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

068-2025-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°068	Fecha: 22-03-2025
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Cómo los ciberdelincuentes explotan la información pública para sus ataques		
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:

Los ciberdelincuentes son expertos en usar información pública para su beneficio. Saber cómo recopilan estos datos puede ayudarte a protegerte y a proteger tu información personal. Suelen obtener información de redes sociales, perfiles en línea y registros públicos para crear ataques convincentes.

Comprender las tácticas que emplean estos delincuentes puede marcar una diferencia significativa en tu seguridad en línea.

2. DETALLES:

Los ciberdelincuentes utilizan diversos métodos para explotar información pública en sus ataques. Estos métodos les permiten recopilar información y atacar eficazmente a sus víctimas:

- **Identificación de objetivos a través de datos públicos:** Los ciberdelincuentes suelen recopilar información de fuentes abiertas , conocidas como inteligencia de fuentes abiertas (OSINT). Buscan datos en redes sociales, registros públicos y sitios web para identificar a posibles víctimas.

  Por ejemplo, pueden buscar ofertas de trabajo para encontrar empleados o consultar las redes sociales para obtener información personal, como cumpleaños y aniversarios.

  Al recopilar esta información, pueden crear perfiles de personas y organizaciones. Este enfoque específico aumenta la eficacia de sus ataques.

- **Tácticas de ingeniería social:** Una vez que los ciberdelincuentes han recopilado suficiente información, suelen emplear tácticas de ingeniería social para manipular a sus objetivos. Esto puede incluir correos electrónicos de phishing, donde se hacen pasar por una fuente confiable, como un banco o un compañero.

  Pueden redactar mensajes que incluyan datos personales para hacerlos más convincentes.

  También pueden hacer llamadas telefónicas usando la información que han encontrado, haciéndose pasar por una figura de autoridad para extraer datos confidenciales.

- **Phishing y Spear Phishing:** El phishing consiste en enviar correos electrónicos falsos para engañar a las personas y que compartan información personal. Estos correos pueden parecer reales y, a menudo, imitan fuentes confiables.

  El phishing selectivo es una versión más específica. En lugar de atacar a muchas personas, se centra en una persona u organización específica. Los atacantes recopilan información personal de redes sociales y otras fuentes. Esto hace que sus mensajes parezcan creíbles y aumenta sus posibilidades de éxito.

- **Compromiso de correo electrónico empresarial (BEC):** El ataque de correo electrónico empresarial (PDF) se centra en las cuentas de correo electrónico empresariales. Los ciberdelincuentes se hacen pasar por altos ejecutivos o proveedores de confianza para manipular a los empleados.

  Pueden enviar correos electrónicos solicitando transferencias de fondos o información confidencial. Las víctimas suelen creer que se están comunicando con alguien de confianza. Esto puede ocasionar pérdidas financieras significativas.

- **Implementación de ransomware:** El ransomware es un malware que impide el acceso a los archivos o al sistema hasta que se pague un rescate. Este tipo de ataque puede comenzar cuando los ciberdelincuentes recopilan información sobre las operaciones de la empresa.

  Una vez que comprenden los sistemas de su organización, pueden implementar ransomware con mayor eficacia. Podrían enviar enlaces maliciosos o archivos adjuntos infectados mediante correos electrónicos aparentemente legítimos.

3. RECOMENDACIONES:

- Realizar y normalizar copias de seguridad periódicas de los datos importantes.
- Utilizar el cifrado para datos confidenciales, tanto en reposo como en tránsito. Esto protege la información incluso si es interceptada.
- Instalar un firewall para bloquear el acceso no autorizado a su red.
- Mantener el software y los sistemas actualizados. Esto incluye sistemas operativos, aplicaciones y software de seguridad para corregir vulnerabilidades.
- Programar evaluaciones de seguridad periódicas para ayudar a encontrar y solucionar problemas potenciales antes de que sean explotados.
- Fomentar el uso de contraseñas seguras y únicas. Herramientas como los gestores de contraseñas pueden ser útiles.
- Enseñar al personal a reconocer correos electrónicos y mensajes sospechosos. Utilizar ejemplos reales para una mejor comprensión.
- Concientizar a los empleados para que limiten la información personal que comparten en línea. Esto puede evitar que los ciberdelincuentes recopilen información.

Fuente de Información:	• hxxps://hackread.com/how-cybercriminals-exploit-public-info-attacks-risks-prevention/

Índice alfabético