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

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc

Lima, 24 de julio de 2022

N° 199-2022-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 Aérea del 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 las empresas 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

El gigante de la seguridad digital Entrust atacado por banda de ransomware....4
Phishing, suplantado la identidad de la compañía multinacional Amazon....5
Índice alfabético....7

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 199	Fecha: 24-07-2022
		Página 04 de 07

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	El gigante de la seguridad digital Entrust atacado por banda de ransomware		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

A través del monitoreo y búsqueda de amenazas en el ciberespacio del día 23 de Julio del 2022, se tomó conocimiento sobre que el gigante de la seguridad digital Entrust ha confirmado que sufrió un ciberataque donde los actores de amenazas violaron su red y robaron datos de los sistemas internos.

ANTECEDENTES:

Entrust es una empresa de seguridad centrada en la gestión de la confianza e identidad en línea, que ofrece una amplia gama de servicios, incluidas comunicaciones cifradas, pagos digitales seguros y soluciones de emisión de identificación, dependiendo de los datos robados, este ataque podría afectar a un gran número de organizaciones críticas y sensibles que utilizan Entrust para la gestión y autenticación de identidades.

Esto incluye agencias gubernamentales de los Estados Unidos, como el Departamento de Energía, el Departamento de Seguridad Nacional, el Departamento del Tesoro, el Departamento de Salud y Servicios Humanos, el Departamento de Asuntos de Veteranos, el Departamento de Agricultura y muchos más.

Si bien no está claro si los dispositivos fueron encriptados durante el ataque, las bandas de ransomware comúnmente roban datos antes de lanzar sus encriptadores para ser utilizados en esquemas de doble extorsión. Según el CEO de AdvIntel, Vitali Kremez, una operación de ransomware compró credenciales de Entrust comprometidas y las utilizó para violar su red interna.

La operación del grupo responsable se basó en la red confiable de vendedores de acceso a la red para obtener acceso inicial al entorno Entrust, lo que llevó a la posterior exposición de cifrado y exfiltración a través de un grupo de ransomware conocido.

RECOMENDACIONES:

- Mantenga siempre actualizado el sistema operativo y ejecutar análisis antivirus.
- Realice periódicamente copia de seguridad de los datos.

Fuentes de información	▪ www.bleepingcomputer.com/news/security/digital-security-giant-entrust-breached-by-ransomware-gang/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 199	Fecha: 24-07-2022
		Página 05 de 07

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantado la identidad de la compañía multinacional Amazon		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Subfamilia	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la compañía multinacional de comercio electrónico Amazon, el cual indican que el centro de facturación de la empresa requiere una verificación de actualización de datos bancarios de la posible víctima, como nombre y número la de tarjeta, fecha de vencimiento, código de seguridad, entre otros.

2. **Imagen**: Proceso del ataque Phishing:

Imagen 1: Solicita dirección de correo electrónico y contraseña.

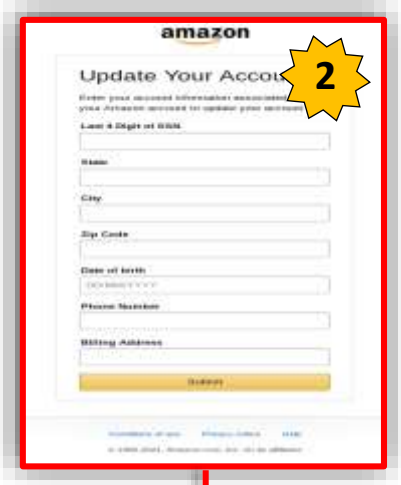


Imagen 2: Una vez hecho clic en <iniciar sesión> redirige a una supuesta página de Amazon, donde pide ingresar datos personales y bancarios, a fin de realizar una verificación de cuenta.

Imagen 3: Luego, solicita verificar su correo electrónico.

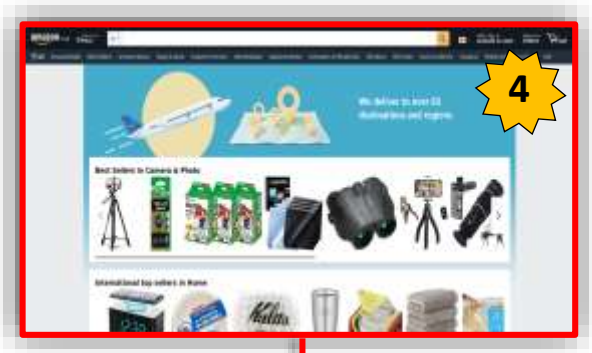
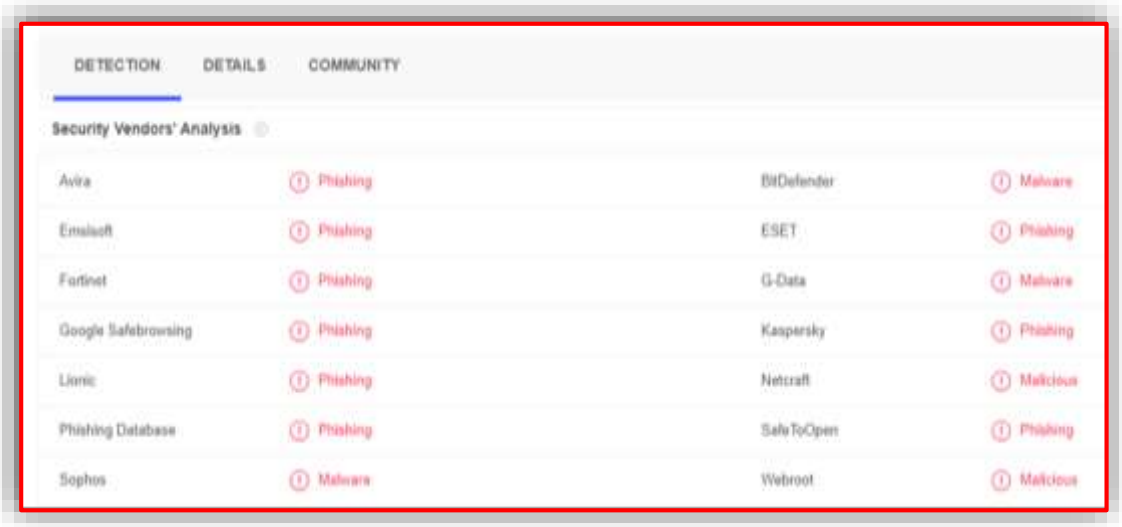


Imagen 4: Por último, es redirigido automáticamente a un supuesto sitio web de Amazon, donde la víctima puede verificar una serie de consultas como se aprecia en la imagen.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps[:]//fsuppotryd[.]com/makeamove/amazon/amazon/
  - ✓ **Dominio:** fsuppotryd[.]com
  - ✓ **IP:** 213[.]165[.]239[.]54
  - ✓ **Código:** 404
  - ✓ **Longitud:** 315 B
  - ✓ **SHA-256**: d5a89e26beae0bc03ad18a0b0d1d3d75f87c32047879d25da11970cb5c4662a3



- **OTRAS DETECCIONES:**

4. **ALGUNAS RECOMENDACIONES:**

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta

Índice alfabético

Amazon 5, 6
Ciberespacio 4, 5
Phishing 5
Ransomware 4