Alerta de Seguridad Informática (2CMV-00017-002)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 09 de Julio de 2019 | Última revisión 10 de Julio de 2019

Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), con la colaboración del Departamento TI del Servicio Nacional de Aduanas, ha identificado dos campañas de Phishing con Malware asociado, a través de un correo electrónico que supuestamente proviene del Servicio de Impuesto Internos.

Los delincuentes buscan engañar a los usuarios insinuando en el título del correo que se trataría de un segundo aviso, lo que haría presumir al usuario que habría un correo anterior que no leyó, por lo que genera un incentivo para revisar el contenido de esta supuesta cadena de correos.

El contenido del mensaje advierte a los usuarios que, para evitar una sanción económica que podría ascender a 100 UTM, deben descargar un supuesto documento de restitución de la declaración.

El otro correo indica que el usuario tiene una deuda pendiente y debe descargar el detalle a través de un enlace. Al seleccionar dicho enlace, se desencadena la descarga de archivos maliciosos, que tienen la capacidad de recopilar información sin el consentimiento del usuario, dejando además, puertas traseras con la posibilidad de infectar con otros malware según sea el propositito del atacante.

Indicadores de compromisos

Url's:

http[:]//descargadoc[.]com/downs/?DescargarFactura9123812839457
http[:]//descargadoc[.]com/downs/?Descargar=sii
http[:]//int.vhagy[.]sk//hagy/sites/descargas/Doc_Win974195209[.]zip
http[:]//m.berel[.]com[.]mx/themes/y241/y241[.]btc
https[:]//download650[.]mediafire[.]com/8mc2e8fcrimg/tkpdgrftruloyqy/Doc-98t78976e78[.]zip
https[:]//www[.]mediafire[.]com/file/tkpdgrftruloyqy/Doc-98t78976e78[.]zip
http[:]//pastebin[.]com/raw/zimNpaQV
http[:]//www[.]camereco[.]com/wp-content/uploads/2019/05/impuestos[.]exe
http[:]//www[.]worldtravellab[.]com/sh/?
https[:]//rebrand[.]ly/siisea62bd
http[:]//165[.]22[.]54[.]19/extrye

Smtp Host

mail2.censi.com.br [177.101.124.66]
pau.com [45.12.213.223]
pau.com [45.12.213.222]
pau.com [45.12.213.224]
pau.com [45.12.213.225]
pau.com [45.12.213.226]
pau.com [45.12.213.228]
mau.com [45.12.213.57]
mau.com [45.12.213.213]
mau.com [45.12.213.214]
mau.com [45.12.213.215]
mau.com [45.12.213.216]
mau.com [45.12.213.217]
mau.com [85.209.90.172]
mau.com [85.209.90.221]
butterfly.birch.relay.mailchannels.net [23.83.209.27]

zomro.com [212.86.115.72]
zomro.com [212.86.102.56]
zomro.com [212.86.114.189]
zomro.com [212.86.108.135]
zomro.com [212.86.114.24]
zomro.com [212.86.115.237]
zomro.com [212.86.108.133]
vds.com [185.224.133.23]
vds.com [185.224.135.16]
vds.com [185.231.68.198]
vds.com [185.224.135.143]
vds.com [185.224.134.127]
vds.com [185.219.83.87]
vds.com [185.224.134.225]
gmhost.ua [185.86.76.145]
gmhost.ua [194.9.70.202]
gmhost.ua [194.9.70.188]
gmhost.ua [194.9.70.186]
gmhost.ua [194.9.70.179]
gmhost.ua [185.86.76.99]
dcmmail.dcmcable.com [204.10.176.14]
mcegress-14-lw-3.correio.biz [191.252.14.3]
cp201.zonasprivadasdns.com [185.50.196.201]
srvmx.alsol.com.br [177.39.175.13]
dcmmail.dcmcable.com [204.10.176.14]
smtp2.sinos.net [200.160.158.222]
ns1.ncarsmagazine.com [203.146.117.233]
win-tudmcb4hq4t.sahel.mrsservers.com [85.185.93.86]
pablito.fap.com.br [189.85.146.141]
mail2.censi.com.br [177.101.124.66]
cockroach.oak.relay.mailchannels.ne [t23.83.215.37]
smtp-sp201-189.kinghost.net [177.185.201.189]
smtp-sp203-146.hospedagem.net [177.185.203.146]

mail.wla.hu [84.21.0.3]
cp201.zonasprivadasdns.com [185.50.196.201]
mail.br.inter.net [187.191.127.28]

