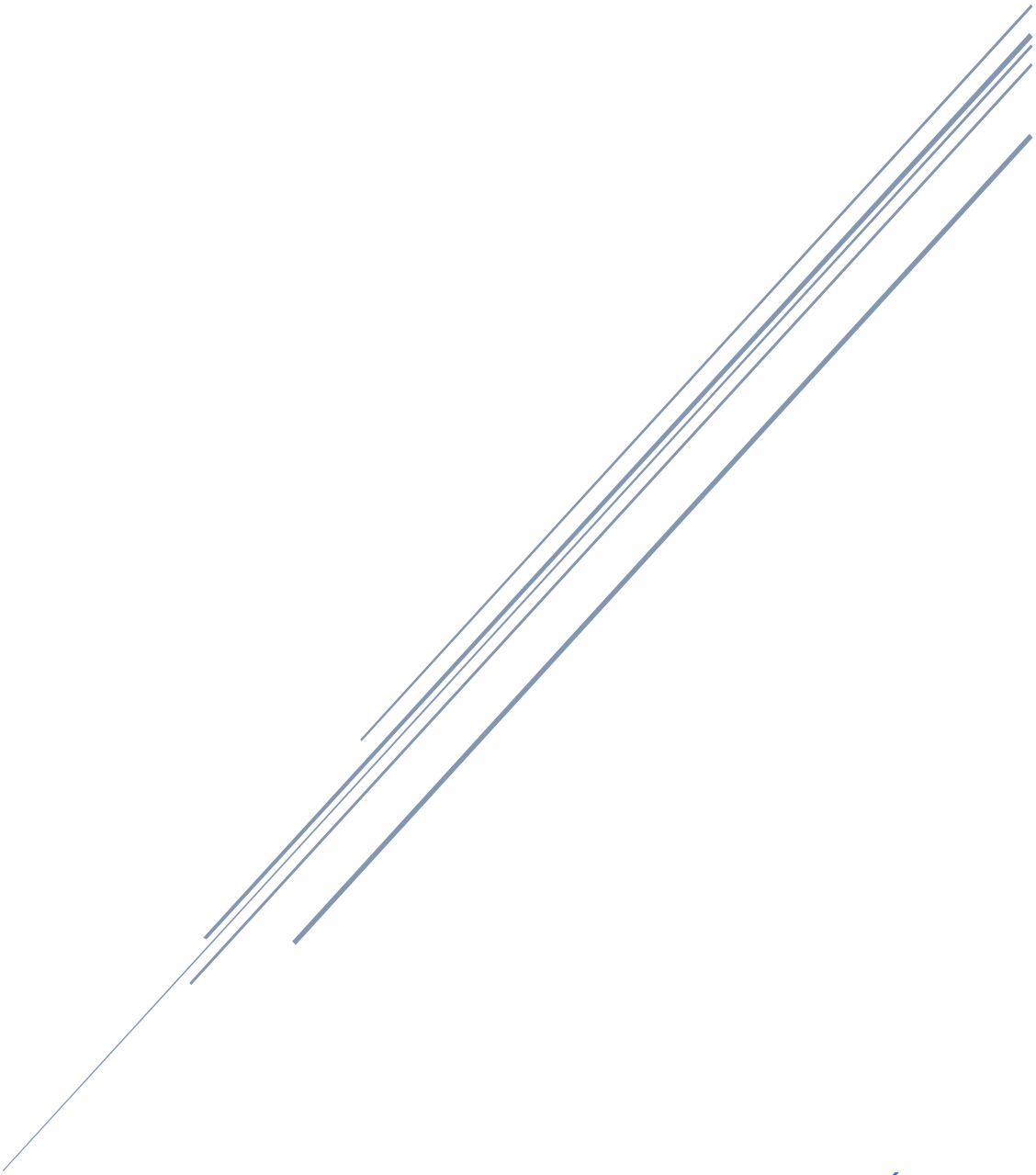
Investigar una campaña de smishing

Técnicas de investigación



El Hacker Ético
elhackeretico.com

ÍNDICE

Investigar una campaña de smishing

Una campana de envío masivo de SMS maliciosos generalizada contra usuarios de diversos países llamó mi atención.

