Alerta de seguridad cibernética	2CMV20-00081-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Septiembre de 2020
Última revisión	08 de Septiembre de 2020

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.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), comparte una serie de Indicadores de Compromiso (IoC) obtenidos del análisis realizado a múltiples campañas de phishing con archivos adjuntos que contienen malware, los que están circulando en el ciberespacio nacional y representan un riesgo para los sistemas informáticos, así como para los usuarios en general.

CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC hash

Hash SHA-256

019c37268b08ec8bdf64efc52f889ef1cc2e39d7fd45aa69fd2d22cb27e6b581
0d50239f78bb312fb2c0bea2628104db8e45fea2cb31208b18782b950e0befa1
15de7545c8d13285e5cb83c314b0f47ad6428d10169a8d82ab09ab7d7b16bef3
168b5da0b0b11a0bfb519c5efdce6d03fa2c2e576a7e7cdeffda1c09641f7556
1f5b6b69bba1de252b6f92057b798a07be36fc8cbf6f0425d9527e7729a2ab3d
2127c6d9a336fa4b6fc48dae6590bdf9604ad60d073aa74355949e5378f0270e
251a3ce3e3b69e991f5a1e8d1d10b493111e9e2215fb4e4dde32281778a056b9
25c4930127bd03f5272a817b8337b5f08f195807fd7cade11011599d2eee99b3
2da3cafc45a2fd98c91b3f1bea2a48e5dd01c09713454be8ef98e2d16d3af8e7
36337c45a233dbc9f106b4415584520ea6e50712417d9b1fdd7751d1cd5b8780
3768bc365b9b7d45afe4cb30adeda81e1a20fcea35de8ff0af38a226b65e52af
3ac12d0795612fc72b1a0a9e732d2effbf4d9c967be20dd2a76539cd75591529
3be6d0fac78c13868de42d0d8ebdc679fde81153ceff09df7cda34cd0dff9cf6
46037857291f877b0c4b8eee55a142aee04c2bd94c7545af5123e22985c3ffaf
4a9633ecae342b013bcc0c34fc1709600e70e90a43701c9f3218bf80916b6d43
4eb0be1c1604bdc56352f0550ced01ff198d7d1455b56b35ea8e16ef026e842c
4f696d59be410a76e8a6c89b400d7aa032d623c362454caccbf322bd400f0a73
565956a11acdd3a7c41d291dec85e0e394b70f0d7244497986482d778fdc012d
566d866fb7d9577cd92837143d13ee122a5a3a0ba3464d1e75a8f2d095309be7
599a861ba05b57347331fbb180078cc4074c60d71c1e24c6b1469d18f139c4e7
60016b594d0f144e6af1160157ac8185fa8de5b6c76e9e45ad71ce13adb9b15f
60ad914d6efd04baf8fbc5b0b6448042d688bc49352930fba4cc4c4370221d32
65565c13a250f72a089b0306c372d4bc3dc778c6ab9d1b1825e5d505e8c8e306
6b6ee7c3eebce87fbf093253a28ca90fb94e7c53134722d7c285b52dbf2f51c7
6d172d720cf3f98f6ba22e6a6b4e813f2c2300d8a30591b831d75ea628adacfb
70acca94041bb5834f3948f6ad9f87d4e0e9339c393774e4b9452af0b85ef537
71595cc89b180dbd13282860b351ca4fb2859e46b72a75126c3976ea16fa46f9
74ff45732723b71e80c075cab3d3a0c776234c8b0cddd41260691581365150ea
7c178f6f73eda5a5e0a4de819f092772ad4cb0ac2f6d996f7b9b072883b04bc0
83a608a684d531170d1d962a923ec80ff882ad17ac5a24ce4477d634e575c74e
8a4c384c2f0e89b7a1561aae298715c3981e9ade62e7d41b4acf6f6138af0caf
95e06de334578875b8a103e5ceb5befc765c081e75bf39907b2c8f910b8b1eb3
9e0b617d1f1079cb339de903f320274b428c1e8723580e2152f8b5af88563c20

a32e3083bd066fd21f716cbb3063fd0daf6cc2644c4ff7630d831f06f7eb6553
a4742aa9bc3444d4d3406dd0006e62ccbe08a89589e023fd842629208a3127f9
aded839540bb039ff325a997f2bb52dd495ca8aa6cf458e81d408fb942df6218
b8b883d714658e0a4974d4356dfebdb2e628ae3e7355d42a15ccc6034b01a0d4
d4abe10db55578ef5df589545e27e8e8a008f9a1744d8c6112b57215e4cd86da
d6d2ca7a33955eb437bd4f529e9768eab28715aa30332737f94151c223f9a851
ddb867fccaecd7085462b092e5dacff90d666301868981d35ce4cf6a994c4537
f380bc34e4d8bed89782b5d6d81c176586c2b34e95efefcb30687220d03e3485
f42309e5bfad3404989189b18254dd8157ec5f170544081a5dc8e4607fe364d1

