

A dark, atmospheric hallway with red curtains and a bright light at the end.

# 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 AI.

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.**



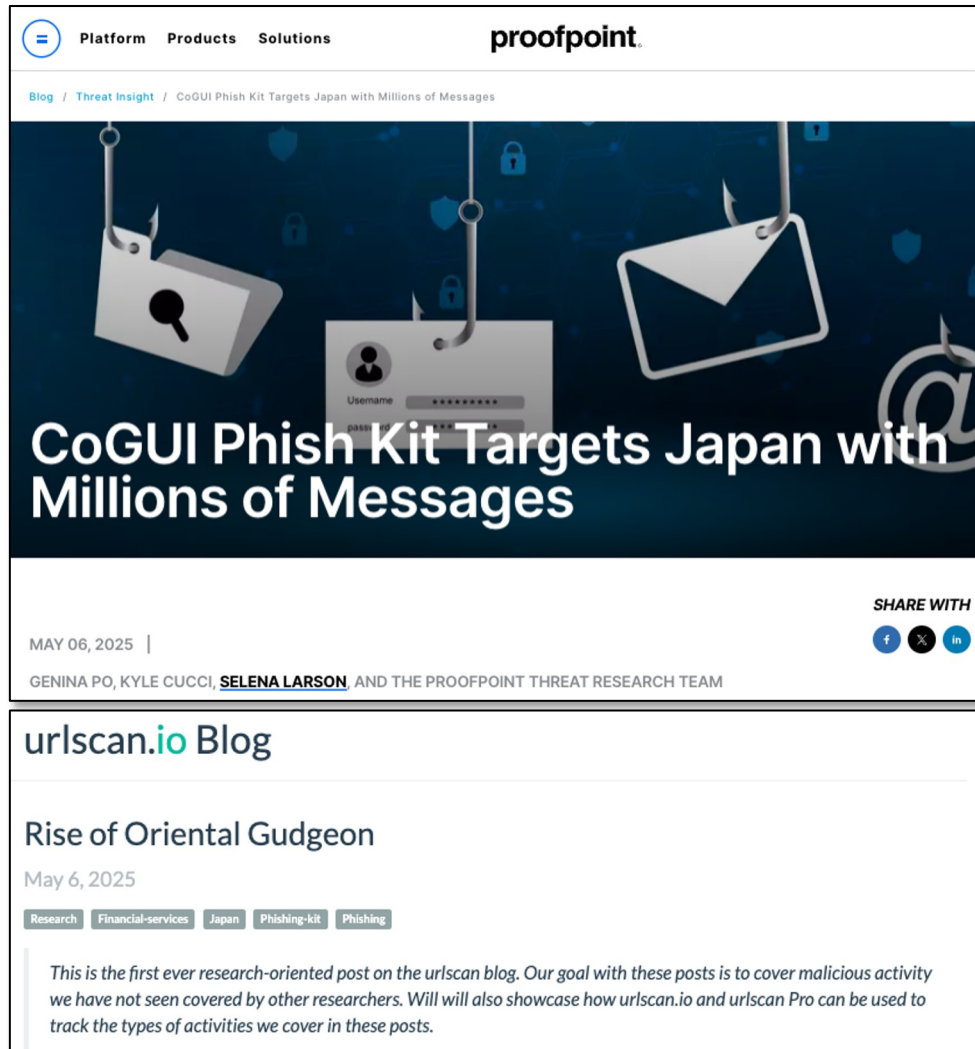


# CoGUI Phishing Attacks Targeting Japan

# 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](#)



The screenshot shows a web browser displaying a blog post from Proofpoint. The top navigation bar includes a menu icon, 'Platform', 'Products', 'Solutions', and the 'proofpoint.' logo. Below the navigation bar, a breadcrumb trail reads 'Blog / Threat insight / CoGUI Phish Kit Targets Japan with Millions of Messages'. The main content area features a dark blue header image with illustrations of a magnifying glass, a login form with fields for 'Username' and 'password', and an envelope. The title 'CoGUI Phish Kit Targets Japan with Millions of Messages' is prominently displayed in white text. To the right of the title, there is a 'SHARE WITH' section with icons for Facebook, Twitter, and LinkedIn. Below the title, the date 'MAY 06, 2025' is shown, followed by the author information: 'GENINA PO, KYLE CUCCI, [SELENA LARSON](#), AND THE PROOFPOINT THREAT RESEARCH TEAM'. The bottom section of the screenshot shows the 'urlscan.io Blog' header, the title 'Rise of Oriental Gudgeon', the date 'May 6, 2025', and a row of tags: 'Research', 'Financial-services', 'Japan', 'Phishing-kit', and 'Phishing'. A paragraph of text follows, starting with 'This is the first ever research-oriented post on the urlscan blog. Our goal with these posts is to cover malicious activity we have not seen covered by other researchers. Will will also showcase how urlscan.io and urlscan Pro can be used to track the types of activities we cover in these posts.'

Platform Products Solutions proofpoint.

Blog / Threat insight / CoGUI Phish Kit Targets Japan with Millions of Messages

CoGUI Phish Kit Targets Japan with Millions of Messages

SHARE WITH

MAY 06, 2025 |

GENINA PO, KYLE CUCCI, [SELENA LARSON](#), AND THE PROOFPOINT THREAT RESEARCH TEAM

urlscan.io Blog

Rise of Oriental Gudgeon

May 6, 2025

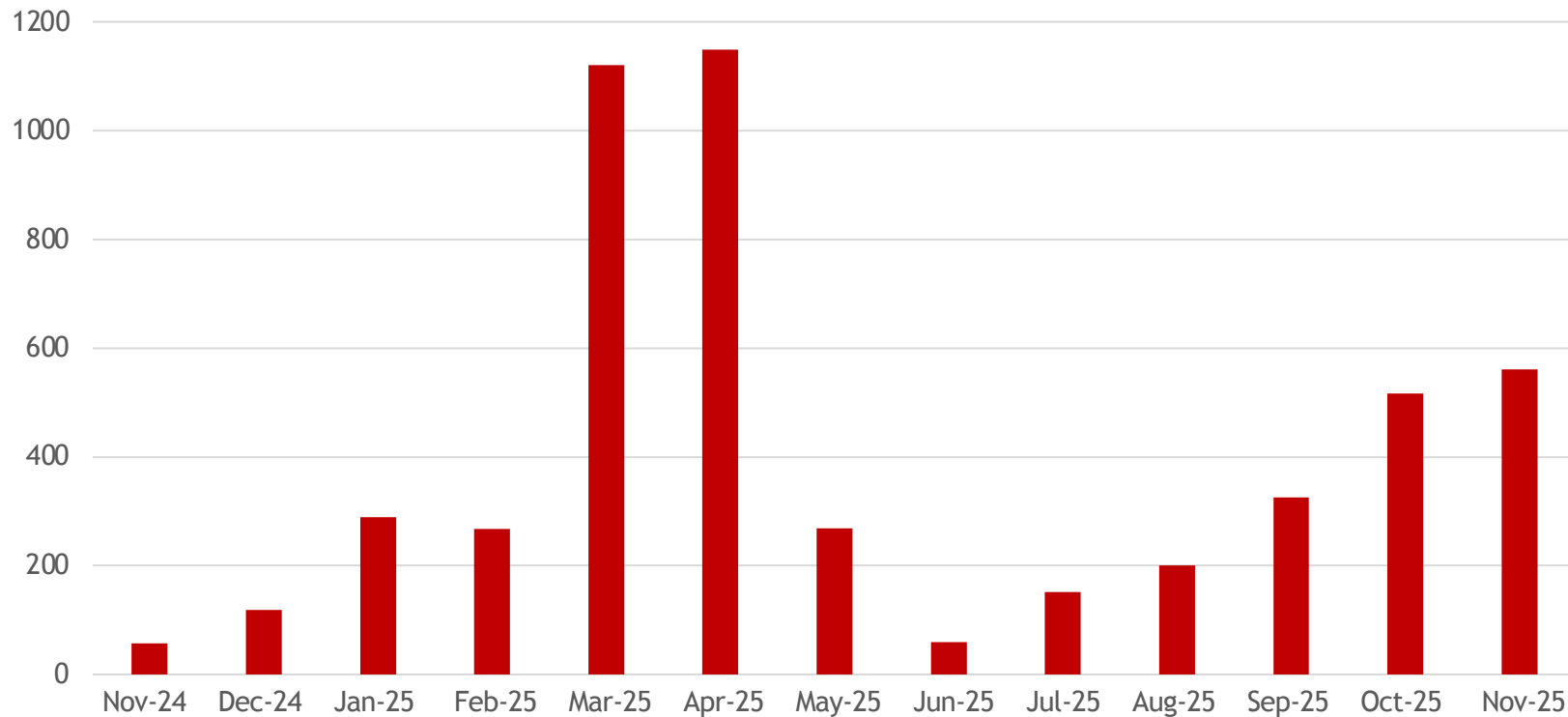
Research Financial-services Japan Phishing-kit Phishing

This is the first ever research-oriented post on the urlscan blog. Our goal with these posts is to cover malicious activity we have not seen covered by other researchers. Will will also showcase how urlscan.io and urlscan Pro can be used to track the types of activities we cover in these posts.

