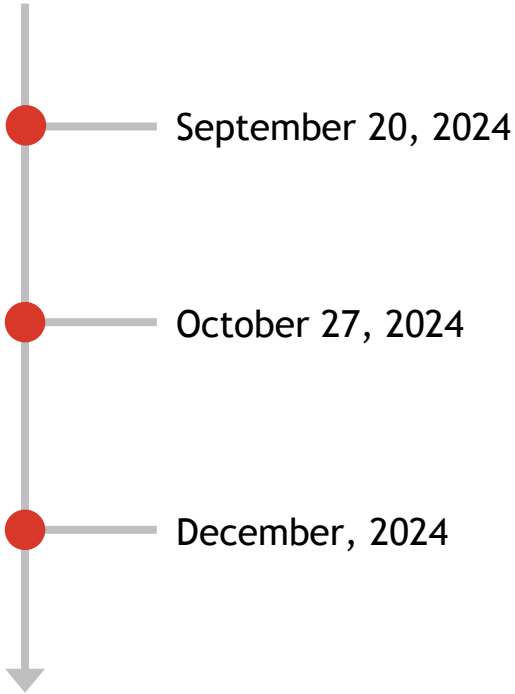
Period: 2025-06 ~ 2025-11
TG Channel: @nx001channel
TG User: @nx0073

FA

Period: 2025-11 ~
TG User: @redfaff

Launch of FishingMaster PhaaS

Launch of FishingMaster PhaaS



September 20, 2024

FishingMaster Telegram channel launched

October 27, 2024

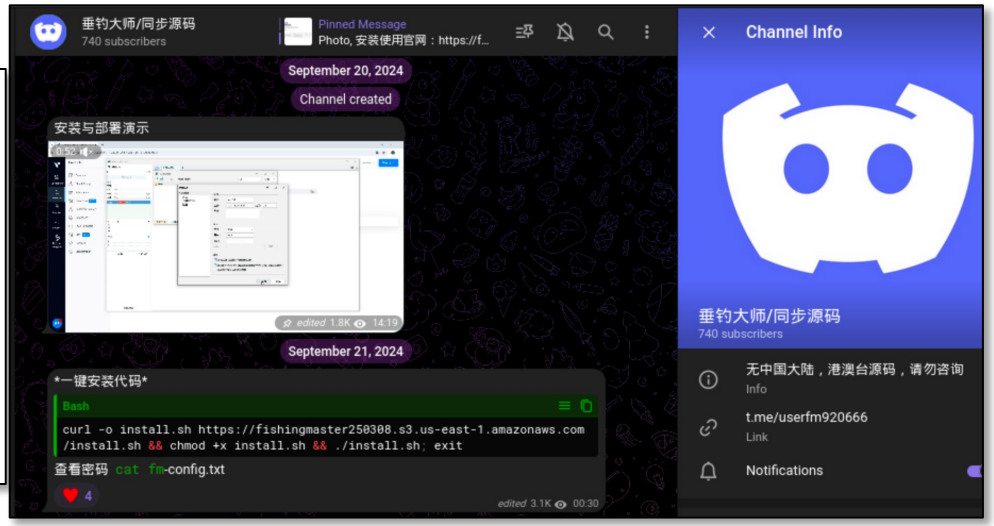
Our telemetry first detected FishingMaster phishing sites

December, 2024

The `codeName` variable added to phishing kit templates

FishingMaster PhaaS 垂钓大师

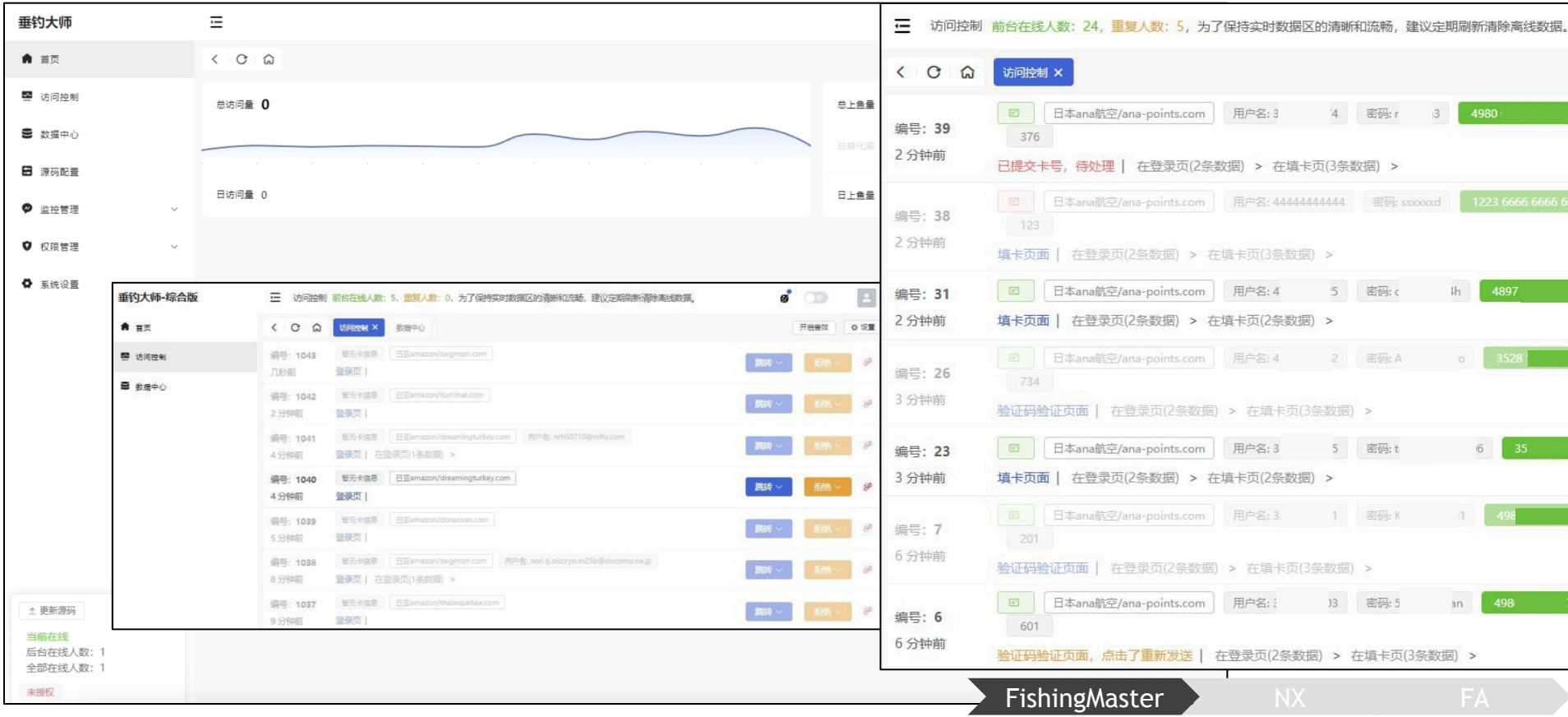
- **Telegram Channel Created Date:** 2024-09-20
- **Telegram Channel:** @userfm920666
- **Telegram User ID:** @userfm920
- **Setup guide:** fmdocs[.]world



FishingMaster Setup Guide

1. Purchase license key from the PhaaS author
2. Setup the VPS according to the manual
   - System requirements (OS: Ubuntu)
   - Install command (copy & paste one-liner to execute install.sh)
3. The script displays randomized admin panel credentials; login and activate the license
4. Point the phishing domain to your VPS
5. Pick a phishing theme, pair it with the domain

FishingMaster PhaaS Admin Panel



Early Activities of FishingMaster

- Initially, FishingMaster frequently advertised its services in various Telegram communities
- Between November and December 2024, the group claimed that they were able to provide phishing kits for over 40 Japanese services

Early Activities of FishingMaster

Translated FishingMaster Advertisement

Swept along by the tides of the 20th century, China endured endless suffering. One of the most searing lessons was forged during the agony of the War of Resistance against Japan invasion. At that time, China was a nation with backward weaponry and a fragile economy. Faced with foreign aggression, the people could only exhaust themselves to the limit, engaging in a brutal, all-or-nothing resistance.

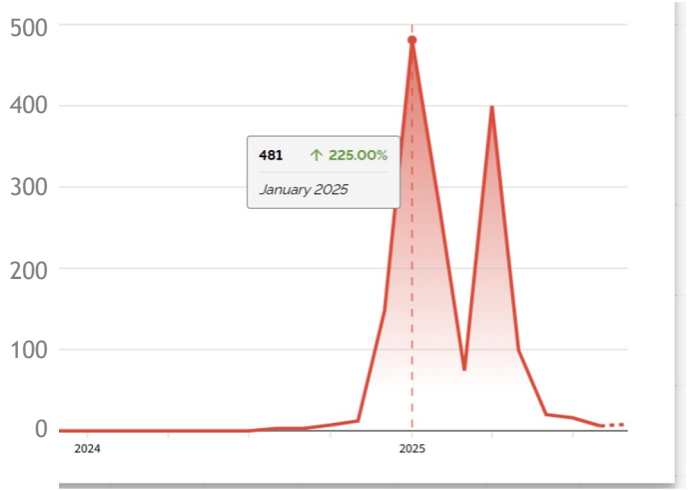
Times have changed. Today's China is no longer what it once was: technology has advanced, weapons are modernized, and national power has grown dramatically. But unlike the gun-smoke-filled past, we are born into an era of peace. We cannot simply pick up rifles and charge at the enemy as our forebears did.

Instead, we can use 🔥 The Fishing Master (over 60 Japanese source kits) 🔥 to initiate a **new kind of war** — one that forces those postwar generation Japs, who have never paid for their crimes, to finally understand this:
The fire of revenge is now lit, no one can escape it.

- **Weaponized Nationalism:** Leverages historical anger (WWII/Sino-Japanese War) to frame financial cybercrime as "patriotic" duty
- **The "Digital Revenge" Narrative:** Positions PhaaS tools not as theft, but as a moral crusade to force modern Japanese generations to "pay for past crimes"

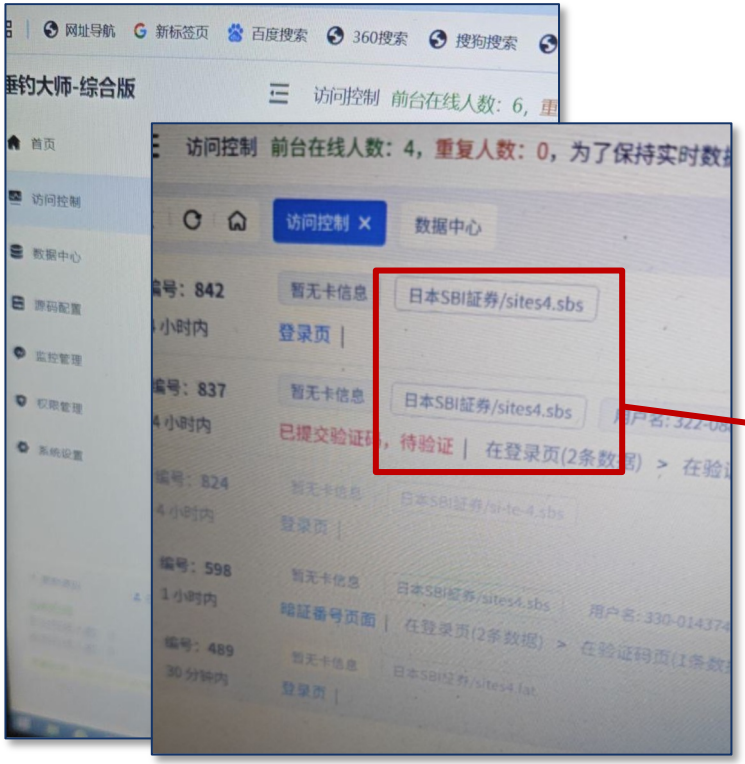
Widely-Used PhaaS in Japanese Phishing Campaigns

- Shodan shows that FishingMaster admin panels have been active since 2024/8
- In 2025/1, approximately 500 admin panels were concurrently operational, coinciding with a period of active phishing campaigns against Japan organizations