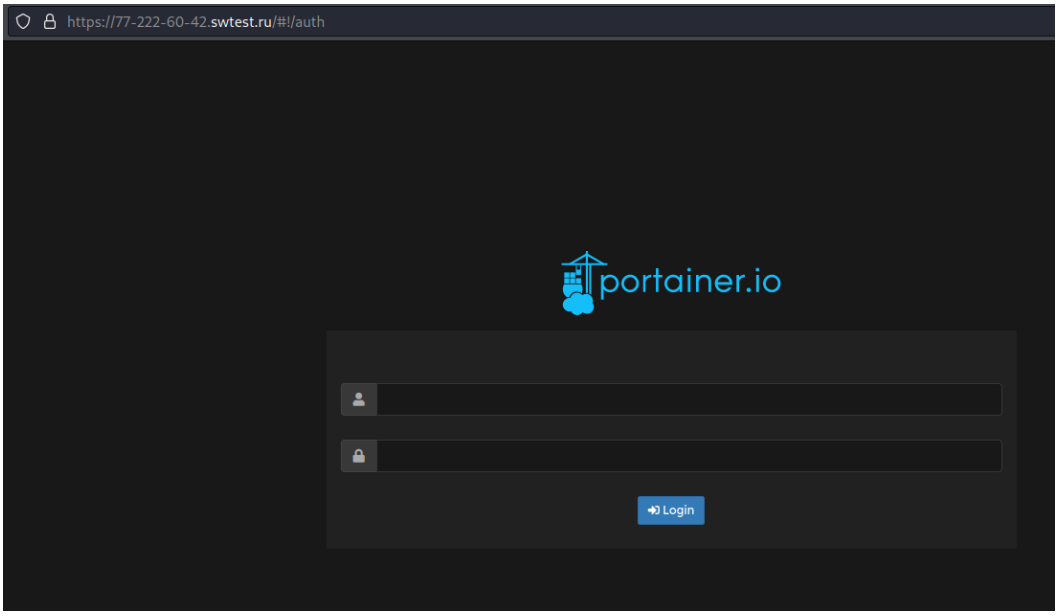
Los actores maliciosos detrás de estos envíos han creado cientos de dominios falsos, haciéndose pasar por bancos de España, Francia, Arabia Saudí, servicios de Correos, TV, entre otras empresas de servicios.

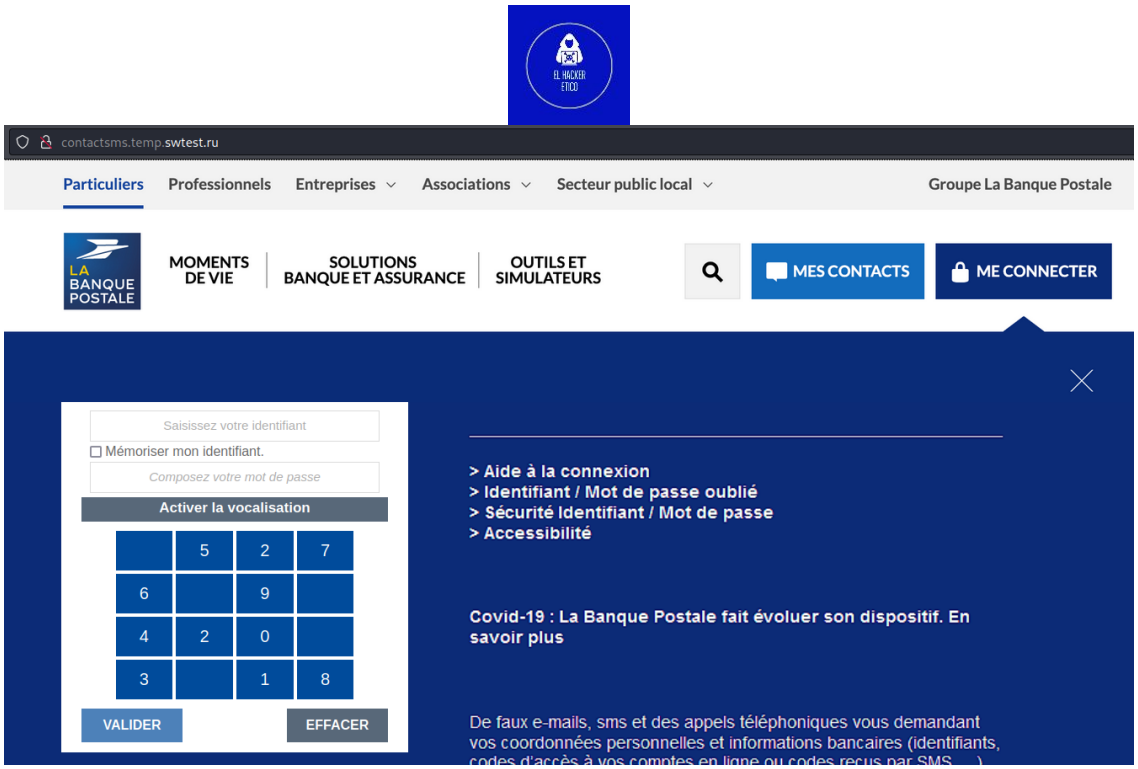
La IP en cuestión es 77.222.40.224, pertenece a SpaceWeb Ltd y en el momento de escribir este artículo tenía nombres de 398 dominios y 119 URLs.