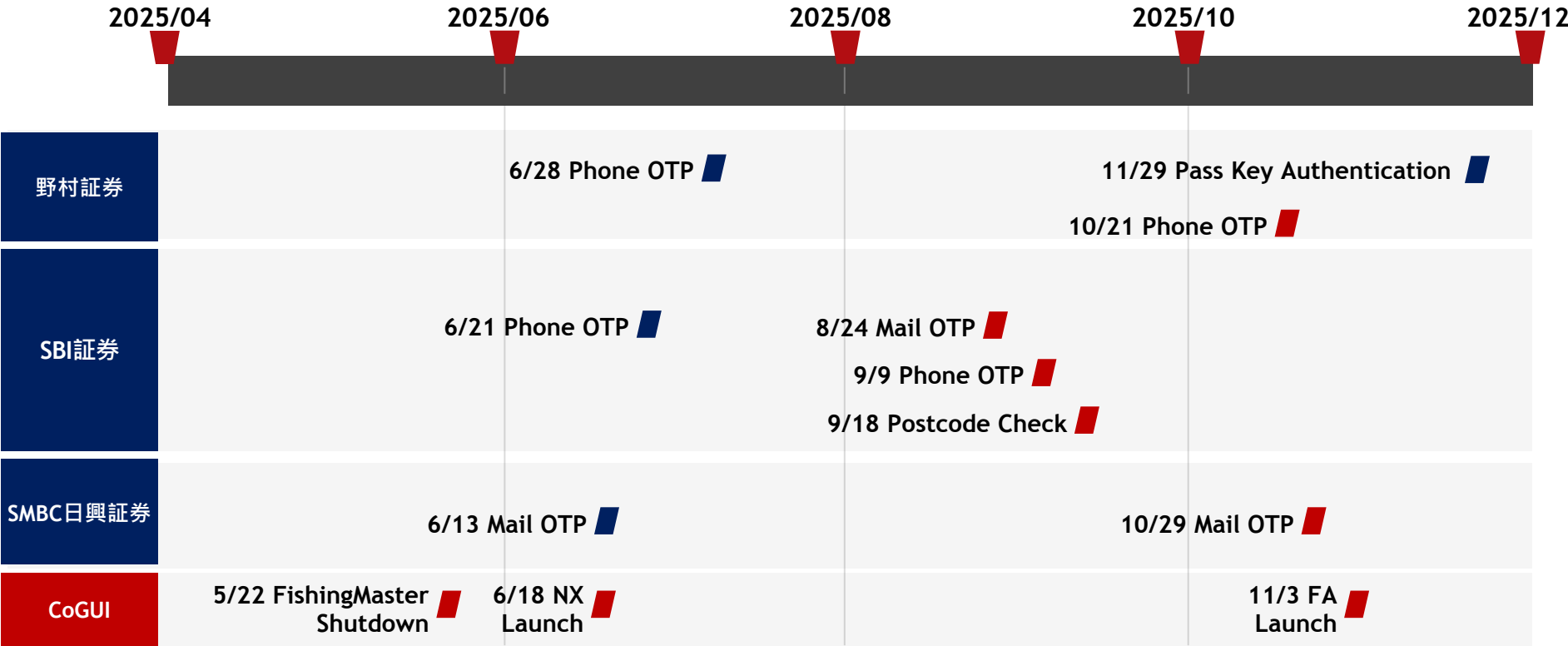
70+  
JP Brands



# 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



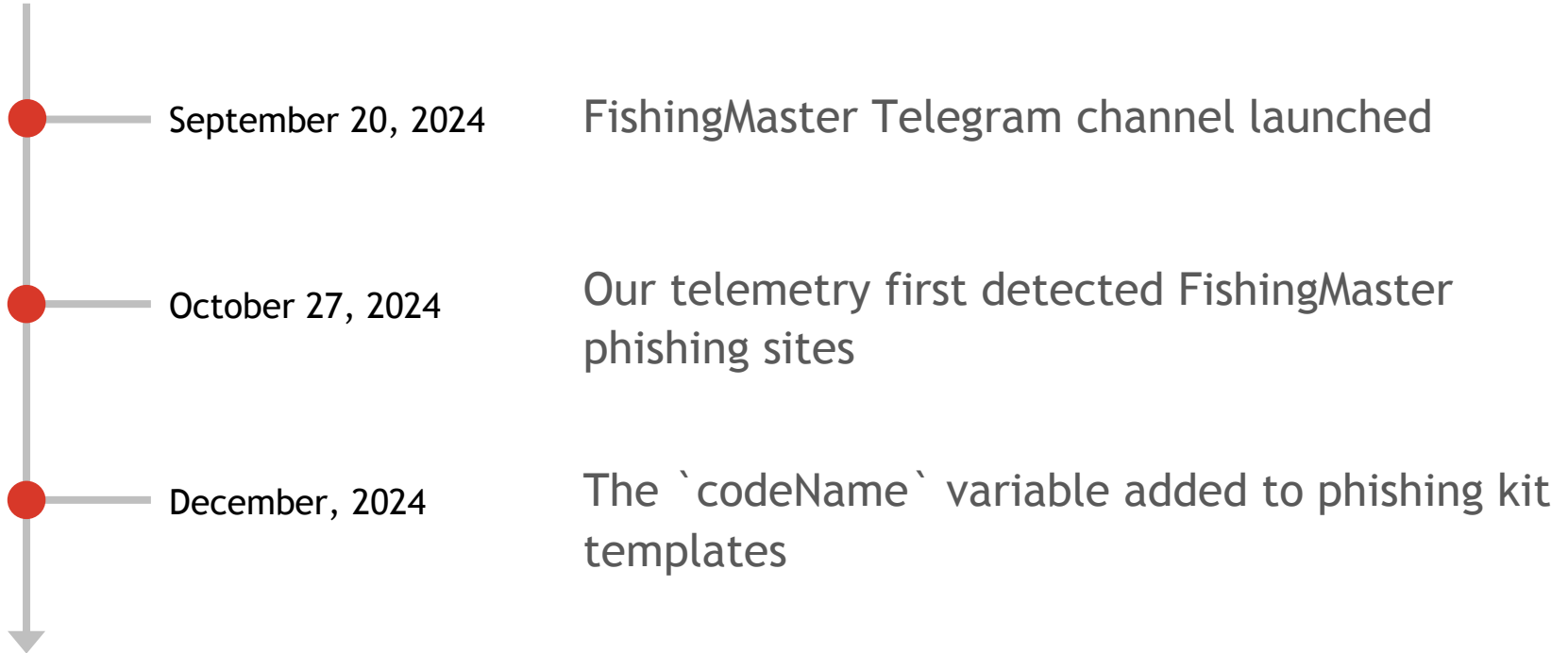
**FA**

Period: 2025-11 ~  
TG User: @redfaff



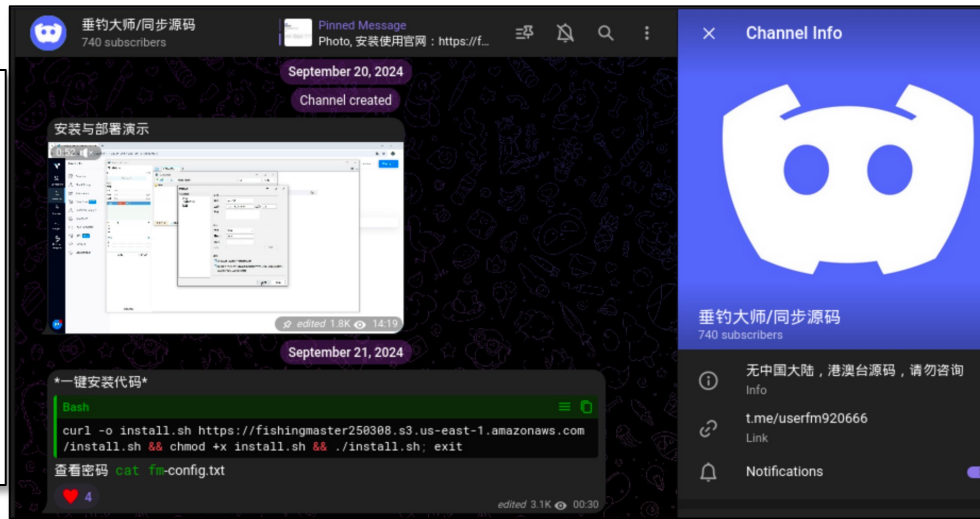
# Launch of FishingMaster PhaaS

# Launch of FishingMaster PhaaS



# 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

 垂钓大师

Menu

Return to top

## 安装与部署

不想安装的 也可以联系我，提供服务器给我 我帮忙安装

别看内容很多 安装其实很简单，第一步查看防火墙是否开启，第二步执行安装脚本。大多数内容都是用来处理安装出错后的操作

**DANGER**  
打开防火墙 打开防火墙 打开防火墙 不开会有人偷鱼

**TIP**

- 有些服务器默认防火墙是关闭状态
- 可以使用下面命令查看防火墙是否开启，开启防火墙可以防止一些恶意攻击和入侵数据库偷鱼
- 如果安装失败，下面有常见的失败解决办法 安装和处理失败问题全程都是在root权限下，如果你使用的是Ubuntu账户登录，当安装失败或者服务器断开后 都要使用sudo su重新开启root权限

使用下面命令查看防火墙是否开启，如果输出端口号说明 防火墙是开启状态

```
sudo ufw status verbose
```

bash

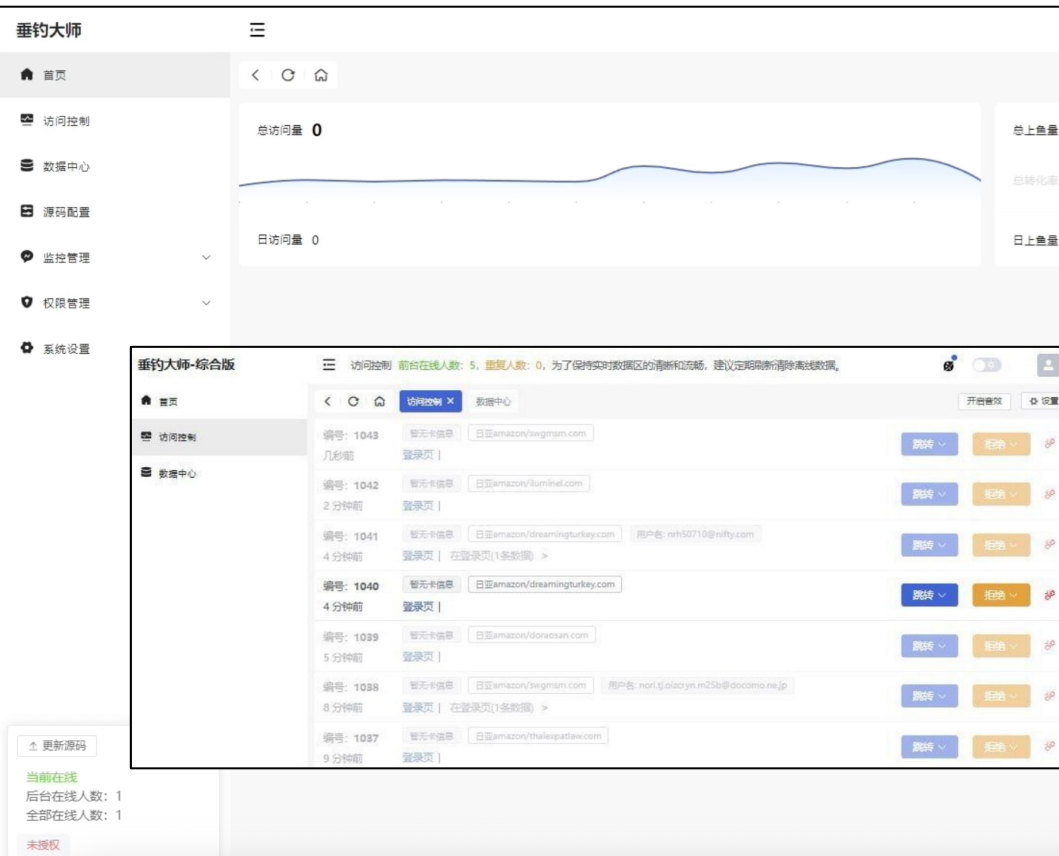
如果防火墙是关闭状态 需要开启防火墙的话，使用下面命令先开放22端口，防止防火墙开启后服务器无法连接

```
sudo ufw allow 22/tcp
```

bash

然后使用下面命令开启防火墙(出现提示输入 y 然后回车)

# FishingMaster PhaaS Admin Panel



# Early Activities of FishingMaster

垂钓大师【全球同步源码】 • Author ID: 2261057438

Posted on September 22, 2024 at 03:24:04 UTC

全球同步鱼台出租/定制/合作

实时动态，一键部署，多重防红，多种语音播报，高亮卡头，自动拒绝卡头，卡头备注，证书申请，无人值守，监控管理，权限管理，在线更新...

一个后台全球源码皆可使用

userfm920 • Author ID: 6290631954

Posted on November 28, 2024 at 05:42:49 UTC

在20世纪的漩涡中，中国经历了诸多磨难，其中深刻的一课来自于抗日战争时期的苦难。那时，中国还是一个武器技术落后、经济基础薄弱的国家，在

时光流转，今天的中国已然不同，科技进步，武器现代化，国力显著增强。然而，与过去的硝烟不同，吾辈生于这个和平年代，并不能直接拿起枪杆子

🔥“垂钓大师同步源码(40多套日本源码)”🔥

来发起新形式的“战争”让那些曾经犯下罪行的日寇后代明白：复仇之火已点燃，谁也无法逃避。

userfm920 • Author ID: 6290631954

Posted on December 02, 2024 at 12:08:10 UTC

在20世纪的漩涡中，中国经历了诸多磨难，其中深刻的一课来自于抗日战争时期的苦难。那时，中国还是一个武器技术落后、经济基础薄弱的国家，在

时光流转，今天的中国已然不同，科技进步，武器现代化，国力显著增强。然而，与过去的硝烟不同，吾辈生于这个和平年代，并不能直接拿起枪杆子

🔥“垂钓大师同步源码(60多套日本源码)”🔥

来发起新形式的“战争”让那些曾经犯下罪行的日寇后代明白：复仇之火已点燃，谁也无法逃避。

- 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.

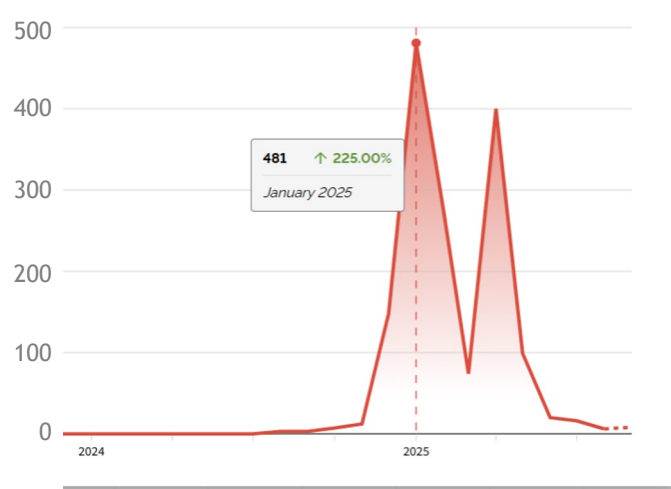
Instead, we can use 🔥 The Fishing Master (over 60 Japanese source kits) 🔥 to initiate a **new kind of war** — one that forces those postwar generation Japs, who have never paid for their crimes, to finally understand this:  
**The fire of revenge is now lit, no one can escape it.**

- **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"



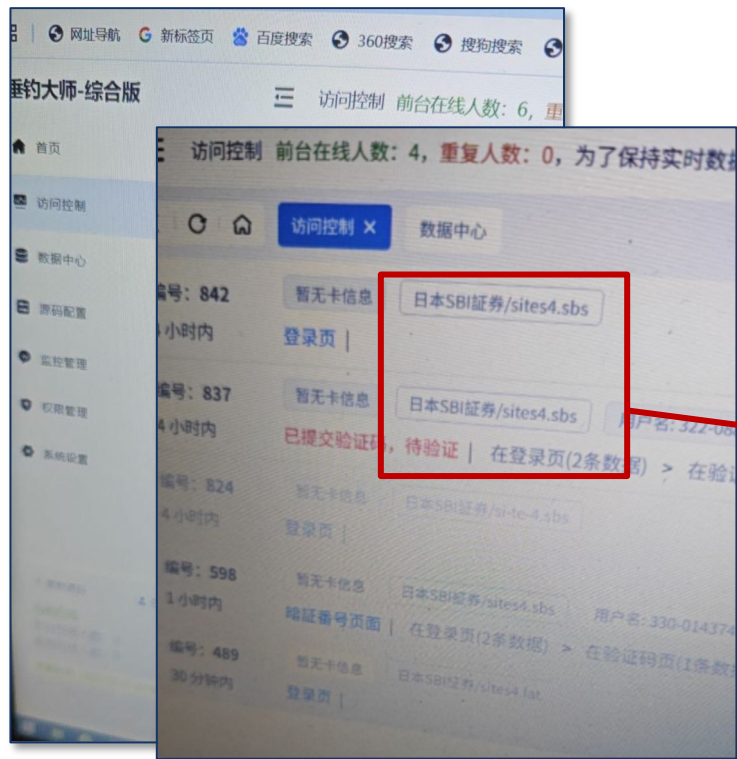
# Widely-Used PhaaS in Japanese Phishing Campaigns

