
# MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

## ANÁLISIS DE TÉCNICAS DE PREVENCIÓN, DETECCIÓN Y ATAQUES DE PHISHING

AUTORA: Carmen María Mayo del Amo
DIRECTOR: Antonio Robles Gómez
Curso 2021/2022
Zamora, septiembre 2022

## RESUMEN

En la actualidad, es muy relevante la implementación de técnicas que sean capaces de evitar las consecuencias producidas por *phishing*, una de las mayores amenazas de la ingeniería social, o al menos minimizar lo más posible las vulnerabilidades derivadas de ataques a organizaciones, sobre todo en el ámbito de infraestructuras críticas o de altas prestaciones. En este sentido, tiene un gran interés asociado el realizar el análisis de *malware* mediante herramientas específicas para tal efecto.

Primeramente, en este trabajo se describirán los tipos de phishing existentes en la actualidad, así como las técnicas de prevención y detección desarrolladas para intentar frenar este tipo de ataques contra la integridad de datos personales, empresariales o institucionales, haciendo hincapié en la utilización de *machine learning.*

A continuación, se analizarán en profundidad algunas de las herramientas y algoritmos propuestos en la literatura científica para la detección de *phishing* y finalmente se harán pruebas con varios ataques de *phishing* estudiados previamente, a través de aplicaciones existentes para tal efecto y así, mostrar gráficamente su potencial y daños posibles a usuarios y organizaciones, de una manera rápida y sencilla, con alta probabilidad de éxito.

### PALABRAS CLAVE

Phishing, aprendizaje automático, algoritmo, malware, ingeniería social, ciberataques.

## ABSTRACT

At present, the implementation of techniques that are capable of avoiding the consequences produced by phishing, one of the greatest threats of social engineering, or at least minimizing as much as possible the vulnerabilities derived from attacks on organizations, especially in the field of critical or high-performance infrastructures. In this sense, it is of great interest to perform malware analysis using specific tools for this purpose.

Firstly, this paper will describe the types of phishing currently in existence, as well as the prevention and detection techniques developed to try to stop this type of attack against the integrity of personal, business or institutional data, emphasizing the use of machine learning.

Next, some of the tools and algorithms proposed in the scientific literature for phishing detection will be analyzed in depth and finally tests will be carried out with several previously studied phishing attacks, through existing applications for this purpose and thus, graphically show their potential and possible damage to users and organizations, quickly and easily, with a high probability of success.

**KEYWORDS**

Phishing, Machine Learning, algorithm, malware, social engineering, cyberattacks.

# AGRADECIMIENTOS

Muy especialmente quiero darle las gracias a mi tutor, Antonio Robles. Este Trabajo Fin de Máster se ha tenido que retrasar varios años debido a problemas de salud y él, en todo momento, me ha apoyado y animado, no dejando que tirara nunca la toalla, siendo varias las veces en las que quise rendirme. Muchas gracias por todo, Antonio.

En segundo lugar, quiero agradecer a la UNED la posibilidad de haber podido cursar este Máster a distancia, y en particular a UNED Zamora, donde llevo trabajando más de 13 años. Mis compañeros son las mejores personas que podía tener a mi lado, por ser mi otra familia, por sus ánimos y ayuda continua en mi día a día, sus consejos y su amistad. Sin ellos no hubiera podido realizar este máster. Siempre están, incondicionalmente.

A todas las personas que la UNED ha puesto en mi camino durante todos estos años, porque muchas de ellas hoy en día, son grandes amigos. Es un orgullo pertenecer a esta institución por ambas partes, como trabajadora y como alumna.

A mi familia, porque después de la tempestad, parece que está llegando la calma… y sobre todo a mi madre, que ha deseado casi más que yo que llegase este momento.

A todas mis amigas y amigos, porque han sido muchas las veces que les he tenido que decir que no a muchos planes por tener que estudiar. Por estar a mi lado siempre, en los momentos más difíciles de mi vida, pero también, por tantos buenos momentos que hemos vivido hasta ahora y por los que vendrán, que serán aún mejores.

***"Que los mejores momentos sean los que están por llegar,***
***que no se agote la fe y que la suerte nos venga a buscar***
***y aunque los años vuelen y no quieran esperar***
***si quedan causas perdidas queda una oportunidad".***
**(SHINOVA).**

# ÍNDICE GENERAL

*ÍNDICE DE FIGURAS* ..... *11*
*ÍNDICE DE TABLAS* ..... *15*
*GLOSARIO DE TÉRMINOS Y ABREVIATURAS* ..... *17*
*1. INTRODUCCIÓN* ..... *19*
1.1. MOTIVACIÓN ..... 19
1.2. OBJETIVOS ..... 21
1.3. METODOLOGÍA ..... 21
*2. PLANIFICACIÓN* ..... *23*
2.1. RECURSOS HARDWARE ..... 24
2.2. RECURSOS SOFTWARE ..... 24
2.3. COSTES ..... 25
*3. PHISHING* ..... *27*
3.1. QUÉ ES ..... 27
3.2. TIPOS Y TÉCNICAS DE ATAQUES ..... 27
3.3. EJEMPLOS REALES ..... 41
*4. ANTI – PHISHING* ..... *51*
4.1. TÉCNICAS DE PREVENCIÓN ..... 51
4.2. TÉCNICAS DE DETECCIÓN ..... 53
4.3. HERRAMIENTAS DE DETECCIÓN Y ANÁLISIS ..... 58
*5. SIMULACIONES DE PHISHING* ..... *79*
5.1. SOFTWARE DE ATAQUE ..... 79
5.2. PENTESTING ..... 90
*6. CONCLUSIONES* ..... *107*
6.1. LOGROS ALCANZADOS ..... 108
6.2. TRABAJO FUTURO ..... 109
*REFERENCIAS BIBLIOGRÁFICAS* ..... *111*

# ÍNDICE DE FIGURAS

Figura 1. Ciclo de vida del phishing [5]. .....29
Figura 2. Esquema Phishing DNS-Based [8].....31
Figura 3. Ataque Man-in-the-Middle [6]. .....37
Figura 4. Capa transparente superpuesta en un sitio web legítimo [6]. .....39
Figura 5. Ejemplo de ataque Cross-site scripting a un sitio web legítimo [6]. .....39
Figura 6. Evolución de los ataques de Phishing hasta el primer trimestre de 2022 [9]. .....42
Figura 7. Sectores más atacados por phishing en el primer trimestre de 2022 [9]. ...43
Figura 8. Usuarios que visitan sitios de phishing relacionados con criptomonedas [10].....44
Figura 9. Resultados de ataques de phishing que consiguieron su objetivo [11]. .....45
Figura 10. Marcas más imitadas por phishing durante la pandemia COVID-19 [12]. 46
Figura 11. SMS Phishing Banco Santander. .....48
Figura 12. SMS Phishing Correos.....48
Figura 13. SMS Phishing CaixaBank. .....48
Figura 14. SMS Phishing Agencia Tributaria. .....49
Figura 15. Autenticación de dos factores a través de SMS [13]. .....52
Figura 16. Esquema detección certificados SSL. .....57
Figura 17. Phishing Quiz de Google. .....59
Figura 18. PhishingQuiz - Introducción datos. .....60
Figura 19. PhishingQuiz - Correo electrónico. .....60
Figura 20. PhishingQuiz - Ejemplo email enviado. .....61
Figura 21. Whoxy - Motor de búsqueda de WHOIS. .....62
Figura 22. Herramienta Phishtank. .....63
Figura 23. Ejemplo de funcionamiento de Phishtak. .....63
Figura 24. Resultado análisis enlace con Phishtank. .....63
Figura 25. Análisis www.google.com con Phishtank. .....64
Figura 26. Resultado de analizar un sitio legítimo con Phishtank. .....64
Figura 27. Análisis sitio ilegítimo con Phishtank. .....64
Figura 28. Resultado análisis phishing detectado con Phishtank. .....65
Figura 29. Escaneo de la web de la UNED con ScanSearch. .....65

Figura 30. Sitio legítimo que nunca se ha reportado como Phishing. .....66
Figura 31. Comprobación sitio identificado como phishing. .....66
Figura 32. Muestra del último reporte de sitio phishing. .....67
Figura 33. Sitio detectado como phishing y último reporte. .....67
Figura 34. VirusTotal - Antivirus en línea. .....68
Figura 35. VirusTotal - Resultados análisis sitio web. .....69
Figura 36. Google Informe de Transparencia. .....69
Figura 37. Interfaz web de URL Void. .....70
Figura 38. Resultados del análisis con URL Void. .....71
Figura 39. Interfaz ISIT Phishing. .....71
Figura 40. Interfaz Desenmascara. .....72
Figura 41. Análisis www.amazon.es con Desenmascara. .....73
Figura 42. Resultados del análisis de Amazon con Desenmascara. .....73
Figura 43. Interfaz de OpenPhish. .....74
Figura 44. Talos Intelligence - Cisco. .....75
Figura 45. Muestra de sitios detectados por Talos. .....76
Figura 46. Resultados de búsqueda en Talos. .....76
Figura 47. Codeshield - Seguridad en la nube. .....77
Figura 48. Interfaz DNSTwister. .....78
Figura 49. Resultados búsqueda de dominio con DNSTwister. .....78
Figura 50. Social Engineer Toolkit (SET). .....80
Figura 51. Sitio web de SET. .....80
Figura 52. Herramienta Social Engineer Toolkit (SET). .....81
Figura 53. Logo de Hidden Eyer. .....81
Figura 54. Herramienta Hidden Eyer. .....82
Figura 55. Logo WifiPhisher. .....83
Figura 56. Herramienta WifiPhisher. .....83
Figura 57. Logo King Phisher. .....84
Figura 58. Herramienta King Phisher. .....84
Figura 59. Logo Gophish. .....85
Figura 60. Herramienta Gophish. .....85
Figura 61. Sitio web oficial de Gophish. .....86
Figura 62. Logo Evilginx2. .....86

Figura 63. Herramienta Evilginx2. ....87
Figura 64. Logo Blackeye. ....87
Figura 65. Herramienta Blackeye. ....88
Figura 66. Herramienta Modlishka. ....89
Figura 67. Interfaz principal Kali Linux. ....90
Figura 68. Herramientas disponibles en Kali Linux. ....91
Figura 69. Social Engineering Toolkit integrado en Kali Linux. ....91
Figura 70. Acceso a SET a través de la terminal. ....92
Figura 71. Herramienta SET proporcionada por Kali Linux. ....92
Figura 72. Menú principal de SET. ....93
Figura 73. Menú de ataque de Spear-Phishing con SET. ....93
Figura 74. Tipos de archivo para envío masivo de emails phishing. ....94
Figura 75. Uso de archivo PDF para envío de phishing por correo electrónico. ....94
Figura 76. Selección tipo de ataque. ....95
Figura 77. Generación de archivo. pdf. ....95
Figura 78. Envío de ataque a una sola víctima o envío masivo. ....96
Figura 79. Plantillas predefinidas para utilizar en el envío de correo electrónico phishing. ....96
Figura 80. Destinatario del envío. ....97
Figura 81. Elección de gestor de envío de correo. ....97
Figura 82. Login Gmail para envío de phishing. ....98
Figura 83. Modo escucha del atacante. ....98
Figura 84. Menú principal SET - Ataque web. ....99
Figura 85. Ataque SET clonar un sitio web. ....99
Figura 86. Ataque clonación web. ....100
Figura 87. Selección plantilla. ....100
Figura 88. Ataque a la espera de recibir credenciales de Google. ....100
Figura 89. Interfaz de Google clonada. ....101
Figura 90. Recepción de credenciales de Google. ....101
Figura 91. Ataque a la espera de recibir credenciales de Twitter. ....102
Figura 92. Interfaz de Twitter clonada. ....102
Figura 93. Recepción de credenciales de Twitter. ....103
Figura 94. Menú principal SET - Creación de Payload y agente de escucha. ....103

Figura 95. Tipo de ataque. .....103
Figura 96. Selección de IP y puerto de escucha. .....104
Figura 97. Herramienta Metasploit. .....104
Figura 98. Atacante en modo escucha. .....105
Figura 99. Ejecutable que contiene el virus / troyano.....105

# ÍNDICE DE TABLAS

Tabla 1. Tiempo empleado en la realización del TFM. .....23
Tabla 2. Costes de los recursos hardware utilizados. .....25
Tabla 3. Costes de los recursos software utilizados. .....25

# GLOSARIO DE TÉRMINOS Y ABREVIATURAS

AI – *Artificial Intelligence.*

AP – Acess Point.

API – *Application Programming Interface.*

APWG - *Anti-Phishing Working Group.*

CSV – *Comma Separated Values.*

CVV - *Card Verification Value.*

DKIM – *DomainKeys Identified Email.*

DL – *Deep Learning.*

DMARC – *Domain-Based Message Authentication.*

FL – *Fuzzy Logic.*

HTML – *HyperText Markup Language.*

IAM – *Identity Access Management.*

INCIBE – Instituto Nacional de Ciberseguridad de España.

IP – *Internet Protocol.*

JSON – *JavaScript Object Notation.*

MITM – *Man In The Middle.*

ML – *Machine Learning.*

OSI – Oficina de Seguridad del Internauta.

PHP – *Hypertext PreProcessor.*

SAAS – *Software As A Service.*

SET – *Social Engineer Tooklit.*

SPF – *Sender Policy Framework.*

SSL – *Secure Sockets Layer.*

SVM – *Support Vector Machine.*

TFM – Trabajo Fin de Máster.

TLS – *Transport Layer Security.*

URL – *Uniform Resource Locator*.

XML – *eXtensible Markup Language.*

XSS – *Cross-Site Scripting.*

# 1. INTRODUCCIÓN

Con este trabajo se pretende realizar el estudio de uno de los ataques de ingeniería social más común y frecuente hoy en día: el *phishing*, que supone importantes amenazas en organizaciones empresariales de altas prestaciones, por no decir que, a nivel personal, casi diariamente se recibe algún correo basado en esta técnica.
Los ataques de *phishing* además pueden estar basados en la utilización de *malware* para conseguir el objetivo de los ciberatacantes.

Por todo esto, es de suma importancia la revisión de técnicas que sean capaces de evitar las consecuencias producidas por *phishing*, o al menos minimizar lo más posible las vulnerabilidades derivadas de ataques a organizaciones, sobre todo en el ámbito de infraestructuras críticas o de altas prestaciones. En este sentido, tiene un gran interés asociado realizar el análisis de *malware* mediante herramientas específicas para tal efecto.

Primeramente, se hará un exhaustivo estudio del concepto de *phishing* y los distintos tipos que existen actualmente, describiendo cada uno de ellos y sus principales formas de ataque.

Seguidamente, se analizarán y describirán las técnicas y herramientas más actuales que se han propuesto e investigado por expertos en ciberseguridad y más concretamente en "*antiphishing*" de todo el mundo, desarrollando sistemas de detección con la ayuda de algoritmos, inteligencia artificial (*Deep learning*, *Machine Learning*, *Hibrid learning*…) y otras técnicas.

## 1.1. MOTIVACIÓN

Como bien es sabido y se ha indicado en la introducción, hoy en día el *phishing* es uno de los principales ataques de ingeniería social existentes a nivel mundial, siendo un gran problema, tanto a nivel personal como empresarial, puesto que los ciberdelincuentes tienen una tasa muy alta de éxito a la hora de acceder a los datos de usuarios y cada vez es más difícil de controlar y prevenir.

Con la llegada de internet hace unos años unido al gran auge de los dispositivos móviles, redes sociales, teletrabajo, etc., el estilo de vida de las personas ha cambiado. Los niños casi desde que nacen se acostumbran a ver teléfonos móviles, tabletas y ordenadores portátiles, donde sus padres les ponen música o vídeos de *Youtube*, lo que hace que la tecnología forme parte de su día a día a medida que van creciendo, hasta llegar a la población de mediana y avanzada edad, donde los últimos años con el auge de aplicaciones de mensajería instantánea como *Whatsapp* o redes sociales, se ha fomentado su uso cada vez más en un rango de edad no demasiado habitual.

Por lo tanto, se puede decir que la población en general pasa muchas horas al día en internet, lo que implica que esté expuesta a recibir algún ciberataque, especialmente de *phishing*.

Los ciberdelincuentes aumentan sus tácticas de ingeniería social a medida que las empresas y organizaciones ponen más medios de prevención de ataques. En la actualidad, con el aumento de los sistemas de almacenamiento en la nube, la inteligencia artificial, el big data, etc., las organizaciones e instituciones manejan cada vez más grandes volúmenes de datos. De igual manera, las herramientas automatizadas están aumentando entre los atacantes, lo que hace que, aunque tengan conocimientos básicos de la materia, puedan provocar enormes daños. En el mercado negro se pueden encontrar kits de *phishing* que contienen lo necesario para realizar con facilidad un ataque de *phishing* por correo electrónico o una web falsa.

A raíz de la pandemia de la COVID-19, el *phishing* aumentó a pasos agigantados. Según un informe realizado por ESET, durante los últimos meses de 2021, España ha sido uno de los países que ha tenido mayor número de ataques de *phishing*, en parte propiciado por el teletrabajo y la falta de seguridad en los equipos.

Según el informe *"State of the Pish Report 2022"* de la empresa americana de seguridad *Proofpoint*, que realizó a través de encuestas a profesionales de ciberseguridad de Estados Unidos, España, Reino Unido, Francia, Alemania y Japón

durante el pasado 2021, un 83% de las organizaciones experimentaron ataques de *phishing* con éxito, robando datos de clientes y credenciales comprometidas.

Otro importante informe de amenazas de la también americana *Zscaler* coincide con Proofpoint en el aumento del *phishing* durante el 2021 (un 29% más que en 2020), siendo *Microsoft, Telegram, Amazon, Onedrive* o *Paypal* los principales objetivos, creciendo el phishing por SMS debido a que los usuarios ya sospechan más de los correos electrónicos que reciben.

## 1.2. OBJETIVOS

El principal objetivo de este Trabajo Fin de Máster será revisar los distintos tipos de *phishing* existentes hoy en día y analizar las técnicas, herramientas y sistemas de prevención y detección de los ataques producidos para recabar información y datos personales de manera ilegal y fraudulenta, haciendo hincapié en la importancia del daño que supone recibir un ataque de este tipo en grandes empresas o instituciones.

Se hará un pequeño estudio de las herramientas de detección que utilizan algoritmos de *Machine Learning*, para ver con cuáles de ellos se obtendrán mejores resultados a la hora de analizar las técnicas de suplantación de identidad más utilizadas por los ciberdelincuentes. Para ello hará falta conocer el funcionamiento de los sistemas de *Machine Learning* y las técnicas de clasificación de los algoritmos en los que se basan, además de revisar distintas herramientas de ataque que usan los atacantes y probar algunas de las herramientas utilizadas por los testeadores de ingeniería social.

## 1.3. METODOLOGÍA

Como existen infinidad de métodos para abordar los ataques de *phishing*, este trabajo no se va a enfocar en uno en concreto, sino que debido al gran volumen de este tipo de ataques y propagación por parte de los ciberdelicuentes, se estudiarán con detalle cada uno de ellos y los métodos más actuales y de mayor alcance que intentan alcanzar el engaño del mayor número de usuarios y así el robo de sus datos sensibles.

La metodología que se desarrollará para que se puedan cumplir los objetivos de este TFM será la siguiente:

- Estudio del estado del arte del contexto de trabajo, donde se hará un análisis en profundidad de la literatura científica existente.
- Análisis de las técnicas de detección previa a los ataques, revisando y explicando las más importantes.
- Pruebas de ataques de *phishing*, donde se analizarán algunos kits utilizados por probadores de ciberseguridad, simulando ataques reales.
- Conclusiones y resultados finales.

# 2. PLANIFICACIÓN

La realización de este Trabajo Fin de Máster en Ingeniería Informática no ha sido de manera continua, por lo que cuantificar el tiempo es complicado, ya que han sido varias las etapas de trabajo llevadas a cabo para su finalización en un intervalo de tres años.

Primeramente, se realizó una investigación exhaustiva del estado del arte de las técnicas de ataques de *phishing* actuales y sus diferentes maneras de combatirlas o al menos, frenar sus consecuencias, a través de diferentes recursos científicos, libros y páginas web relacionadas con el tema.

Como justamente llegó la pandemia de la COVID-19 en marzo de 2020 y tras un intervalo de pausa del estudio del estado del arte, se revisaron nuevos estudios científicos puesto que el número de víctimas a raíz de dicha pandemia creció a niveles exponenciales durante 2020, 2021 y 2022.

Haciendo un cálculo suponiendo un trabajo continuado, podemos desglosar el tiempo empleado de esta manera:

| TAREA | Horas |
|---|---|
| **Toma de contacto e información inicial sobre el tema** | 40 |
| **Estado del arte y lectura de publicaciones científicas** | 80 |
| **Búsqueda de información sobre soluciones propuestas** | 20 |
| **Aprendizaje y revisión de algoritmos de Machine Learning** | 30 |
| **Pruebas** | 20 |
| **Evaluación de resultados** | 10 |
| **Realización de la memoria del TFM** | 100 |
| | 300 |

*Tabla 1. Tiempo empleado en la realización del TFM.*

## 2.1. RECURSOS HARDWARE

En cuanto a recursos hardware, para la realización de este proyecto se han utilizado dos ordenadores portátiles y dos monitores adicionales, conectados a ambos ordenadores para optimizar el rendimiento y visualización a la hora de trabajar:

- *Macbook Pro* de 13 ‘’ con procesador 2,9 Ghz Intel Core i5 de doble núcleo, memoria RAM de 8 GB, tarjeta gráfica Intel Iris Graphics 550 1536 MB y sistema operativo macOS Monterey.
- *Dell Latitude* de 13.3 ‘’, con procesador Intel i7 y 16 GB de memoria RAM, con Sistema Operativo Windows Pro 10 de 64 bits.
- Monitor HP 27 fw.
- Monitor HP Compaq LA2306x.

El ordenador *Mac* se ha utilizado para la realización de la memoria y la búsqueda, lectura y gestión de la literatura científica utilizada para el desarrollo del estado del arte.

En el ordenador con *Windows*, se ha instalado una máquina virtual con la distribución *Linux* de *Ubuntu* y *Kali Linux* para la realización de pruebas con códigos y algoritmos.

Se decidió así para optimizar el tiempo y rendimiento obtenido al tener cada uno para unas tareas concretas y, sobre todo, para poder ir trabajando en la memoria mientras se probaban los algoritmos, ya que consumen muchos recursos.

## 2.2. RECURSOS SOFTWARE

Los recursos software utilizados han sido los siguientes:

- Paquete *Microsoft Office 365* para *Mac*.
- *Sublime Text*.
- Navegadores: Ópera, Google Chrome y Safari.
- *Python* 3.9.1.

- *Oracle VM VirtualBox* 6.1.
- *Linux Ubuntu* 22.04.1.
- *Kali Linux*.

## 2.3. COSTES

| RECURSOS HARDWARE | Coste |
|---|---|
| MacBook Pro | 1700 € |
| Dell Latitude | 990 € |
| | **2690 €** |

*Tabla 2. Costes de los recursos hardware utilizados.*

| RECURSOS SOFTWARE | Coste |
|---|---|
| Licencia Windows 10 Pro 64 bits | 200 € |
| Licencia Microsoft Office 365 (licencia anual) | 69 € |
| Sublime Text | 0 € |
| Navegadores | 0 € |
| Python | 0 € |
| Oracle VM VirtualBox | 0 € |
| Ubuntu | 0 € |
| Kali Linux | 0 € |
| | **269 €** |

*Tabla 3. Costes de los recursos software utilizados.*

# 3. PHISHING

## 3.1. QUÉ ES

Como se ha comentado en epígrafes anteriores, el *phishing* es uno de los ataques de ingeniería social más utilizados en todo el mundo por los ciberdelincuentes para engañar a los usuarios y así obtener información sensible, privada y personal, sobre todo datos bancarios. Es por ello por lo que existen infinidad de estudios y literatura científica sobre los tipos de *phishing*, sus técnicas de análisis, detección y prevención de sus ataques, casos de estudio concretos, trabajos futuros y posibles soluciones a día de hoy.

Estas soluciones y tipos de prevención van cambiando rápidamente, por lo que los investigadores tienen que estar analizándolas continuamente, ya que los atacantes cada vez utilizan técnicas novedosas más difíciles de frenar o minimizar el riesgo de sus daños, además del auge de la computación en la nube, los dispositivos móviles y el Internet de las Cosas, haciendo más vulnerables los datos y credenciales de los usuarios en infraestructuras y organizaciones potencialmente vulnerables.

Por lo tanto, en este apartado se desarrollará una exhaustiva investigación acerca de las amenazas, riesgos, vulnerabilidades sobre el *phishing* actual y todo lo que lo rodea.

## 3.2. TIPOS Y TÉCNICAS DE ATAQUES

Los ciberdelincuentes intentan engañar a las víctimas a través del envío de un mensaje electrónico, haciéndose pasar por una empresa, entidad, red social, servicio o persona de confianza para que éstas crean que se trata de algo fiable y real y así “piquen” en el anzuelo. De ahí precisamente proviene el nombre este tipo de ataque, de la palabra en inglés “*fishing*”, con la misma pronunciación que “*phishing*”, que significa “pesca” y a través de un “cebo” que llame la atención de la víctima, ésta “pica”. Las letras *ph* de «*phishing*» proceden de mediados del siglo XX, el llamado «*phone phreaking*», que consistía en experimentar con las redes de

telecomunicaciones para averiguar su funcionamiento. Así, Phreaking + Fishing = Phishing. [1], [2], [3].

Independientemente del medio de acción, los ciberdelincuentes que utilizan el *phishing* como ataque siguen un mismo patrón para alcanzar su fin: engañar a la víctima para que acceda a algún enlace, abra un archivo adjunto, realice un pago, etc.

Al final, el atacante puede personalizar a la perfección su engaño para que sea más creíble y atractivo a su objetivo. Esto ha sido fomentado por el gran auge de las redes sociales, ya que los delincuentes poseen mucha más información de sus objetivos a atacar.

Según Abdelhamid, et al. [5], el ciclo de vida se puede resumir en cinco pasos:

1) Se envía un enlace utilizando uno de los canales antes mencionados a posibles víctimas.

2) Al hacer clic, el enlace redirigirá a las posibles víctimas a un sitio web malicioso.

3) Los usuarios se vuelven vulnerables cuando intentan iniciar sesión con sus credenciales en el sitio web malicioso.

4) Después, las credenciales de inicio de sesión se transfieren a un servidor o se instala un registrador de claves en el dispositivo informático del usuario.

5) El *phisher* puede utilizar las credenciales para cometer delitos cibernéticos adicionales.

En la Figura 1 se muestra un esquema del ciclo de vida del *phishing*, quedando bien diferenciadas cada una de las fases:

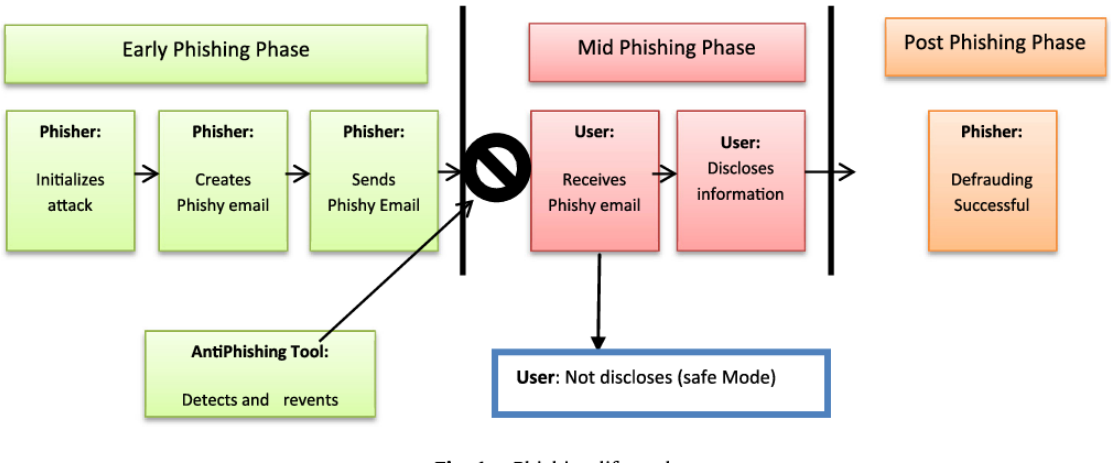


*Figura 1. Ciclo de vida del phishing [5].*

Por todos es sabido que estos ataques están a la orden del día y con los años se han vuelto más sofisticados y difíciles de detectar. Muchas veces es complicado reconocerlos y darse cuenta a tiempo, antes de que los atacantes se hagan con la información y datos sensibles.

A continuación, se describen los tipos de ataques de *phishing* (y técnicas derivadas de éste para el robo de datos) que existen hoy en día, con sus características principales [4], [6], [7].

- ***Deceptive Phishing.***

Es el *phishing* tradicional y más común. El atacante se hace pasar por una persona conocida o una empresa, marca o institución que cuente con la confianza de la víctima, con el objetivo de conseguir información personal o credenciales para acceder a un sitio determinado. Utiliza para ello el envío de un correo electrónico para intentar sacarle esta información personal o bien, envía en el correo un enlace web a un sitio malicioso. Una de las maneras bastante habitual para robarle los datos bancarios a las víctimas, es solicitar que actualice sus contraseñas a través del enlace que envían, por ejemplo [8].