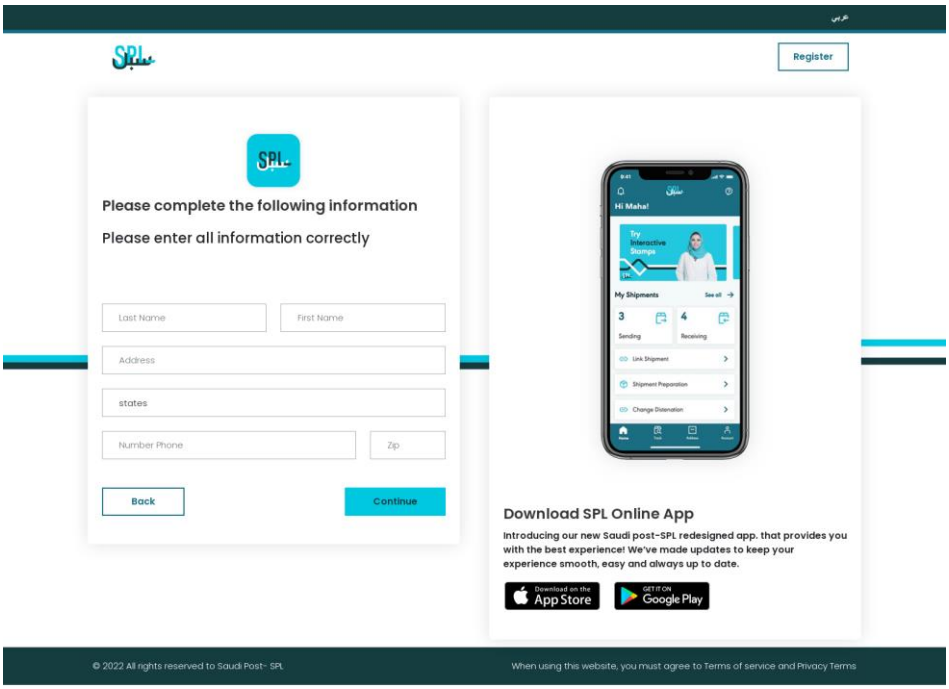
Los dominios activos alojados en esta IP incluidos DNS pasivos y dominios más antiguos, se pueden encontrar aquí.

La forma de actuar de la mayoría de estos sitios web en esta dirección IP maliciosa indica phishing, algunos de los sitios web almacenados parecen contener archivos ejecutables maliciosos de Windows, según un escaneo realizado con Virus Total.

A continuación, se adjuntan capturas de pantallas de sitios de phishing.







Técnicas de investigación

Para investigar estos dominios, podemos tomar varias rutas de investigación.

Verificar la reputación de la dirección IP

Permite conocer si estamos tratando con una amenaza conocida o es nueva. Por ejemplo, podemos verificar si la dirección IP se ha relacionado con actividades no deseadas o sospechosas, como spam. Disponemos de varias herramientas para este fin:

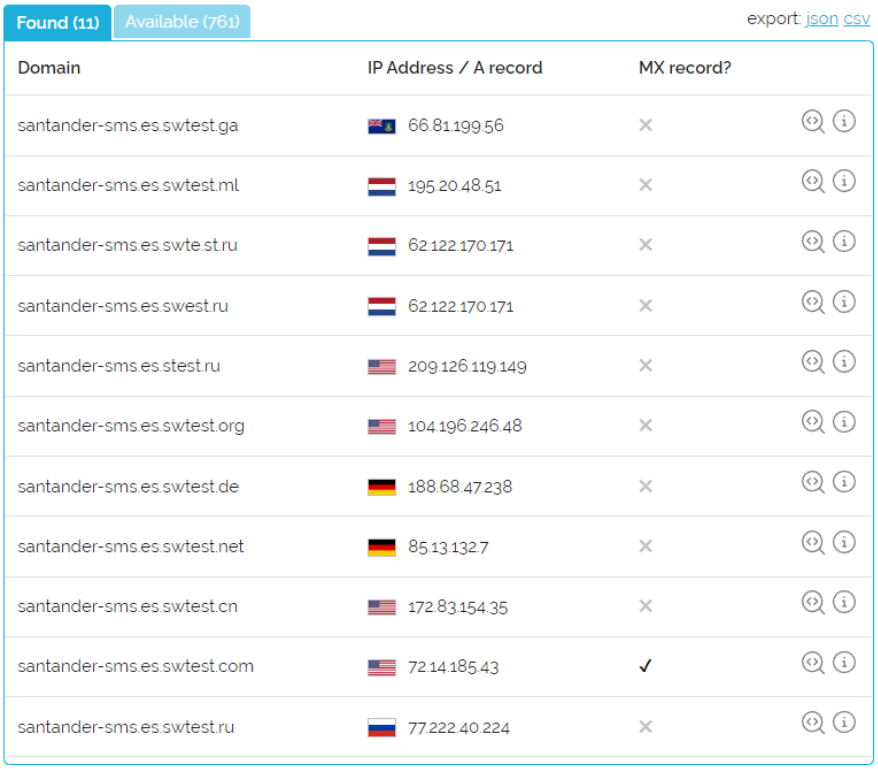
- MX Toolbox: Nos permite comparar la dirección IP investigada con listas negras conocidas. Podemos ver los resultados para la IP investigada, aquí.
- Virus Total: es una herramienta muy útil para búsquedas de direcciones IP, con información que abarca desde la reputación, DNS pasivo, whois, comentarios de la comunidad…
- Alien Vault: es una una herramienta que nos aporta indicadores e información muy detallada.
- Cisco Talos Intelligence: herramienta utilizada para comprobar las actividades asociadas a una IP.