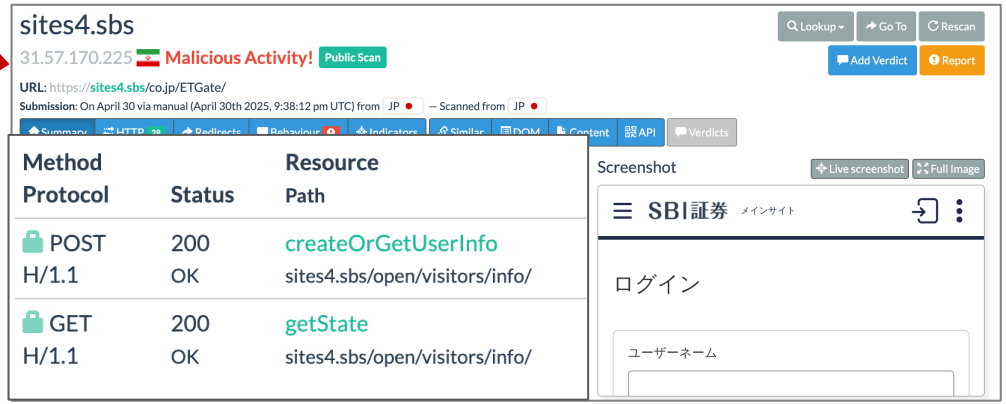


Shodan Trend Search
title:”fishingmaster”

Telegram Monitoring Revealed FishingMaster Phishing Websites



- We analyze domains in screenshots posted on TG to identify recurring API patterns
- This `sites4[.]sbs` domain is cited in URLScan's Oriental Gudgeon report, which is consistent with Proofpoint's CoGUI report



Phishing Website Deployments

- **FishingMaster's phishing websites use a simple HTML template:** content is built from a single CSS file and a single JavaScript file **bundled with vite and using Vue.js**, with all API endpoints defined inside
- **Each phishing kit use its own JavaScript file**, and thus the logic remains analyzable even if scanners fail to load the live phishing page

```
<!DOCTYPE html>
<html lang="jp">
  <head>
    <meta charset="UTF-8">
    <link rel="icon" type="image/png" href="./faviconV2.png">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="robots" content="noindex, nofollow">
    <title></title>
    <script type="module" crossorigin src="./assets/index-DrMXsVoI.js"></script>
    <link rel="stylesheet" crossorigin href="./assets/index-BPpz02Uo.css">
  </head>
  <body>
    <div id="app"></div>
  </body>
</html>
```

FishingMaster API and codeName

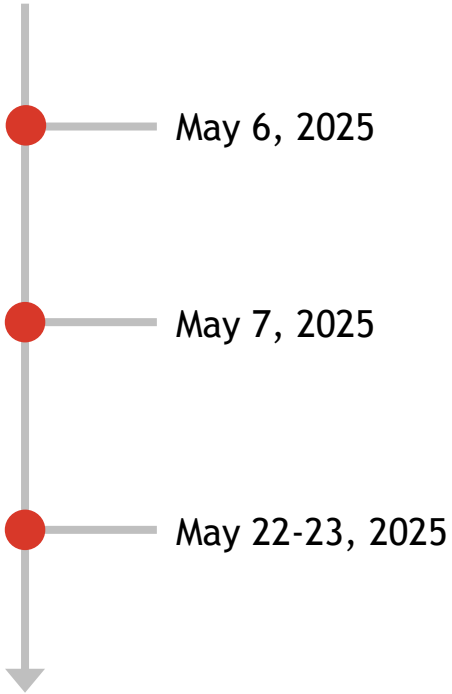
```
    if (!t.isConnected()) t.connect().then(() => {
        const s = As(Is);
        s.provide("socketClient", t), s.use(ks()), s.mount("#app")
    }).catch(s => {
        console.error("WebSocket连接失败", s)
    });
    else {
        const s = As(Is);
        s.provide("socketClient", t), s.use(ks()), s.mount("#app")
    }
} else {
    const t = await ie.post("/visitors/info/createOrGetUserInfo", {
            currentState: 2,
            browserInfo: Lh(),
            domain: window.location.hostname,
            codeName: "日本SBI証券",
```

```
function Kt() {
    const e = z({
            officialWebsite: "https://faq.sbisec.co.jp/category/
            49193331-ae5a-4ba7-8d29-740f5a82a31b/"
        }),
        t = z({
            title: "配送状況",
            packageNumberTitle: "あなたの荷物番号",
            notice: "配送失敗の通知",
            description1: "配送先住所が不明瞭のため、お荷物は配達されませんでした",
            description2: "お荷物は当社の運用センターに戻りました",
            description3: "住所を更新してください。再配送を行います",
            button: "続ける"
```

- *codeName* is the phishing kit template name listed in admin panel
- *officialWebsite* is the redirected destination for cloaking
- API calls are meaningful path, e.g.
  - /open/visitors/info/createOrGetUserInfo
  - /open/visitors/info/saveLoginInfo
  - /open/visitors/info/saveCustomCaptcha
  - /open/visitors/info/isBlacklist

Change and Disappear of FishingMaster PhaaS

Evolution and Disappearance of FishingMaster PhaaS



May 6, 2025

A vendor report named “CoGUI” phishing kit

May 7, 2025

FishingMaster’s key API path changed to `coguicogui`

May 22-23, 2025

FishingMaster PhaaS license server and Telegram channel were shut down

The “CoGUI” API Becomes Real After Vendor Report

- New API call tied to fingerprinting: /open/visitors/info/validateHuman
  - Show 404 error page if fingerprint check fails.
- Most API calls are meaningless path
  - createOrGetUserInfo -> coguicogui

```
async function G5() {
    await v3(), await Jx(200, 500);
    const x = await E3();
    if ((await Vx.post("/visitors/info/validateHuman", {
        fp: x,
        domain: window.location.hostname
    })).code !== 1e3) {
        document.body.innerHTML = "";
        const n = document.createElement("h2");
        n.textContent = "404 Error: Page not found,Sorry, we couldn't
        find the page you're looking for.", n.style.margin = "14px",
        document.body.appendChild(n);
        return
    }
```

JS > fm-key-func.js > Zr

```
1   async function Zr() {
19          }
20      } else {
21          const t = await ae.post("/visitors/info/
            createOrGetUserInfo", {
22              currentState: 2,
23              browserInfo: up(),
24              domain: window.location.hostname,
25              codeName: "日本SBI証券",
26              buttons: {
27                  skip: ["2", "5", "14", "77"],
28                  reject: ["2", "5", "14"]
29              },
30              views: ["1"]
31          }),
```

JS > cogui-key-func.js > G5

```
1   async function _4() {
            await m4()
19      } else {
20          await Jx(100, 200);
21          const n = await Vx.post("/visitors/info/coguicogui", {
22              currentState: 2,
23              browserInfo: w3(),
24              domain: window.location.hostname,
25              codeName: "日本SBI証券",
26              buttons: e,
27              views: a6(["1"])
28          }),
29              {
30
31
```

FishingMaster PhaaS API: /open/visitors/info/{apiname}

Active period: Sep. 2024 ~ early May 2025

same function with different name

- createOrGetUserInfo
- isBlacklist
- getState
- saveLoginInfo
- saveAccountInfo
- savePasscode
- saveUserInfo
- saveCustomCaptcha
- updateState
- …

Active period: May 7th ~ late June 2025

- coguicogui
- ibsibs
- gsgsgsgs
- slisli
- saveAccountInfo
- savePasscode
- suisui
- scciscci
- ususus
- **validateHuman (*)**
- …

Shared Features:

1. Used the same “codeName” and “officialWebsite” across all domains of each campaign; shared the same hash
2. Able to identify the targeted brand even after redirection

(*) Newly added:

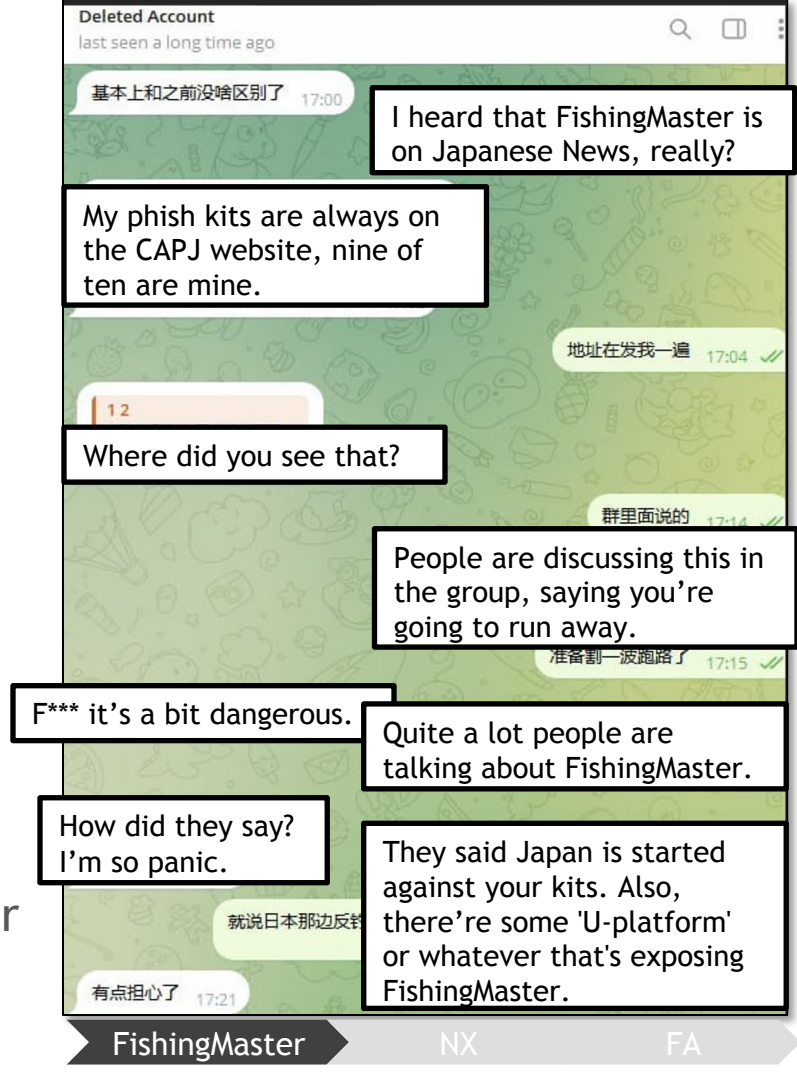
1. Introduced evasion techniques such as obfuscation, fingerprinting modules (**validateHuman**), and Selenium detection
2. Modularized JavaScript files with different imported functions
3. Used meaningless strings as API path

Panic and Shutdown

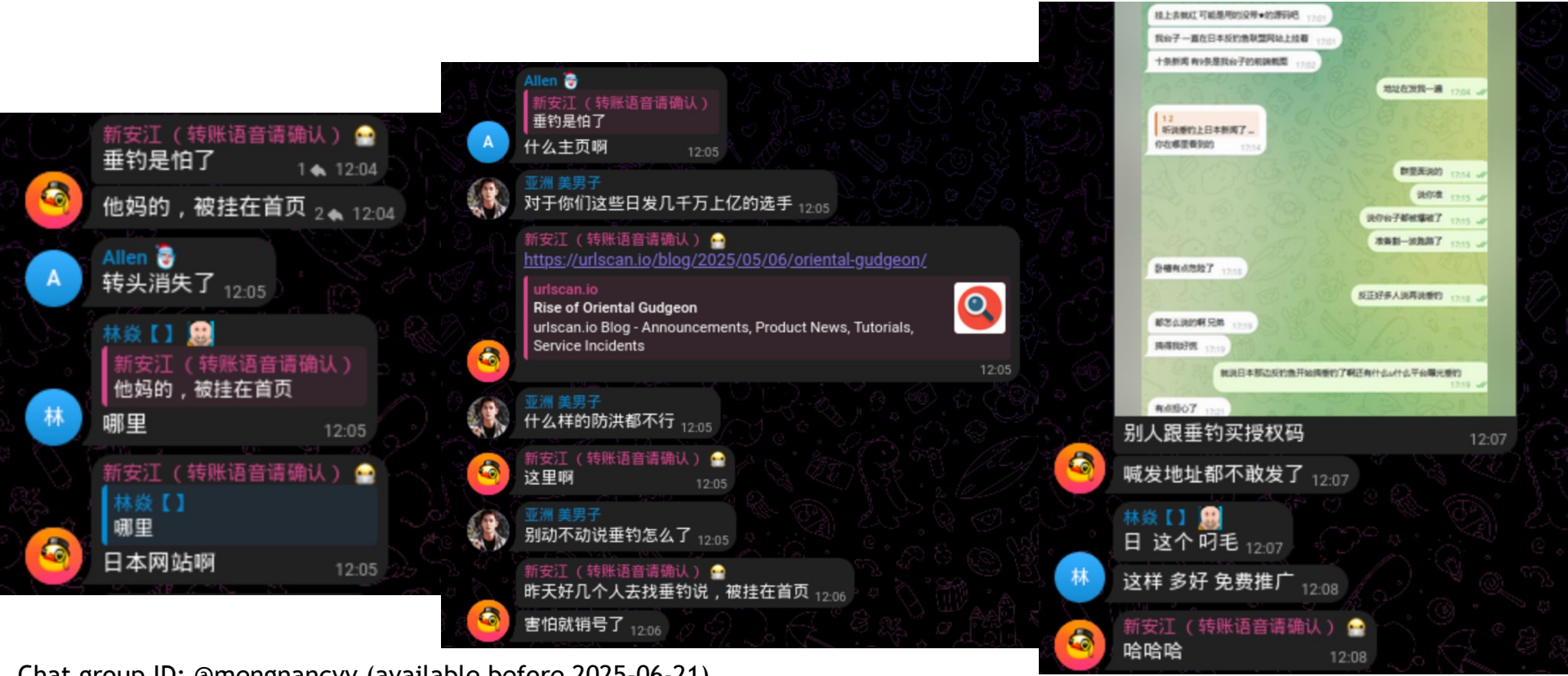
- Telegram chat between FishingMaster (@userfm920) and a client (@z17169708)
- The author is aware that his phishing websites are consistently featured in Council of Anti-Phishing Japan (フィッシング対策協議会) announcements
- However, recent vendor analysis reports targeting FishingMaster have caused him to panic
- Instantly, FishingMaster PhaaS license server and Telegram channel were shut down