- 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

sites4.sbs

31.57.170.225 **Malicious Activity!** Public Scan

URL: <https://sites4.sbs.co.jp/ETGate/>  
Submission: On April 30 via manual (April 30th 2025, 9:38:12 pm UTC) from JP - Scanned from JP

Method	Protocol	Status	Resource Path
POST	H/1.1	200 OK	<a href="#">createOrGetUserInfo</a> sites4.sbs/open/visitors/info/
GET	H/1.1	200 OK	<a href="#">getState</a> sites4.sbs/open/visitors/info/

Screenshot

Live screenshot Full Image

三 SBI証券 メインサイト

ログイン

ユーザーネーム

# 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>
```

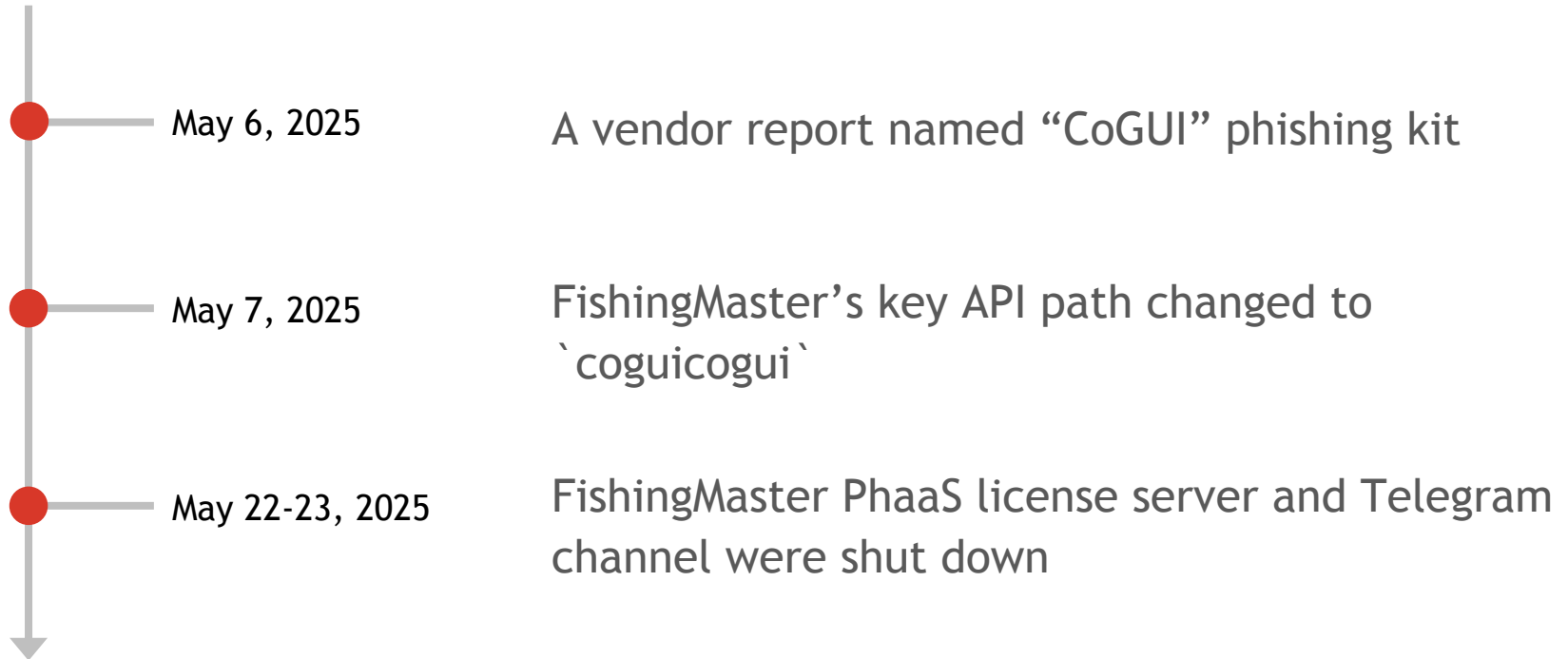
# FishingMaster API and codeName

```
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",
      packageNameTitle: "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