- ***Malware - Based Phishing.***

En este tipo de *phishing*, se envía a través del correo electrónico algún tipo de *malware* como archivo adjunto o a través de la descarga en algún enlace web enviado en el cuerpo del mensaje, que tenga interés para la víctima y así lo descargue en su ordenador. Mediante esto, los atacantes solamente quieren hacer daño a la víctima, sin robarle credenciales ni datos sensibles [8].

- ***Content – Injection phishing.***

En este caso los atacantes inyectan código malicioso en la web de alguna compañía, en el caso de que dicha web no se encuentre actualizada y sea vulnerable, produciendo una modificación en ella y logrando una difícil detección del ataque, que puede pasar desapercibido para la empresa durante largo un tiempo, redirigiendo al usuario de esa web a un sitio fraudulento o bien, instalar *malware* que dirija a los usuarios a la web de los atacantes [8].

- ***Spear phishing.***

Ataque más personalizado, dirigido a un número reducido de personas de una empresa u organización específica, y, por tanto, objetivo conocido por el atacante. Al ser ataques más sofisticados y adaptados a los receptores de estos correos electrónicos, suelen ser muy difíciles de detectar y altamente efectivos. Tiene como principal objetivo el robo de datos, aunque a veces, los atacantes también instalan algún tipo de *malware* en los equipos de la víctima. A menudo, puede pasar que una persona cercana y de confianza para las empresas y organizaciones llegue a ser un ciberdelincuente contra ellas.

- ***Pharming (DNS-Based phishing).***

Las víctimas son atacadas a través de los servidores DNS que utilizan para resolver los dominios de los sitios de internet que visitan. Dicho ataque puede hacerse tanto a los DNS públicos como locales de los equipos de las víctimas. Con este tipo

de ataque, cuando las víctimas visiten sitios web de confianza, realmente están visitando otras webs fraudulentas para robarles información.

Los tipos de *pharming* más conocidos son el "*pharming* de *malware*" y el "envenenamiento de DNS", teniendo el único objetivo de robar datos a las víctimas. El primero normalmente utiliza un malware enviado adjunto en un correo electrónico o bien en un enlace para descargarlo, que hará que cambie algún archivo del equipo de la víctima para que, al introducir alguna dirección web en el navegador, sea redirigido a otra web fraudulenta que aparentemente es igual a la que le interesa al usuario.

El "envenenamiento de DNS" se aprovecha de algunas vulnerabilidades que puedan existir en el servidor DNS que los ciberdelincuentes quieran atacar, así cuando los usuarios accedan a la web deseada, se les redigirá a un sitio web fraudulento [8], tal como se muestra en la Figura 2.

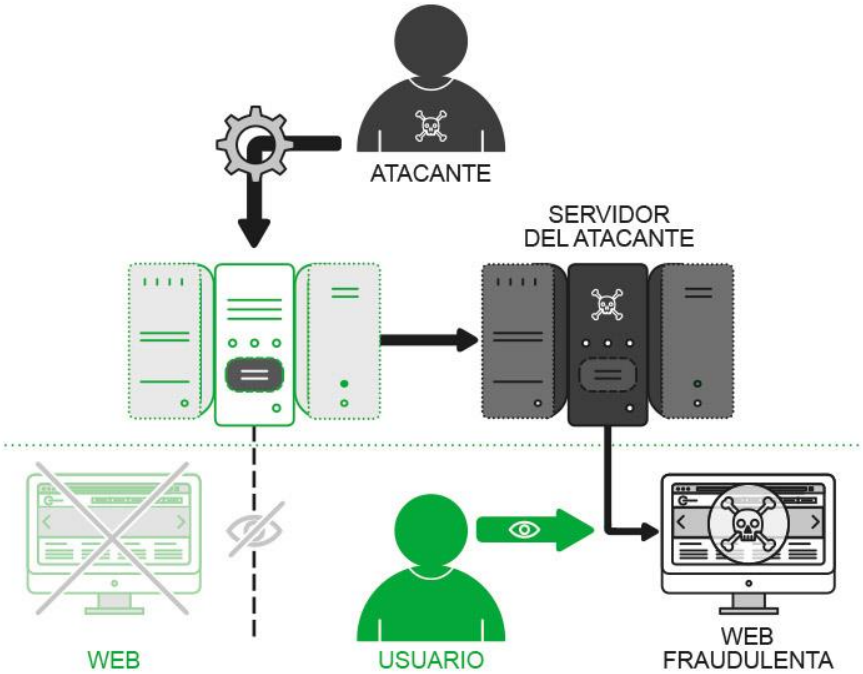


*Figura 2. Esquema Phishing DNS-Based [8].*

- ***Vishing.***

En lugar de utilizar el correo electrónico para suplantar la identidad de un tercero, la suplantación se realiza a través de una llamada telefónica. El nombre es una combinación de "*voice*" y "*phishing*".

El canal para intentar robar los datos de los usuarios es lo que diferencia al *vishing* del propio *phishing* (a través del correo electrónico) y del *smishing* (a través de un mensaje de texto SMS).

En muchas ocasiones, los atacantes fingen ser miembros de empresas y organizaciones de confianza, o llaman en nombre de algún familiar que finge encontrase en situaciones de peligro y así lograr datos personales y bancarios.

- ***Defacement.***

Es un tipo de ataque que va dirigido a algún sitio web, modificando la apariencia de algunas de sus páginas. Esto lo hacen aprovechando alguna vulnerabilidad que encuentran en el sitio web y así modificar el aspecto para llegar a sus objetivos, como pueden ser la instalación de algún *malware*, llevar a cabo algún robo de datos sensibles o realizar vandalismo informático (ciber protestantes).

- ***Whaling.***

Este tipo de *phishing* es conocido como "*phishing* ejecutivo". Utiliza el envío de correos electrónicos fraudulentos haciéndose pasar por directivos de niveles superiores de alguna empresa u organización que se dirigen a altos ejecutivos y personas con gran peso dentro de éstas, con el principal objetivo del robo de información sensible y confidencial o de otro tipo de acción fraudulenta.

Los blancos principales de los ciberdelincuentes son los trabajadores de alta jerarquía de las organizaciones, instituciones o empresas.

- ***Smishing.***

En este tipo de phishing está basado en la utilización de teléfonos móviles, así, los ataques se generan mediante mensajes de texto SMS o mensajes a través de WhatsApp, Telegram y otras aplicaciones de mensajería. La palabra "*smishing*" deriva de SMS (SMiShing).

Es muy frecuente que los atacantes utilicen este sistema para hacerse pasar por entidades financieras con números de teléfono falsos, pidiendo al usuario en sus mensajes algún tipo de dato, como actualización de sus contraseñas, avisos de que si no se accede al enlace que envían le cerrarán la cuenta, también es muy común el aviso de que se ha hecho alguna compra con la tarjeta de crédito, puesto que muchos bancos hacen esto frecuentemente para verificar la seguridad de la transacción pidiendo algún código que envían por SMS y los atacantes intentan confundir y engañar a los usuarios.

En otros casos, en vez de contener algún enlace, directamente se le solicita al usuario que llame urgentemente al número de teléfono que le aparece en el SMS (en la mayoría de las ocasiones puede ser uno número de tarificación especial), y si el usuario hace caso, le solicitan datos confidenciales para intentar cancelar la compra que se ha hecho con la tarjeta, y es ahí donde se produce el robo de las credenciales.

- ***QRishing.***

Esta técnica se ha popularizado debido al aumento del uso de los códigos QR a raíz de la pandemia de la COVID-19. Su nombre viene de la combinación los términos código QR (en inglés "Quick Response Code") y la palabra phishing.

Los ciberdelincuentes manipulan los códigos QR para que cuando los usuarios los escaneen con sus dispositivos móviles les lleve a un enlace fraudulento y no al real que el usuario busca, aunque la apariencia a simple vista sea la misma. Por ejemplo, en los restaurantes o bares aumentó el uso de códigos QR para ver las cartas de productos y así no tener que tocar varias personas una misma carta en papel.

Como en otros tipos de *phishing*, aquí el ciberdelincuente puede hacer que el código QR enlace a un sitio web o bien, que se instale un *malware* en el dispositivo del usuario víctima.

- ***Angler.***

En este tipo de ataque, los ciberdelincuentes se aprovechan de las víctimas a través de sus cuentas de redes sociales, haciéndose pasar por personal de atención al cliente de alguna empresa con la cuál estén insatisfechos porque no le hayan prestado el servicio adecuado, y así, revelan sus datos personales para que "les ayuden" con sus consultas.

- ***Spoofing de correo electrónico.***

Consiste en la creación de mensajes de correo electrónico con un encabezado o dirección de remitente falso, pareciendo original, es decir suplantando la identidad de alguien. Esta técnica es muy popular en los ataques de *phishing*, porque las víctimas confían en fuentes que conocen o son cercanas a ellas.

- ***Data Theft.***

Como su nombre indica, es el robo de datos del sistema de un usuario. Es probable que estos usuarios sean grandes cargos de empresas y organizaciones, o incluso relacionados con el gobierno o similares, en los que el robo de información cause grandes catástrofes tanto personales al hacerse públicos sus datos como a nivel económico, causando pérdidas.

Puede referirse también a prácticas de espionaje para la obtención de datos secretos sobre otros gobiernos o empresas de la competencia.

- ***Typosquating.***

Es un tipo de engaño que se basa en los errores tipográficos que los usuarios puedan cometer al introducir las direcciones de los sitios web a los que quieran

acceder en su navegador. A veces, por rapidez, los usuarios introducen manualmente la dirección en el navegador sin acceder a ella a través de un buscador y esto es lo que hace que puedan confundirse al escribirla (pulsar una tecla contigua, que le falte teclear un determinado carácter, etc.) y ser dirigidos al sitio fraudulento.

Una vez dentro, como en otros casos vistos anteriormente, los usuarios pueden ser engañados para introducir datos comprometidos o bien descargase algún tipo de *malware* en sus dispositivos.

Este tipo de engaño comienza cuando los ciberdelincuentes registran y compran dominios con errores tipográficos en sus nombres, similares a alguna web con cierta repercusión, como buscadores, sitios web de bancos, gobiernos, etc, para después crear sitios web fraudulentos, similares a las páginas reales, para que los usuarios caigan en la trampa. Utilizan logotipos y diseños a simple vista idénticos a las webs legítimas. Al fin y al cabo, es como si fuese un secuestro de la URL al ser una URL falsa y encubierta.

- ***IDN homograph.***

Consiste en engañar al usuario a través de nombres de dominio similares a los sitios reales, pero con caracteres diferentes. Esto es, son homógrafos, de ahí su nombre.

Es similar al Typosquating, pero en este caso, las víctimas son engañadas por los ciberdelincuentes a través de hipervínculos que no se distinguen visualmente.

- ***Search Engine Phishing.***

Debido a que hoy en día los usuarios realizan una gran parte de compras, reservas de transportes, viajes y demás gestiones online, los atacantes realizan ofertas y anuncios posicionados en los primeros puestos de los buscadores, para que los usuarios entren con facilidad, con ofertas atractivas que llamen la atención y así cuando accedan, en realidad van a entregarle sus datos personales y bancarios a los ciberdelincuentes. Aparte de descuentos y ofertas, los atacantes suelen también

darles publicidad a ofertas de trabajo o catástrofes y situaciones de emergencia, lo que hace que los usuarios puedan llegar a asustarse ante a determinadas situaciones y cedan a las indicaciones de los delincuentes.

- ***Clone Phishing.***

Es un subconjunto del *phishing* tradicional, que consiste en la clonación de un correo electrónico de una empresa u organización que ha sido recibido previamente. Así, el correo recibido parece legítimo y como en los demás casos estudiados, solicitar datos sensibles a los usuarios. Se diferencia con el *phishing* normal en que la información que contiene el correo electrónico original permanece intacta, pero se ha duplicado. Suele estar dirigido a personas con perfiles altos dentro de las organizaciones.

- ***Keyloggers y Screenloggers.***

Los ciberdelincuentes pueden enviar a los usuarios un *malware* que instalan en su equipo para rastrear las entradas del teclado y enviar la información relevante a través de Internet a sus sistemas para robarle sus datos personales y financieros.

- ***Session Hijacking.***

Tipo de ataque de *malware* en el que el atacante ha rastreado el sistema del usuario para que todo lo que haga sea monitoreado, de modo que cuando el usuario inicie sesión con los datos bancarios u otra información útil para el atacante, el software malicioso se hará cargo de él y transferirá la información sin el conocimiento del usuario. Se llama sesión porque se realiza por sesiones y no continuamente.

- ***Web Trojans.***

Es similar al *Session Hijacking*, pero es invisible para el usuario y aparece cuando el usuario inicia sesión en cualquier sitio web importante o realiza

transacciones y recopila toda la información que el usuario ha completado y la transmite al atacante.

- ***Host File Poisoning.***

Lo que hace es engañar al usuario para que piense que está iniciando sesión en el sitio web correcto sin saber que ha sido engañado para iniciar sesión en un sitio web falso de igual apariencia que el sitio web original. Esto se logra "evenenando" el archivo del host donde el atacante quiere robar la información.

- ***System Reconfiguration Attacks.***

La configuración en el sistema de los usuarios se modifica intencionalmente con fines maliciosos para cambiar los nombres de URL presentes en los favoritos guardados en los navegadores de los usuarios, de modo que cuando intentan iniciar sesión en el sitio web requerido, en realidad inician sesión en un sitio falso.

- ***Man-in-the-Middle Phishing.***

Este tipo de *phishing* es muy difícil de detectar. En este caso, el atacante se encuentra entre el usuario y el sitio web, como se muestra en la Figura 3, y cuando el usuario está realizando una transacción en línea, es cuando toma el control y copia toda la información y las credenciales del usuario, pero proporciona a los usuarios todos los pasos necesarios para que revise todo y no sospeche, usando la información más tarde. Normalmente está relacionado con tarjetas de crédito, cuentas bancarias, etc. [6].


*Figura 3. Ataque Man-in-the-Middle [6].*

- ***Malvertising.***

Malvertising utiliza el servicio de alojamiento de anuncios online como un medio para distribuir *malware* a las víctimas. Los atacantes publican anuncios con *malware* incrustado para lograr el ataque de *phishing*. Cuando una víctima hace clic en el anuncio, un *malware* dinámico infectará su sistema y explotará su vulnerabilidad con el objetivo de robar información personal de la víctima.

Los atacantes pueden distribuir su *malware* a través de sitios web legítimos usando publicidad sin la necesidad de comprometer los sitios web y así, el usuario no sospechará al visitar el sitio web publicitario, ya que el anuncio está alojado en un sitio web real [5].

- ***Javascript Obfuscation.***

Los ciberdelincuentes utilizan Javascript para enmascarar las ventanas del navegador. Así, puede falsificar la barra de direcciones o la barra de estado para hacer que el sitio web parezca legítimo, incluso llegando a aparentar un que es un sitio seguro con “https” y el icono del candado, para que el usuario no se dé cuenta de que el sitio web es la versión con *phishing* del sitio web real [6].

- ***Clickjacking.***

Consiste en la manipulación de la interfaz de usuario de una página web que lleva al usuario a realizar una acción sin saberlo al interactuar con la interfaz de usuario comprometida, así el usuario puede hacer *click* en un botón o enlace en un sitio web que aparentemente es fiable, pero esconde o está enmascarando otro elemento html, es decir, se superpone un sitio web fraudulento sobre el sitio web real de manera transparente (Figura 4). Los ciber atacantes pueden ocultar en la página web invisible una página maliciosa con el fin de obtener datos sensibles de los usuarios [6].

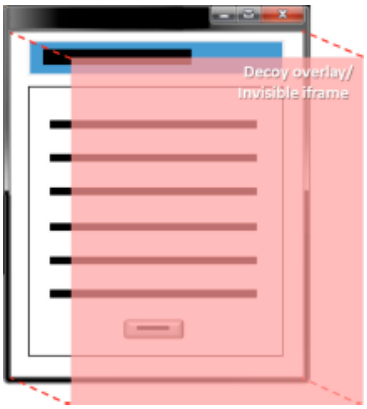


*Figura 4. Capa transparente superpuesta en un sitio web legítimo [6].*

- ***Cross-site scripting.***

Consiste en que los *phishers* aprovechan la vulnerabilidad de un sitio web, inyectando algún código malicioso en los campos de datos o haciendo uso de una URL personalizada en un sitio web para robar la información personal de los usuarios, normalmente utilizando *javascript*. Se puede ver su esquema de funcionamiento en la Figura 5. A este tipo de ataque se le conoce por las siglas XSS [6].

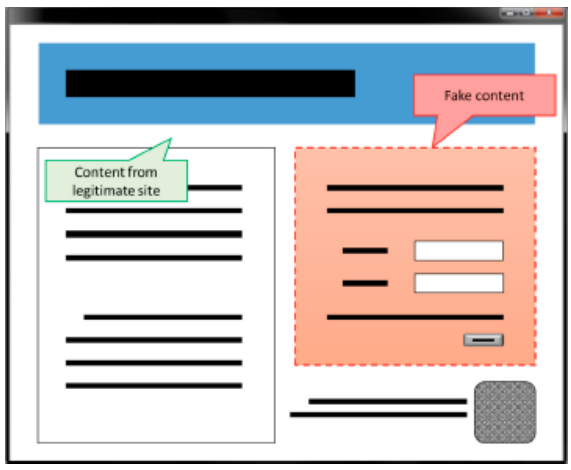


*Figura 5. Ejemplo de ataque Cross-site scripting a un sitio web legítimo [6].*

- ***Drive-by-download.***

Es una técnica de que inyecta *malware*, virus o scripts en un sistema simplemente cuando el usuario visita un sitio web o lee un correo electrónico HTML. El código malicioso se suele escribir en JavaScript para atacar la vulnerabilidad de un navegador o el complemento de un navegador y se aloja en un servidor o se inyecta en un sitio web o en un correo electrónico HTML. En este caso, suele ser sin el consentimiento del usuario, puesto que no se da cuenta de que se ha descargado ningún *malware* para el robo de su información personal [6].

- ***Sound-squatting.***

Es una técnica que consiste en el registro de nombres de dominio que suenen similares a un sitio web legítimo. Tales palabras que suenan similares se llaman homónimos. Los atacantes también pueden usar la palabra o el dígito de un número como homónimo, así se aprovechan de que el usuario confunda los homónimos e introduce la palabra equivocada, pero con el mismo sonido al teclear la URL. Así, el usuario accede a la versión que contiene el *phishing* creyendo que es un sitio web legítimo. Por lo general, registran varios nombres de dominio con homónimos de un nombre de dominio legítimo [6].

- ***Tabnapping.***

Podemos decir que el Tabnapping consiste en un ataque basado en una forma de "secuestro" de una pestaña en un navegador, haciendo uso de la manipulación de los sitios web inactivos. Primero, el atacante envía por correo electrónico el enlace de un sitio web de *phishing* a un usuario. Una vez que el usuario haga clic en dicho enlace, se abrirá una pestaña en el navegador del usuario para cargar el sitio web de *phishing* que parece un sitio web legítimo.

El JavaScript incrustado en el sitio web de *phishing* monitorea la actividad de navegación del usuario. Una vez que el usuario navega a otras pestañas en el navegador y deja la pestaña con el sitio web de *phishing* abierto, la pestaña carga una

pantalla de inicio de sesión de *phishing* y cambia el icono de favoritos y el título de la pestaña para falsificar un sitio web legítimo. Cuando el usuario navega por las pestañas abiertas y observa la pantalla de inicio de sesión de *phishing*, el usuario podría pensar que la sesión iniciada en ese sitio web ha caducado y el usuario necesita iniciar sesión de nuevo. Por lo tanto, el usuario envía las credenciales de inicio de sesión a través de la pantalla de inicio de sesión de *phishing* sin darse cuenta de que se trata de un sitio web falso [8].

- ***Whiphishing – Evil twin.***

Es una técnica de *phishing* que utiliza una red inalámbrica. El atacante se coloca entre el usuario de Internet y un punto de acceso inalámbrico (AP) legítimo mediante el uso de un AP no autorizado. El atacante pone en funcionamiento un punto de acceso no autorizado con el mismo identificador SSID y frecuencia de un punto de acceso legítimo existente y lo coloca más cerca de la víctima para que reciba más señal y se conecte a este punto y no al legítimo, lo que hará que los atacantes puedas espiar todo el tráfico de red. Este tipo de ataque es frecuente en lugares públicos como estaciones de tren, aeropuertos, hoteles, etc.

## 3.3. EJEMPLOS REALES

El "*Phishing Activity Trends Report*" de APWG analiza los ataques de *phishing* y otras técnicas de robo de identidad, así como los datos que reciben por sus miembros (*Global Research Partners*) a través de su sitio web (www.apwg.org) y por correo electrónico. APWG mide la evolución, proliferación y propagación de métodos de robo de identidad a partir de la investigación sus empresas asociadas y expertos de la industria [8].

El informe revela que, en el primer trimestre de 2022, se observaron un total de 1.025.968 ataques de *phishing*, el peor trimestre para el *phishing* que APWG ha analizado hasta la fecha. Ha sido la primera vez que trimestralmente se superó el millón de casos. El APWG detectó 384.291 ataques en marzo de 2022, batiendo el

récord total mensual. En la Figura 6 se ve reflejada la evolución de los ataques de *phishing* desde abril de 2021 hasta marzo de 2022, con un claro aumento.

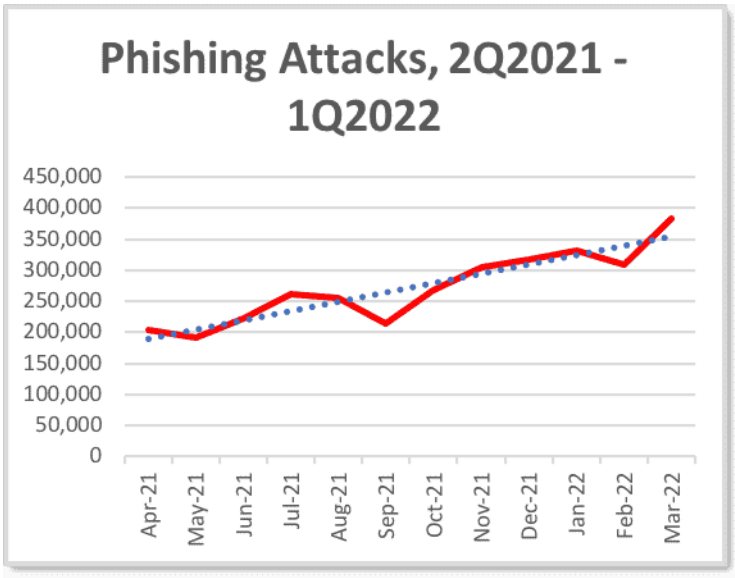


*Figura 6. Evolución de los ataques de Phishing hasta el primer trimestre de 2022 [9].*

Hubo un aumento del 7% en el robo de credenciales *phishing* contra usuarios empresariales y, además, el sector financiero fue el que más sufrió frecuentemente ataques de *phishing* en el primer trimestre, con el 23,6 % del total de ataques.

Según la APWG, y como se indica en la Figura 7, el mayor sector en recibir ataques de *phishing* sigue siendo el sector financiero y bancario, representando gran parte del total de los ataques de *phishing*. Han sido frecuentes los ataques contra proveedores de correo electrónico y software como servicio (SAAS). El comercio electrónico y las redes sociales ocupan los siguientes puestos en ataques de *phishing* y se ha notado levemente el ataque hacia el objetivo de las criptomonedas [9].


*Figura 7. Sectores más atacados por phishing en el primer trimestre de 2022 [9].*

Hoy en día, el mercado de las criptomonedas ha cobrado una especial importancia y una fuerza digital cada vez mayor (Figura 8), tanto que puede que no alcancen a tener actualizados sus sistemas y configuraciones de seguridad, lo que hace que los ciberdelincuentes se aprovechen de ello. La subida del valor del *Bitcoin* en los últimos tiempos ha hecho aumentar los ataques y estafas relacionados con las criptomonedas y sus carteras, recibiendo cantidad de *malware* [10].

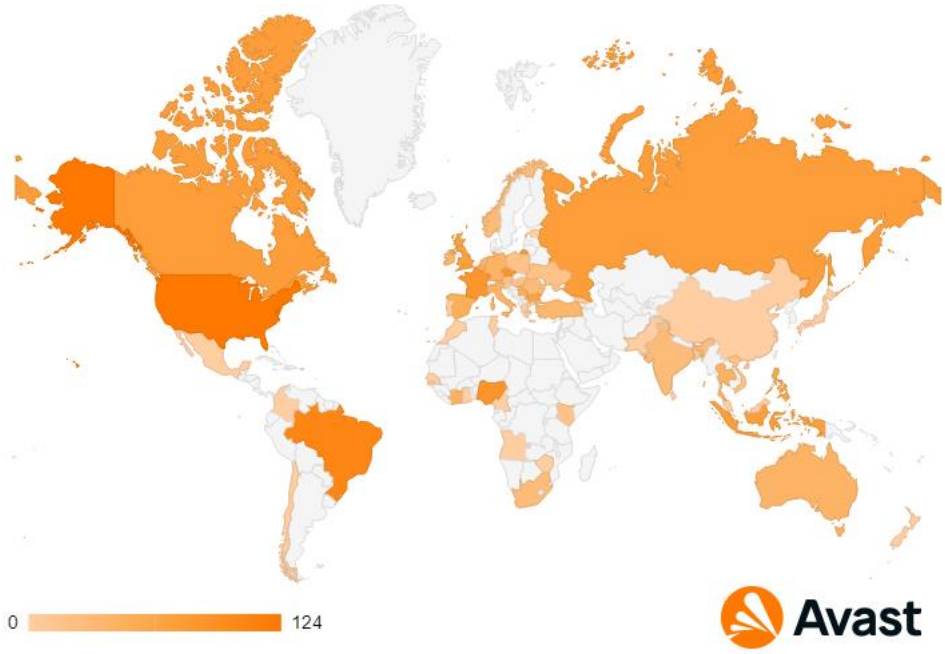


*Figura 8. Usuarios que visitan sitios de phishing relacionados con criptomonedas [10].*

Los ciberdelincuentes están en continuo estudio de técnicas de ataques, cada vez más avanzadas, para conseguir objetivos mayores y de elevado valor.

Recientemente han sido muchos los sistemas y servicios que se han visto afectados por algún tipo de ataque de *phishing*, desde empresas privada como *Dropbox*, *Microsoft*, Iberia, *Apple*…, instituciones públicas como la Agencia Tributaria y Servicio de Correos y Telégrafos, pasando por Fuerzas y Cuerpos de Seguridad del Estado como la Policía o la Guardia Civil y en una gran medida, entidades bancarias, en las que los ciberdelincuentes intentan robar las claves de acceso al servicio de banca online de los clientes o sus los datos bancarios, como el número de tarjeta de crédito o el CVV.

Con la llegada de la pandemia de la COVID-19 aumentaron los ataques relacionados con ella, sacando partido a las novedades que cada día nos llegaban sobre ella (Figura 9). Todo el mundo pasaba por momentos de incertidumbre, preocupación, falta de información en algunos casos y exceso en otros, en definitiva, los atacantes utilizaron el estado emocional de las personas para lanzar nuevos ataques [11].

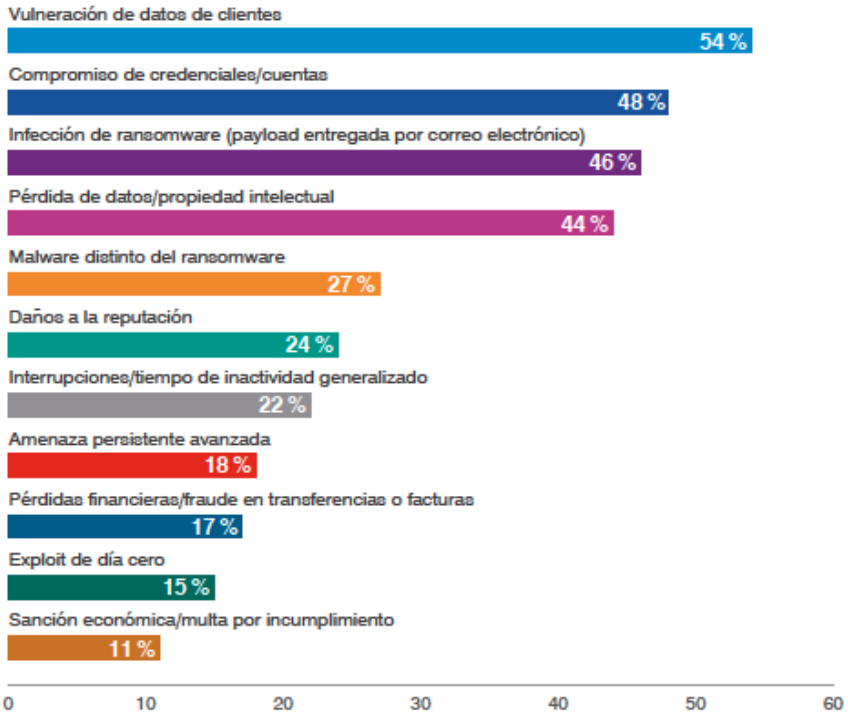


*Figura 9. Resultados de ataques de phishing que consiguieron su objetivo [11].*

Al aumentar las compras online debido a los confinamientos, tanto al por menor como al por mayor, empresas como *Amazon* o *Paypal* sufrieron varios ataques de *phishing*, al igual que *Microsoft*, *Google*, *Telegram* o *Zoom*, con el auge del teletrabajo en las empresas o el no poder ver a los familiares, que hicieron que las videollamadas crecieran exponencialmente en todo el mundo.

