Pass
the SALT

HUNT FOR PHISHING URLS SCAMMERS AND THEIR MATERIALS

StalkPhish

Who?

photo by Philippe Teuwen

Thomas ‘tAd’ Damonneville

. Blue team (CERT)

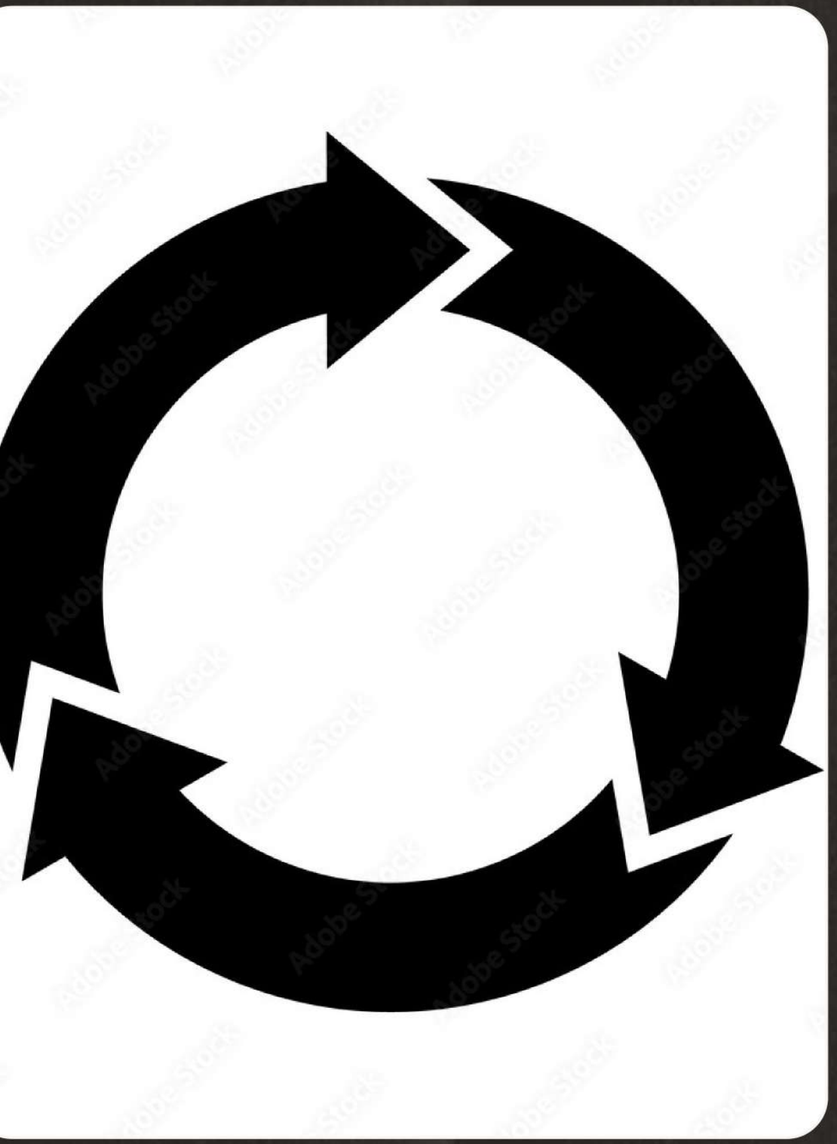
. StalkPhish company founder

. Coding phishing detection tools

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

Why?

.too much phishing for SOC
.not very familiar threat, for me
.who are these people?
.what do they want?
.how they work?
.how to detect?
.how to takedown?
...



How?

. lurking
. learning
. coding
. lurking
. learning
. stalking
. coding
. learning
. ...

PhishingKitHunter

Start: 2017

Purpose: parsing company logs to find phishing

Why: “phishing kits” sometimes use official files of a page


```
 _ \  | / |   |           |
 |   | ' /  |   | |   | __ \   __|  _ \   __|
 ___/  . \   ___ | |   | |   | |    __/ |
_|    _|\_\_|  _|\__,_|_|_|  _|\__|\___|_|

-= Phishing Kit Hunter - v0.8.1 =-

[+] http://badscam.org/includes/ap/?a=2
                |   Timestamp: 01/May/2017:13:00:03
                | HTTP status: can't connect (HTTP Erro
[+] http://scamme.com/aple/985884e5b60732b1245fdfaf2a49
                |   Timestamp: 01/May/2017:13:00:49
                | HTTP status: can't connect (<urlopen
[+] http://badscam-er.com/eb/?e=4
                |   Timestamp: 01/May/2017:13:01:06
                | HTTP status: can't connect (<urlopen
[+] http://assur.cam.tech/scam/brand/new/2bd5a55bc5e768
                |   Timestamp: 01/May/2017:13:01:14
                | HTTP status: UP
                | HTTP shash : 0032588b8d93a807cf0f48a8
                | DOMAIN registrar: ASCIO TECHNOLOGIES,
                | DOMAIN creation date: 2008-07-10 00:0
                | DOMAIN expiration date: 2017-07-10 00
[+] http://phish-other.eu/assur/big/phish/2be1c6afdbfc0
                |   Timestamp: 01/May/2017:13:01:15
                | HTTP status: UP
                | HTTP shash : 2a545c4d321e3b3cbb34af62
                | DOMAIN registrar: Hostmaster Strato R
                | DOMAIN creation date: None found
                | DOMAIN expiration date: None found
697475it [06:41, 1208.14it/s]
```

https://github.com/t4d/PhishingKitHunter

PhishingKitHunter - goal

- Parsing RP logs to check HTTP_REFERER
- Search for specific strings (file names) mostly used by a kit

```
[21/Apr/2024:13:14:47 +0200] "GET /assets/img/content/carte-paiement-AFM.svg HTTP/1.1" 200 629368 "http://bad-url.com/phishing/"
"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.110 Safari/537.36" "-" 443
```

```
Le numéro de télépaiement et la clé se situent sur la carte de paiement. Le numéro de télépaiement
<br>
<img src="https://www.amendes.gouv.fr/assets/img/content/carte-paiement-AFM.svg" width="100%">
```

PhishingKitHunter - output

- stdout
- CSV file:

PK_URL: found URL
Domain: extracted domain name
HTTP_sha256: page hash
HTTP_status: connexion status
date: date of connexion
domain registrar
domain creation date
domain expiration date

```
 _ \  |  / |   |           |
 |   | ' /  |   | |   | __ \   __|  _ \   __|
 ___/  . \   ___ | |   | |   | |    __/ |
_|    _|\_\_|  _|\__,_|_|_|  _|\__|\___|_|

-= Phishing Kit Hunter - v0.8.1 =-

[+] http://badscam.org/includes/ap/?a=2
                |   Timestamp: 01/May/2017:13:00:03
                | HTTP status: can't connect (HTTP Erro
[+] http://scamme.com/aple/985884e5b60732b1245fdfaf2a49
                |   Timestamp: 01/May/2017:13:00:49
                | HTTP status: can't connect (<urlopen
[+] http://badscam-er.com/eb/?e=4
                |   Timestamp: 01/May/2017:13:01:06
                | HTTP status: can't connect (<urlopen
[+] http://assur.cam.tech/scam/brand/new/2bd5a55bc5e768
                |   Timestamp: 01/May/2017:13:01:14
                | HTTP status: UP
                | HTTP shash : 0032588b8d93a807cf0f48a8
                | DOMAIN registrar: ASCIO TECHNOLOGIES,
                | DOMAIN creation date: 2008-07-10 00:0
                | DOMAIN expiration date: 2017-07-10 00
[+] http://phish-other.eu/assur/big/phish/2be1c6afdbfc0
                |   Timestamp: 01/May/2017:13:01:15
                | HTTP status: UP
                | HTTP shash : 2a545c4d321e3b3cbb34af62
                | DOMAIN registrar: Hostmaster Strato R
                | DOMAIN creation date: None found
                | DOMAIN expiration date: None found
697475it [06:41, 1208.14it/s]
```

PhishingKitHunter - configuration

```
  _ \  |  / |   |                |
 |   | ' /  |   | |   | __ \  __|  _ \  __|
 ___/  . \  ___ | |   | |   | |    __/ |
_|    _|\_\_|  _|\__,_|_|_|  _|\__|\___|_|

-= Phishing Kit Hunter - v0.8.1 =-

                        -h --help   Prints this
                        -i --ifile    Input logfile to analyse
                        -o --ofile    Output CSV report file (default: ./PKHunter-report-'date
                        -c --config   Configuration file to use (default: ./conf/defaults.conf
```

PhishingKitHunter - configuration

→ 4 configuration items:

```
[DEFAULT]
# tracking_file_request:
# Provide a RegEx describing the name of the file used by a Phishing kit
# ex: tracking_file_request = \.specific\.js$
tracking_file_request = (.)+file\.min\.js

# legitimate_referer:
# Provide a RegEx describing legitimate URL referer
# ex: Legitimate_referer = '\.google(user)?\.fr(:443)?$'
legitimate_referer = \.my-orga(-andme)?\.org(:443)?$

# log_pattern:
# Provide a RegEx used to parse your log file
# You need 3 parameters in this order: timestamp, HTTP file request, HTTP referer
# ex: Big-IP:
log_pattern = ^[^\[]+\[([^\s]+)\s[^\s]+\]\s+\"[^\s]+\s+([^\s]+)\s+[^\"]+\"[^\"]+\"([^\"]+)


[CONNECT]
# http_proxy:
# (optional) Declare a HTTP proxy to use for HTTP Get informations
# ex: http_proxy = http://127.0.0.1:8080 for a HTTP_proxy server
# ex: http_proxy = socks://127.0.0.1:9050 for a SOCKS proxy server
;http_proxy = socks://127.0.0.1:9050
```

PhishingKitHunter - output

```
$ ./PhishingKitHunter.py -i LogFile2017.log -o PKHunter-report-20170502-013307.csv -c conf/tes

  _ \  |  / |   |            |
 |   | ' /  |   | |   | __ \  __|  _ \  __|
 ___/  . \  ___ | |   | |   | |    __/ |
_|    _|\_\_|  _|\__,_|_|  _|\__|\___|_|

-= Phishing Kit Hunter - v0.8.1 =-

[+] http://badscam.org/includes/ap/?a=2
                |   Timestamp: 01/May/2017:13:00:03
                | HTTP status: can't connect (HTTP Error 404: Not Found)
[+] http://scamme.com/aple/985884e5b60732b1245fdfaf2a49cdfe/
                |   Timestamp: 01/May/2017:13:00:49
                | HTTP status: can't connect (<urlopen error [Errno -2] Name or service not kn
[+] http://badscam-er.com/eb/?e=4
                |   Timestamp: 01/May/2017:13:01:06
                | HTTP status: can't connect (<urlopen error [Errno -2] Name or service not kn
[+] http://assur.cam.tech/scam/brand/new/2bd5a55bc5e768e530d8bda80a9b8593/
                |   Timestamp: 01/May/2017:13:01:14
                | HTTP status: UP
                | HTTP shash : 0032588b8d93a807cf0f48a806ccf125677503a6fabe4105a6dc69e81ace609
                | DOMAIN registrar: ASCIO TECHNOLOGIES, INC. DANMARK - FILIAL AF ASCIO TECHNOL
                | DOMAIN creation date: 2008-07-10 00:00:00
                | DOMAIN expiration date: 2017-07-10 00:00:00
[+] http://phish-other.eu/assur/big/phish/2be1c6afdbfc065c410d36ba88e7e4c9/
                |   Timestamp: 01/May/2017:13:01:15
                | HTTP status: UP
                | HTTP shash : 2a545c4d321e3b3cbb34af62e6e6fbfbdbc00a400bf70280cb00f4f6bb0eac4
                | DOMAIN registrar: Hostmaster Strato Rechenzentrum
                | DOMAIN creation date: None found
                | DOMAIN expiration date: None found
697475it [06:41, 1208.14it/s]
```

... but I can get much more ...