Panic and Shutdown

- Telegram chat between FishingMaster (@userfm920) and a client (@z17169708)
- The author is aware that his phishing websites are consistently featured in Council of Anti-Phishing Japan (フィッシング対策協議会) announcements
- However, recent vendor analysis reports targeting FishingMaster have caused him to panic
- Instantly, FishingMaster PhaaS license server and Telegram channel were shut down.

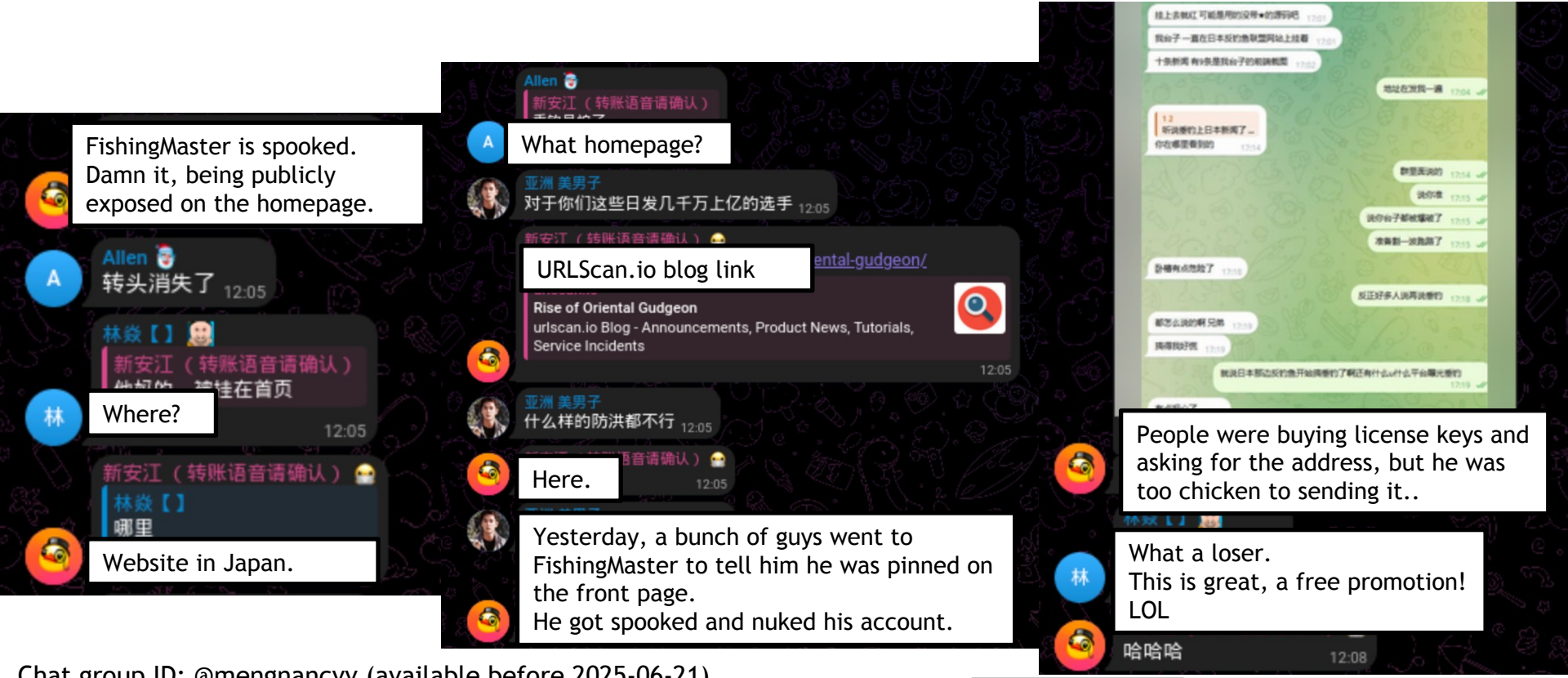


Underground Discussions Regarding the FishingMaster Shutdown



Chat group ID: @mengnancvv (available before 2025-06-21)

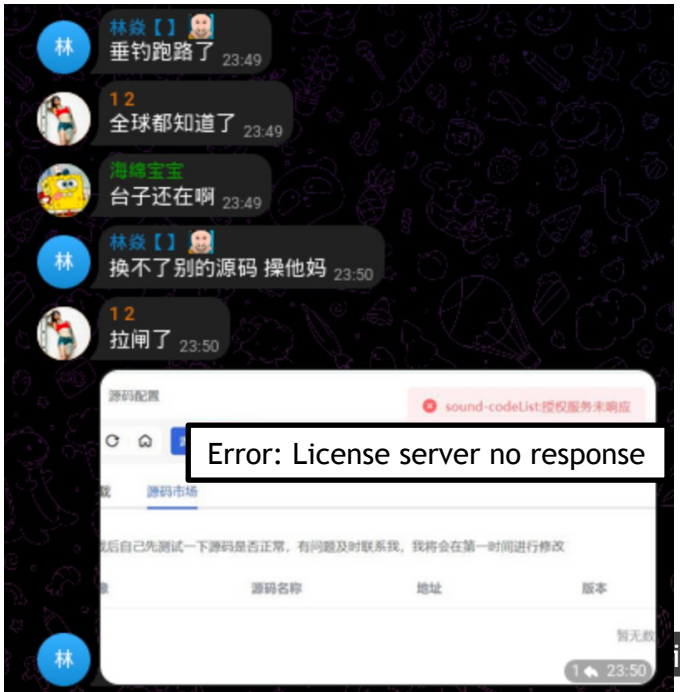
Underground Discussions Regarding the FishingMaster Shutdown



Chat group ID: @mengnancvv (available before 2025-06-21)

Underground Discussions Regarding the FishingMaster Shutdown

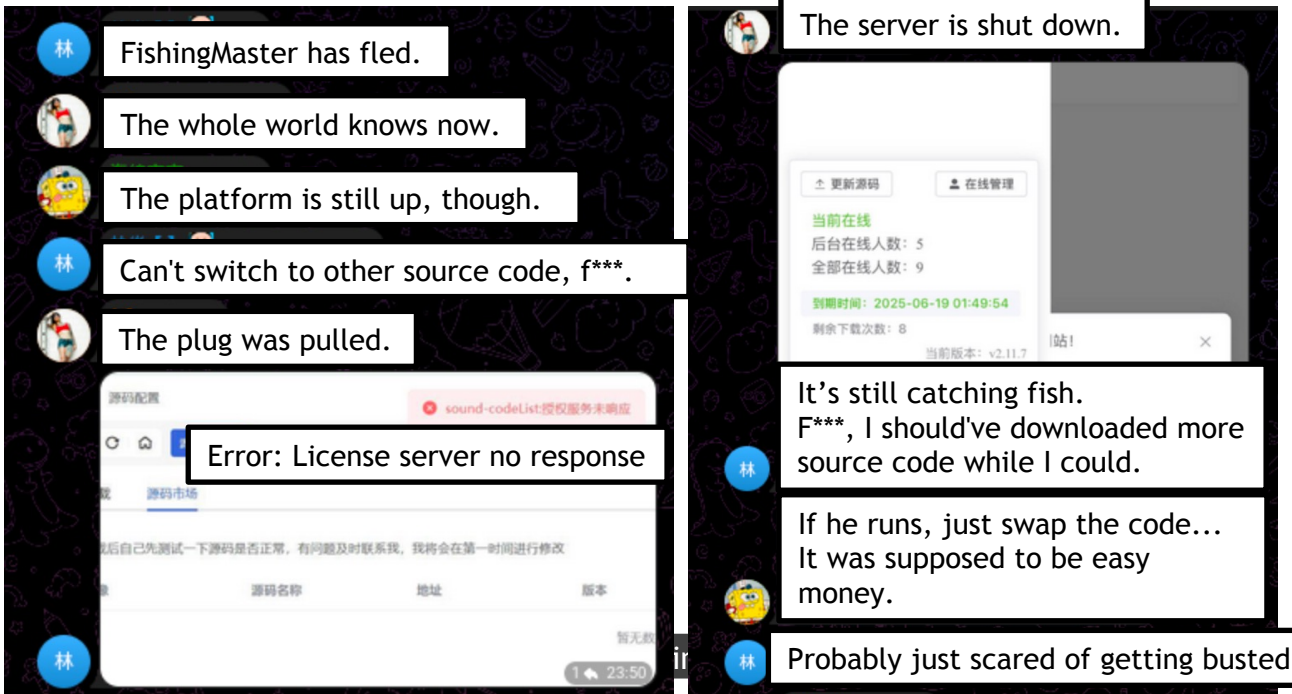
- Kits remain functional for users who previously downloaded them
- However, **connection to the license server is no longer possible**
- Once the license code deactivates, there’s no way to activate



Chat group ID: @mengnancvv

Underground Discussions Regarding the FishingMaster Shutdown

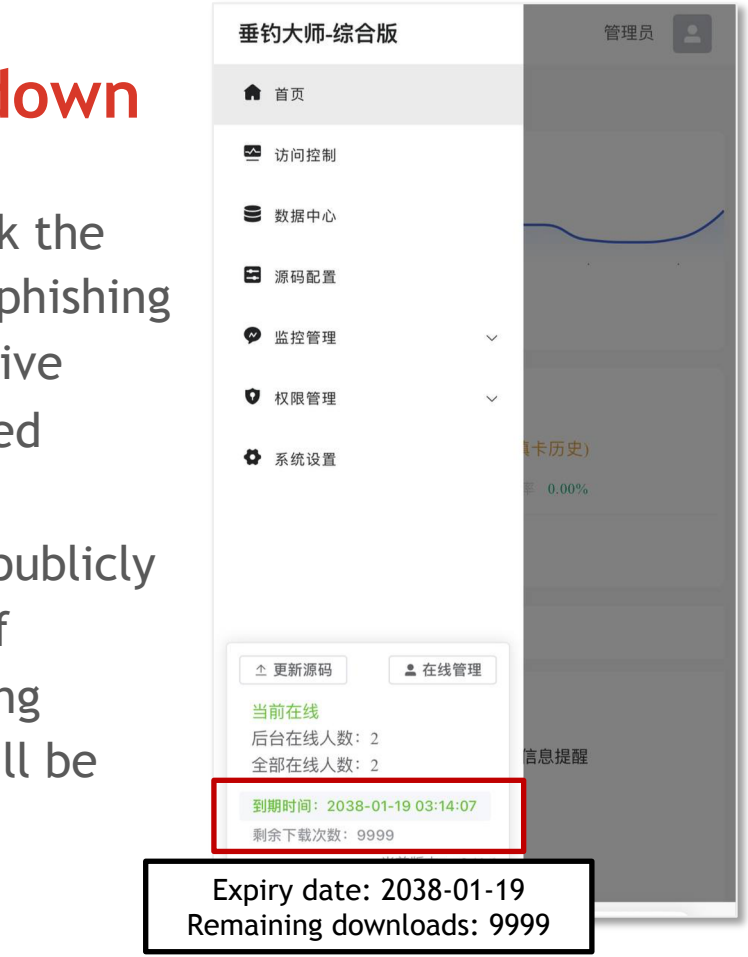
- Kits remain functional for users who previously downloaded them
- However, **connection to the license server is no longer possible**
- Once the license code deactivates, there’s no way to activate



