

# Beyond CoGUI: Exposing the FishingMaster PhaaS Ecosystem Behind Global Phishing Campaigns

Shadow Liu, Albert Song, Lime Chen, Strawberry Donut

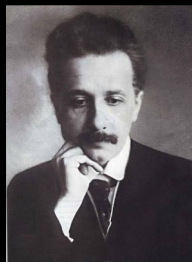
# TeamDonut Contributors

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.

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.

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.

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

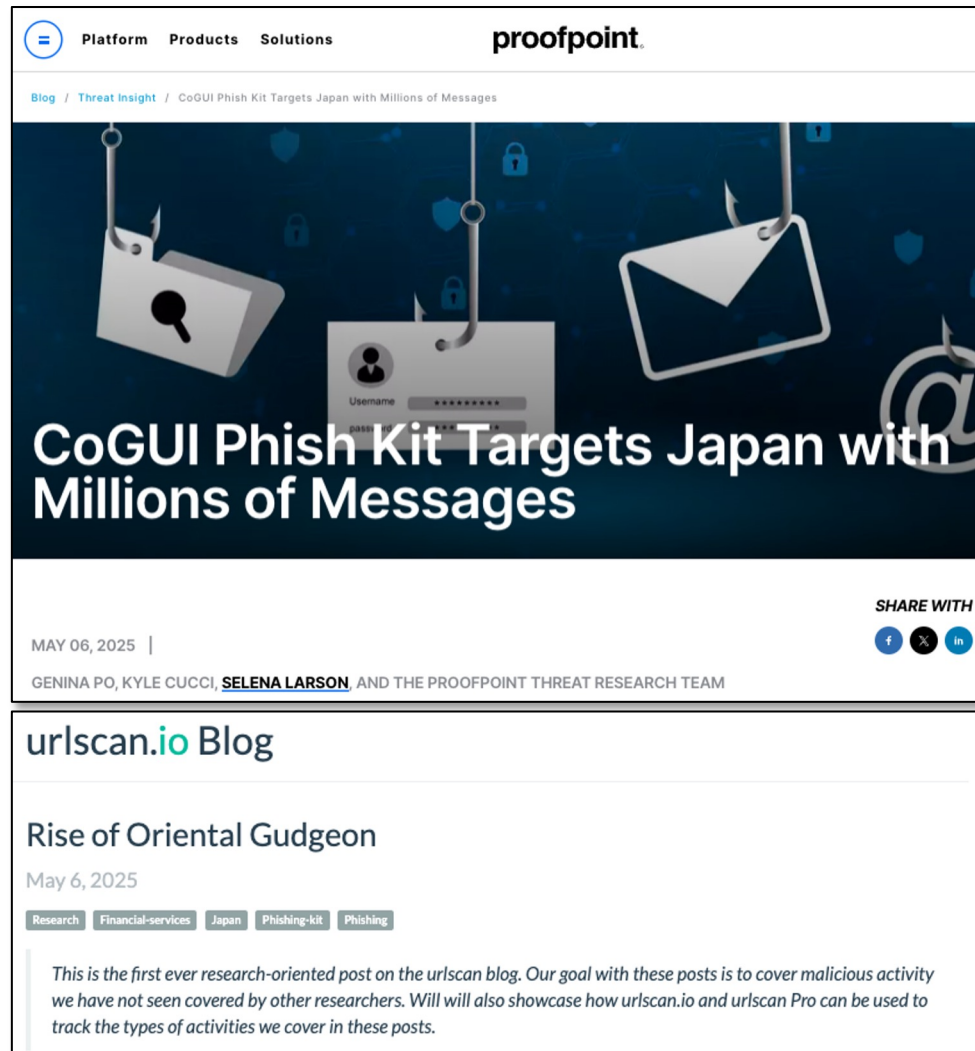
**This research is conducted in  
full compliance with the law,  
no criminal activity was  
involved.**

# 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 image shows a screenshot of a Proofpoint blog post. The top navigation bar includes 'Platform', 'Products', and 'Solutions', with the Proofpoint logo on the right. The breadcrumb trail reads 'Blog / Threat Insight / CoGUI Phish Kit Targets Japan with Millions of Messages'. The main content area features a dark blue background with illustrations of a magnifying glass, a login form with 'Username' and 'password' fields, and an envelope icon. The title 'CoGUI Phish Kit Targets Japan with Millions of Messages' is prominently displayed in white. Below the title, the date 'MAY 06, 2025' and the author 'GENINA PO, KYLE CUCCI, SELENA LARSON, AND THE PROOFPOINT THREAT RESEARCH TEAM' are listed. Social sharing icons for Facebook, Twitter, and LinkedIn are present. The bottom section of the screenshot shows the 'urlscan.io Blog' header, the article title 'Rise of Oriental Gudgeon', the date 'May 6, 2025', and a list of tags: 'Research', 'Financial-services', 'Japan', 'Phishing-kit', and 'Phishing'. A short introductory paragraph is visible at the bottom.

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

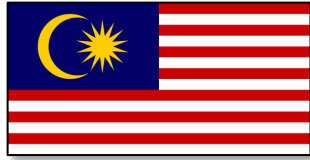
Research Financial-services Japan Phishing-kit Phishing

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.

