MALWARE INFRASTRUCTURE

Modern Malware

A LOT OF INFRASTRUCTURE IS SOMEONE ELSE'S

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

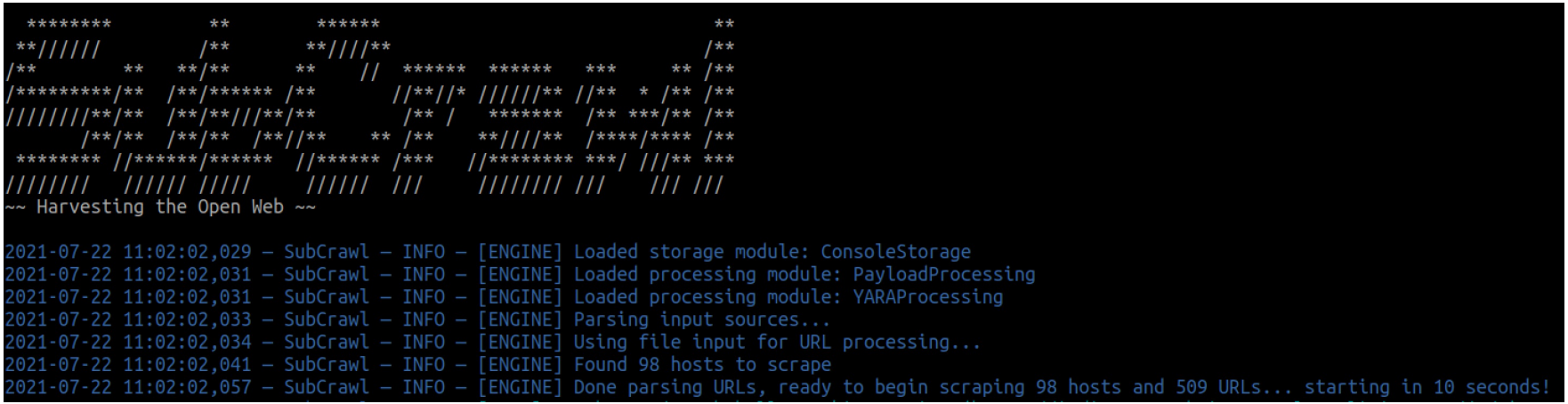
```
curl --data "tag=dridex" https://urlhaus-api.abuse.ch/v1/tag/ | jq '.urls[] | .url' | sed 's/"//g' > dridex.urls
```

```
"https://rogersmatrizes.com.br/wp-includes/js/tinymce/skins/lightgray/OywfppLsJ8j.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.sanopan.cl/boletas/B4nG0O74L2fJIyX.php"
"https://arabictv.ml/catalog/controller/payment/mollie-api-client/build/YS0LfExPc7MJU3.php"
"https://airefriodehonduras.com/wp-includes/sodium_compat/namespaced/Core/ChaCha20/5tqClSAgLV2.php"
"https://southerntechroofinginc.com/wp-content/plugins/sucuri-scanner/inc/css/9m6wF7L633bpNRa.php"
"https://decambra.com/zphoto/zp-core/zp-extensions/common/adGallery/HJFYQJVQ9xQ.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/0vqJDBttlli.php"
```