Así, se observó un amento en ataques telefónicos, junto con los mensajes de correo electrónico, sitios web o aplicaciones de dispositivos móviles, diseñadas de una manera cuidadosa para que el usuario caiga en la trampa más fácil y rápidamente. También aumentaron los ataques a los correos personales y no solo a los empresariales, ya que los trabajadores y sus familias usaron durante la pandemia equipos de las empresas, con lo que los atacantes se aprovecharon de la situación, al tener una delgada línea entre la vida personal y la laboral de los trabajadores.

Según el estudio del informe de *TreatLabz* de *Zscaler*, *Microsoft* fue la marca más imitada por los atacantes den 2021, con más del 31% de los ataques. Seguido de los sitios ilegales de *streaming*, sobre todo los relacionados con eventos deportivos [12]. En la Figura 10 se muestran las principales compañías atacadas.

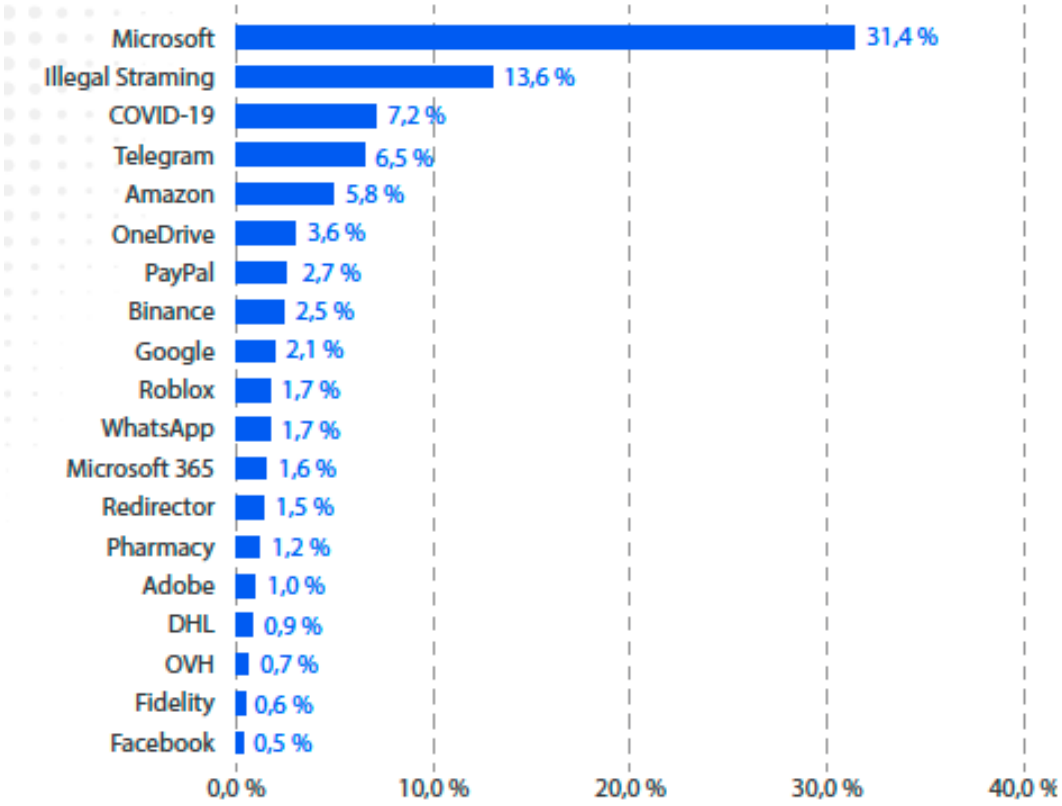


*Figura 10. Marcas más imitadas por phishing durante la pandemia COVID-19 [12].*

Como se ha mencionado anteriormente, está potenciándose el uso de kits de *phishing* entre los ciberdelincuentes, puesto que contienen lo necesario para realizar en tiempo récord un ataque contra miles de páginas o clientes, sin necesidad de tener unos conocimientos amplios de la materia.

Es más, incluso atacantes con amplios conocimientos en *phishing*, están ganando tiempo utilizando estos kits, sin la necesidad de romperse la cabeza desarrollando códigos o programas maliciosos para sus campañas de *phishing*, además de tener grandes posibilidades de éxito con sus ataques, puesto que son más difíciles de detectar por las víctimas.

Estos kits normalmente contienen archivos HTML junto con PHP, contenidos en un empaquetado con todo lo necesario para realizar el ataque, además de usar servicios externos para recopilas más información de las víctimas, como por ejemplo su localización o su IP.

Durante el tiempo de realización de este trabajo, se han recibido a través de SMS (*Smishing*) mensajes suplantando la identidad de diversos organismos. El Instituto Nacional de Ciberseguridad de España (INCIBE), a través de su Oficina de Seguridad del Internauta (OSI), y el Banco de España, han alertado de un notable aumento de los ataques de *Smishing* contra los clientes bancarios. Según [13], el uso de este tipo de ataque ha crecido exponencialmente, llegando a aumentar un 700 % en la primera mitad de 2021.

A continuación, se muestran algunos mensajes reales recibidos de *Smishing* durante los últimos meses de la realización de este trabajo. En las Figuras 11 y 13 se trata de casos de phishing entidades bancarias, mientras que en la Figura 12 se refleja un caso de ataque a Correos y en la Figura 14 a la Agencia Tributaria. Todos ellos contienen un enlace para que el destinatario pueda picar en el engaño y acceder a introducir sus credenciales en un sitio que para él pueda resultar real. Lo curioso de este tipo de intento de ataques es la recepción de mensajes de entidades bancarias con las que el usuario no trabaja, con lo que es muy fácil desecharlos y bloquear al número remitente. El problema está cuando el usuario sí es cliente de esas entidades bancarias, puesto que puede que ahí sienta cierta confianza y pique.

Empresas como Correos o la propia Agencia Tributaria son comunes en este tipo de ataques debido a que todo el mundo puede tener más probabilidades de acceder a esos enlaces malignos:

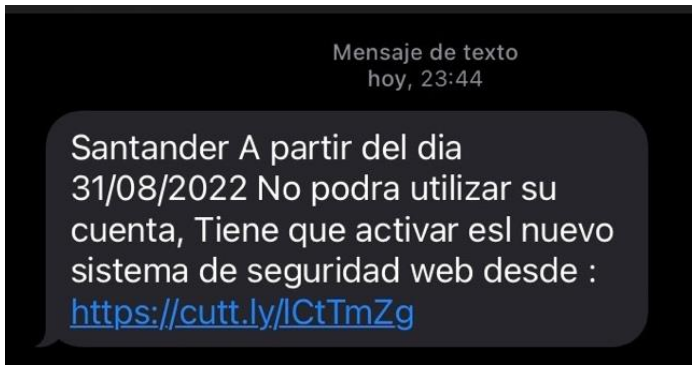


*Figura 11. SMS Phishing Banco Santander.*

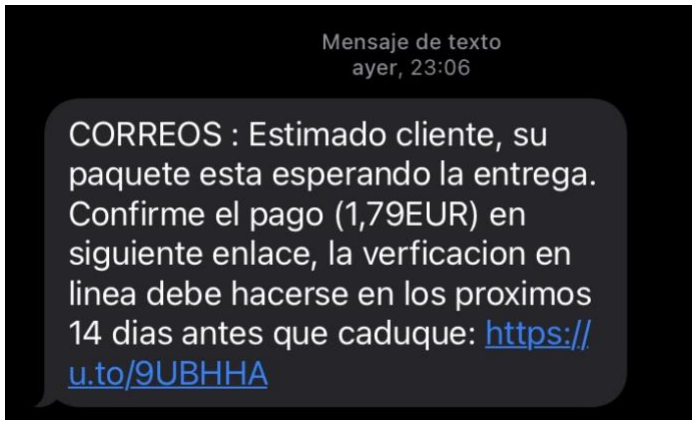


*Figura 12. SMS Phishing Correos.*

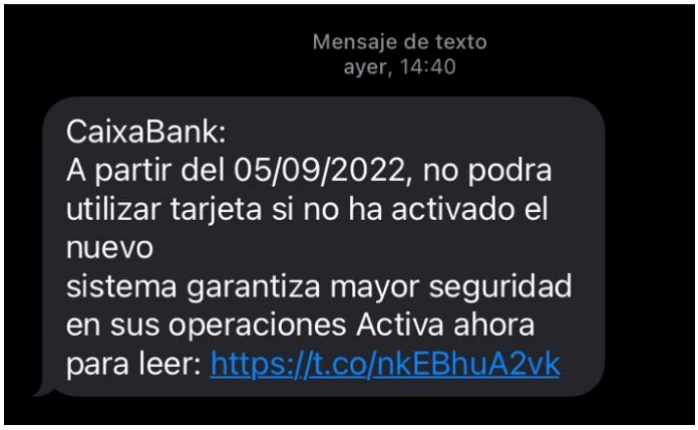


*Figura 13. SMS Phishing CaixaBank.*

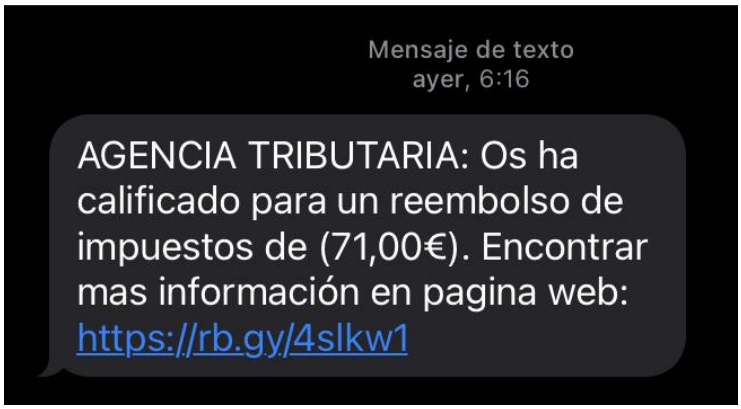


*Figura 14. SMS Phishing Agencia Tributaria.*

# 4. ANTI – PHISHING

En este capítulo se analizarán las distintas técnicas que existen para la prevención y detección de ataques de phishing, además de hacer una revisión de las herramientas de detección y análisis más utilizadas.

## 4.1. TÉCNICAS DE PREVENCIÓN

No existe un método infalible que nos haga prevenir los ataques de ingeniería social, ni mucho menos el *phishing*, que es uno de los más comunes. Es muy complicado detectarlos, más aún viendo el gran auge que tienen hoy en día. Los ciberatacantes estudian cada día nuevas técnicas más difíciles de detectar que las anteriores y así es imposible estar alerta siempre.

Los usuarios de dispositivos móviles y ordenadores deben mantener su información lo más privada posible, sobre todo la relacionada con datos bancarios, direcciones habituales de trabajo o domicilio, contraseñas y demás datos que puedan llevar a los ciberdelincuentes a causar daños importantes.

No deben dejarse engañar por correos electrónicos que reciban de sitios desconocidos preguntándoles por información personal, llegando a dar incluso plazos estrictos de respuesta ni se debe confiar en aquellos en los que avisan de premios e invitan a enviarles el número de cuenta o tarjeta bancaria para recibirlos, ejemplos muy comunes.

Se deben tener actualizados los sistemas con el software de seguridad más reciente, tener antivirus, filtros de spam, cortafuegos, etc. y conviene tener en los navegadores bloqueadores de publicidad, puesto que las ventanas emergentes, son en muchos casos una llamada de atención a algún enlace que contenga *phishing*, donde una vez que se accede, ya no hay marcha atrás.

La ingeniería social juega con la emoción y estado del usuario, que tiene miedo a perder información valiosa, por lo que puede decidirse a revelar a los atacantes su

información personal. Por otro lado, como se ha comentado anteriormente, los atacantes pueden hacer uso de algún tipo de *malware* que instala secretamente algún software en el dispositivo del usuario para acceder a sus datos.

Para prevenir ataques de *phishing*, se puede añadir una capa de seguridad cuando los usuarios inician sesión en algún sitio web: la autenticación de dos factores, lo que hace que el usuario tenga que confirmar su identidad antes de tener acceso al inicio de sesión de dicha web.

En la imagen que aparece a continuación (Figura 15) se muestra un ejemplo de autenticación de dos factores a través de SMS, algo muy común en sitios como *Gmail* o *Facebook*. Cuando el usuario introduce el nombre de usuario o correo electrónico y su contraseña para iniciar la sesión en el sitio web que desee, se le enviará a su teléfono móvil (previamente registrado como dato de contacto en dicha web) un SMS con un código de verificación que debe introducir para iniciar sesión en dicho sitio web. Además, estos códigos tienen un corto período de tiempo para ser introducidos antes de que caduquen y se tenga que volver a iniciar el proceso.


*Figura 15. Autenticación de dos factores a través de SMS [13].*

Son importantes también los gestores de contraseñas como medida de prevención de ataques de phishing. Almacenan los nombres de usuarios y las contraseñas, pudiendo también generar éstas de una manera segura, robustas, con una gran seguridad. Estos datos se almacenan en el navegador del usuario y se añaden automáticamente cuando se accede a algún sitio web con las credenciales almacenadas.

## 4.2. TÉCNICAS DE DETECCIÓN

Si comparamos la detección de *phishing* con la prevención, la primera es mucho más importante para poder solventar las consecuencias de un ataque. Se puede decir que la detección está dividida en dos categorías, como son la conciencia del propio usuario del dispositivo y la detección del software. A su vez, la detección del software puede dividirse en dos tipos: Métodos tradicionales y métodos automáticos [13].

La conciencia de los usuarios debe fomentar la identificación de los intentos de *phishing* que reciban. Deben de tener cuidado a la hora de visitar algunas páginas web, revisando la URL si sospechan que pueda ser algo malicioso, aunque pueden ser fácilmente engañados por los atacantes para que accedan al sitio web de *phishing* y para ello se debe introducir la detección por software para saber si la web es legítima o es *phishing*.

Según las estadísticas que se han visto, las organizaciones reciben a diario gran cantidad de ataques *phishing*. Es una labor muy complicada enfrentarse a esto, y aunque resulta imposible no tener ningún riesgo, sí se puede aprender a minimizarlo [12].

Lo más importante es que los usuarios comprendan los propios riesgos que corren para tomar decisiones sobre las tecnologías usadas, utilizar herramientas automatizadas, como antivirus y otras aplicaciones de seguridad, que las empresas impartan formación a sus trabajadores fomentando la concienciación de éstos sobre la importancia de la seguridad de los datos. Es muy importante también para las grandes organizaciones que realicen simulaciones de ataques de *phishing* para localizar los puntos débiles de ataque y mantenerse alerta.

El usuario debe prestar especial importancia cuando reciba un correo electrónico sospechoso, debe revisar los archivos adjuntos que contiene y no abrir ninguno de apariencia rara, fijarse bien en la redacción, ortografía, dirección de correo del remitente, en su firma y su manera de saludarle y dirigirse y también es importante que se pase el cursor por los hipervínculos que reciba en el mensaje, para ver si coincide el enlace con el texto.

En cuanto al método tradicional de detección por software, se utilizan las llamadas "*blacklist*" para administrar listas de sitios web de *phishing*, que son introducidas y actualizadas manualmente, teniendo como ventaja una gran precisión, pero como inconvenientes, puede pasar que no llegue a identificarse los sitios web de *phishing* de vida útil corta. Las litas negras más conocidas y utilizadas son *Google Safe Browsing, PhishTank* y *OpenPhish*.

Se ha intentado crear también listas blancas "*whitelist*", que por el contrario que las listas negras, contienen bases de datos de sitios web legítimos. Esto conlleva el problema de que la gran mayoría de los sitios web nuevos son identificados como sospechosos, por lo que los sitios que se espera que los usuarios visiten, deben estar incluidos en estas listas blancas, así que no es muy práctico ni fiable saber por adelantado lo que los usuarios visitan antes de dar con lo que realmente buscan.

Existe una técnica basada en listas blancas llamada *Pishzoo*, desarrollada por Afroz y Greenstat (2011) que lograba una precisión similar al enfoque basado en listas negras, utilizando criterios que diferencian un sitio web de otro, como imágenes, código HTML o certificados SSL. Se crea un perfil cuando un usuario accede a un sitio web y se contrasta con otros perfiles que existan en la lista blanca y si este coincide con alguno, se marca como fiable y sino, se marcará como sospechoso [15].

Los métodos automáticos de detección de software se clasifican en dos tipos: las barras de herramientas para los navegadores, que puedan detectar sitios fraudulentos que contengan *phishing*, advirtiendo al usuario y alertándolo cuando visita un sitio sospechoso, y los esquemas de detección/clasificación de *phishing*.

Los esquemas de detección/clasificación de *phishing* tienen como finalidad identificar y clasificar los sitios web en legítimos o *phishing*. Utilizan la inteligencia artificial (IA) mediante algoritmos de clasificación de aprendizaje supervisado para realizar la clasificación binaria del sitio web, siendo legítimo o *phishing*.

Hay muchos tipos de algoritmos de aprendizaje automático (ML) y aprendizaje profundo (DL). Los más comunes utilizados para la detección de phishing son SVM, regresión logística y métodos Bayesianos.

El uso de la inteligencia artificial se ha visto aumentado en los últimos tiempos en todos los campos, incluido, por supuesto, el de la ciberseguridad, aportando velocidad, precisión y detección de diferentes tipos de ataques (*spam*, *phishing*, etc…) utilizando conjuntos de datos previos.
Las técnicas de ataque se agrupan en dos categorías:

***Lanzamiento del ataque***, en el que se identifican varias técnicas, como la suplantación de correo electrónico, archivos adjuntos, suplantación de URLs, suplantación de sitios web, ataque MITM, *spear phishing*, falsos navegadores webs de dispositivos móviles, contenidos instalados a través de una web, etc.

***Recopilación de datos*** durante y después de la interacción de la víctima con los ataques, se utilizan diversas técnicas:

- *Automatizadas* (como formularios de sitios web falsos y *key loggers*).
- *Manuales* (como la distracción humana y las redes sociales).

Existen contramedidas para los datos que los atacantes recopilan de las víctimas o los que utilizan antes y después del ataque, que se utilizan para detectar y prevenir dichos ataques, las cuales se pueden clasificar en cuatro grupos [14]:

- Técnicas basadas en *Deep Learning* (DL).
- Técnicas basadas en *Machine Learning* (ML).
- Técnicas basadas en escenarios.
- Técnicas híbridas.

Las técnicas basadas en aprendizaje automático combinan la implementación de algoritmos y de métodos heurísticos para extraer los datos de los sitios web que se quieren analizar para saber si son *phishing* o son legítimos, puesto que al ser el *phishing* un problema de clasificación, parecen apropiadas para obtener las características de los sitios web y poder minimizar el problema de ser atacados.

Los sitios web tienen muchas funciones vinculadas, para mejorar el rendimiento del sistema predictivo es necesario procesar previamente las mismas para seleccionar las que sean más efectivas, midiéndolas a través de distintos métodos computacionales, como análisis de correlación, por ejemplo.
Se debe elegir el conjunto de características iniciales y después seleccionar el algoritmo para aplicarlo a éstas, generando el sistema predictivo. Estas características vienen dadas por una serie de heurísticas, como son la identidad de la URL, la identidad de los formularios de acceso, las direcciones IP sin nombre de dominio asociado, los números de puerto inválidos, las validaciones del código de país, etc [15]. Durante las últimas décadas, han sido muchos los algoritmos desarrollados de DL y ML para la clasificación, utilizando principalmente los siguientes métodos [16]:

- Árboles de decisión.
- Modelos probabilísticos.
- Reglas de clasificación (clasificación asociativa, basada en asociación múltiple o en asociación multiclase).
- Redes neuronales.
- SVM.
- Lógica difusa (FL).
- Métodos de paginación o impulso.
- Métodos de búsqueda (algoritmos genéricos).

Es posible detectar casos de *phishing* con la supervisión de los certificados SSL emitidos para un sitio web, de manera que el dueño de ese sitio web pueda ver que el certificado emitido correcto. Esto se hace a través de la llamada *Certificate Transparency*, que se ha convertido en un proyecto al que se han unido ya muchas grandes instituciones o empresas, como por ejemplo Google o Facebook, mediante el cual se supervisan conjuntamente la legitimidad de los certificados. Se puede observar un esquema en la Figura 16:

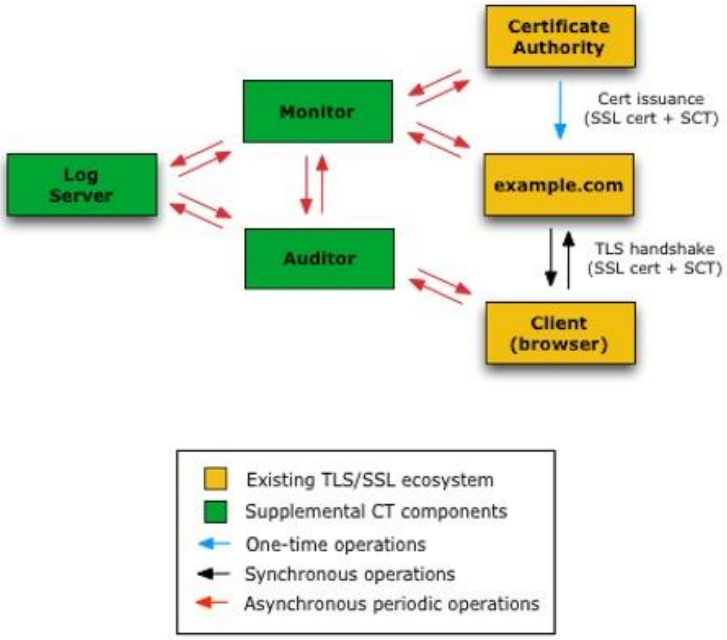


Figura 16. Esquema detección certificados SSL.

Una de las técnicas más comunes utilizadas por los *phishers* es engañar a los usuarios a través del correo electrónico, lo que se conoce como *spoofing*, que se ha visto anteriormente en el apartado 3.2.

Para evitar que los atacantes envíen correos intentando suplantar la identidad de algún organismo, institución o persona, proporcionando más seguridad a los servidores de destino y evitando ser catalogados como spam, existen los protocolos de autenticación SPF, DKIM y DMARC [17].

- SPF especifica qué IP's pueden enviar correos electrónicos utilizando el dominio en cuestión. Es eficaz contra los ataques de *phishing*.
- DKIM añade una firma digital a los mensajes que se envían, permitiendo a los servidores comprobar que realmente proceden de una organización real.
- DMARC indica a los servidores que reciben los correos qué se debe hacer con los mensajes que no han sido filtrados con los protocolos SPF y DKIM.

## 4.3. HERRAMIENTAS DE DETECCIÓN Y ANÁLISIS

La mayoría de las herramientas de detección se basan en la similitud de una página fraudulenta a otra legítima, estando basados en reconocimiento de imágenes mediante inteligencia artificial, o utilizando el análisis semántico con *machine learning*.

También es frecuente la extracción de una serie de indicadores de compromiso de una página legítima para contrastarla con páginas fraudulentas, siendo esto más sencillo computacionalmente que con inteligencia artificial, minería de datos o *machine learning*.

Se han revisado también estudios que utilizan el uso de las redes sociales y búsqueda en fuentes abiertas para la detección de páginas fraudulentas, como "*PhishAri*", que se basaba en la detección de *phishing* en tiempo real en *Twitter* (Aggarwal, A., Rajadesingan, A., Kumaraguru, P.).

En los últimos tiempos han sido creados muchos sitios web privados que ofrecen servicios a los usuarios con información acerca de los dominios que se registran a diario, ofrecen la posibilidad de analizar y evaluar los sitios web que los usuarios introducen con diversos antivirus y servicios de detección de malware, creando reportes que ayudan a los futuros visitantes de estos servicios.

A continuación, se van a describir algunos de estos servicios web más utilizados para ayudar a los usuarios a detectar sitios *phishing* y disminuir sus posibles ataques y daños:

- **Phishing Quiz**

Es un test de autoevaluación lanzado por *Google* donde hace ver a los usuarios la importancia de revisar las URL's que contienen el mail antes de acceder a ellas. *Google* quiere que el usuario se autoevalúe para que entienda los riesgos que puede correr y ser consciente de las trampas a las que está expuesto día tras día, debiendo tener especial cuidado con los dominios engañosos que aparentemente parecen legítimos, pero terminan siendo falsos.

Se puede acceder a este test a través del siguiente enlace:
https://phishingquiz.withgoogle.com/

En las Figuras 17, 18, 19 y 20 se muestra su funcionamiento:

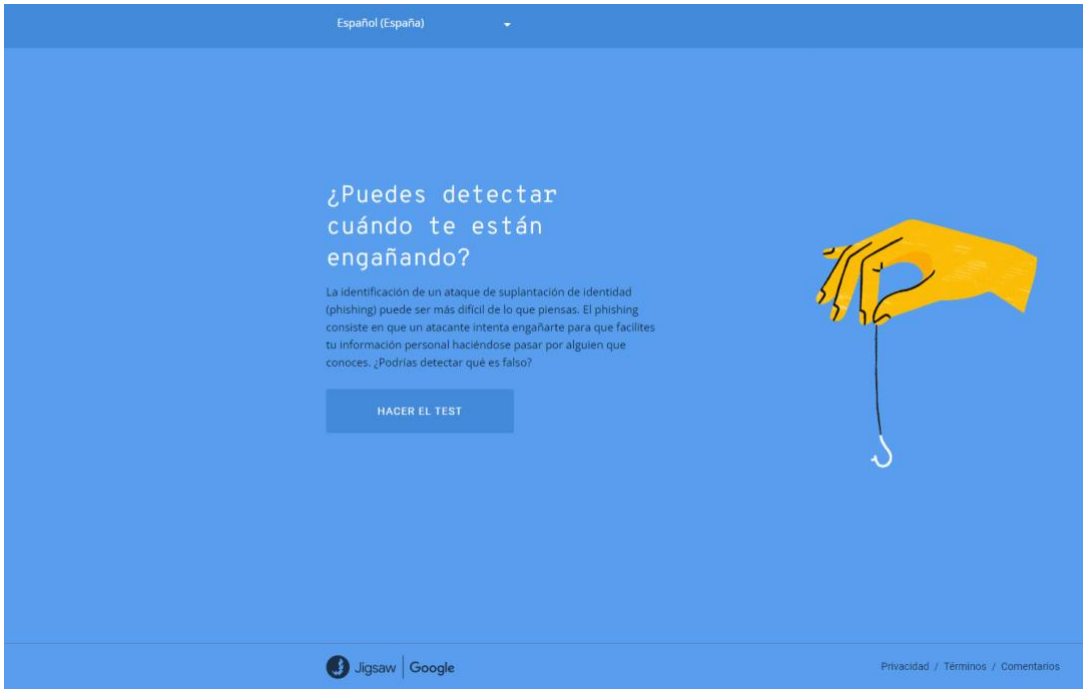


*Figura 17. Phishing Quiz de Google.*


*Figura 18. PhishingQuiz - Introducción datos.*

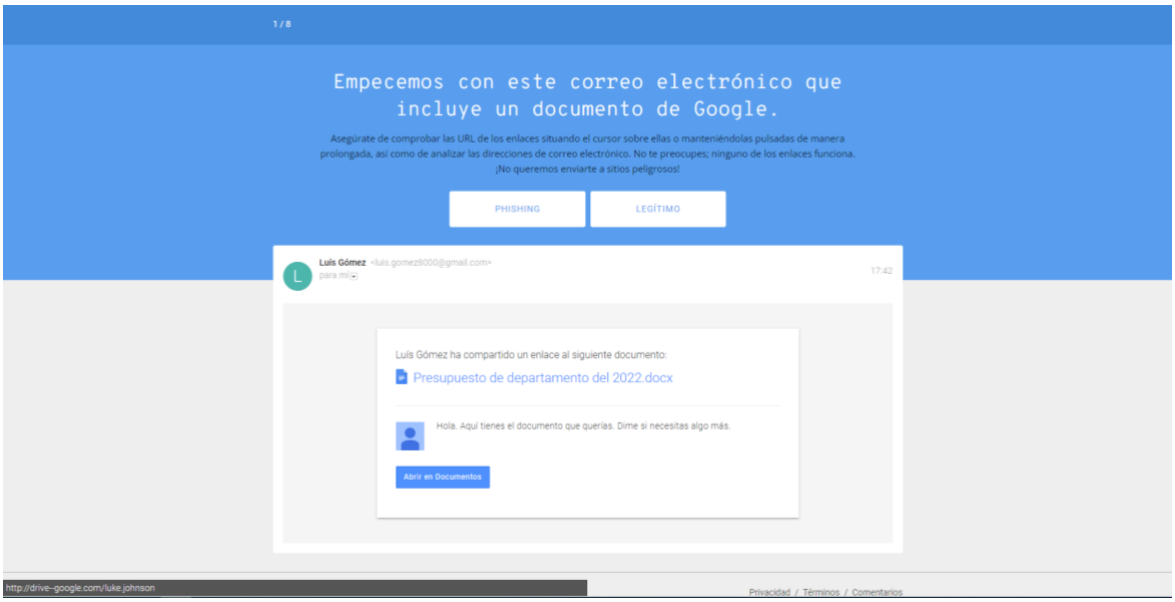


*Figura 19. PhishingQuiz - Correo electrónico.*

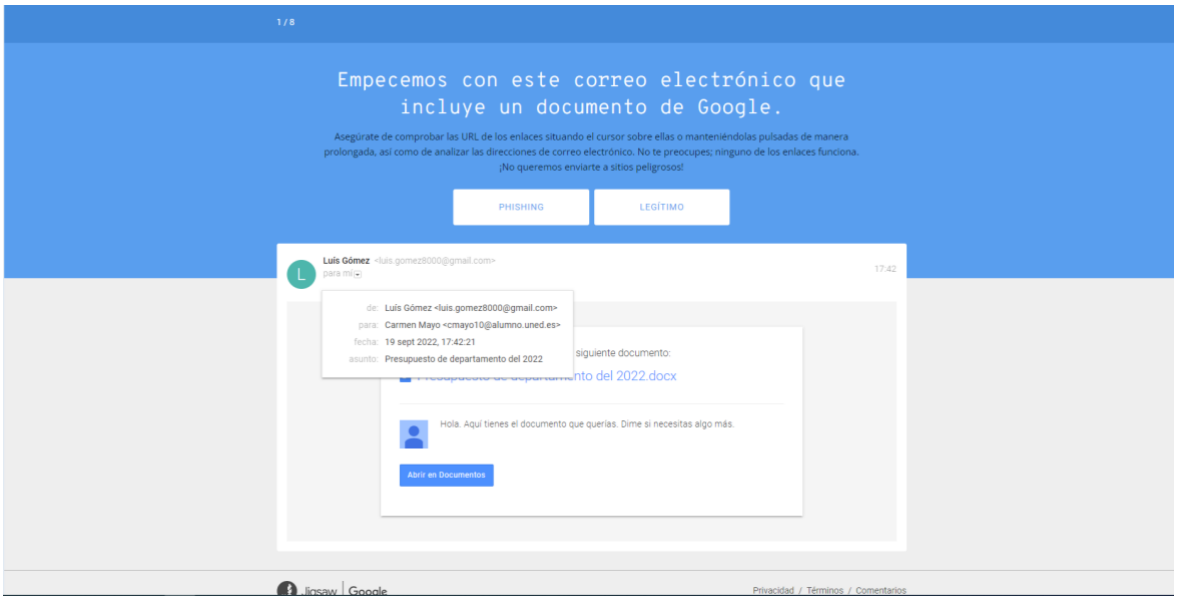


*Figura 20. PhishingQuiz - Ejemplo email enviado.*

- **Whoxy**

*Whoxy* es un motor de búsqueda de WHOIS. La API de *Whoxy* es un servicio web que consulta los registros de WHOIS de días concretos y analiza los datos devueltos en XML o JSON bien estructurados, pudiendo filtrar los resultados de los dominios que contengan palabras parecidas al dominio que se desee analizar. *Whoxy* también ofrece búsqueda inversa o búsqueda de historial, como se puede observar en la Figura 21. La API está disponible en planes de servicio de suscripción gratuitos o de pago para poder utilizar sus opciones más completas.

