Alerta de seguridad cibernética	2CMV20-00087-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Septiembre de 2020
Última revisión	19 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

007235d5a7194d94f5ea60ef1b957c3cee5c1d97918ef115e77b1d4b1836577a
030e0ee7107ff862978624e9ceec877986b12f5b259b24783a39f427434c91b3
03caf29484a047db9c68e15e6117f665c59b1cc6ea7cdacba9042f80149861b9
0500d9340ad3906abd3b1e971f21832f7e71b62f0f47ca9e6043f07d29c29bd8
073ee65dff4751d1ee820522c15601890a54bb94c0ce8fdb89ac2aafe4e70aff
07d057a61d3df77ff64c6e81ebfa3e05ac6fb288ec8104f7b215032445fcd4cb
0946fbe35bf360b6bbf9c6f32f0ad0e3630135daf698b64158c3a8a3d5dcf192
0a18fed225d22e39aff79199651d91a2206b781439ad8017da76ce668ec88095
0a30c4b942b9c613a9c5df445b932e1468358cbd04d1ecd613fd547da4ec84ed
0f01b7b50e1a0dc6b2330e0b7fcee6338ee666328dc8ce31efccce16391db8da
12184c3b864ed546a8c1c0b94d18631228a2cd6caa38e1d6c332c113d327f21b
1bf95dd5920c9ab0b519c10b39e7de04eff938ea86f834885f202a0cec87d4bf
1d188489aa0c86820ef03aef6d4c6737367a5872ca87080c9fb14670099d756d
1e68ebd904cacf30d35734935dc212a7484e063e1a3519783249d890572a19ec
22f5f6c960c4008f562bf7d34f803b15610e0542c351a24a43d90c7d86a63df0
25c51061c2d3618e6fe43b51487ff7abad46d648b8d3b9661d757ab481a3a4f4
2d22cb6bb2684459c707f30b23c49d03c4077803ebd1e4256c071f8d365ada55
2e08d4af746ba90b49a8af24bca94ae3e15bbbe98b5550b32046ef49208ba1bb
3794f324eaaa25b46f1e7f2d4c169c9839efa90483f52fd6816bd621f0984562
38e7fa7dcfa64e6daecea109f43d9c5cc104cf0bc66873449b03ebe6eb6df03a
3d2475f1f03f476fecd00aa205c7ebb68b4f0e923250f5f095c597b19f394632
3e91e2dc00b6c65d2130de941da4c08808356d2a7f5de0ca3e32a11f25a6dade
4000d1ab30db6a5d94686c02f9a7e6e687231ff9bfd42bf56e3f9f1e8750ede2
4a48c8e60fbeb16b73dc2ea00d3e61fda7c88c0e0318e47b735bbefb20e93d98
4e500dc20300e081376f4f6951330ba0b37700ae0b23ac5662a2e96e2cd9a755
53fafa16b2ea840e72130c9fb45c5f43b99a594a2a86e318cff8650c032c3f10
54ac560845b09ce00a48b604ac7c440331cbde4362839a3dbf14c378230bee21
5cc754b56ea15b372576406cb73285d5c74e09ee434b62bb955e5c02caca6b68
5dcb34b82840165da4c8d3f693522093656d8731ab6ffade09c8f5d2b8376408
606c981a35630090fe7df6ea2bd78be7c01eb20f5d266ba2432b209e9bf26eb8
653398829c8ce1b2f6338277718cbbaa771e7028b8eb746b93f98753c9e4f474
6584db21f3b24953242d8d42e4ffa62e8026aebaea9f5c6b5cae066f4c279370
6f4056b5788309662db3fedc3a283374030d298d547719366521b1e1cf795be6

756815a0ad541c35d83925a96176c045f44ee3c61a1fb8641e14d6d7207c09c2
7584f6b7aedc7718d3df27ea387d19d0965e245dd1badd45a9f84bfe656fc7bc
7eef2ee6f6deaaa0411c93b5166573c267696a97acc6fe67cd10c7c1d49c8103
84015141ee67fd7d83bb8c912c6b0b32a1caf9d27e65b62d47494985973d0c45
897cbd1c3f685c12be9696f69d948ee8bbb076934b0c0f13e3ba293b935907dd
8a3a2eecd83a01a3a12933b730e8ef7c752c7bbee0818f77940551ba926cf847
906eb841dd00ed7c09bdb5dc7c0d3722f6313536e45201301a2db07d0fe04bea
923692821eb7f6837085e7bef93e95d87c7d841697e21fa1730ee5d217312f14
92c3884fbaf42eed1a9fe3e40b1d45e34f443dbf39226dc81b1a5d33541181c8
94035005c1b01a7ee5cdc000f6cc2128dd739606543d29bf12949670c34ad78c
94d5445a36c1741b9e7cf1a4a3d93f84511094b007a15afa0da3f586cf405132
9baf95e19acd9646921f0e0a86c78f2621f34bc485c4ca59c97e15cf200f403a
a4a33971129c80d8e4a6f163b6df265fc6ef694b64a1b973114dafa6af5da736
a8fbe20181a901e4ee77e91e558cb97c24abdf0654a81d254124fc9dbcfce07a
aa61215227bbb2fc0c03a6494d4fe362360dcf90d7e78c8a2ec14936833a827d
b709505d72068d9b8b222a2b52a8178f0b8fc95b0256124c72f2fbcdea4dc417
bccc6031b088f432a5b9d9303eceeb6d9ba9da4ec4f85997f393f67e2d552819
c0ccd8b4db157fc157f57b6b29b037d0a5f34e83c399a372b0a58e3495bcc49e
c536931bec7f39621f1f86cd9b7b49ba58e35ba7a7f6ce7b92724de491137e3d
d05dfb23daae9a5649bfb3524abe2e785019321bafdc50d9dc3bcc48b2aa17d0
d0b4b470d5e523a36a9751cec3eb8c5e1fae85904ab8637b745f1aebea3aa8cd
d30150c62052607c9dd68065e9bf07da7c7490bdc0be48077a770b13f28d77b3
d72ed0de937a76be853c584575728f2eb9cd72140deafb23f961c0c1ac7e8941
e373b51731dd9794dfbb3967839423a04999996ee921f1d3642d9fb53b0f107b
e4873536ba7b163dc9a87dd2dc7d447b502e63eaaebf88fcf4635d423772db47
ea3f4a83b149f5bf4590d75b36f3e23d864687e575245ed61200c8aa6c6db3af
fbb0768a54c96daabef7659e5ec321d26211a023027f8beb9b9b5bf49f36d583
fd925205136ce3b71945709fdfbbdda52ea8fd455f8e4e410f942ee48f893b76

IoC Descarga malware Urls

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

hxxps://vstbar[.]com/wp-admin/Hs/
hxxp://amettatravel[.]com/wp-admin/1/
hxxp://amyemitchell[.]com/themes/w/
hxxp://binarywebtechsolutions[.]com/mobile-website-designing-company-in-gurgaon/CLZ/
hxxp://blog[.]geekpai[.]top/rmebw/x/
hxxp://calledtochange[.]org/CalledtoChange/Uh/
hxxp://crewnecksusa[.]com/wp-content/NJ/
hxxp://cybersign-001-site5[.]gtempurl[.]com/2xwzq/bve/
hxxp://forestanalytics[.]net/images/57A7/
hxxp://freespiritmind[.]com/MASD/HowTo/css/J/
hxxp://geisterhouse[.]com/cgi-bin/LAb1/
hxxp://iqauthority[.]com/wp-admin/9Id/
hxxp://jiafunongye[.]com/application/zh3/
hxxp://jpwoodfordco[.]com/admin/sDs/
hxxp://justinscott[.]com[.]au/sites/rRS/
hxxp://luzzeri[.]com/wp-includes/o9G/
hxxp://matadebenfica[.]com/permanente/u/
hxxp://msmartyford[.]com/assets/BIO/
hxxp://oneinsix[.]com/test/0/
hxxp://paganwitch[.]com/wp-admin/CmubpSk/
hxxp://riandutra[.]com/img/wOMENgh/
hxxp://sasystemsuk[.]com/index_files/j9b/
hxxp://shahqutubuddin[.]org/U/
hxxp://strike3productions[.]com/squad/3aV6xrH/
hxxp://swiftlogisticseg[.]com/wp-admin/7/
hxxp://valleymedicalandsurgicalclinic[.]com/ujftb/p/
hxxp://vandamebuilders[.]com/wp-includes/OEyjc9x/
hxxp://votesteve[.]us/closed_zone/Bk/
hxxp://www[.]dougsuniverse[.]com/pics/yL8/
hxxp://www[.]ekramco[.]ir/english/fn/
hxxp://www[.]sifesro[.]com/wp-includes/o/
hxxp://zplusshopping[.]com/wp-content/plugins/8ek/
hxxps://case[.]gonukkad[.]com/sys-cache/fmC/
hxxps://cimsjr[.]com/hospital/x2f/
hxxps://datxanhmienbac[.]info/lfb8ii/LmG/
hxxps://dezurve[.]sa/webmail/installer/mqi/

hxxps://dramacool9[.]live/scbvq1/sPT/
hxxps://guhaasmart[.]com/wp-content/s/
hxxps://hapyc[.]com/wp-content/s/
hxxps://idilsoft[.]com/admin/B/
hxxps://janataralo[.]com/public_html/k/
hxxps://konican[.]com/cgi-bin/cWu/
hxxps://nilinkeji[.]com/online/Dmz/
hxxps://star-speed[.]vip/wp-admin/Ttv/
hxxps://treneg[.]com[.]br/rfvmbh/a/
hxxps://www[.]breedenandsilver[.]com/wp-content/j/
hxxps://www[.]cupgel[.]com/__MACOSX/3/
hxxps://zyccccccc[.]top/wp-content/lx3/

IoC nombre de archivo

Nombres de Archivos con Malware

7028-18-2020-N-2856.doc
835_77635.doc
9323370_2020_CE_45745.doc
Adjunto_092020_670519.doc
Adjunto_18_10-50591.doc
ALMECO S.p.A_Dimension1300-4800-480M.xls
AOBO MOULD QUOTATION -1752002.zip
ARCH 2020.doc
Arch_18_94-9274641.doc
ARCH-1809-4_2744299.doc
ARCH-B_15052.doc
Archivo-18-092020.doc
ARCHIVOFile_19_592-70074798.doc
ARCHIVOFile-18-33_9737694.doc
BWD-090120 QNU-091820.doc
Certs.iso
COVID-19 report 09 18 2020.doc
DAT 1909 78-5007.doc
DAT_092020_BF_53381370.doc
DAT-18343998.doc
DN-000886.doc
Documento_1809_7-455043.doc
F1971439 1809 092020 892_14359256.doc
Ffactura.html
File 2020_09_19 78174.doc
file U_2716047.doc
file-18-TON-87668540.doc
file-2020.doc
Form - Sep 18, 2020.doc
HW-3525 Medical report COVID-19.doc
Informacion 1909 DC-439661.doc
Inv_4657.doc
invoice #9049.doc
JF4256470594CQ.doc
MEK-090120 SPK-091820.doc
mensaje_092020.doc
mensaje_T_8817226.doc
ND2146947866AK.doc
NYD-090120 GLO-091820.doc
PMC Statement.gz
PO# 09182020.doc
PO# 09182020Ex.doc
PO#4507816340.htm
Products and specification Automotive Industry.rar

DT9977669463HR.doc
Vessels particulars.iso
VTF-090120 FIH-091820.doc
YI2336200009KR.doc
YN-3747 Medical report COVID-19.doc
PROFORMA INV98745654.PDF.jar
Proforma Invoice pdf.zip
RM9211983009NW.doc
Shipping_doc,INV+BL_copy.zip

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

65.254.253.158	210.2.153.132	185.222.57.195
67.205.166.180	210.245.23.20	186.202.7.105
74.220.201.250	212.39.90.96	186.202.7.17
74.220.223.244	217.61.130.193	186.64.116.167
98.142.235.184	217.61.130.193	190.6.77.242
139.162.211.168	217.61.130.193	191.252.30.23
184.168.200.140	45.137.22.45	192.185.179.26
190.107.176.215	50.31.134.17	193.107.29.98
193.169.253.177	54.240.8.16	201.140.166.4
198.178.121.238	61.20.35.131	201.140.166.4
202.191.119.101	61.20.35.22	203.183.80.2
207.180.249.200	62.149.156.66	209.59.191.1
103.27.207.142	65.254.253.24	210.196.193.64
125.99.252.7	65.254.253.44	69.64.34.152
138.68.62.81	65.254.253.54	69.89.18.232
148.251.27.44	65.254.253.61	69.89.22.3
153.153.62.100	65.254.253.86	69.89.30.159
161.47.110.149	65.254.253.90	70.40.201.62
161.97.65.142	65.254.254.66	72.52.197.97
161.97.65.142	67.209.127.72	74.220.194.83
173.233.83.158	67.222.45.165	74.220.222.55
185.22.144.142	67.222.45.220	80.80.228.81
185.22.144.142	67.222.49.151	95.128.74.33
95.128.74.33		

IoC Correo Electrónico

Correo electrónico de donde fue enviado

eghurtado@pgjebc.gob.mx
account@pg.co.th
admin@entel.ph
administracion@fescapsa.com
anderson.sauer@agrocat.com.br
andika@e.pthunga.com
antrepomersin@martasgroup.com
ariel@hondamegatama.com
arif.goncu@akcadag.com.tr
arm@arm-bg.net
atencionalcliente@autocolor.com.gt
audit@chase.pk
auxpessoal@escritorioalmeida.com.br
ayber@ayberteknik.com
bm.dps@saptasaritama.co.id
BNR@ciegolde.com
bodega.gye@romanliquors.com.ec
carlos.gutierrez@grupocobra.cl
celina_duque@coomeva.com.co
centro_caixa@assess.com.br
courses@philip-son.com
cs@asiainsurance.com.pk
danaminis@rotecautomation.lk
denkiya@clio.ne.jp
editor.jpps@rimedjournals.com
eghurtado@pgjebc.gob.mx
fernandez@interdominios.com
gdisalvo@transtecservices.com
haijia.huang@auscahk.com
hhuerta@glavima.cl
hr@thienhong.vn
info@biohermes.com
jose.opazo@transportesbermudez.cl
kamil@belgium-mep.com
kennith@ramencoa.cf
k-ishizawa@okhotsk.or.jp
laura.romeo@unsic.it
limoges.1187@jlrfrance.fr
livia@ferrovelhojacare.com.br
maftuhi@barata.com
marija.milic@delfi.rs
marine.opallah@kemsa.co.ke
matteo.cortiana@plast4labs.com
medicinaocupacional@vyt.com.pe
merchant@writexperts.com
nishchithh@bejealous.com
no-reply@dhl.com
rohit.kathuria@corpseed.com
rr-fey@rimsy.de
sales@rouletcompany.com
sales@tajurbangrains.com
Sally.rivas@balmoral.co.uk
savithri.da@cognitiondesigners.com
shinko-m@kyushu-shinko.co.jp
snoww@fireacoustic.com
solucoes@expressocanoas.com.br
spiedra@creohav.co.cu
s-satou@rose-bs.com
stian@nytrapp.no
tausif.raza@chase.pk
tsala.cornelie@anorcameroun.info
Vincenzo.Ripepi@meuencartedigital.com.br
wh.suprv.qtr@midasfurniture.com
yao02@gaspro.jp
zinhle@virlmicrofinance.co.zw
jsud@leadingecuador.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.