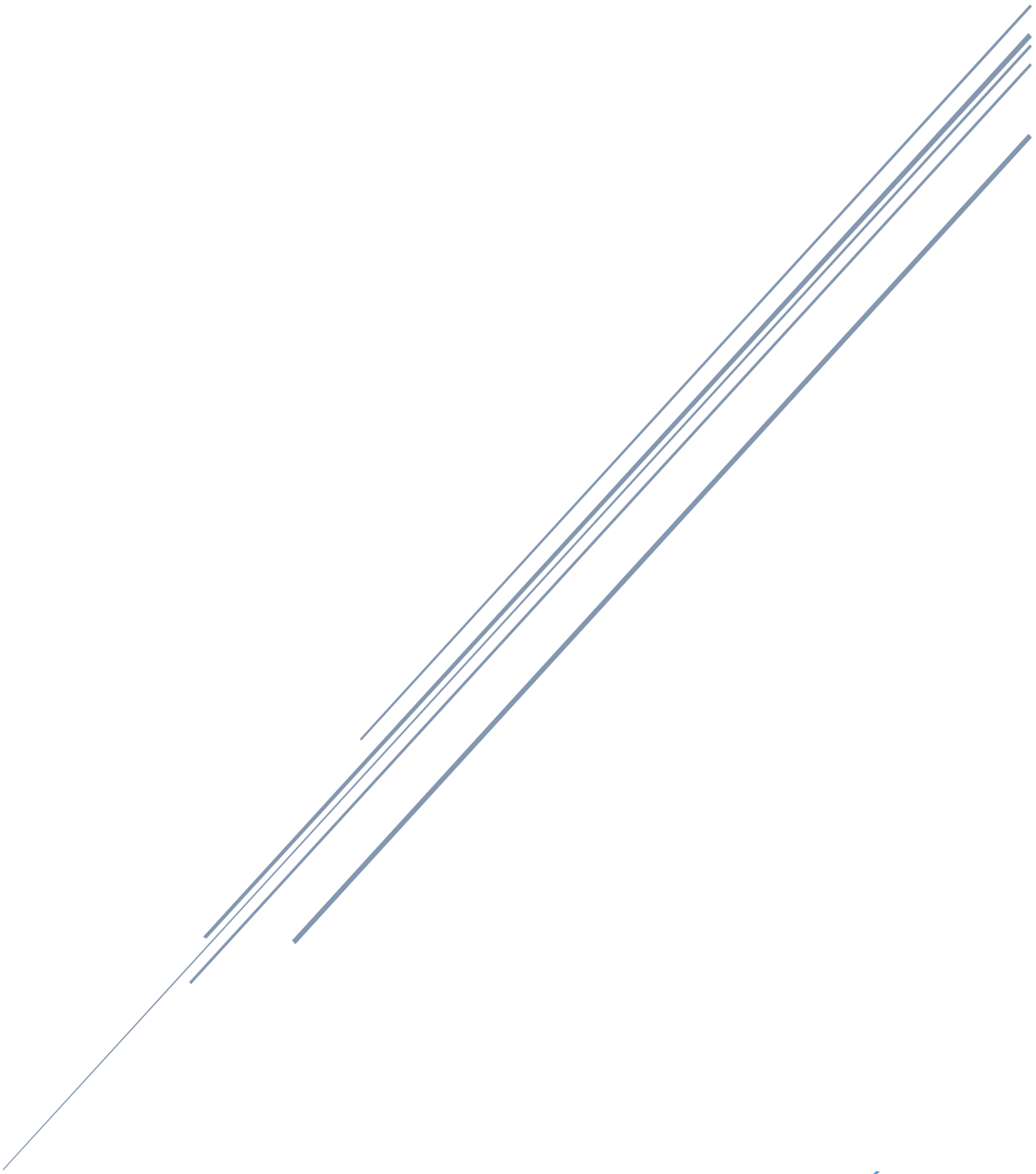
¿QUÉ ES “TYPOSQUATTING”?



EL HACKER ÉTICO

ÍNDICE

Typosquatting

1- ¿Qué es “Typosquatting”?