# 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 > 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 > JS cogui-key-func.js > G5

```
1  async function _4() {
  await m4()
  } 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

- **createOrGetUserInfo**
  - isBlacklist
  - getState
  - saveLoginInfo
  - saveAccountInfo
  - savePasscode
  - saveUserInfo
  - saveCustomCaptcha
  - updateState
  - ...
- same function with different name

## 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

Active period: May 7<sup>th</sup> ~ late June 2025

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

## (\*) 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

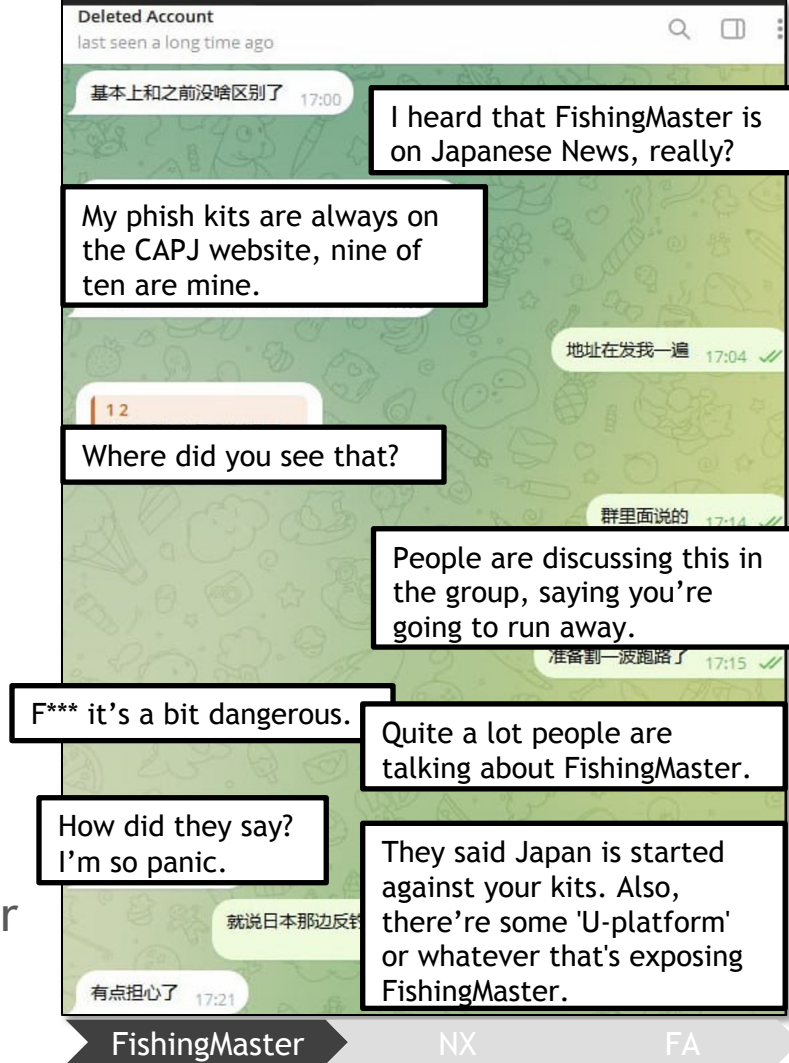
# Panic and Shutdown

- 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

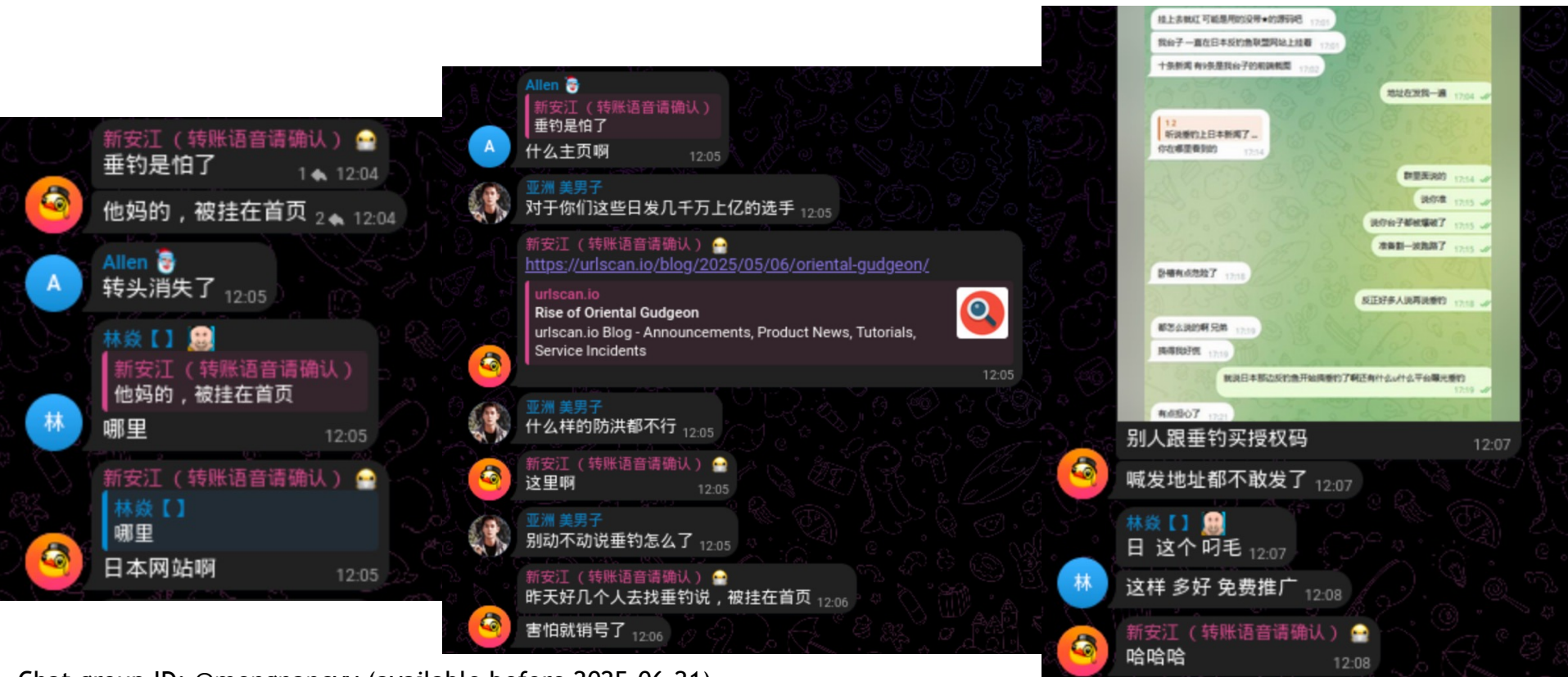


# Panic and Shutdown

- 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)

FishingMaster

NX

FA



# Underground Discussions Regarding the FishingMaster Shutdown

FishingMaster is spooked.  
Damn it, being publicly  
exposed on the homepage.

Allen  
转头消失了 12:05

林焱【】  
新安江 (转账语音请确认)  
他的... 挂在首页

Where?

新安江 (转账语音请确认)  
林焱【】  
哪里

Website in Japan.

Allen  
新安江 (转账语音请确认)  
What homepage?

亚洲 美男子  
对于你们这些日发几千万上亿的选手 12:05

URLScan.io blog link

Rise of Oriental Gudgeon  
urlscan.io Blog - Announcements, Product News, Tutorials,  
Service Incidents

亚洲 美男子  
什么样的防洪都不行 12:05

Here.

Yesterday, a bunch of guys went to  
FishingMaster to tell him he was pinned on  
the front page.  
He got spooked and nuked his account.

People were buying license keys and  
asking for the address, but he was  
too chicken to sending it..

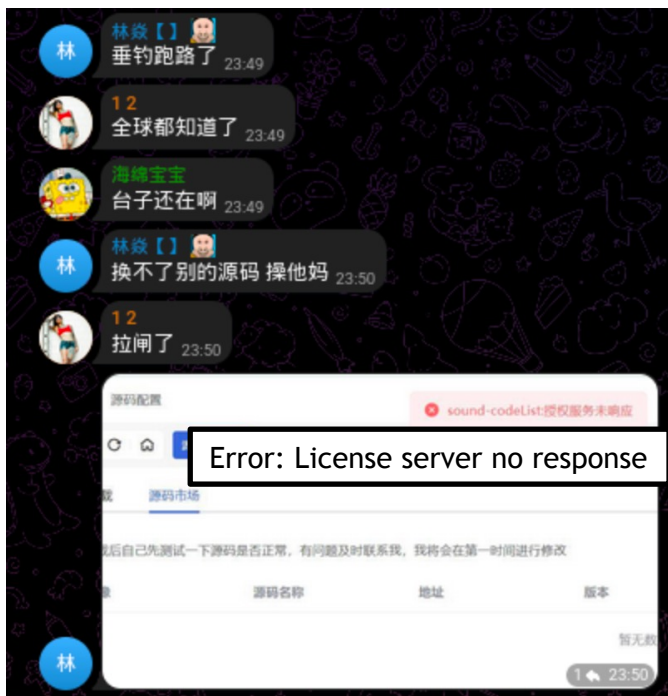
What a loser.  
This is great, a free promotion!  
LOL

哈哈

12:08

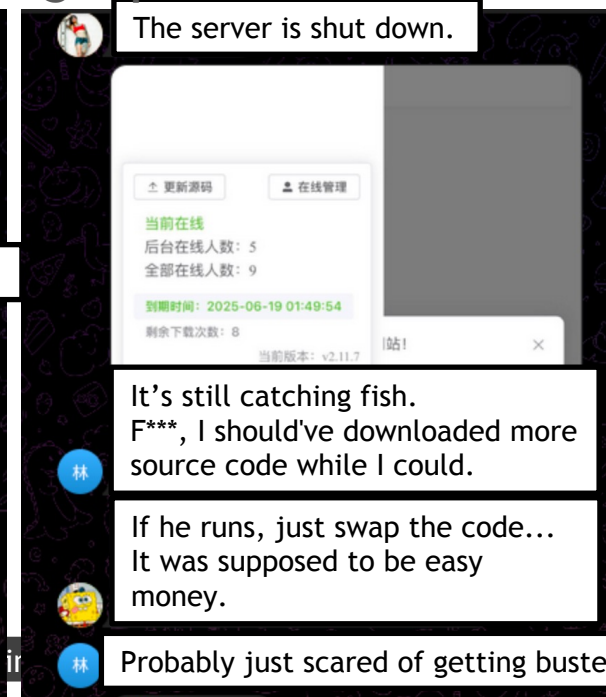
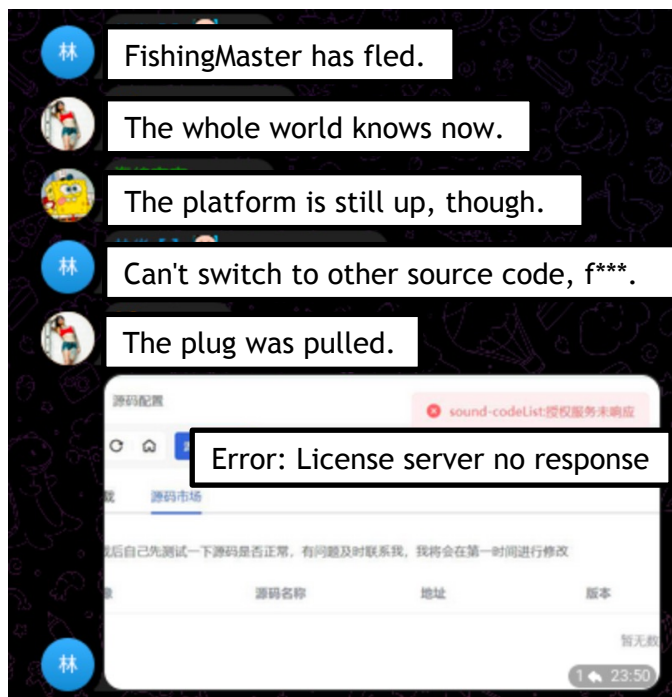
# Underground Discussions Regarding the FishingMaster Shutdown

- 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



# Underground Discussions Regarding the FishingMaster Shutdown

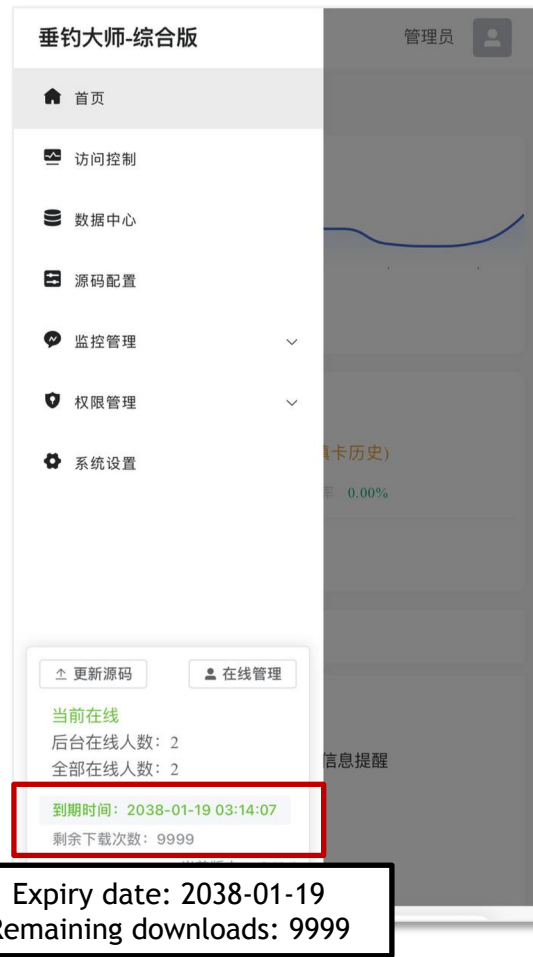
- Kits remain functional for users who previously downloaded them
- However, connection to the license server is no longer possible
- Once the license code deactivates, there's no way to activate





# 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。

## ShadowGarden

用户名

admin

密码

.....

验证码

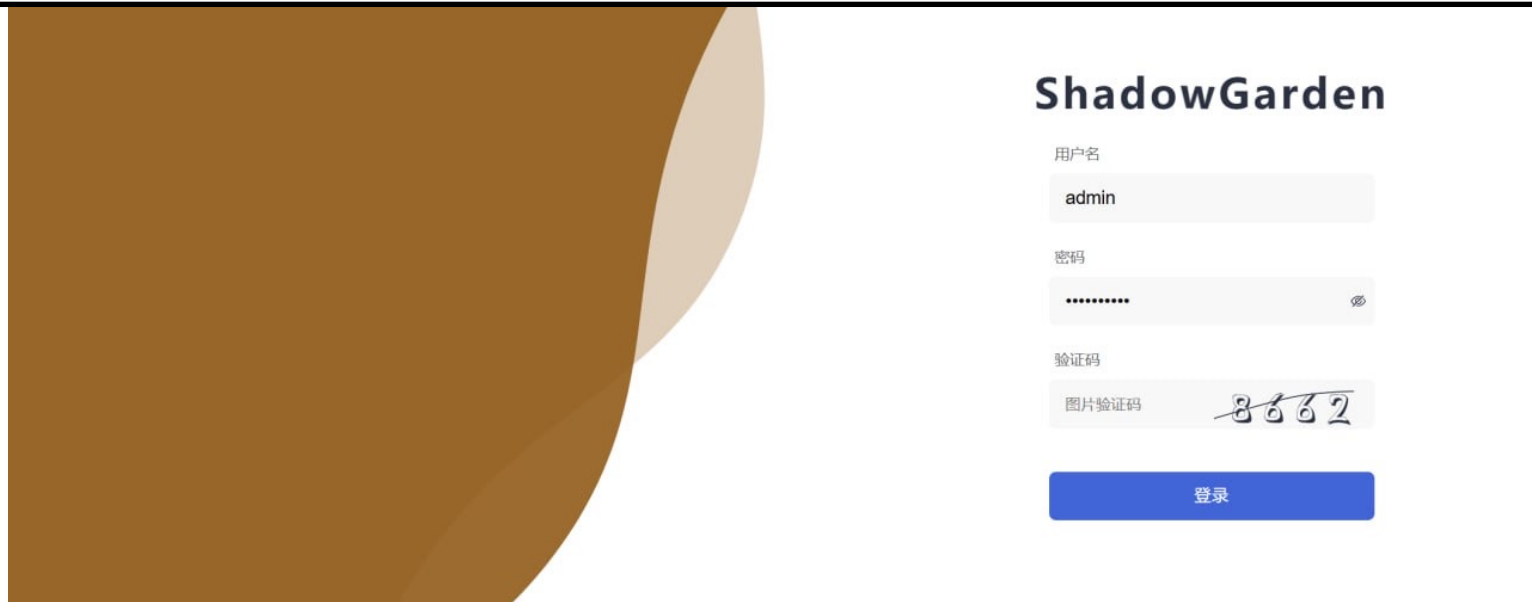
图片验证码

8662

登录

# 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.



ShadowGarden

用户名

admin

密码

.....

验证码

图片验证码 8862

登录

# Current FishingMaster on OSINT Search

## Shodan Report

http.title:"fishingmaster"

// GENERAL



### Ports

8001	1
8888	1

### Organization

NTT America, Inc.	1
RackNerd LLC	1

FQFA

title=="FISHINGMASTER垂钓大师"



AI 实验室 会员 支持及工具

HApP...

4

最近一个月

国家/地区排名

- >> 中国香港... 1
- >> 日本 1
- >> 马来西亚 1
- >> 美国 1

序号

主机名/Id

1	▶ 156.245.235.246:8001	HAp...
2	▶ 107.172.83.114:8888	HAp...
3	▶ 103.20.241.238:8001	HAp...
4	▶ 207.56.13.194:8001	HAp...



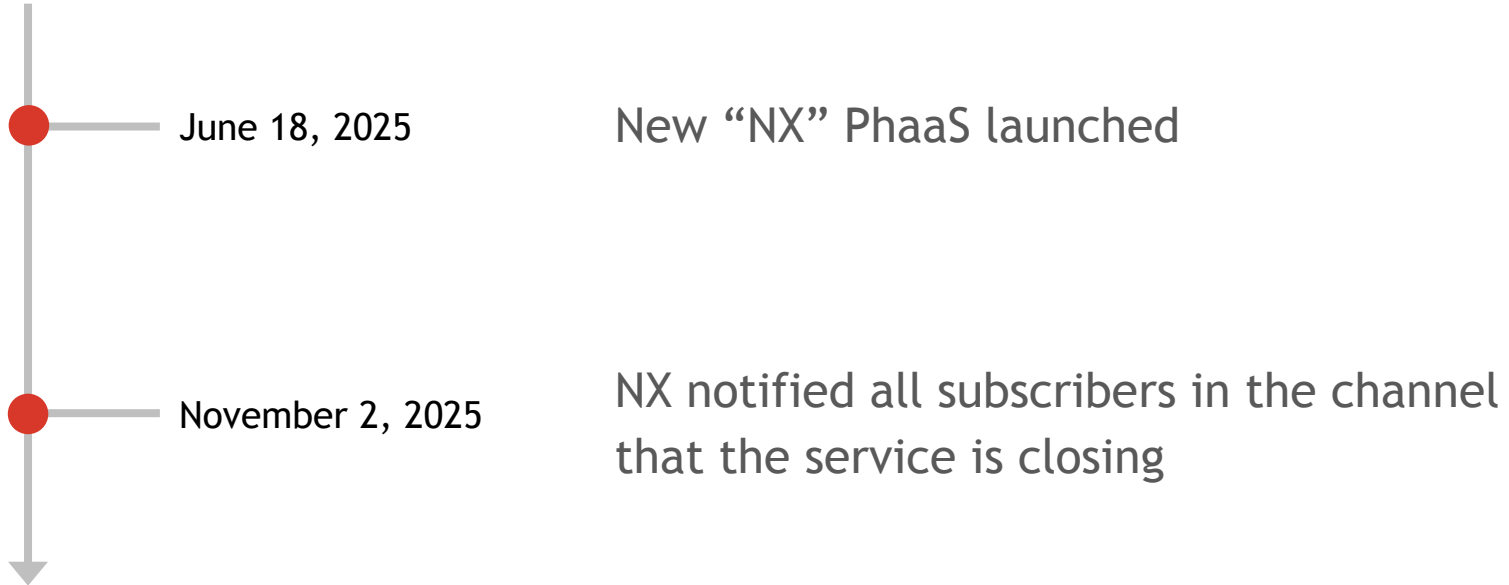
共 4 条

10条/页



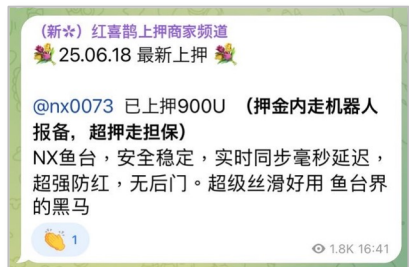
Rebrand to NX PhaaS

# Rebrand - Launch of NX PhaaS



# 1<sup>st</sup> Reincarnation - Rebranded as NX PhaaS

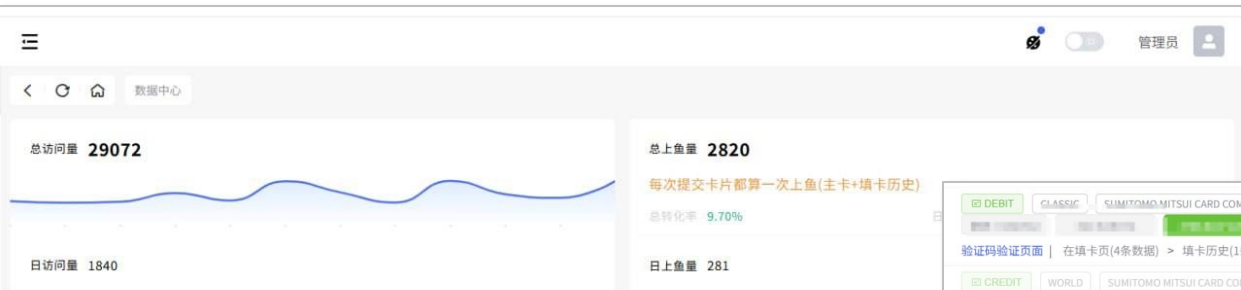
- Channel ID: @nx001channel
- User ID: @nx0073
- Setup guide: nxdocs[.]world



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



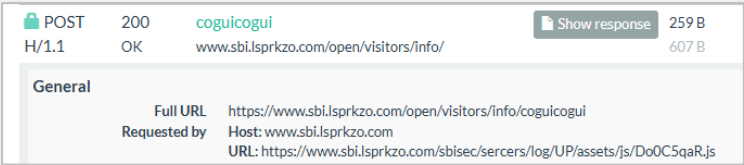
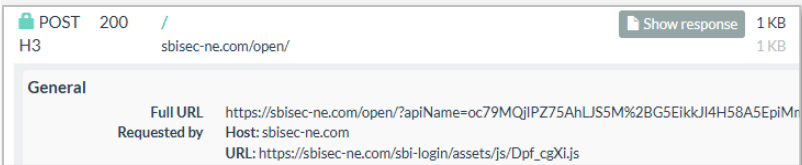

# NX PhaaS Admin Panel



<div> <div>DEBIT</div> <div>CLASSIC</div> <div>SUMITOMO CARD COMPANY, LTD.</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 09027457898</div> </div> <div> <div>验证码验证页面</div> <div>在填卡页(4条数据)</div> <div>在填卡历史(1条数据)</div> </div>	<div> <div>DEBIT</div> <div>CLASSIC</div> <div>SUMITOMO CARD COMPANY, LTD.</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 09027457898</div> </div> <div> <div>跳转</div> <div>拒绝</div> <div>↑</div> <div>⌂</div> <div>⌕</div> </div>
<div> <div>CREDIT</div> <div>WORLD</div> <div>SUMITOMO MITSUBI CARD COMPANY, LTD.</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>验证码: 865510</div> </div> <div> <div>验证码验证页面</div> <div>在填卡页(4条数据)</div> <div>在验证码页(1条数据)</div> </div>	<div> <div>CREDIT</div> <div>WORLD</div> <div>SUMITOMO MITSUBI CARD COMPANY, LTD.</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>验证码: 865510</div> </div> <div> <div>跳转</div> <div>拒绝</div> <div>↑</div> <div>⌂</div> <div>⌕</div> </div>
<div> <div>DEBIT</div> <div>OTHER</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 07040682385</div> <div>密码: yuino2109</div> <div>SAYURI SUZUKI</div> </div> <div> <div>验证码: 64477832</div> </div> <div> <div>提交验证码, 特验证</div> <div>在填卡页(4条数据)</div> <div>在验证码页(1条数据)</div> </div>	<div> <div>DEBIT</div> <div>OTHER</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 07040682385</div> <div>密码: yuino2109</div> <div>SAYURI SUZUKI</div> </div> <div> <div>验证码: 64477832</div> </div> <div> <div>跳转</div> <div>拒绝</div> <div>↑</div> <div>⌂</div> <div>⌕</div> </div>
<div> <div>CREDIT</div> <div>GOLD</div> <div>VJA</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: supikapika6160@icloud.com</div> <div>密码: supika0616</div> </div> <div> <div>验证码: 67733124</div> </div> <div> <div>提交验证码, 特验证</div> <div>在填卡页(4条数据)</div> <div>在验证码页(1条数据)</div> </div>	<div> <div>CREDIT</div> <div>GOLD</div> <div>VJA</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: supikapika6160@icloud.com</div> <div>密码: supika0616</div> </div> <div> <div>验证码: 67733124</div> </div> <div> <div>跳转</div> <div>拒绝</div> <div>↑</div> <div>⌂</div> <div>⌕</div> </div>
<div> <div>CREDIT</div> <div>CLASSIC</div> <div>CREDIT SAISON CO., LTD.</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 08048727022</div> </div> <div> <div>验证码: 645376</div> </div> <div> <div>验证码验证页面</div> <div>在填卡页(4条数据)</div> <div>在验证码页(1条数据)</div> </div>	<div> <div>CREDIT</div> <div>CLASSIC</div> <div>CREDIT SAISON CO., LTD.</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 08048727022</div> </div> <div> <div>验证码: 645376</div> </div> <div> <div>跳转</div> <div>拒绝</div> <div>↑</div> <div>⌂</div> <div>⌕</div> </div>
<div> <div>DEBIT</div> <div>CLASSIC</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: ma0yu7ma2yu6chi@icloud.com</div> <div>密码: posse0726</div> <div>MAYUKO KIBA</div> </div> <div> <div>验证码: 078309</div> </div> <div> <div>验证码验证页面</div> <div>在填卡页(4条数据)</div> <div>在验证码页(1条数据)</div> </div>	<div> <div>DEBIT</div> <div>CLASSIC</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: ma0yu7ma2yu6chi@icloud.com</div> <div>密码: posse0726</div> <div>MAYUKO KIBA</div> </div> <div> <div>验证码: 078309</div> </div> <div> <div>跳转</div> <div>拒绝</div> <div>↑</div> <div>⌂</div> <div>⌕</div> </div>
<div> <div>DEBIT</div> <div>CLASSIC</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 09019501389</div> <div>密码: YuutaYuuta0929</div> <div>KOBAYAKAWA YUTA</div> </div> <div> <div>验证码: 831582</div> </div> <div> <div>验证码验证页面</div> <div>在填卡页(4条数据)</div> <div>在验证码页(1条数据)</div> </div>	<div> <div>DEBIT</div> <div>CLASSIC</div> <div>日本亚马逊amazon无限单重购2/st-casting.com</div> <div>用户名: 09019501389</div> <div>密码: YuutaYuuta0929</div> <div>KOBAYAKAWA YUTA</div> </div> <div> <div>验证码: 831582</div> </div> <div> <div>跳转</div> <div>拒绝</div> <div>↑</div> <div>⌂</div> <div>⌕</div> </div>



# Key Changes in NX PhaaS

	FishingMaster	NX
Masked Codename	<pre>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)", });</pre>	<pre>const v1616 = await v1500.post("/visitors/info/createUser", {   currentstate: 2,   browserInfo: f365(),   domain: window.location.hostname,   codeName: undefined, });</pre>
Obfuscated Request & Response		
Special Kits	N/A	

