

MALWARE INFRASTRUCTURE

Modern Malware



A LOT OF INFRASTRUCTURE IS SOMEONE ELSE'S

- Consider data on the URLHaus with a tag of “Dridex”

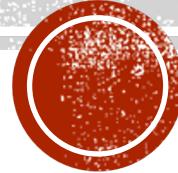
```
curl --data "tag=dridex" https://urlhaus-api.abuse.ch/v1/tag/ | jq '.urls[] | .url' | sed 's///g' > dridex.urls
```

```
"https://rogersmatrizes.com.br/wp-includes/js/tinymce/skins/lightgray/0ywfppLsJ8j.php"
"https://rodrigoreismumu.com.br/manager/bower_components/colorbox/example3/images/RJ1iTDbR.php"
"https://social.bazarpoint.com.bd/themes/FBCLONE/javascript/slick/fonts/qw98g8EaT.php"
"https://demo.perfumegardenofficial.com/wp-content/plugins/contact-form-7/includes/block-editor/LCEhx4RCcQGA.php"
"https://ana.aulasdigitais.site/wp-content/plugins/elementor/data/base/wEsBZ3Z2sCG5.php"
"https://store2.phptasks.com/bundles/sonatacore/vendor/components-font-awesome/css/NiPgMv49W.php"
"https://braincase.lechicprix.com/wp-content/plugins/contact-form-7-to-database-extension/Spout-2.7.1/Autoloader/dezxckulk.php"
"https://saudagar.pk/wp-content/themes/twentytwentyone/template-parts/content/jupJixGzH.php"
"https://sutekh.org.au/wp-content/plugins/twitter/src/Twitter/H1M88hE5.php"
"https://boletas.sanpan.cl/boletas/B4nG0074L2fJIyX.php"
"https://arabictv.ml/catalog/controller/payment/mollie-api-client/build/YS0LfExPc7MJU3.php"
"https://airefriodehonduras.com/wp-includes/sodium_compat/namespaced/Core/ChaCha20/5tqC1SAgLV2.php"
"https://southerntechroofinginc.com/wp-content/plugins/sucuri-scanner/inc/css/9m6wF7L633bpNRa.php"
"https://decambra.com/zphoto/zp-core/zp-extensions/common/adGallery/HJFYQJVQ9x0.php"
"https://legalmongolia.com/blog.example.com/font-awesome/css/nXJjANzDP882N0N.php"
"https://thewalkingdads.eu/wp-content/plugins/shortcodes-ultimate/includes/config/r0L08po3PpD2q.php"
"https://exquisitelycrafted4u.com/wp-includes/js/tinymce/skins/lightgray/ujVJoiXEkzJzah.php"
"https://aspilosel1IFH0aia.cf1IFH0s1IFH0erVer3.net/wp-content/plugins/pol1IFH0ylang/js/build/ek117gBgoNad.php"
"https://mobartec.com.br/loja/wp-content/plugins/jetpack/3rd-party/0vqJDBtlli.php"
```



HARVESTING THE OPEN WEB

Introducing SubCrawl



SUBCRAWL

```
*****      **      *****      **
**//**      **      **//**      **
/**      **      **/**      **      **      /**
*****/**      **//*****/**      //****/*      //****/*      //**      * /**      /**
//****/**      /**//**//**/**      /** /      *****      /** ***/**      /**
/**/**      /**/**      /**/**      **/**      **//**      /**//**      /**
***** //*****/**      //*****/**      //*****/**      //*****/**      /**
//**** //**** //**** //**** //**** //**** //**** //**** //**** //**** //
~~ Harvesting the Open Web ~~
```

