



Phishing detection and investigation
with OSINT feeds and free softwares



Thomas 'tAd' Damonneville

Blue team (CERT)

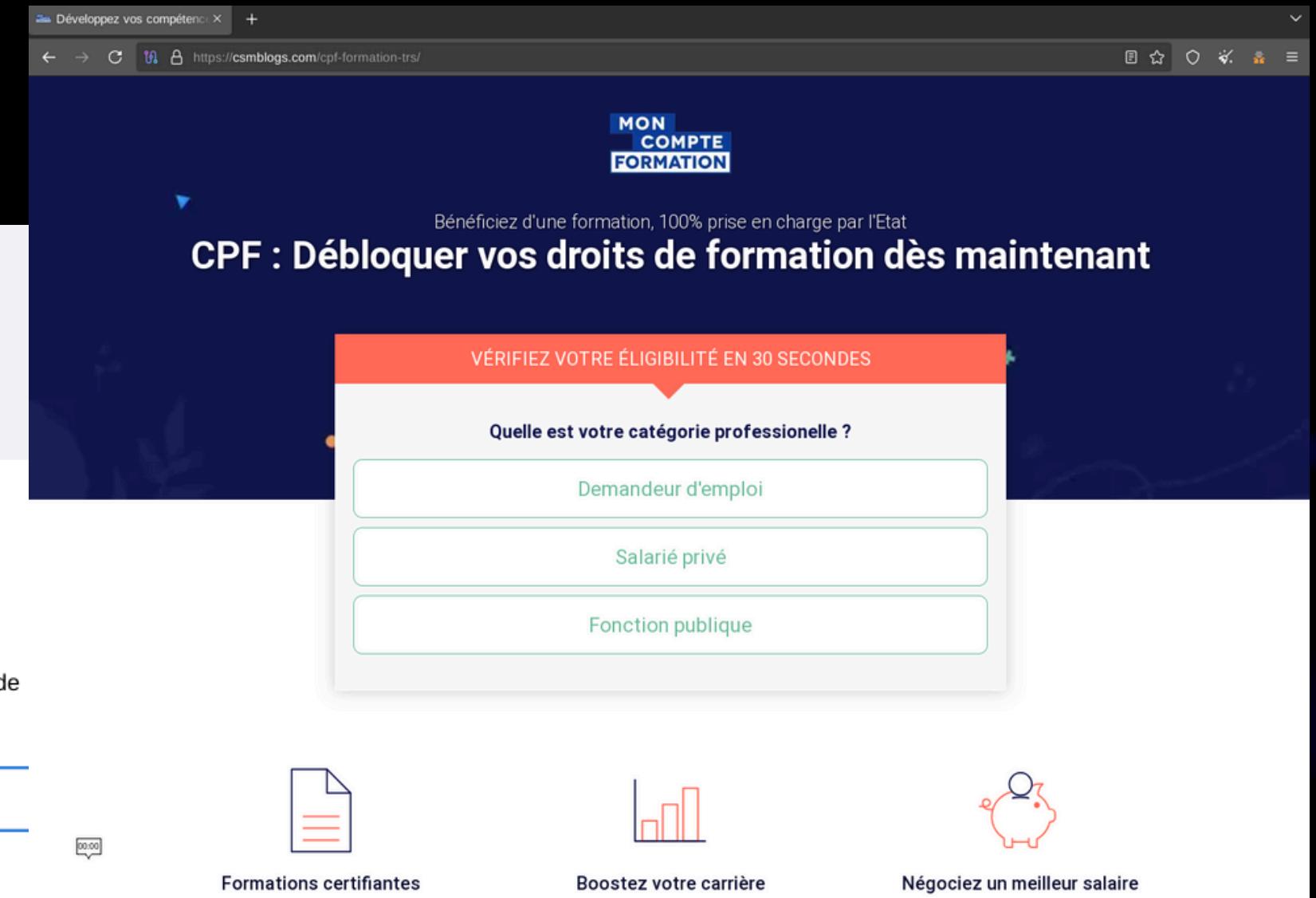
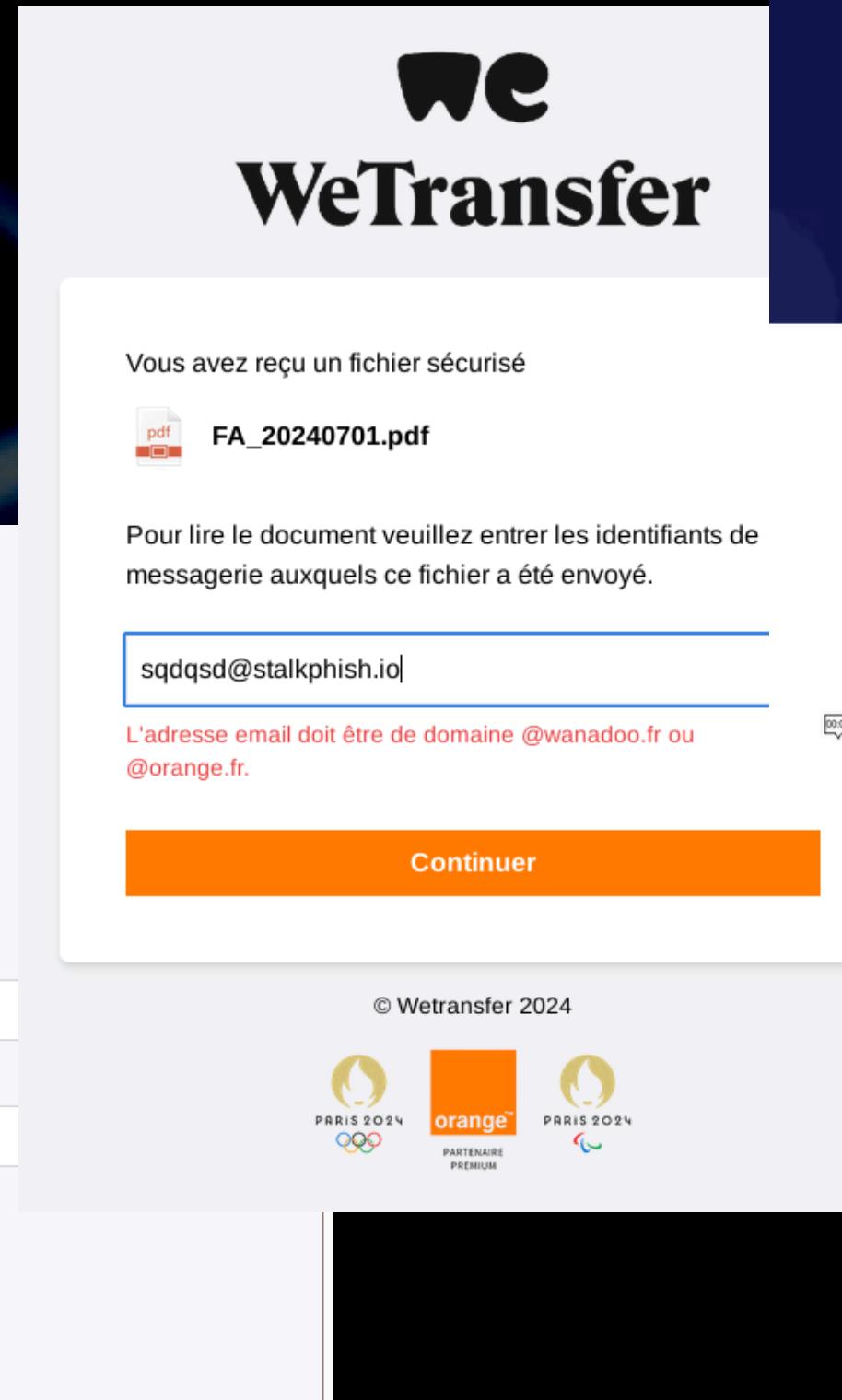
StalkPhish company founder

