.: 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
               | DOMAIN registrar: ASCIO TECHNOLOGIES, INC. DANMA
               | 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 Rechenzentru
               | DOMAIN creation date: None found
               | DOMAIN expiration date: None found
697475it [06:41, 1208.14it/s]
```

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

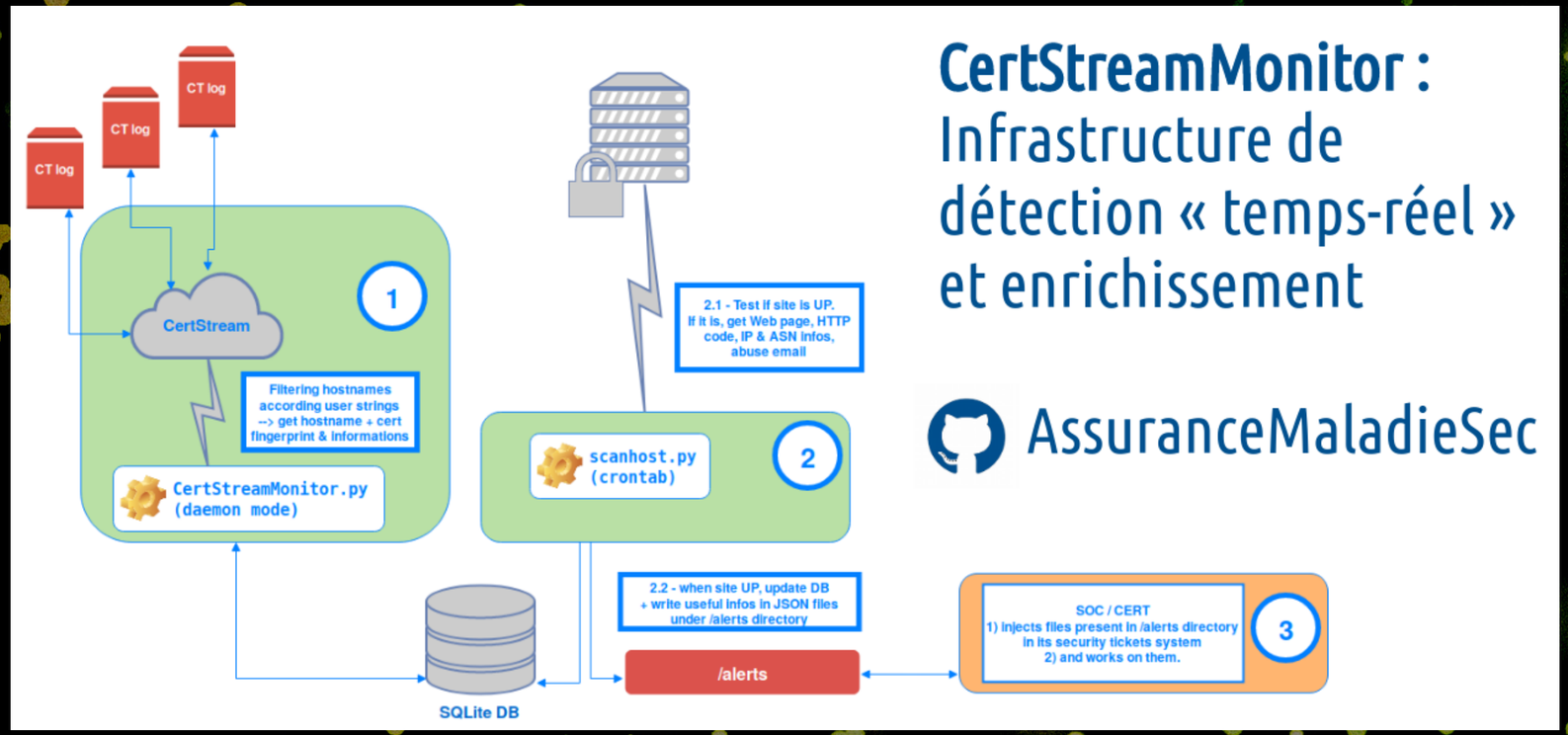
```
$ ./PhishingKitHunter.py --help

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

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

→ RegEx search
→ Enrichment
→ CSV report

https://github.com/t4d/PhishingKitHunter

.: CertStreamMonitor :.