Está disponible en: https://www.whoxy.com/.


*Figura 21. Whoxy - Motor de búsqueda de WHOIS.*

- **Phishtank**

Es una herramienta gratuita que fue lanzada en 2006 para detectar URL's maliciosas, entre las que se incluyen *malware* y enlaces de *phishing*.

Este verificador de enlaces escanea las direcciones en busca de *malware*, virus, estafas y enlaces de *phishing* y además los usuarios pueden reportar las URL's maliciosas que encuentren. En la figura 22 se muestra la página principal de *Phishtank*.

Esta herramienta se encuentra disponible en: https://phishtank.org.

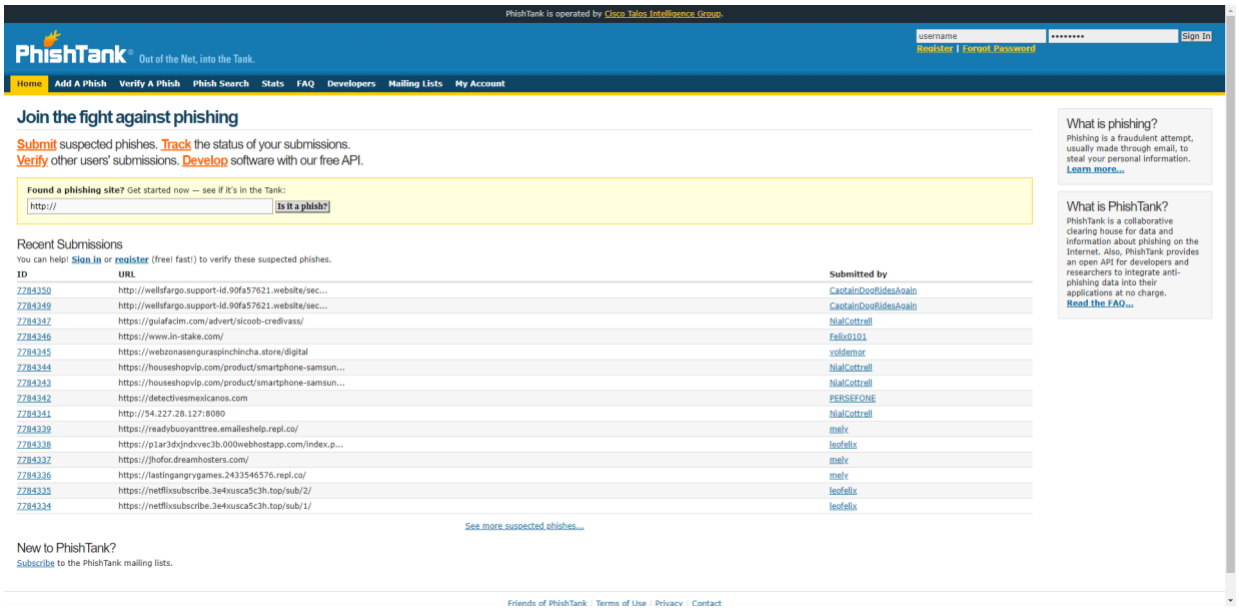


*Figura 22. Herramienta Phishtank.*

Analizamos la URL de www.uned.es (Figura 23):

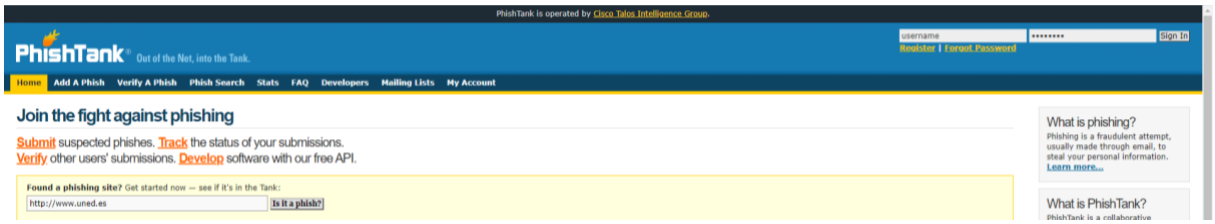


*Figura 23. Ejemplo de funcionamiento de Phishtak.*

El resultado que nos aparece es que el sistema no conoce nada acerca de esta web, como se aprecia en la Figura 24.

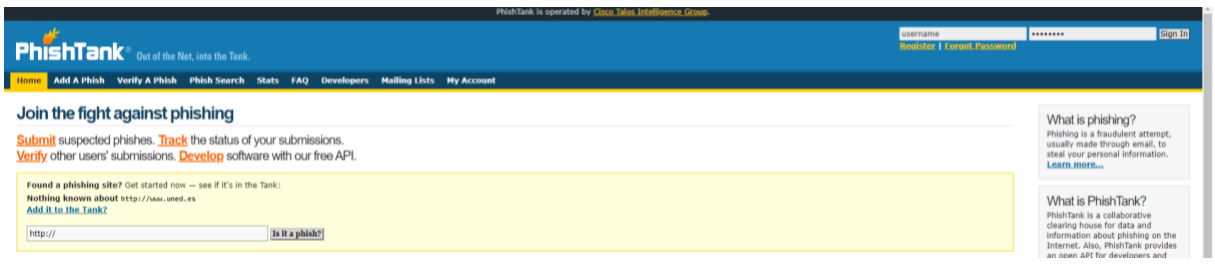


*Figura 24. Resultado análisis enlace con Phishtank.*

Ahora vamos a introducir el *link* de Google, tal como mostramos a continuación en la Figura 25:


*Figura 25. Análisis www.google.com con Phishtank.*

Y evidentemente nos aparece que el sitio es legítimo (Figura 26):

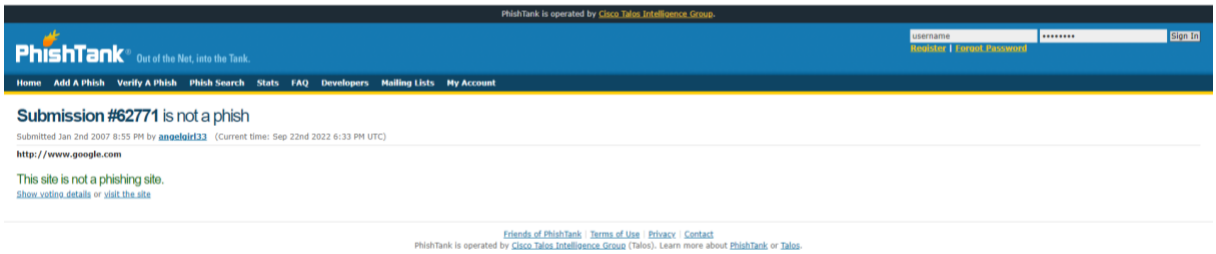


*Figura 26. Resultado de analizar un sitio legítimo con Phishtank.*

En cambio, si analizamos una de las últimas búsquedas que otros usuarios han hecho en *Phishtank*, nos encontramos con que es un sitio ilegítimo, como se ve en la Figuras 27 y 28:

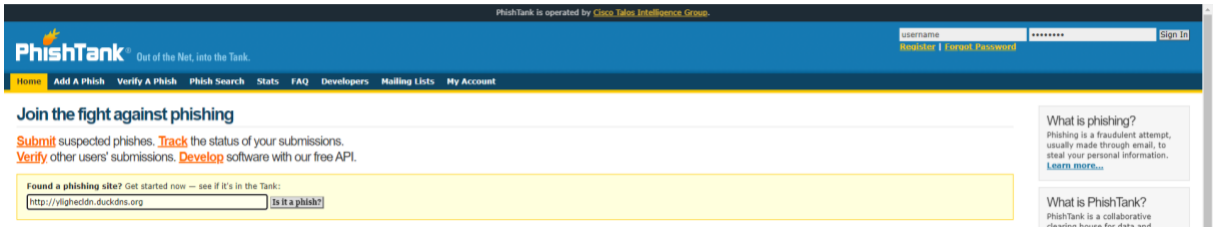


*Figura 27. Análisis sitio ilegítimo con Phishtank.*

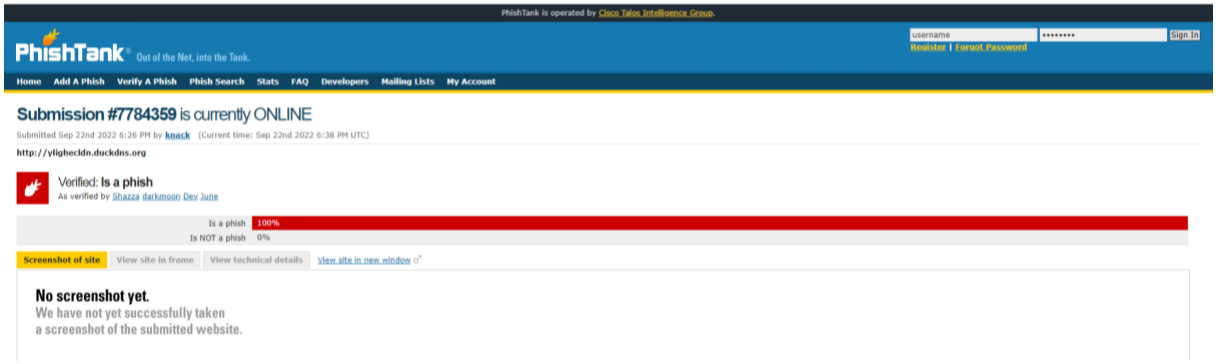


*Figura 28. Resultado análisis phishing detectado con Phishtank.*

- **ScamSearch**

El usuario puede tanto reportar como buscar sitios fraudulentos a través de imágenes, correos electrónicos, nombres de usuario, teléfonos o sitios web. Dispone de una versión gratuita de prueba y versiones más completas de pago, con diferentes suscripciones.

Se puede acceder a través de: https://scamsearch.io/.

En este caso, como en anteriores pruebas, se ha buscado el sitio www.uned.es (Figura 29).

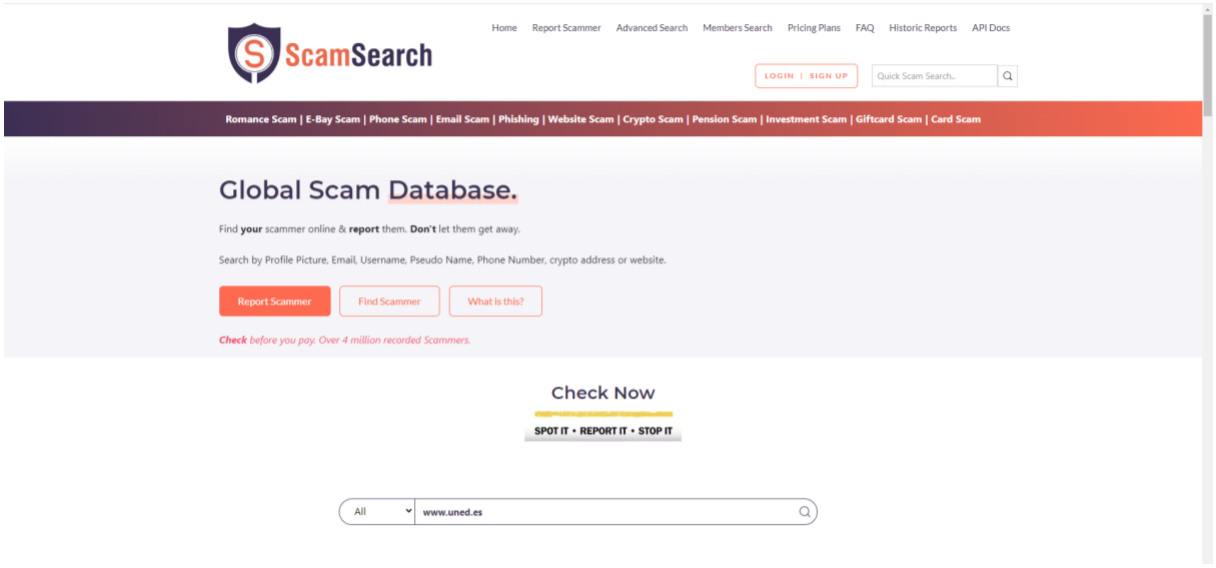


*Figura 29. Escaneo de la web de la UNED con ScanSearch.*

Como se aprecia en la Figura 30, el sitio analizado de www.uned.es no ha sido nunca reportado como *phishing*.

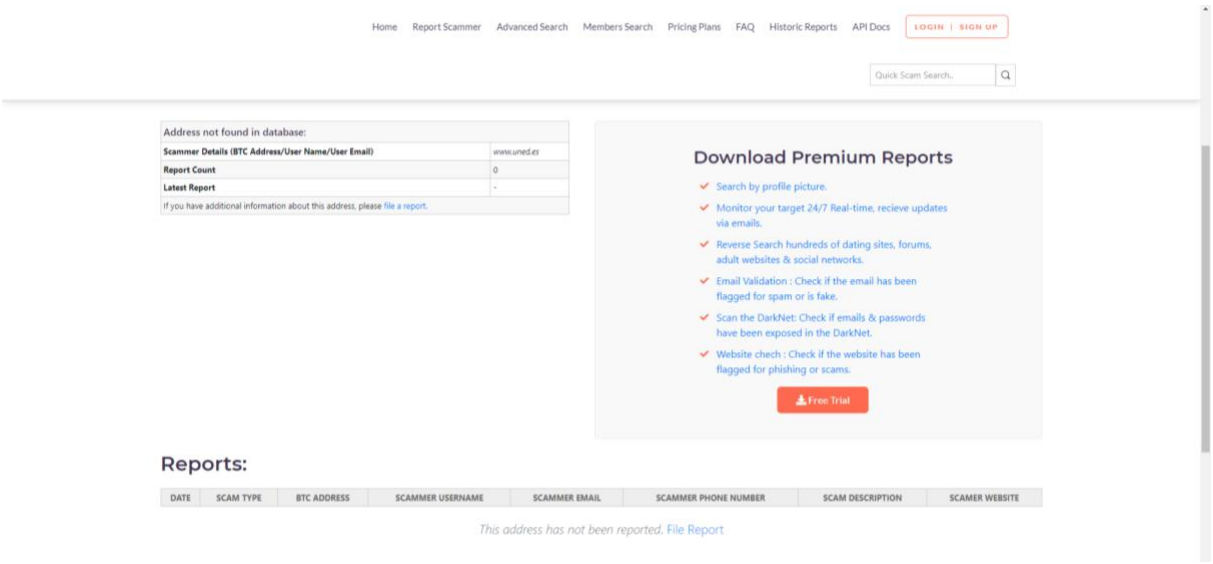


*Figura 30. Sitio legítimo que nunca se ha reportado como Phishing.*

Ahora analizamos un sitio que se ha localizado anteriormente como *phishing* (Figura 31) y se muestran los resultados obtenidos en las Figuras 32 y 33:

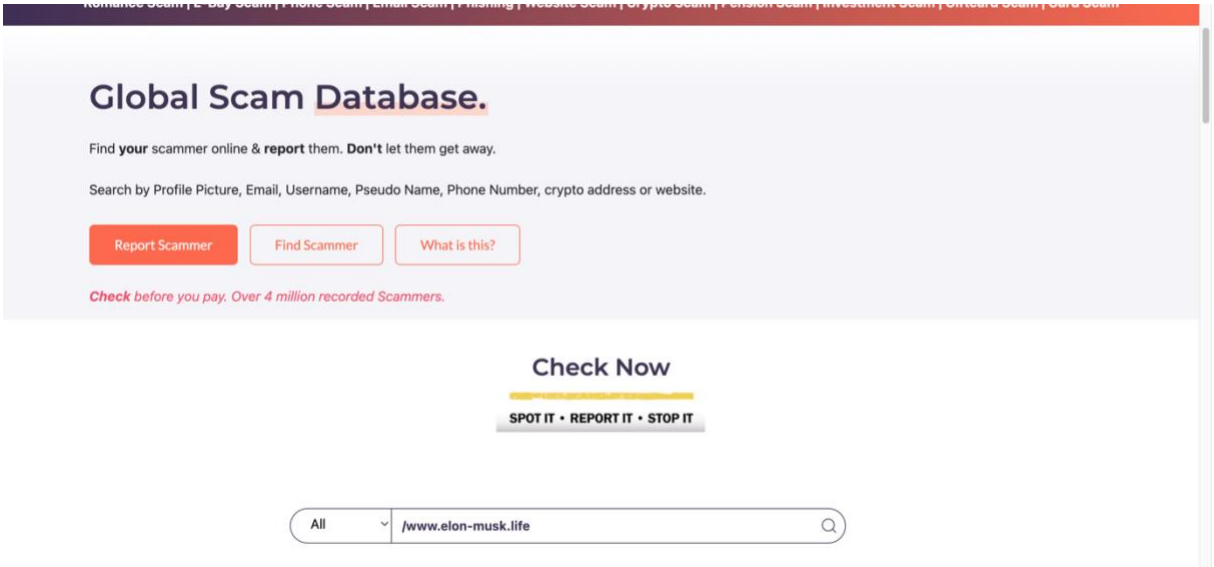


*Figura 31. Comprobación sitio identificado como phishing.*

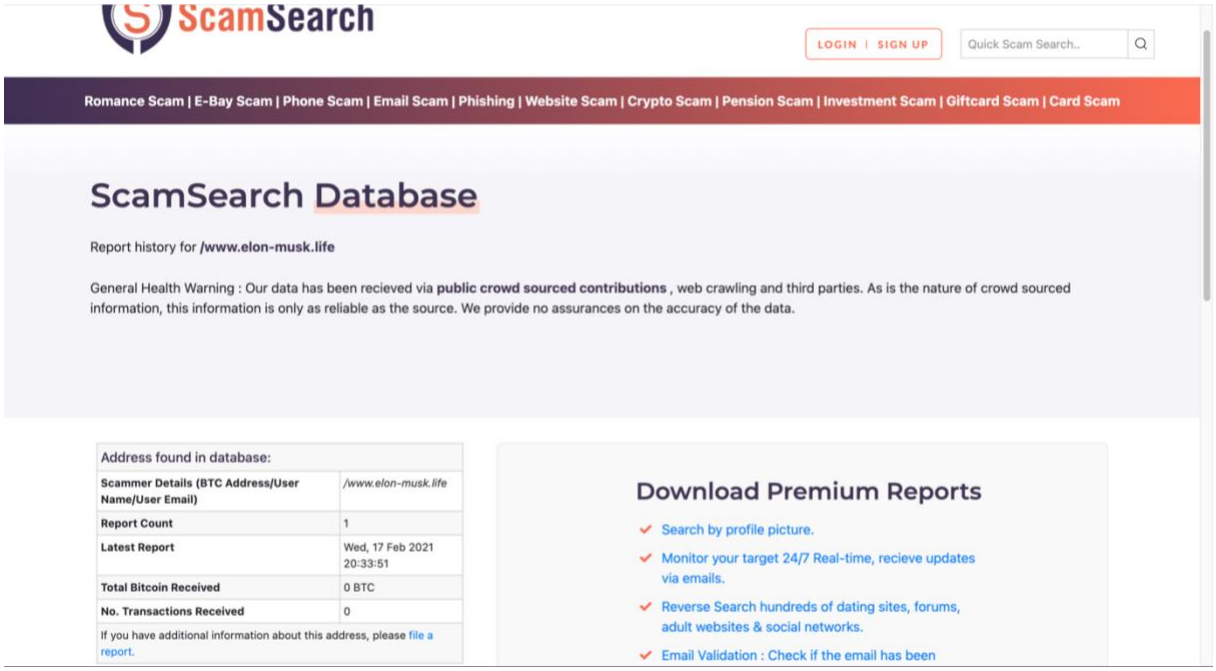


*Figura 32. Muestra del último reporte de sitio phishing.*

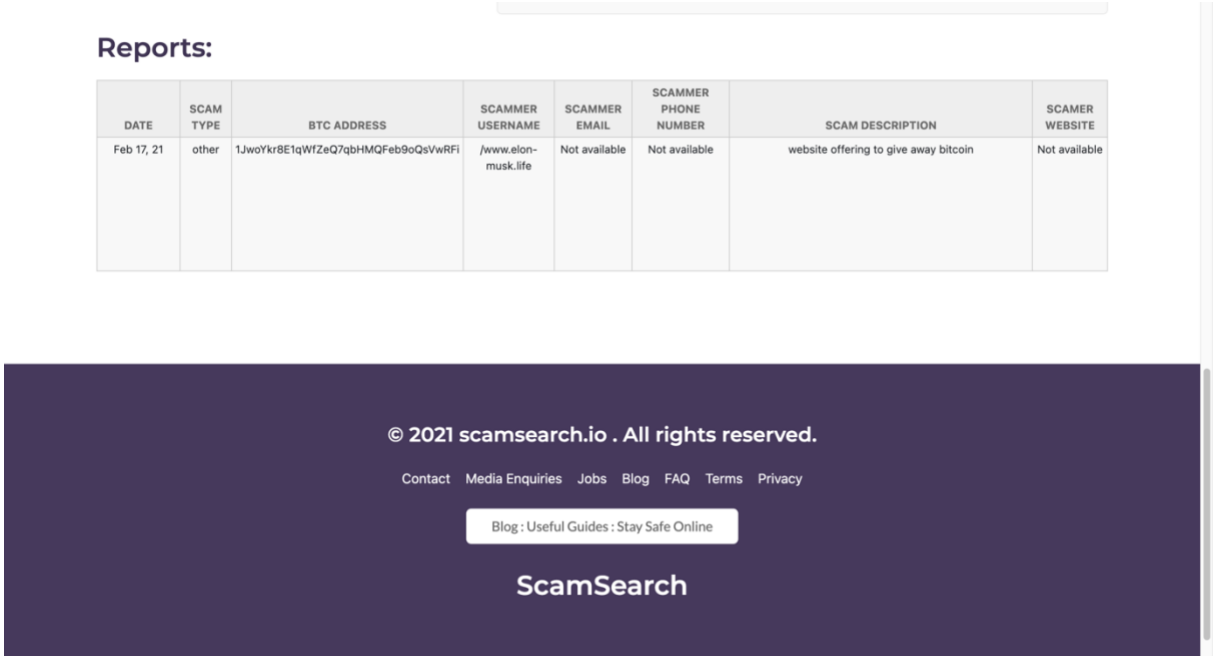


*Figura 33. Sitio detectado como phishing y último reporte.*

- **VirusTotal**

Es un sitio web desarrollado en España por la empresa de seguridad Hispasec Sistemas, donde se proporciona gratuitamente el análisis de archivos y sitios web mediante una serie de antivirus en línea (Ver Figura 34). Desde hace unos años es propiedad de Google.

Funciona con la integración de más de 50 antivirus que le proporcionan su servicio, entre los que se encuentran algunos muy conocidos, como *AVAST, AVG, Doctor Web*, *Kaspersky*, *McAfee* o *Norton*.

Disponible en: https://www.virustotal.com/gui/home/upload.


*Figura 34. VirusTotal - Antivirus en línea.*

Si analizamos un sitio web identificado anteriormente en el estudio de este trabajo, podemos ver en la Figura 35 cómo se muestran los resultados en los diferentes antivirus, siendo detectado como *phishing* en 9 de ellos.

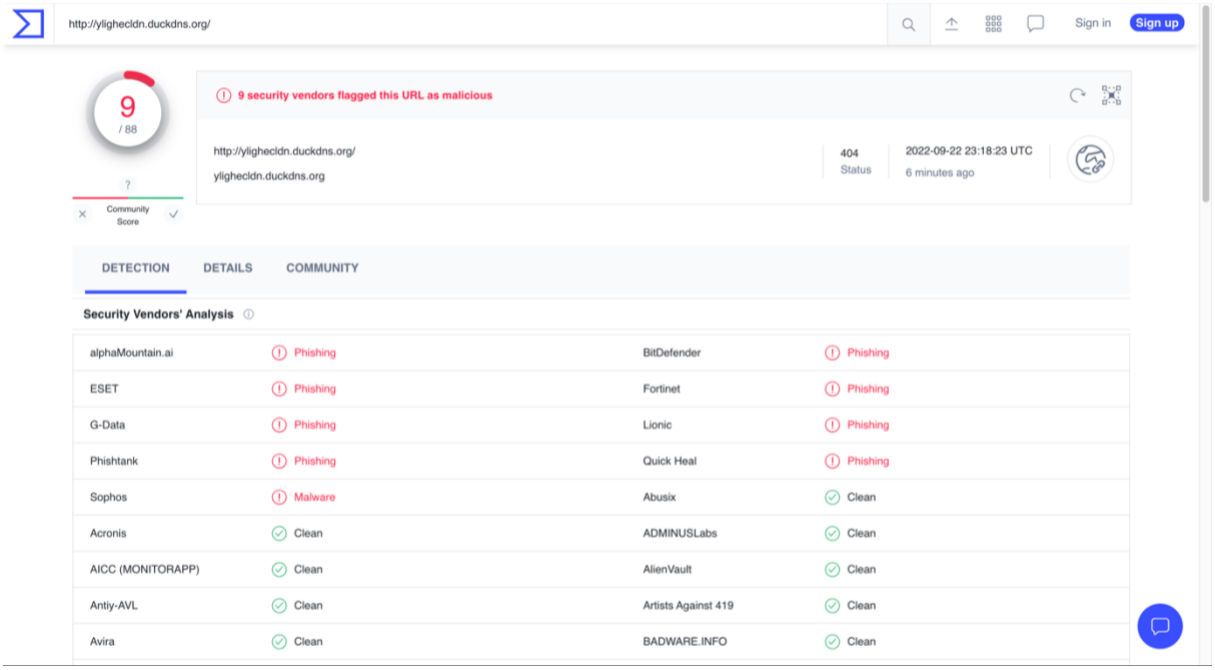


*Figura 35. VirusTotal - Resultados análisis sitio web.*

- **Google Informe de Transparencia**

En este portal, *Google* recoge información sobre cómo políticas y acciones de empresas, instituciones o gobiernos pueden afectar a la privacidad, seguridad y acceso a la información (Figura 36).

Está disponible en: https://transparencyreport.google.com/?hl=es.


*Figura 36. Google Informe de Transparencia.*

- **URL Void**

Esta herramienta permite detectar sitios web que contengan *phishing* o cualquier otro tipo de *malware*, analizándolos en busca de amenazas y verificando si están en alguna *blacklist*. Finalmente reporta al usuario un informe detallado con el análisis.

Entre sus funciones principales, además de analizar sitios web, destacan la búsqueda de Whois, DNS, generador de contraseñas, geolocalización de IP, etc. Es una herramienta muy completa y que ofrece muchas posibilidades.

Se encuentra en: https://www.urlvoid.com/.