HARVESTING THE OPEN WEB

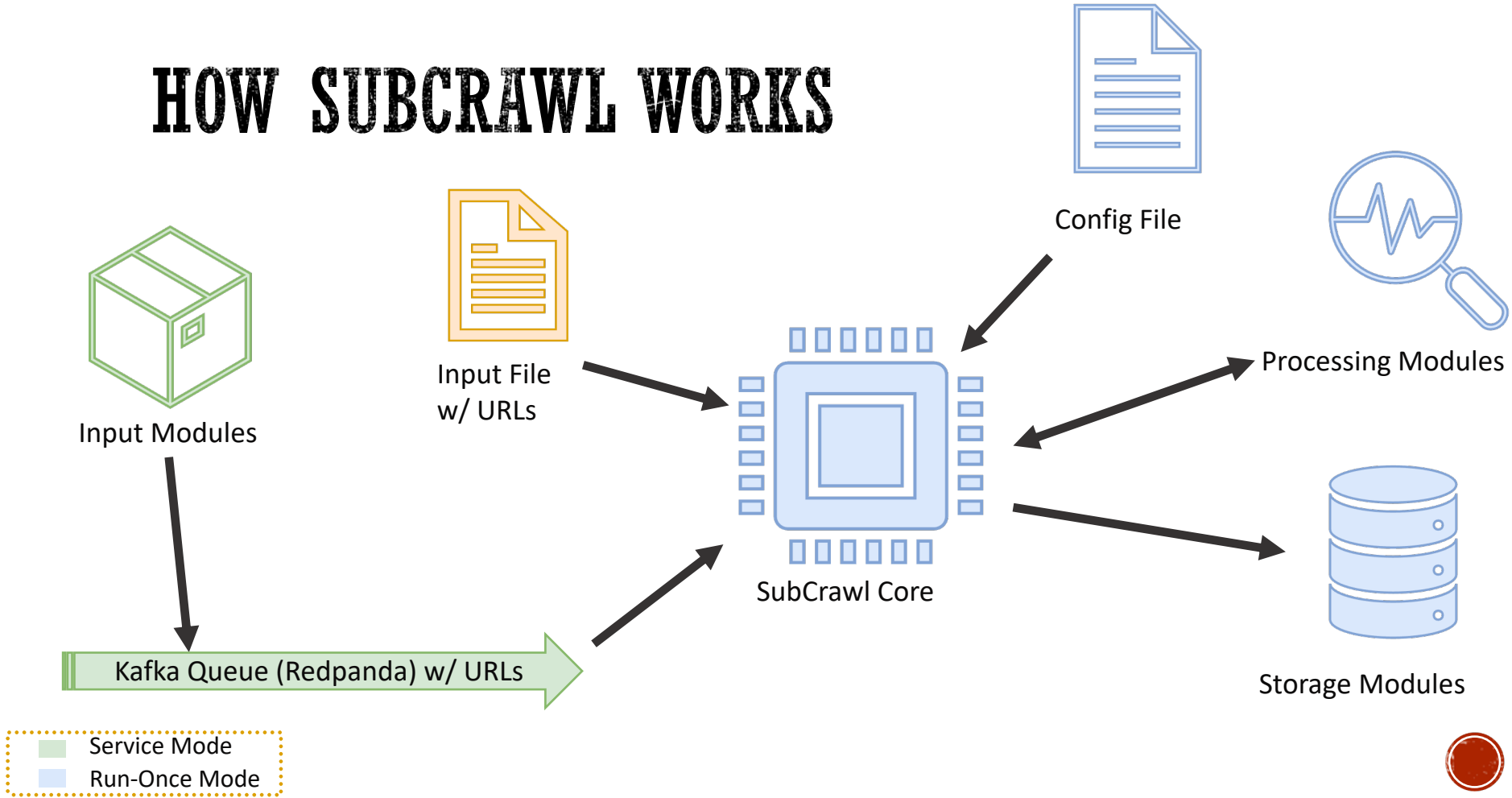
Introducing SubCrawl

SUBCRAWL



- 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

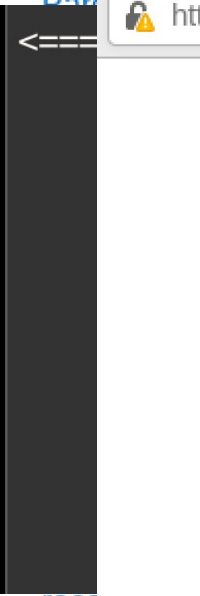
---

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



WEBSHELLS

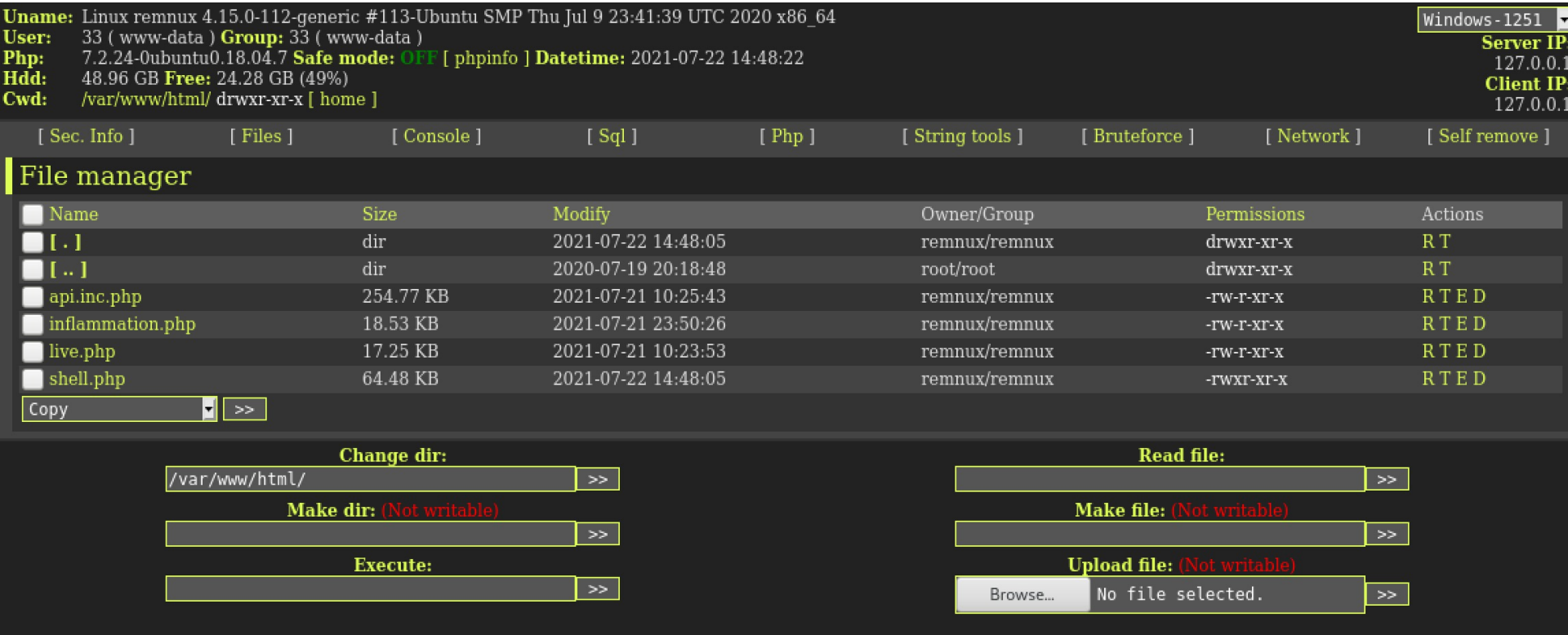
- Webshells are often used to maintain access to a compromised site
  - Usually encounter two setups – password protected or open