Chat group ID: @mengnancvv

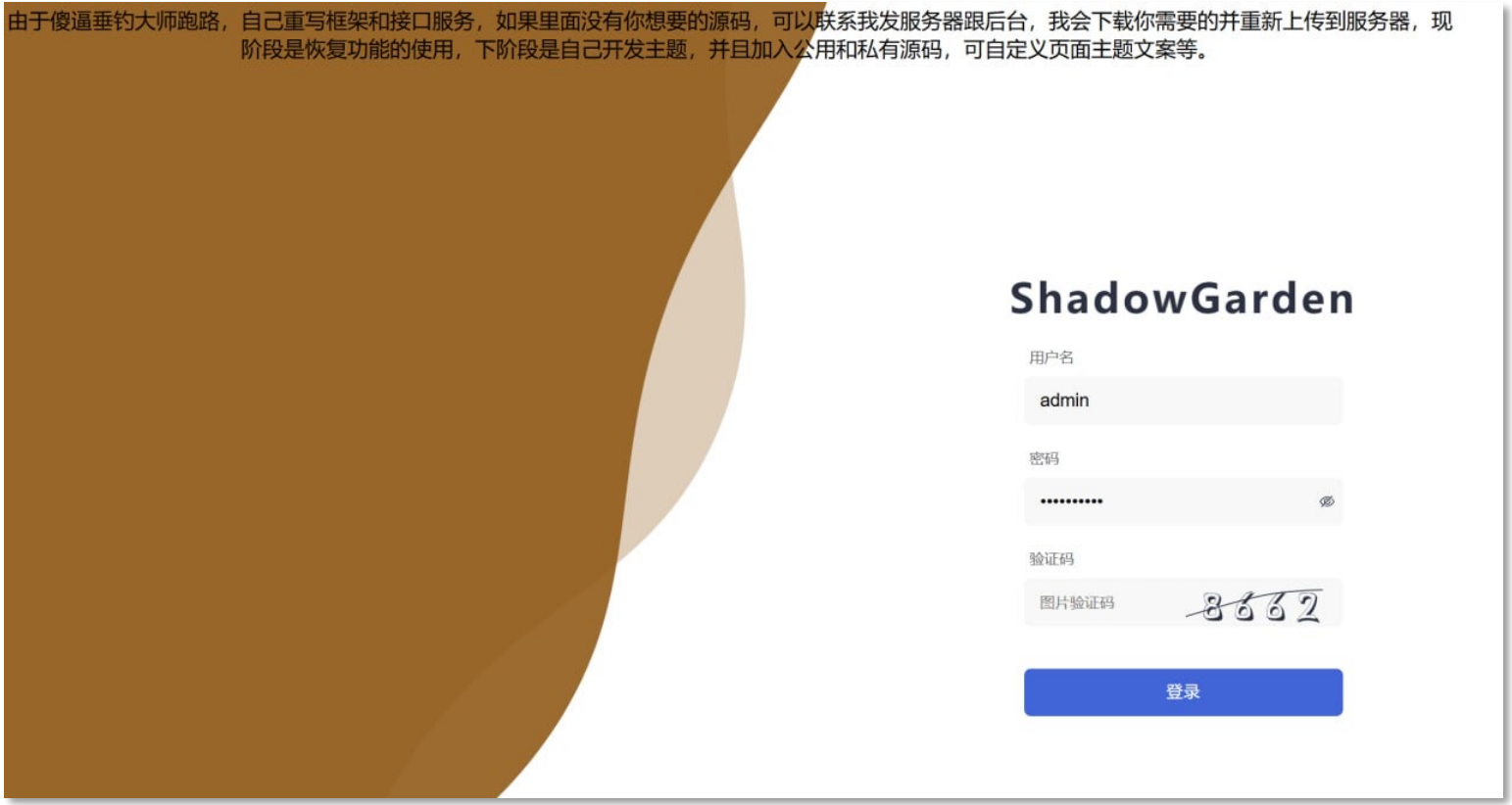
Pirated Version after Service Shutdown

- The disappearance of the actor does not mark the end of FishingMaster PhaaS. Many buyers, or phishing operators, still consider the kits highly effective
- A pirated version of FishingMaster has emerged through community contributions
- The pirated version “Shadow Garden” is not publicly for sale and is only used by a small number of individuals; therefore, newly reported phishing websites with the same initial pattern can still be found



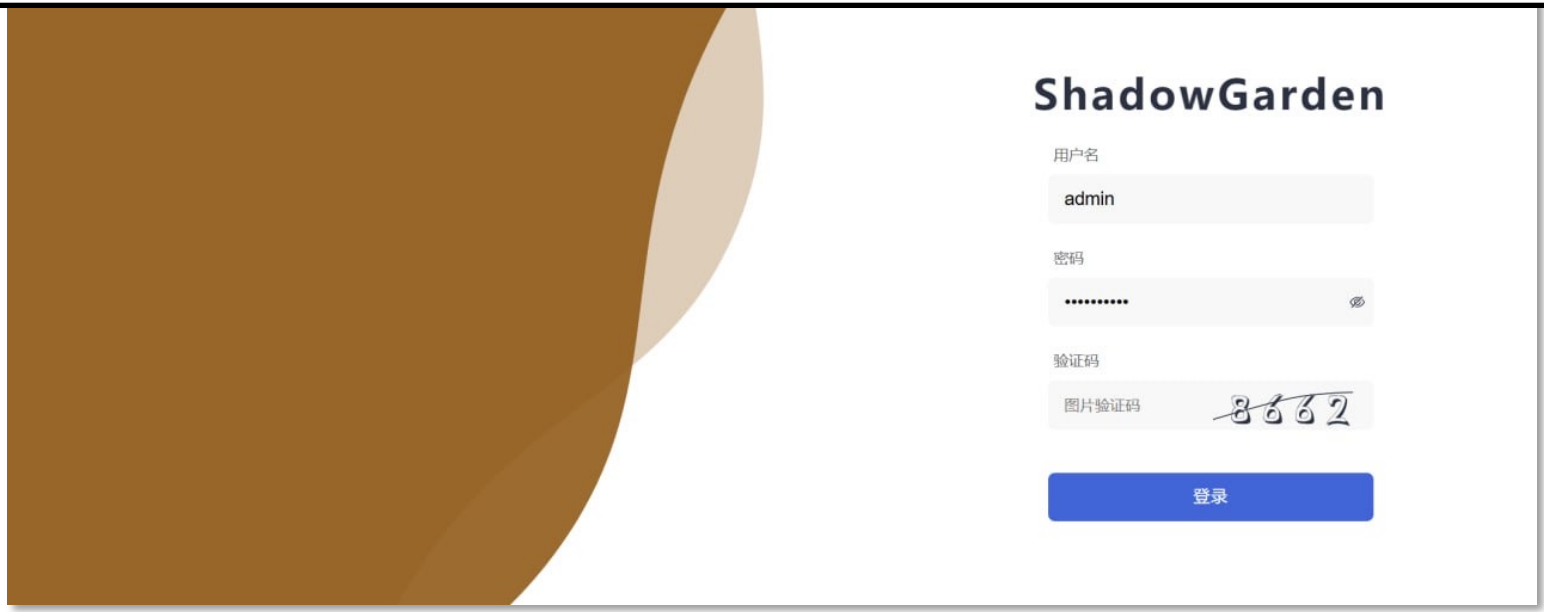
Pirated Version after Service Shutdown

由于傻逼垂钓大师跑路，自己重写框架和接口服务，如果里面没有你想要的源码，可以联系我发服务器跟后台，我会下载你需要的并重新上传到服务器，现阶段是恢复功能的使用，下阶段是自己开发主题，并且加入公用和私有源码，可自定义页面主题文案等。



Pirated Version after Service Shutdown

Since that IDIOT FishingMaster author ran off, I had to rebuild the whole framework and API myself. If there's any phishing kit you can't find in there, just contact me with information of the server and backend panel, and I'll download what you need and re-upload it to your server.
Right now, I'm just restoring basic functions. Next stage, I'll start making my own themes, plus add both public and private phishing kit so you can customize page themes, text, and so on.



Current FishingMaster on OSINT Search

Rebrand to NX PhaaS

Rebrand - Launch of NX PhaaS

June 18, 2025

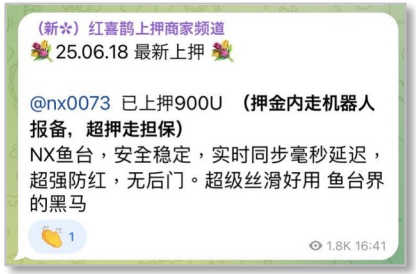
New “NX” PhaaS launched

November 2, 2025

NX notified all subscribers in the channel that the service is closing

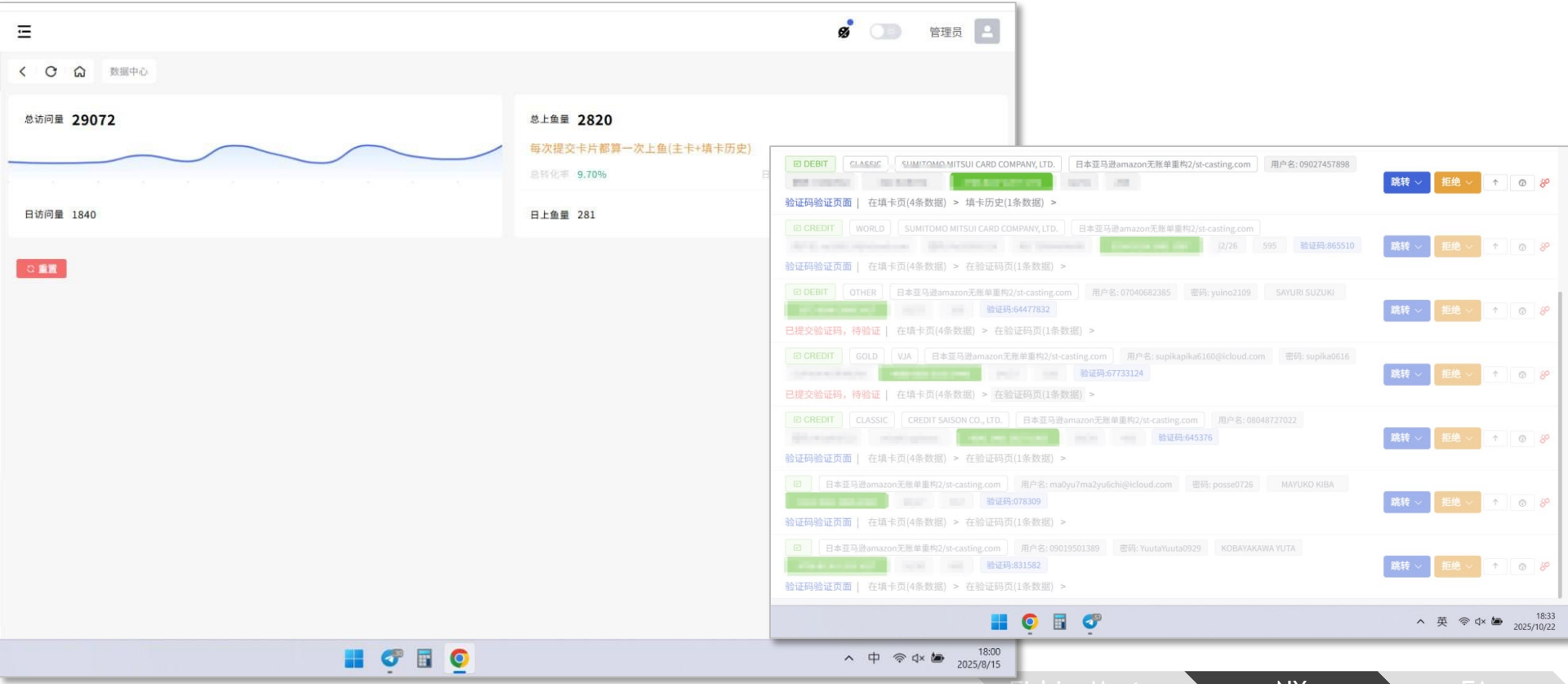
1st Reincarnation - Rebranded as NX PhaaS

- **Channel ID:** @nx001channel
- **User ID:** @nx0073
- **Setup guide:** nxdocs[.]world