En la Figura 37 se muestra cómo es su interfaz y se introduce un sitio web anteriormente hallado como phishing para que nos muestre su análisis:

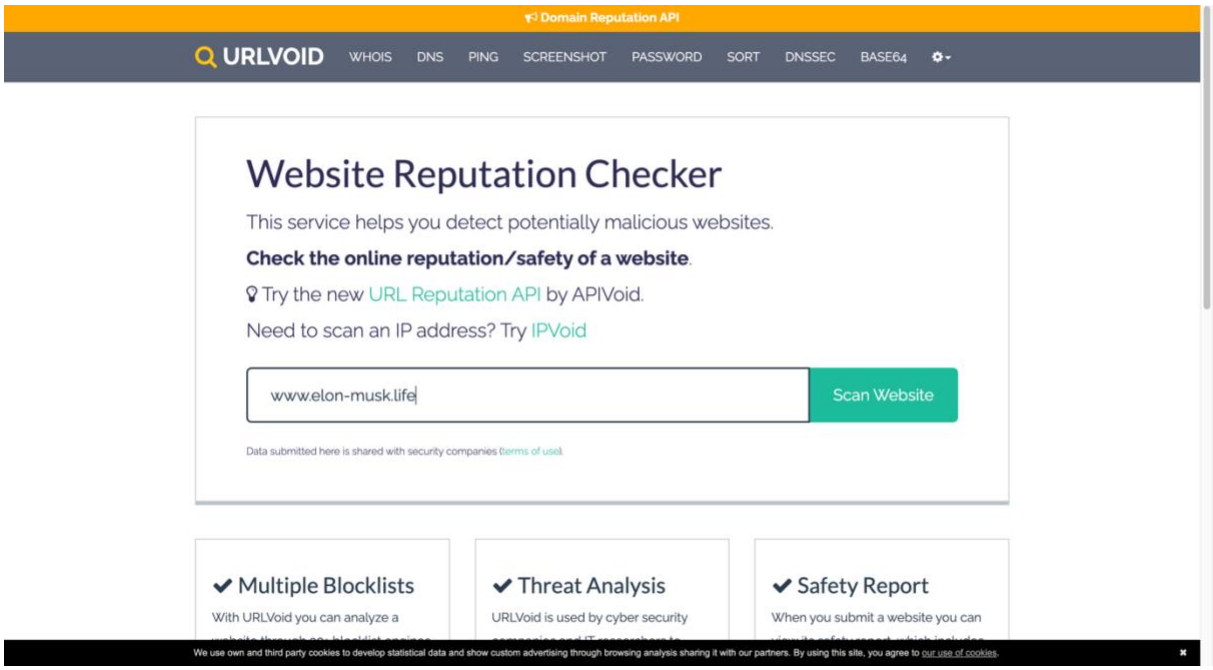


*Figura 37. Interfaz web de URL Void.*

A continuación, en la Figura 38, se muestran los resultados del análisis:

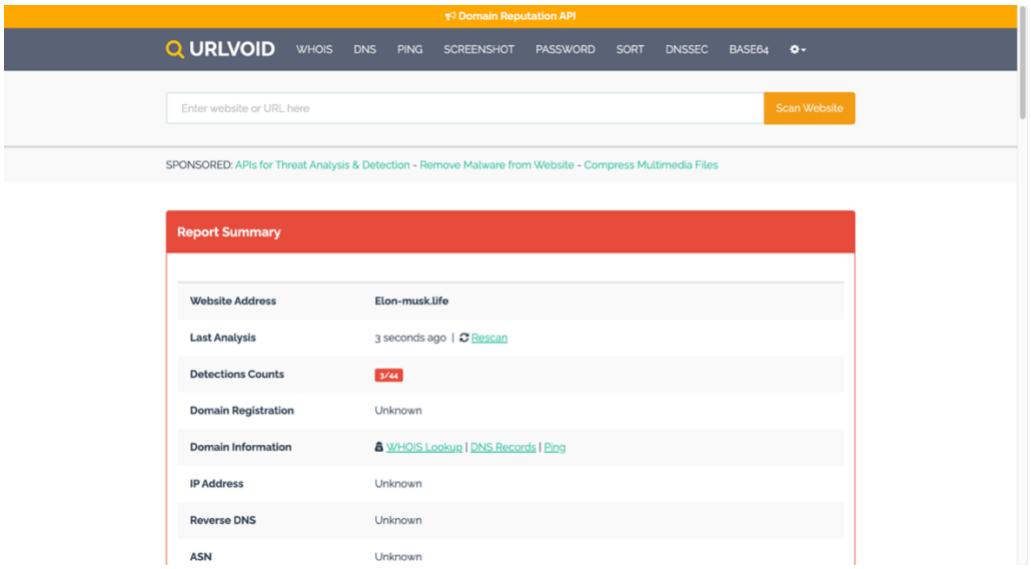


*Figura 38. Resultados del análisis con URL Void.*

- **ISIT Phishing**

Desarrollado por *Vade*, es un servicio que se ofrece gratuitamente con el deseo expreso de combatir el phishing. En la Figura 39 se muestra su interfaz.

Se encuentra disponible en https://www.isitphishing.ai/.

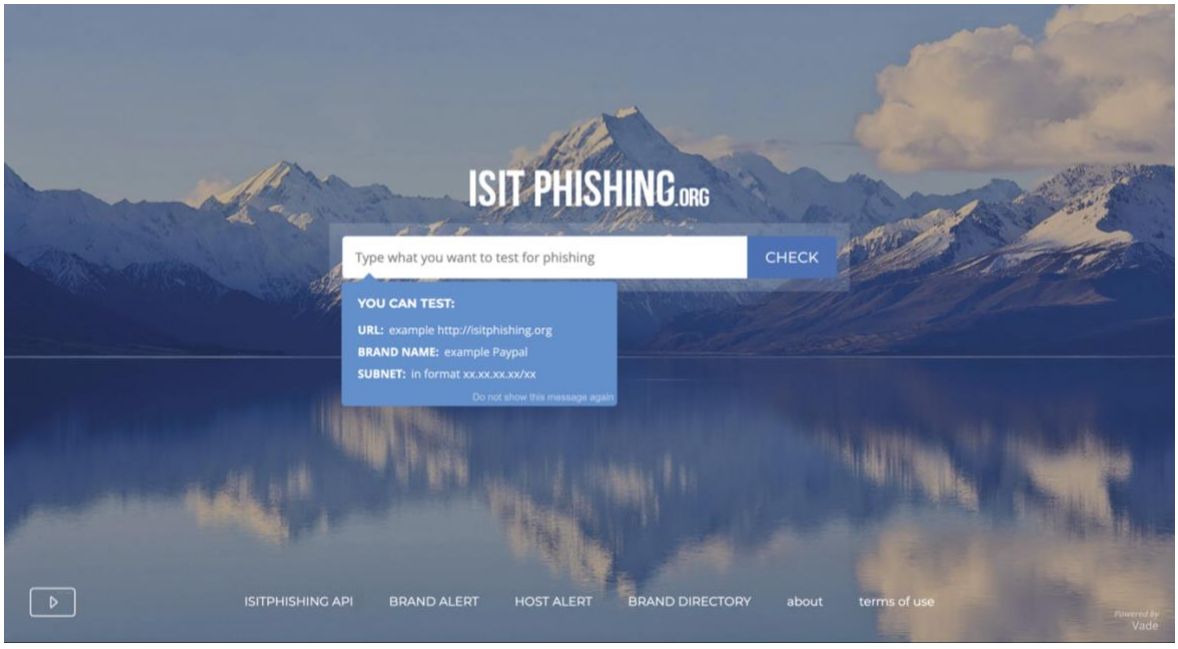


*Figura 39. Interfaz ISIT Phishing.*

- **Desenmascara**

Es un servicio de seguridad web especializado en tiendas. Analiza los resultados de los enlaces web para mostrar si es fiable y oficial o es un sitio falso y, por tanto, podría ser phishing, ya que cuando un usuario realiza una compra online son muchos los datos que se introducen y un buen cebo para los ciberdelincuentes. Se muestran los sitios web más falsificados en el momento (Figura 40).

Disponible en: https://desenmascara.me/.

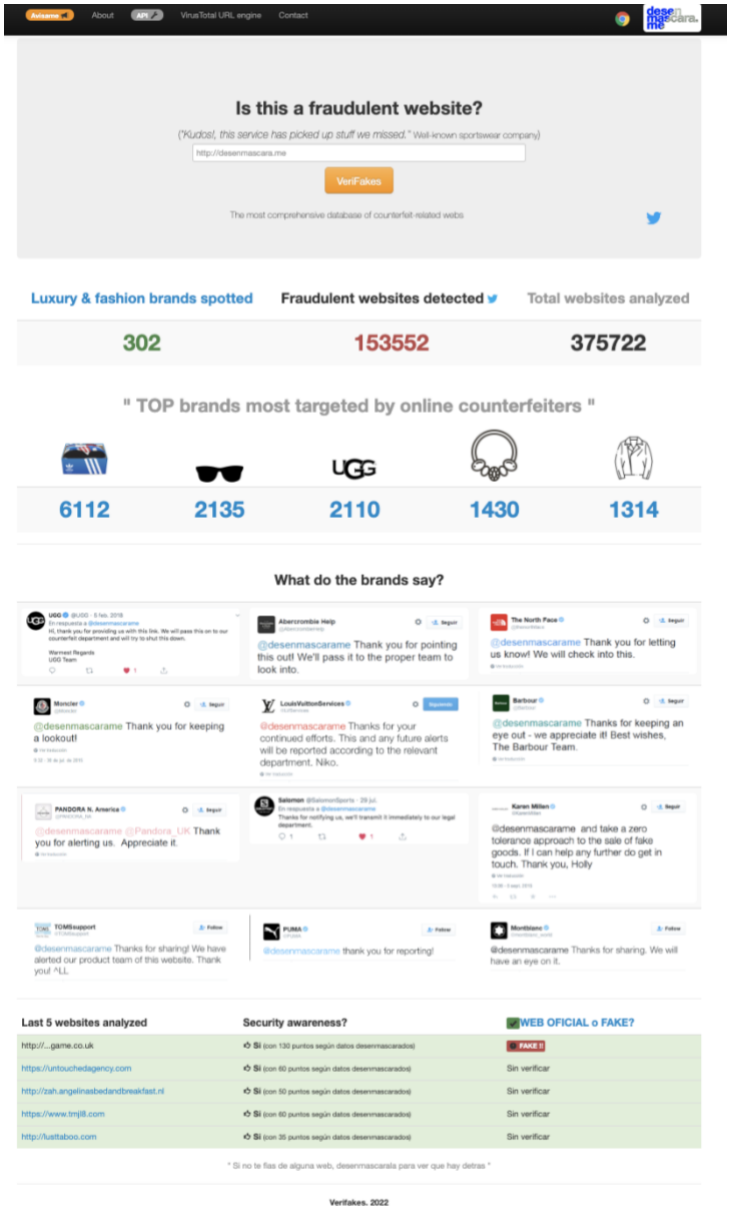


*Figura 40. Interfaz Desenmascara.*

Se ha buscado el sitio web de *Amazon*, y en las Figuras 41 y 42 se muestran los resultados obtenidos. Como se puede apreciar, son muy completos y precisos.

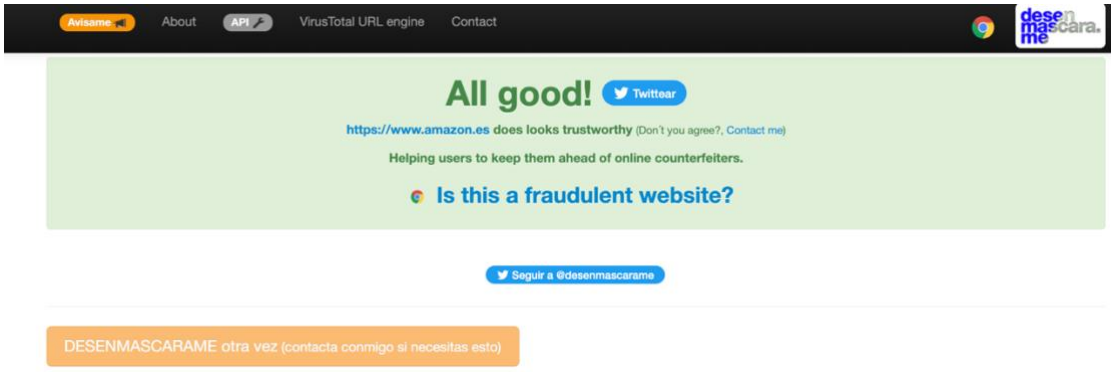


*Figura 41. Análisis www.amazon.es con Desenmascara.*

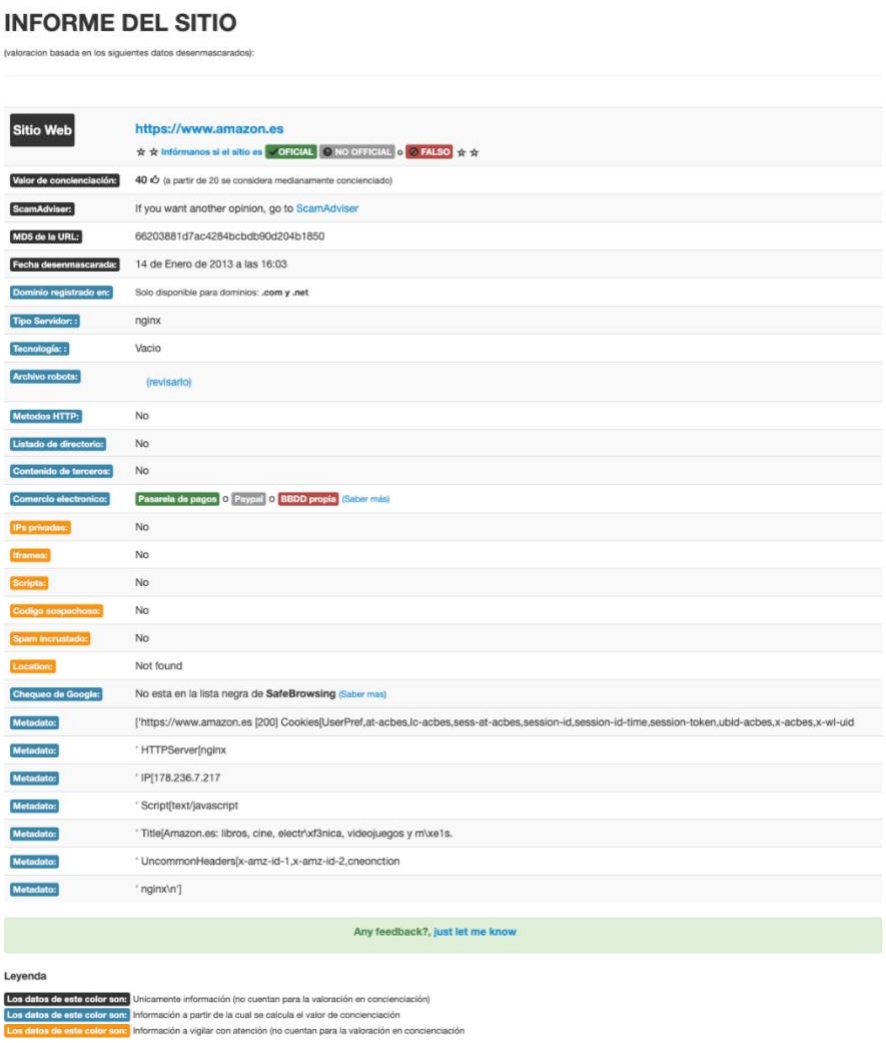


*Figura 42. Resultados del análisis de Amazon con Desenmascara.*

- **OpenPhish**

Ofrece un listado de sitios web que han sido detectados y categorizados como *phishing* por una comunidad de usuarios. Se pueden descargar y exportar. En la Figura 43 se pueden ver los últimos enlaces detectados como *phishing* en el momento del acceso al portal.

Disponible en: https://openphish.com/.

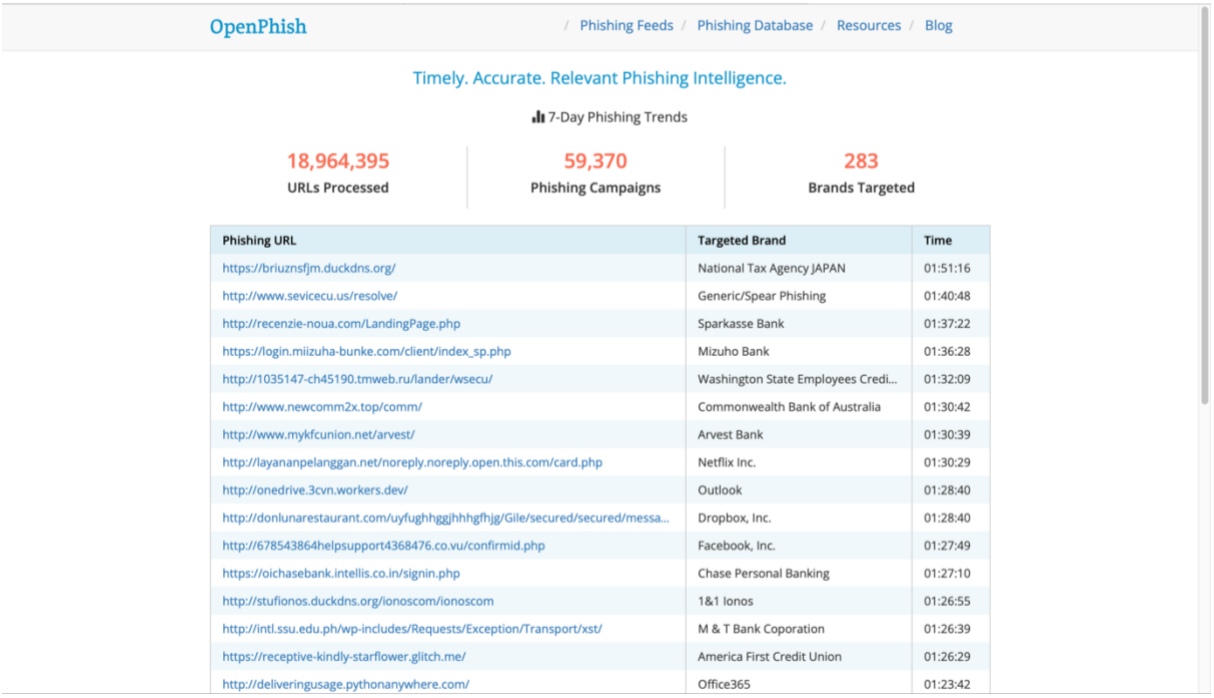


*Figura 43. Interfaz de OpenPhish.*

- **Talos Intelligence**

*Talos* es una división de *Cisco* creada para hacer frente a las amenazas. Está formada por cientos de ingenieros y expertos en ciberseguridad que hacen que la aplicación detecte y proteja de las amenazas. Se basa en la utilización de las redes de *Cisco*, combinando y analizando datos como peticiones web, emails o *malware*.

Está formada por cinco grandes áreas [18]:

- *Detection Research* (análisis de *malware* y vulnerabilidades para diseñar el código capaz de detener las amenazas en todos los **dispositivos de seguridad** de *Cisco*).

- *Threat Intelligence* (correlación y seguimiento de amenazas).

- *Engine Development* (mantenimiento y actualización de los motores de inspección para que puedan detectar amenazas emergentes).

- *Vulnerability Research & Development* (diseño de las herramientas y metodología para identificar ataques de 'día cero' y brechas de seguridad en plataformas y sistemas operativos que utilizan los clientes de *Cisco*).

- *Outreach* (investigación, identificación y divulgación de nuevas tendencias y técnicas de los ciberdelincuentes).

En la Figura 44 se muestra la interfaz del portal *Talos*, que se encuentra disponible en: https://www.talosintelligence.com/.

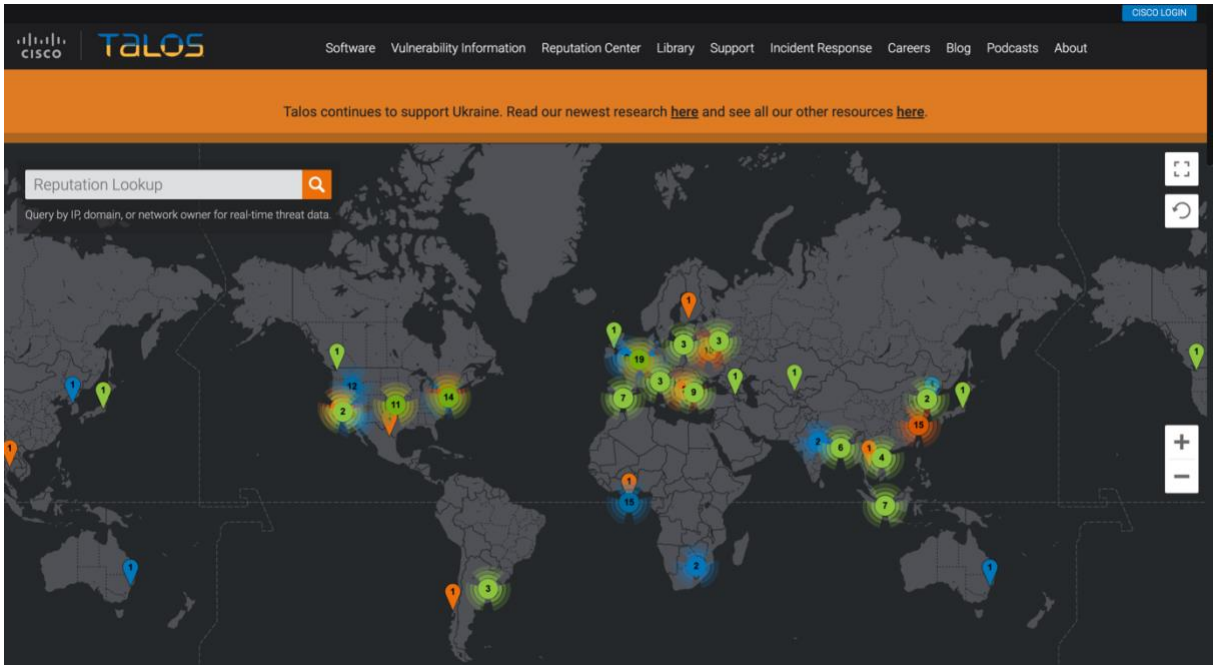


*Figura 44. Talos Intelligence - Cisco.*

Si se pincha en cada punto señalado, se muestran las últimas amenazas detectadas (Figura 45). Se estima que *Talos* detecta cada día más de medio millón de sitios *malware* y hace un bloqueo de más de 20000 millones de amenazas en todo el mundo.

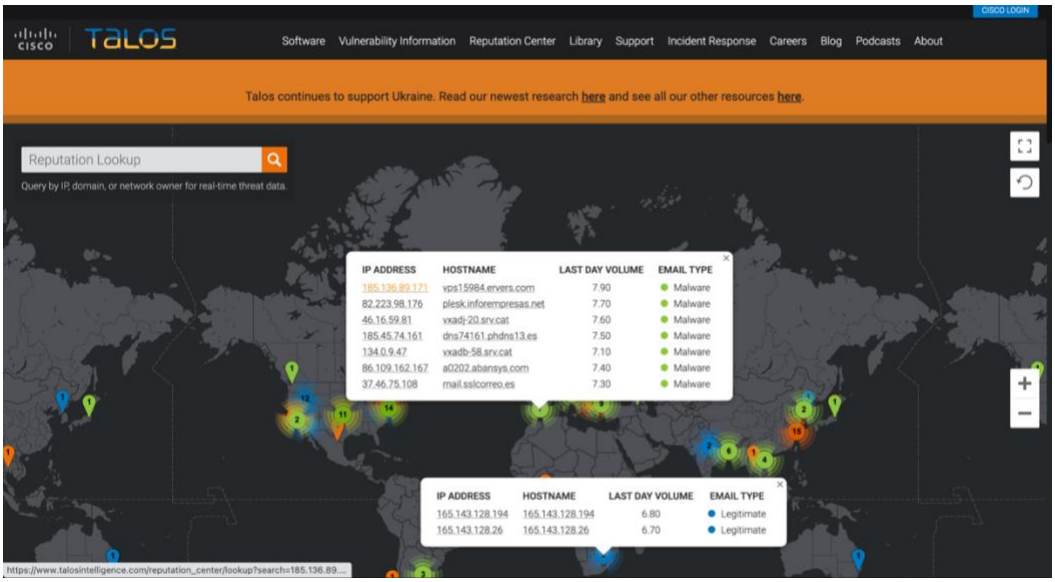


*Figura 45. Muestra de sitios detectados por Talos.*

*Talos* da la posibilidad de buscar en tiempo real por IP, por dominio o por propietario de la red. Si se introduce un sitio web, nos muestra con detalle varios datos (ver Figura 46):

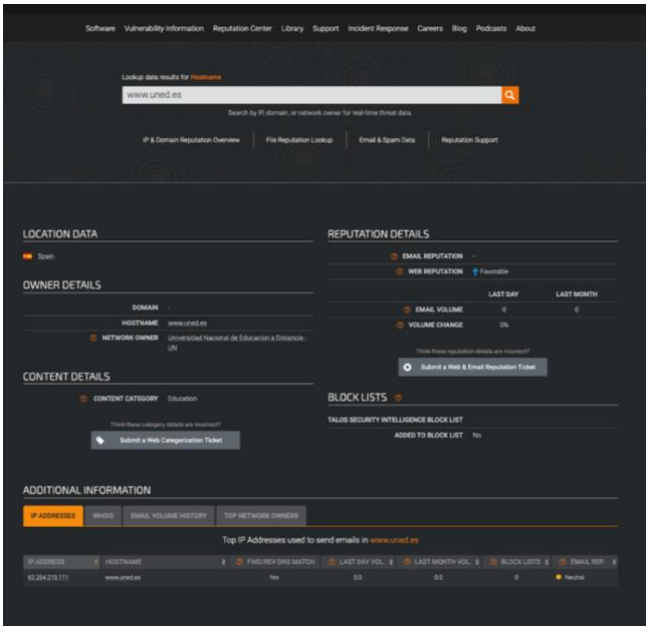


*Figura 46. Resultados de búsqueda en Talos.*

- **Codeshield**

*Codeshield* está especializado en la seguridad en la nube. Identifica las vulnerabilidades y las brechas de seguridad y rompe las rutas de ataque que los ciberatacantes pueden utilizar para explotar sus daños. Revela conexiones ocultas y comprueba si existen políticas de IAM con más peligro que permitan a un atacante moverse más dentro de su nube.

Muestra qué recursos concretos de la nube están en riesgo, lo que hace que se pueda identificar más rápidamente los elementos a priorizar. En definitiva, *Codeshield* evalúa con rapidez el impacto de cualquier ataque detectado y obtiene los recursos que pueden ser comprometidos al sufrir un ataque.

Tiene un plan gratuito que permite diez escaneos al mes y otros planes profesionales y empresariales, que pueden ser de gran interés para grandes organizaciones e instituciones.

Se encuentra disponible en el siguiente enlace: https://codeshield.io/.

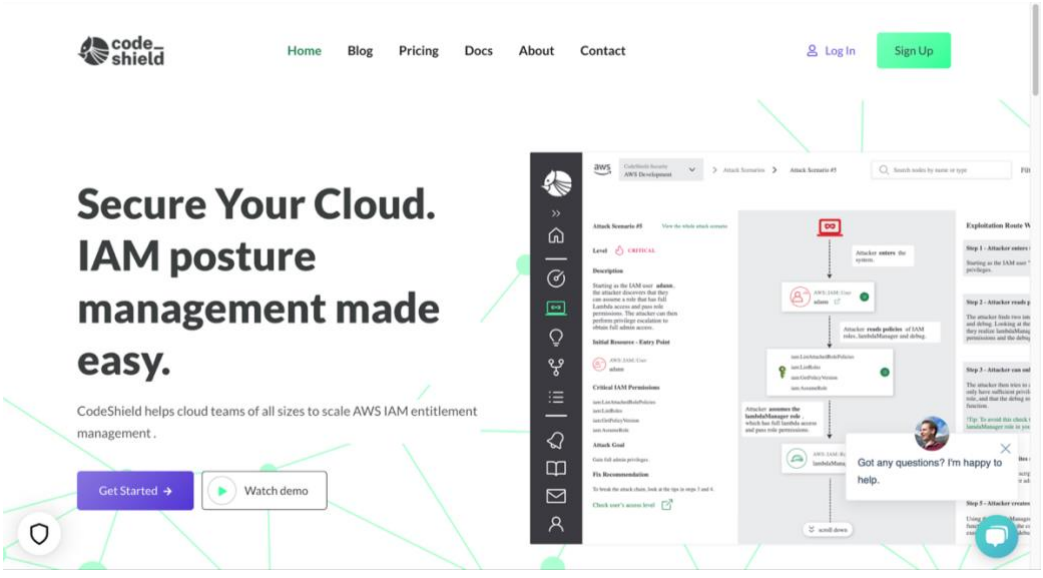


*Figura 47. Codeshield - Seguridad en la nube.*

- **DNSTwister**

Es un motor de búsqueda de nombres de dominio *antiphishing* (Figura 48) que está basado en "*dnstwist*", que es un proyecto que, dado un dominio web, detecta dominios similares (ver Figura 49) que los ciberdelincuentes pueden utilizar para realizar sus ataques. Detecta errores tipográficos, ataques de *phishing* o suplantación de la identidad de alguna marca, pudiendo exportar los resultados en formatos JSON y CSV.

Se puede acceder a él a través de: https://dnstwister.report/.

