Alerta de seguridad cibernética	2CMV21-00205-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Julio de 2021
Última revisión	28 de Julio 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:

N°	HASH	Tipo Malware
1	02c10e4943caad34e424ca72a545a2d416b73eee0d3099d80e2ee3cb86c1932f	MSIL/Kryptik.ACCR!tr
2	18321caf87215750bb9821aca4c50c13de7d30e69fa056e1894f644332043909	MSIL/Agent.GIQ!tr
3	1a94be42daac6ce93b9cb5564934898f2b1bdcfbd24c9db7d37b9e04639a49d9	MSIL/Kryptik.ABZB!tr
4	239ab5d4355bfbeb28962fa372ff4004d94f5aa7d5c423be9c84548c521908fa	MSIL/Kryptik.ABZB!tr
5	3fc21fc6c204930b144bffcd4eb0ad572908533a199e2008e1508613f9be785e	MSOffice/CVE_2017_11882.C!exploit
6	44064d93545f38520fcadc58302473ea99087deb716b245fcec3d3bd78b9ba34	RTF/CVE_2017_8570.VQR!exploit
7	5c602bf190d06a7b541c9629bd48bb63745ef463c24e572c7a285f9891e507ec	MSIL/GenKryptik.FHZB!tr
8	6a61427fa26132640faa4616ef57d8d13785f8f73e2697720e036da63c7acdf3	MSIL/Agent.GIQ!tr
9	6dd997c225f5e598cb1cfe95b5689a51599cc0f4b8f1dfa610f92a63469c281f	RTF/CVE_2017_8570.VQR!exploit
10	6f7d6ab9dd45bebc793602779f132e11a28884dfc688f7710cdad670931e9864	MSIL/Kryptik.ABZB!tr
11	7409ceb633397a1854309a81169d6391bb87abd66705baf71abcdbad755c500a	MSIL/GenKryptik.FHZB!tr
12	8d3dcceb1f017ceb60e22af0abff3f67095eb9327068e38eb872ccb7570d7779	HTML/Phishing.5532!tr
13	8f5b6b2c0c2204797c4b29217eab69c341fe06d8cbc6f54f9ac04481f17861f9	MSIL/Agent.GIQ!tr
14	9c203a23b7ca95d7b840c9e3fa451d691a2e8a53df5e22bd1c872a55acbdb386	MSIL/Kryptik.65DA!tr
15	b7f4d8718eed4813c9326fa3e977e7dfdd6de80e6b597db61a9c5583c755dfed	RTF/Abnormal.F!tr
16	ba7731b6dc348e539c3e92a30f7811579de525f4346b223430b0b668e68e30c0	VBA/Agent.1873!tr.dldr
17	c435ee050c32e9de7560a2f0b9f08b7a9b3919c7761bdb2140fc7f80d16fe35f	Malware_Generic.P0
18	cfac96c006899be8f8793a5da85b1264c5b7a696ee7bc775262d2082c534e4be	HTML/Phish.BMD!tr
19	d1b4347d7887ca25444518b4250fcde245d9136a79237ef28b5f93f355c6c2b8	W32/Injector.EPVF!tr
20	e273e3fe4d92b5b08db5cbd12db9542fba9aa559c3cfde3fe5e4c52d3dbdb7e7	MSIL/Agent.GIQ!tr
21	ee7979d6fd168eac5e0cdfc2438e99454ff3b6144c9e08133bc255073b028d4a	MSIL/Agent.GIQ!tr
22	fa963d4d83f84c063302d32d411f535cbd4965539869e2752efda5d0d267c2bc	MSIL/Agent.GIQ!tr
23	fe04378dd45882a26898da0e74a054847878eb1d9b4515edb317d5c30805acd4	MSIL/Agent.GIQ!tr
24	ffaddd9987582634ac6b9e8955b3a85caaf1a4a96f410cd931455d630a76de3c	MSIL/Agent.GIQ!tr

IoC nombre de archivo

Nombres de archivos con malware:

N°	Archivo Malware
1	Air Waybill.PDF.htm
2	CV.zip
3	Enquiry 210701.xlsx
4	Request for offer.gz
5	Payment Copy.r15
6	swift copy.pdf.z
7	PURCHASE ORDER-PO-S.L 45675675.pdf.r09
8	PO.r15
9	Pedido urgente.zip
10	ESTADOS DE CUENTA BANCARIOS.gz
11	cotizacin de pedido solicitado.gz
12	PI - ORDER IS01JL28.gz
13	Solicitud de cotizacion_____pdf_____.zip
14	req quote.lzh
15	Payment_invoice.zip
16	TT COPY.r15
17	RFI 0993583_SCRP.xlsx
18	ORDER -ASLF1SR00116-PDF.ISO-XLS.ISO
19	PI 8922.doc
20	FedEx AWB #8002566716536.doc
21	Pago.xls
22	Ordre DExtensi 27072021.gz
23	Saldo_Cuentas_Mensual.pdf
24	Cartola Trim Hipotecario.pdf

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.

N°	IP	Etiqueta de sistema autónomo
1	209.85.167.69	Google LLC
2	77.105.0.60	Orion Telekom Tim d.o.o
3	45.137.22.67	RootLayer Web Services Ltd.
4	77.247.110.225	PEENQ.NL
5	185.222.57.156	bd-rootlayer-1-mnt
6	208.70.251.202	Colocation America Corporation
7	185.222.57.68	bd-rootlayer-1-mnt
8	103.139.45.212	Trung Hieu Services Trading Investment Company Limited
9	185.222.57.94	bd-rootlayer-1-mnt
10	185.29.10.119	Virtual Servers
11	5.181.166.234	Heymman Servers Corporation
12	185.29.8.39	DataClub S.A.
13	159.65.97.226	DigitalOcean LLC
14	200.10.184.122	Corporacion Administrativa del Poder Judicial de C
15	167.89.60.5	SendGrid Inc.
16	40.107.236.50	Microsoft Corporation
17	200.55.203.148	AFP Habitat S.A.
18	170.233.152.50	Latin American and Caribbean IP address Regional Registry
19	167.89.62.71	SendGrid Inc.
20	167.89.58.195	SendGrid Inc.
21	170.233.152.67	Latin American and Caribbean IP address Regional Registry
22	209.85.167.181	Google LLC
23	170.233.152.49	Latin American and Caribbean IP address Regional Registry
24	170.233.152.61	Latin American and Caribbean IP address Regional Registry
25	209.85.208.71	Google LLC
26	209.85.208.72	Google LLC
27	209.85.210.71	Google LLC
28	209.85.216.69	Google LLC
29	40.107.95.83	Microsoft Corporation
30	209.85.219.169	Google LLC
31	209.85.210.69	Google LLC

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: 2021.07.29 09:37:05 -04'00'