Verificar las variaciones de DNS

Los actores maliciosos buscaran crear dominios errores tipográficos similares al dominio real para crear confusión al usuario, y engañar a las víctimas desprevenidas.

Una herramienta muy útil para esto es DNS Twister. Muy útil para alertar de dominios similares y la creación de nuevos dominios. También es otra forma de detectar campañas de phishing similares.

Vamos a ver los resultados en DNS Twister para la IP investigada.



De las 11 direcciones IP encontradas, 10 de ellas no coinciden directamente con la IP que nos encontramos investigando. Los resultados obtenidos son los siguientes:

Dirección IP	DNS Pasivo	URLs
66.81.199.56	500	8765
195.20.48.51	500	153
62.122.170.171	500	1401
209.126.119.149	58	3
104.196.246.48	407	409
188.68.47.238	500	67
85.13.132.7	260	54
172.83.154.35	500	2525
72.14.185.43	500	3350
77.222.40.224	407	123

Tenemos un total de 4132 dominios y 16850 URL utilizadas en campañas de phishing, la mayoría de ellas en la actualidad ya desactivadas y detectadas por los diferentes búscadores web.

Examinar la tecnología web

Todo sitio web, incluido aquellas páginas destinadas a fines maliciosos disponen de una tecnología para su montaje (servidor, widgets, documentos, CMS…). Para estudiar esto disponemos de una seria de herramientas web que nos puede ayudar en esta tarea.

- Awesometechstack
- Construidocon
- Netcraft

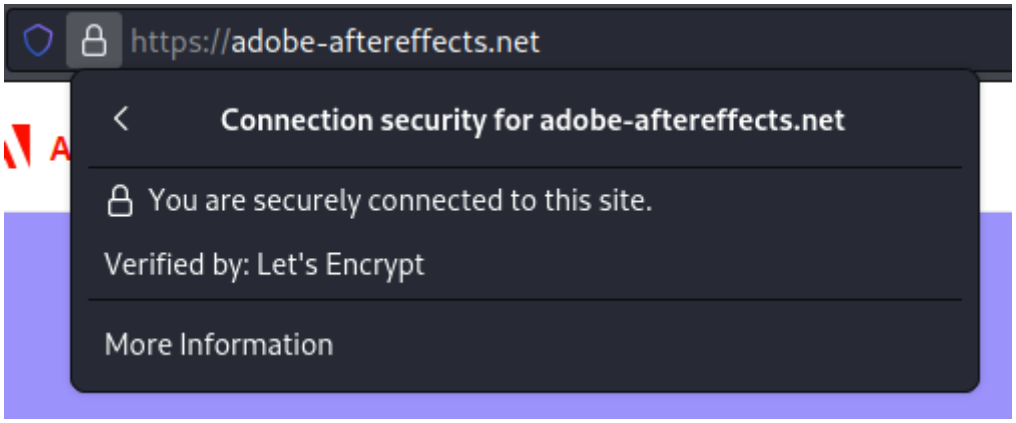
Estas comprobaciones pueden servir para comparar sitios web y poder descubrir sitios que ejecutan actividades maliciosas relacionadas.

Verificar los certificados de seguridad

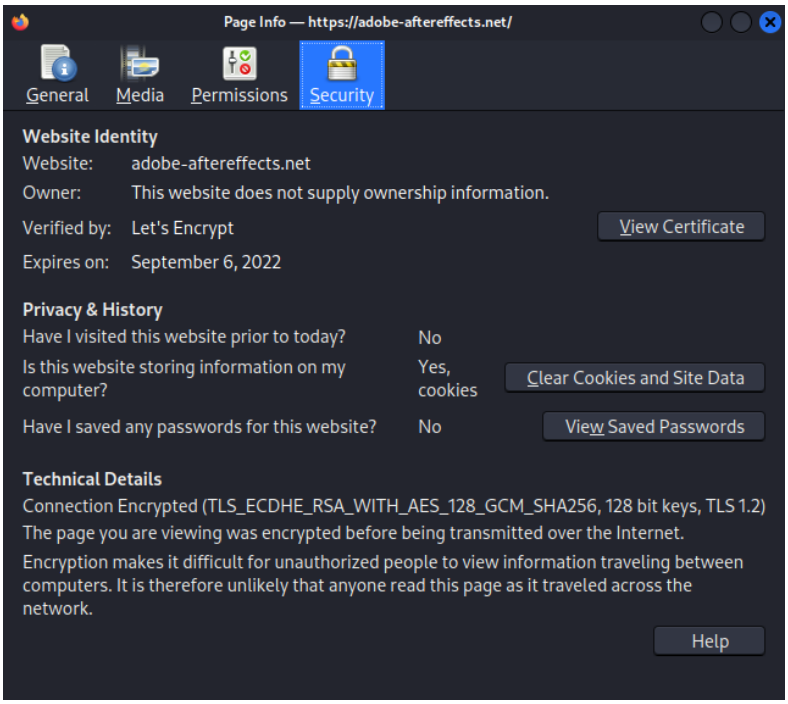
No todos los sitios web destinados a phishing disponen de conexión encriptada https, pero ya existen algunos y la cifra de sitios con conexión encriptada va a ir subiendo porque

aporta una supuesta legitimidad, ya que siguen existiendo personas que creen que el candado verde significa que el sitio web es real y seguro. Estos certificados se pueden obtener abusando de servicios gratuitos como Let's Encrypt.