```

10096-   type: "user",
10097-   uuid: v857,
10098-   isNewuser: false
10099- });
10100- await v858.connect();
10101- const vvf144 = vf144(vvf214);
10102- vvf144.provide("socketClient", v858);
10103- vvf144.use(f209());
10104- vvf144.mount("#app");
10105- await f303();
10106- } else {
10107-   await f301(100, 200);
10108-   const v859 = await v827.post("/visitors/info/cogucicogui", {
10109-     currentState: 2,
10110-     browserinfo: f299(),
10111-     domain: window.location.hostname,
10112-     codename: "日本sbi証券(增加信息页)",
10113-     buttons: v099,
10114-     views: f304(["1"])

```

Masked "codeName"

```

14515-   type: "user",
14516+   uuid: v1614,
14517+   p: 2
14518+ });
14519+ await v1615.connect();
14520+ const vVF148 = vF148(vVF217);
14521+ vVF148.provide("socketClient", v1615);
14522+ vVF148.use(f203());
14523+ vVF148.mount("#app");
14524- } else {
14525+   await f368(100, 300);
14526+   const v1616 = await v1500.post("/visitors/info/createUser", {
14527+     currentState: 2,
14528+     browserInfo: f365(),
14529+     domain: window.location.hostname,
14530+     codeName: undefined,
14531+     buttons: v0147,
14532+     codeType: 6,
14533+     extraData: {
14534+       phonemessage: "号码1|号码2"
14535+     },
14536+     views: f371([])

```

```

10137- async function f307() {
10138-   await f302();
10139-   await f301(200, 500);
10140-   const v861 = await f300();
10141-   if ((await v827.post("/visitors/info/validatehuman", {
10142-     fp: v861,

```

Internally still refers the same APIs

```

10143-   domain: window.location.hostname
10144- })).code !== 1000) {
10145-   document.body.innerHTML = "";
10146-   const v862 = document.createElement("h2");
10147-   v862.textContent = "404 error: page not found, sorry, we couldn't find the page you're looking";
10148-   v862.style.margin = "14px";
10149-   document.body.appendChild(v862);

```