- 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
RvYtGgq6.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
lD82qV4GyIN2	2021-07-05 09:26	12K
lTnV8lnh.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

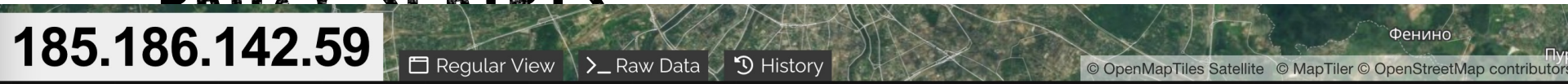
```
<form action="" method="post"><input type="text" name="_tv"><input type="submit" value=">>"></form>
```

WEBSHELL – ORB 2.6



PROXY SCRIPTS

185.186.142.59



// 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

222779344 | 2021-07-02T01:36:34.986668

OpenSSH 7.4p1 Debian 10+deb9u7

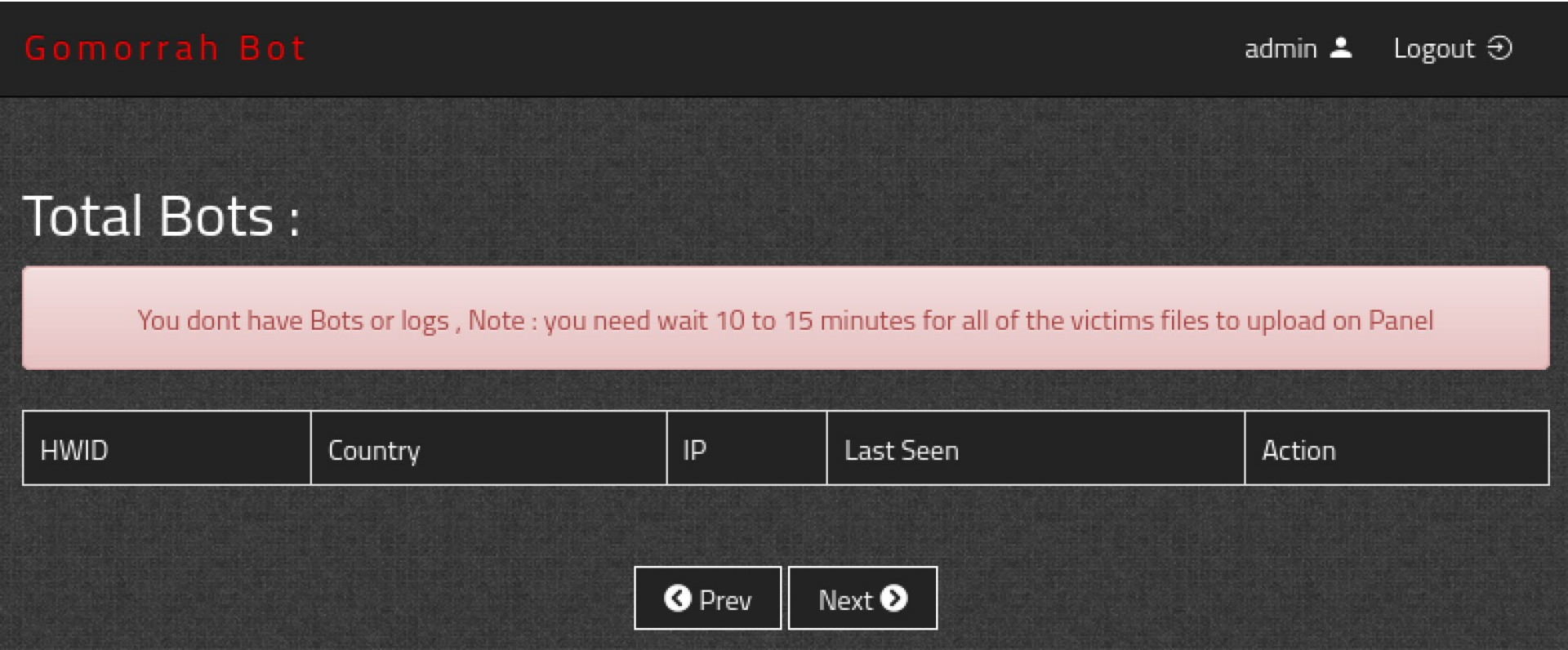
```
SSH-2.0-OpenSSH_7.4p1 Debian-10+deb9u7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCkqivx0azIgfYWBcd0csc01AaW1lYsHErA8GHfGYhHv1
Dd
85xzG/tQK9MvDqEx1WIBVMwdMBRrrWgLGjx/AwXPPv+mkRL6axyYA6T/C20L17LaO80jVWfBPMDT
GNIP548VHUN9bN67HWCMyIbOfO27RzJ27KBsa25XYzons7idR7Rj4QUqgLAykqS/JL8eArTIZOGd
Ur6fwlYMj7sh64nJCYuboG4L/Dh++NZJ0TgAuid81N/axzZXnOSFj718q6AMwZ9CGpU4h5c3kgjh
b9hmuIvMPDM1YesAqTGQEJNi3uf1clPT84P1BRot8a+4Ktxz0odbyfuDl6FrfQPwfHAV
Fingerprint: 16:81:ca:c0:12:79:1c:9a:79:2f:bd:b5:2d:10:25:75

Key Algorithms:
```

