PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

110-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°110	Fecha: 11-05-2024
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Europol confirma la existencia de una brecha en su portal web		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. ANTECEDENTES:

Europol, la agencia encargada de hacer cumplir la ley de la Unión Europea, confirmó que su portal de la Plataforma Europol para Expertos (EPE) fue violado y ahora está investigando el incidente después de que un actor de amenazas afirmó que robaron documentos para uso oficial únicamente (FOUO) que contenían datos clasificados.

EPE es una plataforma en línea que los expertos encargados de hacer cumplir la ley utilizan para "compartir conocimientos, mejores prácticas y datos no personales sobre delitos".

2. DETALLES:

En el momento de la publicación, el sitio web de la EPE estaba fuera de línea y un mensaje indicaba que el servicio no estaba disponible debido a tareas de mantenimiento.

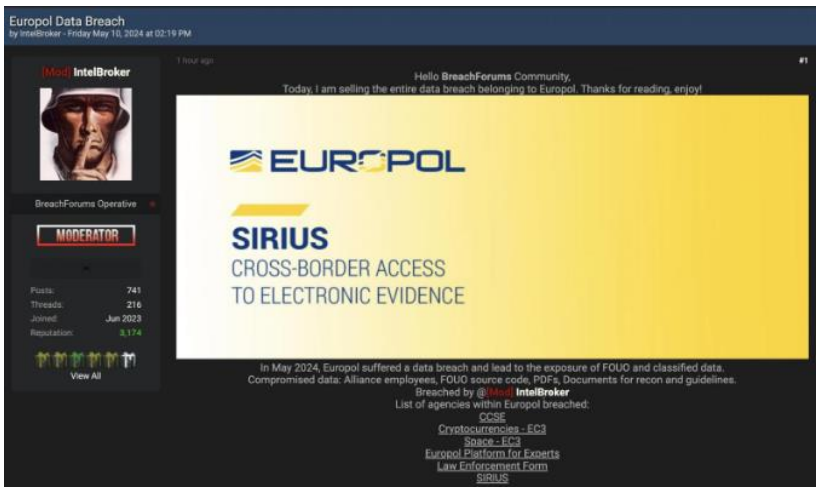
IntelBroker, el actor de la amenaza que está detrás de las acusaciones de violación de datos, describe los archivos como FOUO y que contienen datos clasificados.

El actor de la amenaza afirma que los datos supuestamente robados incluyen información de empleados de la alianza, código fuente FOUO, PDF y documentos de reconocimiento y orientación.

También afirma haber accedido a EC3 SPACE (Plataforma segura para expertos acreditados en ciberdelincuencia), una de las comunidades del portal EPE, que alberga cientos de documentos relacionados con la ciberdelincuencia y es utilizada por más de 6.000 expertos acreditados en ciberdelincuencia de todo el mundo, entre ellos:

- Autoridades policiales de los Estados miembros de la UE y de países no pertenecientes a la UE.
- Autoridades judiciales, instituciones académicas, empresas privadas, organizaciones no gubernamentales e internacionales.
- Personal de Europol.

IntelBroker también afirma haber puesto en peligro la plataforma SIRIUS, utilizada por autoridades judiciales y policiales de 47 países, entre ellos Estados miembros de la UE, el Reino Unido, países con un acuerdo de cooperación con Eurojust y la Fiscalía Europea (EPPO). SIRIUS se utiliza para acceder a pruebas electrónicas transfronterizas en investigaciones y procedimientos penales.



Además de capturas de pantalla de la interfaz de usuario en línea de EPE, IntelBroker también ha filtrado una pequeña muestra de una base de datos EC3 SPACE que supuestamente contiene 9.128 registros. La muestra contiene lo que parece ser información personal de agentes de la ley y expertos en ciberdelincuencia con acceso a la comunidad EC3 SPACE.

Europol dice que el portal no fue pirateado debido a una vulnerabilidad o una mala configuración, sino que, en cambio, los atacantes obtuvieron acceso a los datos utilizando credenciales robadas.

"Europol es consciente del incidente y está evaluando la situación. Ya se han tomado las medidas iniciales. El incidente afecta a un grupo cerrado de usuarios de la Plataforma de Expertos de Europol (EPE)", dijo Europol. "No se procesa información operativa en esta aplicación EPE. Ningún sistema central de Europol se ve afectado y, por lo tanto, ningún dato operativo de Europol se ha visto comprometido".

3. RECOMENDACIONES:

- Controlar sus cuentas para detectar cualquier actividad inusual y que tomen precauciones para proteger su información personal.
- Practicar una higiene estricta de contraseñas. Utilizar contraseñas únicas para cada tarjeta y cambiarlas periódicamente.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.
- Tener cuidado con las estafas telefónicas de soporte técnico que podrían implicar la explotación de los datos robados.

Fuente de Información:	• hxxps://cibernovedades.com/europol-confirma-la-existencia-de-una-brecha-en-su-portal-web/ • hxxps://www.bleepingcomputer.com/news/security/europol-confirms-web-portal-breach-says-no-operational-data-stolen/#google_vignette

Índice alfabético