Coding phishing detection/invest. tools

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

Love clicking phishing links

PHISHING PAGES



PHISHING KIT ZIP FILES

Path	File/Folder	Size
login		
page	assets	6.0 Ko
block_detectors.php	3.4 Ko	
connect.php	1.3 Ko	
connecte.php	1.4 Ko	
error.php	2.0 Ko	
geoplugin.class.php	4.6 Ko	
index.php	2.3 Ko	
assets		
CSS		
images		
js		

File	Nom	Taille	Type	Modifié
cetelem.zip	cetelem			
	1.0.67	1.3 Mo	Dossier	05 January 2024, 02:57
	actions	22.4 Ko	Dossier	08 December 2023, 03:00
	asset	3.6 Mo	Dossier	08 December 2023, 03:00
	BNPPF	4.2 Mo	Dossier	08 December 2023, 03:01
	cetelem	244.9 Ko	Dossier	08 December 2023, 03:01
	css	16.5 Ko	Dossier	08 December 2023, 03:01
	img	169.2 Ko	Dossier	05 January 2024, 02:57
	js	44.6 Ko	Dossier	08 December 2023, 03:01
	fonts	20.7 Ko	Dossier	27 November 2023, 01:59
	steps	366.6 Ko	Dossier	08 December 2023, 03:01
	common	237.9 Ko	Dossier	08 December 2023, 03:01
	server	10.2 Ko	Unknown	24 January 2024, 03:52
	vendor	38.1 Ko	script PHP	24 January 2024, 03:52
	.DS_Store	37.1 Ko	script PHP	24 January 2024, 03:52
	auth.php	41.3 Ko	script PHP	24 January 2024, 03:52
	active.php	41.6 Ko	script PHP	24 January 2024, 03:52
	ajour.php	31.2 Ko	script PHP	24 January 2024, 03:52
	index.php	36.8 Ko	script PHP	24 January 2024, 03:52
	error_auth.php	3.3 Ko	script PHP	24 January 2024, 03:53
	index26e3.php	42.8 Ko	Plain text document	08 December 2023, 03:01
	captured.txt	3.3 Ko	script PHP	24 January 2024, 03:52
	card.php	3.5 Ko	script PHP	24 January 2024, 03:52
	check.php	40.3 Ko	script PHP	24 January 2024, 03:52
	indexcard.php	3.3 Ko	script PHP	24 January 2024, 03:53
	indexFIN.php	993 octets	script PHP	24 January 2024, 03:53
	infos.php	1.1 Ko	Unknown	08 December 2023, 03:01
	upload	39.7 Ko	script PHP	24 January 2024, 03:53
	steps	40.3 Ko	script PHP	24 January 2024, 03:53
	mail.php	219 octets	feuille de style CSS	24 January 2024, 03:53
	main.css	3.0 Ko	programme JavaScript	08 December 2023, 03:01
	main.js			

PHISHING INVESTIGATION

Phishing site

Particuliers | Authentification X +
https://fimpot/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
Nom sur la carte _____
Carte de crédit _____
EXP (MM/YY) _____ CCV _____
Montant de votre remboursement: 420,00EUR

Mes coordonnées bancaires

Continuer

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": "billiataire777"  
    }  
  ]  
}
```

Phishing kit sources

impost.zip

- impost
- app
 - css
 - images
 - js
 - pages
 - templates
 - index.php
 - main.js
 - main.php
 - server

Nom	Taille
css	3,1 Ko
images	139,6 Ko
js	19,2 Ko
pages	38,1 Ko
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";
```

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](https://phishtank.com) free OSINT feed (with or without API key)
- [Openphish](https://openphish.com) free OSINT feed
- [PhishStats](https://phishstats.com) search API
- [Phishing.Database](https://phishingdatabase.com) 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 used for other deployed kits detection (hunting)

t4d / PhishingKit-Yara-Rules

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

master 1 branch 0 tags Go to file Add file Code

About

Repository of Yara rules dedicated to Phishing Kits Zip files

phishing yara phishing-kit phishing-detection

Readme

GPL-3.0 License

Releases

No releases published Create a new release

Packages

No packages published Publish your first package

File	Type	Last Commit
t4d Rules 20210511	Rules	52bc3b7 2 hours ago 66 commits
CONTRIBUTING.md	Initial commit	17 months ago
LICENSE	Initial commit	17 months ago
PK_1and1_mnog.yar	Rules 20201019	7 months ago
PK_ASB_Timslake.yar	Rules 20201019	7 months ago
PK_ATT_Jon.z.yar	Rules 20211114	4 months ago
PK_ATT_jeff.yar	Rules 20201016	7 months ago
PK_Absa_oreoo.yar	Rules 20210119	4 months ago
PK_AdobePDF_1gw3.yar	Rules 20210127	3 months ago
PK_AdobePDF_unknown.yar	Rules 20201101	6 months ago
PK_Airbnb_Bo.yar	Rules 20201110	6 months ago
PK_Alibaba_n0b0dy.yar	Rules 20210121	4 months ago
PK_Alibaba_shaun.yar	Rules 20210310	2 months ago