C2 PANELS

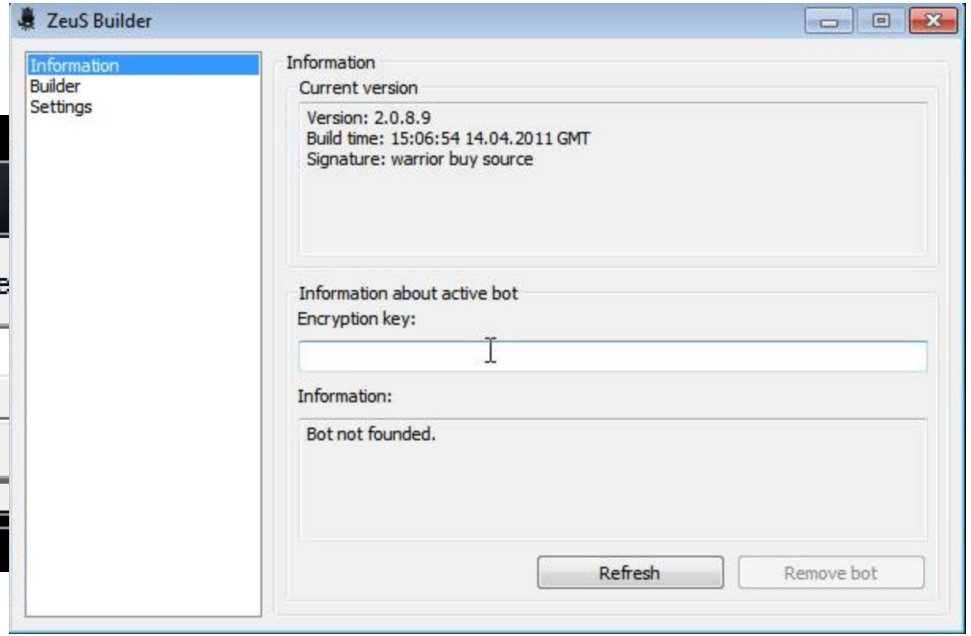
- Panels are also very common for commodity malware
  - Deploy a trojan
  - Manage through the panel – to include stolen data
- Can find the panel in a ZIP from time to time…
  - Lokibot is one of the most common
  - Pony is as well
  - Other panels: Azorult, BlackNET, AgentTesla, Formbook, Raptor, Gomorrah,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

GOMORRAH BOT PANEL



MISCELLANEOUS

```
AZORult stealer/
zeus-builder-opendir/
├── bot.exe
├── client32.exe
├── config.txt
├── settings.ini
├── webinjects.txt
├── zsbcs.exe
└── zsb.exe
├── builder.exe
└── Hacking Tools.url
```



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?