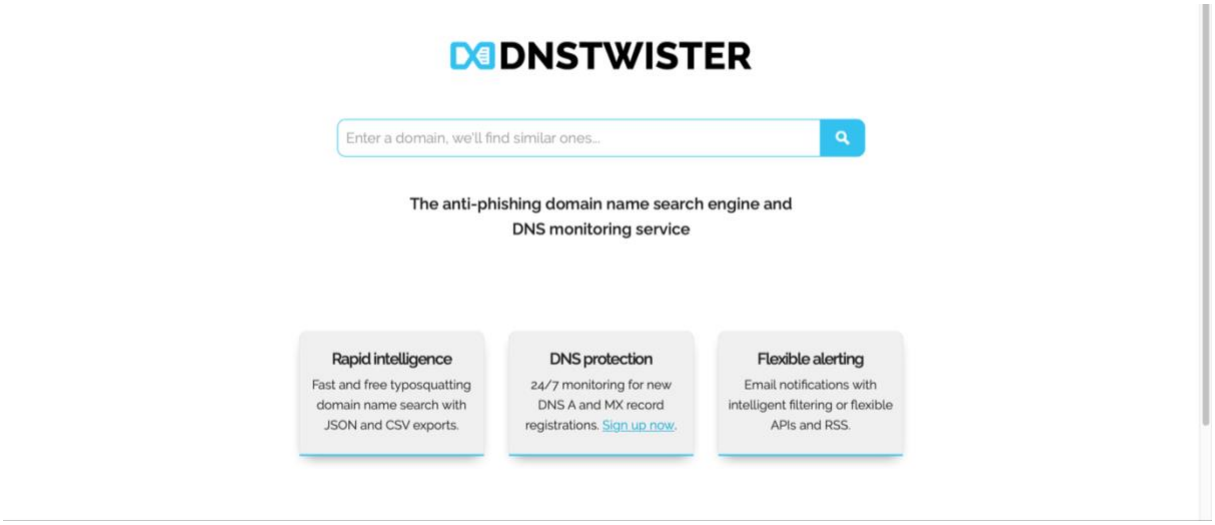


*Figura 48. Interfaz DNSTwister.*

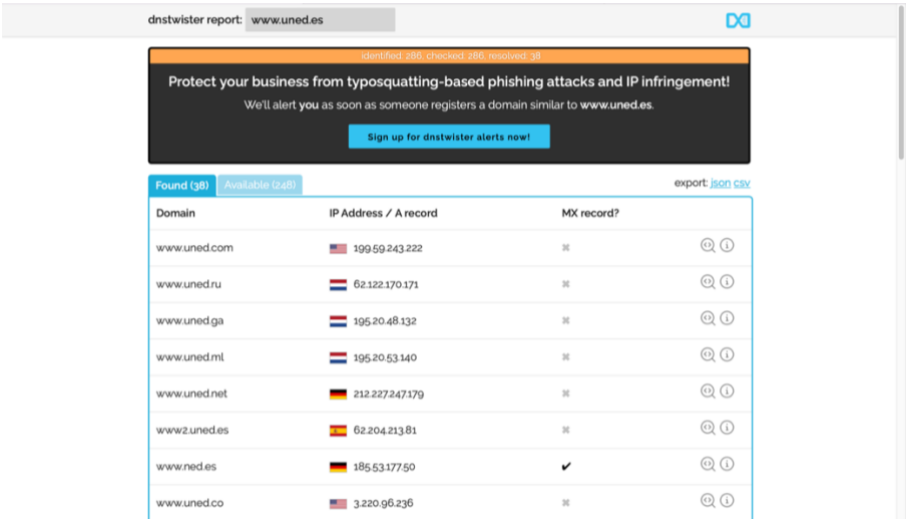


*Figura 49. Resultados búsqueda de dominio con DNSTwister.*

# 5. SIMULACIONES DE PHISHING

Muchas empresas e instituciones recurren a simulaciones de ataques de *phishing* para concienciar a sus trabajadores sobre el peligro que tiene este tipo de ataques de ingeniería social. Esto es lo que se denominan pruebas de intrusión o *pentesters*.

Lo que de verdad pretenden los responsables de ciberseguridad de las empresas es que estas simulaciones sean lo más reales posibles, haciéndoles creer a los trabajadores y usuarios que son reales, y así analizar la capacidad de respuesta de éstos para minimizar el riesgo de un posible ataque real.

## 5.1. SOFTWARE DE ATAQUE

A continuación, se describen algunas de las herramientas más conocidas para realizar ataques de *phishing*. Muchas de ellas utilizadas por los *pentesters*.

- **Social - Engineer Toolkit (SET)**

Fue creado y escrito por Dave Kennedy, el fundador de *TrustedSec*. Es una herramienta de código abierto impulsada por Python (Ver Figura 50) destinada a realizar ataques de prueba en ingeniería social (*pentesting*). Es una de las herramientas más potentes y con mayor uso por los probadores *pentesting*.

Tiene más de 2 millones de descargas y cuenta con un apoyo enorme dentro de las comunidades de seguridad. Su objetivo es aprovechar los ataques tecnológicos avanzados en un entorno de tipo ingeniería social. *TrustedSec* cree que la ingeniería social es uno de los ataques más difíciles de proteger y ahora uno de los más frecuentes.

Su página principal es: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set (Figura 51) y el código está disponible en: https://github.com/trustedsec/social-engineer-toolkit (Figura 52).


*Figura 50. Social Engineer Toolkit (SET).*

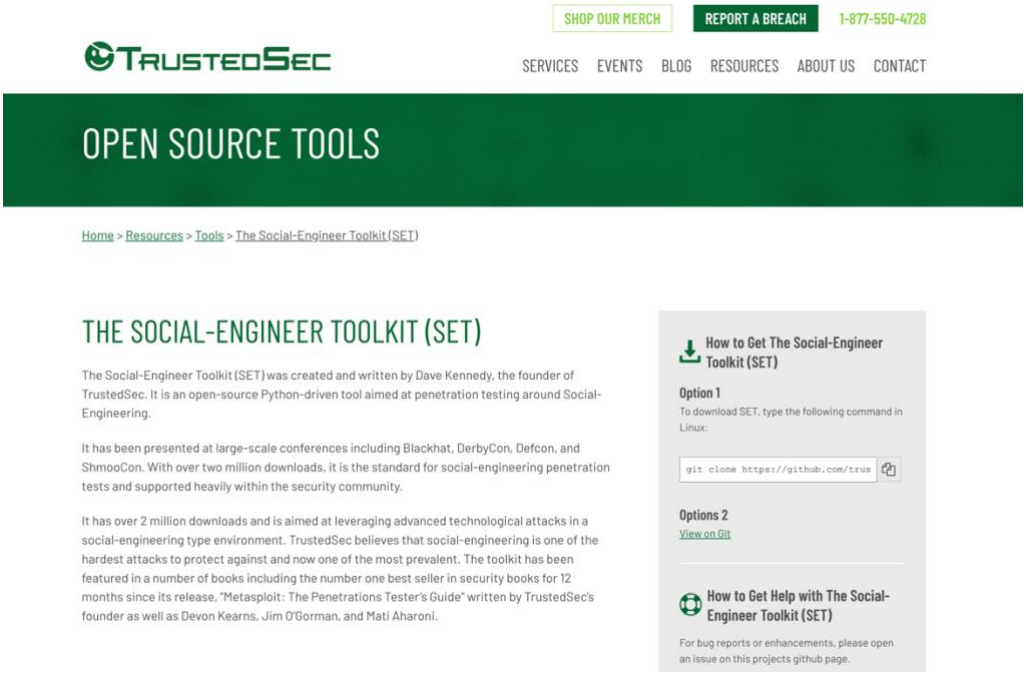


*Figura 51. Sitio web de SET.*

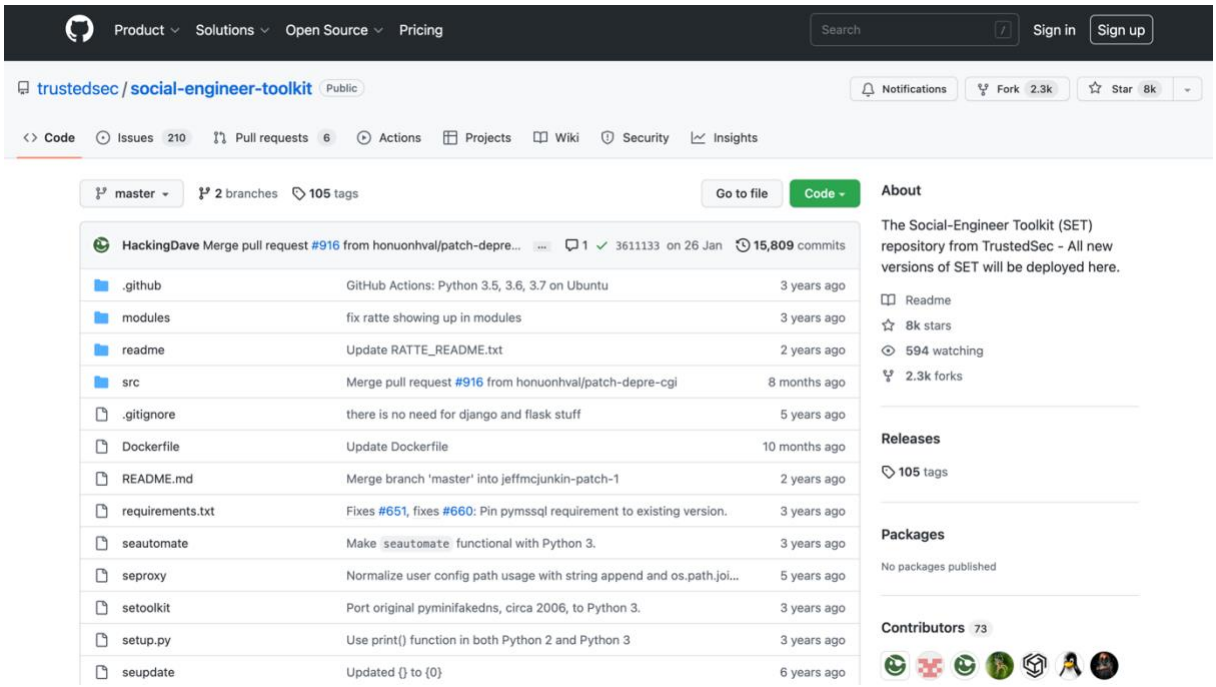


*Figura 52. Herramienta Social Engineer Toolkit (SET).*

- **Hidden Eyer**

Mediante esta herramienta (Figura 53), que está desarrollada en Python, se pueden realizar ataques de los sitios web más conocidos, pudiendo utilizar plantillas simulando la legitimidad de éstos. Aparte de utilizar estas plantillas, se puede utilizar *keyloggers* para recoger todos los datos introducidos por los usuarios.


*Figura 53. Logo de Hidden Eyer.*

Se encuentra disponible en el repositorio Gitlab como aparece reflejado en la Figura 54, y se permite la instalación y ejecución en un equipo de una manera sencilla: https://gitlab.com/An0nUD4Y/hiddeneye.

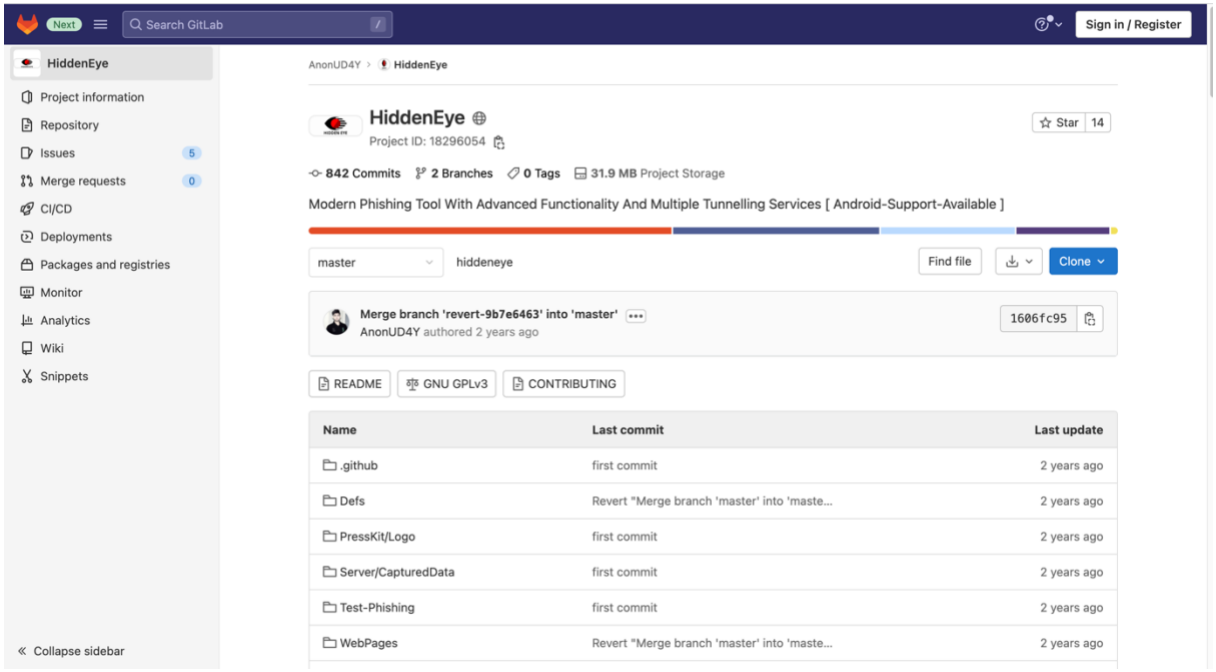


*Figura 54. Herramienta Hidden Eyer.*

- **WifiPhisher**

Permite capturar contraseñas WIFI o crear redes intermedias falsas, pudiendo atacar a los usuarios y obtener sus credenciales o infectarles algún tipo de *malware*. No utiliza ningún ataque de fuerza bruta, sino que se basa en emplear al propio usuario, haciendo uso de la ingeniería social. Su logo, como se aprecia en la Figura 55, muestra un ancla con el icono de una red wifi, haciendo intuir al usuario de qué se trata sin necesidad tan siquiera de ver su nombre.

Esta herramienta se encuentra disponible en el repositorio GitHub: https://github.com/wifiphisher/wifiphisher (Ver Figura 56).

*Figura 55. Logo WifiPhisher.*

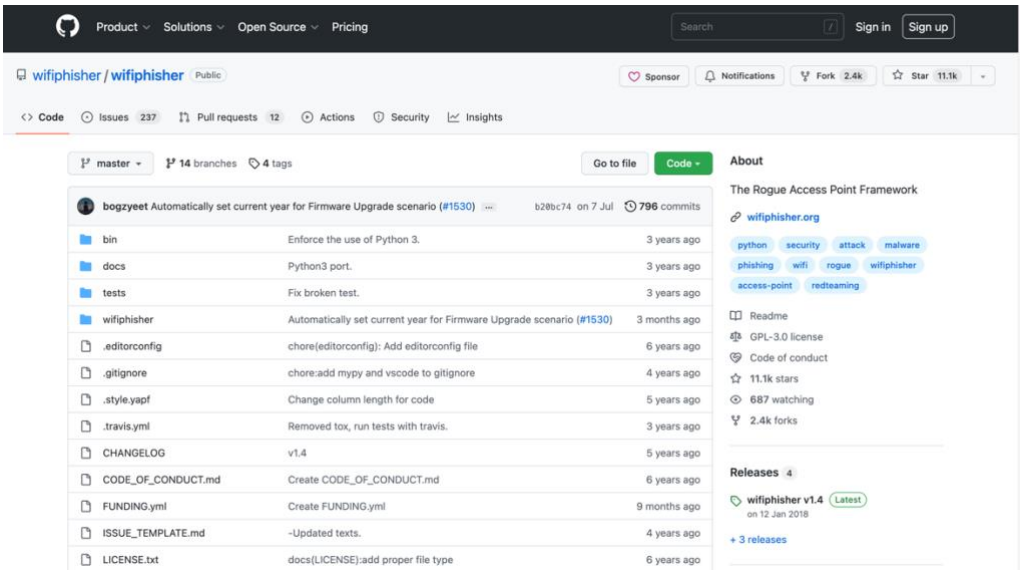


*Figura 56. Herramienta WifiPhisher.*

- **King Phisher**

Es una herramienta para probar y promover la sensibilización de los usuarios mediante la simulación de ataques de *phishing* en el mundo real (Figura 57). Cuenta con una arquitectura fácil de usar y muy flexible, implementada en *Python*, que permite un control total sobre los correos electrónicos y el contenido del servidor. Puede ser utilizado para ejecutar campañas de formación y concienciación sobre ciberseguridad de los usuarios de una organización.

El proyecto se encuentra disponible en: https://github.com/rsmusllp/king-phisher (Figura 58).

*Figura 57. Logo King Phisher.*

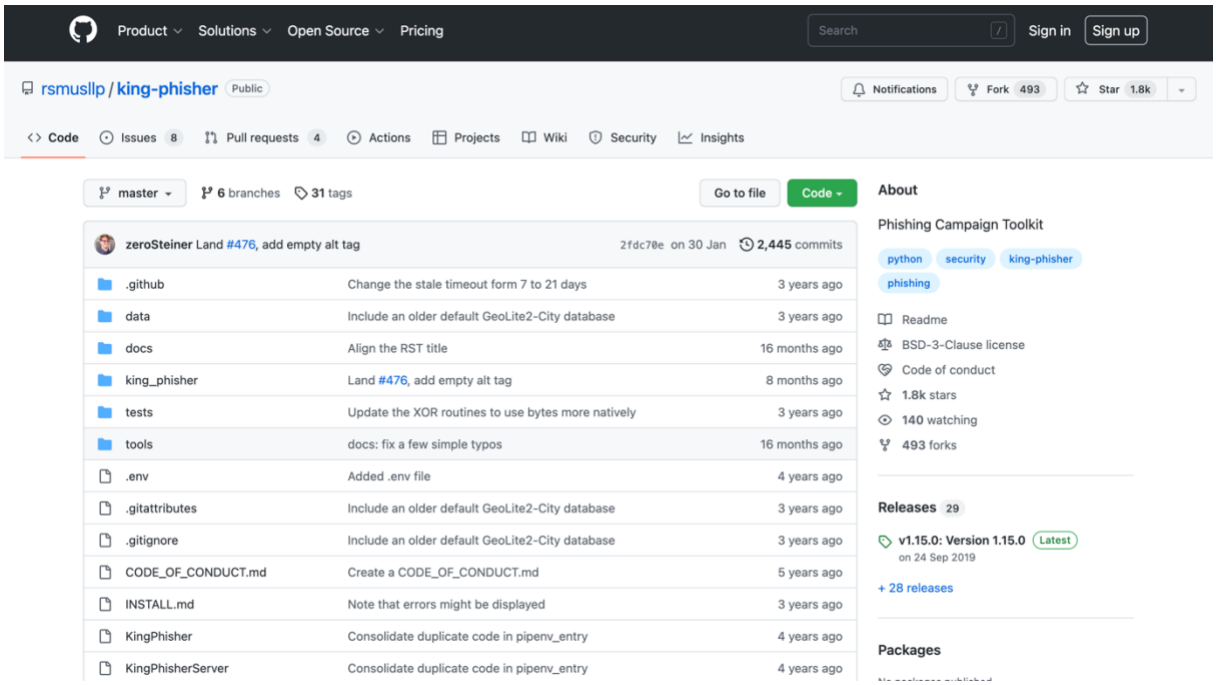


*Figura 58. Herramienta King Phisher.*

- **GoPhish**

Es un conjunto de herramientas de *phishing*, potente, fácil de usar y de código abierto destinado a ayudar a los *pentesters* y a las empresas a realizar simulaciones de *phishing* en el mundo real.

*Gophish* (Figura 59) hace que la simulación de ataques de *phishing* en el mundo real sea muy simple. Es un software de código abierto, completamente gratuito para quien desee su utilización. Está escrito en el lenguaje de programación *Go*, con lo que simplemente se descarga y ejecuta.

*Figura 59. Logo Gophish.*

Está disponible en: https://github.com/gophish/gophish (Figura 60) y su sitio web oficial es: https://getgophish.com/ (Figura 61).

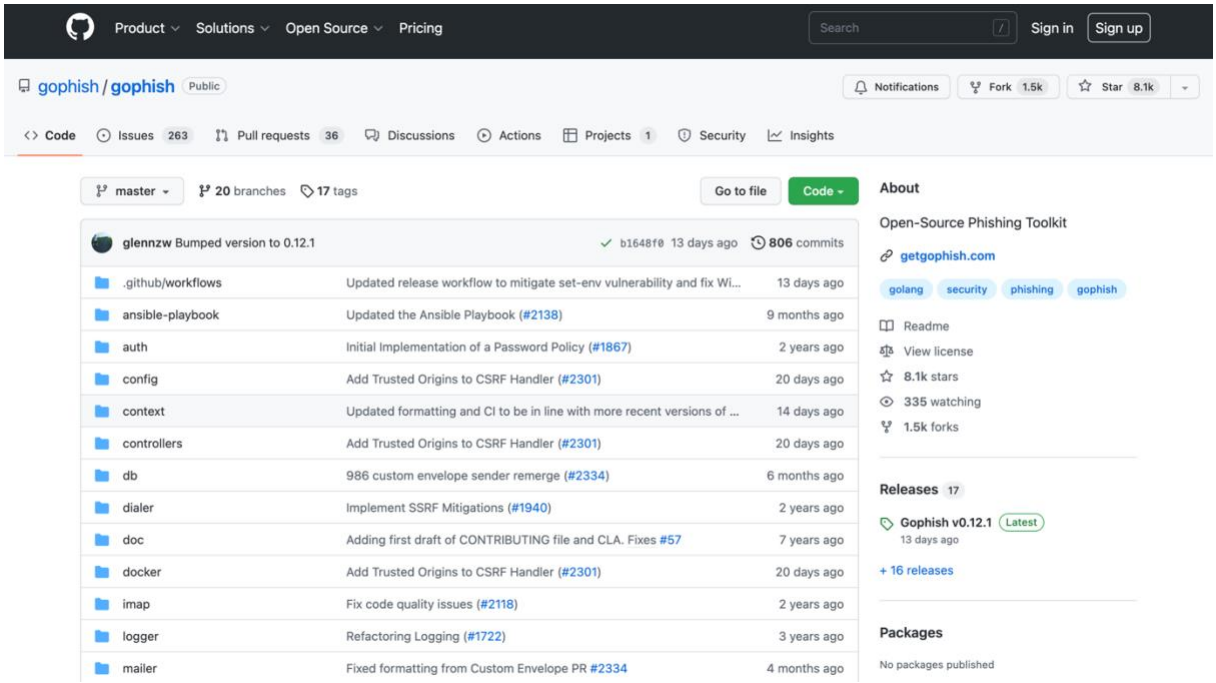


*Figura 60. Herramienta Gophish.*

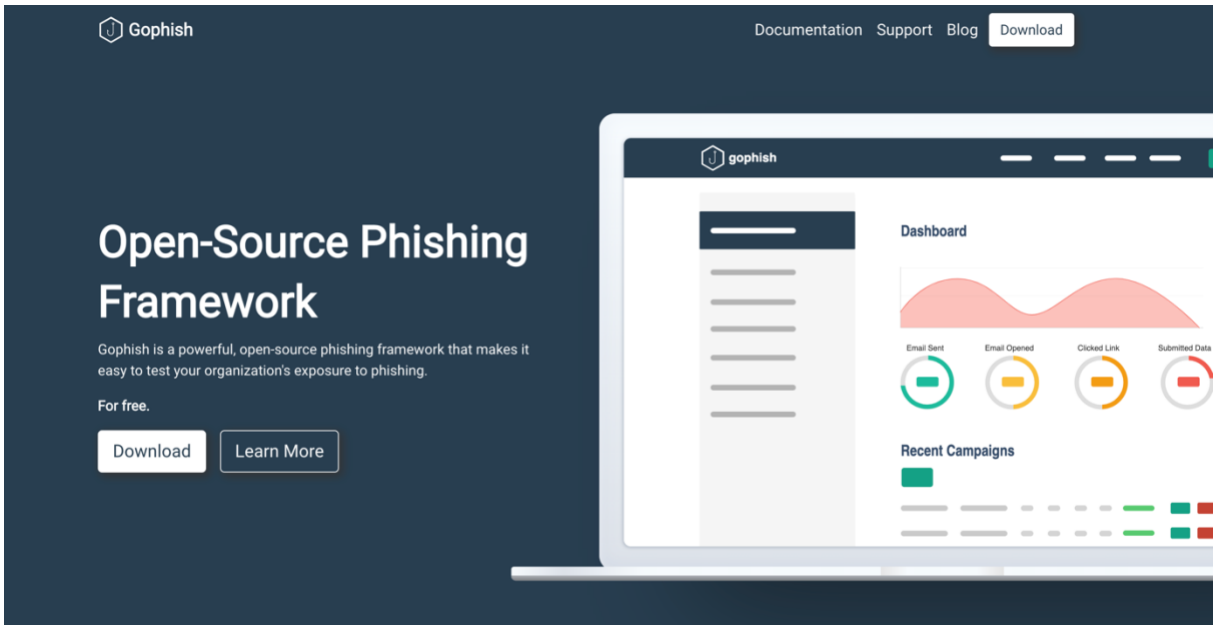


*Figura 61. Sitio web oficial de Gophish.*

- **Evilginx2**

Evilginx2 (Figura 62) está desarrollada también en el lenguaje *Go*. Utiliza un ataque del tipo *man-in-the-middle* para interceptar las credenciales, evadiendo incluso la autenticación de dos factores.

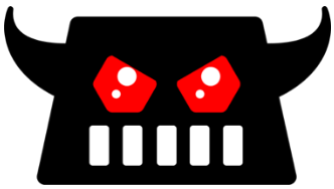

*Figura 62. Logo Evilginx2.*

Esta herramienta se encuentra disponible en: https://github.com/kgretzky/evilginx2 (Figura 63).

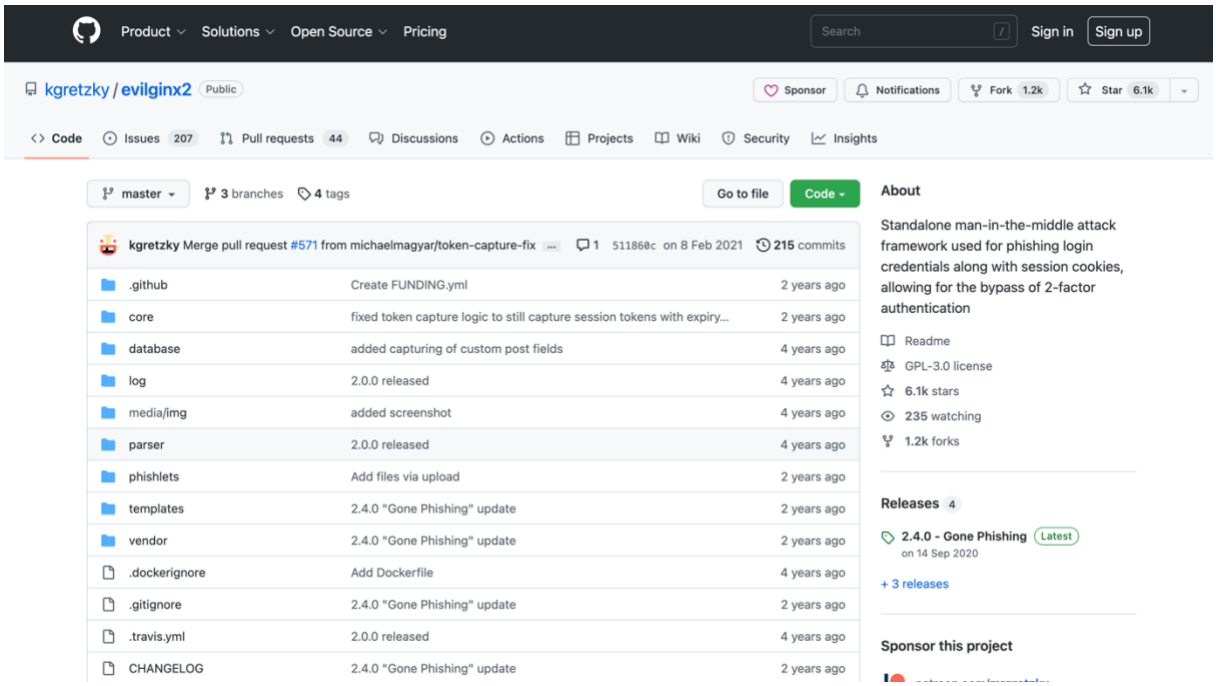


*Figura 63. Herramienta Evilginx2.*

- **Blackeye**

Es una herramienta gratuita y de código abierto que permite realizar ataques de *phishing* de una manera rápida y sencilla, cuyo logo se muestra en la Figura 64. Posee versiones tanto de escritorio como de dispositivos móviles, adaptándose en función del dispositivo.

*Figura 64. Logo Blackeye.*

Dispone de cerca de 40 plantillas para simular los ataques, entre ellas de sitios tan conocidos como Instagram, *Spotify, Netflix* o *Linkedin*. Así, se puede conseguir varios datos de las víctimas, como puede ser su IP o Sistema Operativo, haciéndole creer que está enlazando al sitio legítimo.

Su última versión está disponible en https://github.com/thewickedkarma/blackeye-im (Figura 65).