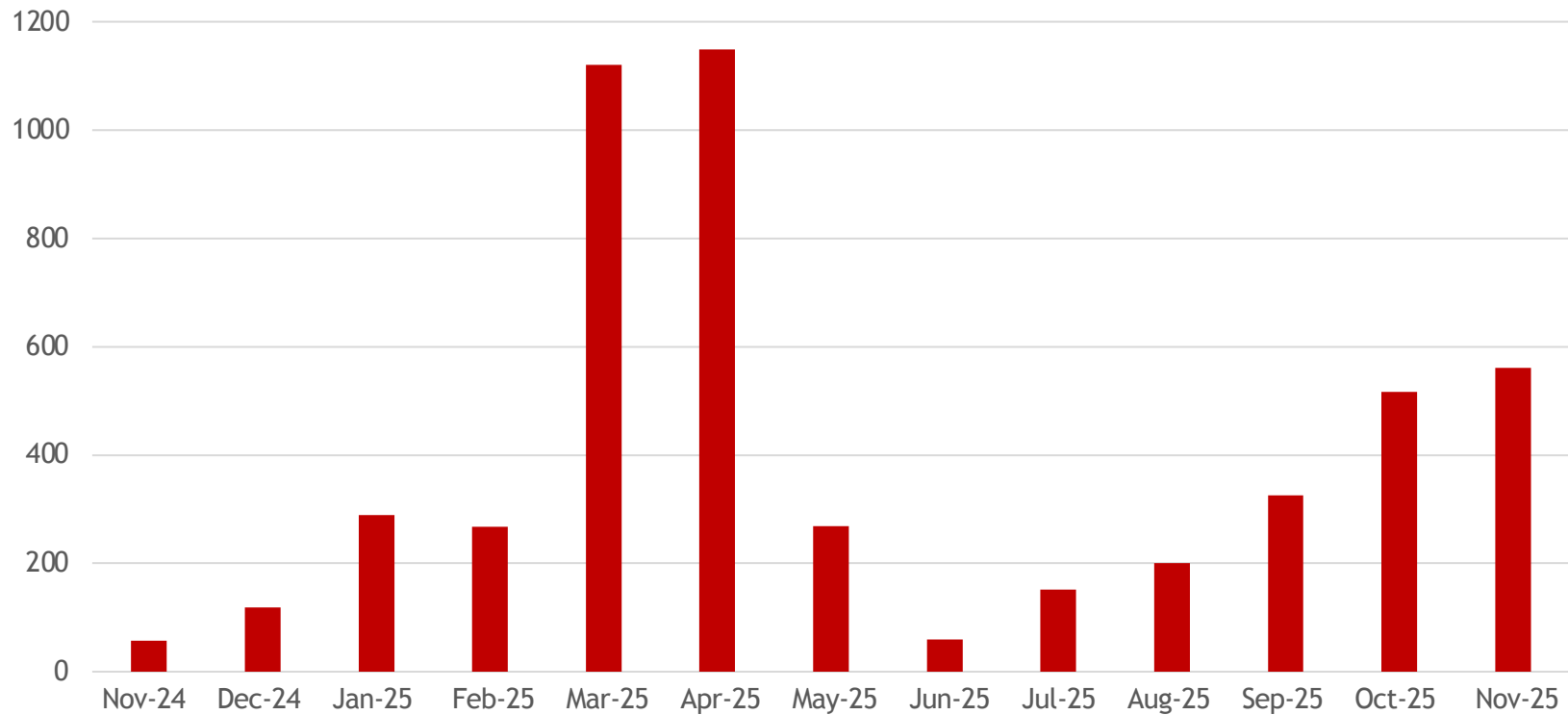
70+  
JP Brands



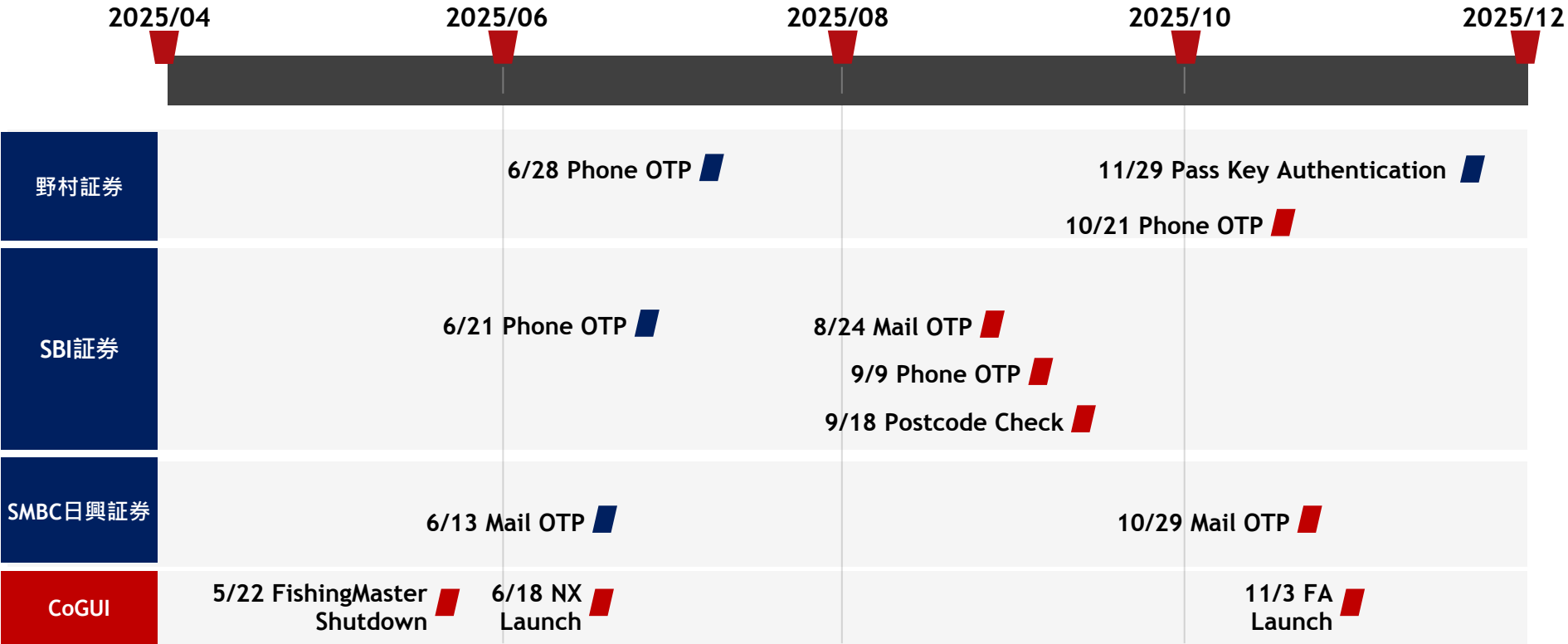
# The Global Reach of Phishing Campaigns



# 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



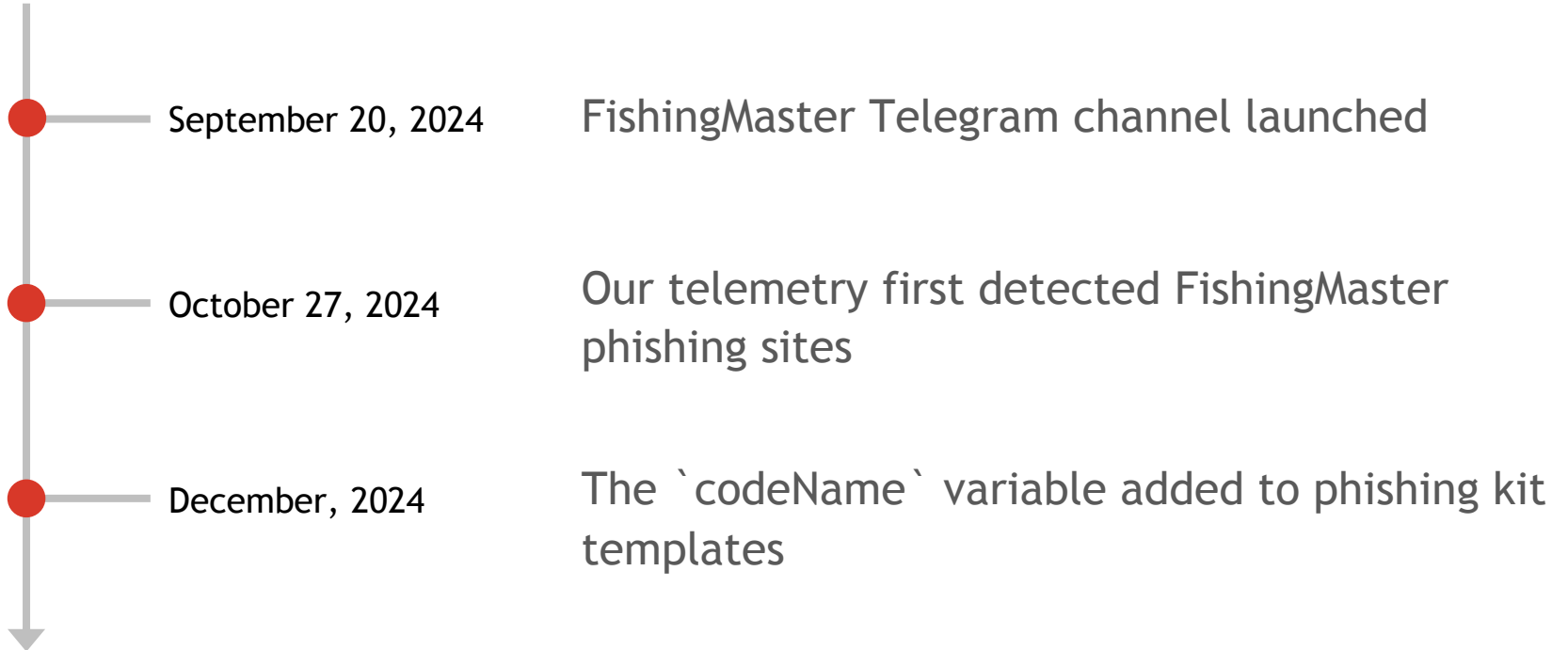
**FA**

Period: 2025-11 ~  
TG User: @redfaff

The background is black with several horizontal red light streaks of varying lengths and thicknesses, some appearing as blurred bands. Additionally, there are several diagonal red light streaks crossing the frame from the bottom-left towards the top-right.

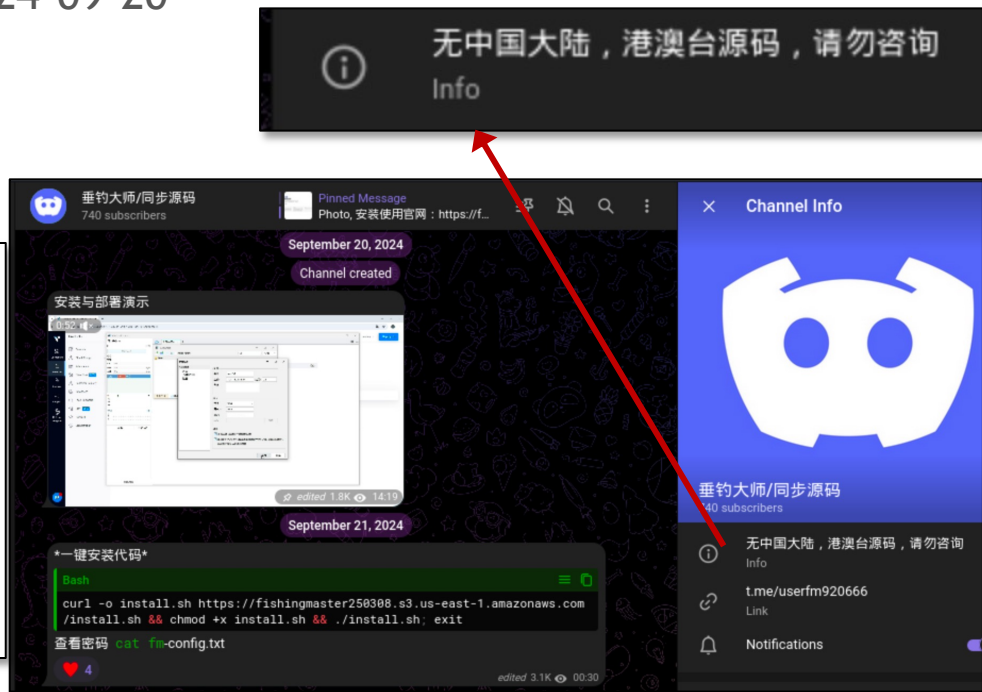
# Launch of FishingMaster PhaaS

# 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

The screenshot shows the FishingMaster website interface. At the top, there is a navigation bar with the FishingMaster logo and a menu icon. Below the navigation bar, the page title is "安装与部署" (Installation and Deployment). The main content area contains several sections:

- 安装与部署** (Installation and Deployment)
- 不想安装的 也可以联系我, 提供服务器给我 我帮忙安装** (If you don't want to install, you can also contact me, provide the server to me, I will help you install)
- 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** (Don't be fooled by the long content, installation is actually very simple, the first step is to check if the firewall is turned on, the second step is to execute the installation script. Most of the content is used to deal with installation errors)
- DANGER** section with the text: **打开防火墙 打开防火墙 打开防火墙 不开会有人偷鱼** (Turn on the firewall, turn on the firewall, turn on the firewall, if you don't, someone will steal your fish)
- TIP** section with a list of tips:
  - 有些服务器默认防火墙是关闭状态 (Some servers have the firewall turned off by default)
  - 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 (You can use the following command to check if the firewall is turned on, turning on the firewall can prevent some malicious attacks and database theft)
  - 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 (If installation fails, there are common solutions for failure below. Installation and handling of failure problems are all done in root permissions. If you use the Ubuntu account to log in, when installation fails or the server disconnects, you must use sudo su to restart root permissions)
- Text: 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 (Use the following command to check if the firewall is turned on, if the output shows the port number, it means the firewall is turned on)
- Code block: `sudo ufw status verbose` (bash)
- Text: 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 (If the firewall is turned off, you need to turn on the firewall. Use the following command to first open port 22, to prevent the server from being unable to connect after the firewall is turned on)
- Code block: `sudo ufw allow 22/tcp` (bash)
- Text: 然后使用下面命令开启防火墙(出现提示输入 y 然后回车) (Then use the following command to turn on the firewall (when prompted, enter y and then press Enter))