Typosquatting, también conocido como secuestro de URL, es un tipo de ciberdelito en el que una persona crea un sitio web con un nombre similar al de un sitio web conocido, pero con una pequeña diferencia, como una palabra mal escrita o un dominio de nivel superior diferente. El objetivo de la "typosquatting" es engañar a los usuarios para que visiten el sitio web falso tecleando mal la dirección del sitio web legítimo. Una vez que el usuario llega al sitio web falso, el ciberdelincuente puede intentar robar su información personal, como credenciales de acceso o números de tarjetas de crédito, o redirigirlo a otro sitio web que contenga software malicioso. El "typosquatting" puede ser una grave amenaza para los usuarios de Internet, ya que a la gente le resulta difícil reconocer la diferencia entre un sitio web legítimo y uno falso. Para protegerse del typosquatting, es importante comprobar cuidadosamente la dirección del sitio web antes de introducir información personal y utilizar un software de seguridad de confianza para proteger el dispositivo de programas maliciosos.

2- Variaciones utilizadas en Typosquatting

Estas son las cinco variaciones que nos podemos encontrar:

1- **El typoquatting utilizando palabras similares:** en este caso, se utilizan palabras que son muy parecidas a la palabra objetivo, pero que tienen una letra cambiada o una sílaba adicional. Por ejemplo, en lugar de "paypal.com", se puede utilizar "papal.com" o "paypall.com".

2- **El typoquatting utilizando caracteres especiales:** en este caso, se utilizan caracteres especiales para reemplazar algunas letras de la palabra objetivo. Por ejemplo, en lugar de "amazon.com", se puede utilizar "ãmazon.com".

3- **El typoquatting utilizando combinaciones de letras:** en este caso, se utilizan combinaciones de letras que pueden ser fácilmente confundidas con la palabra objetivo. Por ejemplo, en lugar de "google.com", se puede utilizar "googlé.com" o "g00gle.com".

4- **El typoquatting utilizando tildes o diéresis:** en este caso, se utilizan tildes o diéresis para reemplazar algunas letras de la palabra objetivo. Por ejemplo, en lugar de "ebay.com", se puede utilizar "ébay.com" o "ebäy.com".
5- **El typoquatting utilizando homófonos:** en este caso, se utilizan palabras que tienen el mismo sonido que la palabra objetivo, pero que tienen un significado diferente. Por ejemplo, en lugar de "apple.com", se puede utilizar "app1e.com" o "applé.com".

3- Detectar “Typosquatting”

Para detectar typosquatting, se pueden seguir los siguientes pasos:

1- **Revisar los nombres de dominio que se parecen a la marca o sitio web:** Realice una búsqueda en línea de nombres de dominio similares a la marca o sitio web que utiliza, incluyendo errores de escritura comunes, cambios de letras, tildes y otros errores.
2- **Utilizar herramientas de búsqueda de dominios:** Existen herramientas en línea que le permiten realizar búsquedas de dominios similares a su marca o sitio web, como DomainTools o Whois.
3- **Realizar un seguimiento de los nombres de dominio:** Realice un seguimiento de los nombres de dominio que se parecen a su marca o sitio web y tome medidas para proteger su marca y evitar el typosquatting.
4- **Alertar a los usuarios:** Avisar a los usuarios sobre la existencia de sitios web con nombres de dominio similares a la marca o sitio web, para que sean más conscientes de los posibles riesgos de divulgación de información confidencial o transacciones fraudulentas.

4- Herramientas para detectar dominios Typosquatting

Como indicamos anteriormente, una de las formas de impedir un ataque de Phishing utilizando dominios con modificaciones es realizar un seguimiento de los nombres de

dominios registrados para detectar aquellas que sean similares a la marca legítima y poder adelantarnos a su utilización maliciosa.

Para esto podemos utilizar las siguientes herramientas:

1- dnstwist
2- evilurl
3- opensquat
4- phishydomains.com
5- dnstwister.report

4.1. dnstwist

DNSTwist es una herramienta que puede ayudar a detectar ataques de phishing y typosquatting de nombres de dominio. Funciona generando variaciones de un nombre de dominio determinado y comprobando después si esas variaciones están registradas o si se están utilizando para alojar sitios web maliciosos. Esto permite a los profesionales de la seguridad identificar y tomar medidas contra amenazas potenciales antes de que puedan causar daños a su organización o a sus usuarios.

