Phishing detection and investigation with OSINT feeds and free softwares

StalkPhish

Thomas ‘tAd’ Damonneville

Blue team (CERT)

StalkPhish company founder

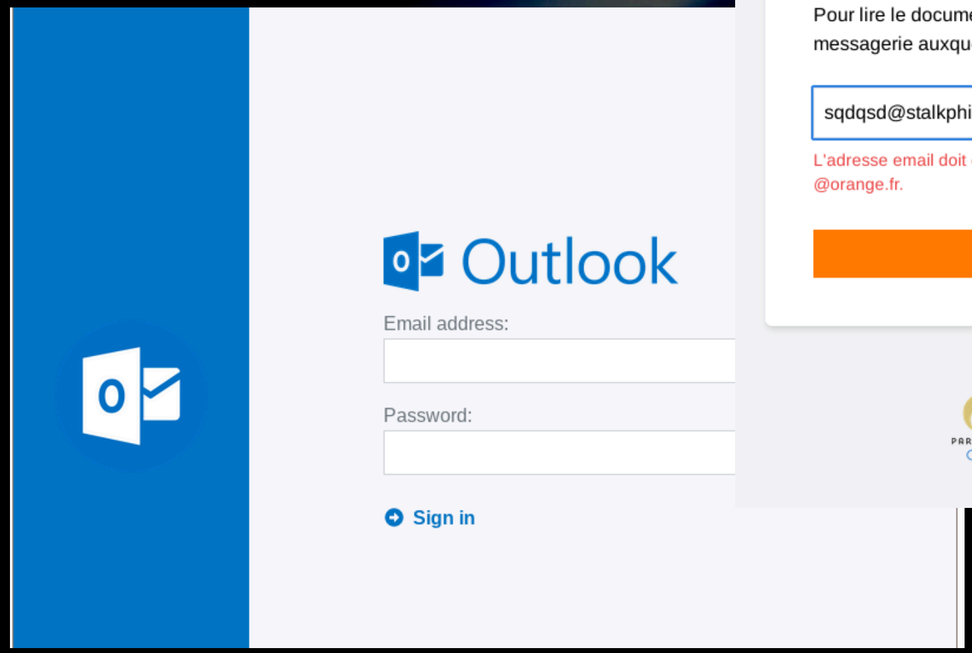
Coding phishing detection/invest. tools

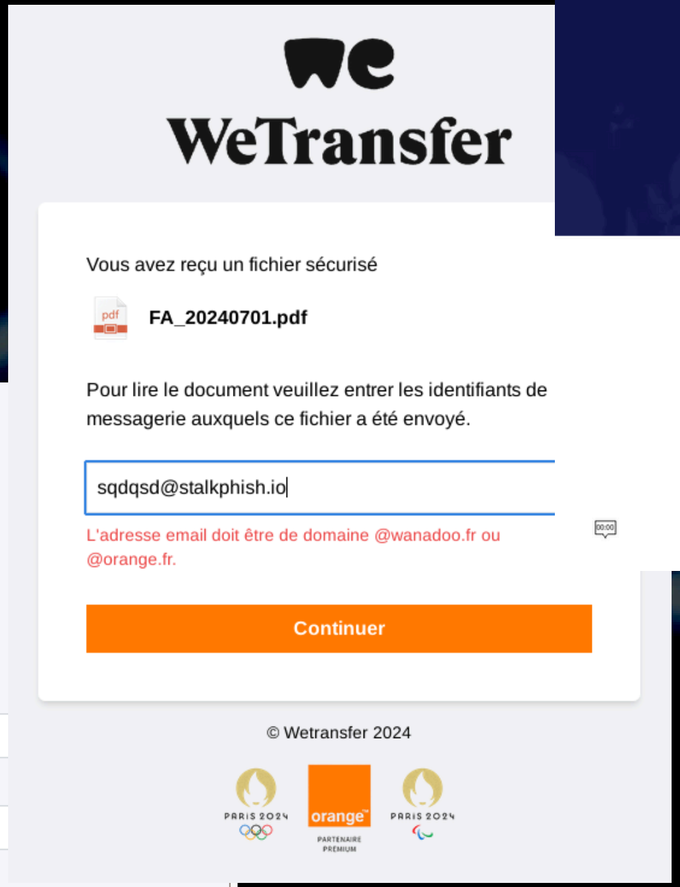
(Hackito Ergo Sum, /tmp/lab, ...)