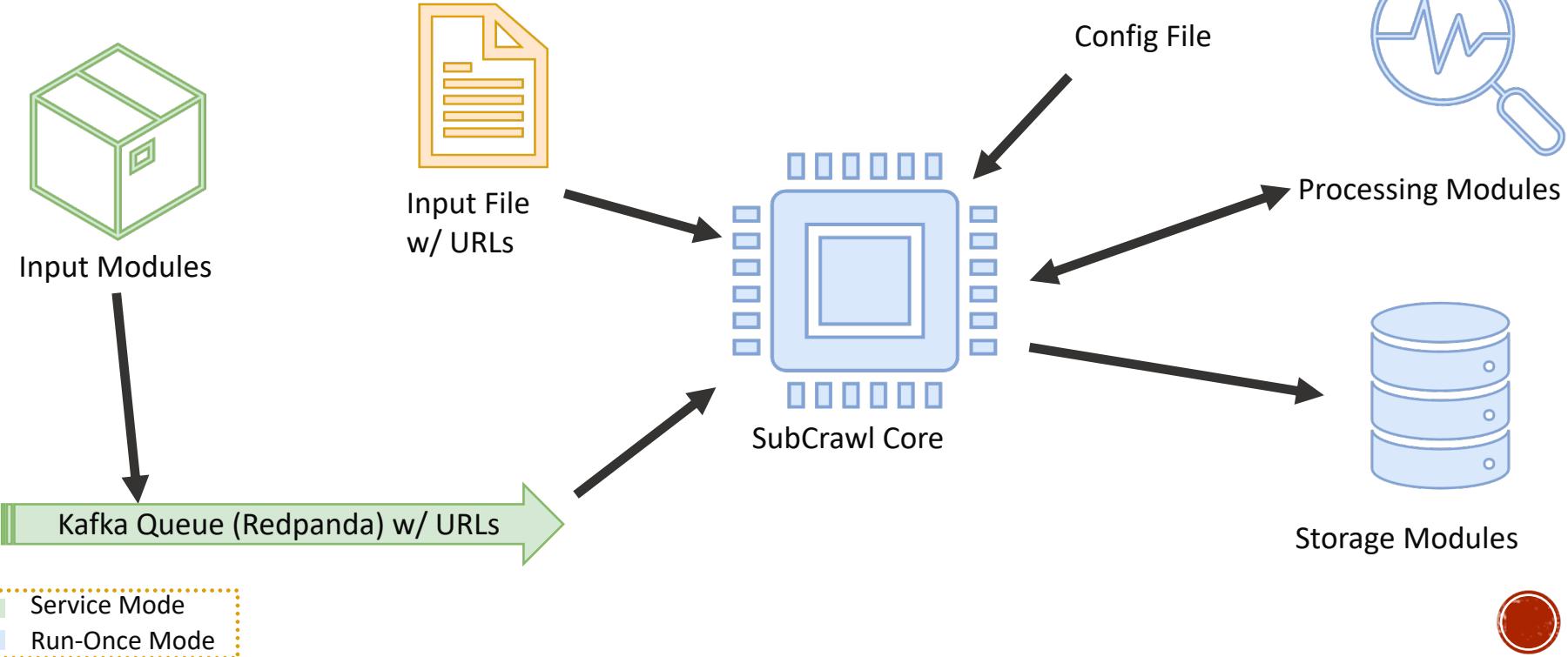


```
2021-07-22 11:02:02,029 - SubCrawl - INFO - [ENGINE] Loaded storage module: ConsoleStorage
2021-07-22 11:02:02,031 - SubCrawl - INFO - [ENGINE] Loaded processing module: PayloadProcessing
2021-07-22 11:02:02,031 - SubCrawl - INFO - [ENGINE] Loaded processing module: YARAProcessing
2021-07-22 11:02:02,033 - SubCrawl - INFO - [ENGINE] Parsing input sources...
2021-07-22 11:02:02,034 - SubCrawl - INFO - [ENGINE] Using file input for URL processing...
2021-07-22 11:02:02,041 - SubCrawl - INFO - [ENGINE] Found 98 hosts to scrape
2021-07-22 11:02:02,057 - SubCrawl - INFO - [ENGINE] Done parsing URLs, ready to begin scraping 98 hosts and 509 URLs... starting in 10 seconds!
```

- SubCrawl was created to ease the discovery and analysis of content found through open directories
- Developed by Josh Stroschein & Patrick Schlapfer
- Available on Github - <https://github.com/hpthreatresearch/subcrawl>



HOW SUBCRAWL WORKS



PHISHING KITS

https://jbshtl.secure52serv.com/receipt/secureNetflix/f742d4fee34402a2a5191867974109f2/login

https://jbshtl.secure52serv.com/receipt/secureNetflix/adminpanel.php

User Login

user Login : karam@ahmed.com

Password Login : asdasdasd

system : Windows 10

browser : Chrome/91.0.4472.124 Safari/537.36

Ip Adress : 81.218.45.215

Date Time : 15-07-2021 02:22:52pm

WEB SHELLS

- Webshells are often used to maintain access to a compromised site
 - Usually encounter two setups – password protected or open
- Even if password-protected, the response can be hashed and tracked
 - For example, we've found overlap in the use of shells by Dridex, Trickbot and Qbot operators