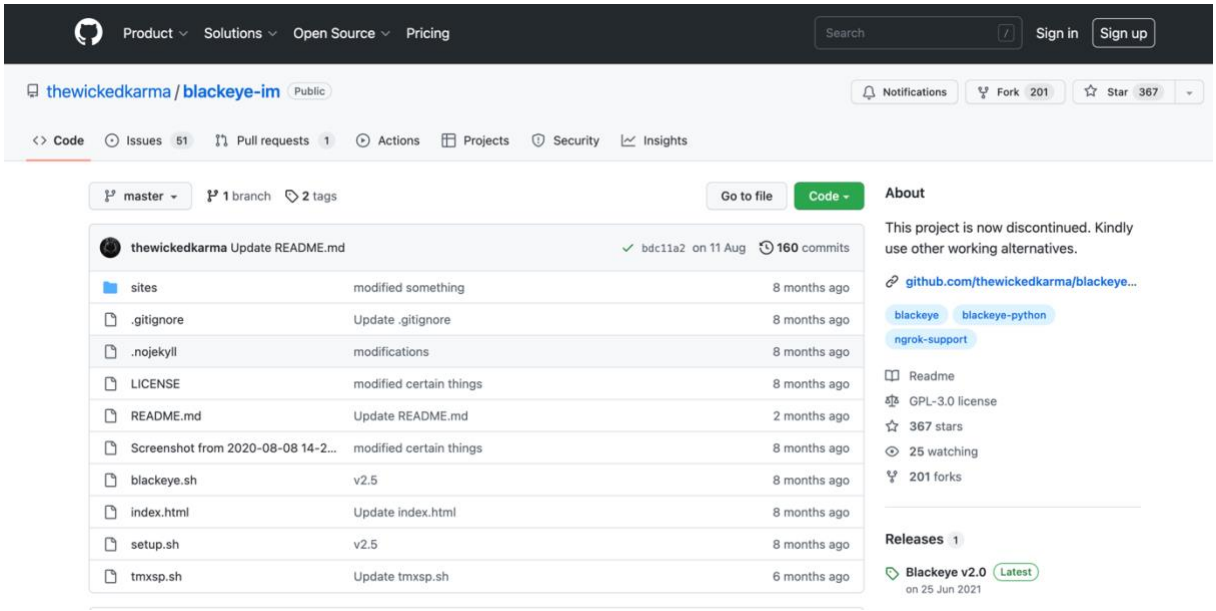


*Figura 65. Herramienta Blackeye.*

- **Modlishka**

Es una herramienta de proxy inverso que automatiza los ataques de *phishing*, omitiendo la autenticación de dos factores. Maneja el tráfico entre las páginas legítimas y los ataques *phishing*.

Permite transmitir el tráfico de destino de varios dominios de una manera transparente sin la necesidad de instalar ningún certificado adicional en el cliente.

Está disponible en: https://github.com/drk1wi/Modlishka (Figura 66).

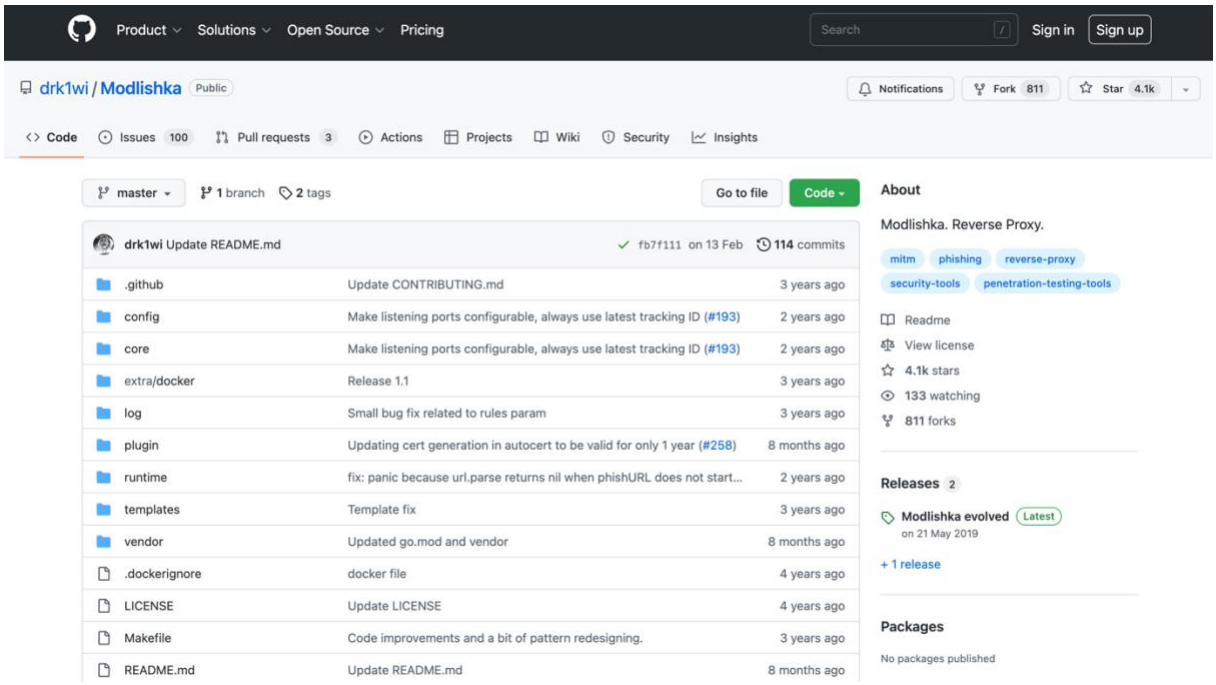


*Figura 66. Herramienta Modlishka.*

## 5.2. PENTESTING

Se ha descargado la distribución *Kali Linux* (última versión disponible 2022.3), que está basada en *Debian GNU/Linux*, y es utilizada principalmente para auditorías y seguridad informática, haciéndola correr en una máquina virtual con *Oracle VirtualBox*, y así poder probar sus diferentes herramientas con total tranquilidad.

*Kali Linux* [19] es una de las distribuciones más utilizadas entre los profesionales de seguridad, para realizar pruebas de *pentesting* o análisis forense, así como utilizada también con fines académicos o personales. Cuenta con una infinidad de herramientas, tanto en modo consola como en modo gráfico, entre las que destacan *Wireshark, Aircrack, Nmap, Maltego, Nmap,* etc., lo que es una ventaja para los usuarios, optimizando su tiempo sin necesidad de tener que instalarlas y configurarlas.

Entre sus principales funciones están la recopilación de información, ataques a través de redes wifi, ingeniería inversa, análisis de vulnerabilidades o hacking de hardware.

En la Figura 67 se puede ver la interfaz principal de *Kali Linux*, con el logo oficial de la distribución como fondo de escritorio.

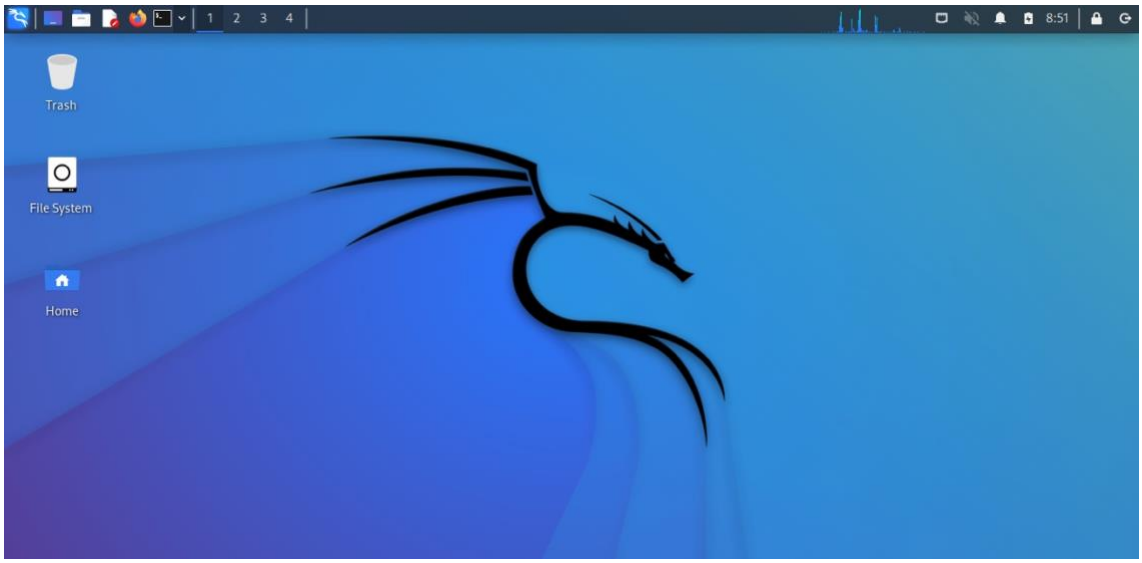


*Figura 67. Interfaz principal Kali Linux.*

Si se despliega el menú, destaca la distribución de todas las herramientas disponibles como se puede ver en la Figura 68.

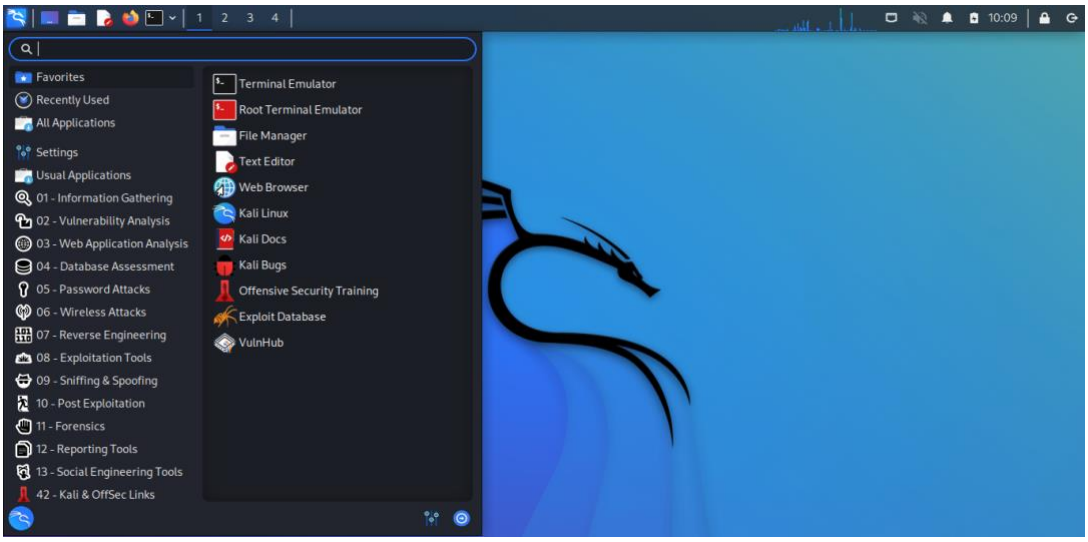


*Figura 68. Herramientas disponibles en Kali Linux.*

En el caso de estudio de este trabajo, el uso de *Kali Linux* se va a centrar en una herramienta muy utilizada por los pentesters, que ha sido descrita anteriormente en el capítulo 5.1: SET (*Social Engineering Toolkit*), destinada principalmente a la ingeniería social, ofreciendo a los usuarios la posibilidad de utilizar herramientas para automatizar tareas de ataques, como envíos masivos de emails o SMS falsos.

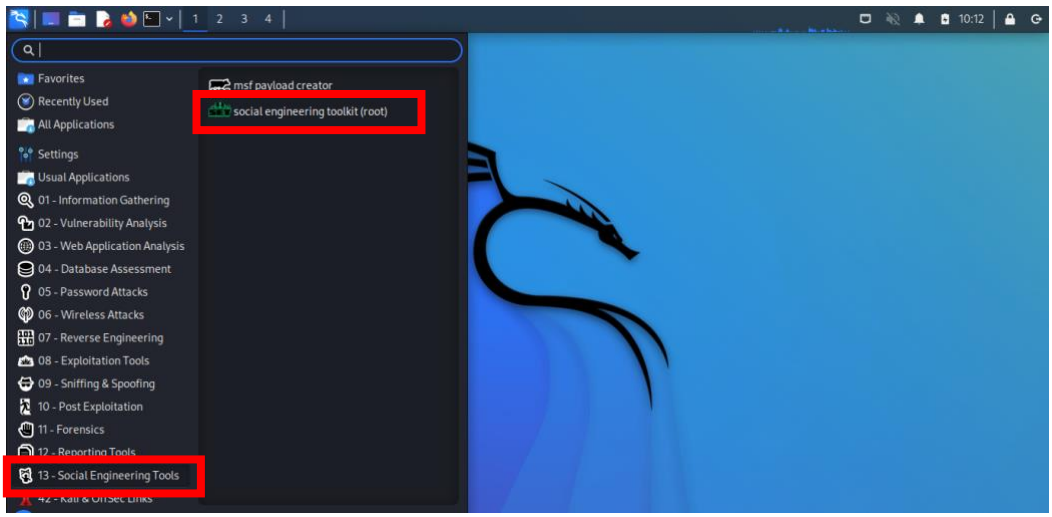


*Figura 69. Social Engineering Toolkit integrado en Kali Linux.*

Además de poder acceder a SET a través del menú, en el apartado "*Social Engineering Tools*" (Figura 69), es posible acceder directamente desde la terminal, entrando como usuario root y utilizando el comando "*setoolkit*", tal como se indica en la Figura 70:

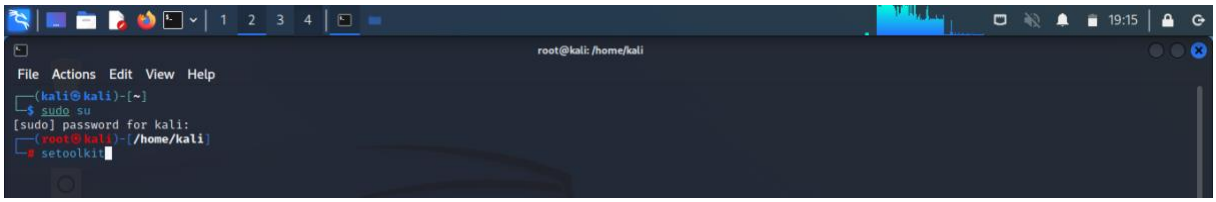


*Figura 70. Acceso a SET a través de la terminal.*

Una vez que se accede, se abre la interfaz de SET en la terminal, y como se aprecia en la Figura 71, aparecen los créditos de la herramienta, donde vemos que es un producto de la conocida organización de seguridad informática *TrustedSec.*

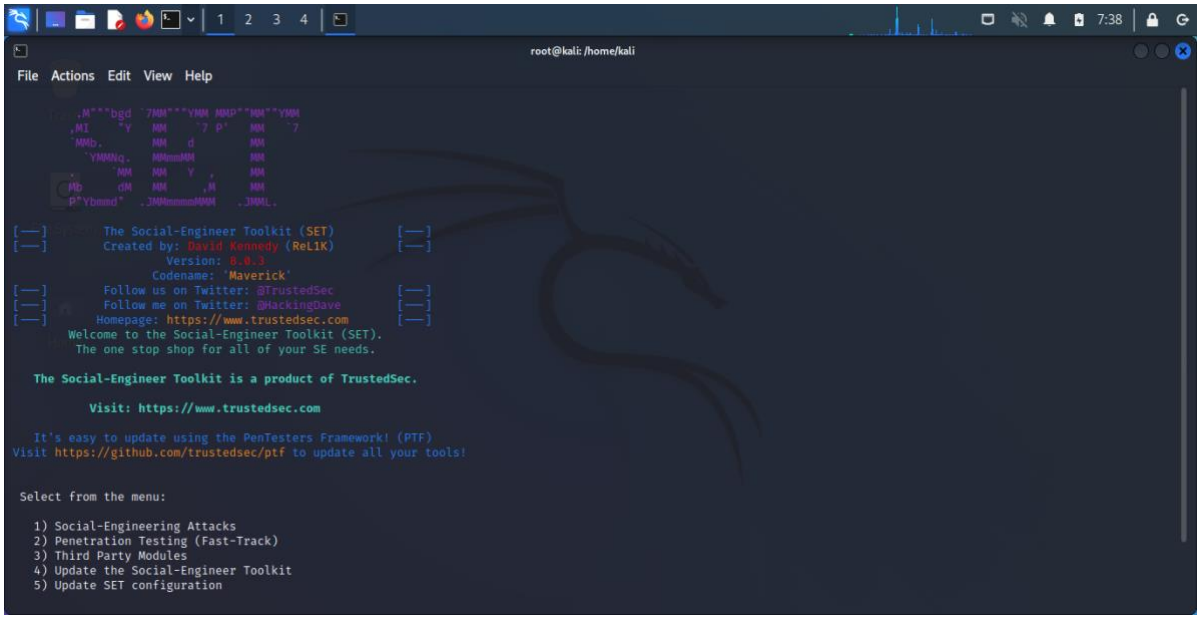


*Figura 71. Herramienta SET proporcionada por Kali Linux.*

A continuación, se hará un estudio de las diferentes técnicas que ofrece SET, centrándose en la opción 1, *"Social-Engineering Attacks".* Como se muestra en la Figura 72, se dispone de 10 opciones de ataques:

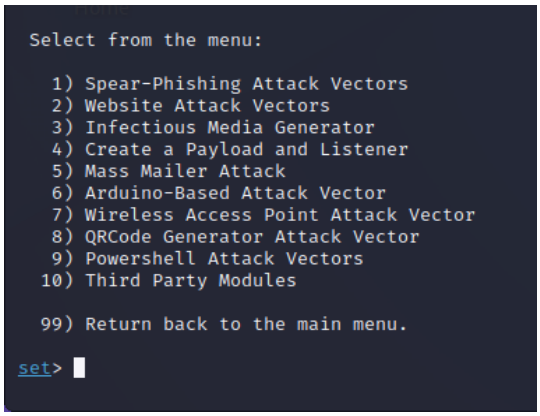


*Figura 72. Menú principal de SET.*

En este caso, vamos a seleccionar la opción 1, "Spear-Phishing Attack Vectors", y en la Figura 73 se muestra una pequeña explicación de lo que este módulo es capaz de realizar, ofreciendo tres opciones de ataque.

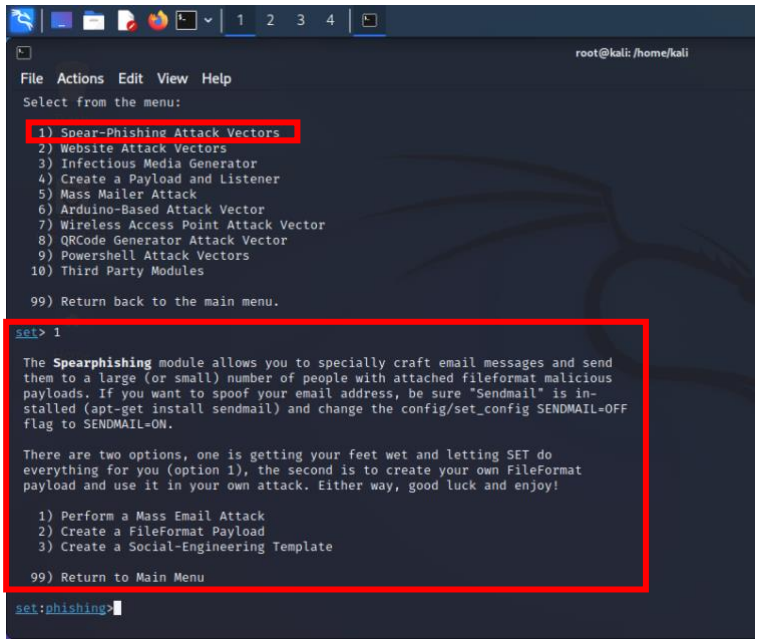


*Figura 73. Menú de ataque de Spear-Phishing con SET.*

Se selecciona la opción 1, *"Perform a Mass Email Attack"* y como se detalla en la Figura 74, se dispone de 22 tipos de archivos para crear y enviar como archivo adjunto.

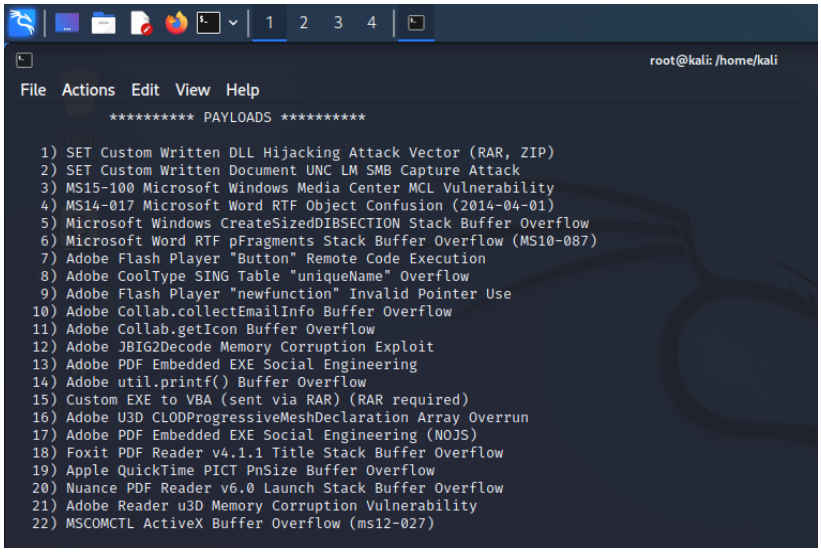


*Figura 74. Tipos de archivo para envío masivo de emails phishing.*

En este caso, se ha seleccionado la opción 13, *"Adobe PDF Embedded EXE Social Engineering"* dándonos dos opciones para su creación: crear nuestro propio archivo PDF o usar uno en blanco (ver Figura 75).

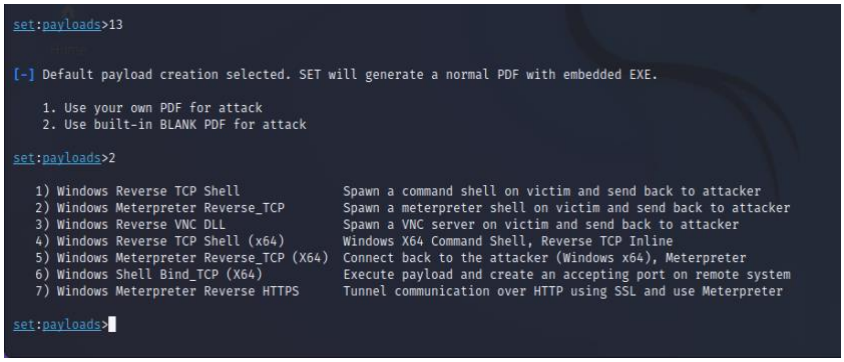


*Figura 75. Uso de archivo PDF para envío de phishing por correo electrónico.*

De todas las opciones que aparece, seleccionamos el tipo 2, *"Windows Meterpreter Reverse_TCP"* y como se muestra en la Figura 76, se dejan la IP local y puerto por defecto 443 para que el atacante se quede a la espera y se crea el directorio donde llegarán los datos que reciba de la víctima.

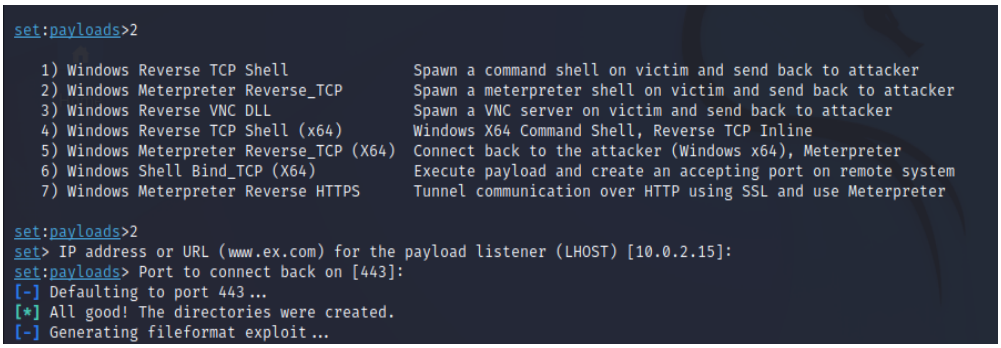


*Figura 76. Selección tipo de ataque.*

Una vez que se ha generado el archivo, se pregunta si se desea cambiar el nombre o dejarlo por defecto con el nombre "template.pdf" (Figura 77).

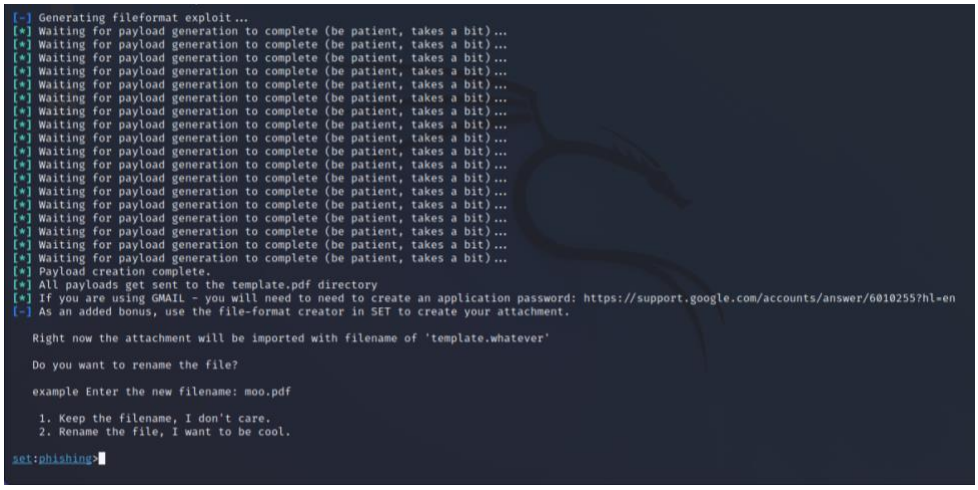


*Figura 77. Generación de archivo. pdf.*

Se deja el nombre del archivo generado por defecto (Figura 78), y una vez generado, nos da la opción de enviar un solo correo electrónico o varios, de forma masiva.

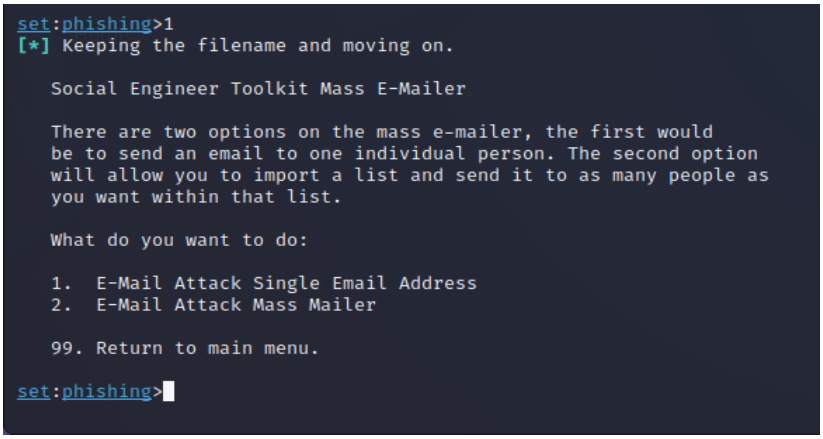


*Figura 78. Envío de ataque a una sola víctima o envío masivo.*

En este caso, como se aprecia en la Figura 79, se elige ataque a un solo correo electrónico y a continuación, nos da a elegir si se quiere hacer una plantilla o elegir una predefinida.

Se selecciona utilizar una predefinida y se muestran las diferentes plantillas disponibles.

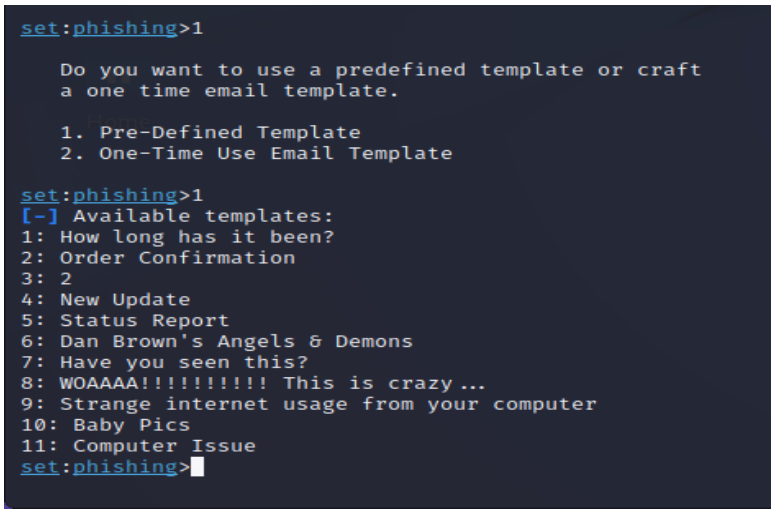


*Figura 79. Plantillas predefinidas para utilizar en el envío de correo electrónico phishing.*

Se ha seleccionado la opción 2, una confirmación de pedido, que hará que la víctima pueda caer fácilmente en el engaño, siendo las compras online habituales entre los usuarios, y ahora se debe introducir la dirección de correo electrónico de la víctima (Figura 80).

