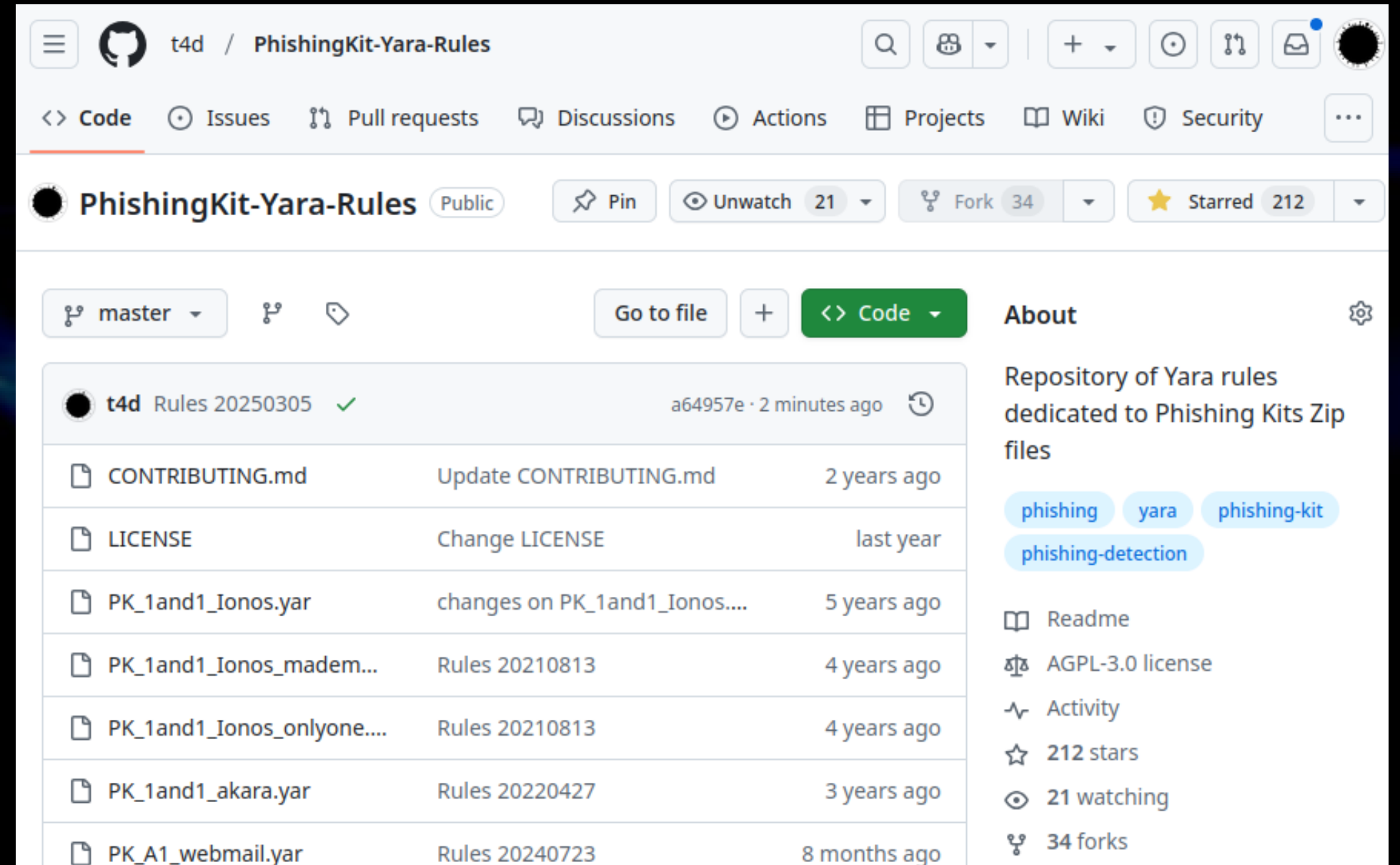


# PhishingKit-Yara-Rules

Project start: 2019

Purpose: Dedicated Yara rules for triage, hunt of phishing kits ZIP files

834 Yara rules



# Phishing site

Particuliers | Authentication x +

https:// /impot/app/

 **impots.gouv.fr**  
un site de la direction générale des Finances publiques

Formulaire de remboursement électronique - N 0551584

### Données personnelles

Nom complet

Prénom  Nom d'usage

Date de naissance

01  01  1930

Informations supplémentaires

Ville  Code postal

Adresse  Portable

### Mes coordonnées bancaire

Informations supplémentaires

Nom sur la carte

Carte de crédit

EXP (MM/YY)  CCV

Montant de votre remboursement: 420,00EUR

## Actors

```
{
  "bot_info": {
    "first_name": "Sgsanssms_Bot",
    "username": "Sgdelagloiresanssms_Bot",
    "id": 7271659943
  },
  "chat_info": {
    "title": "Billiard Résultats Impot",
    "type": "supergroup",
    "invite_link": "https://t.me/"
  },
  "admins_info": [
    {
      "id": 7271659943,
      "is_bot": true,
      "first_name": "Sgsanssms_Bot",
      "last_name": null,
      "language_code": null,
      "username": "Sgdelagloiresanssms_Bot"
    },
    {
      "id": 6504711855,
      "is_bot": false,
      "first_name": "Billiard",
      "last_name": null,
      "language_code": "fr",
      "username": "billiadaire777"
    }
  ]
}
```

