Alerta de seguridad cibernética	2CMV21-00222-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2021
Última revisión	22 de septiembre 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	df0c6f655c170f3b33acfe6dd51c3492fae142c7e7d314f522062da54ace7eb0	MSIL/Kryptik.ACHL!tr
2	4060abf7b75e024090fbd2cb937a60f50698334db53a04f3d82a96bbdd823719	RTF/CVE_2017_11882.C!exploit
3	9ebfbd3beb4239fd17b0fc24b9f1ea8d5b56f172e43044d9d4ddba8a4d360dfd	MSIL/Kryptik.ACVR!tr
4	2c21dda7bfd0ec4aca1a77ecc65ac7e87996fd72e2f05ed2161b2ee26461008f	MSOffice/Agent.BD77!tr.dldr
5	7da588f04fa53101d5383de2ddb7cf503c59adb6598e10be0d91ece4fdf6dd6d	MSIL/Agent.AES!tr
6	3eb7d51b8bc7bca27400be167b265335d205e8936312d1b33c2c3dab04385d15	RTF/CVE_2017_11882.C!exploit
7	c3c71e328575ee408f70f8c88f00df195e7f7e40839b2736ee6baf1858eb9262	MSIL/Kryptik.ACVR!tr
8	90a7307e6814ddd45dee083d9bb39ff07eb9caf9a7cbd2b9f82e34879d9cdb93	MSIL/Kryptik.ACHL!tr
9	f71f3c99d8d1673f71b619e402e6c3c511d03b6d2d8aa64bc65015677d09458b	MSIL/Kryptik.ACVR!tr
10	860d9421928312c17111d020aaa3193597d1f557adda489cd67899a8274f799c	W32/Agent.ICOL!tr
11	747d33cf088dc73aeb077ce2b91f161bcef7b0471a5f89aad364091893929f65	MSIL/Kryptik.ACVJ!tr
12	acc8b2859dbd2adcab62bdc752c358d1ff4464b773ba6dd52ff26aa146eb527e	MSIL/Kryptik.ACVJ!tr
13	2cd33b67cedb84528ce335e93eb78187cf37e0d69c66cb55f7ab3deda7050828	Java/GenericGB.29230!tr

IoC nombre de archivo

Nombres de archivos con malware:

N°	Archivo Malware
1	Payment Advice Copy.zip
2	ORDER-20212209-02938273.doc
3	New purchase order____pdf.html
4	SHIPPING DOC (CI,COO,PL,BL).rar
5	PO CB-15GL.docx
6	New Order Specifications pdf.iso
7	ATG order #55.doc
8	message29803.pif
9	AWB_1153703596.zip
10	pqf0009876545678.zip
11	Image001.img
12	ginzunza@mbienes.cl/Purchase Order
13	fondobecaslab Delivery_FORM 9/22/2021 5:06:15 a.m..htm
14	p.muck Delivery_FORM 9/22/2021 4:47:29 a.m..htm
15	shipping documents.rar
16	Quotation - Urgent.zip
17	Company-catalog.zip
18	Company-Profile.zip
19	Quotation.jar

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	157.245.103.184	DIGITALOCEAN-ASN
2	103.153.77.192	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
3	103.89.88.75	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
4	137.184.134.82	DIGITALOCEAN-ASN
5	138.68.30.3	DIGITALOCEAN-ASN
6	178.128.31.232	DIGITALOCEAN-ASN
7	185.222.57.134	RootLayer Web Services Ltd.
8	185.222.57.150	RootLayer Web Services Ltd.
9	185.222.57.153	RootLayer Web Services Ltd.
10	185.222.58.140	RootLayer Web Services Ltd.
11	45.137.22.115	RootLayer Web Services Ltd.
12	46.231.127.25	RootLayer Web Services Ltd.
13	157.245.103.184	DIGITALOCEAN-ASN
14	103.153.77.192	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP

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: 2021.09.24 13:32:31 -03'00'