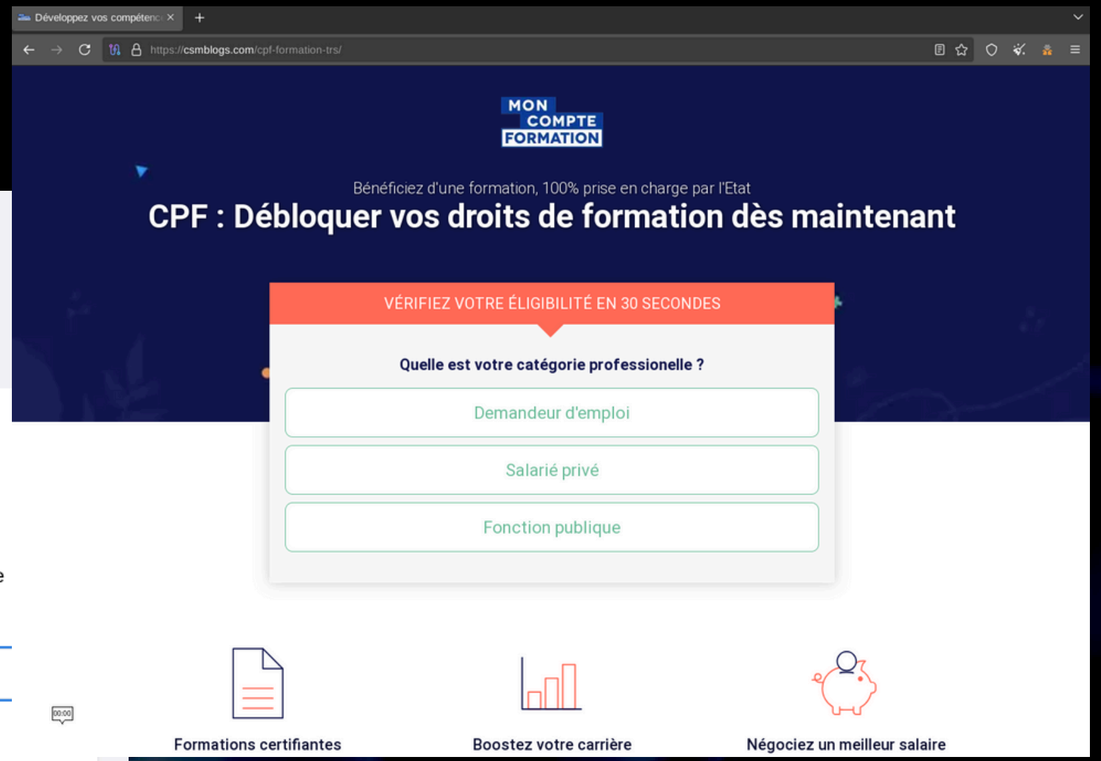
Love clicking phishing links

StalkPhish

PHISHING PAGES

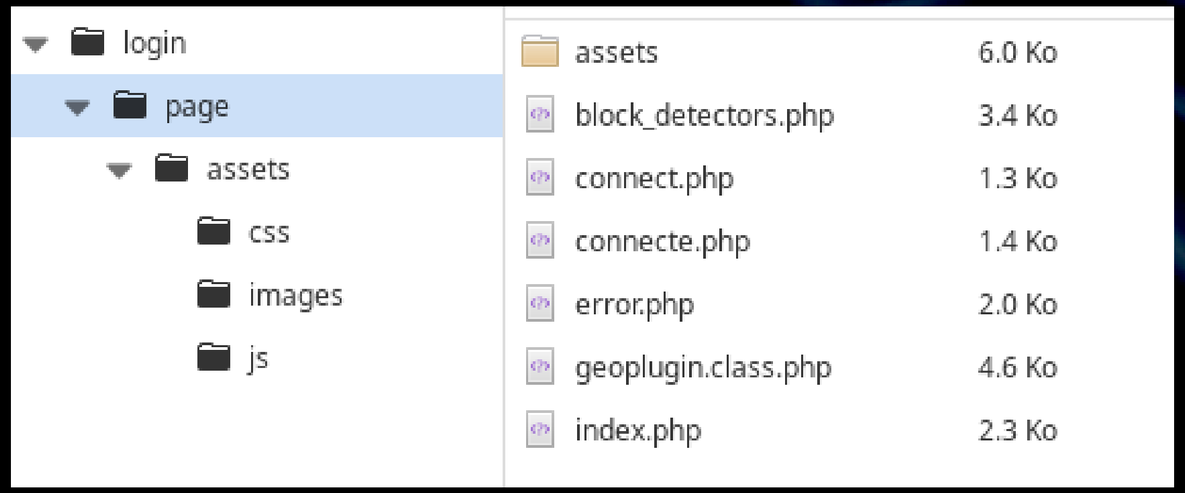


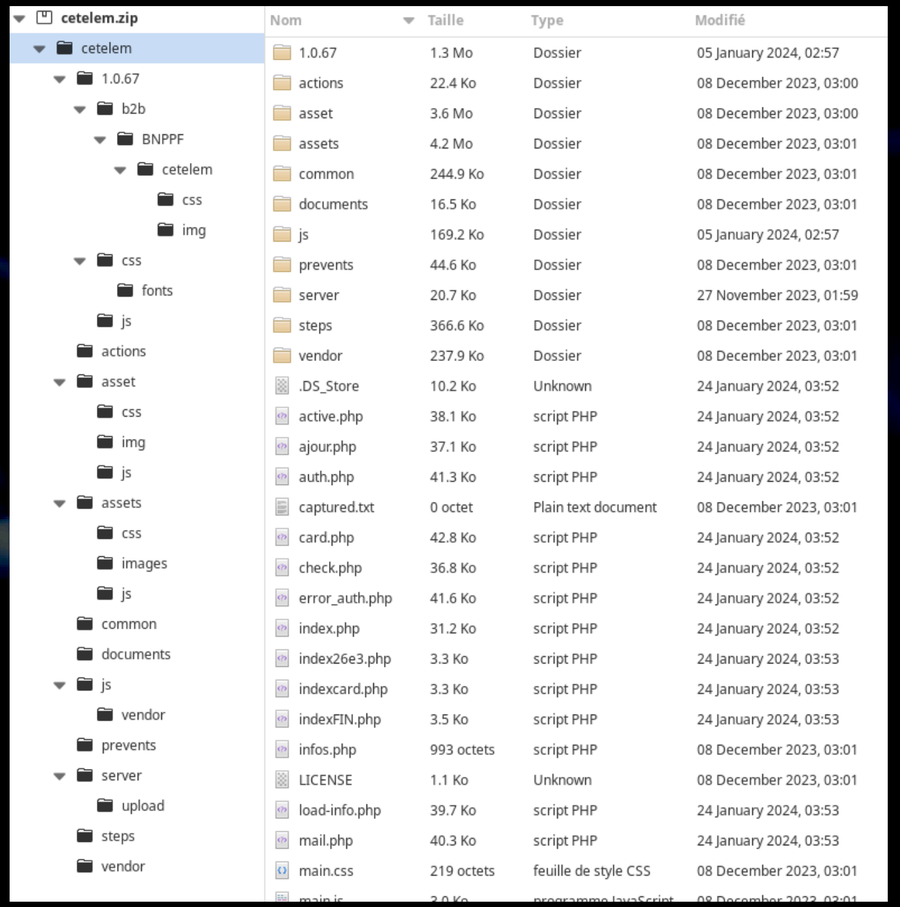




StalkPhish

PHISHING KIT ZIP FILES

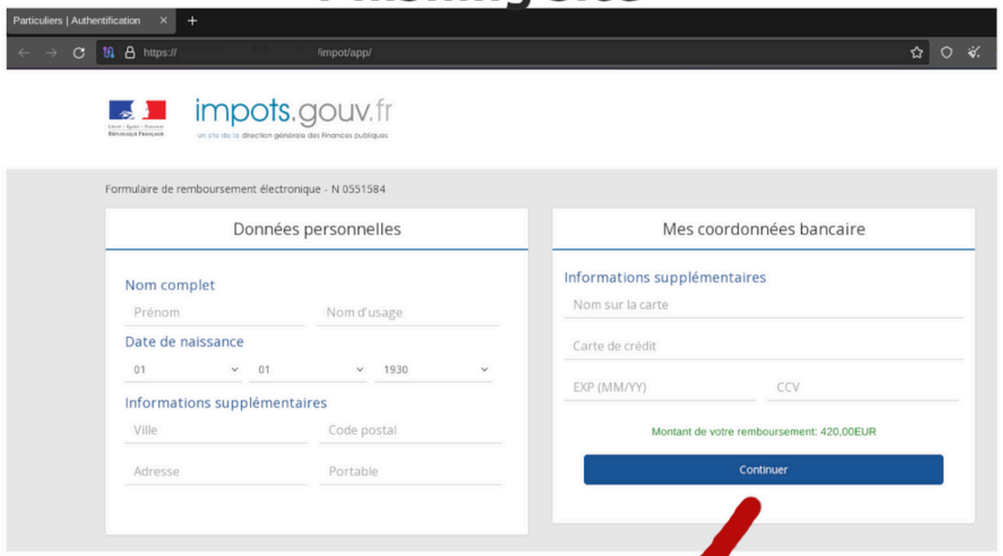




StalkPhish

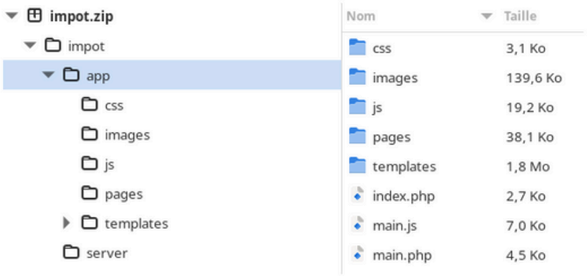
PHISHING INVESTIGATION