Estos certificados pueden aportar información interesante, como el nombre del sujeto, emisor, validez, …



Por ejemplo, esta web no legítima que suplanta Adobe dispone de conexión https con certificado emitido por Let's Encrypt.



De esta manera podemos obtener los dominios cubiertos por el certificado y sus huellas digitales únicas.

- SHA 256
  36:B4:59:88:7A:CA:F5:97:F8:2B:68:B2:D6:22:97:57:3A:7C:BA:D4:3D:37:42:59:17:BD:90:83:80:E3:A3:17
- SHA 1
  A8:F9:D8:25:A2:70:17:0E:AC:C2:EE:EC:80:29:48:A4:BF:D8:05:FB
- Serial
  03:2E:70:E4:9A:F6:87:8D:9F:D2:F4:DC:0F:D1:77:C0:63:BE

Estos valores se pueden utilizar para verificar si el certificado es compartido por varios sitios web o IP. Para ello utilizaremos los siguientes servicios:

- Censys
- Shodan
- Crt.sh

Sintaxis para las consultas en las herramientas de búsqueda anteriores:

- Shodan: ssl.cert.serial:hash
- Crt.sh y Censys no requieren de sintaxis específica y se puede colocar el valor directamente en el campo de búsqueda.

Cálculo del hash SHA256

¿Se puede calcular este hash del contenido de un sitio web?

Los sitios web phishing suelen ser por norma general copias entre unos y otros, simple y sencillo, cuyo objetivo es el robo de credenciales. Esto también puede simplificar la tarea de investigarlos.

Nos dirigimos a una terminal de comandos y escribimos el siguiente comando:

curl http://sapeme3412.temp.swtest.ru/ | sha256sum

```
kali@kali  ~  curl http://sapeme3412.temp.swtest.ru/ | sha256sum
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  9122  100  9122    0     0  19452      0 --:--:-- --:--:-- --:--:-- 19491
ce9e071e38be113f6330865f99b64cbde2c7b80d3908f820d6dcdc46b37ccf98  -
```

El hash resultante sería:

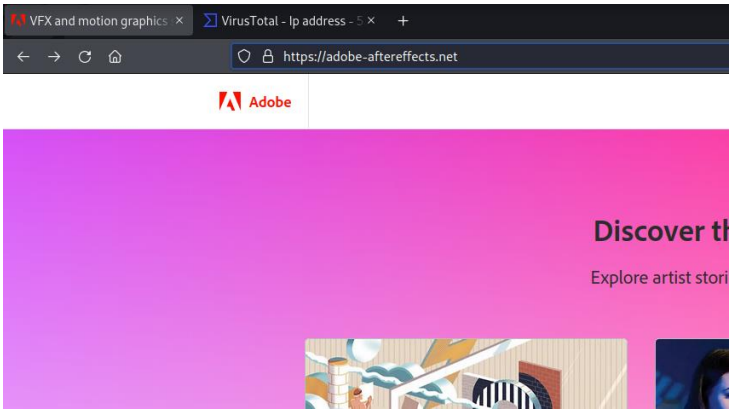
ce9e071e38be113f6330865f99b64cbde2c7b80d3908f820d6dcdc46b37ccf98

El valor de hash se puede utilizar en herramientas como Virus Total y nos devolverá multitud de resultados relacionados.

Búsqueda con Favicon.ico y Shodan

Favicon es un pequeño icono que se muestra en la ventana del navegador junto con un nombre. El propósito de este es ayudar a reconocer la marca además de ayudar al usuario a distinguir esta pestaña entre todas las que tenga abierta en el navegador.

En el caso de sitios no legítimos, se copia este icono o incluso se vincula con el original al que se intenta suplantar.



El enlace a este favicon se encuentra en el código fuente de la web. Así podemos encontrarlo en el código del sitio web que estamos investigando:

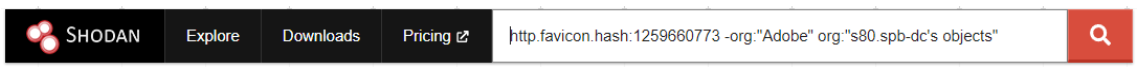
Buscar el favicon por reversing de imagen nos devolverá muchos falsos positivos. Para una búsqueda más certera, debemos utilizar algo único, el valor de hash del favicon.