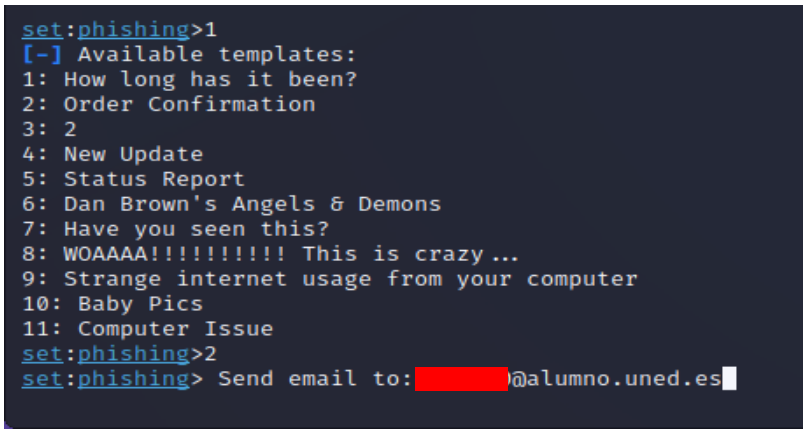


*Figura 80. Destinatario del envío.*

Como Gmail es uno de los gestores de correo electrónico más utilizado, directamente se da la opción en el menú de utilizarlo, o bien, seleccionar otro servidor (Figura 81).

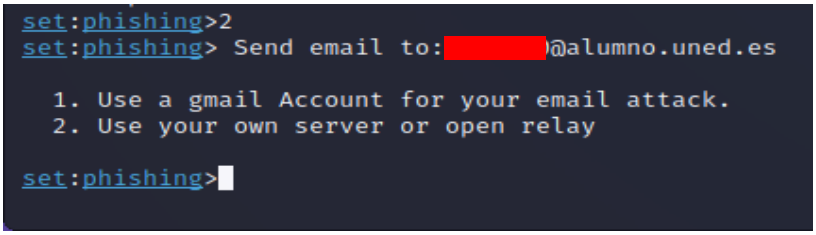


*Figura 81. Elección de gestor de envío de correo.*

En este caso, se utilizará Gmail y a continuación se solicitan una serie de datos, como el nombre del remitente que le aparecerá a la víctima, marcar como prioritario el envío de este correo electrónico, indicar si el servidor de correo soporta cifrado TLS y finalmente le da la opción al atacante de crear el agente de escucha, según se muestra en la Figura 82.

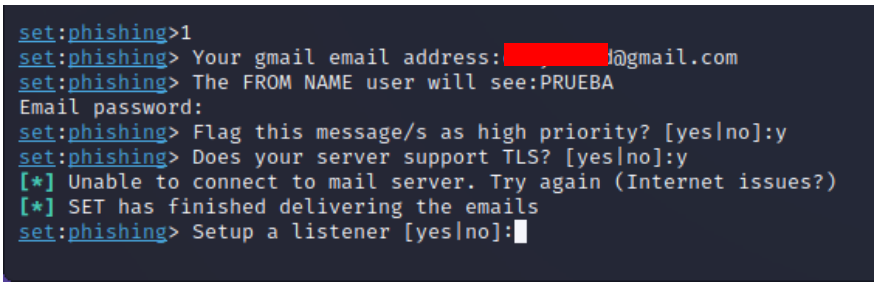


*Figura 82. Login Gmail para envío de phishing.*

Ahora, y una vez enviado el correo electrónico con el archivo adjunto a la víctima, el programa del atacante se pondrá en modo escucha (ver Figura 83), esperando a recibir datos de la víctima una vez que haya abierto el correo electrónico recibido y ejecutado el archivo adjunto.

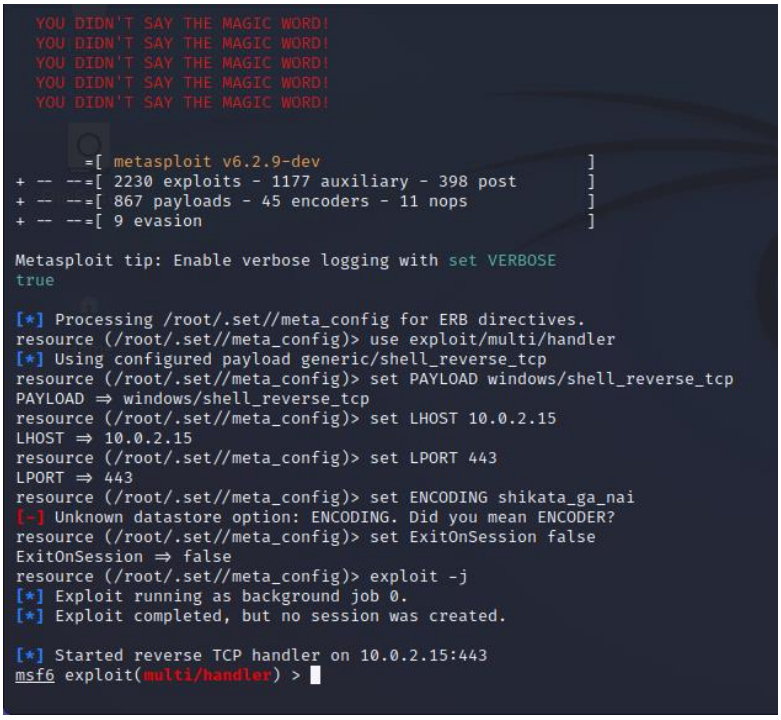


*Figura 83. Modo escucha del atacante.*

A continuación, se hará otra prueba de ataque, seleccionando en el menú principal de ataques de ingeniería social la opción 2, "*Website Attack Vectors",* según la Figura 84.

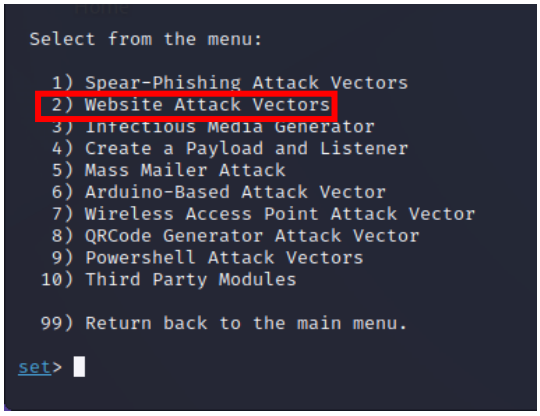


*Figura 84. Menú principal SET - Ataque web.*

Si nos fijamos en la Figura 85, al seleccionar el ataque, nos da una pequeña explicación de qué se puede hacer y qué tipos de recogida de credenciales proporciona el ataque.

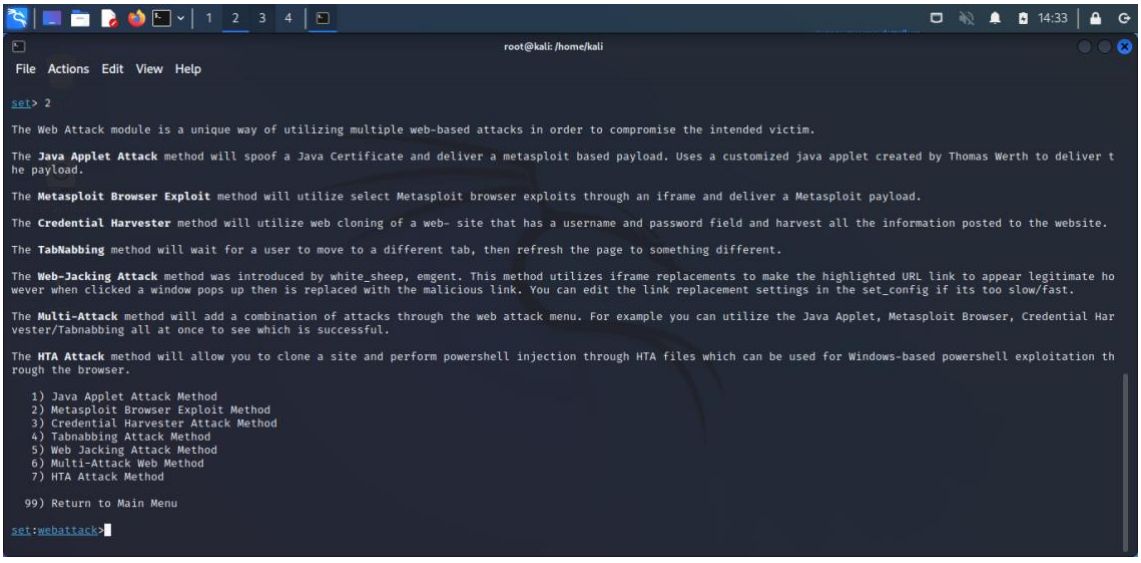


*Figura 85. Ataque SET clonar un sitio web.*

En este caso, se utilizará la opción 3, *"Credential Harvester Attack Method"* (Figura 86) y nos aparecen tres opciones de clonación.

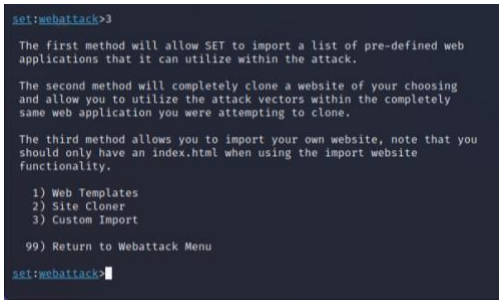


*Figura 86. Ataque clonación web.*

Se selecciona la opción1, para utilizar una plantilla ya creada y como se aprecia en la Figura 87, están disponibles tres plantillas para utilizarlas como clonación.

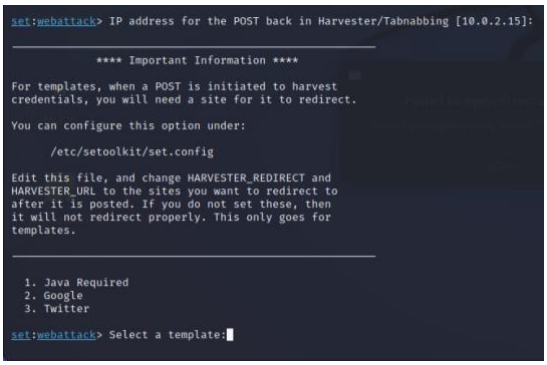


*Figura 87. Selección plantilla.*

Elegimos clonar Google. Se crea el sitio web clonado y se queda a la espera de recibir las credenciales que la víctima introduzca (Figura 88).


*Figura 88. Ataque a la espera de recibir credenciales de Google.*

Si se abre en el navegador la dirección local, donde se ha creado el sitio web clonado, se aprecia en la Figura 89 que es exactamente igual al sitio real de Google – Gmail. Se han introducido unas credenciales falsas de prueba.

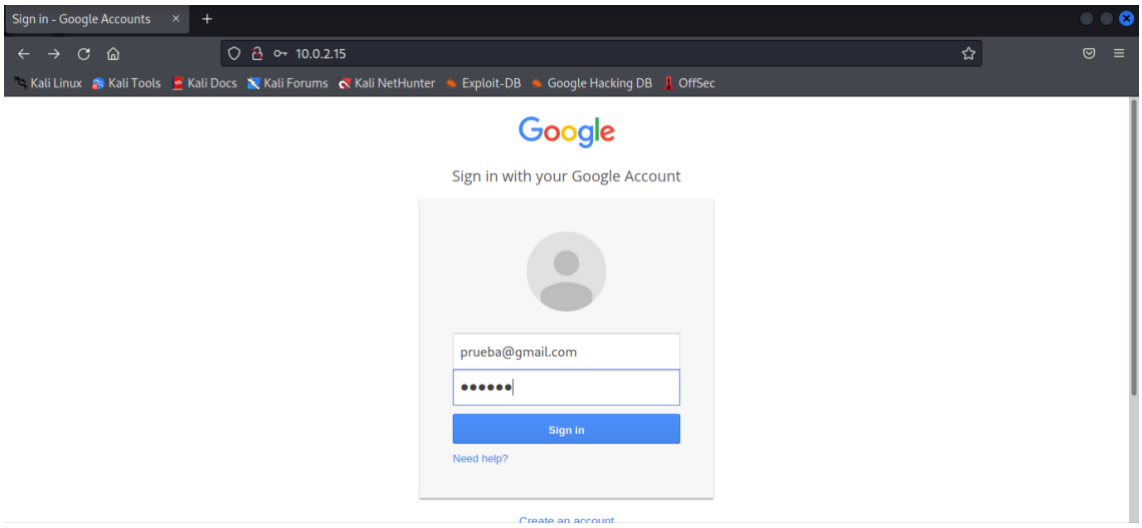


*Figura 89. Interfaz de Google clonada.*

El atacante recibe los datos que la víctima ha introducido en el sitio suplantado de Google (Figura 90).


*Figura 90. Recepción de credenciales de Google.*

Ahora se selecciona la plantilla de Twitter para probar y ver la interfaz del sitio clonado (Figura 91).


*Figura 91. Ataque a la espera de recibir credenciales de Twitter.*

Si se abre en el navegador la dirección local, donde se ha creado el sitio web clonado, se aprecia en la Figura 92 que es igual al sitio real de Twitter. Se han introducido unas credenciales falsas de prueba.

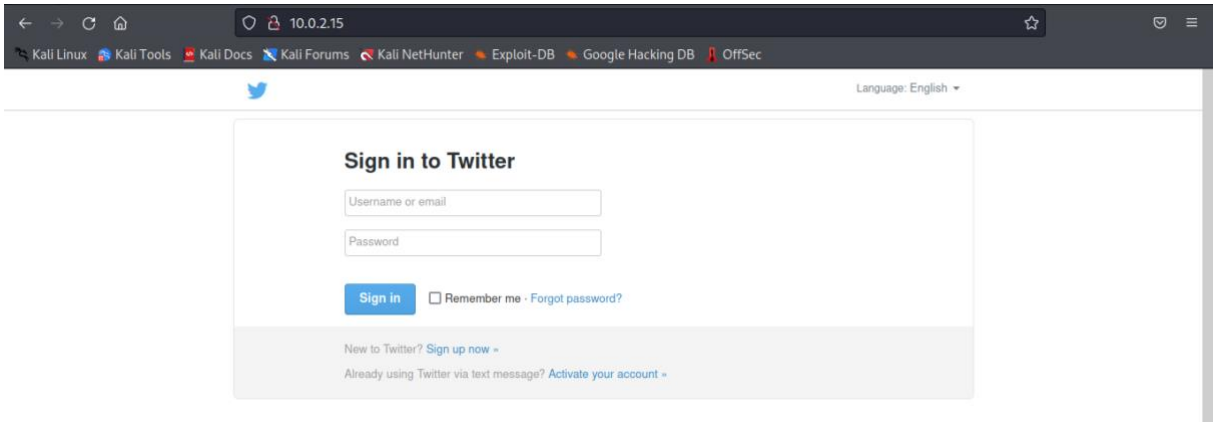


*Figura 92. Interfaz de Twitter clonada.*

El atacante recibe el usuario y la contraseña que la víctima ha introducido en el sitio suplantado de Twitter (Figura 93).


*Figura 93. Recepción de credenciales de Twitter.*

Por último, se ha seleccionado la opción 4 del menú principal de ingeniería social de la herramienta SET, *"Create a Payload and Listener"* (Figura 94).

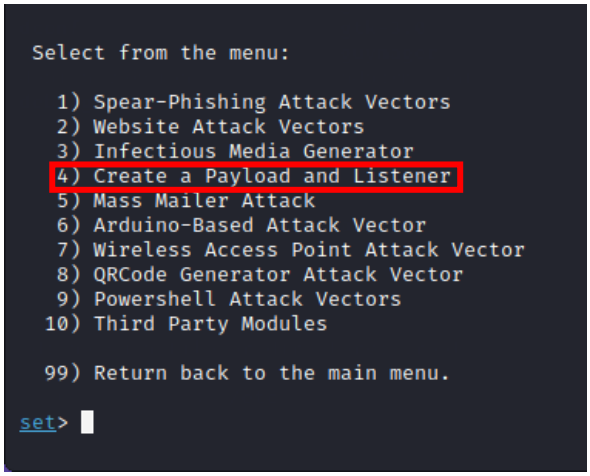


*Figura 94. Menú principal SET - Creación de Payload y agente de escucha.*

De todas las opciones posibles que aparecen en el siguiente menú, se ha elegido la 5, *"Windows Meterpreter Reverse_TCP X64"* (Figura 95) y se indica la dirección IP local y el puerto.

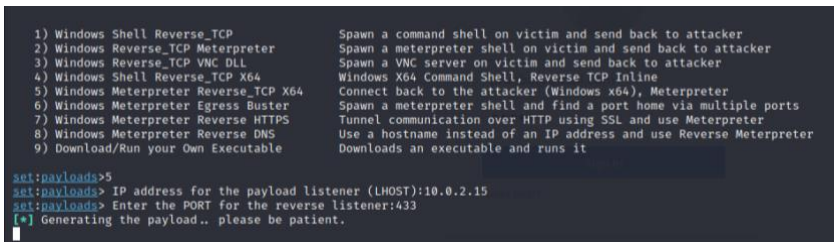


*Figura 95. Tipo de ataque.*

Se genera el archivo que contiene el virus o troyano y se guarda en la carpeta que se indica en la Figura 96 y el atacante puede empezar la escucha.

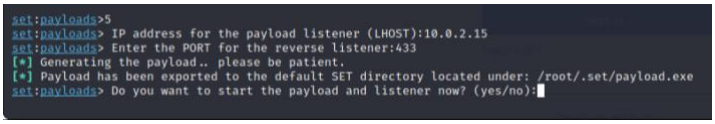


*Figura 96. Selección de IP y puerto de escucha.*

A partir de ahora, se procederá a generar el archivo ejecutable que la víctima ejecutará en su sistema para que el atacante pueda acceder a él (Figuras 97).

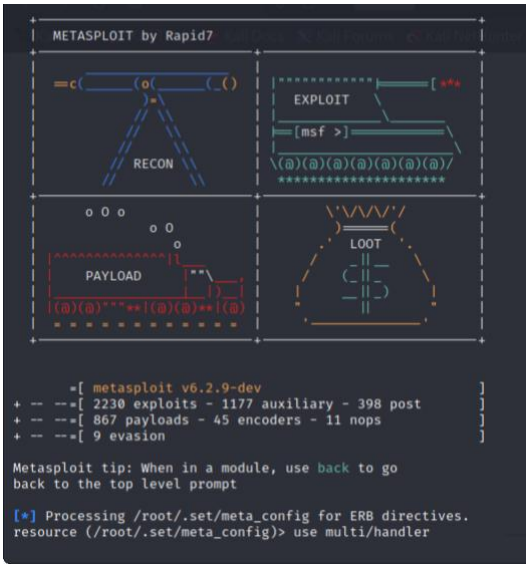


*Figura 97. Herramienta Metasploit.*

El atacante se queda a la espera de que la víctima ejecute el archivo con el troyano generado, como muestra la Figura 98. Para ello, deberá ponerle un nombre que llame su atención para acceder a él.

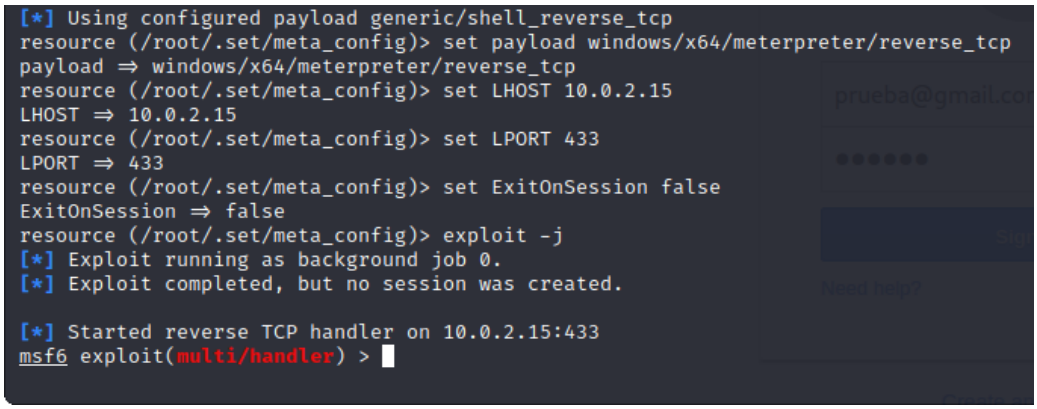


*Figura 98. Atacante en modo escucha.*

En este caso se ha dejado el nombre por defecto al generar el ejecutable que se enviará a la víctima (Figura 99).

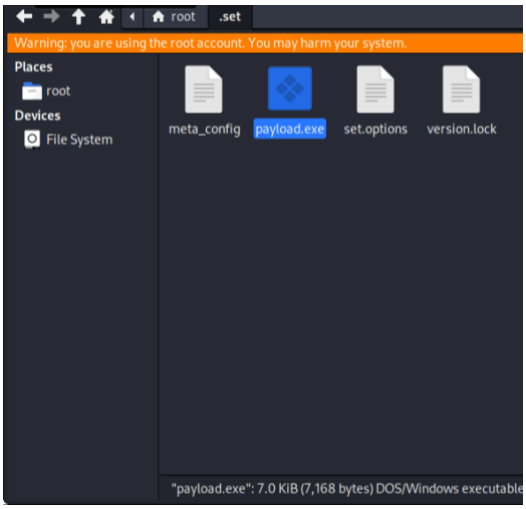


*Figura 99. Ejecutable que contiene el virus / troyano.*

# 6. CONCLUSIONES

Durante los capítulos de este trabajo, se ha hecho un repaso por uno de los ataques de ingeniería social más utilizados, el *phishing*, donde los usuarios son el principal objetivo de los ciberatacantes.

Empezando por una pequeña introducción y la explicación del porqué se ha querido hacer este trabajo, se han ido cumpliendo los objetivos propuestos al inicio siguiendo la planificación estipulada, explicando los recursos utilizados para lograrlos.

El estudio se ha centrado en definir el concepto del *phishing*, haciendo una búsqueda exhaustiva de los tipos de ataques existentes hoy en día junto con una recopilación de ataques reales, mostrando un claro aumento desde la llegada de la pandemia de la COVID-19 en marzo de 2020.

Lo que queda claro después de este completo estudio sobre phishing es que está en constante evolución, a pasos agigantados se podría decir. Las organizaciones, instituciones, empresas o incluso usuarios particulares reciben diariamente algún correo o mensajes en sus dispositivos móviles intentando ser engañados por los atacantes, lo que hace aumentar la preocupación de los directivos y personal de seguridad de la información de las empresas, que intentan cada vez más concienciar y dar formación a sus trabajadores para prevenir o mitigar los posibles ataques en busca de información personal y confidencial, que pueden llegar a hacerles perder grandes cantidades económicas.

Es un reto para los trabajadores y usuarios estar en una alerta continua para que no les pille de sorpresa un ataque de phishing, siendo conscientes de los riesgos a los que están expuestos día tras día, con el aumento del uso de las nuevas tecnologías.

Los atacantes estudian cada día nuevas técnicas, son muy cuidadosos, intentan simular sitios web idénticos, utilizan las tecnologías más recientes, como el *cloud computing* o el Internet de las Cosas, todo con un único fin: engañar al usuario

haciéndole creer que aquello que le dicen que haga los va a llevar a un sitio legítimo y real.

En la última parte de este trabajo se han analizado diferentes utilidades software de ataque y mediante una serie de herramientas se han probado varias simulaciones de *phishing*, mostrando lo sencillo que resulta clonar un sitio web o enviar una serie de correos masivos, dándonos cuenta de que los ciberdelincuentes disponen de sencillas herramientas para automatizar los ataques y maximizar el daño, disponibles en la web, sin necesidad de tener unos conocimientos avanzados en la materia.

## 6.1. LOGROS ALCANZADOS

Tras mostrar una perspectiva general, se cree que este trabajo puede ayudar a prevenir y concienciar a personas interesadas en la materia, haciéndoles entender la facilidad de robo de datos y la importancia de estar prevenidos frente a los distintos medios de ataque, por desgracia, en auge día tras día.

A nivel personal, después del tiempo de realización de este trabajo, se ha logrado un profundo conocimiento sobre los ataques de *phishing*, habiendo despertado un gran interés en el estudio de la materia, que seguirá ampliándose durante los próximos meses.

El mundo de la ciberseguridad, y más concretamente de la ingeniería social, es tan inmenso y crece tan rápido, que debemos mantenernos actualizados de manera continua si queremos seguir dedicándonos al estudio de esta rama de la informática, lo que hará posible estar preparados para prevenir y minimizar los riesgos y a su vez, ayudar a terceras personas a proteger sus datos e información sensible.

## 6.2. TRABAJO FUTURO

Puesto que, salvo los últimos puntos de este trabajo, en los que se ha probado alguna herramienta, se considera fundamentalmente un estudio teórico de la materia, en el futuro se podría implementar alguna técnica de detección y evitación de *phishing*, con la ayuda de algoritmos de inteligencia artificial, principalmente los basados en *Machine Learning*, utilizando *Python* como lenguaje de programación, ya que cuenta con infinidad de librerías relacionadas con ella.

La idea es continuar este estudio y ampliarlo de una manera más práctica en otro trabajo de investigación que se hará en un futuro próximo, cuando se curse el Máster Universitario en Ciberseguridad, también en la UNED, que se comenzará las próximas semanas.

# REFERENCIAS BIBLIOGRÁFICAS

- [1] ¿Qué es el *Phishing*? [En línea] https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-phishing (24 de agosto 2022).

- [2] Conoce a fondo qué es el *phishing* [En línea] https://www.osi.es/es/banca-electronica (24 de agosto 2022).

- [3] ¿Qué es exactamente el *Phishing*? [En línea] https://www.avast.com/es-es/c-phishing (26 de agosto 2022).

- [4] Syiemlieh, P., Khongsit, GM., Sharma, UM., Sharma, B. (2015). Phising-An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation.

- [5] Abdelhamid, N., Ayesh, A., Thabtah, F. (2014). Phishing detection based associative classification data mining. Expert systems with Applications.

- [6] Leng Chiew, K., Sheng Chek Yong, K., Lin Tan, C. (2018). A survey of phishing attacks: Their types, vector and technical approaches. Expert Systems With Applications.

- [7] *Phishing*: Qué es y tipos. Identificarlo y protegerse [En línea] https://protecciondatos-lopd.com/empresas/phishing (28 de agosto 2022).

- [8] ¿Qué es *phishing* y qué tipos existen? [En línea] https://es.godaddy.com/blog/que-es-el-phishing-y-que-tipos-existen (28 de agosto 2022).

- [9] APWG [En línea] http://apwg.org (29 de agosto 2022).

- [10] Blog del software antivirus Avast [En línea] https://blog.avast.com/es y https://blog.avast.com (29 de agosto 2022).

- [11] Informe 2022 State of the Phish [En línea] https://www.proofpoint.com/es/resources/threat-reports/state-of-phish (29 de Agosto 2022).

- [12] Informe de amenazas sobre el *phishing* 2022 – TreatLabz [En línea] https://info.zscaler.com/resources-industry-report-threatlabz-state-of-phishing-report-es (29 de agosto 2022).

- [13] Hawa Apandi, S., Sallim J., Sidek R. (2020). Types of anti-phishing solutions for phishing attack.

- [14] Basit, A., Zafar, M., Liu X., Javed AR., Jalil, Z., Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques.

- [15] Gowtham, R., Krishnamurthib, I. (2014): A comprehensive and efficacious architecture for detecting phishing webpages.

- [16] Qabajeh, I., Thabtah, F., Chiclana, F. (2018). A recent review of conventional vs. automated cybersecurity anti-phishing techniques.

- [17] Phishing Protection: SPF, DKIM, DMARC. [En línea] https://cipher.com/blog/phishing-protection-spf-dkim-dmarc (18 de septiembre 2022).

- [18] Tallos Intelligence – Cisco. [En línea] https://www.redseguridad.com/actualidad/cisco-da-a-conocer-talos-su-nueva-division-de-ciberseguridad_20170201.html (18 de septiembre 2022).

- [19] Kali Linux [En línea] https://www.kali.org (19 de septiembre 2022).

Otros:

- Amiri, I. S., Akanbi, O. A., Fazeldehkordi, E. (2014). A Machine-Learning Approach to Phishing Detection and Defense. Syingress.

- Chio C, Freeman D. E. (2018). Machine Learning and Security.

- Tsukerman, E. E. (2019). Machine Learning for Cybersecurity Cookbook.

- Rains, T. E. (2020). Cybersecurity Threats, Malware Trends, and Strategies.

- Gupta, B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems.

- Lin, C.-H., Pao, H.-K., & Liao, J.-W. (2018). Efficient dynamic malware analysis using virtual time control mechanics.

- Nicho M., Fakhry H., & Egbue U. (2018). When spear phishers craft contextually and convincing emails. International Conferences on WWW/Internet and Applied Computing 2018.

- Vayansky, I., & Kumar, S. (2018). Phishing–challenges and solutions. Computer Fraud & Security.

- Alsharnouby M., Alaca F., & Chiasson S. (2015) Why phishing still works: User strategies for combating phishing attacks.

- Floyd, Kevin. What is Email Spoofing and How to Detect It [En línea] https://blogs.cisco.com/security/what-is-email-spoofing-and-how-to-detect-it (20 de marzo 2022).

- Bush, Paython. Why Brand Monitoring is a Security Issue – Typosquatting [En línea] https://www.anomali.com/blog/why-brand-monitoring-is-a-security-issue-typosquatting (24 de marzo 2022).

- Paganini, Pierluigi. Homograph Phishing Attacks are almost impossible to detect on major browsers [En línea] https://securityaffairs.co/wordpress/58120/breaking-news/homograph-phishing-attacks.html (24 de marzo 2022).

- Kaspersky Centro de recursos [En línea] https://latam.kaspersky.com/resource-center (24 de marzo 2022).