Alerta de seguridad cibernética	2CMV21-00201-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de julio de 2021
Última revisión	07 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:

ID	Hash	Tipo Malware
1	b210c1d75ecf14c15990acd5524688680b99c5f7284f8a14d3a42458e9bc737d	MSIL/CoinMiner.YII!tr
2	b6841eaa5efc709cf762532ec8af2daa90cf08a4a8cda12edd2adb10001bc31a	MSIL/Kryptik.DLO!tr
3	9d8eec2a5899f9d9d0a14bd7e7b6a39aa582cbbf60db5b5043648d2696b0a319	MSIL/Zmutzy.10!tr
4	3c2a5d950317aa50d37b191ba295162c02d14a6ff3c025af487bc99783eff414	MSIL/Kryptik.ABSN!tr
5	0fd6652f7c270e1305795106182c94dd053ba35c2f3e3f418ddf4d778015f569	MSIL/CoinMiner.YII!tr
6	af3d79e42de3f8759ad4ada86a8952a4aae9250b56779465bac4c5764adb0dcd	MSIL/GenKryptik.FHHH!tr
7	a9b03983f5a4ee070a257b4abceb58ad40100b0222d4a16b13eecdb376d9e119	MSIL/Zmutzy.10!tr
8	cd12a0dfbfcc5d7722934554a45661900dcb2b516b802e092d1a4bff2e53d8c7	MSIL/Zmutzy.10!tr
9	72b2e3c62ce309dc3ad54629be509aeb8c7b3e641cc2b20e773875102a355f72	MSIL/Zmutzy.10!tr
10	e417a3467627ffc0faf36de78a5a4157dd03221f6acdf991cbf12aadf8b4c032	Malicious_Behavior.SB
11	02849d08315cde8a0b40ef84efa6a124335b8cc3059e62cc6276c396716afd48	MSExcel/Agent.1C28!tr
12	c0ab2eba9b259d824d95faf3402e25a2166bfa3abf8b05ae13ddd45db10c89fd	MSIL/Zmutzy.10!tr
13	98241126288b257ea140884e7c4f0f88f4694d8fe2f1a7bc0b006db35644e3be	W32/Injector.EPMJ!tr
14	f785d92c7dc3988cc720cd0b75d2d7ffb55fe22c972b85ca2ce6e0cd9a7b393d	MSIL/Zmutzy.10!tr
15	e643cd12513d5b497dc929f3b9bcc4ced2dba43c572854fdab3f9191b2d42d2c	MSIL/CoinMiner.YII!tr
16	9ab06dad5958032d92be8b54abfd84e4a7828df3accffca30a459ad3a87ff4ec	Malware_Generic.P0
17	829bf6c033b2eb64533471fe8b10a3681219afcdaf61ab47efa30133098db6b1	MSIL/Zmutzy.10!tr
18	c8b2192f933e3b3124abbf20d43e8de51cfceea1469ef40413d3fc83d98c8d03	W32/Malicious_Behavior
19	9627f98b6a50fed8620dae19198edfce38b9ac6e405431ef3b02f90a3904aaa2	MSIL/Zmutzy.10!tr
20	1e4a78b8b23dadfd585b80f8cb12431e6b6b56a0d858c37274dfec5362ebde40	Malicious_Behavior.SB
21	72eebffcbd8b447b411063c73c3de336ac6c7f924451ca701ff66ac4087ec875	MSIL/Kryptik.DLO!tr
22	4092cc3841bc5e1377fb65e343cb837f0255e33d2194c3b24c8dde82a28511ba	Malicious_Behavior.SB

IoC nombre de archivo

Nombres de archivos con malware:

INV+PL+BL-00464758.IMG
Declaración-2021-06-29.img
PAYMENT ADVICE.rar
cotización.xlsx.img
PROFORMA INVOICE.lzh
MV SHENG CHENG HAI VESSEL PARTICULARS.zip
12-17.r00
Aditi Tiwari.7z.zip
RFQ-Order contract requirements.r01
00098QW6890JHG_SWIFT.r09
USD 765,000.xlsx
TY9653623.zip
Payment Advice-BG_EDG9502021090102570032_4430_950.zip
SWIFT- COPY.IMG
v5pjiAHs3HLOr70.rar
Arabic letter .ppt
7U4Gxf2.zip
Payment Details.zip
PI.7.7.2021.r00
Ships Particulars (CANOPUS).zip
cotizaciòn001.PDF.img
S O A -44E45T76468.zip

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
45.35.196.146	Psychz Networks
23.254.230.107	Hostwinds LLC.
77.247.110.72	Myweb Limited
70.35.201.40	Fasthosts Internet Inc
185.222.57.78	Data Center/Web Hosting/Transit
185.222.57.135	RootLayer Web Services Ltd
103.155.83.165	Vietspeed Service Company Limited
135.148.114.42	OVH US LLC
103.139.44.229	Trung Hieu Services Trading Investment Company Limited
103.155.80.68	Viet Speed Service Company Limited
103.133.106.175	NOCIX Trading and Service Limited Company
185.244.38.120	Hyonix LLC
203.146.21.245	CSLOXINFO IDC
165.22.8.198	DigitalOcean LLC
103.141.137.99	Echip Service Trading Company Limited
185.222.57.89	RootLayer Web Services Ltd.
77.247.110.249	Myweb Limited
209.126.124.211	GoDaddy.com LLC
185.222.57.72	RootLayer Web Services Ltd.

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: 2021.07.07 13:58:59 -04'00'