Para ello, como ya hicimos anteriormente, nos dirigimos a una terminal de Linux y escribimos el siguiente script:

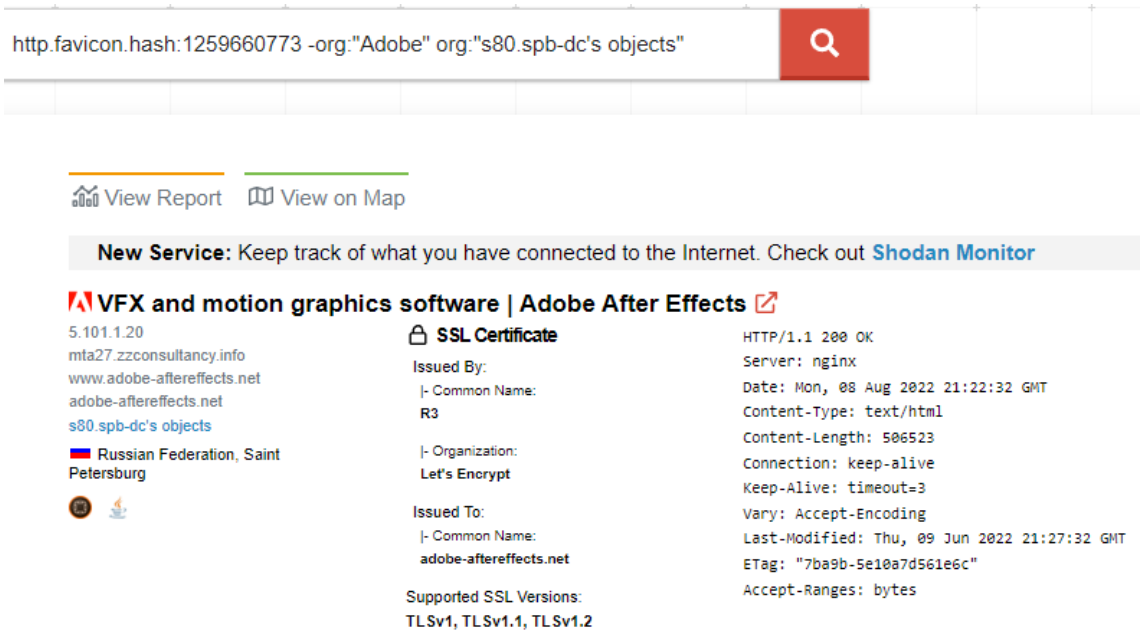
```
import requests
import mmh3
import base64

response = requests.get('https://www.adobe.com/content/dam/cc/Adobe_favicon.ico')

favicon = base64.encodebytes(response.content)

hash = mmh3.hash(favicon)

print(hash)
```

El hash resultante sería: 1259660773

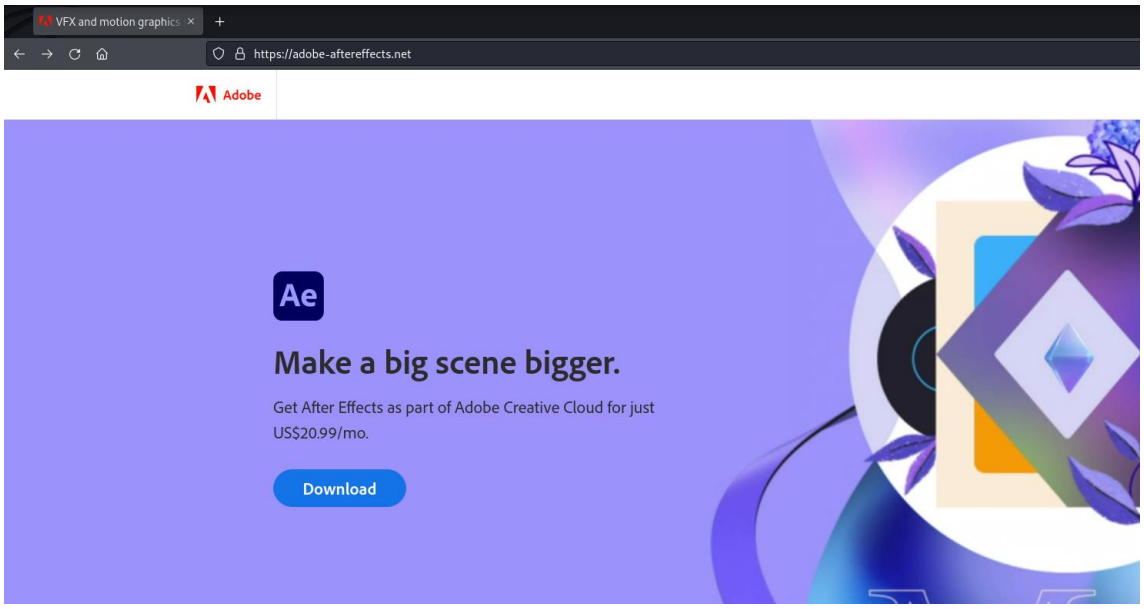
Claro, haciendo esta búsqueda nos devuelve resultados legítimos y no legítimos. El siguiente paso sería filtrar los resultados.



Buscando por organizaciones llegamos a un resultado interesante.



Abrimos la URL en nuestro entorno seguro, y vemos su contenido.



