

..: Phishing Kit Hunter :..

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

```

    -= 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 known>)
```

```
[+] 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 known>)
```

[+] <http://assur.cam.tech/scam/brand/new/2bd5a55bc5e768e530d8bda80a9b8593/>

```
| Timestamp: 01/May/2017:13:01:14
```

```
| HTTP status: UP
```

```
| HTTP shash : 0032588b8d93a807cf0f48a806ccf125677! $ ./PhishingKitHunter.py --help
```

```
| DOMAIN registrar: ASCIO TECHNOLOGIES, INC. DANMAI
```

```
| 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/2be1c6afdbfc065c410d36ba!
```

```
| Timestamp: 01/May/2017:13:01:15
```

```
| HTTP status: UP
```

```
| HTTP shash : 2a545c4d321e3b3cbb34af62e6e6fbfbdbc|
```

```
| DOMAIN registrar: Hostmaster Strato Rechenzentrum
```

```
| DOMAIN creation date: None found
```

```
| DOMAIN expiration date: None found
```

```
697475it [06:41, 1208.14it/s]
```

```
-= Phishing Kit Hunter - v0.8.1 =-
```

Parsing logs to detect phishing campaigns which use your own material or redirect users to your infra.

Based on the analysis of referer's URL

→ RegEx search

→ Enrichment

→ CSV report

```
-h --help  Prints this
```

```
-i --ifile      Input logfile to analyse
```

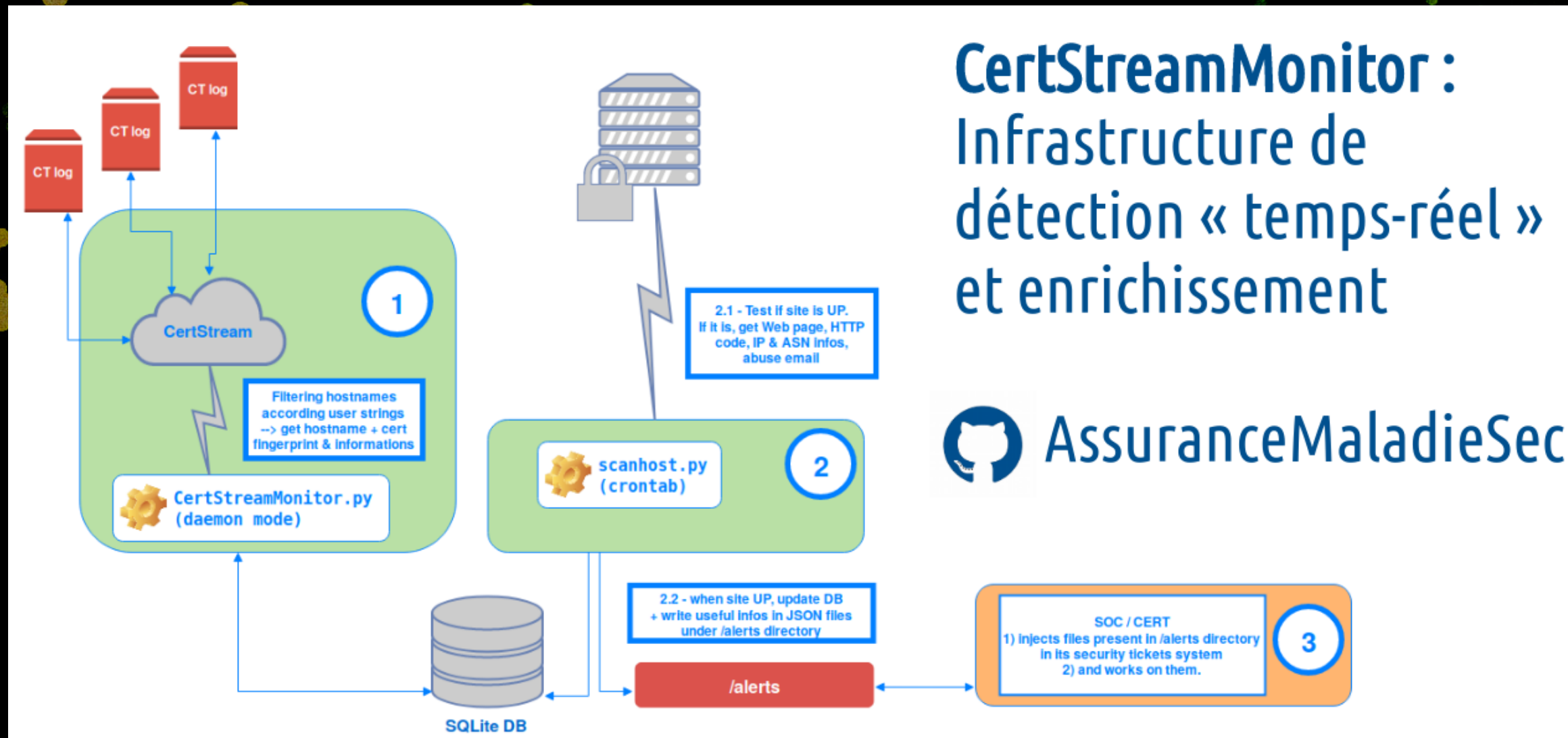
```
-o --ofile      Output CSV report file (default: ./PKHunter-report-'date'-'hou
```

```
-c --config Configuration file to use (default: ./conf/defaults.conf)
```

<https://github.com/t4d/PhishingKitHunter>

:: CertStreamMonitor ::

Parsing real-time Certificate Transparency logs to detect impersonation/typo squatting



CertStreamMonitor :
Infrastructure de
détection « temps-réel »
et enrichissement

 AssuranceMaladieSec

→ Strings detection
→ Enrichment
→ SQLite storage

..:StalkPhish :.

Parsing several dedicated phishing OSINT feeds.
Searching for specific strings

Download Phishing Kit sources (.zip)

- Strings search
- Enrichment
- Get phishing kit sources (.zip)
- Extract exfiltration Email
- SQLite storage

```
$ ./StalkPhish.py -c conf/example.conf -G -N

_ _ _ _ _
/_|_| |   ||| | _ \|| | ( ) | |
| ( _ | | _ _ | | | _ |_) | | _ _ | |
\_ \ | _ / ` | | | / / _ \| ' _ \ | ' _ \
_ ) | | ( _ | | < | | | | | \_ \ | |
|_/ \_\_,_|_|_|_\_| | | |_|_|_|_|_|_|

-= StalkPhish - The Phishing Kit stalker - v0.9.8-2 -=

2019-06-18 20:56:52,818 - StalkPhish.py - INFO - Configuration file to use: conf/example.conf
2019-06-18 20:56:52,818 - StalkPhish.py - INFO - Database: ./test/db/StalkPhish.sqlite3
2019-06-18 20:56:52,818 - StalkPhish.py - INFO - Main table: StalkPhish
2019-06-18 20:56:52,819 - StalkPhish.py - INFO - Investigation table: StalkPhishInvestig
2019-06-18 20:56:52,819 - StalkPhish.py - INFO - Files directory: ./test/files/
2019-06-18 20:56:52,819 - StalkPhish.py - INFO - Download directory: ./test/dl/
2019-06-18 20:56:52,819 - StalkPhish.py - INFO - Declared Proxy: socks5://127.0.0.1:9050

2019-06-18 20:56:52,819 - StalkPhish.py - INFO - Starting trying to download phishing kits sources..
2019-06-18 20:56:55,086 - download.py - INFO - [200] http://donnarogersimagery.com/wp-includes/pomo/
2019-06-18 20:56:56,925 - download.py - INFO - Alibaba Manufacturer Directory - Suppliers, Manufactu
2019-06-18 20:56:56,934 - download.py - INFO - trying http://donnarogersimagery.com/wp-includes.zip
2019-06-18 20:57:00,663 - download.py - INFO - trying http://donnarogersimagery.com/wp-includes/pomo
2019-06-18 20:57:04,709 - download.py - INFO - trying http://donnarogersimagery.com/wp-includes/pomo
2019-06-18 20:57:12,643 - download.py - INFO - [DL ] Found archive, downloaded it as: ./test/dl/http
2019-06-18 20:57:12,677 - download.py - INFO - [Email] Found: shaddyokoh@hotmail.com
[...]
```