Phishing site



Actors

Phishing kit sources



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";
```


StalkPhish

FINDING PHISHING URLS/KITS

- Search specific strings in available OSINT data
- Enrich data
- Try to get phishing_kit.zip
- Extract data from phishing kit (emails, TG to come)
- Store data in a database (SQLite)

https://github.com/t4d/StalkPhish-OSS

FINDING PHISHING URLS/KITS - FEEDS

- urlscan.io search API
- urlquery.net search web crawler
- Phishtank free OSINT feed (with or without API key)
- Openphish free OSINT feed
- PhishStats search API
- Phishing.Database free OSINT feed

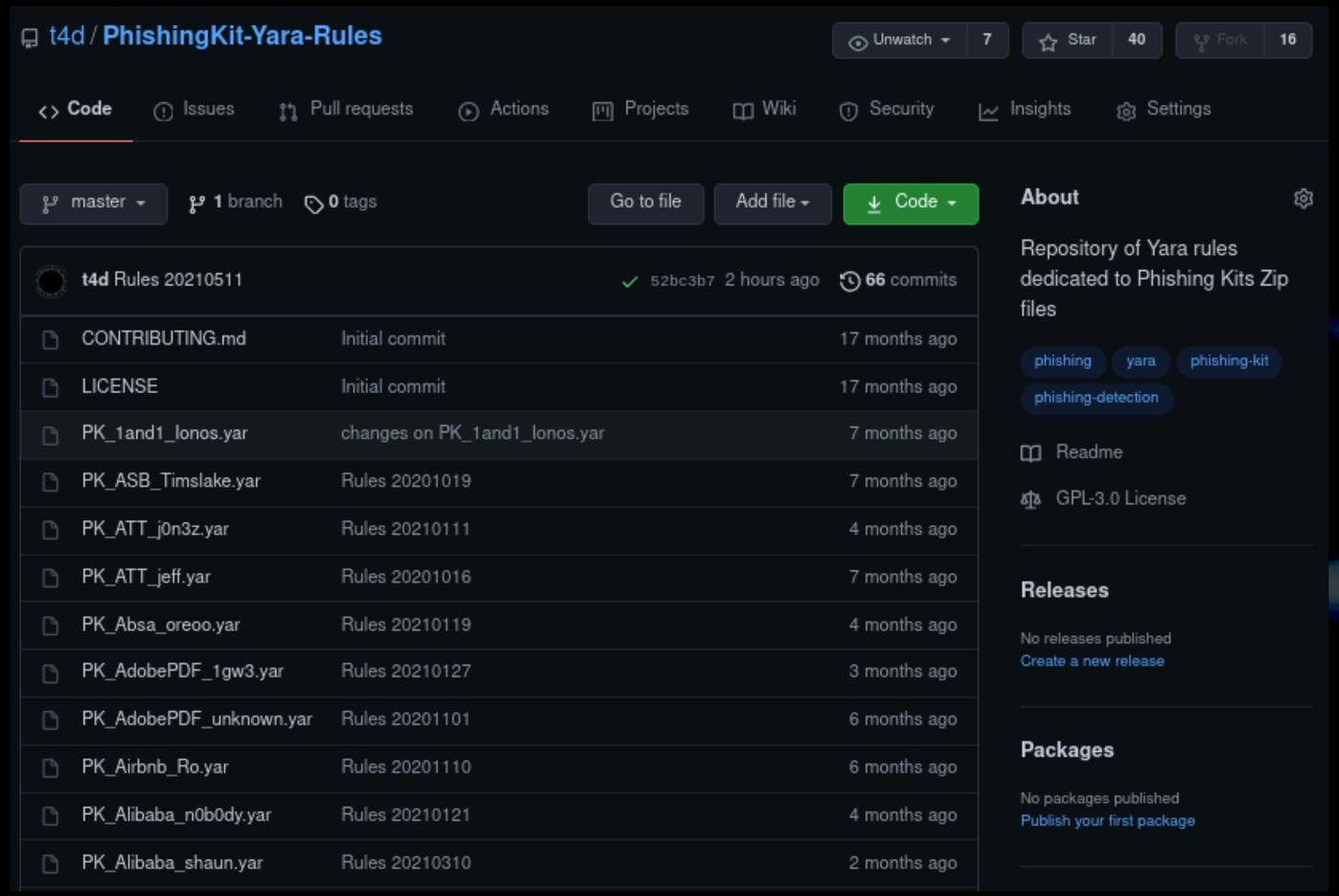
PHISHING KITS TRIAGE/IDENTIFICATION