>>

Parent Directory	-	
3ZqjzXa1Mc.php	2021-05-24 09:53	24K
E0RQXxs69gbYW0	2021-07-07 13:06	16K
ITRFiaEIC	2021-07-05 09:27	112K
N54Np7SDz	2021-07-05 11:46	331K
OfkM7yOWPvD.txt	2021-07-05 11:46	4.2K
RvYtGgg6.txt	2021-07-07 13:06	351
erOCV1q9.txt	2021-07-05 09:26	3.5K
field.php	2021-05-24 09:53	27K
imagesloaded.pkgd.js	2021-05-24 09:53	28K
imagesloaded.pkgd.mi..>	2021-05-24 09:53	8.2K
jquery.fitvids.js	2021-05-24 09:53	3.3K
jquery.fitvids.min.js	2021-05-24 09:53	2.0K
ID82qV4GylN2	2021-07-05 09:26	12K
ITnV8lnh.php	2021-05-24 09:53	24K
packery.pkgd.js	2021-05-24 09:53	83K
packery.pkgd.min.js	2021-05-24 09:53	33K
pikaday.css	2021-05-24 09:53	4.5K
pikaday.jquery.js	2021-05-24 09:53	1.5K
pikaday.jquery.min.js	2021-05-24 09:53	738
pikaday.js	2021-05-24 09:53	39K
pikaday.min.js	2021-05-24 09:53	15K
slick.js	2021-05-24 09:53	87K
slick.min.js	2021-05-24 09:53	42K
uujypbVfi.php	2021-05-24 09:53	23K
wMcPHXlkdY4DDq.txt	2021-07-05 09:27	2.4K
zTpVntrW5A.php	2021-05-24 09:53	24K

```
<form action="" method="post"><input type="text" name="_tv"><input type="submit" value=">>"></form>
```

WEB SHELL - ORB 2.6

Uname: Linux remnux 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64
User: 33 (www-data) **Group:** 33 (www-data)
Php: 7.2.24-0ubuntu0.18.04.7 **Safe mode:** OFF [phpinfo] **Datetime:** 2021-07-22 14:48:22
Hdd: 48.96 GB **Free:** 24.28 GB (49%)
Cwd: /var/www/html/ drwxr-xr-x [home]

Windows-1251
Server IP: 127.0.0.1
Client IP: 127.0.0.1

[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Network] [Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[.]	dir	2021-07-22 14:48:05	remnux/remnux	drwxr-xr-x	R T
[..]	dir	2020-07-19 20:18:48	root/root	drwxr-xr-x	R T
api.inc.php	254.77 KB	2021-07-21 10:25:43	remnux/remnux	-rw-r-xr-x	R T E D
inflammation.php	18.53 KB	2021-07-21 23:50:26	remnux/remnux	-rw-r-xr-x	R T E D
live.php	17.25 KB	2021-07-21 10:23:53	remnux/remnux	-rw-r-xr-x	R T E D
shell.php	64.48 KB	2021-07-22 14:48:05	remnux/remnux	-rwxr-xr-x	R T E D

Copy

Change dir:

/var/www/html/

Make dir: (Not writable)

Execute:

Read file:

Make file: (Not writable)

Upload file: (Not writable)

Browse... No file selected.

DR0VV SCR1DTC

185.186.142.59

[Regular View](#)[Raw Data](#)[History](#)