# FishingMaster PhaaS Admin Panel

垂钓大师

访问控制 前台在线人数: 5, 重复人数: 0, 为了保持实时数据区的清晰和流畅, 建议定期刷新清除离线数据。

垂钓大师-综合版

| 编号   | 时间   | 状态                 | 用户信息   | 操作    |
|------|------|--------------------|--|-------|
| 1043 | 几秒前  | 登录页                | 日本amazon/wegmsm.com  | 跳转 拒绝 |
| 1042 | 2分钟前 | 登录页                | 日本amazon/luminal.com                                       | 跳转 拒绝 |
| 1041 | 4分钟前 | 登录页   在登录页(1条数据) > | 日本amazon/dreamingturkey.com 用户名: nh50710@city.com          | 跳转 拒绝 |
| 1040 | 4分钟前 | 登录页                | 日本amazon/dreamingturkey.com                                | 跳转 拒绝 |
| 1039 | 5分钟前 | 登录页                | 日本amazon/doncasan.com                                      | 跳转 拒绝 |
| 1038 | 8分钟前 | 登录页   在登录页(1条数据) > | 日本amazon/wegmsm.com 用户名: nort.ij.oiazryk.m25e@docomo.ne.jp | 跳转 拒绝 |
| 1037 | 9分钟前 | 登录页                | 日本amazon/thalexpataw.com                                   | 跳转 拒绝 |

当前在线  
后台在线人数: 1  
全部在线人数: 1

未授权

访问控制 前台在线人数: 24, 重复人数: 5, 为了保持实时数据区的清晰和流畅, 建议定期刷新清除离线数据。

访问控制

|        |      |  |  |
|--------|------|--|--|
| 编号: 39 | 2分钟前 | 已提交卡片, 待处理   在登录页(2条数据) > 在填卡页(3条数据) >       | 日本ana航空/ana-points.com 用户名: 3 4 密码: r 3 4980                         |
| 编号: 38 | 2分钟前 | 填卡页面   在登录页(2条数据) > 在填卡页(3条数据) >             | 日本ana航空/ana-points.com 用户名: 444444444444 密码: sxxxxd 1223 6666 6666 6 |
| 编号: 31 | 2分钟前 | 填卡页面   在登录页(2条数据) > 在填卡页(2条数据) >             | 日本ana航空/ana-points.com 用户名: 4 5 密码: c lh 4897                        |
| 编号: 26 | 3分钟前 | 验证码验证页面   在登录页(2条数据) > 在填卡页(3条数据) >          | 日本ana航空/ana-points.com 用户名: 4 2 密码: A o 3528                         |
| 编号: 23 | 3分钟前 | 填卡页面   在登录页(2条数据) > 在填卡页(2条数据) >             | 日本ana航空/ana-points.com 用户名: 3 5 密码: t 6 35                           |
| 编号: 7  | 6分钟前 | 验证码验证页面   在登录页(2条数据) > 在填卡页(3条数据) >          | 日本ana航空/ana-points.com 用户名: 3 1 密码: k r 498                          |
| 编号: 6  | 6分钟前 | 验证码验证页面, 点击了重新发送   在登录页(2条数据) > 在填卡页(3条数据) > | 日本ana航空/ana-points.com 用户名: : )3 密码: 5 an 498                        |

# 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, [

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, [

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

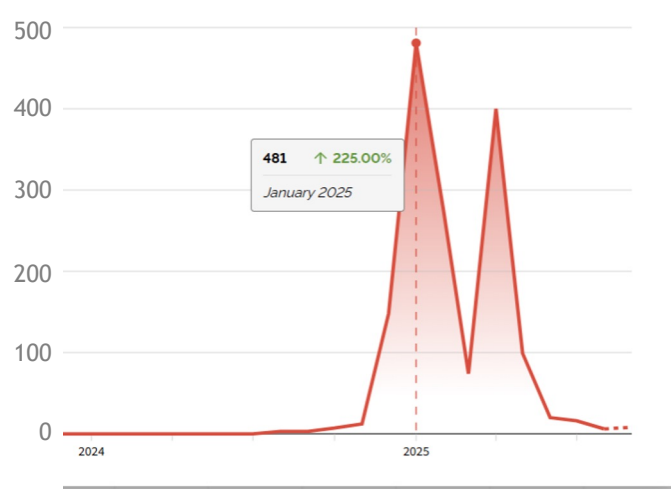
垂釣大師【全球同步源碼】 · Author ID: 2261057438  
Posted on September 22, 2024 at 03:24:04 UTC

在20世紀的漩渦中，中國經歷了許多磨難，其中深刻的一課來自於抗日戰爭時期的苦難。那時，中國還是一個武器技術落後、經濟基礎薄弱的國家，面對外來侵略，民眾用盡自己所能，進行了艱苦卓絕的抵抗。時光流轉，今日的中國已然不同，科技進步，武器現代化，國力顯著增強。然而，與過去的硝煙不同，吾輩生於這個和平年代，並不能直接拿起槍桿子向先輩一樣去乾他們，但是我們可以使用🔥“垂釣大師同步源碼(40多套日本源碼)”🔥來發起新形式的“戰爭”讓那些曾經犯下罪行的日寇後代明白：復仇之火已點燃，誰也無法逃避罪行。

- **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"

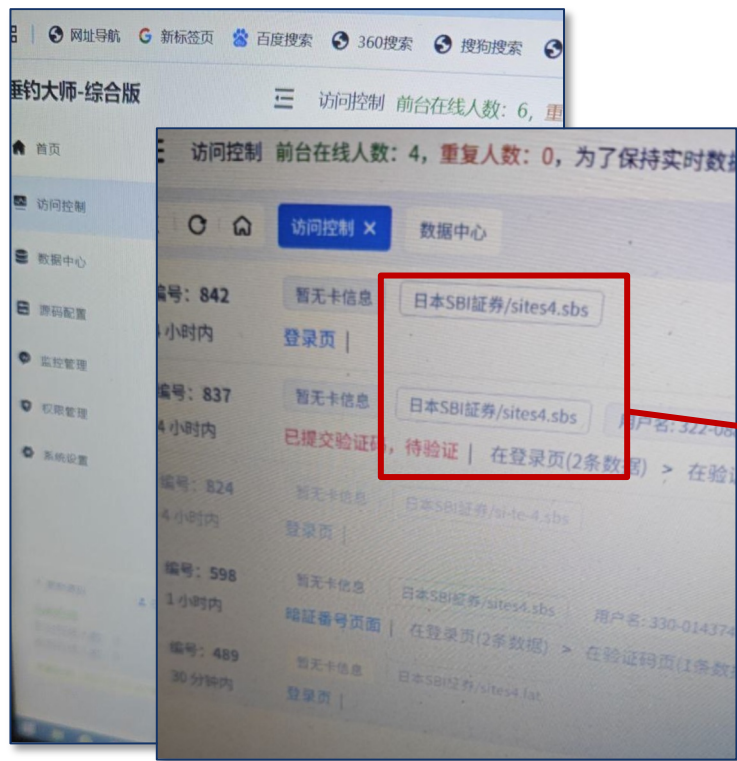
# Widely-Used PhaaS in Japanese Phishing Campaigns

- 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

The screenshot shows a URLScan report for the domain `sites4.sbs`. The report indicates a **Malicious Activity!** with a **Public Scan** badge. The URL being scanned is `https://sites4.sbs/co.jp/ETGate/`. Below the report, there is a table of API requests and a screenshot of the phishing website.

| Method | Protocol | Status | Resource  |
|--------|----------|--------|---|
| POST   | H/1.1    | 200 OK | <code>createOrGetUserInfo</code><br><code>sites4.sbs/open/visitors/info/</code> |
| GET    | H/1.1    | 200 OK | <code>getState</code><br><code>sites4.sbs/open/visitors/info/</code>            |

The screenshot of the phishing website shows a login page with the title 'SBI証券 メインサイト' and a 'ログイン' (Login) button. There is a text input field for 'ユーザーネーム' (Username).