Para su instalación ejecutamos lo siguiente:

1- git clone https://github.com/elceef/dnstwist.git
2- cd dnstwist
3- pip install .

```
┌──(osint㉿osint)-[~]
└─$ dnstwist -h
dnstwist 20221022 by <marcin@ulikowski.pl>

usage: /usr/local/bin/dnstwist [OPTION] ... DOMAIN

Domain name permutation engine for detecting homograph phishing attacks, typosquatting, fraud and brand impersonation.

positional arguments:
  domain                Domain name or URL to scan

options:
  -a, --all             Show all DNS records
  -b, --banners         Determine HTTP and SMTP service banners
  -d FILE, --dictionary FILE  Generate more domains using dictionary FILE
  -f FORMAT, --format FORMAT  Output format: cli, csv, json, list (default: cli)
  --fuzzers LIST        Use only selected fuzzing algorithms (separated with commas)
  -g, --geoip           Lookup for GeoIP location
  -m, --mxcheck         Check if MX can be used to intercept emails
  -o FILE, --output FILE  Save output to FILE
  -r, --registered      Show only registered domain names
  -u, --unregistered    Show only unregistered domain names
  -p, --phash           Render web pages and evaluate visual similarity
  --phash-url URL       Override URL to render the original web page from
  --screenshots DIR     Save web page screenshots into DIR
  -s, --ssdeep          Fetch web pages and compare their fuzzy hashes to evaluate similarity
  --ssdeep-url URL      Override URL to fetch the original web page from
  -t NUMBER, --threads NUMBER
                        Start specified NUMBER of threads (default: 6)
  -w, --whois           Lookup WHOIS database for creation date
  --tld FILE            Swap TLD for the original domain from FILE
  --nameservers LIST    DNS or DoH servers to query (separated with commas)
  --useragent STRING    User-Agent STRING to send with HTTP requests (default: Mozilla/5.0 (linux 64-bit) dnstwist/20221022)
  --debug               Display debug messages

┌──(osint㉿osint)-[~]
└─$
```

Vamos a realizar una búsqueda básica utilizando nuestro dominio elhackeretico.com

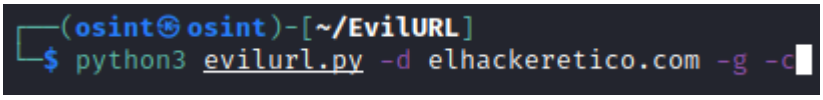
4.2. evilurl

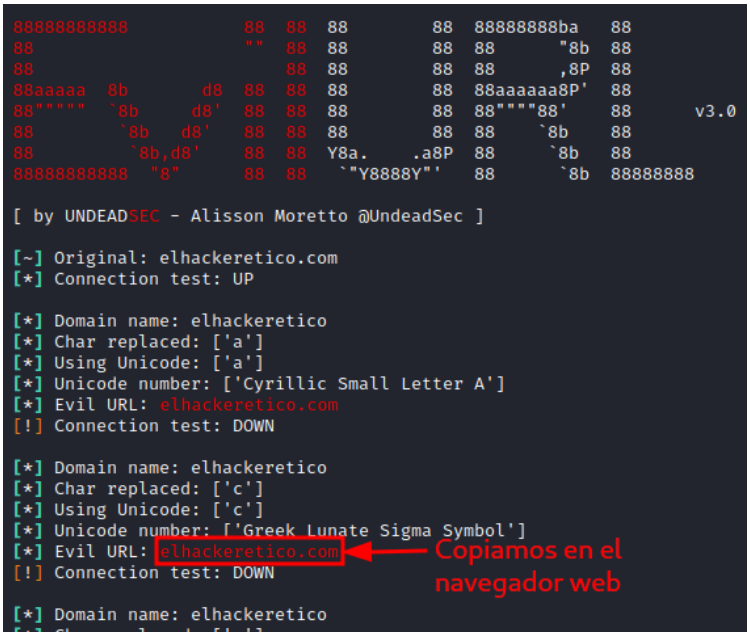
Los ataques homográficos en nombres de dominio internacionalizados (IDN) son una forma de phishing en la que se utiliza un nombre de dominio que parece idéntico a un nombre de dominio legítimo, pero que está escrito con caracteres que se asemejan visualmente a los caracteres del nombre de dominio legítimo. Por ejemplo, un atacante podría utilizar el carácter griego "Σ" (sigma) en lugar del carácter latino "S" para crear un nombre de dominio homográfico para un sitio Web de phishing.