StalkPhish-OSS

Start: 2018

Purpose: use OSINT to get phishing URLs, get material (phishing kits), enrich data

Why: expand your knowledge of the threat

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

StalkPhish-OSS - goal

- 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)

StalkPhish-OSS - usage

```
  _____ _        _ _     _____  _     _     _
 / ____| |      | | |   |  __ \| |   (_)   | |
| (___ | |_ __ _| | | _| |__) | |__  _ ___| |__
 \___ \| __/ _` | | |/ /  ___/| '_ \| / __| '_ \
 ____) | || (_| | |   <| |    | | | | \__ \ | | |
|_____/ \__\__,_|_|_|\_\_|    |_| |_|_|___/_| |_| OSS

-= StalkPhish-OSS - The Phishing Kit stalker - v0.10 =-


    -h --help       Prints this help
    -c --config     Configuration file to use (mandatory)
    -G --get        Try to download zip file containing phishing kit sources (long and noisy)
    -N --nosint     Don't use OSINT databases
    -u --url        Add only one URL
    -s --search     Search for a specific string on OSINT modules
```

StalkPhish-OSS - OSINT modules

- Phishtank
- Openphish
- Phishstats
- Phishing.Database
- URLQuery
- URLScan.io

```
[URLQUERY]
# urlquery.net search web crawler
activate = yes
OSINT_url = https://urlquery.net/search

[PHISHTANK]
# Phishtank OSINT feed
activate = yes
OSINT_url = https://data.phishtank.com/data/online-valid.js
keep_files = no
API_key =

[OPENPHISH]
# Openphish OSINT feed
activate = yes
OSINT_url = https://www.openphish.com/feed.txt
keep_files = no
```

StalkPhish-OSS - main conf

- Strings you look for
- Logs path
- Download directories
- Database (SQLite)

```
# External source keywords to search for (keywords separated by a comma)
search = webmail,secure,email

[PATHS]
# Logging
log_conf = ./conf/logging.conf
log_dir = ./log/
log_file = stalkphish.log

# Where you download Phishing kits
Kits_download_Dir = ./dl/

# Where you download external source files to parse
Ext_src_Files = ./files/

[DATABASE]
# Where you store your Databases
Databases_files = ./db
sqliteDB_filename = %(Databases_files)s/StalkPhish.sqlite3
sqliteDB_tablename = StalkPhish
sqliteDB_Investig_tablename = StalkPhishInvestig
```

StalkPhish-OSS - connect conf

→ Proxy (Socks5/HTTP)

due to geo-location filtering:

```
allowCountry: ["FR", "CI", "MA", "BE"], // Allowed Country code
```

ISP filtering:

```
if ($status == "botisp") {
    header('Location: Antibot/Isp.php');
    die('<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head>
    Found</title></head><body><h1>Not Found</h1><p>The requested URL was
    blocker server.</p><p>Additionally, a 404 Not Found error was encoun
    use an ErrorDocument to handle the request.</p></body></html>');
}
```

or anti-bot lists:

```
$bannedIP = array("^81.161.59.*", "^66.135.200.*", "^66.10
if (in_array($_SERVER['REMOTE_ADDR'], $bannedIP)) {
    exit(header('Location: https://www.google.com/'));
```

```
[CONNECT]
# http_proxy:
# (optional) Declare a HTTP proxy to use for
# (you can comment the 'http_proxy' line if y
# ex: http_proxy = http://127.0.0.1:8080 for
# ex: http_proxy = socks5://127.0.0.1:9050 fo
http_proxy = socks5://127.0.0.1:9050

# StalkPhish's default user-agent (don't remo
http_UA = Mozilla/5.0 (Windows NT 10.0; Win64
# Use a HTTP user-agents file to use for phis
UAfile = ./useragent_list.txt
```

StalkPhish-OSS - connect conf

→ User-Agent
due to UA filtering:

```php
$detect = new Mobile_Detect;
if(!$detect->isMobile() AND strtolower($block_pc) == "yes"){
     header("location: out.php");
     exit;
}
```

or anti-bot lists:

```php
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words = array("above", "google", "softlayer", "amazonaws", "cyveillance", "phishtank"
foreach($blocked_words as $word) {
    if (substr_count($hostname, $word) > 0) {
        exit(header('Location: https://www.google.com/'));
    }
```

```
[CONNECT]
# http_proxy:
# (optional) Declare a HTTP proxy to use for
# (you can comment the 'http_proxy' line if y
# ex: http_proxy = http://127.0.0.1:8080 for
# ex: http_proxy = socks5://127.0.0.1:9050 fo
http_proxy = socks5://127.0.0.1:9050

# StalkPhish's default user-agent (don't remo
http_UA = Mozilla/5.0 (Windows NT 10.0; Win64
# Use a HTTP user-agents file to use for phis
UAfile = ./useragent_list.txt
```

StalkPhish-OSS - phishing kit collect

- we can sometimes find ZIP files
  - in OpenDir
  - or still available on the website

```
[200] http://donnarogersimagery.com/wp-includes/pomo/login.alibaba.com/
Alibaba Manufacturer Directory - Suppliers, Manufacturers, Exporters &amp;amp; Importers
trying http://donnarogersimagery.com/wp-includes.zip
trying http://donnarogersimagery.com/wp-includes/pomo.zip
trying http://donnarogersimagery.com/wp-includes/pomo/login.alibaba.com.zip
[DL ] Found archive, downloaded it as: ./test/dl/http__donnarogersimagery.com_wp-includes_pom
[Email] Found: shaddyokoh@hotmail.com
```