# 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

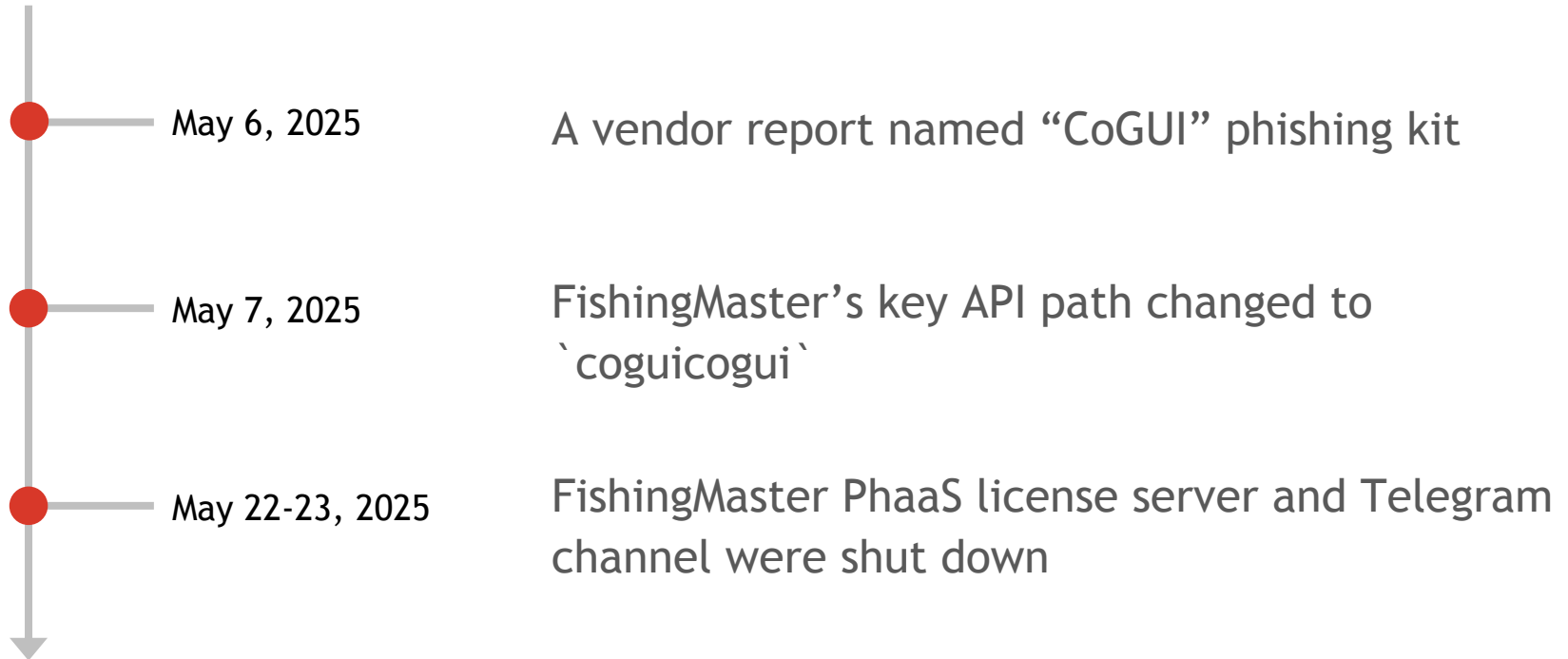
```
if (!t.isConnected()) t.connect().then(() => {
  const s = As(Is);
  s.provide("socketClient", t), s.use(ks()), s.mount("#app")
}).catch(s => {
  console.error("WebSocket连接失败", s)
});
else {
  const s = As(Is);
  s.provide("socketClient", t), s.use(ks()), s.mount("#app")
}
} else {
  const t = await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

- *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

```
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"
```

# 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()
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

- **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:

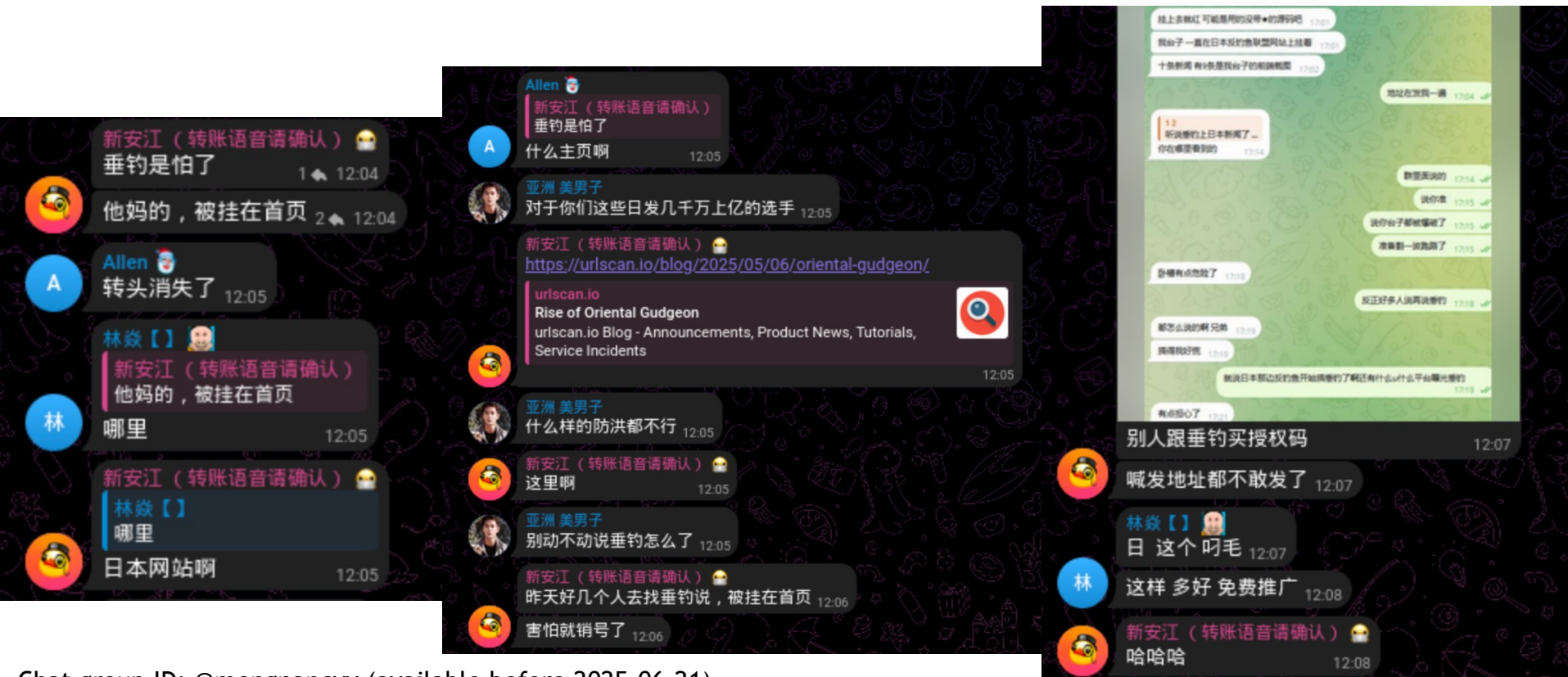
1. Introduced evasion techniques such as obfuscation, fingerprinting modules (**validateHuman**), and Selenium detection
2. Modularized JavaScript files with different imported functions
3. Used meaningless strings as API path

# 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



# Underground Discussions Regarding the FishingMaster Shutdown



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

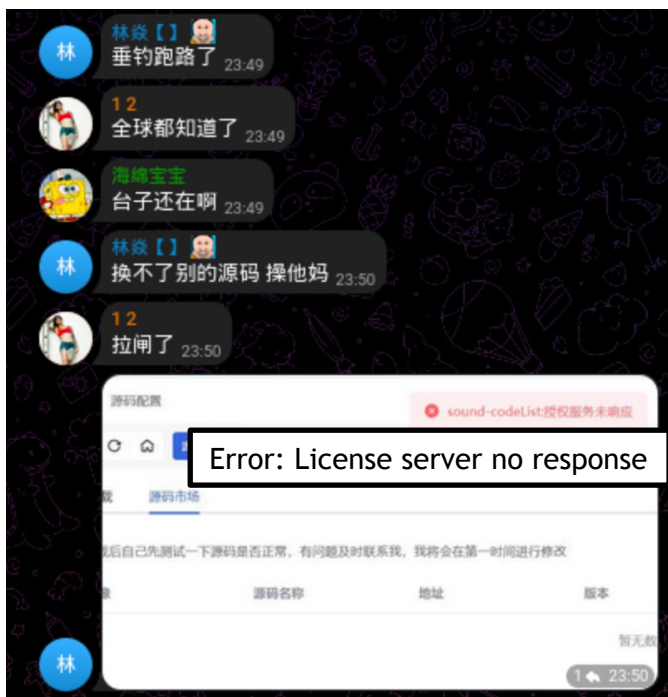
FishingMaster

NX

FA

# 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

The screenshot displays the '垂钓大师-综合版' (FishingMaster - Comprehensive Edition) dashboard. The interface includes a navigation menu on the left with options like '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), '权限管理' (Permissions Management), and '系统设置' (System Settings). A central panel shows '当前在线' (Currently Online) statistics: '后台在线人数: 2' (Backend online users: 2) and '全部在线人数: 2' (Total online users: 2). A red box highlights the '到期时间: 2038-01-19 03:14:07' (Expiration time: 2038-01-19 03:14:07) and '剩余下载次数: 9999' (Remaining download count: 9999) fields. A black box below the screenshot repeats this information in English: 'Expiry date: 2038-01-19' and 'Remaining downloads: 9999'. The top right corner shows the user role '管理员' (Administrator) and a profile icon.

# 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

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

序号 主机名/rid

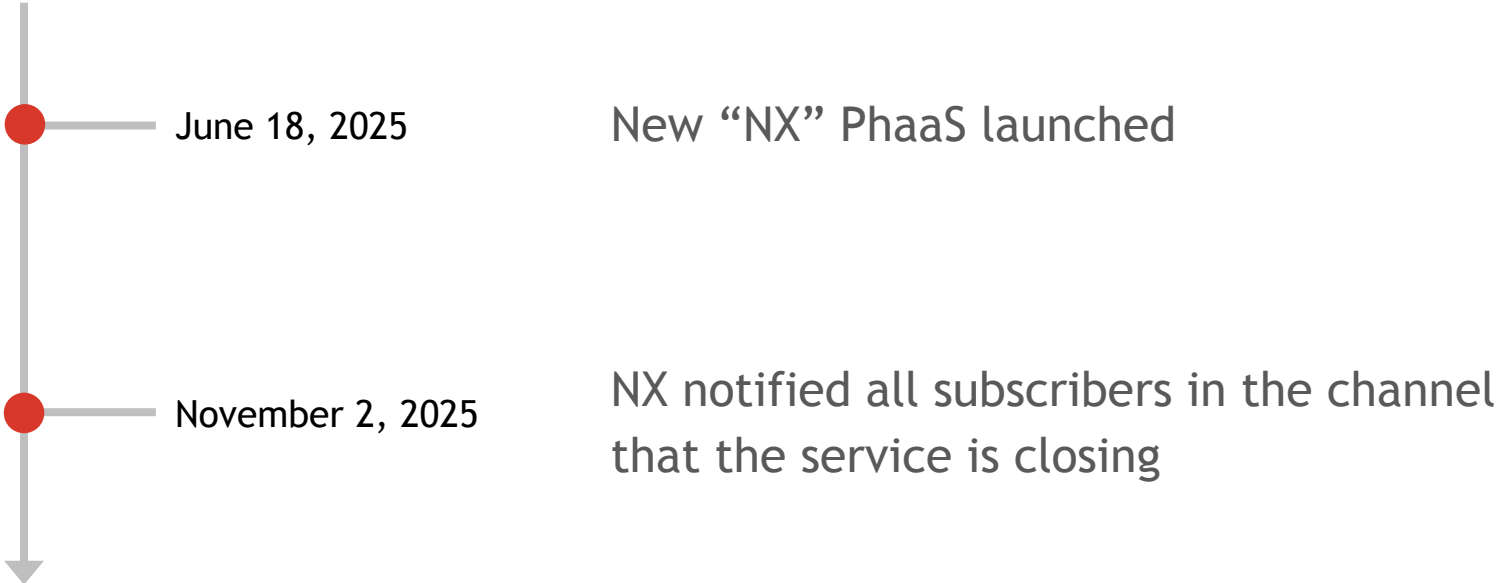
|            |   |
|------------|---|
| >> 中国香港... | 1   |
| >> 日本      | 1   |
| >> 马来西亚    | 1   |
| >> 美国      | 1   |
| 1          | ▶ 156.245.235.246:8001 HAp... <sup>999%</sup> |
| 2          | ▶ 107.172.83.114:8888 HAp... <sup>999%</sup>  |
| 3          | ▶ 103.20.241.238:8001 HAp... <sup>999%</sup>  |
| 4          | ▶ 207.56.13.194:8001 HAp... <sup>999%</sup>   |

共 4 条

10条/页

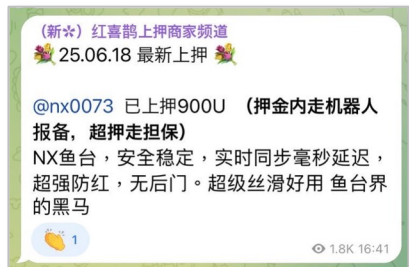
**Rebrand to NX PhaaS**

# Rebrand - Launch of NX PhaaS

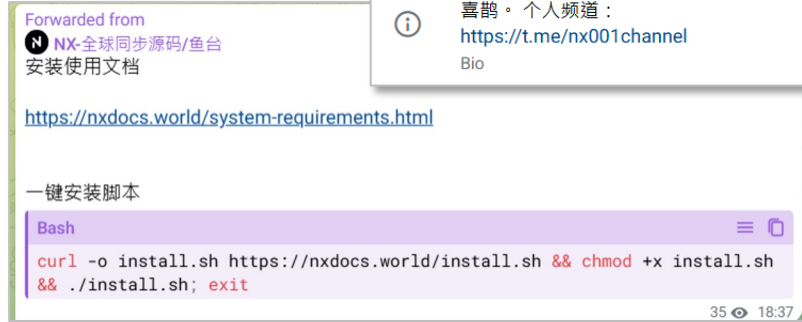


# 1<sup>st</sup> Reincarnation - Rebranded as NX PhaaS

- 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

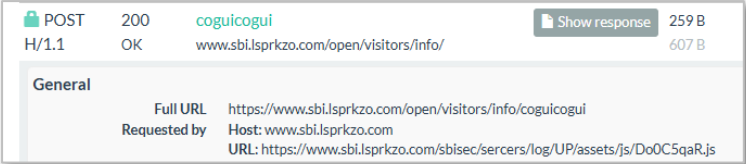
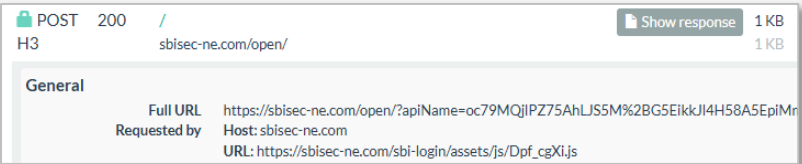

The screenshot displays the NX PhaaS Admin Panel interface. The top navigation bar includes a hamburger menu, a toggle switch, and the user role '管理员' (Administrator). The main dashboard features a '数据中心' (Data Center) section with a line chart showing '总访问量' (Total Visits) at 29072 and '日访问量' (Daily Visits) at 1840. A '重置' (Reset) button is located below the chart. To the right, summary statistics show '总上鱼量' (Total Fish Caught) at 2820, '每次提交卡片都算一次上鱼(主卡+填卡历史)' (Each card submission counts as one fish caught (main card + card history)), '总转化率' (Total Conversion Rate) at 9.70%, and '日上鱼量' (Daily Fish Caught) at 281.

The main content area displays a list of transactions with the following details:

- Transaction 1:** DEBIT CLASSIC SUMITOMO MITSUI CARD COMPANY, LTD. 日本亚马逊amazon无限单重构2/st-casting.com 用户名: 09027457898. 验证码验证页面 | 在填卡页(4条数据) > 填卡历史(1条数据) >. Buttons: 跳转, 拒绝.
- Transaction 2:** CREDIT WORLD SUMITOMO MITSUI CARD COMPANY, LTD. 日本亚马逊amazon无限单重构2/st-casting.com. 验证码验证页面 | 在填卡页(4条数据) > 在验证码页(1条数据) >. Buttons: 跳转, 拒绝.
- Transaction 3:** DEBIT OTHER 日本亚马逊amazon无限单重构2/st-casting.com 用户名: 07040682385 密码: yuino2109 SAYURI SUZUKI. 验证码: 64477832. 已提交验证码, 待验证 | 在填卡页(4条数据) > 在验证码页(1条数据) >. Buttons: 跳转, 拒绝.
- Transaction 4:** CREDIT GOLD VJA 日本亚马逊amazon无限单重构2/st-casting.com 用户名: supikapika616@icloud.com 密码: supika616. 验证码: 67733124. 已提交验证码, 待验证 | 在填卡页(4条数据) > 在验证码页(1条数据) >. Buttons: 跳转, 拒绝.
- Transaction 5:** CREDIT CLASSIC CREDIT SAISON CO., LTD. 日本亚马逊amazon无限单重构2/st-casting.com 用户名: 08048727022. 验证码: 645376. 验证码验证页面 | 在填卡页(4条数据) > 在验证码页(1条数据) >. Buttons: 跳转, 拒绝.
- Transaction 6:** 日本亚马逊amazon无限单重构2/st-casting.com 用户名: maoyu7ma2yufuchi@icloud.com 密码: posse0726 MAYUKO KIBA. 验证码: 078309. 验证码验证页面 | 在填卡页(4条数据) > 在验证码页(1条数据) >. Buttons: 跳转, 拒绝.
- Transaction 7:** 日本亚马逊amazon无限单重构2/st-casting.com 用户名: 09019501389 密码: YuutaYuuta0929 KOBAYAKAWA YUTA. 验证码: 831582. 验证码验证页面 | 在填卡页(4条数据) > 在验证码页(1条数据) >. Buttons: 跳转, 拒绝.

The bottom of the interface shows a Windows taskbar with the date 2025/8/15, time 18:00, and system tray icons. The system tray also displays '英', 'Wi-Fi', and '2025/10/22'.

# Key Changes in NX PhaaS

|                               | FishingMaster  | NX  |
|-------------------------------|--|---|
| Masked Codename               | <pre>const v859 = await v827.post("/visitors/info/cogucogui", {   currentstate: 2,   browserinfo: f299(),   domain: window.location.hostname,   codename: "日本sbi証券(増加情報)", });</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: v899,
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: v8147,
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,
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);
```