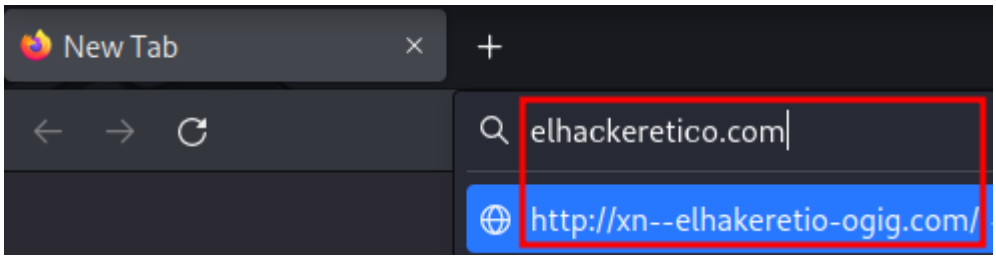
La herramienta EvilURL permite generar dominios maliciosos Unicode para realizar ataques homográficos IDN y además poder detectarlos.

Para su instalación ejecutamos lo siguiente:

1- git clone https://github.com/UndeadSec/EvilURL.git
2- pip install python-nmap python-whois
3- cd EvilURL
4- python evilurl.py







4.3. opensquat

openSquat es una herramienta OSINT utilizado para detectar campañas de Phishing, usurpación de dominio, errores tipográficos.

Para instalar:

1- git clone https://github.com/atenreiro/opensquat.git
2- cd opensquat.py
3- sudo pip3 install –r requierements.txt
4- python3 opensquat.py –h

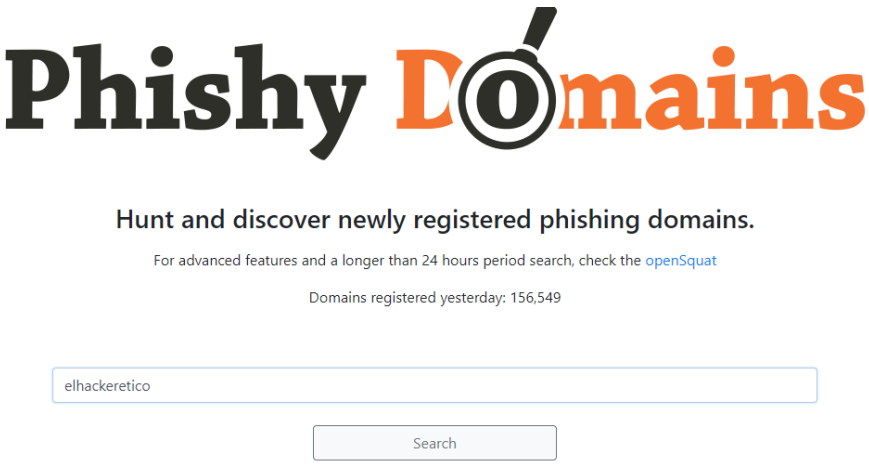
Modos de utilización:

1- Incluir en el archivo keywords.txt aquellos términos que queramos buscar.
2- python3 opensquat.py (modo predeterminado)

3- python3 opensquat.py –k generic.txt (búsqueda utilizando términos comunes en campañas de Phishing)
4- python3 opensquat.py –dns (búsqueda on validación de DNS)
5- python3 opensquat.py –subdominios (búsqueda de subdominios con términos comunes en campañas de Phishing)
6- python3 opensquat.py --portcheck (Comprobamos dominios con el Puerto 80/443 abierto)
7- python3 opensquat.py --phishing phish_result.txt (Búsqueda comparando resultados con una base de datos de Phishing)
8- python3 opensquat.py –o ejemplo.json –t json (Guardar los resultados en formato de salida JSON)
9- python3 opensquat.py –p mes (Búsqueda por periodos, en el ejemplo, búsqueda en el último mes)

4.4. phishydomains.com

Sitio Web cuya utilidad es buscar dominios de Phishing registrados en las últimas 24 horas.



4.5. dnstwister.report

Al igual que en el punto anterior, sitio Web donde podremos buscar nombres de dominios similares al legítimo para poder monitorizarlos antes de que realicen actividades maliciosas suplantando la identidad de la organización real.