Agosto 15 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.msil/androm
Cuenta de correo del remitente:	secretariaplaneacion@granada-meta.gov.co
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	


---------- Forwarded message ---------
De: **Secretaria de Planeación** <secretariaplaneacion@granada-meta.gov.co>
Date: jue, 15 ago 2024 a la(s) 10:11 a.m.
Subject: Información sobre Proceso de Control y Vigilancia
To:

Comunicado Oficial

La República de Colombia, a través de la Contraloría General de la República (CGR), ha decidido iniciar un seguimiento permanente en virtud de las disposiciones establecidas en la Constitución Política y en diversas resoluciones aplicables. Esta medida se enmarca en el ejercicio de las facultades de control y vigilancia sobre la gestión.

Es esencial que las partes involucradas en este proceso reciban la notificación correspondiente sobre su vinculación al mismo. La CGR, en su función de garantizar la transparencia y la correcta utilización de los recursos públicos o privados, llevará a cabo el seguimiento detallado pertinente.

Se insta a los interesados a estar atentos a las notificaciones que se emitan y a colaborar plenamente en el proceso de revisión y análisis que se llevará a cabo. Para cualquier consulta adicional o para obtener más información, los afectados pueden comunicarse con la Delegación Intersectorial a través de los canales oficiales establecidos. Consultar con radicado: 3465708457

Atentamente,

YENCY LORENA CABANZO SANCHEZ
Secretaria
Contraloría General de la República
República de Colombia

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 dirigido a miembros de nuestra comunidad. Es preciso indicar que la técnica de Phishing es un tipo de ataque cibernético 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:	DOCUMENTOS ANEXADOS POR ENTE REGULADOR EXPLO 129461946815718645718465786457846587219486759312435.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Agosto 15, 2024 at 11:36:54
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

MD5:	E7A5C6AFF6F821503A9680AD9FD80E64
SHA1:	A9A13CD3416686EE337D23C36D41713EAB15978E
SHA256:	9864ADFDF839D6EBC68EDB6C128F0E5B6EE54DD82283723BB6276ED24176F065
SSDEEP:	49152:bG7/ri3ZW/n4Ktr3PkOugCz3gKIL+QtTMvEmTGLUFIGloMRLZIIGgWZh70rrXcms:buO3ZxK117Cz3gx+KIXTGLUlxRLZIXgU

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\DOCUMENTOS ANEXADOS POR ENTE REGULADOR EXPLO 1294619468157186457184657864578465 87219486759312435.exe"	"C:\Users\admin\AppData\Local\Temp\DOCUMENTOS ANEXADOS POR ENTE REGULADOR EXPLO 1294619468157186457184657864578465 87219486759312435.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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