- YARA rules parsing .ZIP files
- Search for specific directory/file names
- Identify the impersonated brand/service
- Identify the kit developer/crew
- Could be use for other deployed kits detection (hunting)

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

StalkPhish

PHISHING KITS TRIAGE/IDENTIFICATION



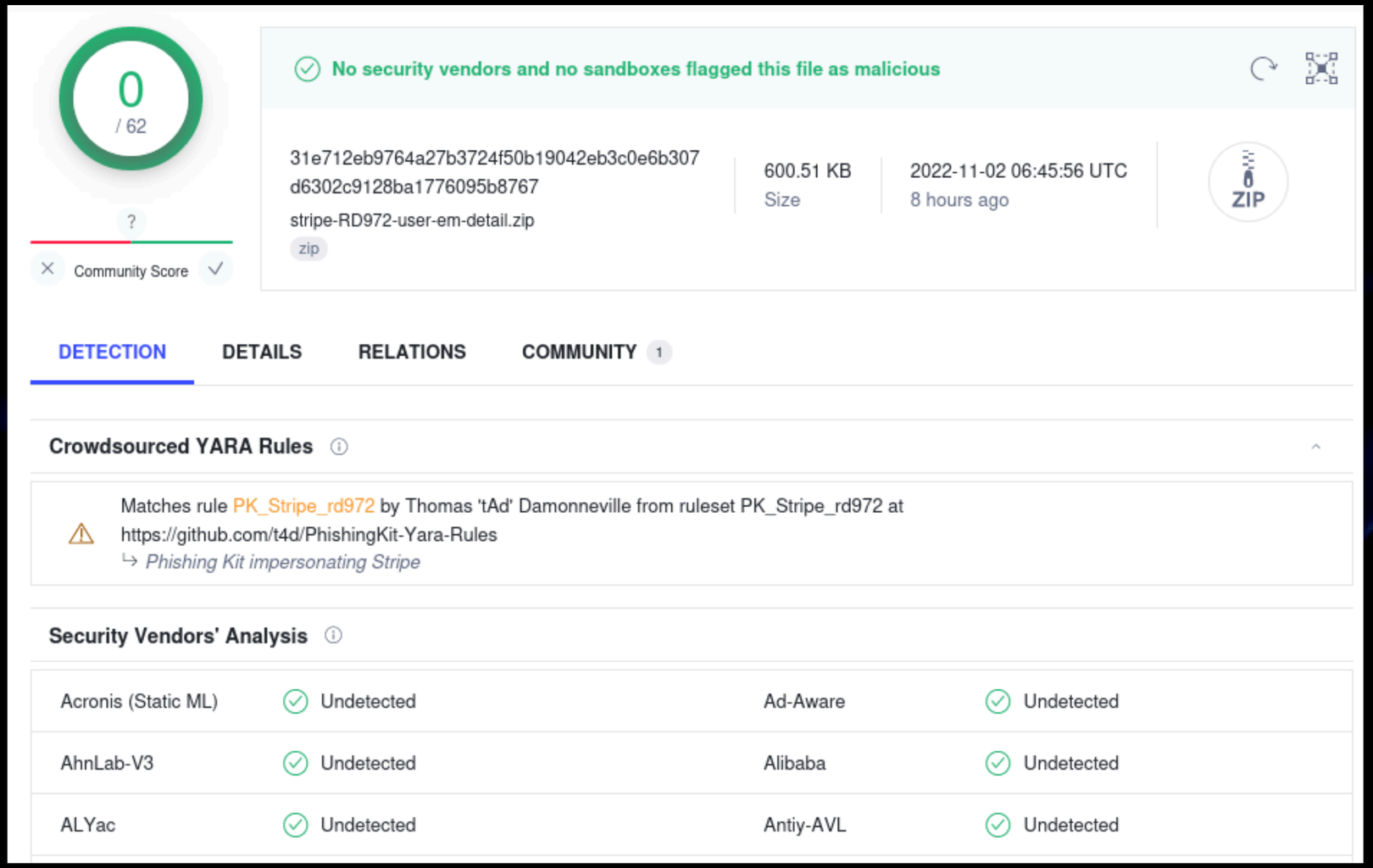