Internally still refers the same APIs

```
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 vLSvisitorsinfosBlackl = "/visitors/info/isBlacklist";
14575+       if (Math.random() < 0.5) {
14576+         await f368(100, 320);
14577+         await v1500.post(vLSvisitorsinfosBlackl;
```

# 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__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",  
    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  
H3 554 B 79ms application/json CLOUDFLARENET

General

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

Requested by Host: sbisec-ne.com

URL: `https://sbisec-ne.com/sbi-login/assets/js/Dpf_cgXi.js`

Protocol H3

Security QUIC, , AES\_128\_GCM

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

Reverse DNS

Software cloudflare /

Resource Hash 8bc55f760a8ad956e66394c3a32b26711b660c74d20d358b35ec1e3b2ba2c728

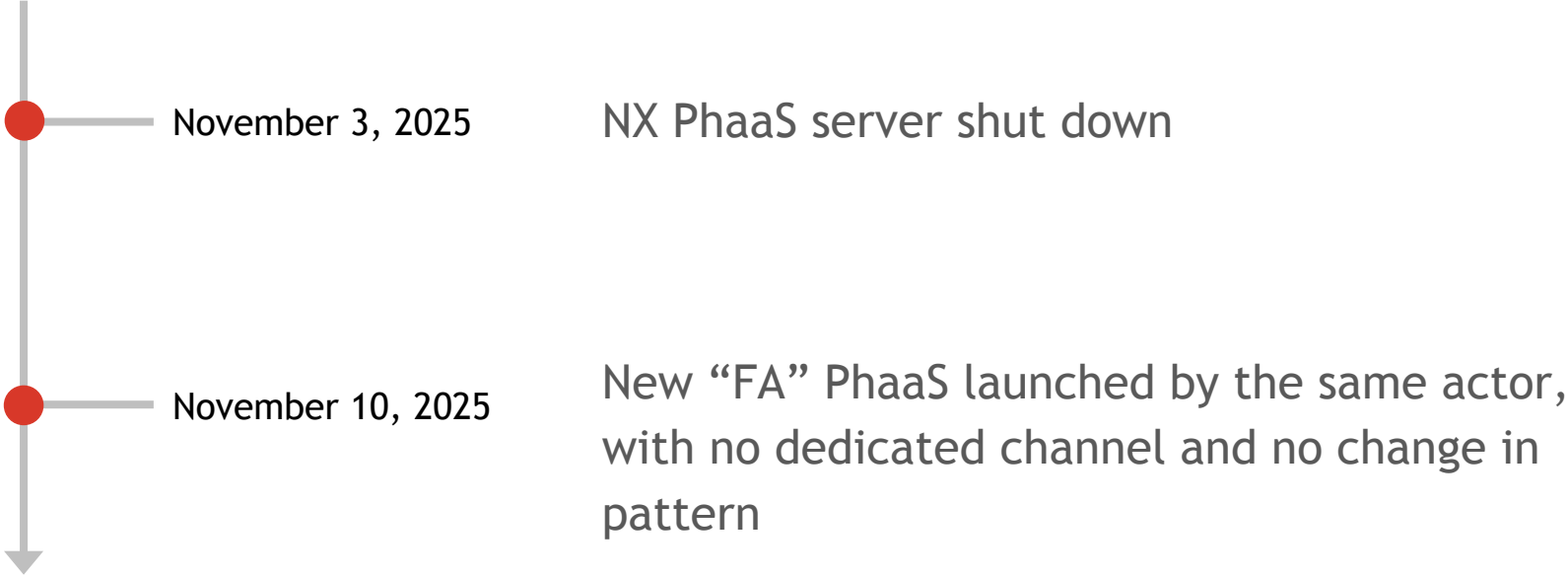
Decrypted: **/visitors/info/validateHuman**

