Alerta de seguridad cibernética	2CMV21-00176-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2021
Última revisión	12 de mayo 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), 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 de los archivos adjuntos en los correos electrónicos:

02fab97fe9b0e2e94abd4917fb5bc88d21445760ee37971b919f47c95a01f195
0cbb6c8b7bf0f108b82ac808211852dac62709ceefb84d8e93b2ef912428d24b
1ebb93102f8b08f724aad0bd312006450853d65266c0558a88da622d75c67bd8
23e012a59ae4794e05bd5de9b353f788d9b9ce7045ca27ff5a93b7b922746db4
2775248702bf6bfc3b01f77ace8b5be9f5281eb9e00a6b92323ea4cdca78b2ab
33fa7ababe331e58c82f5ca9423f269d598f321c3e8f700373775bc6c993992d
389f593eff1b5bc4c552f9765ac8b5070f910428b430a4fc16ca6f8379128a52
4b922b87034981af8f69326f64789363ef2b468fc58ddad34c16c5c6bd82e3ca
4cedb439d35ae9db6b9f25b013c9d7c0bcee78990305bc0764d245c70b0c86b0
4e2543aba8686312bc8212b9c799dc233f91d017b5767e91c5fae744d75d152b
5116d89d1fbc3cf87e842b52acd91b70d1cf5a9cd68157fc9ecf9d1b8d3c498c
5f4e4fbde7ed003dc34954ee301977f697de1cd2d52beafd898023797ab47255
65d09004525ac8e3d844232e6f1f99ec26bcf3a24447ee4a55ef0cf805ca0480
65f0e0590469268511ed7b779808f4178386b7d81ad0447d3ae9b5260a42a4d2
67cc5fdee7630da23e8b6b63bd6da843cd7ea1e0fe05f47c2dc57bab10716342
692d2b764da8c746e7abdcb6d09fc5fa92de2729ddab5fbaa22c42155b9df273
6bd884cbbae349fb1933fb97280d2d84a2b71f8adf6c9feb363941c04bb40ef4
71daea6f6dedd5094544dec50a02050559328113afe48df41c93a42ce56e855c
757e11cf6260b6d84410f18cf27cfb50447e15059fffa296add2469967182d57
7e80eb8594da599e745dc646a4fe02aca27c56457aca6a9c35f387c281202c9c
84f5938bf6b3849d4055c64663e26912dd368506a5ca784ebccdfe39cf6cde10
878a4f96c80d638d087347f2f4d9fd09df01b3bff20ce362c9fff16bca94e5bb
95f7f656ee4dee95a46e971797962bc365f9289923a936d2a9b8190bed88b611
976d036150ddef649c0fdffa89bfcaa19f5743e98e45d9cdccb76b66632c8ee5
9b82331902103e80ae6cdda02fa33bdd00cba59bac68c5d6f1109d1b93020e23
a33d4b647cd9a415a96aa0aaa97bbaf2abf2817cf5eef4faf812a3216e9d1a9e
a3d4f2e5e5c91a17786c7c3cea524a17d513735550b30b3d4494fc11d6e1135d
b38df877b327db04dfa2bea03a94ceec82b1942560acfb6c87256be88f707bb2
c3241d3e58071c903d635550d9dd35da14d3602a349c716527e4a9f147b7e4be
c3333735a22b46fa116054c15ea6f273bbbcedef13b633d0b7721d91a57ba2b4
c53c03a021b14ae039a3115115fdd552892ad3e2e19698492c14121dd582ee07
ca91a8dd6f50202cdc5ed444cb1c1f447f2dc108f2c276658f337c93259fb1ce
d109452c99cd984de885f08d3be104145f9d4f5396c2001fd6e048c5ffcbfb3d
d18e005fa449ab6ac3b7febb25dd6a05e16dc7a87f684ed49d6c093a2c61e6c7
d8cbbb4144d9b4350b367fa89b250b4a35933b77c00d36b3e885f2aa17e0aaff

