Boletín de Ciberseguridad

Mayo 27 de 2024

COMUNICADO DE INDICADORES DE COMPROMISO DE TÉCNICA DE ATAQUE DE PHISHING

Malware detectado: Cuenta de correo del remitente: Subgerencia@rytabogados.com BLANCO Registro grafico relacionado con el Phishing IUZGADO 11 DE PEQUEÑAS CAUSAS Y COMPETENCIA MÚLTIPLE Office lie 0.0008. Cordel saludo, Mediante la presente, me permito remitr auto que admite acción de tutela, escrito de tudela y anexos, que se podrán visualizar en el siguiente documento adjunto. Lo anterior para su notificación, conocemento y competencia. CINSA 1800-11202-04-112100 Citave de logrese 6411 Agradezco su atención y solicito confirmar recibido. Alteritamente, INdia Airline Rodriguez Piñerros Secretaria Juzgado Orote (11) de Pequeñas Causas y Competencia Múltiples Corres adectivos: (Indicación confirmar recibido). 1 archivo adjunto- Analizado por Gmail ()	Técnica Mitre:	Phishing			
Registro grafico relacionado con el Phishing (I) Exception de la placuare Propular de Colombia I) DIZGADO 11 DE PEQUEÑAS CAUSAS Y COMPETENCIA MÚLTIPLE Mayo 27 de 2024. Oficio No. 00808. Cordial salvido, 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. T:11001418801120240187100 Clave de higreso: 8411 Agradezco su atención y solicito confirmar recibido. Atentamente, Midia Airline Rodriguez Piñeros Secretaria Juzgado Once (11) de Pequeñas Causas y Competencia Múltiples Curreo electrónico: 110pccmitat@icentoji ramakuficati gouzo	Malware detectado:	trojan.remcos/ratx			
Registro grafico relacionado con el Phishing Examplescia de de la picicione Experimento per entre entre 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. Experimento per entre entre entre entre 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. Experimento per entre en	Cuenta de correo del remitente:	subgerencia@rytabogados.com			
IUZGADO 11 DE PEQUEÑAS CAUSAS Y COMPETENCIA MÚLTIPLE Mayo 27 de 2024. Oficio No. 00809. Cordal 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. 111001418891120240187100 Citave de higreso: 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: [Illoscembla@cendou ambudicast opuzos	TLP:	BLANCO			
IUZGADO 11 DE PEQUEÑAS CAUSAS Y COMPETENCIA MÚLTIPLE Mayo 27 de 2024. Oficio No. 08080. Cordial saludo, Mediante la presente, me permão 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. E11001418891120240187100 Clave de higreso. 2411 Agradezco su atención y solicito confirmar recibido. Atentamente, Nidia Airline Rodriguez Piñeros Saccretaria Juzgado Otno (11) de Pequeñas Causas y Competencia Múltiples Correo electrónico: [I1050cméta@csendo i amabudicati gou co	Registro grafico relacionado con el Phishing				
Mayo 27 de 2024. Oficio lo 06008. Cordal 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. C111001418801120240187100 Clave de higiraci. 8411 Agradezco su atención y solicito confirmar recibido. Atentamente, Ilidia Afritine Rodriguez Piñeros Secretaria Jurgado Onco (11) de Pequeñas Causas y Competencia Mútiples Correo electrónico. Itopocretata@cendo ramabudical (psv. co	Companies Compan				
Mayo 27 de 2024. Oncio lo 0.00080. 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. C111001418901120240187109 Citave de lagreso: 8411 Agradezco su atención y solicito confirmar recibido. Atentamente, Midia Atrine Rodriguez Piñeros Secretaria Juzgado Once (11) de Pequeñas Causas y Competencia Mútiples Correo electrónico: Impocretata@cerdo/uramayaficali.jouz.co					
Cordal 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. C111001418901120249187109 Citave de lagresc. 8411 Agradezco su atención y solicito confirmar recibido. Atentamente, Nidia Atriine Rodriguez Piñeros Secretaria Juzgado Once (11) de Pequeñas Causas y Competencia Múltiples Correo electrónico: Impocrimita@cardio/ramasaficial.jouz.co	Mayo 27 de 2024.				
competencia. "11001418801120240187100 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: 1 poccmita@cendoi ramayarichal gour co					
Clave de Ingreso: 8411 Agradezco su atención y solicito confirmar recibido. Atentamente, Nidia Airline Rodríguez Piñeros Socretaria Juzgado Once (11) de Pequeñas Causas y Competencia Múltiples Correo electrónico: (11000cmittat@cendo) ramabudicat. (pvz.co					
Atentamente, Nidia Airline Rodriguez Piñeros Secretaria Juzgado Once (11) de Pequeñas Causas y Competencia Múltiples Correo electrónico: <u>J11poccmbta@cendo/ramsixdicial.pov.co</u>					
Nidia Airline Rodriguez Piñeros Secretaria Juzgado Once (11) de Pequeñas Causas y Competencia Múltiples Correo electrónico: <u>Il1pocombta@cendoj.ramajudicial.pov.co</u>	Agradezco su atención y solicito confirmar recibido.				
Secretaria Juzgado Once (11) de Pequeñas Causas y Competencia Mútiples Correo electrónico: <u>Il Topocrabta@cendo i ramavidicial gov.co</u>					
Correo electrónico: (1100ccmbla@cendo).rama);dicial.gov.co	Secretaria				
1 archivo adjunto- Analizado por Gmail ①					
	1 archivo adjunto- Analizado por Gmail (i)				
■ Ofx00808 TUTE R 4					

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

Boletín de Ciberseguridad

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	"C:\Users\admin\AppData\Local\Temp\Ofx0080	explorer.exe
8 TUTE RAD11001418901120240187100.exe"	8 TUTE RAD11001418901120240187100.exe"	

Fuente. CSIRT Académico UNAD

Cordialmente

CSIRT Académico UNAD

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