# Novel Types of Phishing



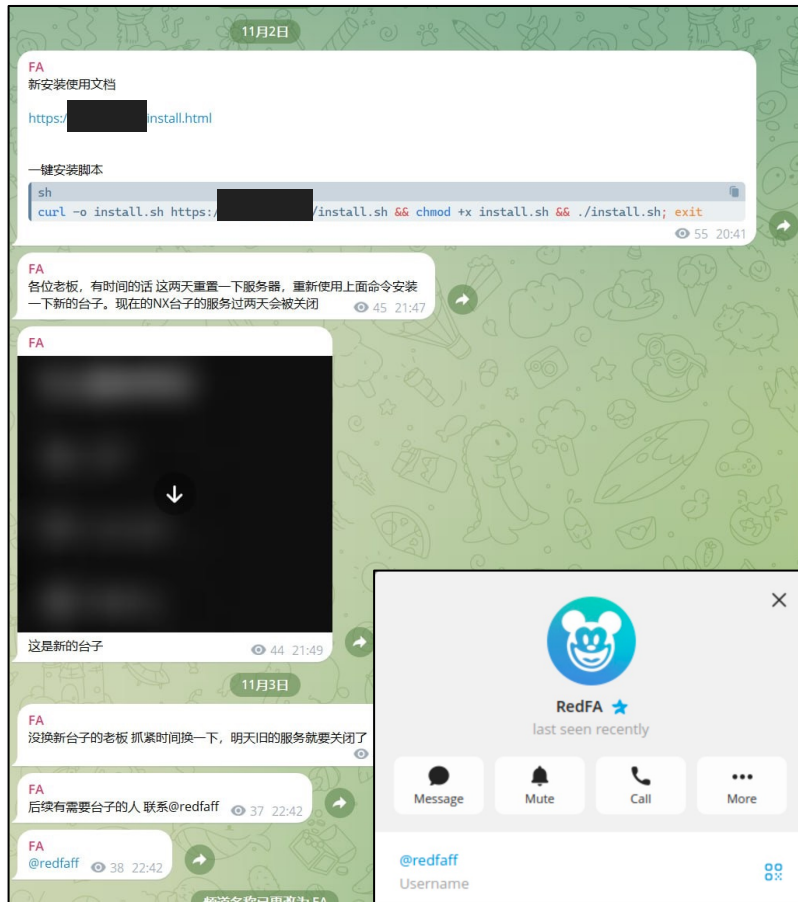
# Latest Migration to FA PhaaS

# 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>



# FA PhaaS Admin Panel

**FA-源码平台**

总访问量: **68768**

总上量: **11400**

每次提交卡都算一次上量

总转化率: **16.56%**

转化率: **14.31%**

日访问量: 3018

日上量: 432

访问控制

数据中心

访问控制

数据中心

源码配置

监控管理

权限管理

系统设置

在线管理

当前在线: 7  
后台在线人数: 7  
全部在线人数: 10

到期时间: 2025-12-12 07:13:28

剩余下载次数: 10

当前版本: v0.0.4

fa 访问控制-FA-源码平台

fa 访问控制-FA-源码平台

不安全

FA-源码平台

访问控制 前台在线人数: 9, 重

访问控制

编号: 215

暂无卡信息

几秒前

登录页 |

访问控制 前台在线人数: 11, 重

访问控制

数据中心

源码配置

监控管理

访问日志

操作日志

黑白名单

权限管理

用户列表

角色列表

系统设置

更新源码

在线管理

当前在线: 3  
后台在线人数: 3  
全部在线人数: 14

|          |             |        |      |                 |
|----------|-------------|--------|------|-----------------|
| 编号: 1402 | 暂无卡信息       | apple无 | 1小时前 | 登录页   在登录页(2条)  |
| 编号: 1399 | 暂无卡信息       | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 1397 | 暂无卡信息       | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 1396 | 暂无卡信息       | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 1395 | 暂无卡信息       | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 1394 | 暂无卡信息       | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 1393 | 暂无卡信息       | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 1392 | 暂无卡信息       | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 1391 | apple无账单/cz | apple无 | 1小时前 | 填卡页面   在登录页(2条) |
| 编号: 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



