Alerta de seguridad cibernética	2CMV21-00163-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Marzo de 2021
Última revisión	06 de Marzo de 2021

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 de Gobierno), 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.

El CSIRT de Gobierno 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 de los archivos adjuntos en los correos electrónicos:

03f7a319c076292517b055d0344bab973d3386be13ca123f5962c267d6afb516
0929f70b8164f9ecc43e2ec56baef3e497a663042935428aafd95dea0a5c9c80
0af95bb33b10c1f830b92587e2145e9ae58b750074f7ece5f16ad6d44c96abc9
0fbb056128f13b0a290047c7b2edd81ff70a5a5108df588a2a031d6bcccc962b
120686ff12e1f3ef4b4e89e8d97a88b141b3611c4d5d7a04181fb00d3c67c8f9
192920e2a3dc8de4619016115322cbbc29ac89ed79d4ac331e1c29d2038c2746
196e9df7946e1d42d80158a7282520da72a737516c8575a179000d1962542ea0
1e4ffff7ac858c089c396daed605ac3a7910082dfc300195663611dbb114ecb6
1ef37249de16d48ff222d5b7d63846a9bb3a2ebff07e23241fc3d13e7341d2bf
24bb3c90eeafad2dca3d742ad0361e90a38a9cebec3238a24d9ddffad7ef45a6
253818f8e55b94a26996a7529583faf9b1d2beaf9953ac3e479e31bf55561f57
264c10ad620c793895f9bb5d31dc3911aff88790a8a8d7e59f0c5bf94226c0b9
2b6dcd2d9942fe47fd85547211d2822d36551610e8cbec24c1570e3c8bc826c3
2dd463937c35210eddced5f4be41e58fd1562a9be3f298693fa1333f75d05c92
2e50ab4de171b446fa9d69601142f27defec291c5cccfb55dc20557463c3f92c
31ec66e163e5ef9eabf672c13034d5561c162d2e28c4351a45ead3a0bd4b526a
32a81b90391f0862db2db6d701ca29772b7c38734f928b302751a8d24d8c4a6b
331ed6ea56aff70500a40f195aeb78fbd5fcd86fb000a5300eebba22926f5c36
351588c6f208e00c046840524635fdcb6690a4e834e50b04cf29eb739960a556
370e2d6aad3b12876fb5d7ce51f7b69438d77f8fa3b6ff9db90ba36591c86fd5
3cc300cf3f4442b147736ab4053f9c37007639314555ba204e2e7b5458bdea2e
419c60982a5ef28c5a9028bd3ff9dd418dfb9a229f0f672b5cc09865c9212c01
45d5b628ea3ebce34feb812984c20b1caaf7ad014744c0d1af92ca4329008d0d
49950ea1d80fcd51eb708d70aebde9ec730d3d1157569a32dc4e8d9686635fe4
51a0cefbc6f455ae11e414dcfd57b339f49b3728d6e77bf62a2b4dc950ff756c
5b400a7336b2386e80d7137462c41d4cb80fb8d80f31474362f966b5bf38c83d
5c333ec91c2ea8d08370cf8f0abfa7a92db29a60b2708245419b332324932052
5cd2017ab7a8c49f77af32cc17418cebc39caae377be4c6082c76c0ff9dce4b1
6131dff0090943da0877cd7eac167190d5cb869b2524757a67bb2f319384f391
61a3efa7284be26c128e00f34d4bd4bdedfc2e217997fbf91dec036da78234a4
6720a131e0f97d7235f3bb336446b99983010d02a3b86e0e0b6cce427ca92675
6abacaf184cab7eec777639ad5b4e4e51a113cb91581eb3eba80f61b5b45b132
6c8eedd82cd11a6817482c215333ed36e4d1af232f0690a9f2bb2240deb0b5e2
6e449da9cbe233008bd08f5df387a790a3c9edfb0f2beda1b432a17c41a47f15
74699899eebe4638fc33dd64adcc4585a4c752e621a3ed7e38abace15621d2f1
7554bedfa0e13c1102c7c8609c81a95df21e886a771e5f99016413942b4fbf00
79e21293eb53717af3dd983167c1d15f56fc525fd126080166bae05e26b77289
7e9d8fa80e3cd36da8a466c163f40bacdac61f2d3921791b96672ed087896c9f