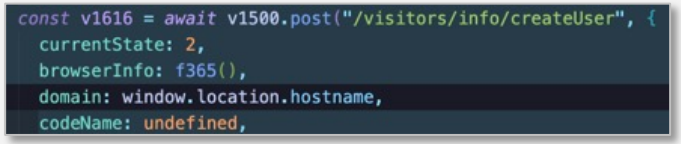
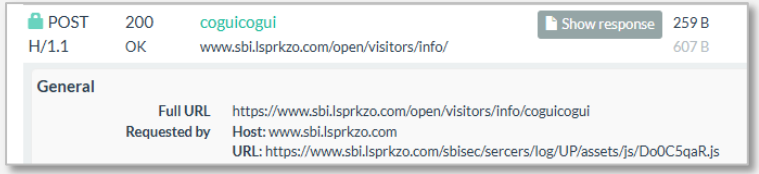
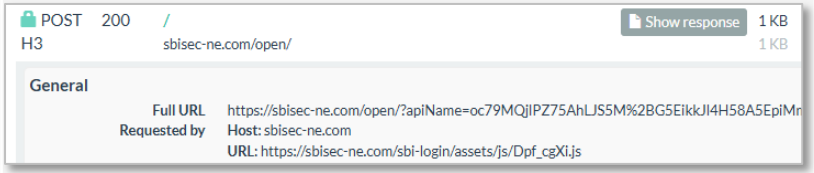


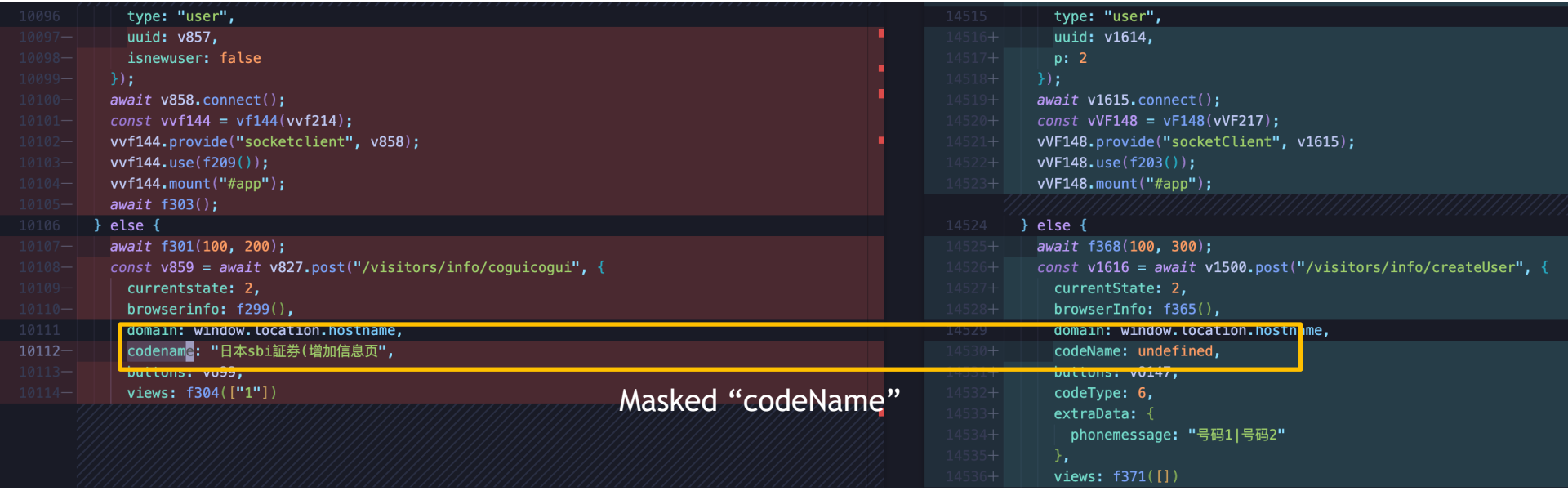
We noticed this PhaaS establishment from the **collateralized listing channel @hxqsj6**

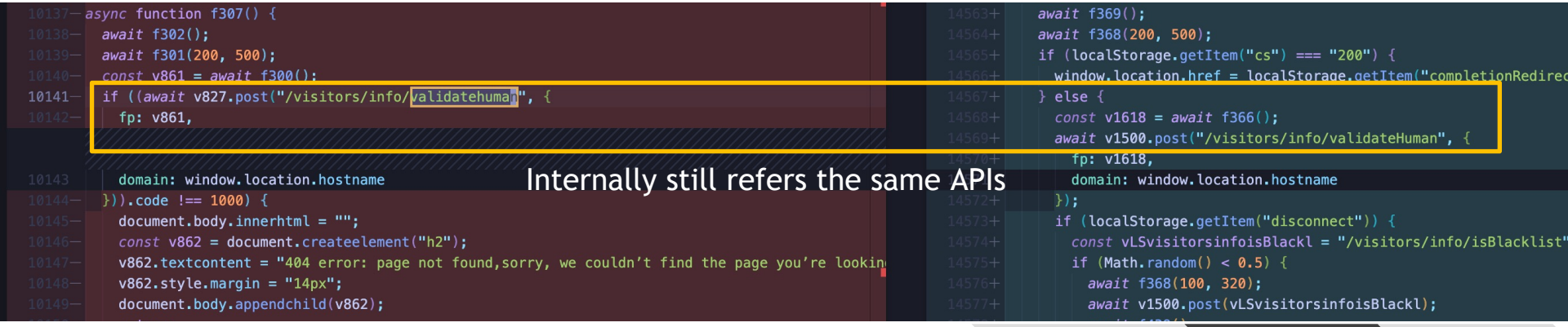
NX PhaaS Admin Panel



Key Changes in NX PhaaS

	FishingMaster	NX
Masked Codename		
Obfuscated Request & Response		
Special Kits	N/A	


type: "user",
uuid: v857,
isnewuser: false
});
await v858.connect();
const vvf144 = vf144(vvf214);
vvf144.provide("socketclient", v858);
vvf144.use(f209());
vvf144.mount("#app");
await f303();
} else {
await f301(100, 200);
const v859 = await v827.post("/visitors/info/coguicogui", {
currentstate: 2,
browserinfo: f299(),
domain: window.location.hostname,
codename: "日本sbi証券(増加信息页",
views: f304(["1"])
type: "user",
uuid: v1614,
p: 2
});
await v1615.connect();
const vVF148 = vF148(vVF217);
vVF148.provide("socketClient", v1615);
vVF148.use(f203());
vVF148.mount("#app");
} else {
await f368(100, 300);
const v1616 = await v1500.post("/visitors/info/createUser", {
currentState: 2,
browserInfo: f365(),
domain: window.location.hostname,
codeName: undefined,
codeType: 6,
extraData: {
phonemessage: "号码1|号码2"
},
views: f371([])
Masked “codeName”


async function f307() {
await f302();
await f301(200, 500);
const v861 = await f300();
if ((await v827.post("/visitors/info/validatehuman", {
fp: v861,
domain: window.location.hostname
})).code !== 1000) {
document.body.innerhtml = "";
const v862 = document.createelement("h2");
v862.textcontent = "404 error: page not found,sorry, we couldn't find the page you're lookin
v862.style.margin = "14px";
document.body.appendchild(v862);
await f369();
await f368(200, 500);
if (localStorage.getItem("cs") === "200") {
window.location.href = localStorage.getItem("completionRedirec
} else {
const v1618 = await f366();
await v1500.post("/visitors/info/validateHuman", {
fp: v1618,
domain: window.location.hostname
});
if (localStorage.getItem("disconnect")) {
const vLSvisitorsinfoisBlackl = "/visitors/info/isBlacklist"
if (Math.random() < 0.5) {
await f368(100, 320);
await v1500.post(vLSvisitorsinfoisBlackl);
Internally still refers the same APIs

Target Confirmation Without Relying on Codename

- The targeted brand is still stored in “officialWebsite” and “document.title”
- In the cases of officialWebsite=“http://localhost”, document.title still reveals the actual target brand

```
$i(async () => {
  document.title = "マネックス証券";
  mx(() => import("./9xlOnhNx.js"), __vite__mi
  mx(() => import("./BKsh7hmb.js"), __vite__mi
  mx(() => import("./BIw27SGl.js"), __vite__mi
  if (!_) {
    throw new Error("Socket.io Error");
  }
  a.verification.suffixNumber = localStorage.
  a.securityAnswer.securityAnswer = localStor
  _.socket.on("adminInstruct", B);
  await v();
});
```

```
function bn() {
  const x = Va({
    officialWebsite: "http://localhost"
  }, false);
  const e = Va({
    title: "配送状況",
    packageNumberTitle: "あなたの荷物番号",
    notice: "配送失敗の通知",
    description1: "配送先住所が不明瞭のため、お荷物は配達されませんでした",
    description2: "お荷物は当社の運用センターに戻りました",
    description3: "住所を更新してください。再配送を行います",
    button: "続ける"
  }, false);
```

Encrypted API Call to /visitors/info/*

- apiName is Base64(16 bytes IV + ciphertext)
- Algorithm: AES-128-CBC
- Fixed Key: 7gH3pL9kVx02zY6b
- For POST requests, body is URL-encoded and wrap in JSON, with key “data”

Novel Types of Phishing

Cloaking in NX PhaaS

- Security Check
- Fingerprint BotD
- Observed New API:
  - `/visitors/info/getSkipParameter`
  - `/visitors/info/getSkipDomain`

Latest Migration to FA PhaaS

Latest Migration to FA PhaaS

November 3, 2025

NX PhaaS server shut down

November 10, 2025

New “FA” PhaaS launched by the same actor, with no dedicated channel and no change in pattern

2nd Reincarnation - Rebranding to FA PhaaS

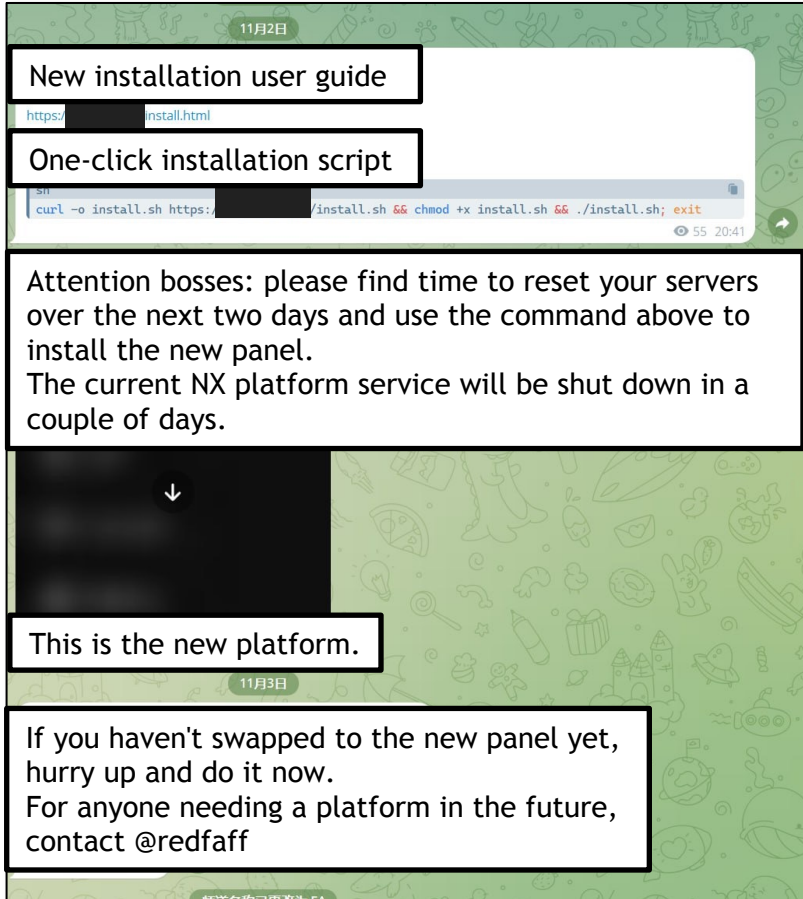
- NX PhaaS channel was renamed to “FA” on Nov. 3rd, 2025. Then the channel was no longer publicly accessible
- The author provides a one-line install command, similar to the previous two stages
- FA PhaaS has now transitioned to a closed-circle model for trusted affiliates only