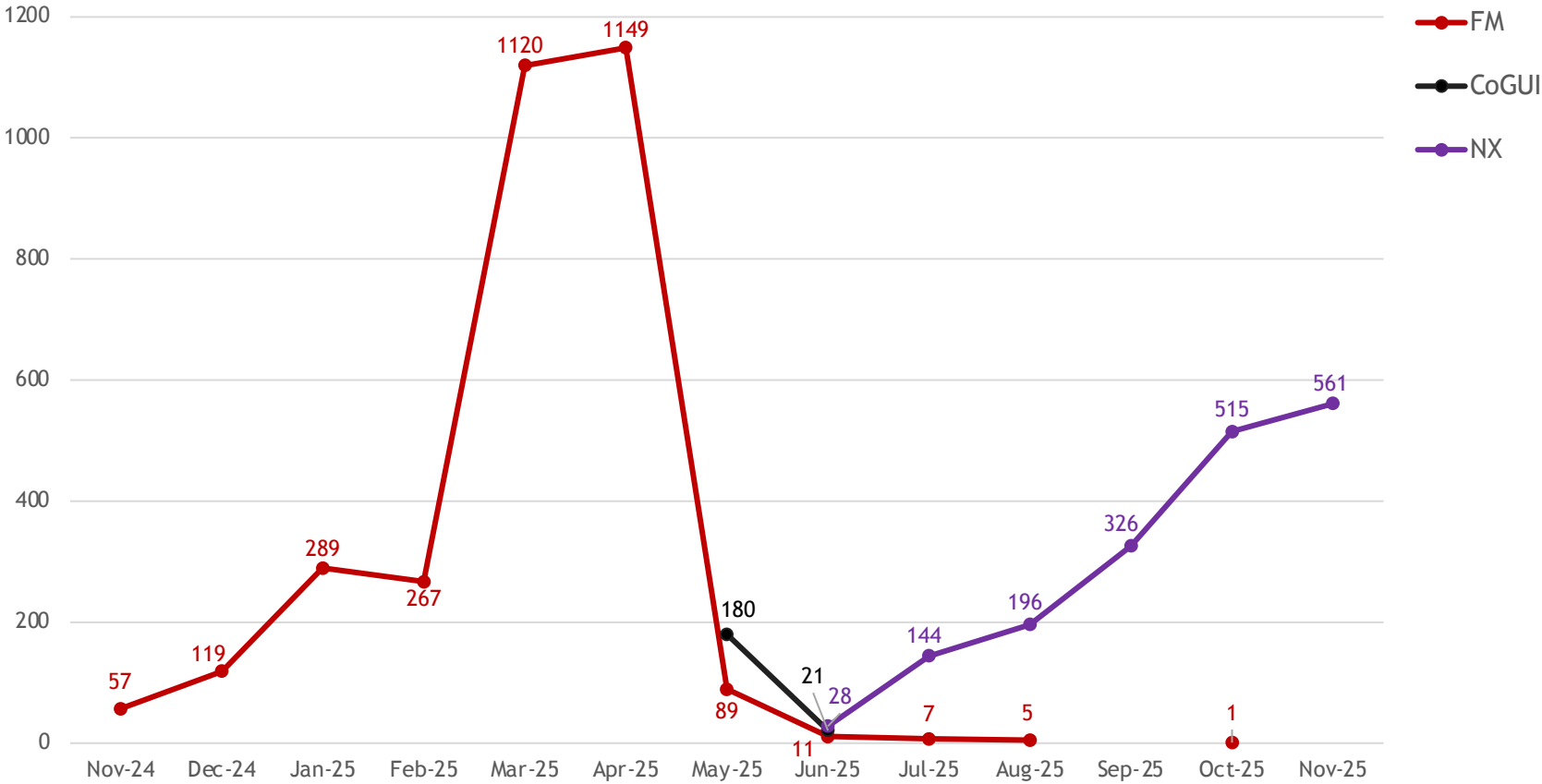
Deleted

Japan-Targeted

Others Countries



# 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

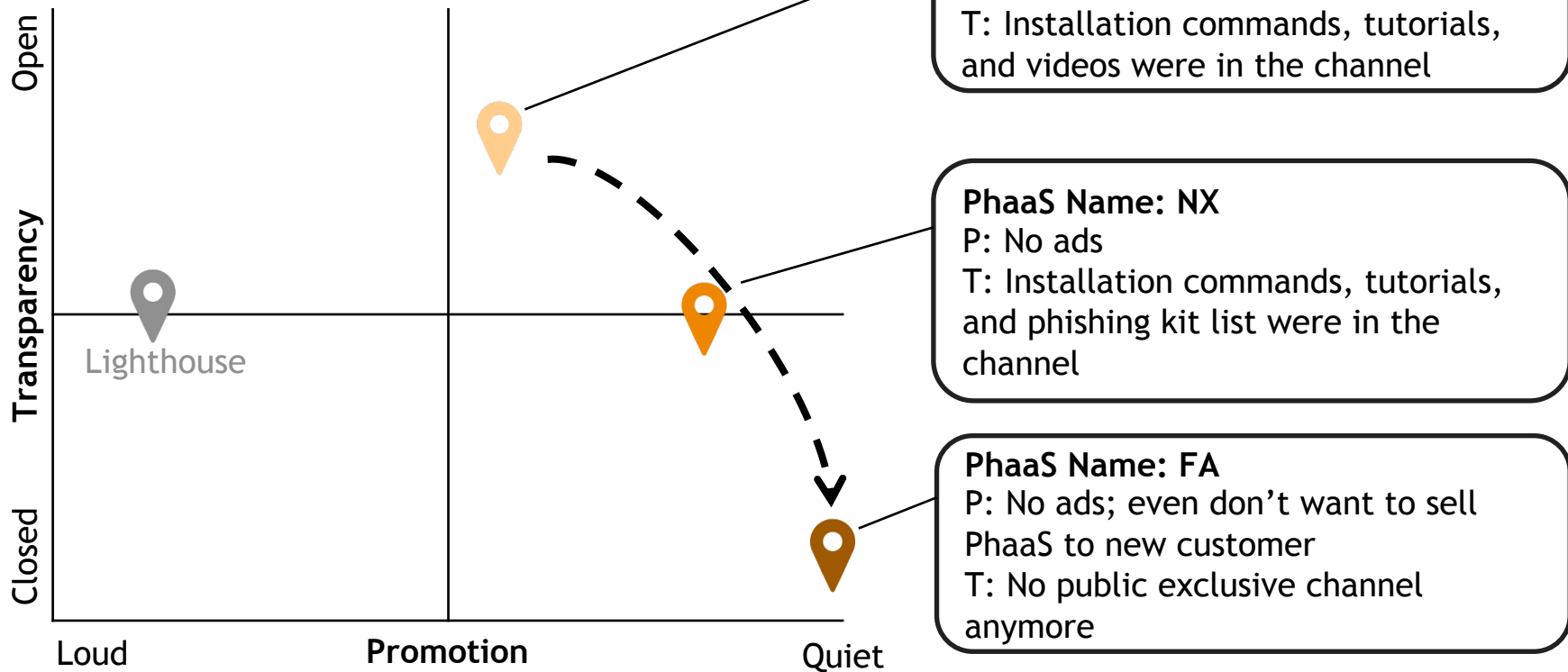
Transparency

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

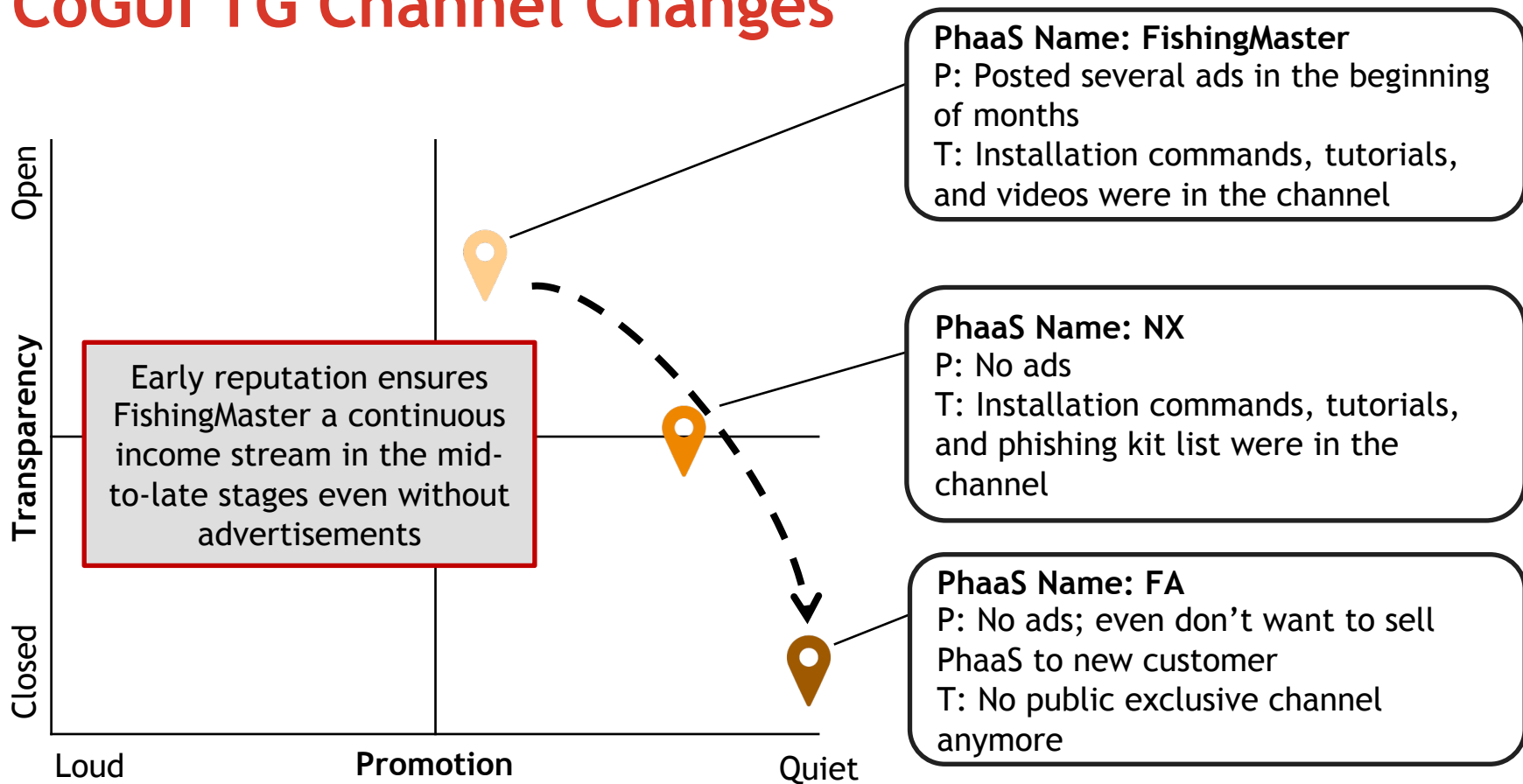


**PhaaS Name: FishingMaster**  
P: Posted several ads in the beginning of months  
T: Installation commands, tutorials, and videos were in the channel

**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



The background features a black field with several horizontal red lines of varying thickness and length, some appearing as blurred streaks. Additionally, there are several diagonal red lines crossing the frame from the bottom-left towards the top-right.

