	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°172	**Fecha: 21-07-2023**
		Página: 15 de 53

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los piratas informáticos utilizan el señuelo “chatgpt5” para engañar a los usuarios para que descarguen malware		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

El 19 de julio del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha tomado conocimiento de Los piratas informáticos utilizan "chatgpt5 [.]zip" para engañar a los usuarios para que descarguen malware.

2. DETALLES:

El phishing sigue siendo una grave amenaza para la ciberseguridad, ya que engaña a los empleados con enlaces maliciosos hábilmente disfrazados y archivos adjuntos de malware, lo que puede causar problemas en toda la empresa durante más de una década. Los actores de amenazas emplean nombres creativos para disfrazar los ataques de phishing, con un nuevo TLD '.ZIP' que presenta una amenaza potencial por chatgpt5 que conduce a sitios maliciosos.

Los investigadores de seguridad cibernética reconocen los riesgos de seguridad del TLD '.ZIP', pero las personas responsables están trabajando activamente para mitigar el abuso de dichos nombres de dominio. pero sorprendentemente, contiene un mensaje de texto neutral en lugar de malware, Para engañar a los usuarios afirmando proteger a los estudiantes del malware, los actores de la amenaza registraron "asignación[.]zip" el 15 de mayo, redirigiendo a los visitantes a la descarga de un archivo ZIP que contiene archivos que son completamente seguros.

Los actores de amenazas aprovechan los caracteres IDN especiales para crear enlaces cuidadosamente disfrazados dentro de correos electrónicos falsos, dirigiendo a los usuarios a dominios .ZIP maliciosos. Si bien aún no se ha determinado el uso de IDN en los TLD .ZIP y .MOV, a diferencia de .COM y .ORG. La parte de autoridad, [infousuario@dominio: número de puerto], incluye campos opcionales como nombre de usuario y contraseña. Sin embargo, algunas partes se pueden omitir según los protocolos, y los sitios web de autenticación básica requieren información del usuario, mientras que otros pueden ignorarla.

3. RECOMENDACIONES:

- Tener bloqueado los dominios .zip a través del firewall y los servicios de filtrado web.
- Mejorar la protección con extensiones de seguridad del navegador y filtros web.
- Asegurarse de mejorar la seguridad con el filtrado de correo electrónico avanzado para evitar correos electrónicos sospechosos que contengan enlaces.
- Tener todo el software, incluidos los antivirus, los navegadores web y los sistemas operativos, esté actualizado.
- Promover la concientización de los usuarios y cierre las brechas de conocimiento a través de simulaciones regulares de phishing y ejercicios de capacitación.

Fuente de Información:	• hxxps://gbhackers.com/hackers-chatgpt5-zip