- **User ID**: @redfaff
- **Setup guide**: <REDACTED>

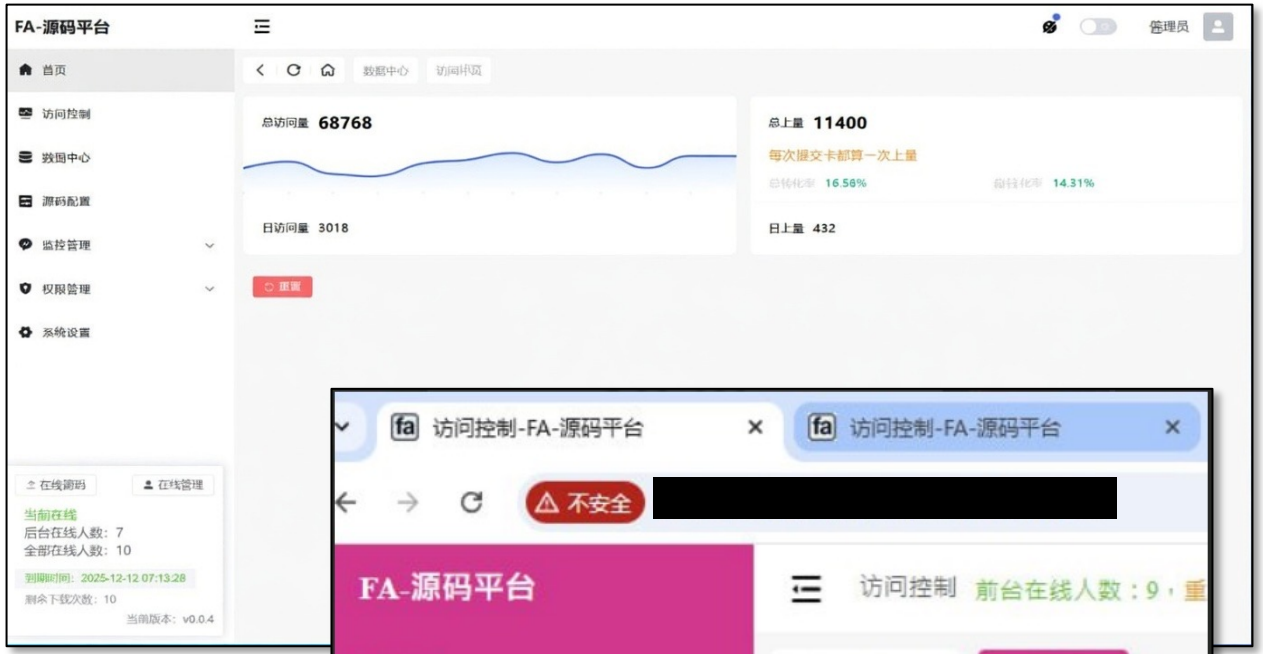
2nd Reincarnation - Rebranding to FA PhaaS

- NX PhaaS channel was renamed to “FA” on Nov. 3rd, 2025. Then the channel was no longer publicly accessible
- The author provides a one-line install command, similar to the previous two stages
- FA PhaaS has now transitioned to a closed-circle model for trusted affiliates only

- **User ID**: @redfaff
- **Setup guide**: <REDACTED>



FA PhaaS Admin Panel



NX to FA: Deleted all kits targeting Japanese securities & other countries

Added

eLTAX (エルタックス)

OMAKASE by GMO

Deleted

Japan-Targeted

JAバンク

PayPay 銀行

SBI 新生銀行

三井住友銀行

MIZUHO

Face to Face 一般社団法人 全国信用金庫協会

横浜銀行

りそな銀行 RESONA

GMOクリック証券

SMBC日興証券

Rakuten 楽天証券

MUFG 三菱UFJモルガン・スタンレー証券

SMBC モビット

アコム

LINE

レイク

Others Countries

coinbase

VANDLECARD

Trip.com

New AES Key for apiName Obfuscation

- New AES Key: q9KxA2mNvT8p7bGh
- This key is hard-coded in JS, all kits were recompiled
- This breaks compactivity between NX and FA

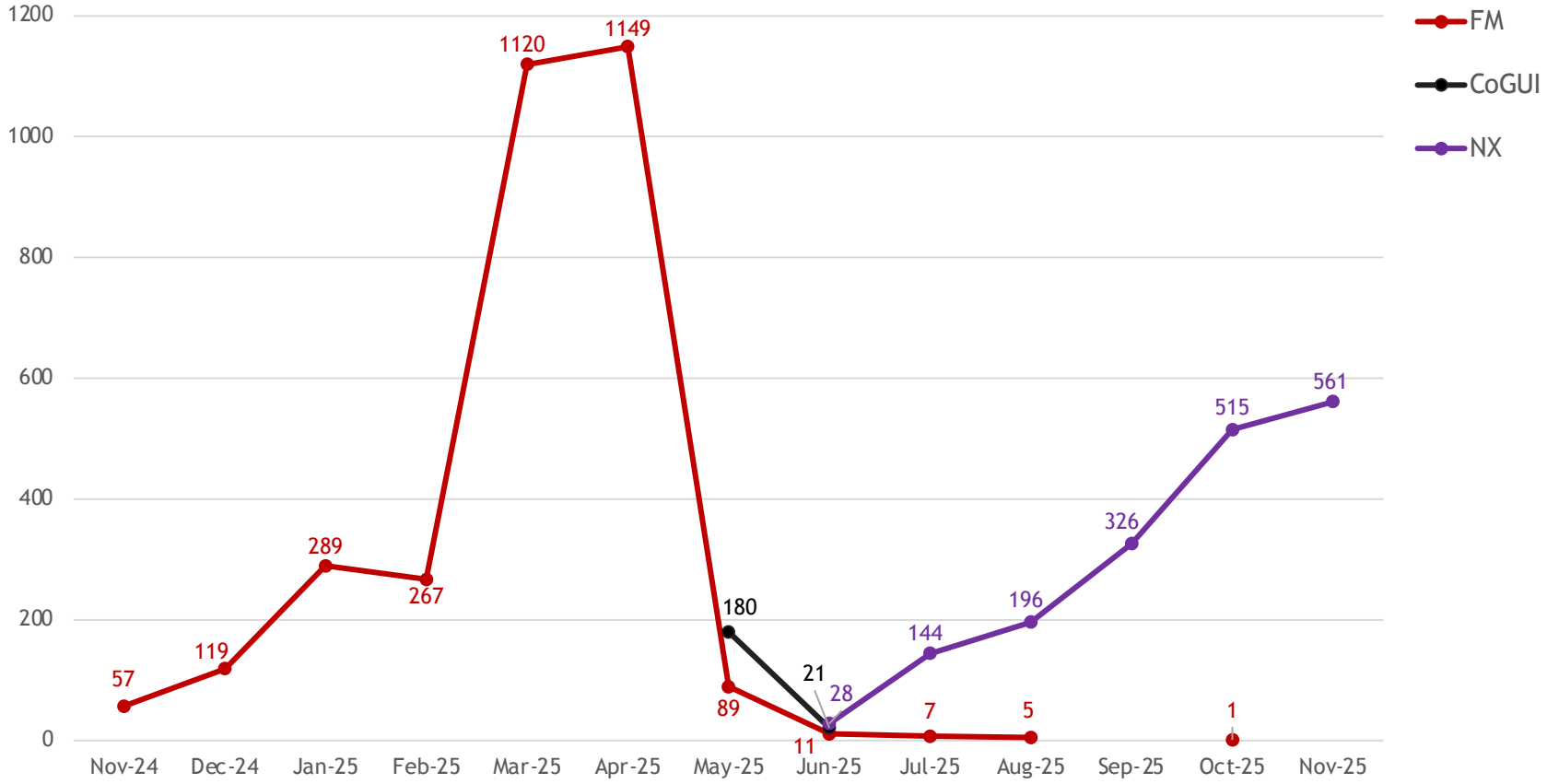
```
var v1493 = v090.exports;
const vF2712 = f271(v1493);
const vA86 = ["7gH3", "pL9k", "Vx02", "zY6b", "8Mcn5D", "3bRtPq"];
const v1494 = vA86.join("");
const v1495 = vF2712.enc.Utf8.parse(v1494.slice(0, 16));
```

NX

```
var v232 = v029.exports;
const vF2282 = f228(v232);
const vA9 = ["q9Kx", "A2mN", "vT8p", "7bGh", "Xz53rL", "c1DwQe"];
const v233 = vA9.join("");
const v234 = vF2282.enc.Utf8.parse(v233.slice(0, 16));
```

FA

Phishing Trends from FishingMaster, CoGUI, and NX



Monitoring Phisher Activities on Telegram

Types of PhaaS Telegram Activities

Main actor or dedicated members aggressively post ads. They often operate multiple specialized channels for community engagement, customer service & tech sharing

All contacts are handled privately by the main actor. This typically indicates a stable, established customer base

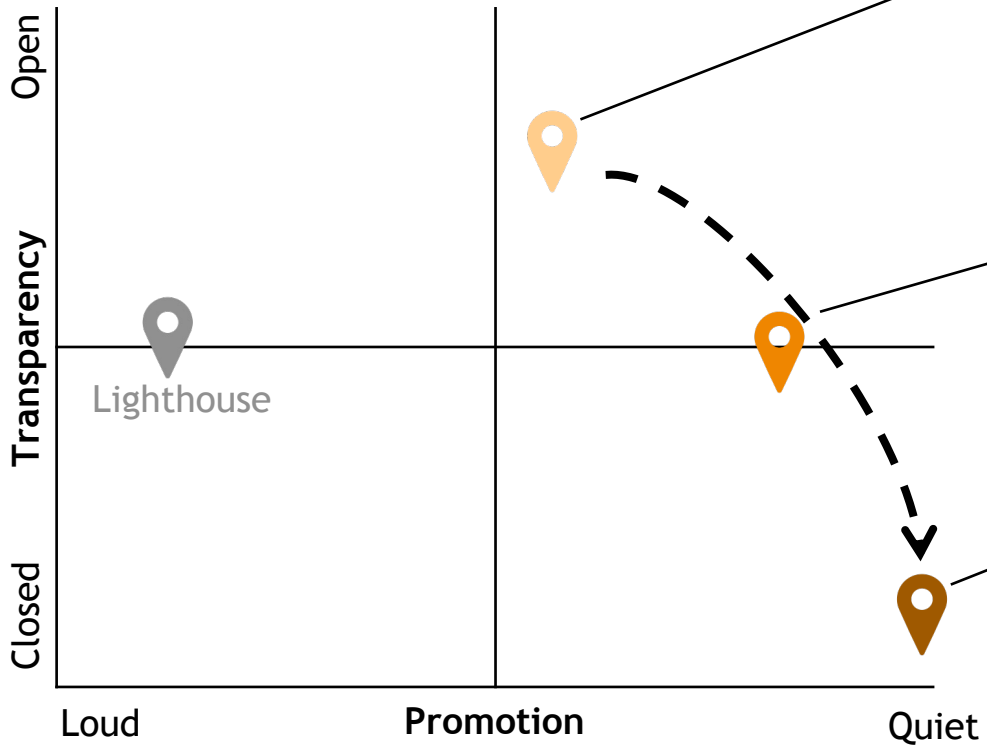
Loud **Promotion** Quiet

Open **Transparency** Closed

Channels directly share installation commands, screenshots, videos, and kit list, to build trust through technical proof

Channels contain little to no information, perhaps with some occasional advertisements