// TAGS: self-signed

// LAST UPDATE: 2021-07-21

General Information

Hostnames **domain.com**

Domains **DOMAIN.COM**

Country **Russian Federation**

City **Moscow**

Organization **Business Consulting LLC**

ISP **Kontel LLC**

ASN **AS204490**

Open Ports

22**80****123****443**

// **22** / TCP

[22277934](#) | 2021-07-02T01:36:34.986668

OpenSSH 7.4p1 Debian 10+deb9u7

SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7

Key type: ssh-rsa

Key: AAAAB3NzaC1yc2EAAAQABAAQCKqivx0azIgfYWbcd0csc01AaWlYsHERA8GHfGYhHv1Dd

85xzG/tQK9MvDqEx1WIBVMwdMBRrrWgLGjx/AwXPPV+mkRL6axyYA6T/C20L17La080jVwfBPMDTGNIP548VHUN9n67HwCMyIb0f027RzJ27KBsa25XYzons7idR7rj4QUqgLAykS/JL8eArTIZ0GdUr6fwLYmj7sh64nJCYuboG4L/Dh++NZJ0TgAuid81N/axzzXnOSFj718q6AMwZ9CGpU4h5c3kgjh
b9hmuIVMPDM1YesAqTQEJNi3uf1cLPT84P1Brota+4Ktxz0odbyfuD16FrfrQPwfHAV

Fingerprint: 16:81:ca:c0:12:79:1c:9a:79:2f:bd:b5:2d:10:25:75

Key Algorithm:

C2 PANELS

- Panels are also very common for commodity malware
 - Deploy a trojan
 - Manage through the panel – to include stolen data
- Can find the panel in a ZIP from time to time...
 - Lokibot is one of the most common
 - Pony is as well
 - Other panels: Azorult, BlackNET, AgentTesla, Formbook, Raptor, Gomorrah, CythosiaV2, Hydra and a number of unknown
- In case you were wondering, most kits come with a self-installer/setup



GOMORRAH BOT PANEL

Gomorrah Bot

admin  Logout 

Total Bots :

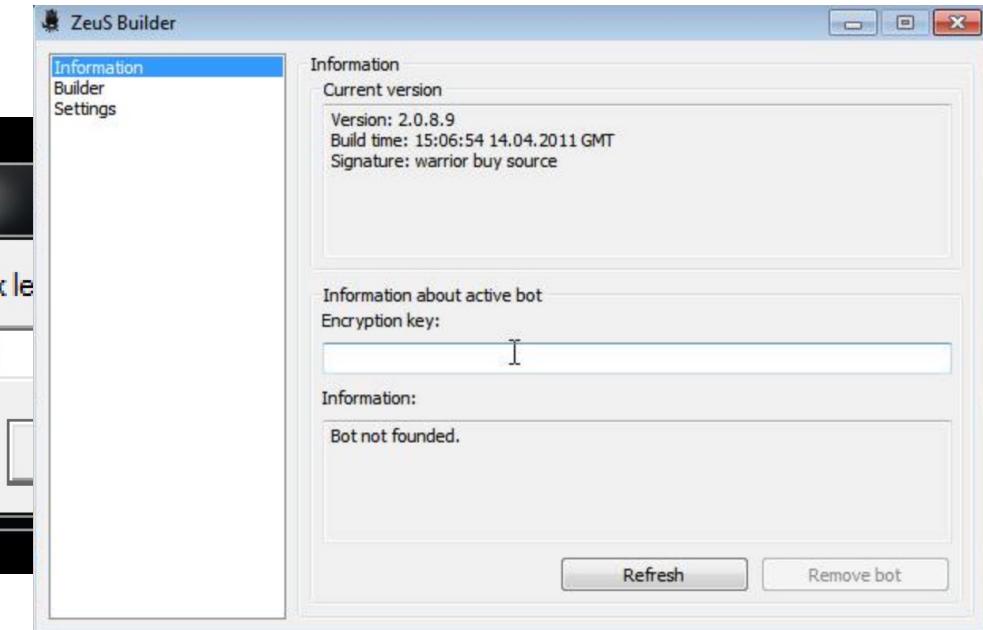
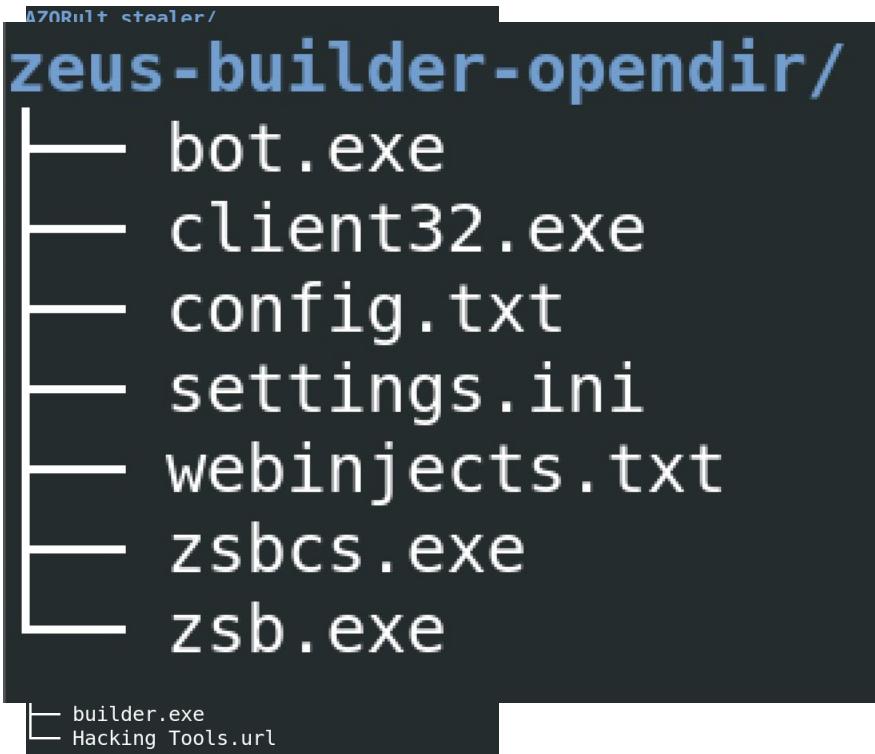
You dont have Bots or logs , Note : you need wait 10 to 15 minutes for all of the victims files to upload on Panel