```yara
rule PK_Binance_nuxt : Binance
{
    meta:
        description = "Phishing Kit impersonating Binance"
        licence = "AGPL-3.0"
        author = "Thomas 'tAd' Damonneville"
        reference = ""
        date = "2025-01-31"
        comment = "Phishing Kit - Binance - using '_nuxt' directory"

    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.BOrJxbIo.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*)
}
```


StalkPhish

MORE HUNTING



StalkPhish

WORKSHOP

Code

→ StalkPhish-OSS (Python)

→ PhishingKit-Yara-Rules (Python)

https://github.com/t4d

Virtual Machine

→ VirtualBox image

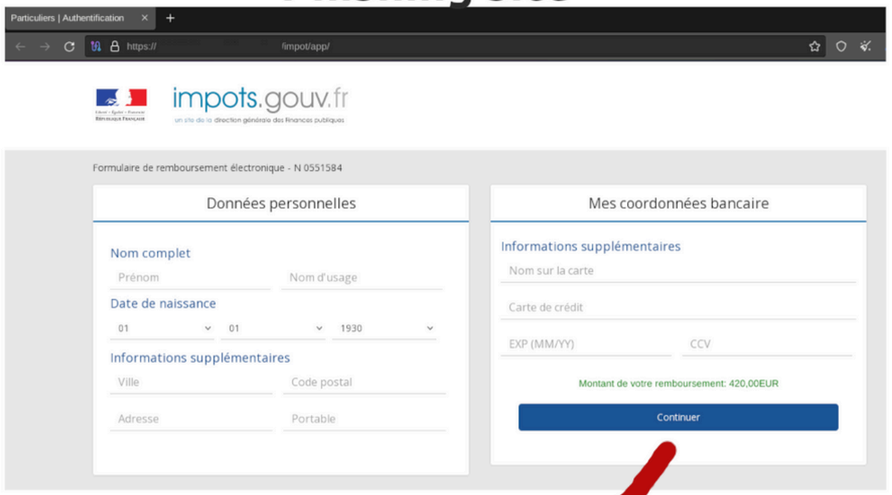
→ Pre-installed tools

→ Pre-filled database

1. Install/check tools
2. Configure StalkPhish-OSS
3. Launch StalkPhish to get URLs
4. Launch StalkPhish to get phishing kits
5. Observe kits
6. Pivot on data

StalkPhish

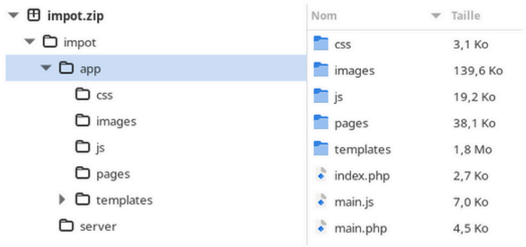
Phishing site



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



Exfiltration configuration

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

# REZ CONFIG
$mail = "infosresultat@gmail.com";
$token = "7271659943:AAEKiFm3G2X-z-obEp9QX-OQ41HJ5e5Km_g";
$chatid = "-1002191395823";
$spammer = "Exodia";

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


StalkPhish

MERCI!

 @o0tAd0o | @stalkphish_io

 thdamon | stalkphish

Blog: https://stalkphish.com

StalkPhish