CoGUI TG Channel Changes

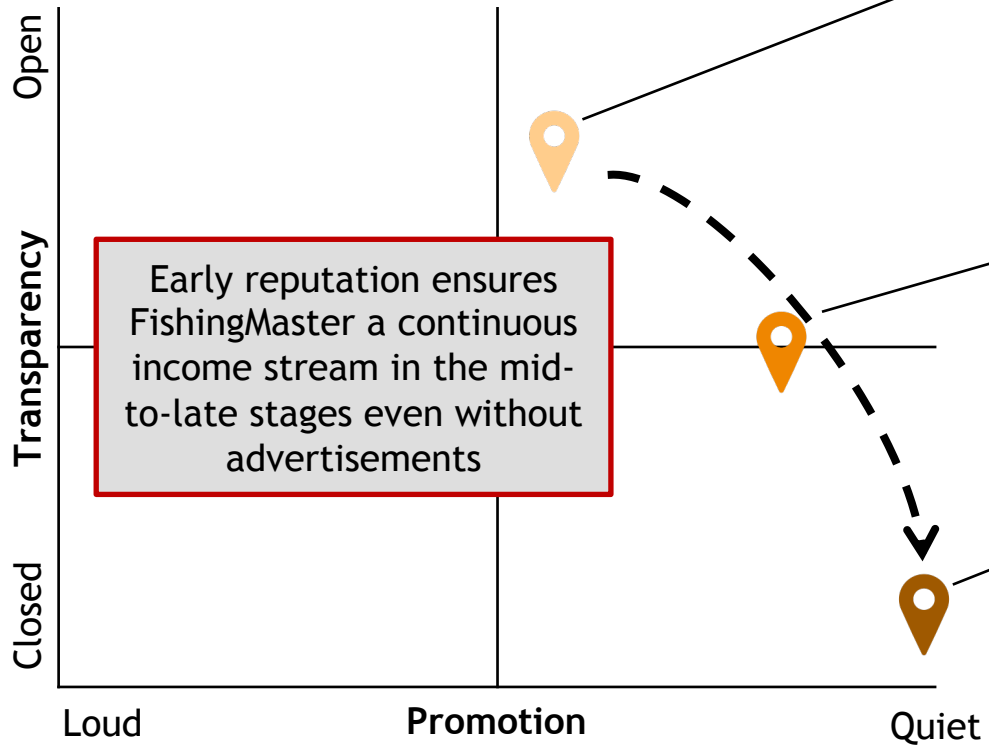


PhaaS Name: FishingMaster
P: Posted several ads in the beginning of months
T: Installation commands, tutorials, and videos were in the channel

PhaaS Name: NX
P: No ads
T: Installation commands, tutorials, and phishing kit list were in the channel

PhaaS Name: FA
P: No ads; even don't want to sell PhaaS to new customer
T: No public exclusive channel anymore

CoGUI TG Channel Changes



Early reputation ensures FishingMaster a continuous income stream in the mid-to-late stages even without advertisements

PhaaS Name: FishingMaster
P: Posted several ads in the beginning of months
T: Installation commands, tutorials, and videos were in the channel

PhaaS Name: NX
P: No ads
T: Installation commands, tutorials, and phishing kit list were in the channel

PhaaS Name: FA
P: No ads; even don't want to sell PhaaS to new customer
T: No public exclusive channel anymore

Threat Actor Profiling

Adversary Profiling: Mother of CoGUI

Infrastructure & Code Evolution

- While core backend architecture remains consistent, the delivery mechanisms have undergone significant hardening, accompanied by increased code obfuscation
- Branding has been removed from admin panels to minimize OSINT signatures and footprint

Tactical Awareness & Adaption

- Closely monitors current affairs and news in Japan to ensure kit templates remain timely and relevant
- Tracks updates to the anti-phishing mechanisms of intended targets to adjust phishing kits accordingly
- Monitors cybersecurity reports to evolve against defensive countermeasures

Reaction: Disruption to Lighthouse PhaaS

- Google filed civil lawsuit in New York against Lighthouse PhaaS on November 13th, 2025

- License server were taken down in the same day, citing court order

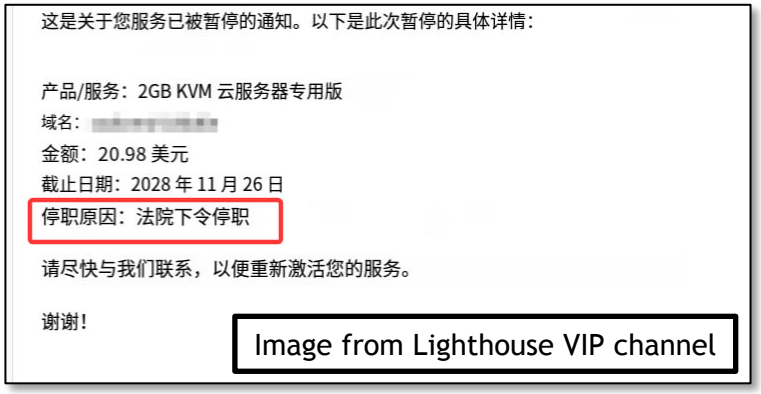
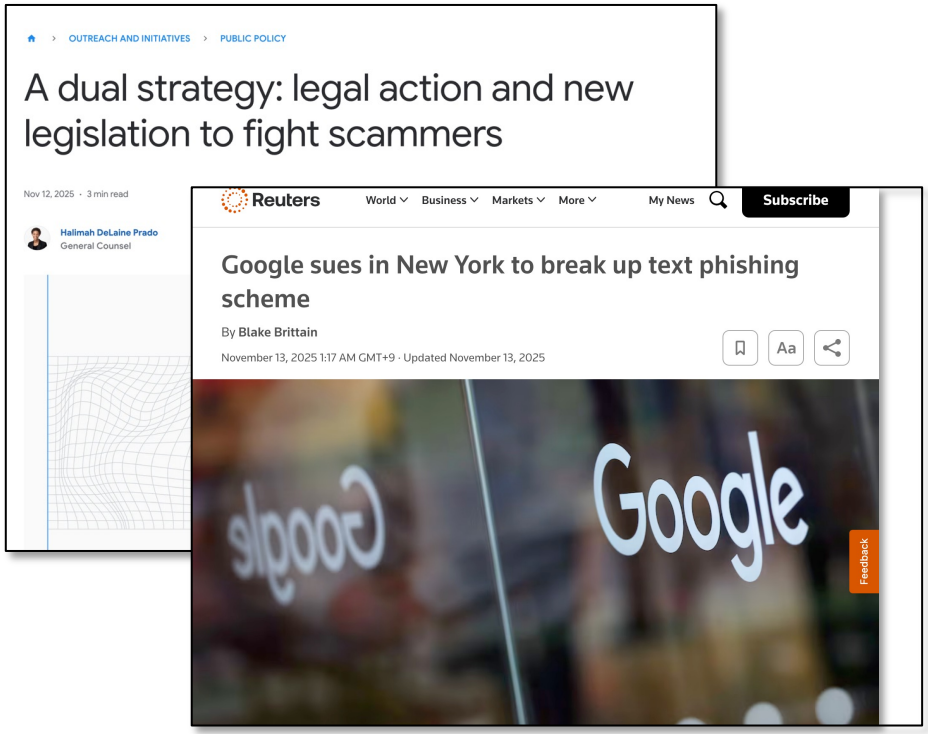
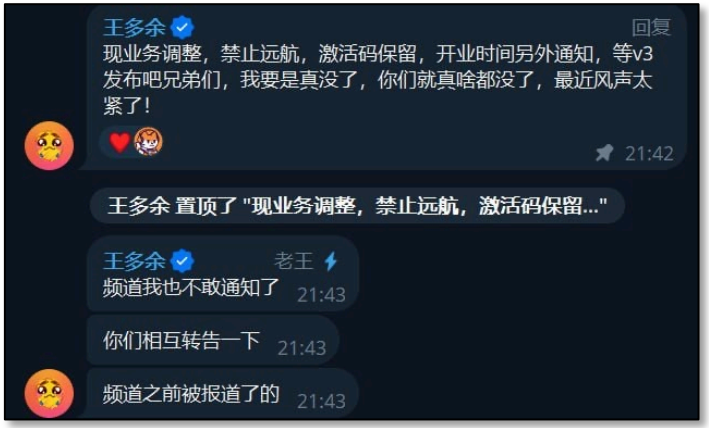


Image from Lighthouse VIP channel



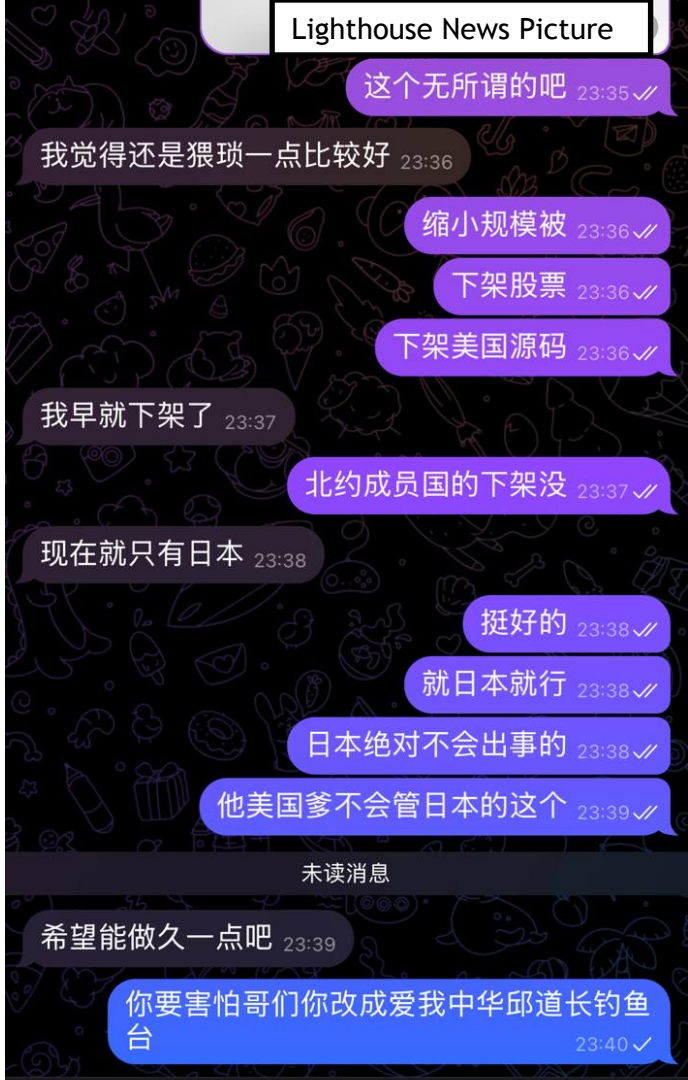
Reaction: Disruption to Lighthouse PhaaS

- Lighthouse seized all operations on November 14th, as “there’s too much attention”
- In December, Lighthouse was rebranded as “T3 PhaaS” with much less popularity



Reaction from CoGUI Author

- At the same day as Lighthouse shut down, prominent CoGUI subscriber @qiudaozhang2020 shared this screenshot in his group, with his comment “Why afraid?”
- This is the chat with CoGUI author
- This indicates the author's low risk tolerance



Reaction from CoGUI Author

- At the same day as Lighthouse shut down, prominent CoGUI subscriber @qiudaozhang2020 shared this screenshot in his group, with his comment “Why afraid?”
- This is the chat with CoGUI author
- This indicates the author's low risk tolerance

Disruption through legal actions is limited but powerful

- Many actors have low risk tolerance and prefer to avoid unwanted attention
  - They engage in activities they believe are tolerated by Chinese law enforcement
  - They are genuinely afraid of Chinese authorities, or any party that could cause them trouble
- Most actors lack the legal knowledge to understand the severity of the consequences they face
- Because the Chinese carding scene is highly decentralized and specialized, it takes significant time to regain momentum after each relaunch

Key Takeaways

Hunting Patterns

- URLscan
  - Current: `filename:"/open/?apiName=”`
  - Legacy/Pirated: `filename:"/open/visitors/info/”`

- Censys (find VPS running CoGUI)
  - host.operating_system.vendor: "canonical" AND
    host.services: (
    port: 80 AND
    endpoints.http.body_hash_sha1: "6f9a83bffd6a26735107b580ab375e6b708b961f”
) AND NOT host.services.protocol: {"SMTP", "PORTMAP", "UNKNOWN", "MINECRAFT"}

Key Takeaways

- **Dominant Regional Specialization**: CoGUI has established itself as a premier Japan-centric PhaaS, leveraging high-fidelity, localized templates that are specifically engineered for the Japanese digital landscape
- **Strategic Risk Mitigation**: To minimize exposure to law enforcement and high-profile attribution, the actor has proactively removed high-risk targets (e.g., securities firms and non-Japan entities) from the platform
- **Commoditization of Cybercrime**: By utilizing Docker-based, one-click deployment, CoGUI significantly lowers the barrier to entry, enabling low-skill affiliates to launch sophisticated campaigns at scale

Key Takeaways

- **Adversarial Agility**: The operator demonstrates deep situational awareness of Japan’s defensive landscape. Rapid updates to cloaking mechanisms and templates indicate a "continuous integration" approach to bypassing regional anti-fraud measures
- **Value of Underground Intelligence**: Persistent monitoring of underground communities is critical for mapping the full PhaaS lifecycle, including infrastructure iterations, versioning history, and affiliate demographics
- **Efficacy of Operational Disruption**: Beyond technical controls like Passkeys, legal action and public exposure are highly effective due to the low risk tolerance of PhaaS developers

Thank you!

