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

104-2024-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° 104	Fecha: 04-05-2024
		Página: 4 de 5

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los piratas informáticos abusan cada vez más de la API Microsoft Graph para comunicaciones sigilosas de malware		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Los actores de amenazas han estado utilizando cada vez más la API de Microsoft Graph como arma con fines maliciosos con el objetivo de evadir la detección.

Esto se hace para "facilitar las comunicaciones con la infraestructura de comando y control (C&C) alojada en los servicios en la nube de Microsoft", dijo el Symantec Threat Hunter Team.

2. DETALLES:

Los grupos de hackers están optando por los servicios en la nube de Microsoft para alojar malware, debido a la buena reputación de la empresa. Este tipo de tráfico no va a hacer saltar ninguna alarma, argumentan: "Las comunicaciones de los atacantes con los servidores C&C a menudo pueden generar señales de alerta en las organizaciones objetivo", dijo Symantec. "La popularidad de Graph API entre los atacantes puede deberse a la creencia de que es menos probable que el tráfico a entidades conocidas, como los servicios en la nube ampliamente utilizados, genere sospechas".

"Además de parecer discreto, también es una fuente de infraestructura barata y segura para los atacantes, ya que las cuentas básicas para servicios como OneDrive son gratuitas".

Symantec dijo que recientemente detectó el uso de la API de Microsoft Graph contra una organización anónima en Ucrania, que implicó el despliegue de un malware previamente no documentado llamado BirdyClient (también conocido como OneDriveBirdyClient).

Un archivo DLL con el nombre "vxdiff.dll", que es lo mismo que un DLL legítimo asociado con una aplicación llamada Apoint ("apoint.exe"), está diseñado para conectarse a la API de Microsoft Graph y usar OneDrive como servidor C&C, para cargar y descargar archivos desde él.

Actualmente se desconoce el método de distribución exacto del archivo DLL y si implica la carga lateral de DLL. Tampoco hay claridad sobre quiénes son los actores de la amenaza o cuáles son sus objetivos finales.

3. RECOMENDACIONES:

- Habilitar la protección de red para evitar que las aplicaciones o los usuarios accedan a dominios maliciosos y otro contenido malicioso en Internet.
- Activar la protección de aplicaciones potencialmente no deseadas (PUA) en modo de bloqueo.
- Habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.

Fuente de Información:	• hxxps://thehackernews.com/2024/05/hackers-increasingly-abusing-microsoft.html • hxxps://ujjina.com/microsoft-graph-se-esta-convirtiendo-en-un-objetivo-popular-para-los-piratas-informaticos/

Índice alfabético