<https://github.com/t4d/StalkPhish>
<https://StalkPhish.io> (Free access API)



:: PhishingKit-Yara-rules ::

```
1 rule PK_Chase_Xbaltiv3 : Chase
2 {
3     meta:
4         description = "Phishing Kit impersonating Chase bank"
5         licence = "GPL-3.0"
6         author = "Thomas 'tAd' Damonville"
7         reference = "https://stalkphish.com/2021/04/22/scammer_vs_scammer_backdoored_phishing_kit/"
8         date = "2021-04-21"
9         comment = "Phishing Kit - Chase Bank - XBalti V3"
10
11     strings:
12         // the zipfile working on
13         $local_file = { 50 4b 03 04 }
14         // specific directory found in PhishingKit
15         $spec_dir = "XBALTI"
16         // specific files found in PhishingKit
17         $spec_file = "desktopnight.jpeg"
18         $spec_file2 = "loststyle.css"
19         $spec_file3 = "Email.php"
20
21     condition:
22         // look for the ZIP header
23         uint32(0) == 0x04034b50 and
24         $local_file and
25         $spec_dir and
26         all of ($spec_file*)
27 }
```

For phishing kit sources .zip triage
No need to unzip
+320 rules available (07/22)

681f47842e9c4bcf361f16fe747c8e751dceb4bd023c6e86dce944c13a02b6d3

15 engines detected this file

681f47842e9c4bcf361f16fe747c8e751dceb4bd023c6e86dce944c13a02b6d3

out.zip

zip

DETECTION DETAILS RELATIONS COMMUNITY 2

Crowdsourced YARA Rules

Matches rule PK_O365_Spin from ruleset PK_O365_Spin at https://github.com/t4d/PhishingKit-Yara-Rules

Phishing Kit impersonating Office 365

Engine	Detection	Engine
Ad-Aware	Trojan.GenericKD.43785045	Arcabit
Avast	HTML.PhishingAdo-Gk [Phish]	AVG
Baidu	Multi.Threats.InArchive	BitDefender
Emisoft	Trojan.GenericKD.43785045 (B)	eScan
FireEye	Trojan.GenericKD.43785045	GOdata
Ikarus	Trojan-Spammer.ComCast	MAX
McAfee-GW-Edition	Artemis	Sophos AV
Sophos ML	PhishPhish-BMM	AegisLab