From: (Original)

edrred@otowhomes.com
elaine@acodisa.com.br
admin@bulevaraltamira.es
pmcr@alsol.com.br
jorgemachado@sinos.net
info@incarsmagazine.com
info@multimaxiran.com
sales@medresty.com
info@mojemobile.ir
info@jonnys-club.com
info@solvepark.com
fabio@fap.com.br
rafael@mail.censi.com.br
cibele@nsncontabil.com.br
simone.castillo@grandhouse.com.br
andrechacrinha@jpaobras.com.br
info@caribecar.hu
souzamarques@br.inter.net
root@w.net
comercial@maispb.com.br
root@zomro.com
root@vds.com
root@gmhost.ua
root@coocnungasl.duckdns.org
root@g0g0tego.duckdns.org
root@g00g00tico.duckdns.org

root@ibramorrer.duckdns.org
root@gugutico.duckdns.org
root@dukidki.duckdns.org
root@bababbebebe.duckdns.org
root@l0wduckdnscom5.blazingfast.io
root@vds.com

Subject:

Deuda Pendiente SII
Segundo Aviso (SII)

Archivos adjuntos

Archivo : Doc_Win974195209.ZIP
MD5 : ff73fb2fb293ed4c20c06b492724789a
SHA-256 : 280a31fc539d1cc4eb5a55f45a7e04da691754f401e1ccc90b5b698406a8f53e

Archivo : Doc_Win974195209.cmd
MD5 : 371039d3ab4695cf8f62b2e3d0107434
SHA-256 : 56293ea1b1471d23a13a1332579371f66d8ff7383bdcb8f05b04837e6ec892fc

Archivo : Ny5bv0oKZe.vbs
MD5 : c23dfb7202f8d3905f35ea3cbe06e13f
SHA-256 : 7e18479bca7f6c52042ca34a9befd8d5a6ecfa8b08f067a3b580a9f02330fa3c

Archivo : y241.btc.txt (zip)
MD5 : 0ce5a9b69840578b1d6c28ad2729e4f5
SHA-256 : c7e2d10122f89564763aa6d89ded42a1d7f30af6d19812743c088792362c74ba

Archivo : I6OCRG29MMJEHTS48HUCV8CIAE6QKFO
MD5 : 2360bbaedc4fa6cee6dab7969b3f2397
SHA-256 : bff312cbeff061a95862f9b4060566ca0e6cd38b04bbf510b18b148877d71312

Archivo : T4D210QRHE9HIXURZ1DK3LU24RY4KQL9LM
MD5 : 66a9e80e620da758ec1ae9ce11b8a41c

Archivo : RD99KQXPN6VFX85BRQYRDB7RCMO
MD5 : b06e67f9767e5023892d9698703ad098
SHA-256 : 8498900e57a490404e7ec4d8159bee29aed5852ae88bd484141780eaadb727bb

Archivo : DOC-98t7896e78.js
MD5 : 62b7141c83784ec1e794b9da4a9caea6
SHA-256 : d95d538362ffe639d472989ddf3a5efd0a6dc49a73ed5ad9cd20fbc1add261d0

Archivo : zimNpaQV.js
MD5 : 21906c511b5cbba53c26447730e5a337
SHA-256 : b3b0cc175ac92b2f785b83ee61f5f293506265248b3e2a21328ab0cebe61df1a

Archivo : impuestos.exe
MD5 : 349d6af6f1710decfcb42a6a6ce1c15e
SHA-256 : 1ce17200496c6ffbbfe6220fa147f7599edce5a4dfb27a0afe14e072ceca5eb6

Imagen

msg100@sii.cl

Segundo Aviso (SII)

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Home /

Estimado **Cliente,** Para evitar una sancion en su contra que puede ser una multa de hasta 100 UTM, le recomendamos:

Servicio de Impuestos Internos

DECLARACION MENSUAL Y PAGO SIMULTANEO DE IMPUESTOS FORMULARIO 29

FOLIO	07	6713478856	
RUT	03	6.628.643-6	
PERIODO	15	01 /2019	

01 Apellido Paterno o Razón Social	02 Apellido Materno	05 Nombres
DUBLAS	GUERRA	RAMON ERASMO

06 Calle	610 Nº	08 Comuna
AVDA. AZOLAS 2758		ARICA

09 Teléfono	55 Correo Electrónico	314 Rut del Representante

Código	Glosa	Valor
515	Nº FACT. COMPRAS REC. RET. TOT. E INICIO	9
110	CANT. DE DCTOS. BOLETAS	3
511	CRÉD. IVA POR DCTOS. ELECTRONICOS	839.549
519	CANT. DE DCTOS. FACT. RECIB. DEL GIRO	104
539	DEV. SOLIC. ART.3º,CRED. RECUP. Y REINT.	879.459
077	REMANENTE DE CRÉDITO FISC.	920.661
151	RET. TASAS DE 10 % SOBRE LAS RENT.	10.000
563	BASE IMPONIBLE	10.657.711
115	TASA PPM 1ra. CATEGORIA	10,60
039	IVA TOT RET. TERC.(TASA ART. 14)	817.782

Código	Glosa	Valor
587	MONTO NETO, FACT. DE COMP. RECIBIDAS	10.651.490
111	DÉBITOS / BOLETAS	1.182
538	TOTAL DÉBITOS	1.182
520	CRÉDITO REC. Y REINT./FACT. DEL GIRO	839.549
504	REMANENTE CREDITO MES ANTERIOR	961.753
537	TOTAL CRÉDITOS	921.843
089	IMP. DETERM. IVA DETERM.	0
062	PPM NETO DET.	1.129.717
595	SUB TOTAL IMP. DETERMINADO ANVERSO	1.139.717
547	TOTAL DETERMINADO	1.957.499
596	RETENCION CAMBIO DE SUJETO	817.782

TOTAL A PAGAR DENTRO DEL PLAZO LEGAL	91	1.957.499	+
Más IPC	92		+
Más Intereses y Multas	93		+
CONDONACION	795		-
TOTAL A PAGAR CON RECARGO	94		=

% Condonación	Número de la Resolución	Fecha de la Condonación

SERVICIO DE IMPUESTOS INTERNOS
RECIBIDA Y PAGADA POR INTERNET
www.sii.cl

Descargar restitución de declaración

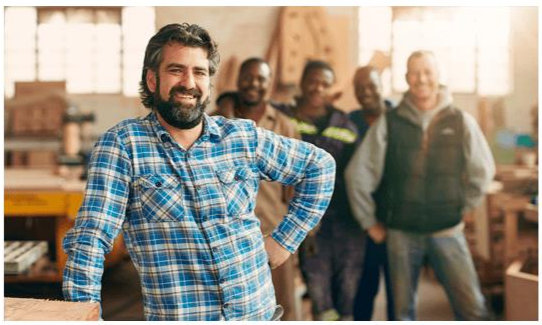
Gobierno **Transparente**

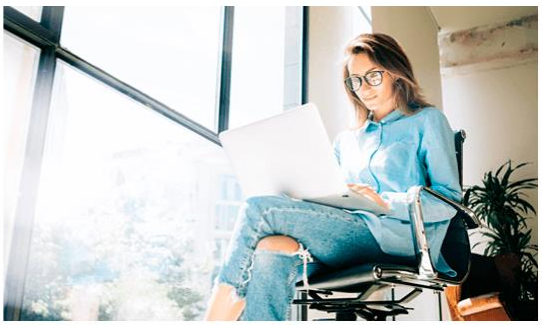
Servicio de Impuestos Internos <rafael@mail.censi.com.br> | abarrientos@interior.gov.cl

Deuda Pendiente SII

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Ingresar a Mi Sii





Sii Servicio de Impuestos Internos

/a

Estimado usuario

Usted tiene una deuda pendiente .
Descargue el detalle a continuacion.

Evitate molestias.

Descargar Detalle de su deuda..

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob