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

# ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

**Lima, 23 de enero de 2023**


# 020-2023-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

Hackers propagan malware en archivos adjuntos de OneNote ..... 4

Índice alfabético ..... 6

| Centro Nacional de Seguridad Digital | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 020 | Fecha: 23-01-2023 |
|---|---|---|
| | | Página 4 de 6 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO NACIONAL DE SEGURIDAD DIGITAL** | | |
| Nombre de la alerta | Hackers propagan malware en archivos adjuntos de OneNote | | |
| Tipo de ataque | Malware | Abreviatura | Malware |
| Medios de propagación | Red, Internet, Correo Electrónico, Redes Sociales | | |
| Código de familia | C | Código de subfamilia | C01 |
| Clasificación temática familia | Código malicioso | | |

Descripción

Los atacantes ahora usan archivos adjuntos de OneNote en correos electrónicos de phishing que infectan a las víctimas con malware de acceso remoto que se puede usar para instalar más malware, robar contraseñas o incluso billeteras de criptomonedas.

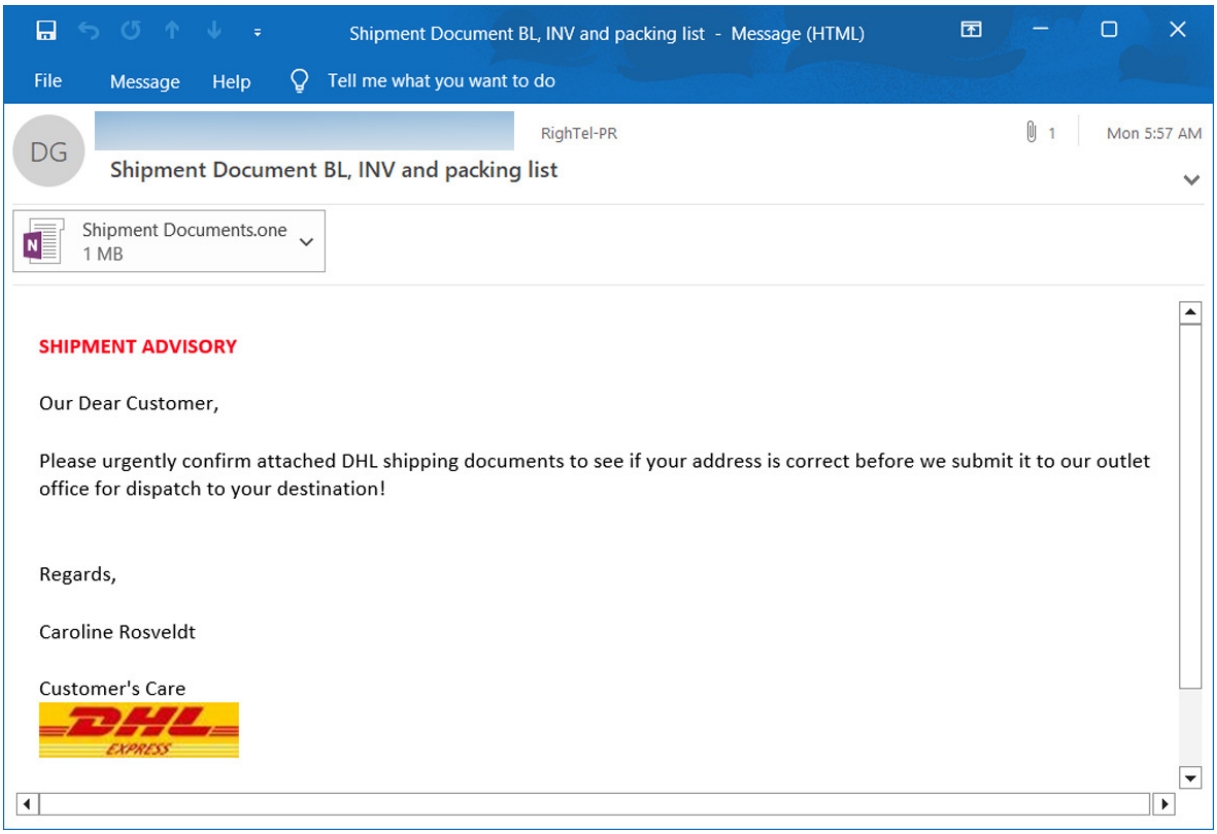
Esto ocurre después de que los atacantes hayan estado distribuyendo malware en correos electrónicos utilizando archivos adjuntos maliciosos de Word y Excel que ejecutan macros para descargar e instalar malware.

**DETALLES:**

Como Microsoft OneNote se instala de manera predeterminada en todas las instalaciones de Microsoft Office/365, incluso si un usuario de Windows no usa la aplicación, todavía está disponible para abrir el formato de archivo.

Desde mediados de diciembre, los investigadores de ciberseguridad advirtieron que los actores de amenazas habían comenzado a distribuir correos electrónicos no deseados maliciosos que contenían archivos adjuntos de OneNote .

A partir de muestras encontradas por BleepingComputer, estos correos electrónicos maliciosos pretenden ser notificaciones de envío de DHL, facturas, formularios de envío de ACH, dibujos mecánicos y documentos de envío.



A diferencia de Word y Excel, OneNote no admite macros, que es como los actores de amenazas lanzaban previamente scripts para instalar malware. En cambio, OneNote permite a los usuarios insertar archivos adjuntos en un cuaderno que, al hacer doble clic, iniciará el archivo adjunto.

Los actores de amenazas abusan de esta función al adjuntar archivos adjuntos VBS maliciosos que inician automáticamente el script cuando se hace doble clic para descargar malware desde un sitio remoto e instalarlo.

En los correos electrónicos maliciosos vistos por BleepingComputer, los archivos de OneNote instalan troyanos de acceso remoto que incluyen funcionalidad para robar información. El investigador de ciberseguridad James confirmó esto y le dijo a BleepingComputer que los archivos adjuntos de OneNote que analizó instalaron los troyanos de acceso remoto AsyncRAT y XWorm. Un archivo adjunto de OneNote visto por BleepingComputer instala lo que se detecta como el troyano Quasar Remote Access.

**RECOMENDACIONES:**

- Evite hacer clic los enlaces de mensajes de spam/phishing o ingresar a sitios web desconocidos.
- Evite revelar información personal mediante un mensaje de texto o un correo electrónico de una fuente que no sea de confianza en donde se le solicita información personal.
- Evitar abrir archivos adjuntos de correos electrónicos sospechosos.
- Mantenga sus programas, antivirus y sistema operativo actualizados.

| | |
|---|---|
| Fuentes de información | ▪ hxxps://www.bleepingcomputer.com/news/security/hackers-now-use-microsoft-onenote-attachments-to-spread-malware/ |

# Índice alfabético

distribuir correos ..... 4
insertar ..... 5
malware ..... 4
notificaciones ..... 4
OneNote ..... 4
phishing ..... 4
robar contraseñas ..... 4