```

14563+   await f369();
14564+   await f368(200, 500);
14565+   if (localStorage.getItem("cs") === "200") {
14566+     window.location.href = localStorage.getItem("completionRedirect");
14567+   } else {
14568+     const v1618 = await f366();
14569+     await v1500.post("/visitors/info/validateHuman", {
14570+       fp: v1618,
14571+       domain: window.location.hostname
14572+     });
14573+     if (localStorage.getItem("disconnect")) {
14574+       const vLSvisitorsinfoisBlackl = "/visitors/info/isBlacklist";
14575+       if (Math.random() < 0.5) {
14576+         await f368(100, 320);
14577+         await v1500.post(vLSvisitorsinfoisBlackl);

```

# 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("./9xl0nhNx.js"), __vite__m;  
  mx(() => import("./BKsh7hmb.js"), __vite__m;  
  mx(() => import("./BIw27SGl.js"), __vite__m;  
  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",  
    packageNameTitle: "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”

 POST 200 / sbisec-ne.com/open/  33 B 81ms XHR 172.67.142.194 CLOUDFLARENET 

General

Full URL

Requested by

Protocol

Security

Server

Reverse DNS

Software

Resource Hash

https://sbisec-ne.com/open/?apiName=U%2BI4IAzznkrOQGBf0gXP5kr4nakHQNghbWm%2Bwhr%2FDS06C3FKqNxySsx%2BzXv0sZOW

Host: sbisec-ne.com

H3

QUIC, , AES\_128\_GCM

172.67.142.194 , Ascension Island, ASN13335 (CLOUDFLARENET, US),

cloudflare /

8bc55f760a8ad956e66394c3a32b26711b660c74d20d358b35ec1e3b2ba2c728

Decrypted: /visitors/info/validateHuman

Check archive.org

Show headers

Download

Go to

# Novel Types of Phishing

A screenshot of a mobile app interface designed to look like an Apple Account page. At the top, there is a dark header with a hamburger menu icon, an Apple logo, and a shopping bag icon. Below the header, the text "Apple Account" is followed by a checkmark icon. The main content area contains two sections for uploading credit card images. The first section is titled "クレジットカードの画像をアップロードしてください。" and includes a sub-label "クレジットカード表面 必須". Below this is a button labeled "アップロードする" with a right-pointing arrow. The second section is titled "クレジットカード裏面 必須" and also has a button labeled "アップロードする" with a right-pointing arrow. At the bottom of the page, there is a blue button labeled "次へ進む". A small footer at the very bottom contains text about purchase methods: "その他の購入方法: お近くのApple Store、またはApple 製品取扱店で製品を購入することもできます。電話による購".

A screenshot of a mobile app interface for au (au), a Japanese telecommunications company. The header features the text "おもしろいほうの未来へ、au" in orange. Below the header, the text "本人確認をお願いします" is displayed in orange. The main content area is titled "ご契約者さま本人確認 必須" in red. Below this, a paragraph explains the verification method: "ご本人さま確認の方法は画像アップロードのみとなります。下記より本人確認書類の画像アップロードをお願いいたします。". A large orange-bordered box contains the text "画像アップロードによる本人確認". Below this box, a blue arrow points down to the text "アップロードする画像を選択 必須". A dropdown menu labeled "マイナンバーカード" is shown. Below the dropdown, a section titled "必ずお読みください" contains two bullet points: "コピーやスキャンしたものはお受付できません" and "全体が見えるように撮影してください". An illustration of a smartphone and a document is shown below the text. At the bottom, a paragraph states: "本人確認書類に記載の住所が現住所と異なる場合、画像アップロードによる本人確認のみになります。".