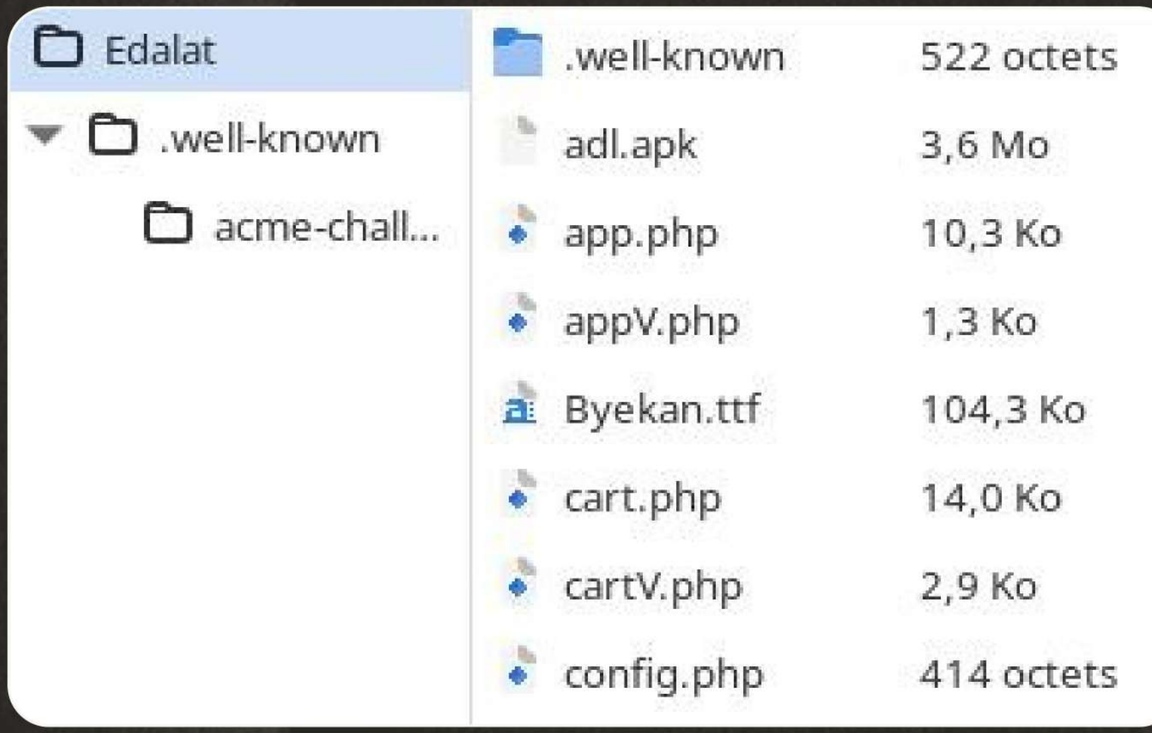
Index of /wp-includes

Name	Last modified	Size	Description
Parent Directory		-	
plugin.php	2023-01-06 01:15	35K	
fnbnorth.com/	2023-01-04 23:01	-	
assets/	2023-01-04 15:33	-	
office/	2023-01-04 05:47	-	
office.zip	2023-01-04 05:46	21K	
cgi.php	2023-01-04 01:48	381K	
cok/	2023-01-04 01:36	-	
myhst-com.mymailsrvr..>	2023-01-03 23:13	-	
unzip.php	2023-01-03 14:58	12K	

StalkPhish-OSS - why collect phishing kits?

- So much information:
  - More strings to look for
  - Developer
  - Actor
  - Exfiltration vector
  - Targets/victims
  - Malwares
  - Other tricks

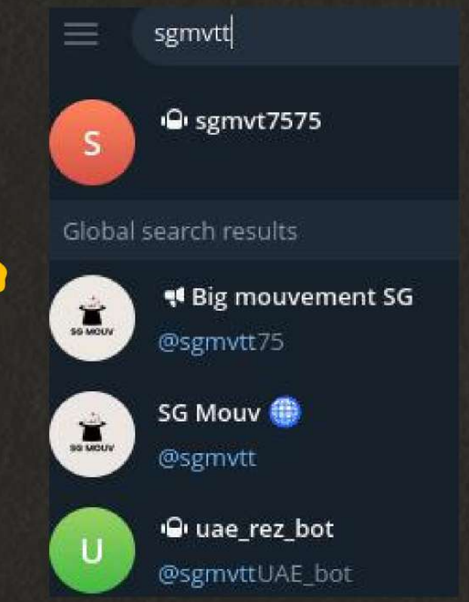
  etc...



StalkPhish-OSS - why collect phishing kits?

→ Telegram stolen data exfiltration:

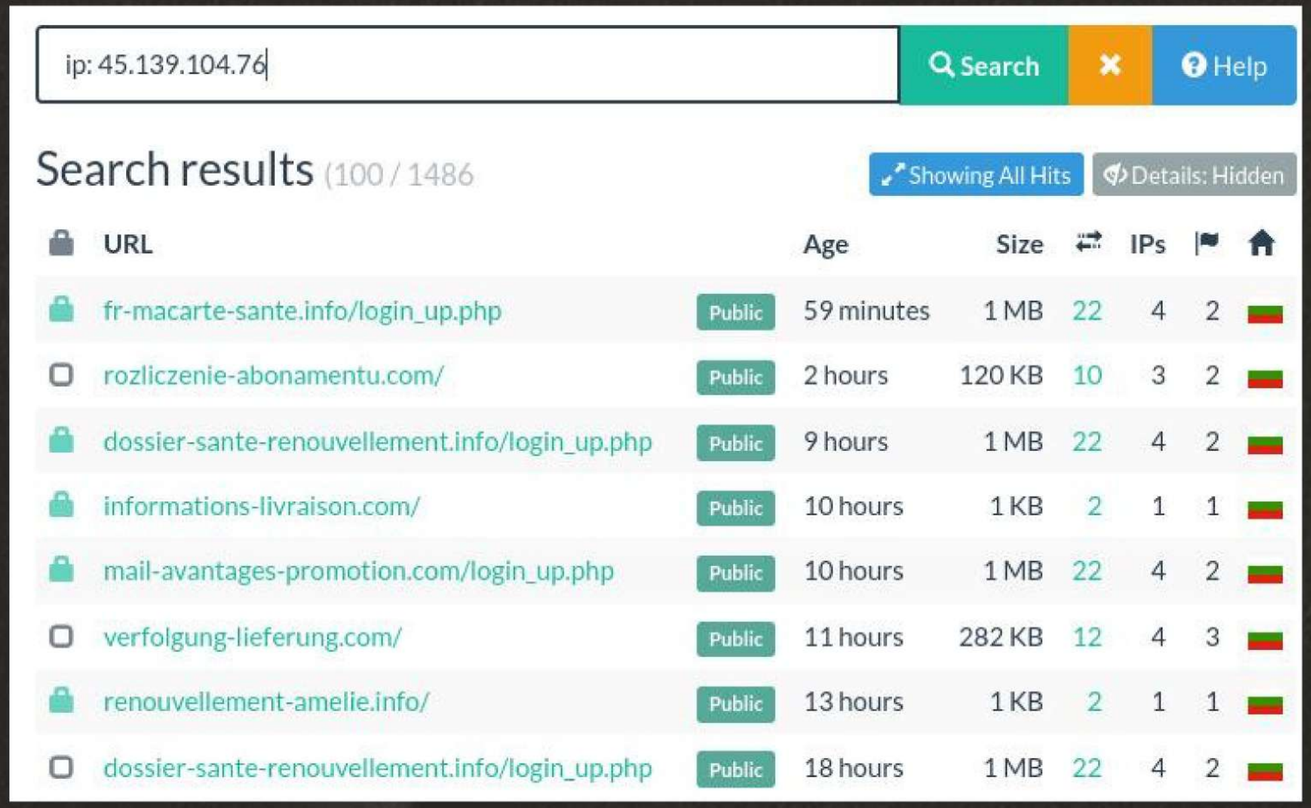

```
{
  "bot_info": {
    "first_name": "sgmvt7575",
    "username": "sgmvtt7575_bot",
    "id": 6992399372
  },
  "chat_info": {
    "title": "REz FRANCA",
    "type": "group",
    "invite_link": null
  },
  "admins_info": [
    {
      "id": 6368140518,
      "is_bot": false,
      "first_name": "SG Mouv",
      "last_name": null,
      "language_code": "fr",
      "username": "sgmvtt"
    }
  ]
}
```