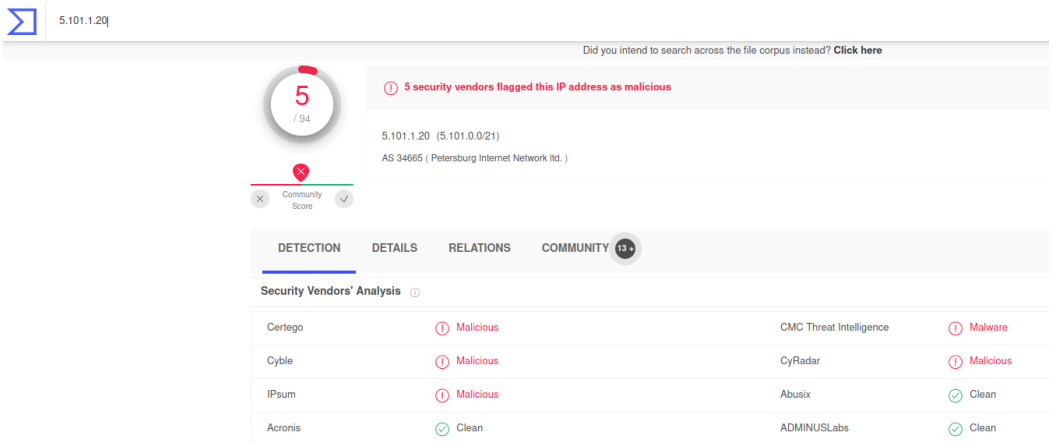
Tendríamos lo que puede ser una web legítima de la empresa Adobe .Inc. Vamos a comprobar si el dominio pertenece a Adobe con la herramienta whois.domaintools.com.

Domain Profile

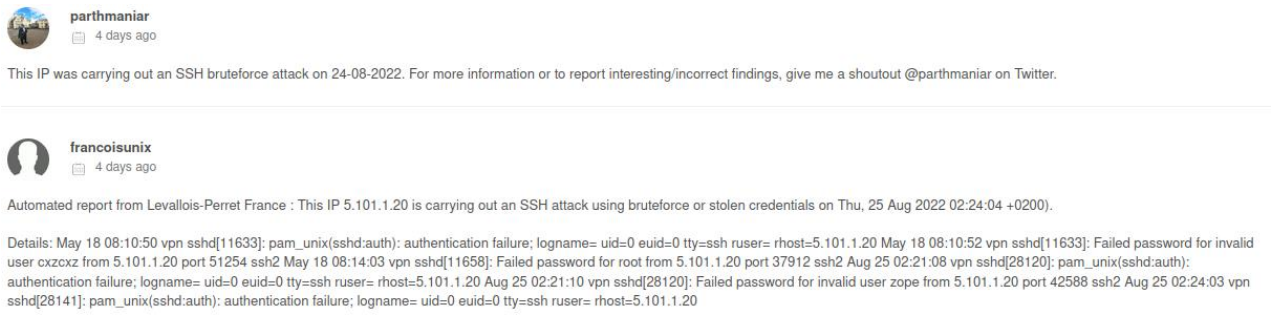
Registrant	Domain Admin
Registrant Org	Whoisprotection.cc
Registrant Country	my
Registrar	WEBCC Web Commerce Communications Limited dba WebNic.cc IANA ID: 460 URL: http://www.webnic.cc,http://https://www.webnic.cc Whois Server: whois.webnic.cc compliance_abuse@webnic.cc (p) 60389966799
Registrar Status	ok
Dates	82 days old Created on 2022-06-08 Expires on 2023-06-08 Updated on 2022-06-08
Name Servers	A.DNSPOD.COM (has 115,053 domains) B.DNSPOD.COM (has 115,053 domains) C.DNSPOD.COM (has 115,053 domains)
Tech Contact	Domain Admin Whoisprotection.cc L4-E-2, Level 4, Enterprise 4, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Wilayah Persekutuan, 57000, my tec_19923009@whoisprotection.cc (p) 60389966788 (f) 60389966788
IP Address	5.101.1.20 - 79 other sites hosted on this server
IP Location	- Sankt-peterburg - Sankt-peterburg - S80.spb-dc S Objects
ASN	AS34665 PINDC-AS, RU (registered Nov 01, 2019)

Como podemos ver el dominio tiene una IP localizada en Rusia y no está registrado por la empresa Adobe Inc.

El siguiente paso es investigar la dirección IP que contiene el dominio. Para ello, vamos a utilizar la herramienta Virus Total.



Empezamos a obtener resultados sobre la IP. Seguimos con la investigación.



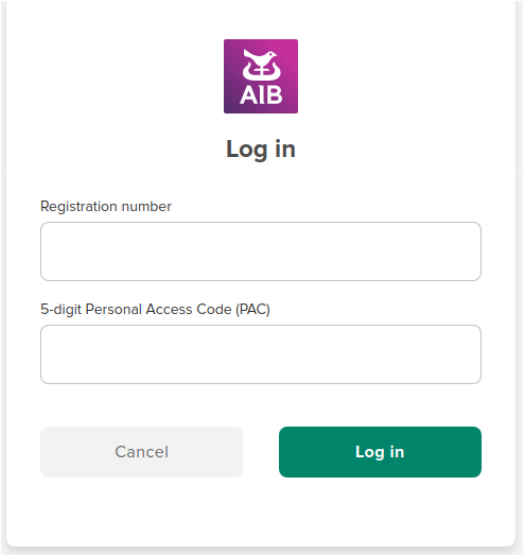
Obtenemos coincidencias con usuarios que indican que desde esa IP se están realizando ataques de fuerza bruta contra el protocolo SSH.

