Agosto 23 de 2023

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing – T1566
Malware detectado:	trojan.cryp
TLP:	**BLANCO**

El CSIRT Académico UNAD informa acerca de un asunto de ciberseguridad que ha sido identificado y abordado por este Equipo. Se ha detectado un evento de phishing. Es preciso indicar que la técnica de Phishing es un tipo de ataque informático en el cual los adversarios intentan engañar a los usuarios para que se revele información confidencial, como contraseñas, números de tarjetas de crédito o información personal.

Se ha realizado la respectiva indagación y se han identificado una serie de indicadores de compromiso (IoCs) asociados con este asunto.

Indicadores de compromiso del archivo adjunto

Nombre del Archivo:	IMAGENES_FOTO_MULTAS-PNG (Archivo .rar) INFORMACION DETALLADA SIMIT IMAGENES FOTO COMPARENDOS #2023-6662-9956-PNG.vbs (Archivo que se encuentra al interior del rar)
Veredicto:	**Actividad maliciosa**
Fecha del análisis:	Agosto 23 de 2023 - Hora 12:12:58
MIME:	text/plain
Información del archivo:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF line terminators
MD5:	C151A88935F7050C43D29C9CF9DD30FF
SHA1:	FCC475CB628A6FFD42F8B27E4DA8F43B6F18383F
SHA256:	2CFA617322BF08D1C0E7F988C6E532DED2DEF6509EA79063962D555CA035984F
SSDEEP:	6144:kqf8YQUi4+4rGsAH7rN4nSZ1NhhFhi1hRhLT9hyhOlOwlXg1tdzvkdVhiygeAvnK:kqf8YQUi4+4rGsAH7rN4nSZ1NhhFhi14

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Procesos relacionados
"C:\Windows\System32\WScript.exe" "C:\Users\admin\AppData\Local\Temp\INFORMACION DETALLADA SIMIT IMAGENES FOTO COMPARENDOS #2023-6662-9956-PNG.vbs	C:\Windows\System32\wscript.exe	• explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD
Correo electrónico: csirt@unad.edu.co
(+57 1) 344 37 00 Ext. 1042516

Firmado por: Luis Fernando Zambrano Hernandez
Cargo: Director
Unidad: CSIRT ACADEMICO UNAD
Correo: luis.zambrano@unad.edu.co

Firmado digitalmente : 2023-08-23 14:48:28