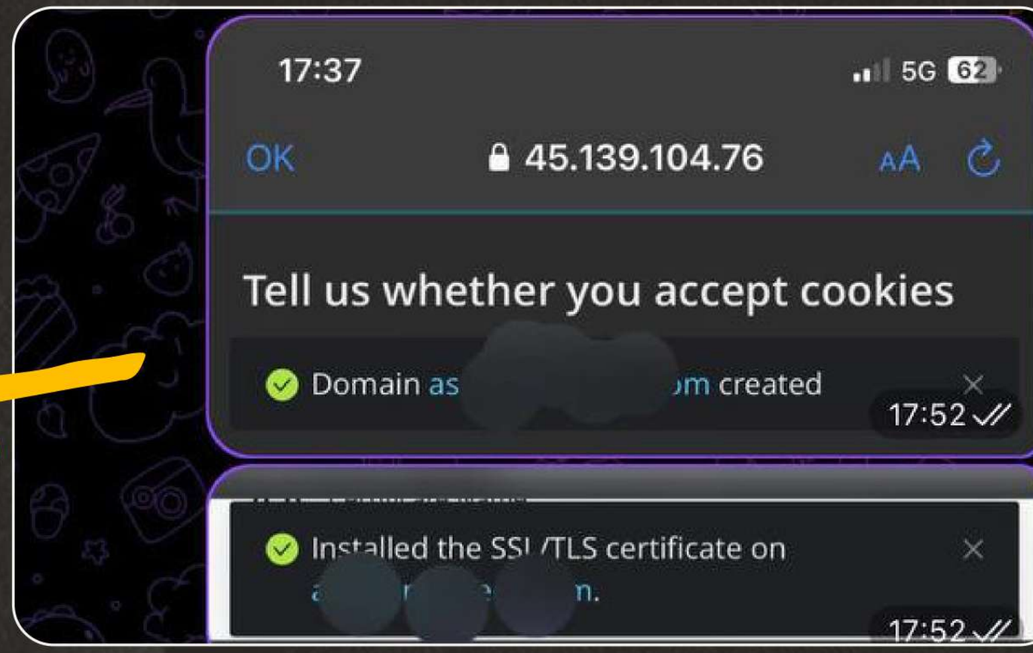




```
# Mail
$mail_send = false;
$my_mail = "";

#Telegram
$tlg_send = true;
$bot_token = "6992399372:AAHmsa35s7XnFPjsvHqj7uEF6XawF
$rez_billing = "-4154769096";
$rez_card = "-4154769096";
$rez_vbv = "-4154769096";

$vbv = false;
$timerVBV = "15";

$pass = ""; # PANEL
$test_mode = false;
```

StalkPhish-OSS - why collect phishing kits?

→ Then pivot on Telegram channels:

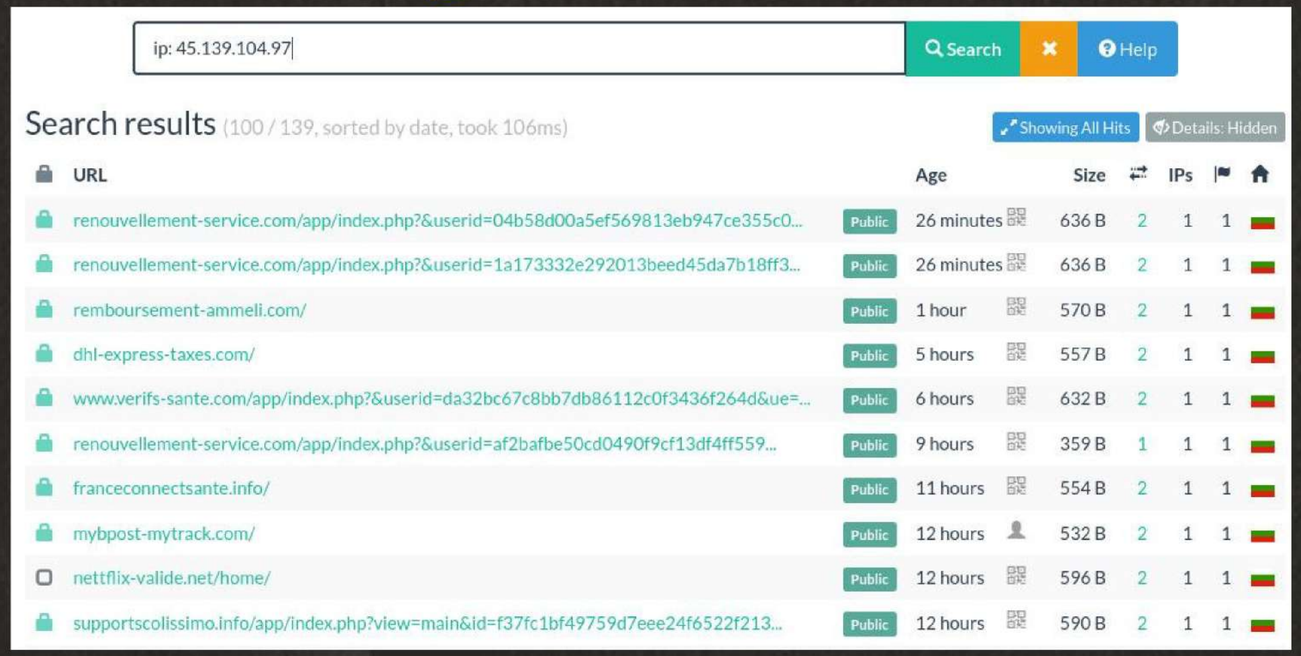


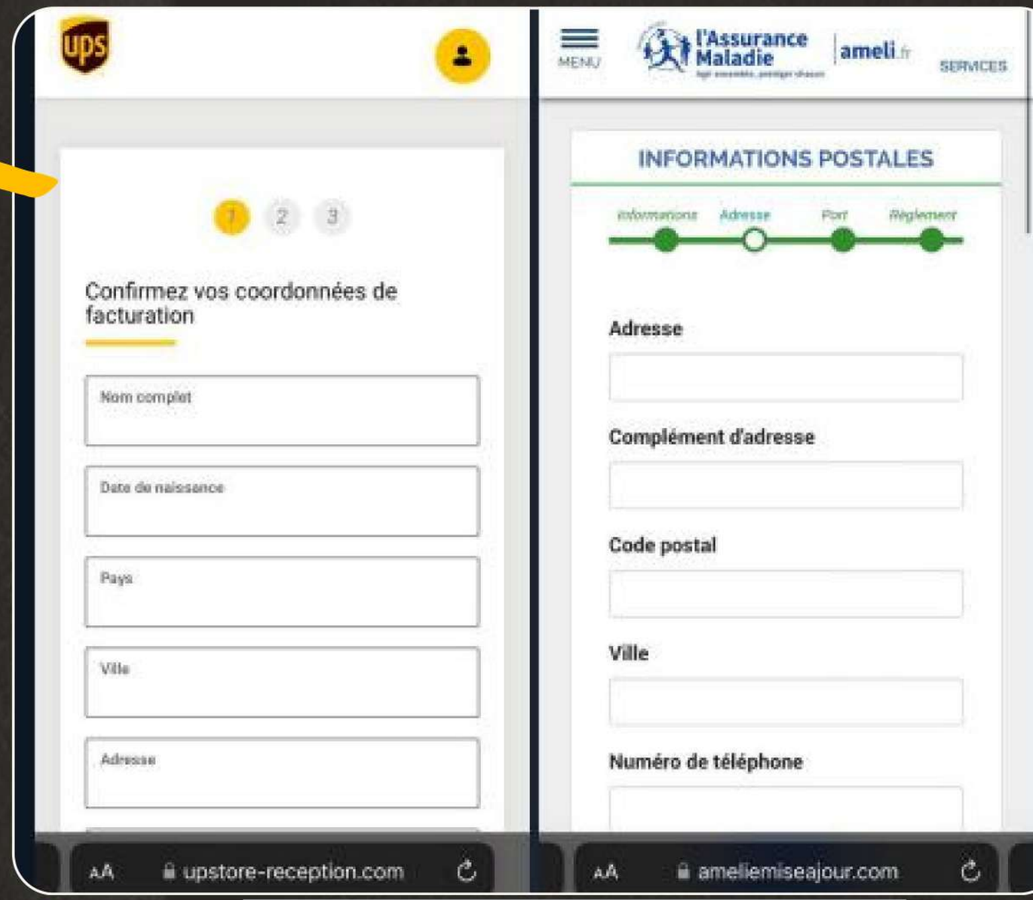


StalkPhish
- The Phishing kits stalker OSS

StalkPhish-OSS - why collect phishing kits?

```
Name:    upstore-reception.com
Address: 45.139.104.97
```