Ruleset: PK_O365_Spin

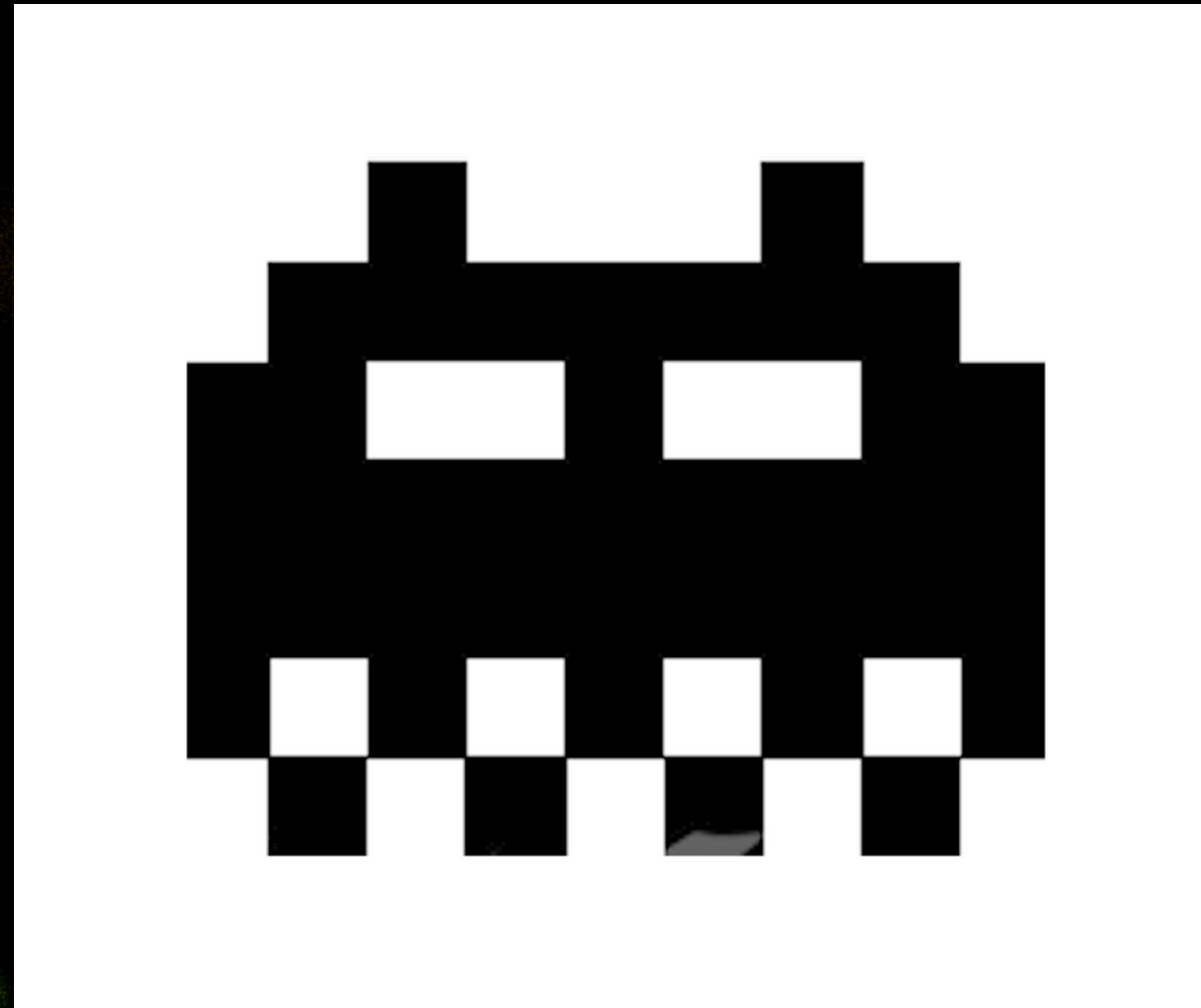
https://github.com/t4d/PhishingKit-Yara-Rules

Go to matched rule Copy ruleset

```
1 rule PK_O365_Spin : Office365
2 {
3     meta:
4         description = "Phishing Kit impersonating Office 365"
5         licence = "GPL-3.0"
6         author = "Thomas 'tAd' Damonville"
7         reference = ""
8         date = "2020-09-27"
9         comment = "Phishing Kit - O365"
10
11     strings:
12         // the zipfile working on
13         $zip_file = { 50 4b 03 04 }
14         // specific directory found in PhishingKit
15         $spec_dir = "do"
16         // specific files found in PhishingKit
17         $spec_file = "spin.php"
18         $spec_file2 = "spin.php"
19         $spec_file3 = "pai.html"
20
21     condition:
22         // look for the ZIP header
23         uint32(0) == 0x04034b50 and
24         // make sure we have a local file header
25         $zip_file and
26         $spec_dir and
27         // check for file
28         $spec_file and
29         $spec_file2 and
30         $spec_file3
31 }
```

- Automate triage
- Identify target
- Identify kit
- Available through VirusTotal

Hackito Ergo Sum 2022



Resurrect!

...end 2022...

<https://2022.hackitoergosum.org>