Boletín de Ciberseguridad

04/2024

—

Servicio Central de Informática
Unidad de Ciberseguridad
ciberseguridad@uma.es

Día 1 - Año 0

Este mes nace este nuevo proyecto, en el que vamos a tratar de acercaros la ciberseguridad, de una manera distendida y cercana, a vuestro día a día.

Pensamos que es un tema que os puede interesar, ya que forma parte de nuestra vida diaria, tanto en lo profesional como en lo personal.

Este boletín pretende llegar a todos los públicos, así que no esperéis un documento de alto nivel técnico, sino algo entretenido pero a su vez, formativo.

Esperemos lograrlo, así que … ¡¡¡ a jugar !!!

Este mes en la UMA

Lucía

A principios del mes de abril, recibimos el informe de incidentes de seguridad reportados al Centro Criptológico Nacional (CCN), a través de la plataforma **Lucía**. El reporte es importante para el control de los ciberataques.

Todo mensaje relacionado con la seguridad, enviado a incidentes@uma.es se recoge en la plataforma, se estudia y se investiga hasta su resolución. Cualquier incidente de seguridad tratado en la UMA, se debe reportar con esta herramienta.

Universidades	Reporta a LUCIA	Total Reportados	Nº Puestos
Universidad Autónoma de Madrid	Anual	0	7800
Universidad de A Coruña	Anual	0	1500
Universidad de Alcalá	Anual	2	1500
Universidad de Alicante	Anual	1072	6564
Universidad de Almería	Anual	0	2115
Universidad de Burgos	Anual	0	2684
Universidad de Cádiz	Anual	0	1500
Universidad de Córdoba	Anual	2	1500
Universidad de La Rioja	Anual	0	3411
Universidad de Málaga	Anual	658	24000
Universidad de Sevilla	Anual	81	1500
Universidad de Vic	Anual	0	2060
Universidad de Zaragoza	Anual	13	15450
Universidad Islas Baleares	Anual	2	1500
Universidad Jaume I de Castellón	Anual	13	1500
Universidad País Vasco	Anual	1	29034
Universidad Politecnica Cataluña (UPC)	Anual	1	502
Universidad Politécnica de Cartagena	Mensual	5	2100
Universidad Politécnica de Madrid	Mensual	27	25000
Universidad Pompeu Fabra	Anual	0	1500
Universidad Rovira i Virgili	Anual	0	1500
UNIVERSITAS XXI Soluciones y Tecnología para la Universidad	Anual	0	1500
Sigma Gestión Universitaria, A.I.E (M.P)	Anual	0	1500
Universidad Complutense de Madrid	Anual	0	1500
Universidad de Granada	Anual	0	1500

Es un informe para todas las administraciones públicas y cuerpos de seguridad, aunque como podéis ver, en la sección de universidades, aún nos queda mucho camino por recorrer, porque no todos reportan o no reportan todo.

```
Ojo!! No reportado, no significa NO atacado
```

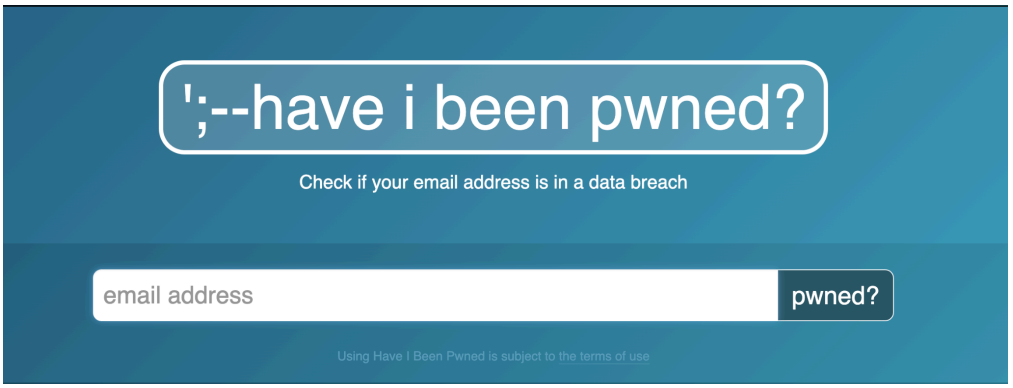
Incidentes de seguridad

Como destacable durante este mes, hemos detectado una filtración que afectaba a **156 direcciones de correo electrónico**, en las que se sabía la contraseña.

- 5 PDI
- 61 Egresados
- 90 Alumnos

Las filtraciones en el lenguaje de ciberseguridad se conocen como **leaks** y en la mayor parte de las ocasiones proceden de **contraseñas reutilizadas**. Esas cuentas vulneradas se suelen utilizar, en la mayoría de los casos, para mandar spam o phishing.