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

PHISHING KITS TRIAGE/IDENTIFICATION

[t4d / PhishingKit-Yara-Rules](#)

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

master 1 branch 0 tags Go to file Add file Code

t4d Rules 20210511	Initial commit	2 hours ago
CONTRIBUTING.md	Initial commit	17 months ago
LICENSE	Initial commit	17 months ago
PK_1and1_lonos.yar	changes on PK_1and1_lonos.yar	7 months ago
PK_ASB_Timslake.yar	Rules 20201019	7 months ago
PK_ATT_j0n3z.yar	Rules 20210111	4 months ago
PK_ATT_jeff.yar	Rules 20201016	7 months ago
PK_Absa_oreoo.yar	Rules 20210119	4 months ago
PK_AdobePDF_1gw3.yar	Rules 20210127	3 months ago
PK_AdobePDF_unknown.yar	Rules 20201101	6 months ago
PK_Airbnb_Ro.yar	Rules 20201110	6 months ago
PK_Alibaba_n0b0dy.yar	Rules 20210121	4 months ago
PK_Alibaba_shaun.yar	Rules 20210310	2 months ago

About Repository of Yara rules dedicated to Phishing Kits Zip files

phishing yara phishing-kit phishing-detection

Readme GPL-3.0 License

Releases No releases published Create a new release

Packages No packages published Publish your first package

```
rule PK_Binance_nuxt : Binance
{
    meta:
        description = "Phishing Kit impersonating Binance"
        licence = "AGPL-3.0"
        author = "Thomas 'tAd' Damonnevile"
        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*)
}
```

MORE HUNTING

The screenshot shows a file analysis interface with the following details:

- Score:** 0 / 62 (Community Score)
- File Details:** MD5: 31e712eb9764a27b3724f50b19042eb3c0e6b307d6302c9128ba1776095b8767, Size: 600.51 KB, Date: 2022-11-02 06:45:56 UTC (8 hours ago). File type: ZIP.
- Detection:** No security vendors and no sandboxes flagged this file as malicious.
- Crowdsourced YARA Rules:** Matches rule **PK_Stripre_rd972** by Thomas 'tAd' Damonneville from ruleset **PK_Stripre_rd972** at <https://github.com/t4d/PhishingKit-Yara-Rules>.
Description: *Phishing Kit impersonating Stripe*
- Security Vendors' Analysis:**

Vendor	Result
Acronis (Static ML)	Undetected
AhnLab-V3	Undetected
ALYac	Undetected
Ad-Aware	Undetected
Alibaba	Undetected
Antiy-AVL	Undetected

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

Phishing site

Particuliers | Authentication x +

https://impot/app/

impots.gouv.fr

Formulaire de remboursement électronique - N 0551584

Données personnelles

Mes coordonnées bancaire

Informations supplémentaires

Nom sur la carte

Carte de crédit

EXP (MM/YY) CCV

Montant de votre remboursement: 420,00EUR

Continuer

Actors

```
{
  "bot_info": {
    "first_name": "Sgsansssms_Bot",
    "username": "Sgdelagloiresansssms_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": "Sgsansssms_Bot",
      "last_name": null,
      "language_code": null,
      "username": "Sgdelagloiresansssms_Bot"
    },
    {
      "id": 6504711855,
      "is_bot": false,
      "first_name": "Billiard",
      "last_name": null,
      "language_code": "fr",
      "username": "billiardaire777"
    }
  ]
}
```

Phishing kit sources

Nom	Taille
css	3,1 Ko
images	139,6 Ko
js	19,2 Ko
pages	38,1 Ko
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";

```

MERCI!



@o0tAd0o | @stalkphish_io



thdamon | stalkphish

Blog: <https://stalkphish.com>