Appendix: Targeted Brands and Services in Japan

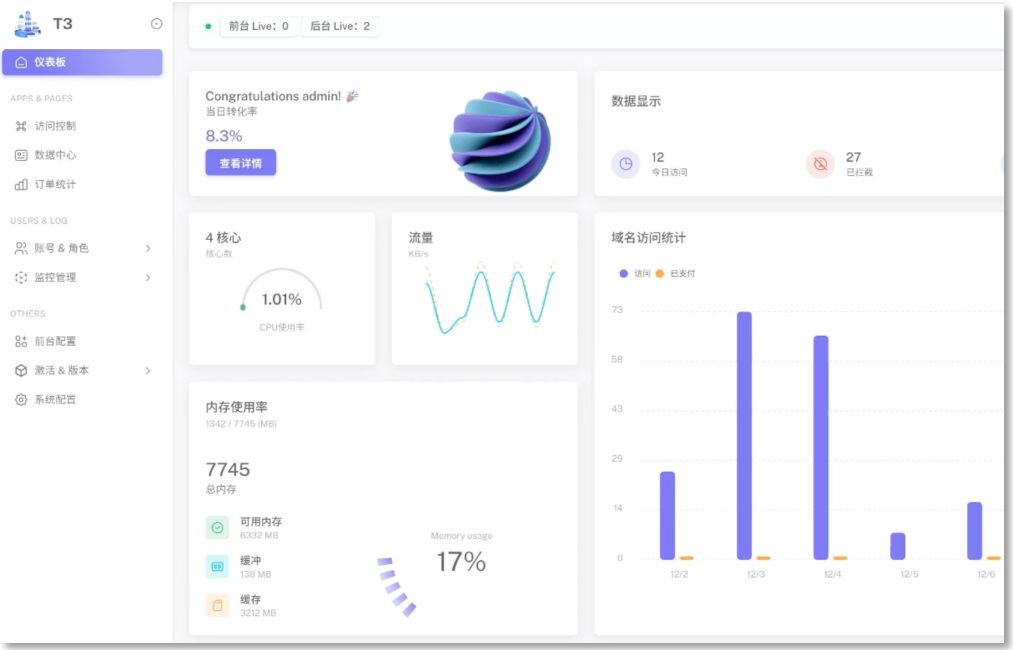
- American Express
- JCB
- Mastercard Japan
- VISA Japan
- Epos Card (エポスカード)
- JACCS (ジャックス)
- Life Card (ライフカード)
- Mitsubishi UFJ NICOS (三菱UFJニコス)
- Nanto VISA Card (南都VISAカード)
- Nissenren Millennia Card (ニッセンレンミレニアムカード)
- Orico Card (オリコカード)
- Pocket Card (ポケットカード)
- Rakuten Card (楽天カード)
- Saison Card (セゾンカード)
- Suica JAL Card (Suica JALカード)
- Tokyu Card (東急カード)
- TS Card (TSカード)
- UC Card (UCカード)
- UCS Card (UCSカード)
- Vandle (バンドルカード)
- au Bank (auじぶん銀行)
- Hokuyo Bank (北洋銀行)
- JA Bank (JAバンク)
- Mizuho Bank (みずほ銀行)
- Nishi-Nippon City Bank(西日本シティバング)
- Resona Bank (りそな銀行)
- SBI Shinsei Bank (SBI新生銀行)
- Shinkin (全国信用金庫協会)
- Sumishin SBI Net Bank (住信SBIネット銀行)
- Yokohama Bank (横浜銀行)
- Acom (アコム)
- Aiful (アイフル)
- Lake (レイク)
- SMBC Mobit (SMBCモビット)
- Daiwa Securities (大和証券)
- GMO Securities (GMO証券)
- Monex Securities (マネックス証券)
- Nomura Securities (野村證券)
- Rakuten Securities (楽天証券)
- SBI Securities (SBI証券)
- SMBC Securities (SMBC日興証券)
- Atone (アトネ)
- au Pay (auペイ)
- FamiPay (ファミペイ)
- Paidy (ペイディ)
- PayPay (ペイペイ)
- AEON (イオン)
- Amazon Japan (アマゾン)
- FamilyMart (ファミリーマート)
- Mercari (メルカリ)
- Rakuten Ichiba (楽天市場)
- Yodobashi Camera (ヨドバシカメラ)
- DMM.com (DMM.com)
- Nintendo (任天堂)
- Sony PlayStation
- ANA (全日本空輸)
- Ekinet (えきねっと)
- ETC
- Japan Airlines (JAL)
- SmartEX
- Trip.com
- DHL (DHL日本)
- Japan Post (日本郵便)
- Sagawa Express (佐川急便)
- Yamato Transport (ヤマト運輸)
- eLTAX (地方税)
- MIC (総務省)
- National Tax Agency (国税庁)
- NHK (日本放送協会)
- Statistics Bureau (統計局)
- TEPCO (東京電力)
- Tokyo Gas (東京ガス)
- au
- Docomo (ドコモ)
- eo Webmail (eoWEBメール)
- Apple Japan (Apple日本)
- LINE
- OMAKASE
- Takarakuji (宝くじ)

Appendix: Targeted Brands and Services (Others)

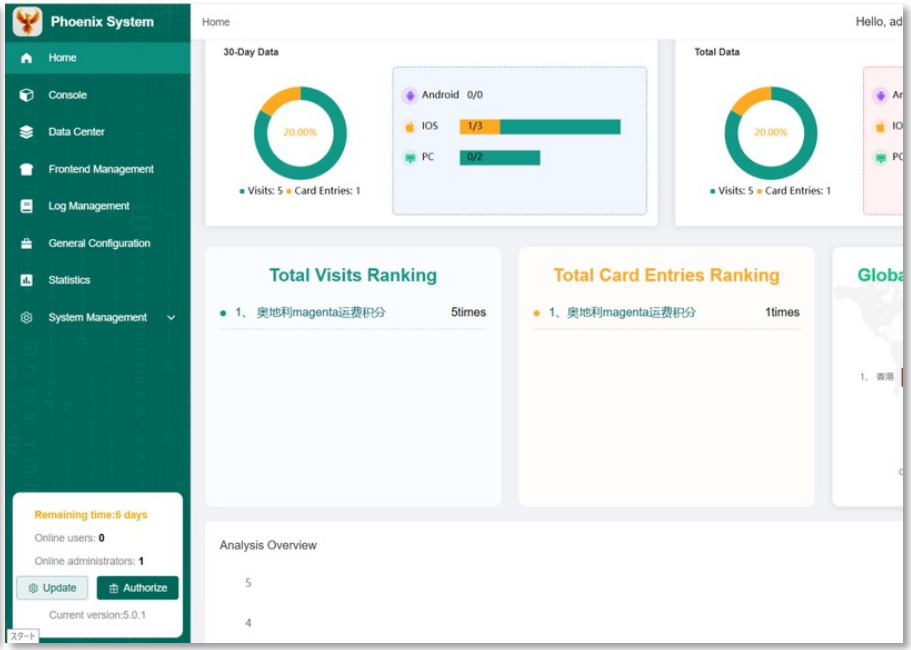
- LG U+ (South Korea)
- Korea Telecom (KT) (South Korea)
- Globe Rewards (Philippines)
- Smart Rewards (Philippines)
- GCash (Philippines)
- SM Markets (Philippines)
- GoTyme Bank (Philippines)
- Bank Central Asia (BCA) Rewards (Indonesia)
- Visa Indonesia (Indonesia)
- Bank Negara Indonesia (BNI) Rewards (Indonesia)
- Indomaret (Indonesia)
- BAC (Indonesia)
- Singapore Post
- Pos Malaysia
- Aramex (UAE)
- kgmETC (Turkey)
- JCCsmart (Cyprus)
- Hargreaves Lansdown (United Kingdom)
- DHL (Germany)
- ETC (Spain)
- DHL (Spain)
- ETCdgt (Spain)
- Fineco (Italy)
- La Poste (France)
- Bulgarian Post
- Apple (US)
- Amazon (US)
- Citi Bank (US)
- Bank of America (US)
- UPS (US)
- USPS (US)
- E-ZPass (US)
- EZdriveMA (US)
- GoodToGo (US)
- SunPass (US)
- FLHSMV (US)
- TxTag (US)
- FasTrak (Canada)
- Canada Post
- Rogers (Canada)
- A30 Express (Canada)
- 4-72 (Columbia)
- Telstra (Australia)
- ETC (Australia)
- CMC (Australia)
- Australia Post
- New Zealand Post
- ETC(New Zealand)
- One.nz (New Zealand)
- CoinBase

Appendix: Major Chinese Phishing-as-a-Service

Lighthouse PhaaS (T3)



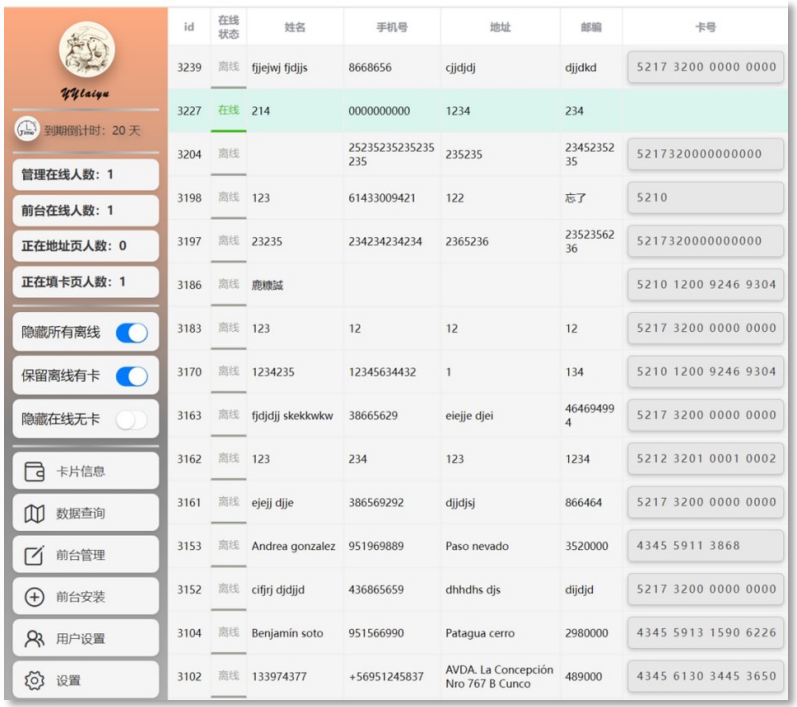
Haozi PhaaS (Pheonix)



Appendix: Major Chinese Phishing-as-a-Service

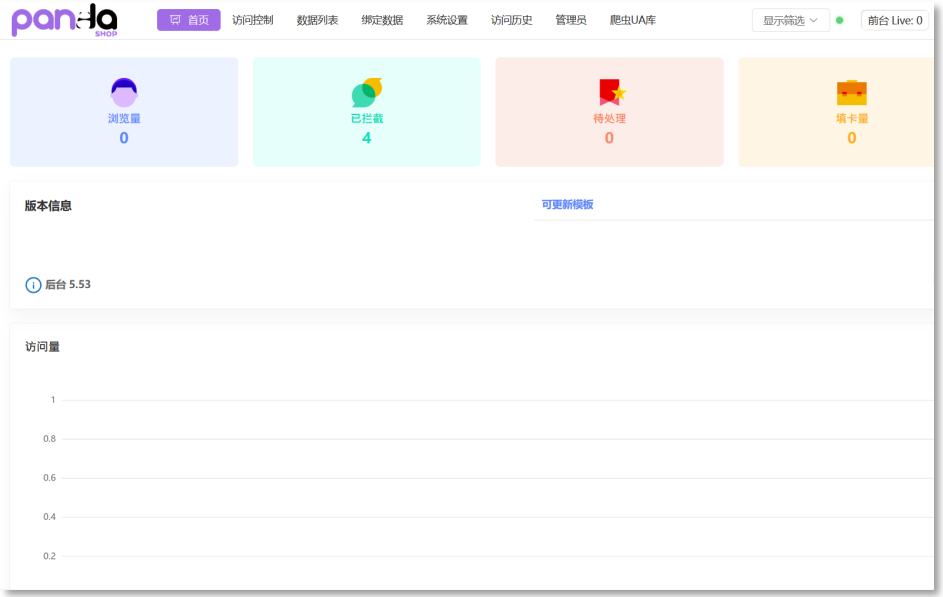
Lucid PhaaS

YYLU PhaaS



Appendix: Major Chinese Phishing-as-a-Service

Panda Shop PhaaS



Outsider PhaaS