A screenshot of a mobile app interface for telephone number verification. The title "電話番号認証" is displayed in large black characters. Below the title, the text "ご本人確認のため、SMSで認証コードを送信します" is shown. A text input field contains the example number "例) 09012345678". Below the input field is a large blue button labeled "コードを送信". At the bottom of the page, the text "認証コードを入力" is followed by "コードが届いたら上記に入力ください".

# Cloaking in NX PhaaS

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



A screenshot of a security check dialog box. At the top, there is a yellow shield icon with a lightning bolt and the text 'セキュリティチェック'. Below this, the main heading is 'ロボットではないことを確認してください'. Underneath, a paragraph explains the purpose: '自動化された攻撃からサービスを保護するため、以下の確認を行ってください'. In the center, there is a checkbox followed by the text '私はロボットではありません'. At the bottom of the dialog, there are two links: 'セキュリティ確認' (with a green checkmark icon) and 'プライバシー・利用規約'. At the very bottom, a line of text states: 'この確認は不正なアクセスからサービスを守るためのものです'.

セキュリティチェック

ロボットではないことを確認してください

自動化された攻撃からサービスを保護するため、以下の確認を行ってください

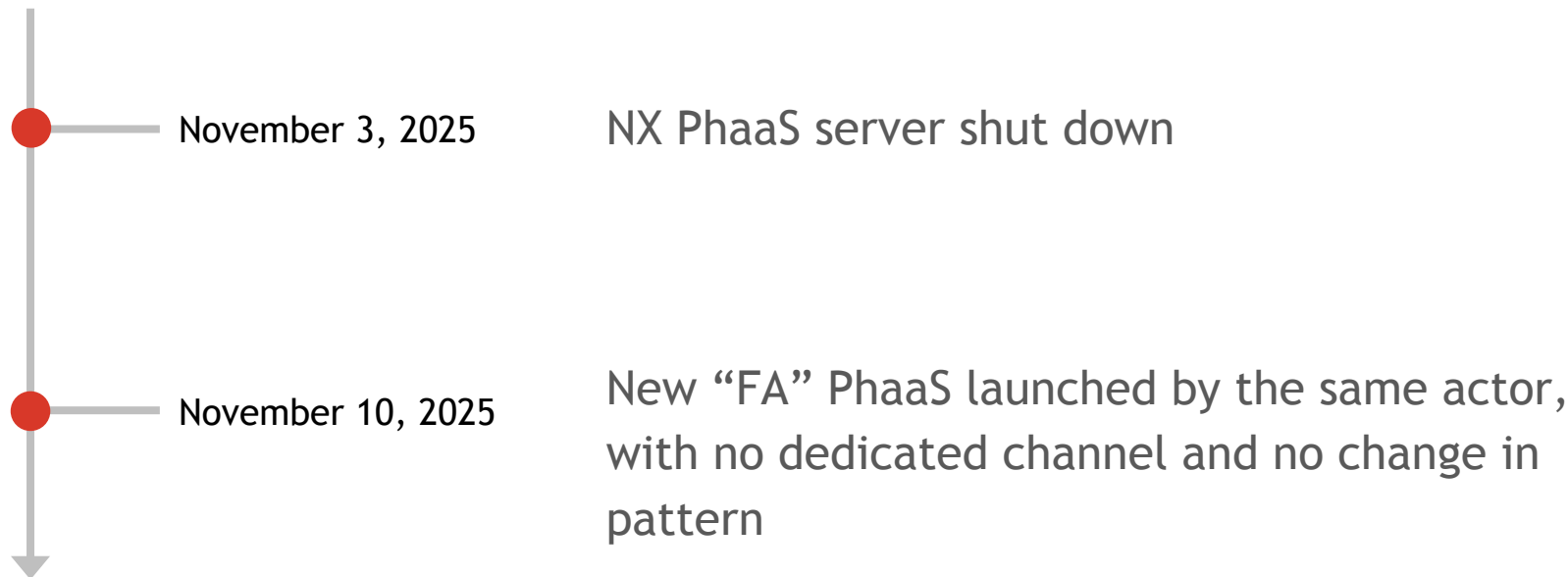
☐ 私はロボットではありません

 セキュリティ確認      プライバシー・利用規約

この確認は不正なアクセスからサービスを守るためのものです

# Latest Migration to FA PhaaS

# Latest Migration to FA PhaaS





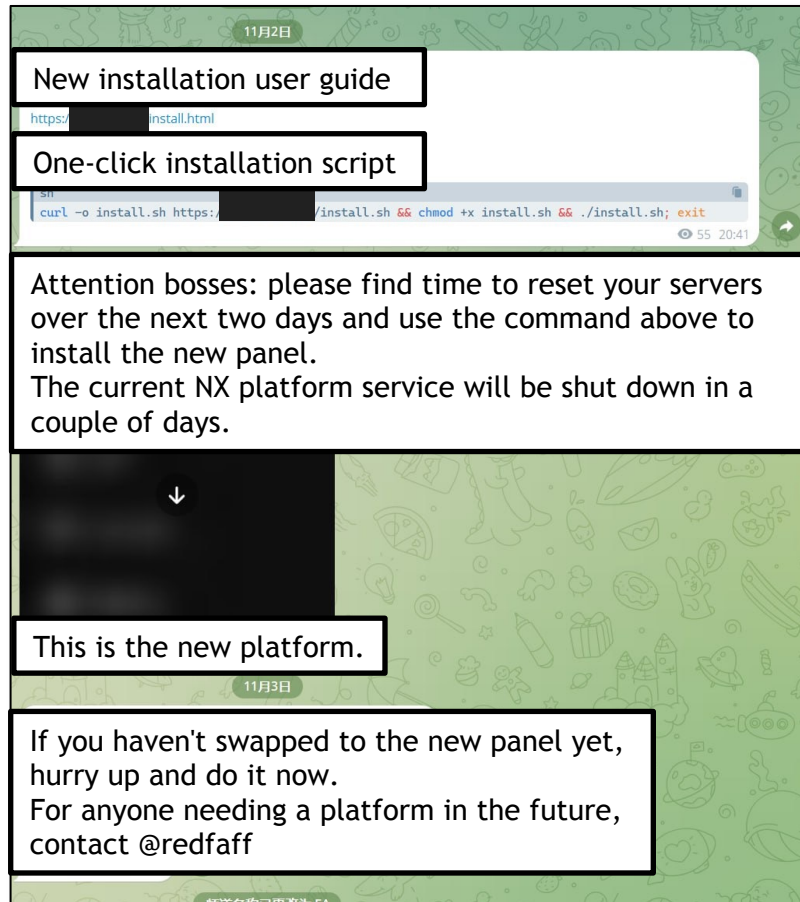
## 2<sup>nd</sup> Reincarnation - Rebranding to FA PhaaS

- NX PhaaS channel was renamed to “FA” on Nov. 3<sup>rd</sup>, 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>**

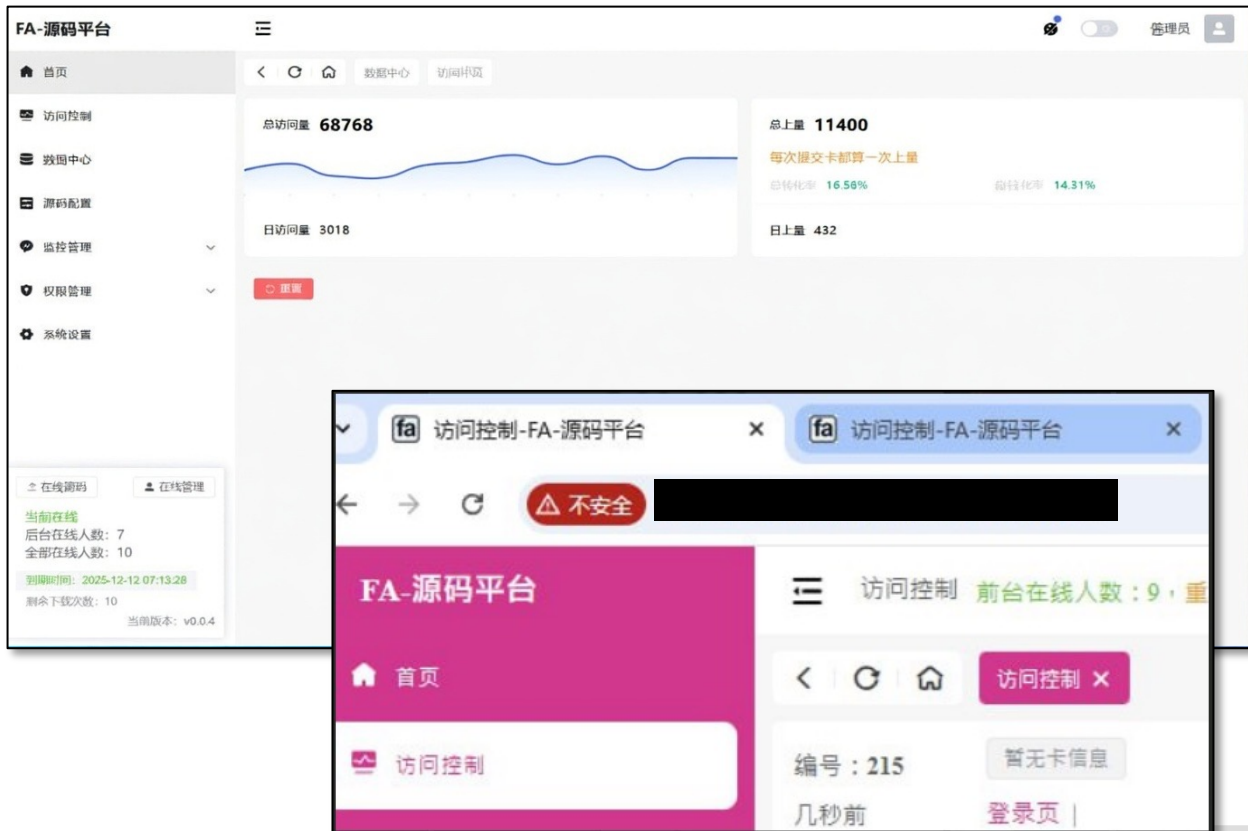


## 2<sup>nd</sup> Reincarnation - Rebranding to FA PhaaS

- NX PhaaS channel was renamed to “FA” on Nov. 3<sup>rd</sup>, 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



The screenshot displays the '访问控制' (Access Control) section of the FA PhaaS Admin Panel. The top navigation bar includes '首页' (Home), '访问控制' (Access Control), '数据中心' (Data Center), '源码配置' (Source Code Configuration), '监控管理' (Monitoring Management), '访问日志' (Access Logs), '操作日志' (Operation Logs), '黑白名单' (Black/White List), '权限管理' (Permission Management), '用户列表' (User List), '角色列表' (Role List), and '系统设置' (System Settings). The main content area shows a list of users with their activity details.

编号	状态	设备	时间	操作
1402	暂无卡信息	apple无	1小时前	登录页   在登录页(2条)
1399	暂无卡信息	apple无	1小时前	填卡页面   在登录页(2条)
1397	暂无卡信息	apple无	1小时前	填卡页面   在登录页(2条)
1396	暂无卡信息	apple无	1小时前	填卡页面   在登录页(2条)
1395	暂无卡信息	apple无	1小时前	填卡页面   在登录页(2条)
1394	暂无卡信息	apple无	1小时前	填卡页面   在登录页(2条)
1393	暂无卡信息	apple无	1小时前	填卡页面   在登录页(2条)
1392	暂无卡信息	apple无	1小时前	填卡页面   在登录页(2条)
1391	apple无账单/充值	apple无	1小时前	填卡页面   在登录页(2条)
1138	暂无卡信息	apple无	5小时前	登录页   在登录页(2条)

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

Added



Deleted

Japan-Targeted

Others Countries



LINE



coinbase



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

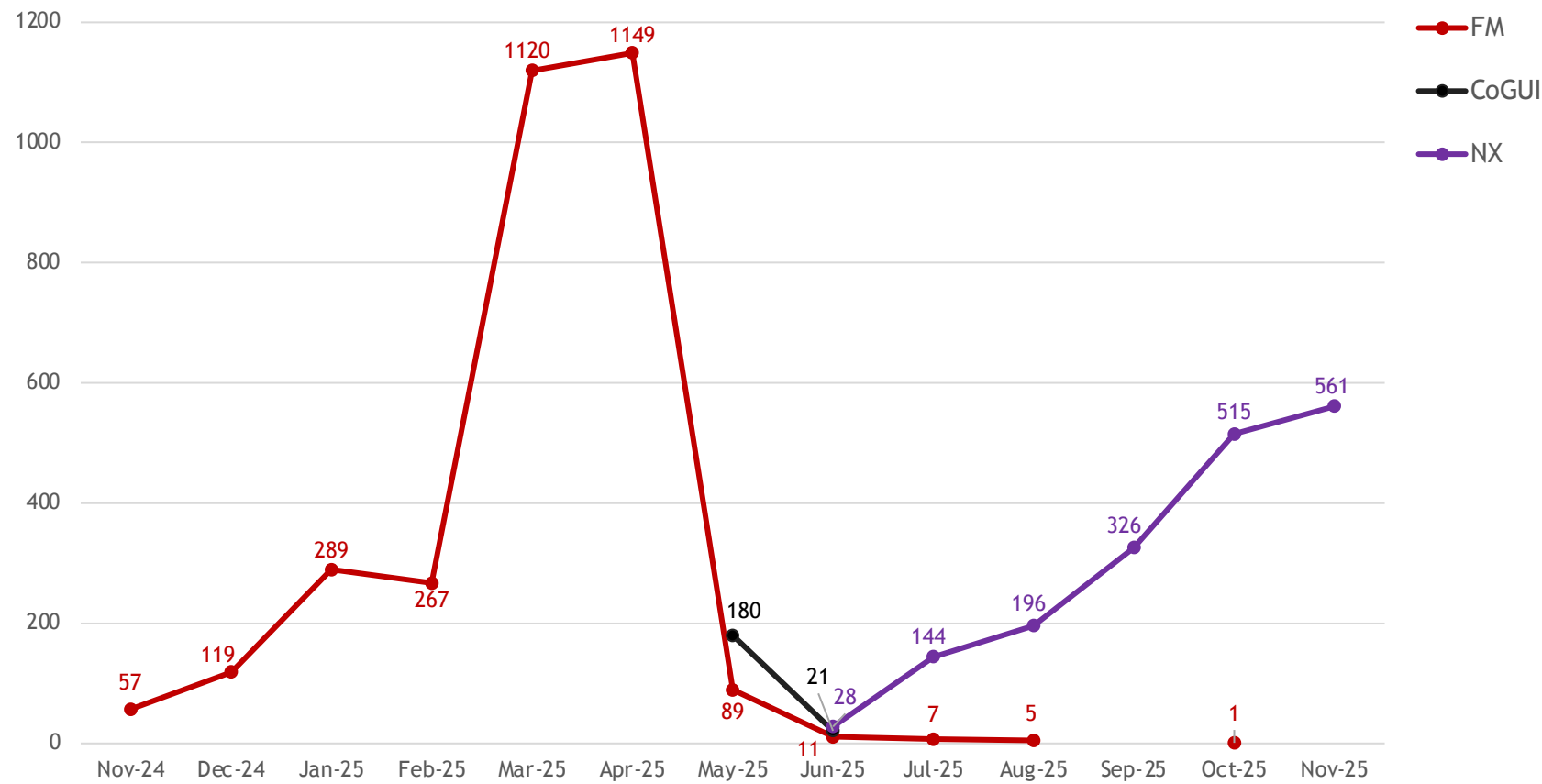
```
- var v1493 = v090.exports;  
- const vF2712 = f271(v1493);  
- const vA86 = ["7gH3", "pL9k", "Vx02", "zY6b", "8Mcn5D", "3bRtPq"];  
- const v1494 = vA86.join("");  
- const v1495 = vF2712.enc.Utf8.parse(v1494.slice(0, 16));  
- function f259() {
