Mayo 27 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Técnica Mitre:	Phishing
Malware detectado:	trojan.remcos/ratx
Cuenta de correo del remitente:	subgerencia@rytabogados.com
TLP:	**BLANCO**
Registro grafico relacionado con el Phishing	

Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

JUZGADO 11 DE PEQUEÑAS CAUSAS Y COMPETENCIA MÚLTIPLE

Mayo 27 de 2024.
Oficio No. 00808.

Cordial saludo,

Mediante la presente, me permito remitir auto que admite acción de tutela, escrito de tutela y anexos, que se podrán visualizar en el siguiente documento adjunto. Lo anterior para su notificación, conocimiento y competencia.

11001418901120240187100
Clave de Ingreso: 8411

Agradezco su atención y solicito confirmar recibido.

Atentamente,

Nidia Airline Rodriguez Piñeros
Secretaria
Juzgado Once (11) de Pequeñas Causas y Competencia Múltiples
Correo electrónico: j11pqccmbta@cendoj.ramajudicial.gov.co

1 archivo adjunto · Analizado por Gmail

Ofx00808 TUTE R...

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:	Ofx00808 TUTE RAD11001418901120240187100.exe
Veredicto:	**Actividad sospechosa**
Fecha del análisis:	Mayo 27, 2024 at 17:10:20
MIME:	application/x-dosexec
Información del archivo:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	BC6FCF5D363403C9F75E828D68B87CA7

SHA1:	E8ECBF12FA0E51EE400DE069C791708BD95061B6
SHA256:	8A252E03D74753F00DEB6E3505E3FDC528CB04C140E35AFDAE2CE23550EF1F61
SSDEEP:	98304:R5hkHOOaapCcYxnSkTM+qnKK+tPliFaJHY0GK67:pgAZG5

Fuente. CSIRT Académico UNAD

Información de proceso

CMD	Ruta Comprometida	Proceso Padre
"C:\Users\admin\AppData\Local\Temp\Ofx0080 8 TUTE RAD110014189011202401871 00.exe"	"C:\Users\admin\AppData\Local\Temp\Ofx0080 8 TUTE RAD110014189011202401871 00.exe"	explorer.exe

Fuente. CSIRT Académico UNAD

Cordialmente

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