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



→ Strings detection
→ Enrichment
→ SQLite storage

https://github.com/AssuranceMaladieSec/CertStreamMonitor

.: StalkPhish :.

```
$ ./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
[...]
```

Parsing several dedicated phishing OSINT feeds.
Searching for specific strings

Download Phishing Kit sources (.zip)

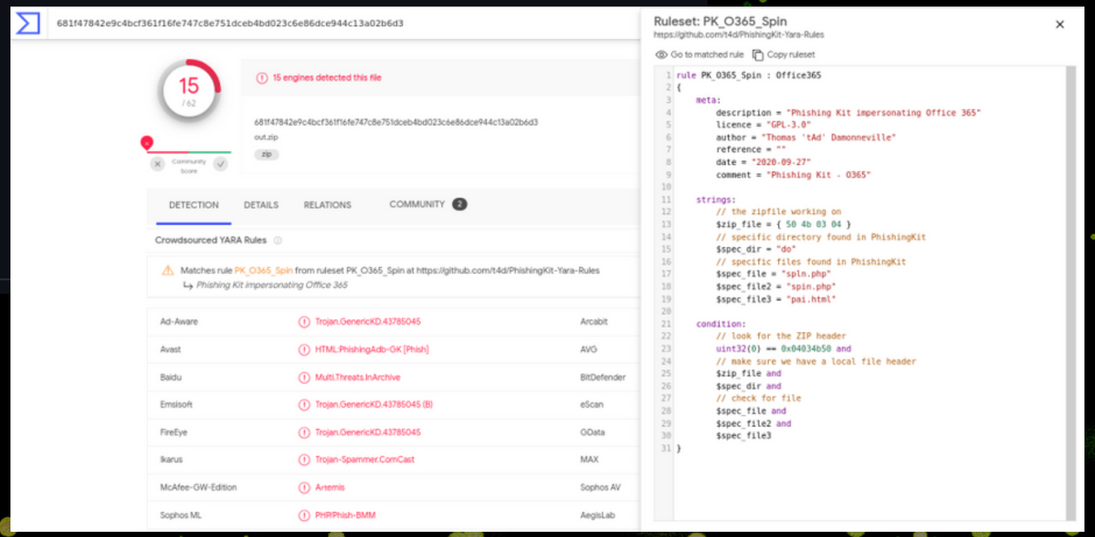
→ Strings search
→ Enrichment
→ Get phishing kit sources (.zip)
→ Extract exfiltration Email
→ SQLite storage

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

StalkPhish
- The Phishing kits stalker -

.: PhishingKit-Yara-rules :.

```yara
rule PK_Chase_Xbaltiv3 : Chase
{
    meta:
        description = "Phishing Kit impersonating Chase bank"
        licence = "GPL-3.0"
        author = "Thomas 'tAd' Damonneville"
        reference = "https://stalkphish.com/2021/04/22/scammer_vs_scammer_backdoored_phishing_kit/"
        date = "2021-04-21"
        comment = "Phishing Kit - Chase Bank - XBalti V3"

    strings:
        // the zipfile working on
        $local_file = { 50 4b 03 04 }
        // specific directory found in PhishingKit
        $spec_dir = "XBALTI"
        // specific files found in PhishingKit
        $spec_file = "desktopnight.jpeg"
        $spec_file2 = "lostyle.css"
        $spec_file3 = "Email.php"

    condition:
        // look for the ZIP header
        uint32(0) == 0x04034b50 and
           $local_file and
           $spec_dir and
           all of ($spec_file*)
}
```

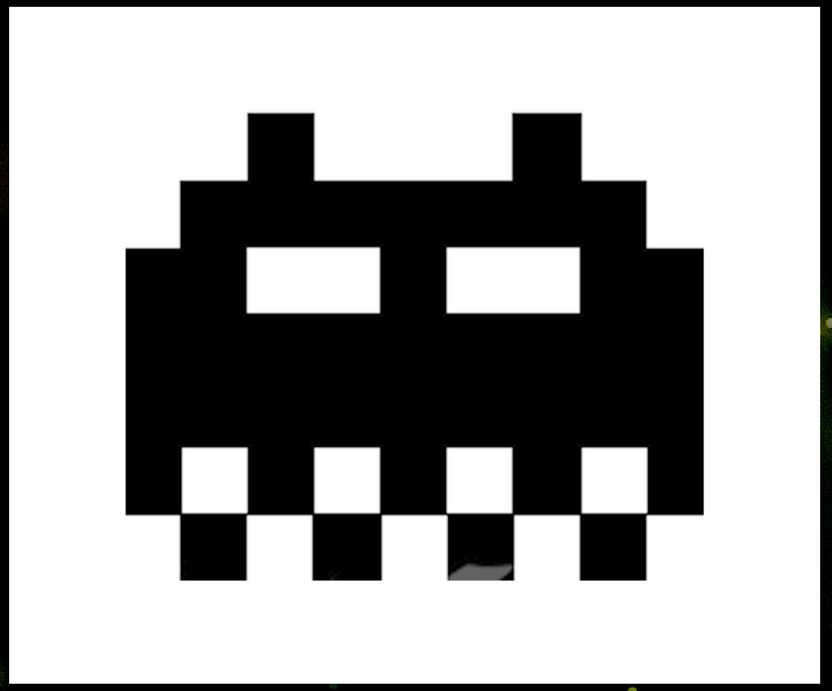


For phishing kit sources .zip triage
No need to unzip
+320 rules available (07/22)

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

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

Hackito Ergo Sum 2022



Resurrect!

...end 2022...

https://2022.hackitoergosum.org