```

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

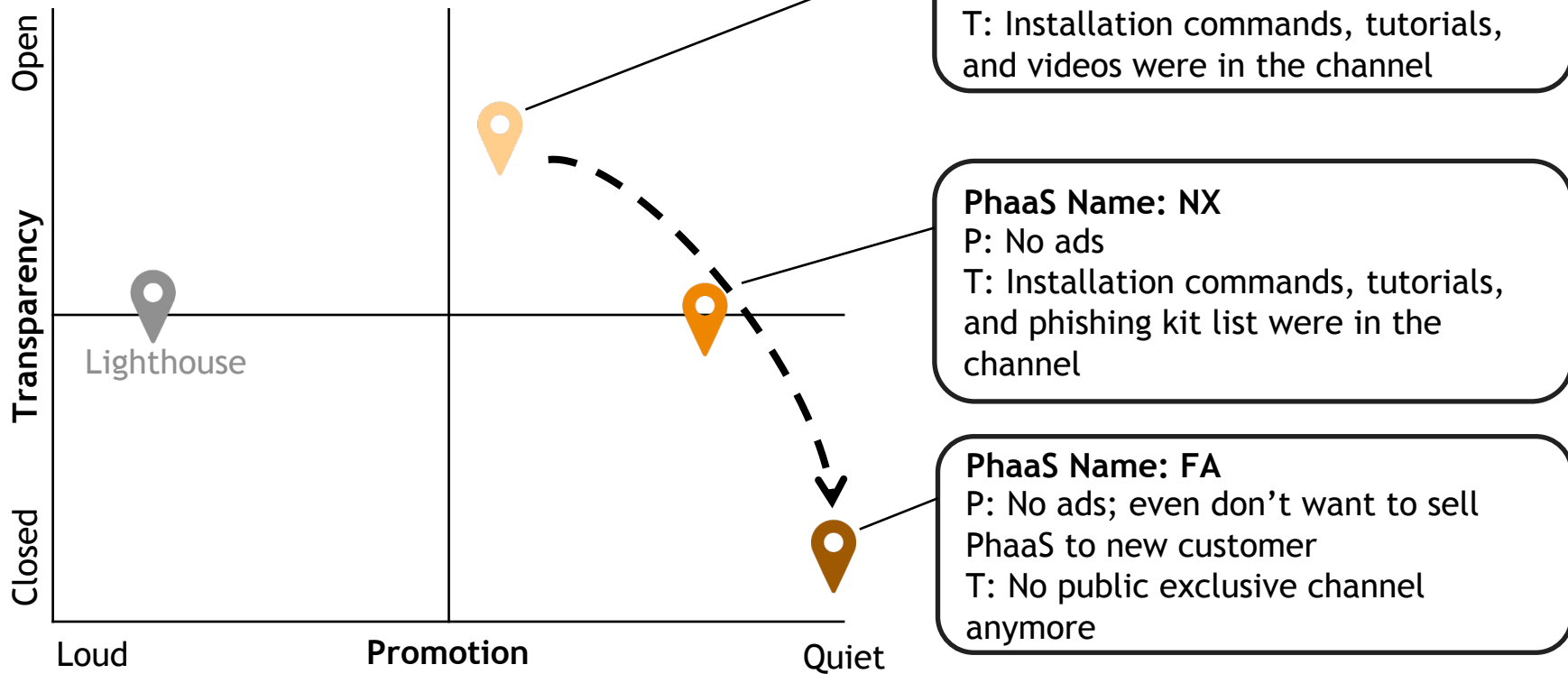
Closed

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

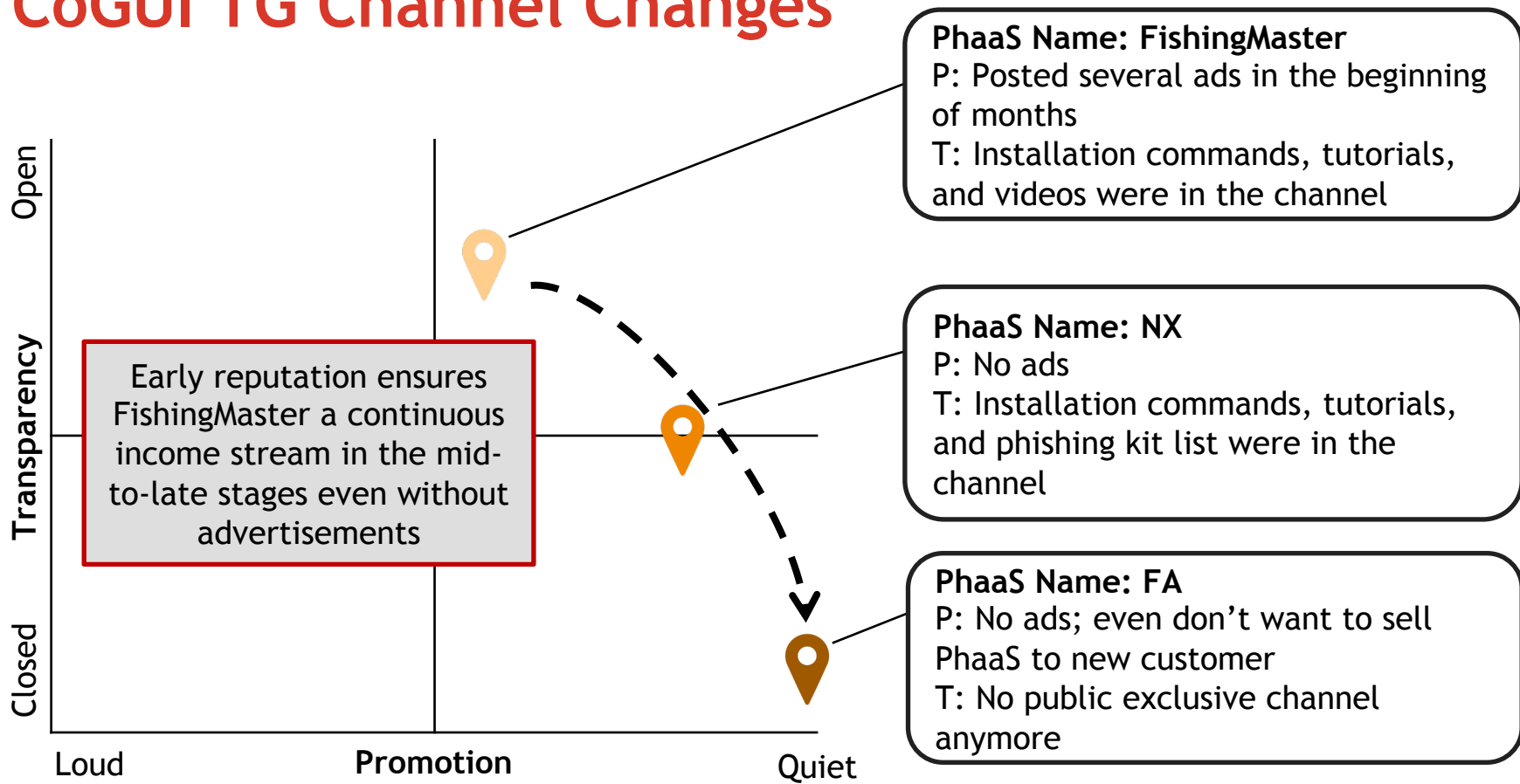
Channels contain little to no information, perhaps with some occasional advertisements



# CoGUI TG Channel Changes



# CoGUI TG Channel Changes





# 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 13<sup>th</sup>, 2025
- License server were taken down in the same day, citing court order

这是关于您服务已被暂停的通知。以下是此次暂停的具体详情：

产品/服务：2GB KVM 云服务器专用版

域名：[REDACTED]

金额：20.98 美元

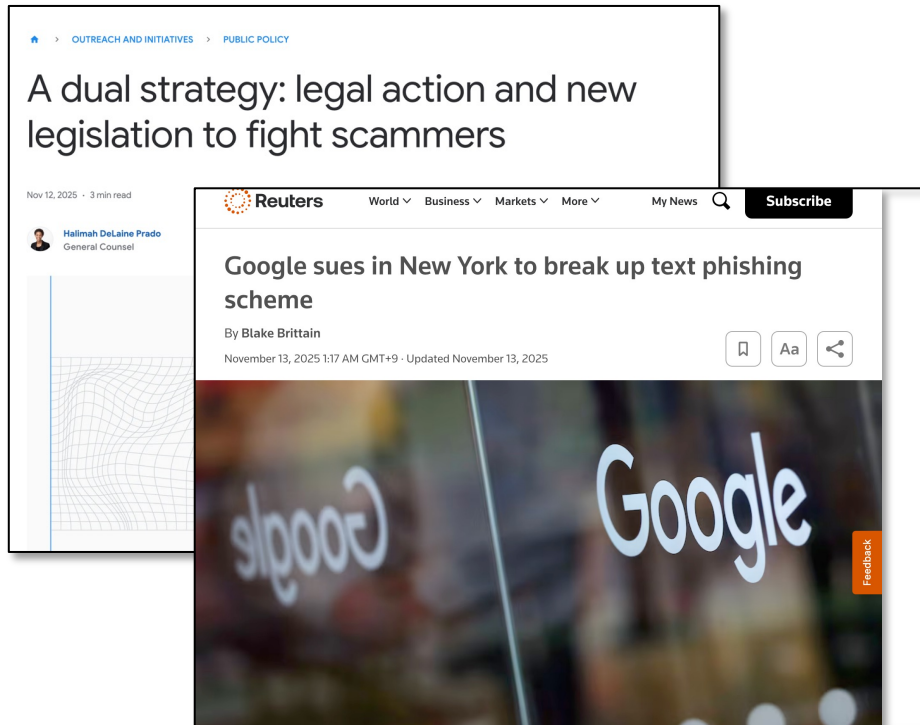
截止日期：2028 年 11 月 26 日

停职原因：法院下令停职

请尽快与我们联系，以便重新激活您的服务。

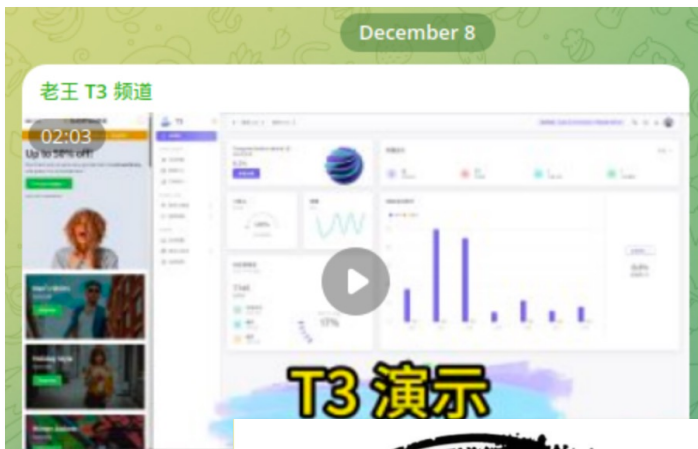
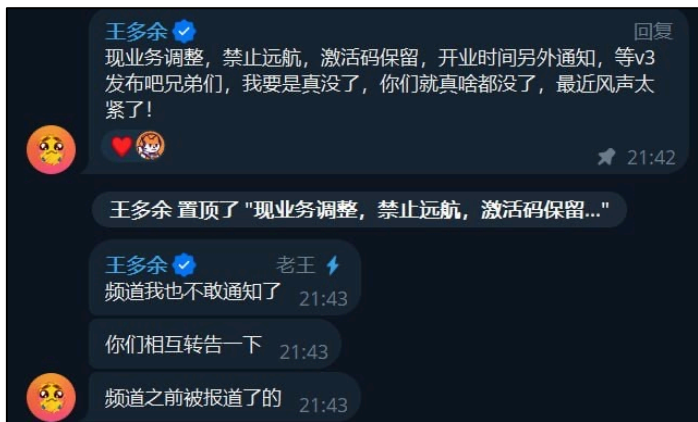
谢谢！

Image from Lighthouse VIP channel



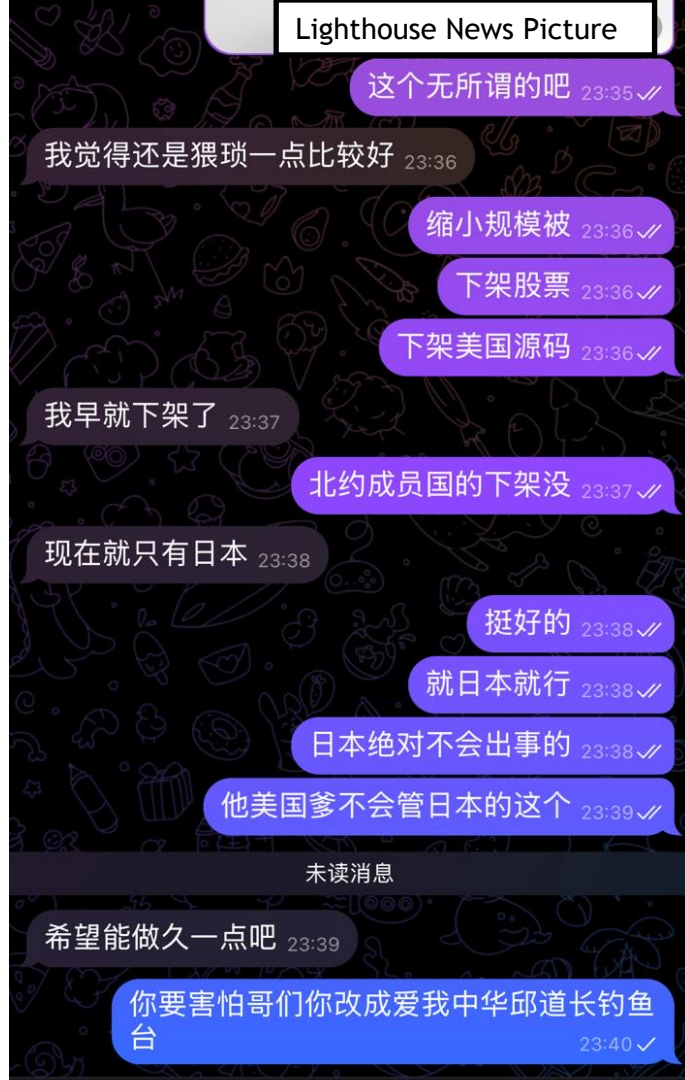
# Reaction: Disruption to Lighthouse PhaaS

- Lighthouse seized all operations on November 14<sup>th</sup>, 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( 西日本シティバンク)
- 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)

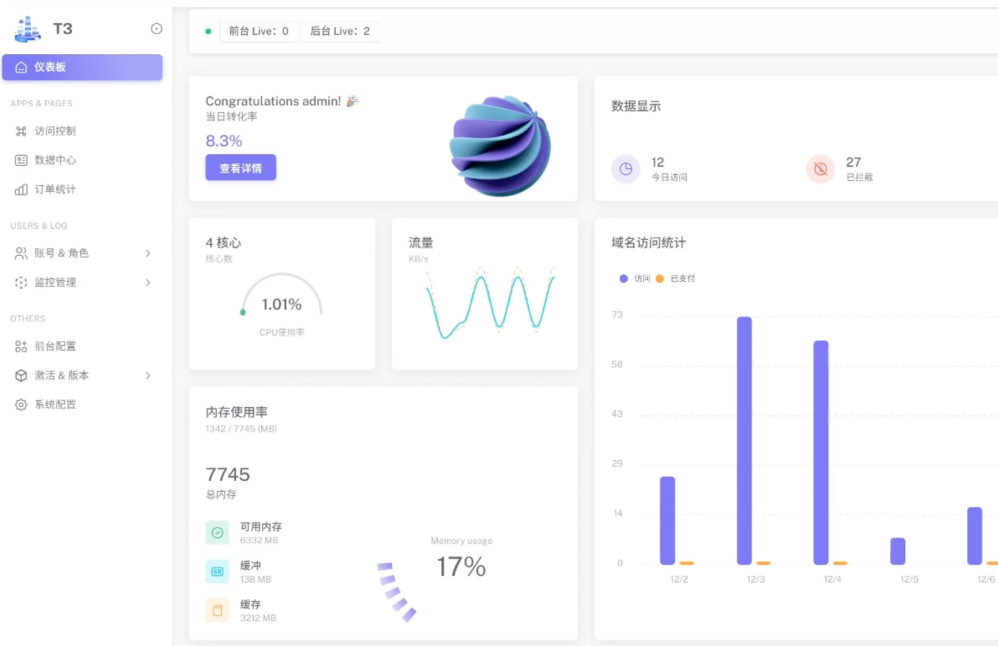
# Appendix: Targeted Brands and Services (Others)

- 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

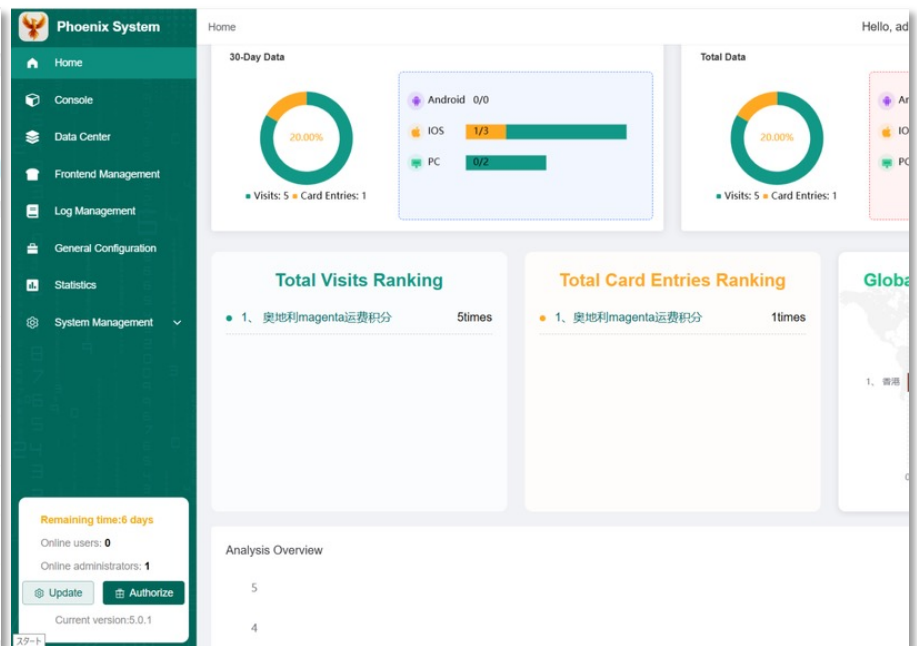


# Appendix: Major Chinese Phishing-as-a-Service

## Lighthouse PhaaS (T3)

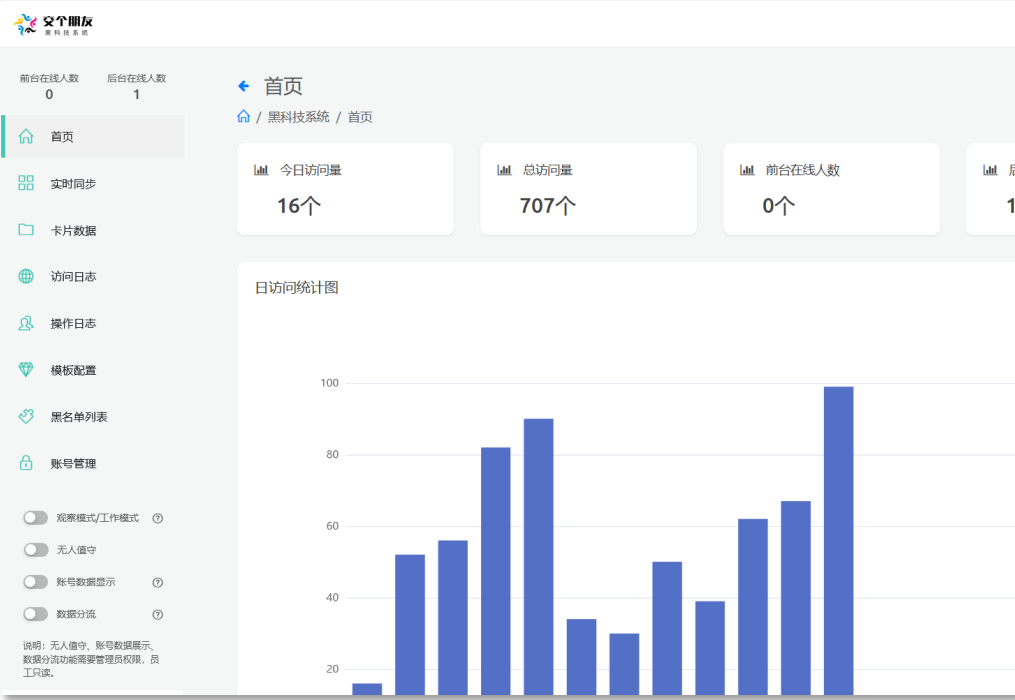


## Haozi PhaaS (Pheonix)



# Appendix: Major Chinese Phishing-as-a-Service

Lucid PhaaS



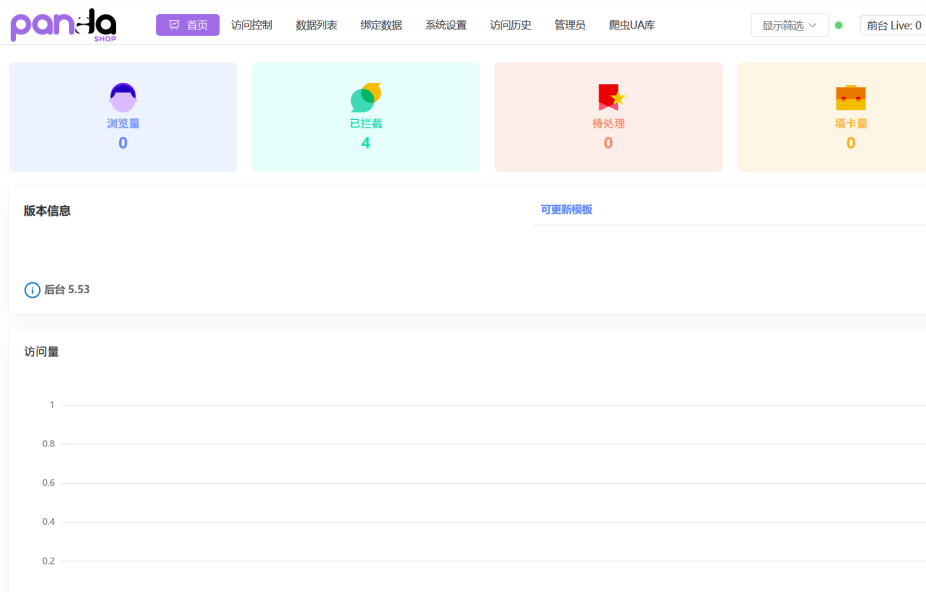
YYLU PhaaS

The screenshot displays the YYLU PhaaS dashboard. On the left is a sidebar menu with options: 管理在线人数 (Manage Online Users), 前台在线人数 (Frontend Online Users), 正在地址页人数 (Users on Address Page), 正在填卡页人数 (Users on Card Page), 隐藏所有离线 (Hide All Offline), 保留离线有卡 (Keep Offline with Card), 隐藏在线无卡 (Hide Online without Card), 卡片信息 (Card Information), 数据查询 (Data Query), 前台管理 (Frontend Management), 前台安装 (Frontend Installation), 用户设置 (User Settings), and 设置 (Settings). The main content area features a table with columns: id, 在线状态 (Online Status), 姓名 (Name), 手机号 (Mobile Number), 地址 (Address), 邮编 (Postal Code), and 卡号 (Card Number). The data is as follows:

id	在线状态	姓名	手机号	地址	邮编	卡号
3239	离线	fjejwj fjdjs	8668656	cjjdjd	djjdjd	5217 3200 0000 0000
3227	在线	214	0000000000	1234	234	
3204	离线		25235235235235 235	235235	23452352 35	5217320000000000
3198	离线	123	61433009421	122	忘了	5210
3197	离线	23235	234234234234	2365236	23523562 36	5217320000000000
3186	离线	鹿糖城				5210 1200 9246 9304
3183	离线	123	12	12	12	5217 3200 0000 0000
3170	离线	1234235	12345634432	1	134	5210 1200 9246 9304
3163	离线	fjdjij skekkkw	38665629	eiejje djei	46469499 4	5217 3200 0000 0000
3162	离线	123	234	123	1234	5212 3201 0001 0002
3161	离线	ejeji dje	386569292	djjdjsj	866464	5217 3200 0000 0000
3153	离线	Andrea gonzalez	951969889	Paso nevado	3520000	4345 5911 3868
3152	离线	cifjr djddjd	436865659	dhhhdh djs	djjdjd	5217 3200 0000 0000
3104	离线	Benjamin soto	951566990	Patagua cerro	2980000	4345 5913 1590 6226
3102	离线	133974377	+56951245837	AVDA. La Concepción Nro 767 B Cunco	489000	4345 6130 3445 3650

# Appendix: Major Chinese Phishing-as-a-Service

## Panda Shop PhaaS



## Outsider PhaaS