IoC Descarga malware Urls

Urls que son disparadas por la infección inicial del malware, podrían existir otras ulrs no detectadas en este proceso.

hxxp://vermasiyaahi[.]com/wp-content/8/
hxxps://bauzeichnung[.]com/cgi-bin/8V/
hxxp://bobenstetter[.]net/cgi-bin/V/
hxxps://bosonit[.]com/wp-includes/We/
hxxp://chinese-photography[.]net/books/T7/
hxxp://compartirwifi[.]com/WordPress_01/ZAa/
hxxp://asn-espirulina[.]com/wp-admin/6hU/
hxxp://accemarbeyal[.]com/wp-includes/meR/
hxxp://somosdrucken[.]com/upload/Wvv/
hxxp://ballatstone[.]com/ballatstone[.]com/Dy0/
hxxp://marmi[.]seoper[.]beget[.]tech/fonts/Aoa/
hxxps://aselsa[.]com/wp-includes/0T/

IoC nombre de archivo

Nombres de Archivos con Malware

16685e152bab6f30df.js
2020lk0907.7z
406_03_2020_79_514790.doc
Adjunto_7-8797.doc
ARG 101.56-0.06 gauge.zip
best-graffiti-alphabets-letters.html
Cotización.r00
DOC_668993-07092023002375.doc

DOCUMENTO_DE_ENVÍO_Y_LISTA_DE_EMBALAJE.pdf.lzh
ejemplo-de-estado-de-resultados-en-excel.html
file 0209 092020.doc
FILE_2020_62-983408.doc
G5129_092020_2_39960637.doc
INFO 092020.doc
INGE2021APR1107.XLSX

UHMW-PE, NATURAL, 0.5 X 48 X 96 SHEET.gz
VEH_500344562865_FGRS.57.pdf

INGE2021APR11078.tar
INQUIRY.zip
jquery.js
letter of intent.pdf.gz
New order.zip
Original BL, Invoice & Packing List.html
PAYMENT.iso
PO_2020_00944.zip
Proforma Invoice Letter 084654332443_pdf.gz
Quotation.doc
recibo de pago..zip
recibo_13980.zip
RFQ#100409072020.gz
RFQ.doc
SOA.iso
Solicitud de presupuesto 09-07-2020_pdf.rar
SWIFT COPY.zip
YOUR-FAVICON-URL

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

23.106.122.108	159.148.73.55
103.125.191.128	199.40.206.35
103.125.191.208	199.40.206.35
103.133.108.114	212.114.52.195
103.141.138.124	37.48.85.220
195.200.252.120	38.64.1.164
201.163.211.245	45.137.22.133
103.150.8.29	45.137.22.158
103.254.13.91	45.137.22.76
103.53.172.9	45.147.228.64
139.138.58.70	95.211.208.25

IoC Correo Electronico

Correo electrónico de donde fue enviado

umjhy@hpmm.com.ar	kajiriart@gmail.com
accounts@pinkmondo.com	Kelvin.Tan@fendercare.com
admin@uchile.cl	krfijc@libreriapaniagua.com.ar
craiggoodman@greatplainsfire.com	maheshwariviresh87@gmail.com
dien.nd@nsets.com.vn	MBagnara@freshdelmonte.com
facturacion@ddsm.mx	nfe@sigmametais.com.br
gguzman@tratausa.com	noliktava@zdkrava.lv
heeyoung.youn@kuehne-nagel.com	odds.f12@gmail.com
info@antaisolar.com	ovy.kurnia14@pgascom.co.id
info@teyseergroup.com	purchase@cenerg.in
info@zzcontrols.com	recibos@cafsa.com
ipm@ipm-korea.co.kr	sales.dhl@bitisgroup.vn
spam@bfs.barracudanetworks.com	Sales@Lisungroup.com
stanko@green.net.ua	sales@yingdapc.com
tec.deckel@globalpack.com.br	twokings992@gmail.com
umjhy@hpmm.com.ar	unitedstatecustom@gmail.com

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- 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.
- Visualizar los sitios web que se ingresen sean los oficiales.