Troy Hunt, desde la web https://haveibeenpwned.com/ nos ayuda a comprobar si alguna de nuestras cuentas está comprometida. No quiere decir que si no aparece no lo esté, pero al menos es una ayuda.



El uso de **una única contraseña para múltiples servicios** como Instagram, Facebook, Dropbox, UMA, entre otros, aumenta nuestra vulnerabilidad. Si esta contraseña es comprometida en alguno de estos servicios, todos los demás quedan expuestos.

```
La contraseña que usas para @uma.es no la reutilices
```

Para almacenar las contraseñas podemos acudir a herramientas especializadas como: **1password, keepass, bitwarden, dashlane.**

Estas herramientas guardan nuestras contraseñas en una base de datos cifrada.

Scareware

Este mes también han entrado algunos correos de este estilo:

Asunto: ✉Conclusion judiciaire–✉
De: Dirección Regional <mariannemay.caballero@deped.gov.ph>
Fecha: 30/3/24, 23:13
Para: undisclosed-recipients:;

Hola

Mi nombre es Stéphane Theimer, comisario elegido para el cargo de jefe de la BPME (Brigada Europol para la Protección de Menores).
Me gustaría informarle que en menos de 72 horas se iniciarán varios procesos judiciales contra él, ya que fue declarado culpable tras una incautación informática realizada por la Comisión Europea de Investigación (CEE) en colaboración con la BPME (Brigada Europol para de Protección de Menores) por posesión y visualización de imágenes pedófilas y pornográficas; Más claramente, cometió varios delitos en Internet después de haber sido atacado en sitios de anuncios clasificados, sitios de citas y ciertas redes sociales por haber visto videos e imágenes de abuso sexual de niños, su historial de navegación fue examinado por nuestra herramienta de extracción de datos (anotación). , fotografías/vídeos de desnudos, especialmente menores, y diversos elementos fueron registrados y constituyen prueba de sus crímenes.
Según la información vinculada a las acusaciones usted es culpable de los hechos, desconoce sus verdaderas intenciones al momento de los hechos, tiene derecho a responder, a ejercerlo, le solicitamos que responda a este mensaje y Da tus verdaderas razones tan pronto como recibas este mensaje.
Para evitar confusiones al resolver este problema, responda a este mensaje y envíe sus documentos de respaldo de inmediato:

Espero escuchar los detalles de sus explicaciones y motivaciones.

AHORA ESTÁS ADVERTIDO.

Atentamente

Stéphane Theimer, comisario de GMP

Director adjunto de EUROPOL
Jefe de la Oficina de Protección Infantil (BPM)
Responsable del Centro Europeo de Ciberdelincuencia – EC3 / Europol

This communication may contain confidential or privileged information, and is intended solely for the individual or entity to whom it is originally addressed. Any disclosure, copying, diss
message are those of the sender and may not necessarily reflect the views of the Department

Lo sé, lo sé, y lo que es más importante, la Guardia Civil también lo sabe: todos sois inocentes.

Este tipo de correos se denominan **scareware** y su objetivo es alarmarnos para que contactemos con ellos. Luego vendrá el fraude.

Así que si nos encontramos un correo de este tipo, a la basura directamente.