# 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：██████████

金额：20.98 美元

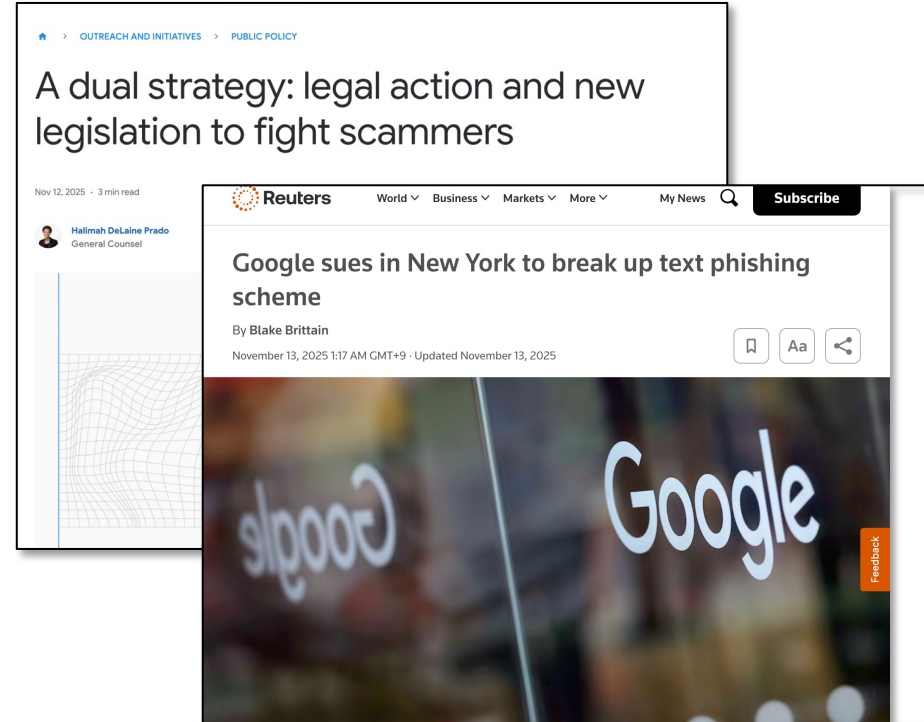
截止日期：2028 年 11 月 26 日

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



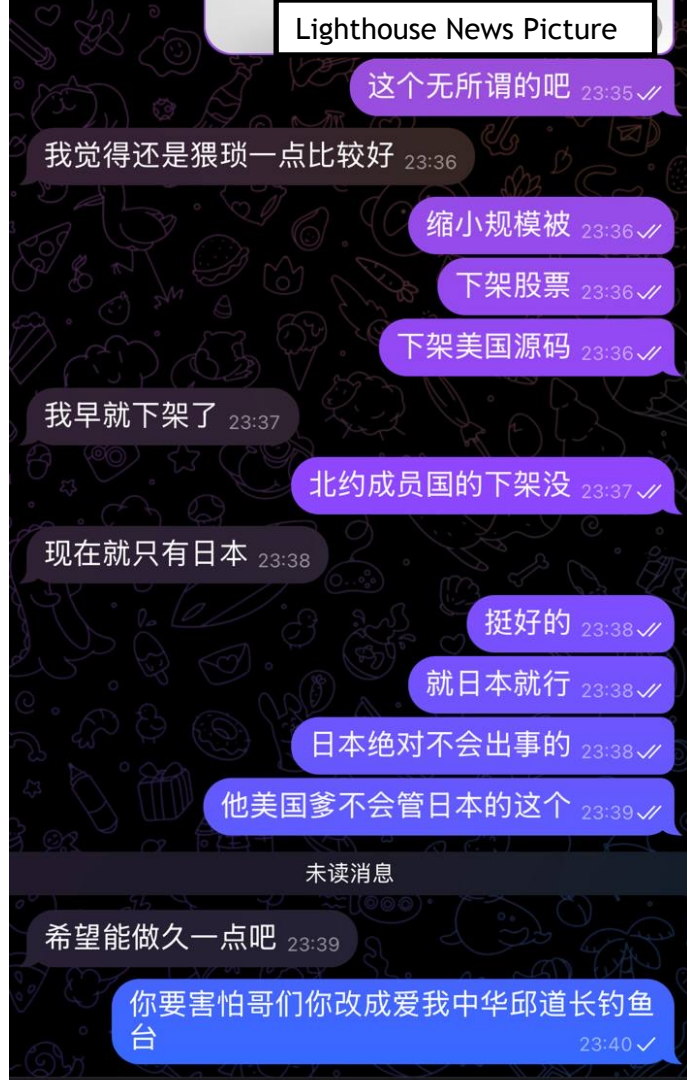
# Reaction: Disruption to Lighthouse PhaaS

- 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



# 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

# 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

# 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"}`

**Thank you!**

# Appendix: Targeted Brands and Services in Japan

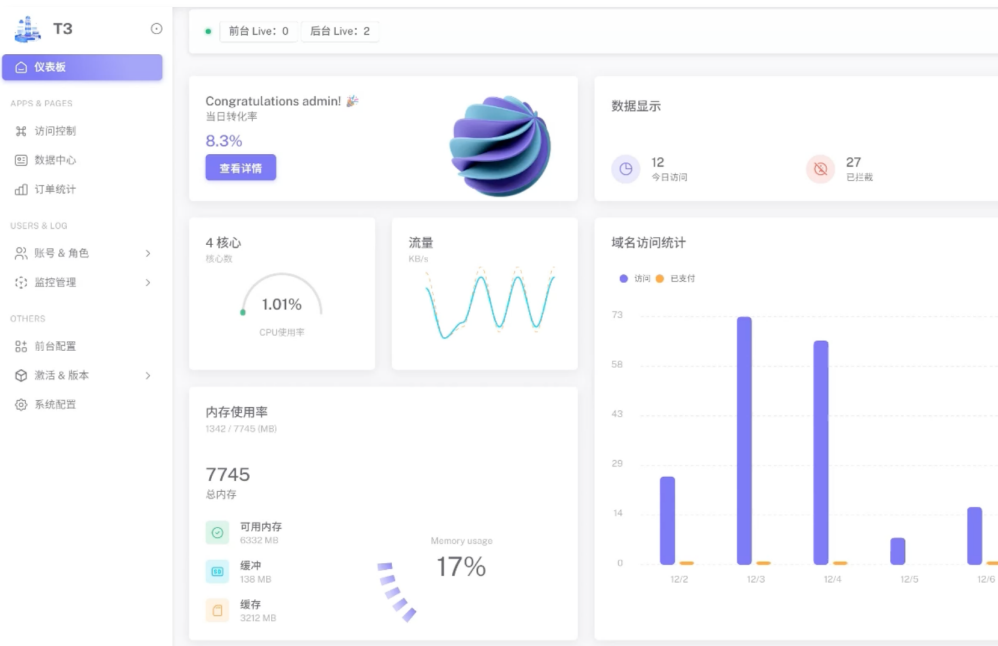
- American Express
- JCB
- Mastercard Japan
- VISA Japan
- Epos Card (エポスカード)
- JACCS (ジャックス)
- Life Card (ライフカード)
- Mitsubishi UFJ NICOS (三菱UFJニコス)
- Nanto VISA Card (南都VISAカード)
- Nissenren Millennia Card (ニッセンレンミレニアムカード)
- Orico Card (オリコカード)
- Pocket Card (ポケットカード)
- Rakuten Card (楽天カード)
- Saison 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 (野村証券)
- 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)

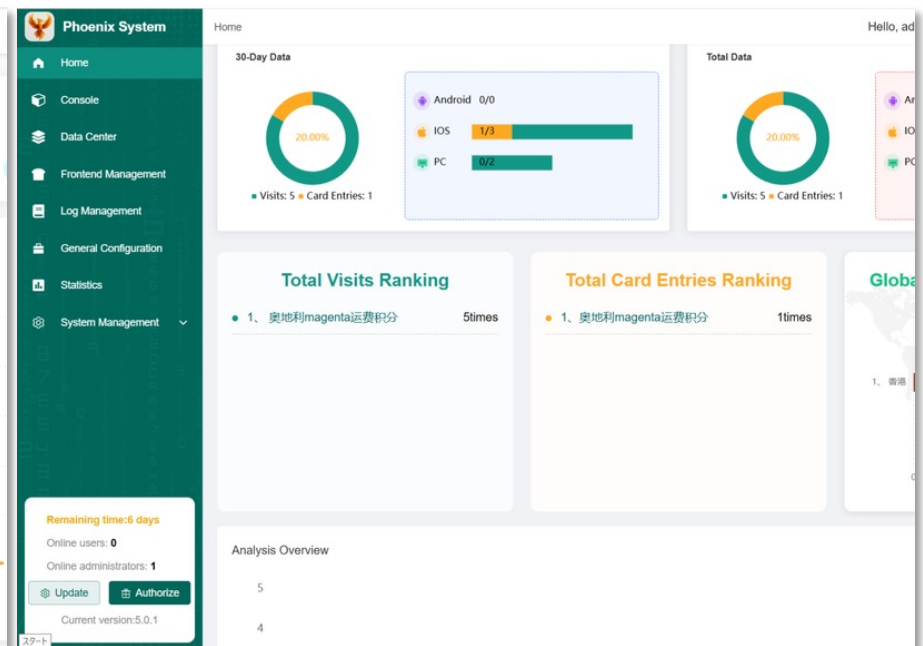
- LG U+ (South Korea)
- Korea Telecom (KT) (South Korea)
- Globe Rewards (Philippines)
- Smart Rewards (Philippines)
- GCash (Philippines)
- SM Markets (Philippines)
- GoTyme Bank (Philippines)
- Bank Central Asia (BCA) Rewards (Indonesia)
- Visa Indonesia (Indonesia)
- Bank Negara Indonesia (BNI) Rewards (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



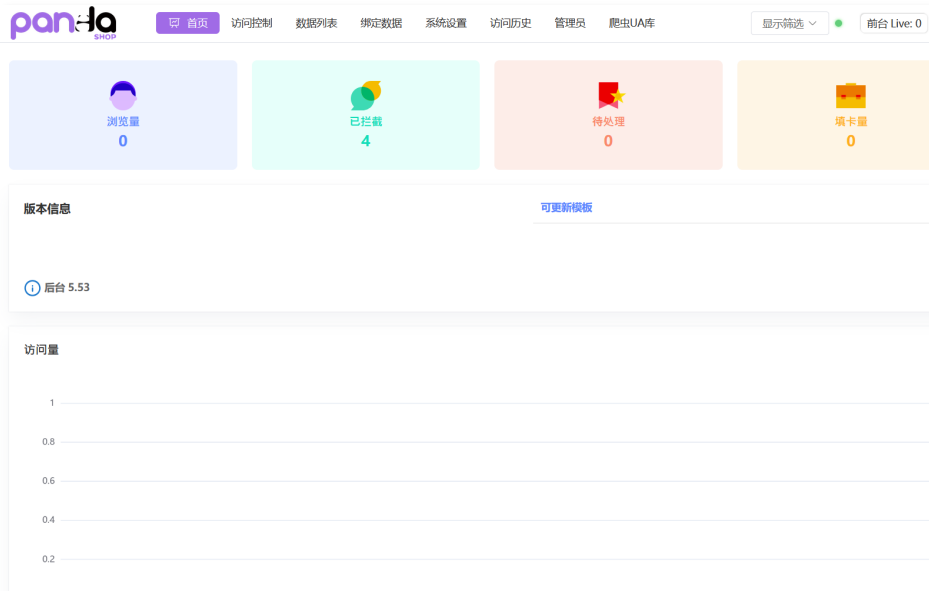
## YYLU PhaaS

The screenshot shows the YYLU PhaaS interface. On the left is a sidebar with a logo and several management options: '管理在线人数: 1', '前台在线人数: 1', '正在填卡页人数: 0', '正在填卡页人数: 1', '隐藏所有离线', '保留离线有卡', '隐藏在线无卡', '卡片信息', '数据查询', '前台管理', '前台安装', '用户设置', and '设置'. On the right is a table of users with the following 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 table contains 15 rows of user data.

| id   | 在线状态 | 姓名              | 手机号                | 地址                                  | 邮编          | 卡号                  |
|------|------|-----------------|--------------------|-------------------------------------|-------------|---------------------|
| 3239 | 离线   | fjzejw fjdjjs   | 8668656            | cjjdjdj                             | djjdkt      | 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   | 鹿峰城             |                    |                                     |             | 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   | ejej djje       | 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