HWID	Country	IP	Last Seen	Action

 Prev

Next 

MISCELLANEOUS



YOU FIND SOME FILES, NOW WHAT?

```
<===== 172.245.119.43 =====>
[ClamAVProcessing] Sanesecurity.Malware.27333.RtfHeur.BadVer.UNOFFICIAL( http://172.245.119.43/d/doc.doc )
[SHA256] a8680fe6b1b96489aa5331018a095d20a4a9c69f3f46bc2f9d1b011242079ba3
[PayloadProcessing] pe32+ executable (console) x86-64, for ms windows( http://172.245.119.43/d/obi.exe )
[SHA256] caff14d450514a35eac5ba34b3e74126360662d7c8fdf60a8008a0e3bb8ed0b3
[PayloadProcessing] pe32+ executable (console) x86-64, for ms windows( http://172.245.119.43/d/pdf.exe )
[SHA256] 51c392870e9f21df2154b4e68a901ca1b5d9fccdcf00a4e6fa60ef07b4dfc541
[PayloadProcessing] pe32+ executable (console) x86-64, for ms windows( http://172.245.119.43/d/sharp.exe )
[SHA256] 39c27e2a7ec3b5603e184f041bbb07196f6feb885813500fec5ac5fdefca8e1d
```

Malware URL	Status	Tags	Reporter
http://172.245.119.43/d/pdf.exe	Online	exe Formbook ↗	@abuse_ch
http://172.245.119.43/d/doc.doc	Online	opendir RTF	@abuse_ch
http://172.245.119.43/d/sharp.exe	Online	exe Formbook ↗ opendir	@abuse_ch
http://172.245.119.43/d/obi.exe	Online	exe Formbook ↗ opendir	@abuse_ch



WHAT DOES THE SANDBOX SAY?

General

Target
51c392870e9f21df2154b4e68a901ca1b5d9fccdcf00a4e6fa60ef07b4dfc541.64.exe.bin

Size
65KB

Sample

Score
10 /10

MD5
06daa4f472383226392964c70e34c376

SHA1
b47a3554b0bf7250caa0f84090fb387cb332f31b

SHA256
51c392870e9f21df2154b4e68a901ca1b5d9fccdcf00a4e6fa60ef07b4dfc541

01 caff14d450514a35eac5ba34b3e74126...

SHA256 caff14d450514a35eac5ba34b3e74126360662d7c8fdf60a8008a0e3bb8ed0b3

VIRUSTOTAL Report (45 / 69 Detections)

pe amd64 vm_protect_packer

Family formbook

Version 4.1

C2 http://www.howmucharemyrarecoinsworth.com/jn7g/

Copy all