17 de mayo: Día Mundial de Internet

Pese a los riesgos de seguridad el typosquatting pasa desapercibido para los usuarios

- *Sin embargo, lidera el ranking de la ciberocupación, ya que los ciberdelincuentes hacen uso del error tipográfico (typosquatting) en sus estrategias de phishing*
- *España se erige en potencia mundial de ciberocupación con el quinto puesto en demandas por ocupación de dominio en internet*

Madrid, martes 16 de mayo de 2023.- El typosquatting, que lidera el ranking de la ciberocupación, consiste en registrar un nombre de dominio modificado o mal escrito para redirigir a los usuarios a un sitio web fraudulento. Según datos de la Organización Mundial de Propiedad Intelectual, en 2022 se presentaron casi 6.000 denuncias a este organismo por ciberocupación, una cifra un 10% superior respecto a 2021 y que, según todas las previsiones, para este año seguirá siendo una tendencia al alza.

Hoy en día, la mayoría de los dueños de negocios ya conocen las técnicas de ciberocupación que utilizan los actores maliciosos. Sin embargo, muchos usuarios habituales de Internet no son conscientes de los peligros y las tácticas empleadas por los ciberocupas como el typosquatting o error tipográfico. El equipo de Seguridad TI de acens Part of Telefónica Tech (**www.acens.com**) ha querido recordar con motivo del Día Mundial de Internet la importancia de estar alerta, cómo identificar el typosquatting y cómo protegernos.

Para llevar a cabo este tipo de técnica fraudulenta, los ciberdelincuentes pueden utilizar diferentes métodos. Los más frecuentes y a los que más atención hay que prestar son:

1. **Extensión**. Los hackers registran un dominio libre de una empresa, normalmente las extensiones menos solicitadas. Por ejemplo, Versace denunció el año pasado la ocupación de extensión de los dominios 'versace.cam' y 'versace.club', entre otros. En España la mayoría de las empresas registra la extensión .es y la .com, quedando extensiones como .eu a disposición de los ciberdelincuentes.
2. **Sustitución**. Sustituyen uno o varios caracteres por otros que, a simple vista, parecen similares. Por ejemplo, si llega un email de 'promos@rnovistar.com' puede parecer que Movistar nos está enviando una promoción, pero si se observa bien el nombre de dominio se aprecia que la "m" ha sido sustituida por "rn".
3. **Inserción**. Es frecuente también añadir una letra que, además, en ocasiones se confunde con la extensión, como 'incibes.es' o 'gooogle.com'.
4. **Intercambio.** Aquí los ciberocupas cambian de posición u omiten alguna letra respecto del nombre real que se busca, por ejemplo 'acesn.com'.

Para Manuel Prada Mateo, Responsable de Seguridad IT en acens: "*Estos sitios web suplantados suelen ir enlazados a emails fraudulentos y a campañas de phishing que, en muchas ocasiones, tienen éxito fácilmente. Las campañas de phishing que explotan el typosquatting no necesitan ser innovadoras para tener éxito ya que cuentan con dos aspectos a su favor. Por un lado, el estilo de vida del usuario, veloz, con prisas, que apenas chequea una URL o un correo electrónico como demuestran los datos. Es alarmante cómo el **60% de los usuarios no presta atención a la extensión** del dominio de una URL, según hemos comprobado desde acens en una encuesta pública. Y por otro lado, cuentan con la confianza del usuario: casi un 50% de los empleados españoles cree que el correo electrónico de su empresa es seguro, lo que*

contrasta con el hecho de que el 90% de las empresas españolas reconoce haber sufrido un ataque de phishing con éxito".

Prada recomienda tres técnicas válidas para protegernos de este tipo de ataques:

1. Por un lado, desde un punto de vista empresarial, **se pueden registrar dominios mal escritos semejantes al dominio raíz** para evitar que sean utilizados. De la misma forma, se pueden redirigir dichos dominios al dominio legítimo.
2. Además, se debe **potenciar la concienciación de los usuarios** para que reconozcan este tipo de trampas, sepan identificar dominios falsos y cómo actuar ante ellos.
3. Por último, se pueden utilizar contramedidas para detectar orígenes que utilicen este tipo de ataques, como **tecnología anti-spoofing o correo electrónico seguro**.

Puedes encontrar más información sobre Cloud Hosting, Internet y Tecnología en el **Blog** de acens. También puedes suscribirte al boletín de noticias **aceNews**, ver vídeos en **acens.tv**, apuntarte a cursos gratuitos en **Formacionacens.com** y seguirnos en **Facebook** (acenstec), **Twitter** (@acens), **Instagram** (@acens_com) e **iVoox** (acens Podcast).

Acerca de acens:

acens Part of Telefónica Tech, es pionera en el desarrollo de soluciones Cloud para pequeñas y medianas empresas a las que ofrece soluciones flexibles, seguras y eficaces, tanto en entornos de cloud privados como en públicos y mixtos. Comenzó su actividad en 1997 y en la actualidad ofrece sus servicios en España, Brasil, Perú y México. Además, posee dos Data Centers en España con más de 6.000 metros cuadrados y su cartera de clientes supera los 160.000.
https://www.acens.com/

Acerca de Telefónica Tech:

Telefónica Tech es la empresa líder en transformación digital. La compañía ofrece una amplia gama de servicios y soluciones tecnológicas integradas en Ciberseguridad, Cloud, IoT, Big Data y Blockchain.
https://telefonicatech.com/es

Para más información:

Noizze Media para acens
Carmen Tapia / Ricardo Schell
ctapia@noizzemedia.com / ricardo.schell@noizzemedia.com
646 892 883 / 699 983 936

acens
Inma Castellanos
inma@acens.com