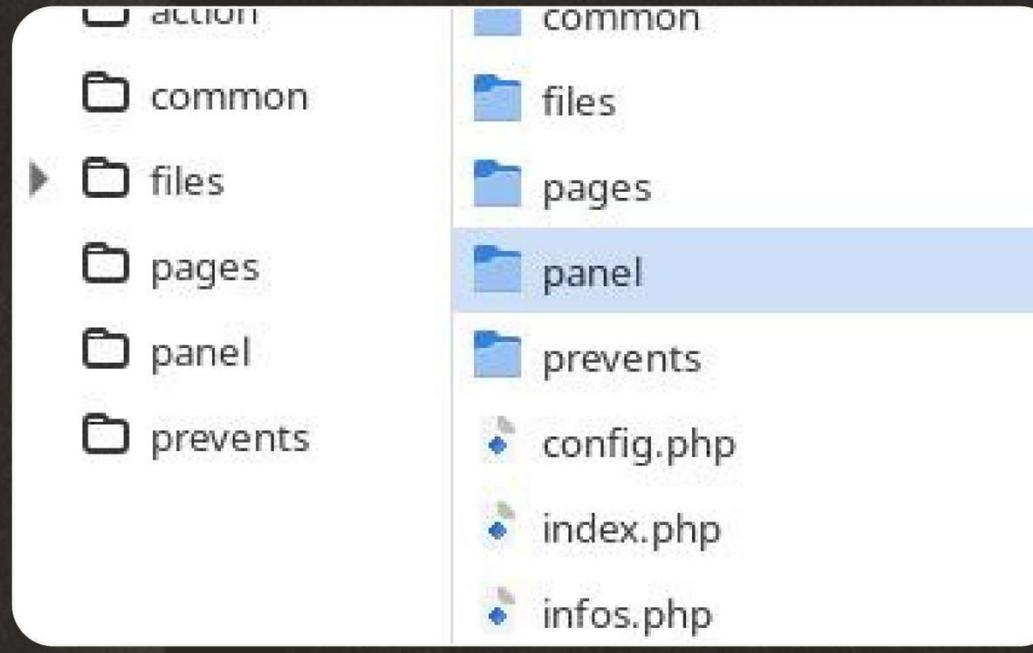


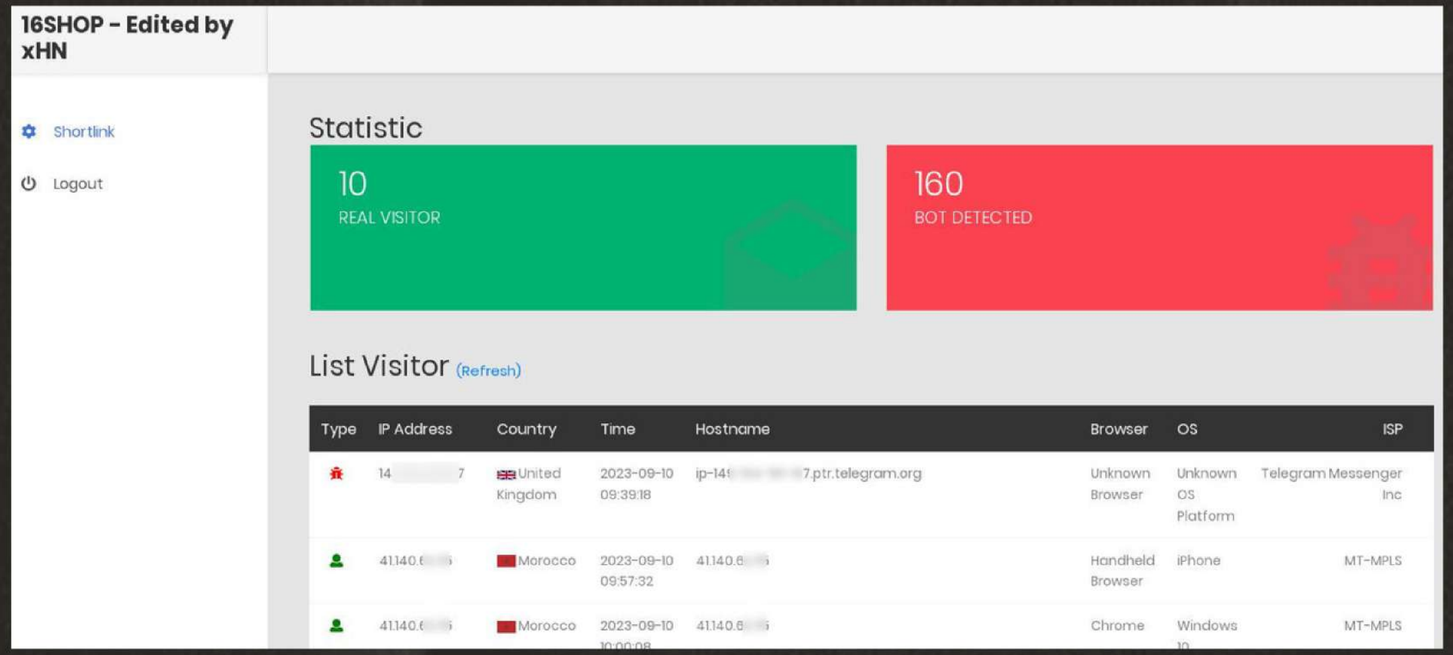


StalkPhish - The Phishing kits stalker OSS

StalkPhish-OSS - why collect phishing kits?

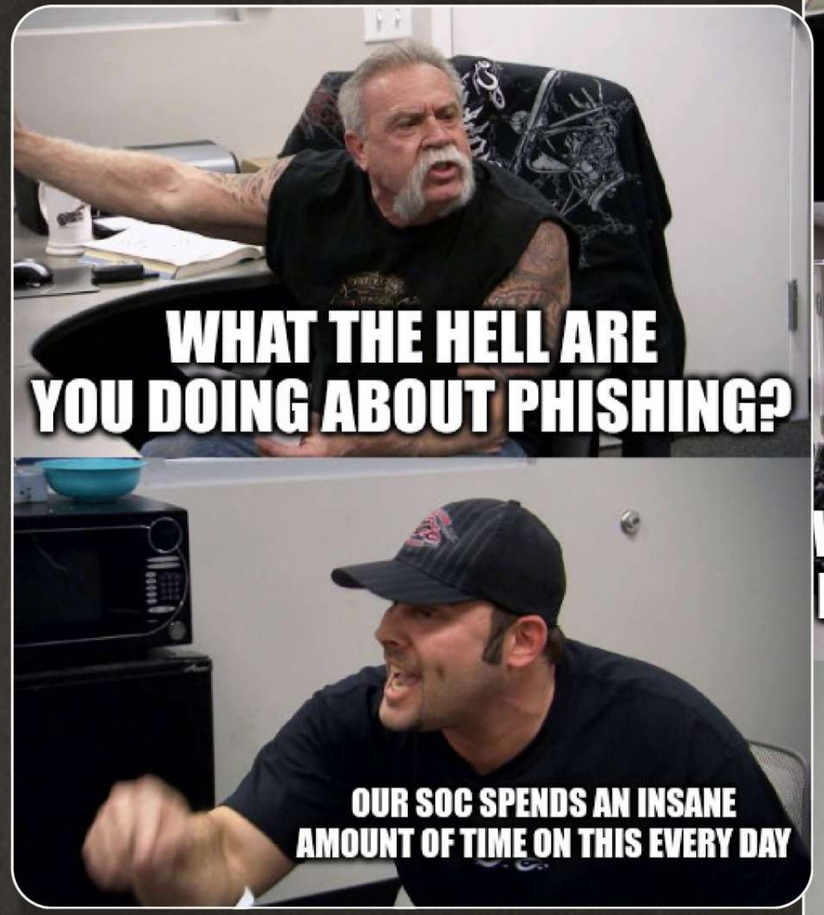
→ Find panel with victims data:

