	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 108	**Fecha: 09-05-2023**
		Página 8 de 22

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Los piratas informáticos utilizan WinRAR como arma cibernética para realizar ataques cibernéticos destructivos.		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

ANTECEDENTES:

El 05 de mayo del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se tomó conocimiento que, los piratas informáticos utilizan WinRAR como arma cibernética para realizar ataques cibernéticos destructivos.

DETALLES:

CERT-UA (Equipo de Respuesta a Emergencias Informáticas del Gobierno de Ucrania) informó recientemente que las redes estatales ucranianas sufrieron un ataque cibernético atribuido al notorio grupo de piratería 'Sandworm' de Rusia.

Al obtener acceso no autorizado a la red objetivo, los perpetradores utilizaron scripts especializados que eliminaron datos críticos en los sistemas Windows y Linux. Su método elegido fue el programa de archivo WinRar, que fue explotado para llevar a cabo los devastadores ataques.

El grupo de piratas informáticos Sandworm empleó un script BAT llamado 'RoarBat' para realizar operaciones maliciosas en dispositivos Windows. Este script fue diseñado para escanear varios discos y directorios específicos, buscando tipos de archivos específicos como: doc, docx, rtf, txt, xls, xlsx, ppt, pptx, vsd, vsdx, pdf, png, jpeg, jpg, zip, rar, 7z, mp4, SQL, PHP, vbk, vib, vrb, p7s, sys, DLL, exe, bin, dat.

Los atacantes emplearon una táctica específica al utilizar WinRar, utilizando la opción de línea de comandos "-df". Esta función elimina automáticamente los archivos a medida que se archivan, lo que permite a los perpetradores destruir datos críticos con facilidad y sistemáticamente.

RECOMENDACIONES:

- No ingresar a enlaces ni páginas web de dudosa procedencia.
- No instalar apps inseguras o de dudosa procedencia.
- Tener instalado un antivirus con protección antimalware.
- Tener WinRAR con licencia.

Fuentes de información	▪ hxxps://gbhackers.com/hackers-winrar-cyberweapon/