Hemos encontrado una URL maliciosa utilizando el hash de favicon y Shodan.

Interaccionar con el sitio web

Las interacciones con el sitio web pueden crear resultados interesantes, sobre todo, si al mismo tiempo trabajamos con las herramientas para desarrolladores. Vamos a ver un ejemplo:

Accedemos al sitio web fraudulento y lo primero que nos encontramos aparentemente es un login para iniciar sesion en nuestra banca digital. Vamos a inicar sesion, es “segurisimo”. Para interactuar con la web se recomienda el uso de una VM aislada de la máquina host para evitar posibles infecciones.



Introducimos unos datos identificativos al azar, y damos login para ver su comportamiento. Tras esto, cambia avanza a la imagen que podemos ver a continuación, pero ya no avanzará más el proceso. ¿Posible captura de credenciales?

Please Wait..

Checking your details

El siguiente paso, las herramientas para desarrolladores.

```
<div class="ping-header">…</div>
<!-- .ping-header --> == $0
<div class="ping-body-container">
  <main>
    <form method="POST" action="#" autocomplete="off" id="loginForm">
      <input type="hidden" name="ip" value="185.107.56.72">
      <input type="hidden" name="ua" value="Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36">
      <div class="ping-messages"></div>
      <label for="username" class="ping-input-label"> Registration number </label>
      <div class="ping-input-container">…</div>
      <label for="password" class="ping-input-label">…</label>
      <div class="ping-input-container password-container">…</div>
      <div class="ping-buttons">…</div>
```

Antes de introducir credenciales, ya tenemos algo que llama la atención. Este sitio web aparentemente captura la IP y el User Agent del navegador que está ejecutando el ordenador de la víctima. La ejecución de este sitio web en la herramienta Any.run, nos confirma las sospechas.

Timeshift	Class	PID	Process name	Message
4144 ms	A Network Trojan was detected	532	chrome.exe	ET CURRENT_EVENTS Ping Identity Landing Page 2022-03-14

El siguiente paso es scrapear la web en busca de más información interesante que nos sirva para identificar el origen del ataque. Para ello vamos a utilizar la herramienta dirsearch.

```
kali@kali ~ dirsearch -u "http://aib-update-securityweb.com/" -i 200 -w /home/kali/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
```

Tenemos el primer resultado, [hxxps://aib-update-securityweb.com/admin/?/login](), en principio no tenemos el password pero tenemos un nombre, Kr3pto. Sabemos que Kr3pto es un kit de phishing utilizando en ataques de suplantación utilizando bancos ingleses (en este caso, Allied Irish Banks). Tenemos ya un vector de investigación.

Los kits dinámicos de phishing de Kr3pto, permiten entre otras cosas, pasar por alto la autenticación de múltiples factores. Estos kits permiten obtener credenciales, datos personales, códigos de seguridad y autenticación de dos factores en tiempo real. Esta naturaleza en tiempo real hace que hace que estos ataques sean difíciles de bloquear y permiten atacar múltiples sitios al mismo tiempo.

Otro resultado interesante encontrado. Recordamos anteriormente que decíamos que el sitio web capturaba la IP y el navegador de la víctima. Hemos encontrado el archivo log donde se almacenan todas las IP y User Agent de los usuarios que han entrado a este sitio web. Podemos verlo en la siguiente imagen.

```
45.           : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125
Safari/537.36
164           : Python/3.6 aiohttp/3.5.4
66           6 : Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
18(           : Mozilla/5.0 (iPhone; CPU iPhone OS 15_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6
Mobile/15E148 Safari/604.1
6             : Mozilla/5.0 (iPhone; CPU iPhone OS 15_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6.1
Mobile/15E148 Safari/604.1
9             : Mozilla/5.0 (Linux; Android 9; SM-G950F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Mobile
Safari/537.36
18            : Mozilla/5.0 (iPhone; CPU iPhone OS 15_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6
Mobile/15E148 Safari/604.1
1(            : Mozilla/5.0 (Linux; Android 11; KB2003) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Mobile
Safari/537.36
80            : Mozilla/5.0 (iPhone; CPU iPhone OS 15_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6
Mobile/15E148 Safari/604.1
8(            : Mozilla/5.0 (iPhone; CPU iPhone OS 15_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6
Mobile/15E148 Safari/604.1
80            : Mozilla/5.0 (iPhone; CPU iPhone OS 15_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.6
Mobile/15E148 Safari/604.1
```

Como veremos en la siguiente imagen, existen 3008 direcciones IP capturadas en el archivo logs.txt de las cuales 2333 son distintas entre sí.

```
kali@kali ~ cat logs.txt | wc -l
3008
```

```
kali@kali ~ cat logs.txt | uniq | sort | wc -l
2333
```

Otra línea de investigación sería recabar información sobre el nombre que encontramos investigando en la web, Kr3pto. Pero es otra historia, que da para varios artículos.