## Phishing kit sources

| ▼ impot.zip |  |           |          |
|-------------|--|-----------|----------|
| ▼ impot     |  |           |          |
| ▼ app       |  |           |          |
| css         |  | Nom       | Taille   |
| images      |  | css       | 3,1 Ko   |
| js          |  | images    | 139,6 Ko |
| pages       |  | js        | 19,2 Ko  |
| templates   |  | pages     | 38,1 Ko  |
| server      |  | templates | 1,8 Mo   |
|             |  | index.php | 2,7 Ko   |
|             |  | main.js   | 7,0 Ko   |
|             |  | main.php  | 4,5 Ko   |

## Exfiltration configuration

```
# API CONFIG
$bincode = "";

# REZ CONFIG
$mail = "infosresultat@gmail.com";
$token = "7271659943:AAEKiFm3G2X-z-obEp9QX-0Q41HJ5e5Km_g";
$chatid = "-1002191395823";
$spammer = "Exodia";

# SCAMA
$login = "yes";
$applepay = "yes";
```

# PhishingKit-Yara-Rules

Check for specific  
files/directories names  
appearing into ZIP file

No need to unzip it

Short phishing kit description  
(impersonated brand)

```
rule PK_Binance_nuxt : Binance
{
    meta:
        description = "Phishing Kit impersonating Binance"
        licence = "AGPL-3.0"
        author = "Thomas 'tAd' Damonville"
        reference = ""
        date = "2025-01-31"
        comment = "Phishing Kit - Binance - using '_nuxt' directory"

    strings:
        $zip_file = { 50 4b 03 04 }
        $spec_dir = "_nuxt"
        $spec_dir2 = "builds"
        $spec_file1 = "C5M-ywlo.js"
        $spec_file2 = "cfg.js"
        $spec_file3 = "bootstrap-icons.B0rJxbIo.woff"
        $spec_file4 = "error-404.CoZKRZXM.css"
        $spec_file5 = "b.png"

    condition:
        uint32(0) == 0x04034b50 and
        $zip_file and
        all of ($spec_dir*) and
        // check for file
        all of ($spec_file*)
}
```

# PhishingKit-Yara-Rules

SG-UPDATED.zip  
2.0 MB

1 02:04

**VirusTotal**

SG-UPDATED.zip

Detections: 7 / 61

- ESET-NOD32
- Avast
- Cynet
- Avira
- Google
- Ikarus
- AVG
- Bkav
- Lionic
- MicroWorld-eScan
- ClamAV

SUMMARY **DETECTION** DETAILS RELATIONS COMMUI

Crowdsourced YARA rules

Matches rule **PK\_SocietaGenerale\_don** by Thomas 'tAd' Damonneville from ruleset PK\_SocietaGenerale\_don

Popular threat label **phishing.phishingbank** Threat categories Family labels phis

Security vendors' analysis Do you want to automate checks?

|                     |                               |
|---------------------|-------------------------------|
| Avast               | HTML:PhishingBank-CMX [Phish] |
| AVG                 | HTML:PhishingBank-CMX [Phish] |
| Avira (no cloud)    | PHISH/Agent.akw               |
| Cynet               | Malicious (score: 99)         |
| ESET-NOD32          | PHP/HackTool.Botsant.S        |
| Google              | Detected                      |
| Ikarus              | PHISH.Agent                   |
| Acronis (Static ML) | Undetected                    |
| AhnLab-V3           | Undetected                    |
| Alibaba             | Undetected                    |

# PhishingKit-Yara-Rules

- . Add context
- . Live hunting
- . Retro hunting

0  
/ 62

?

Community Score

✓ No security vendors and no sandboxes flagged this file as malicious

31e712eb9764a27b3724f50b19042eb3c0e6b307  
d6302c9128ba1776095b8767  
stripe-RD972-user-em-detail.zip  
zip

600.51 KB  
Size

2022-11-02 06:45:56 UTC  
8 hours ago

ZIP

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Crowdsourced YARA Rules ⓘ

⚠

Matches rule **PK\_Stripe\_rd972** by Thomas 'tAd' Damonville from ruleset PK\_Stripe\_rd972 at  
<https://github.com/t4d/PhishingKit-Yara-Rules>  
↳ *Phishing Kit impersonating Stripe*

Security Vendors' Analysis ⓘ

|                     |              |           |              |
|---------------------|--------------|-----------|--------------|
| Acronis (Static ML) | ✓ Undetected | Ad-Aware  | ✓ Undetected |
| AhnLab-V3           | ✓ Undetected | Alibaba   | ✓ Undetected |
| ALYac               | ✓ Undetected | Antiy-AVL | ✓ Undetected |

Help us, contribute!

<https://github.com/t4d/PhishingKit-Yara-Rules>

 @o0tAd0o | stalkphish\_io

 thdemon | stalkphish