80c362ac1daba9bed861dd6bdec57edb7371cefbf57f0716cd00a1150a3f2c9e
80f867db0b140e12a3adf96528a6094897a33b09e7772e6200f6aa5fe5887e5f
82e5df970af2e9630c757d952e7afb028d5ea8f619cf4ef1e486c6debb6d2272
8cfa5047430658225878 62b5e78a3cd3681cb4acd92c7259eac50b6d132b9fa5
903175538ada2720c41a3a7ff54e614568026325b4d086cfcc8cfc2ce60a18cf
930e13ced30020f153017804a29528fdb2fc1916b6097f2f057d2babf2edf204
966ae1f5487c97e66254cfcf65a8544b01457ad6e0653943aeaae9fcae7e323b
98cac80e27906aff0de7bcad4e4160197b6b88e21440c58090e0bf7455b94678
992df3094003c311d056ea54b1314ff2d14e098ba1ec01e7855f93b1d09c07fe
9c1f00036e6095e562632e165d49237bf025caeee5dad1aec7116a77ace16005
9e164b68ccd39c611f4094d3b3bda6d3f4cbcd4a5ffe57fe2591d5bc6407c33b
9ef9776b4f4a207a047cee877cfc7e6c8f26846b4d6924b29c976806fff9cd75
a28066c2be30a1d6b418f7b125afb3f5287f6c1af5eb9b17ab582b81d917a9cf
a7ce31b071b49aa3586ef9d4d09c0dfb545b70662409098f09c73835eb3abd22
a7d555f415293cb3bc2f3e7a7a7c270948c7b300d2901416d21fb0230c2c9f09
abae67b99e638de962803016bffe8996b3517b01883ceb43febd1b5234fe2f8f
ad0443270bedf07dc1c336de9d0b6c03e84a3e5afc7c14b6cb9d6b71694c629f
adb9294ed90373c56bec13204aab9622ce7776109438863d47e2c2ee55efe244
bb0fa4477fa1e2206962c13ceffe51ab9e25731e18a2f773f85b0ee788bdef72
bc21bcf93f3896a66f6e5f7a1d5f24205dc6dd816f53c56537e7f0a26ff38c72
c0708c15b307dafc58f5459c31a3d99c6a2e1503d5fb9b2c02380b00d0e374c5
c07415a96ddfdd416478841e43269f5663690dfa1b0c96d0de7aeed822643d4f
c4f28c3f0376498898df5f09c6a72df1b4486f8f63221d81355ec35005e913a2
c79c3129853540d4a9b53ce473e4d59095bda2268f8a68f34bad09ed780a8325
ca65b935dceb0c3e853a1e5da185c78d8834b7380b820ec4d8721ca03e4be6f5
d115843cf04e23a87de317e013cd6344c646d57a13b000ccce568b6212b0f3bd
d1d25fefb7a29e4beb76ae452a64098deaaf695e7e28f177e951195d1e7521c1
d347609f5b0227e6d69cd7fa9ce4a0ef9a7e28823bd0bee38fd24a3f7bf39548
d356a5d34aeaadbfdbfdf919d09de477f7ceda2fc15aa5739bcc310ded7b082f
d651ada2338aaa92797f8e61166f12efdd9de984f48a8642854ab0ae7038286f
d7227783480275fd6fca7e47bac8fd6c47853691d3ec45ba5acd8ff01ded4e73
dbe8eb0f5c65b9f8cea0ce5fe2480acb468f36294ea6e6130ac8bf1531455dad
dd102cf8ae3a1a3e0abca323fe66c66bddcabcd55ed0335ed274a27d46bf9cf1
dd344380503b6b15532cff7ceaefb44b37adbc2e3417def041f302f7580b0afc
ddbac22b9a8b0955b57925d72e10f6a3502e55cf3284b42cb28033812ff2f668
dfae571370adbcd0aec172094fe7eb385bf694817fae3344c0cca57323358b0f
e30d742c3bbb8a69e269d7ad3503267f5526fbaec097046cd147f7c0be9df800
e6537cd355a0c308866e3da1aa38fdff69cd2a4c9fabd269dae24e0a4203f3b9
e6549c248aa80335756c9d48562902d606439417cdfc838acbc4cdf54527e416
e684137d30a3a0e9389581493e23a79ffc1014060be8f46a395c2ea31dfa92f4
eacb565ca950d6bf755784837bd0f64b76fe1a8952bb1fa9a7b11831191cec2c
eb808de8ed9c7ee0b28f2d19cfea4735e8b0db18c1f1fadb8f587457269eff14

f8c134fb428e811bc27ab1f864570da6e1693e22081e8c1178ed2c876eceda4d
f8d4cc61ddb1432d50cf000e5e06673d8d527f5c8448bc4bfe23a61deea4c73b
fdf8511c5cfaf29e78b0f4abdf022f37f2c5ce7fab42ccb7b3e2acefcc041bb4

IoC nombre de archivo

Nombres de archivos con malware:

LEMA PO 652872-21.ppt
MV CAN YUCEL PARTICULARS FOR DEMOLITION DELIVERY.rar
MV FRIEDRICH SCHULTE AGENCY APPOINTMENT LETTER.rar
New Order.gz
Remittance copy.pdf.ace
AD1-2001028L.pdf.z
dbs.payment.slip.pdf.iso
Gtagle-50434-7539-23-238381.HTM
INVOICE.gz
MT103.pdf.ace
MU3666.gz
MU3666.pdf.z
PO.gz

IoC servidor SMTP

Direcciones IP de servidor SMTP. Se debe tener consideración que podrían aparecer direcciones de Servicios Cloud reconocidos, ya que este apartado informa desde donde salieron los correos electrónicos maliciosos.

IP	Etiqueta de sistema autónomo
185.222.57.232	rootlayer web services ltd.
177.126.23.165	3d telecomunicacoes ltda
177.185.241.139	gox internet
2.136.228.191	telefonica de espana
213.80.93.236	ip-only networks ab
187.86.136.42	vetorialnet inf. e servicos de internet ltda
99.19.124.45	att-internet4
207.246.94.93	as-choopa
160.16.196.187	sakura internet inc.
80.82.67.51	ip volume inc
185.222.57.227	rootlayer web services ltd.
125.214.169.213	dialog axiata plc.

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

foodtrade@fresco.co.kr
abdullaa@mashreq.com
dariusz@stiens.de
docusign@fstworld.com
donna_perry@rogers-brown.com
foodtrade3@fresco.co.kr
galeman@cyrusbrokers.com.ar
mariano.flores@sampa.com
noreply@marklivesproducts.store
ops@wmashipcare.com
waruna@packserve.lk
sales12@ceaworld.com
statu@statushipping.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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.04.06 16:04:49 -04'00'