d9507b9760fb0ab4ad0a6ca6e92bdbb16cccd5ce1d5e60cf158dc21114092ff4
e01ebff50cac856b458473e4e7b47ef942fd93d4327ff8f56bd95a43d954bb3a
e55e03e26e7a9c71f639f9aaf6a3c5dfd0138fa4578f9f86d7fce950027d6d2e
e79c26ed16f145a7282b54b3137f09e4100495c7d06c0ea73052762d0877dbd3
e943753978e4c47b5bca140cbcc1e669b7d900fbe3e55fd37aa1b4925c11fd93
eb797eaf04038f3b1330dc4cf7dbfcaca0758a0340082fa223f5399209acb984
ed30c09693df6de5d1ceff9395eb0c8662ffbcd5f8fdaf641f9d4df9e77910de
f74ad88b84c59f91ebb58052bb7b9a1238a93f86f19f6d9015839d38d26f4364
fbc3fb202e26f02612903679f57dd9406546cb79e18d2a0fb31459a276aabe93
fd6ade6040d775af6ddf8c835a1f7b32bb17ccaf5ca227af55df9accfc75329d

IoC nombre de archivo

Nombres de archivos con malware:

PO.#4500499953.rar
1900273.rar
5-12.xlsx
FP_01307970.xlsx
Adress_onfirmation_Portal.htm
"Request for Payment Information.r00"
"VNDR14003140000000000620 pdf.ace"
"NEW ORDER INQUIRY_B90202821.pdf.gz"
Booking.rar
"Nuevo orden.img"
Scan837400.7z
"BL COPY.zip"
PI.xlsx
NewPO.cab
"Original BL, Invoice & Packing List.html"
PO_000630.rar
"ADVANCE PAYMENT.rar"
"New order.rar"
"Purchase Order_12052021.ace"
EU-Business-Register.pdf
"Urgent RFQ_AP65425652_032421,pdf.cab"
"Order 4503860408.zip"
"Orden de compra 2101903-0.iso"
"COPIA RAPIDA DE PAGO.zip"

VM-(ðŸ“ž)---09_22347.htm
SWIFT20210511094146076.gz
"DHL_Telex Release BL.tar.001"
"Scan_PO AR483-159043 & PO AR483-1590436 FOR J-3000433707.r00"
"SOA_DEBit Notes & Credit Notes.r01"
"RFx 6200238509.xlsx"
"informe bancario.xlsx_____.img"
Solicitud_de_cotizacioÌn.zip
IMG_93_107_80.R01
"Purchase Order 11052021.ace"
"Shipment Document BL,INV and packing List.ace"
"Payment Advice.pdf.rar"
"Purchase Order 12052021.gz"
"VNDR14003140000000000620 pdf.zip"
"RFx DescriptionTerms B35O-18342.xlsx"
"Purchase Order PO-000991.pdf.zip"
UL_LLC_11052021,283763pdf.7z
invoice.zip
"3pending messages.html"
"Order-RFQ # 097663899.gz"
"Factura comercial____PDF.gz"
"Notificacin de dhl_____PDF.gz"
PO.#4500499953.r00

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
45.137.22.149	RootLayer Web Services Ltd.
92.42.36.95	EUROTA INTERNET SERVICES LTD
185.121.120.179	Serverion BV
162.241.205.153	Unified Layer
45.137.22.147	RootLayer Web Services Ltd.
91.212.89.57	UZINFOCOM State Unitary Enterprise
186.65.73.138	Adexus S.A.
45.87.60.140	Hyonix
103.145.254.33	MAINT-VN-VNNIC
77.247.110.104	PEENQ.NL

66.36.234.110	HopOne Internet Corporation
103.99.1.238	MAINT-VN-VNNIC
31.210.21.71	Serverion BV
45.170.245.119	ZEROPING S. DE R.L. DE C.V.
104.47.33.54	Microsoft Corporation
162.241.211.105	Unified Layer
181.119.65.95	IFX Networks Argentina S.R.L.
104.47.56.48	Microsoft Corporation
31.210.20.250	Serverion BV
31.210.21.247	Serverion BV
185.222.58.100	bd-rootlayer-1-mnt
185.29.8.26	DataClub S.A.
190.15.202.141	Informática y Telecomunicaciones S.A.
103.156.92.46	MAINT-VN-VNNIC
45.137.22.52	RootLayer Web Services Ltd.
185.121.120.245	Serverion BV
153.122.55.69	MAINT-JPNIC
185.222.57.174	bd-rootlayer-1-mntB8B2:B28B1:B28

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: 2021.05.13 12:39:52 -04'00'