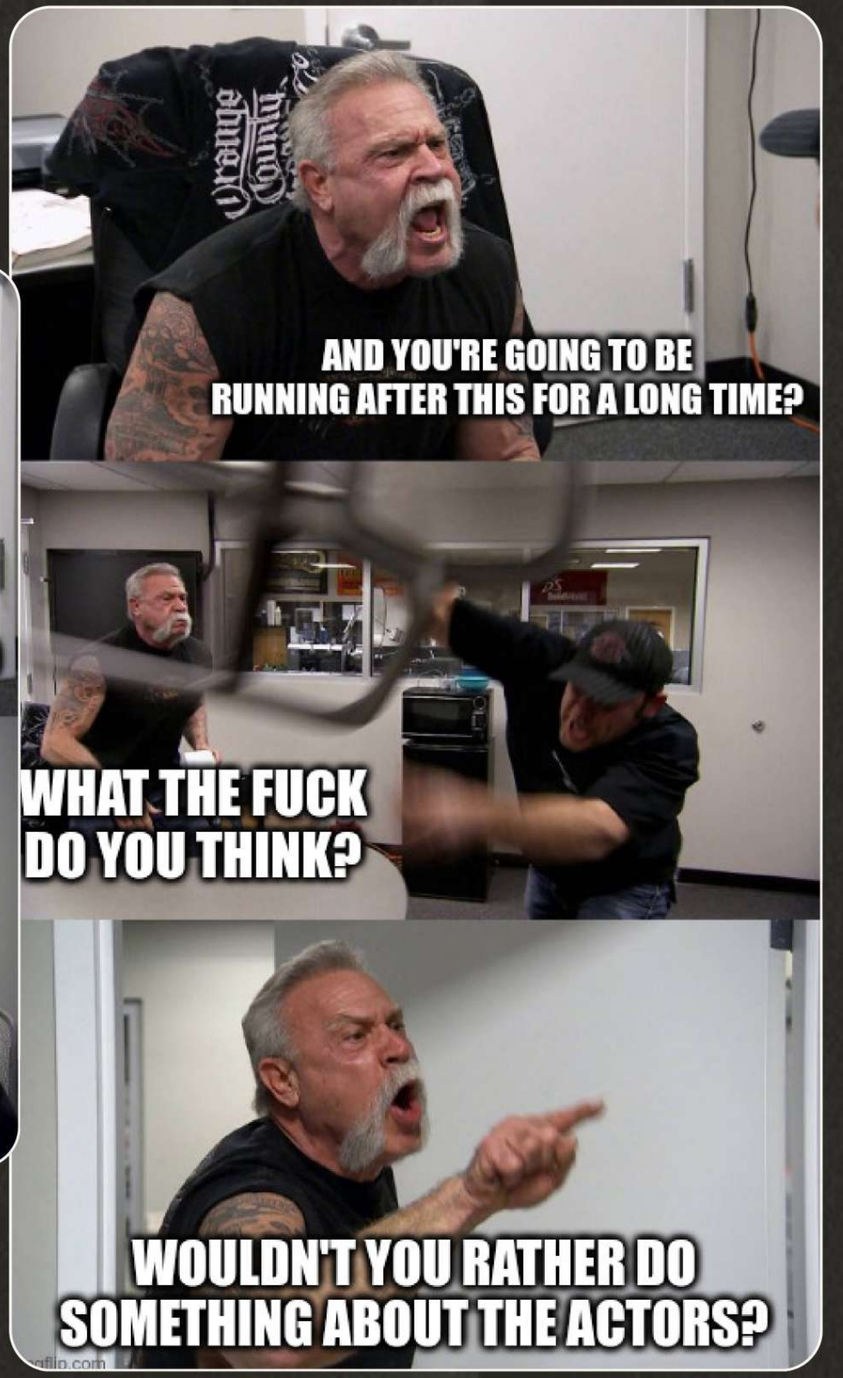




... and not only victims

StalkPhish


WHAT THE HELL ARE
YOU DOING ABOUT PHISHING?
OUR SOC SPENDS AN INSANE
AMOUNT OF TIME ON THIS EVERY DAY


AND YOU'RE GOING TO BE
RUNNING AFTER THIS FOR A LONG TIME?
WHAT THE FUCK
DO YOU THINK?
WOULDN'T YOU RATHER DO
SOMETHING ABOUT THE ACTORS?

... and I got so much kits ...

PhishingKit-Yara-Rules

Start: 2019

Purpose: Yara rules for phishing kit ZIP files

Why: So many phishing kits, I have to know which brand they are impersonating and if I still know it.


```
rule PK_PayPal_H3ATSTR0K3 : PayPal
{
    meta:
        description = "Phishing Kit im
        licence = "GPL-3.0"
        author = "Thomas 'tAd' Damonne
        reference = ""
        date = "2019-11-28"
        comment = "Phishing Kit - PayP

    strings:
        // the zipfile working on
        $zip_file = { 50 4b 03 04 }
        // specific directory found in
        $spec_dir = "prevents"
        // specific file found in Phis
        $spec_file = "mine.php" nocase
        $spec_file2 = "bcce592108d8ec0
        $spec_file3 = "captured.txt"
        $spec_file4 = "H3ATSTR0K3.txt"
```

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

PhishingKit-Yara-Rules

~700 Yara rules

PhishingKit-Yara-Rules - goal

- Works on .ZIP
- Search for specific directory/file names
- Identify the impersonated brand/service
- Identify the kit developer/crew
- Could be use for other deployed kits detection

```
rule PK_Telstra_flow : Telstra
{
    meta:
        description = "Phishing Kit impersonating Telstra"
        licence = "AGPL-3.0"
        author = "Thomas 'tAd' Damonneville"
        reference = ""
        date = "2024-04-15"
        comment = "Phishing Kit - Telstra - using Flow.txt as exfil. file"

    strings:
        // the zipfile working on
        $zip_file = { 50 4b 03 04 }
        // specific directory found in PhishingKit
        $spec_dir = "src"
        // specific file found in PhishingKit
        $spec_file = "cc.php"
        $spec_file2 = "Email.php"
        $spec_file3 = "smserror.php"
        $spec_file4 = "1.svg"
        $spec_file5 = "pn-blue.png"
        $spec_file6 = "done.gif"

    condition:
        // look for the ZIP header
        uint32(0) == 0x04034b50 and
        // make sure we have a local file header
        $zip_file and
        all of ($spec_dir*) and
        // check for file
        all of ($spec_file*)
}
```

Community Score

7/65 security vendors and no sandboxes flagged this file as malicious

Reanalyze | Similar | More

04bbee7cf05952bfbc2e6e0f9969d2cbbc139edb0a45875000…

hostmod.zip

zip

Size
3.15 MB

Last Modification Date
1 hour ago

ZIP

DETECTION | DETAILS | RELATIONS | COMMUNITY 2

Crowdsourced YARA rules

⚠ Matches rule PK_O365_Greatness2 from ruleset PK_O365_Greatness2 at https://github.com/t4d/PhishingKit-Yara-Rules by Thomas Damonneville
↳ *Phishing Kit impersonating Office 365 - Greatness PaaS campaigns - 5 hours ago*

Popular threat label phishing.

Threat categories phishing trojan

Security vendors' analysis

Do you want to automate checks?

Avast	HTML:Phishing-CWN [Phish]	AVG	HTML:Phishing-CWN [Phish]
DrWeb	JS.Proslikefan.13	ESET-NOD32	Multiple Detections
Google	Detected	Ikarus	Trojan.PHP.WebShell
Yandex	Trojan.Pyper.b1DzLj.11	Acronis (Static ML)	Undetected

THANK YOU!

@o0tAd0o | stalkphish_io

thdamon | stalkphish

Blog: https://stalkphish.com