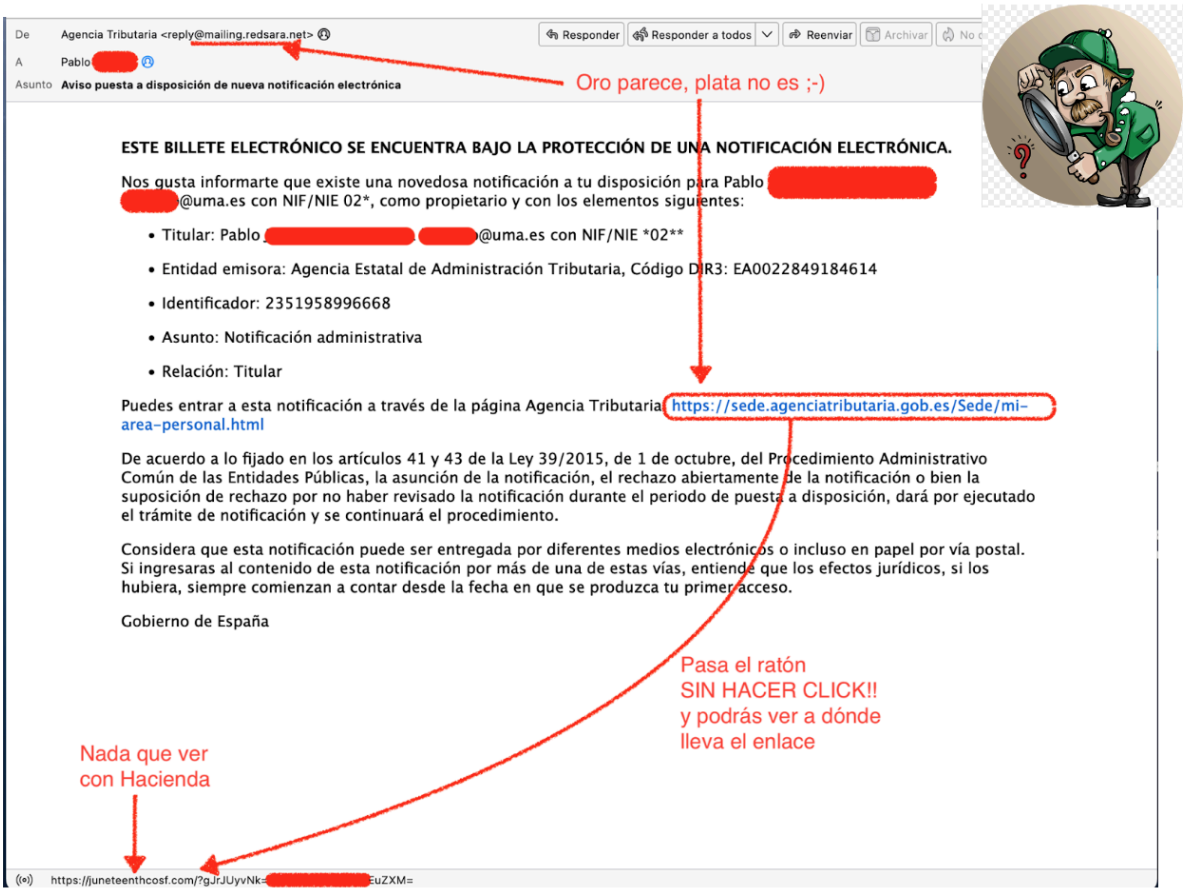
Resto del mundo

Renta 2024

Comienza la campaña de la Renta y debemos estar alerta al phishing o el smishing.

Son técnicas muy parecidas, la primera es un correo electrónico y la segunda un SMS. En ambas se intenta suplantar a alguien, en este caso al ministerio de hacienda. Suelen venir con un enlace que nos redirige a un sitio fraudulento.

Os pego uno que entró el año pasado y al que le puse unos comentarios

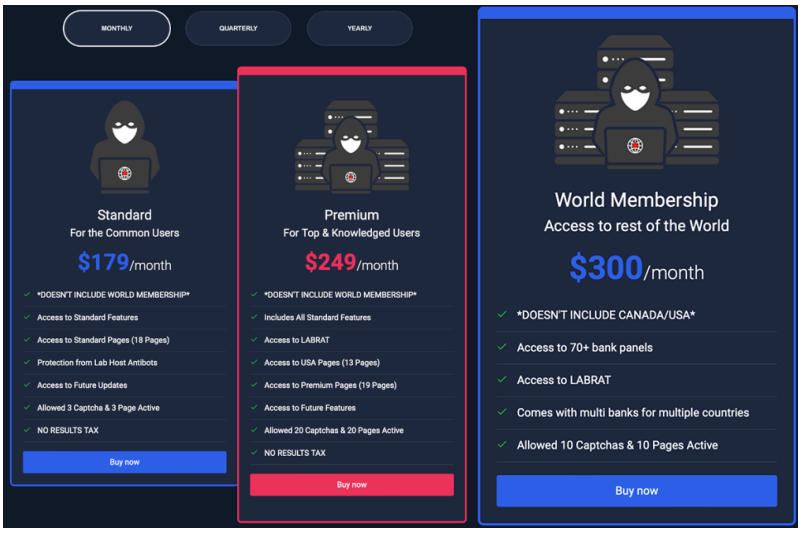


Desarticulado el grupo Labhost[1]

El 18 de abril, la policía metropolitana de UK, Europol y otros cuerpos de seguridad desarticularon a un grupo cibercriminal conocido como **Labhost** dedicados al *Phishing As A Service* (PhaaS).

¿Qué significa esto de PhaaS?

Fácil, si alguien quiere hacer phishing a una organización, no tiene que montar una infraestructura para ello. Va a uno de estos "supermercados del crimen" y contrata el servicio. No hacen falta conocimientos en phishing, ciberseguridad o lo que se os ocurra, sólo tener bitcoins para contratarlo.



La plataforma ofrecía una serie de beneficios a su clientela, dependiendo del tipo de membresía contratada.

- Páginas de phishing para bancos, servicios postales, seguros, spotify
- Plantillas de phishing altamente personalizables. Incluso especializadas en el objetivo/organización a atacar (spear phishing).
- Estadísticas detalladas de la campaña.
- Posibilidad de hacer phishing con los mensajes a móviles (smishing)

Y hasta aquí este primer boletín que espero os haya resultado entretenido y didáctico.

¿Nos vemos en el próximo?

[1] https://www.trendmicro.com/en_us/research/24/d/labhost-takedown.html
Imágenes: Freepick