Alerta de seguridad cibernética	2CMV21-00232-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de octubre de 2021
Última revisión	13 de octubre 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	3a770b73665621c5ca5c3fcc5478d39ea130cc31eeeaff926d9b3ec39c7048d4	MSIL/GenKryptik.FLYH!tr
2	ec1ebb7d6744634e8f82e87c03e821a90e84ea038760dbec89e2c75ede498547	MSIL/GenKryptik.FLYH!tr
3	e13afdd0fd1fb07099a8caa32bdba8c0d15ab2b5ad40f9bee89d88556e60bf34	MSIL/GenKryptik.FLYH!tr
4	e6322af0f75dcb3b545798985a6d2e70f57cdf2abc91048aecdb8ac464fe6db4	MSIL/GenKryptik.FLYH!tr
5	1290ef7be0befbdc31eb2dc29ba4ae7526e74d3a1c085f51762b03475a9ef4d5	MSIL/GenKryptik.FLYH!tr
6	44a4ae7b430c4159409101b325d8122dbadfbd4e9d6b9275aaba7589a831ceca	MSIL/GenKryptik.FLYH!tr
7	551c222081882fcb8968d315fd1c74b57572404d9f1a0d15767c4a2ed9ca348e	MSIL/GenKryptik.FLYH!tr
8	c13a3022f2212e4e16fb2147f6fd0c09ed4439a49b4313603a5e48b7b3174167	MSOffice/Agent.GV!tr
9	bcb06cd6c24b4d5d8cfef85a519fe11ea51f70ce7c27eab722647c14fd566bda	HTML/Phish.081B!tr
10	b204a44b893af9affc8791266472d7d588d726eae2ea80be76f5d8dec872b497	MSIL/GenKryptik.FLYH!tr
11	dcef89febad36a6f8d08588731f337077c1291d750e4ea1774b731520f5791cf	MSIL/GenKryptik.DYQU!tr
12	24d19268e9534a4aebc6b70334b552779b06759612002545a901771ce5a42126	MSIL/GenKryptik.FLYH!tr
13	af8d202e018654f3726733634610ade28f16d01db80490d18e3b678460e1751e	HTML/Phishing.BEK!tr
14	3cf850b14aa5ccb72108e860c789ee89b413f2c1656965e788f8b9be6439b775	HTML/Phishing.BEK!tr
15	8a70bba72136c9b91823ef1d98addd5531cf1f9068d34eb9ba8fccb2fe5bb79b	HTML/Phishing.BEK!tr
16	8327b44284237279b83ce93229f789149a36176dd4ccb9e762f75c25f875bea7	HTML/Phishing.BEK!tr
17	b83387eb700c463dfa62960861a237e70859704f9941f7323c3a6c88e686444d	HTML/Phishing.BEK!tr
18	d979bed683723bfed4bd772156f2b3886982dbafab1088e3161968eed062b2b4	HTML/Phishing.BEK!tr
19	394d5fb455fe2342e6f9c4cc0110cb3676913a33a32fa12bb39eb81c186a8917	HTML/Phishing.BEK!tr
20	0ae635296c372922f9c3ce3d99448c4f304f8eb5b3590015141d1f7cb4a0253c	HTML/Phishing.BEK!tr
21	f4718c0c07b79e8815f966701ee6c433e83c08a5c80afa5081747548ef02adc8	HTML/Phishing.BEK!tr
22	1cad9a70978d0a20f1971405b8fca0cbaea59f9873e5475acbc07c3c6382c751	HTML/Phishing.BEK!tr
23	4ca3a94aa79b0176a132e3fbc0f6e0879ab738da90f2d052dcfb42c305a0aa8d	HTML/Phishing.BEK!tr
24	0463dd0a9db07cd789455c6b1e4a35e75361e261b4e9e9cbef29e43312179467	HTML/Phishing.BEK!tr
25	28a875e447fb2c017ba2aee1dee6d6f2c0b4ad9a87139f3563eb57f107e42ab3	HTML/Phishing.BEK!tr
26	1b799d74d26a4db5e9d88c4ba9577acf6d0b0afc0131bb28f182a586872c9d2e	HTML/Phishing.BEK!tr
27	ad4f6b93a3bb80e3bfe1b9942439447e9499939d6bb55da1e7c7c6622cceb112	HTML/Phishing.BEK!tr

N°	HASH	Tipo Malware
29	a8fdb0ef76dfdf5d2b3cf46444c67f190ebe54a1c4fe11f4a319f35366c9f23f	HTML/Phishing.BEK!tr
30	991ab954b535a7ea751b884014e54d6c85a4730b0a08125c5e0b6f567d787657	HTML/Phishing.BEK!tr
31	031206e4c2e7efef7cf1468a330eeae338a03b7fb8540207d347c3ca367f92ba	HTML/Phishing.BEK!tr
32	2b98b9c4f0e1ab05b493d404480e580a5aa0b8cdd8da9ac7b3e5c095a14ff995	HTML/Phishing.BEK!tr
33	bd320d6b811d03cc6c6dbd17f39b2eabf408099d8a75ee9a37480845103e12f1	HTML/Phishing.BEK!tr
34	509f6e362059becf86d2dca7fda7bcb24ab374fc16f5ae25e2ada184ef770771	HTML/Phishing.BEK!tr
35	1cf47a430e3e32a6b980d9bf09db6077d22af86e10425247fe92e378186525d6	HTML/Phishing.BEK!tr
36	2e44f5358b35f29f2c327bf1aa34ca289556f1bd2877fc2006fef071d753ced9	HTML/Phishing.BEK!tr
37	c3262d1804750736f48f347f4bf07ec979699661b191cedc8ff16cc41a9a426f	HTML/Phishing.BEK!tr
38	8ec7234527d959f65f769855ba9b505bbe769c15ca0b5a477d23028ad99d3e99	HTML/Phishing.BEK!tr
39	d3dab5f7d68f7c0b84ea53de750204f675ec079abf61d5ca64cc2f4df9a3d2d2	HTML/Phishing.BEK!tr
40	d72bebc5929f441370e2333a7647abfa3b6d88c1547e63f179fcfcc2ea49641c	HTML/Phishing.BEK!tr
41	5cc807ba226cb53589e8a470b1394a51c81c5bb22c97a496c3115131b80d72b1	HTML/Phishing.BEK!tr
42	c112d7a36323b5776d3bcdde85d861382c50e51b3f79231c50c96f8772622510	HTML/Phishing.BEK!tr
43	b9d5fd8fb71343e0a954e98e53ea8a0b3804ffec8ff0519c2c657d4f09147c27	HTML/Phishing.BEK!tr
44	be43e27a16f5fbf6890def5a7c2cba9e7d9ae9ce52db6c739ea672f97aac1c03	HTML/Phishing.BEK!tr
45	a5d0f8abafed61c9230536234517cdf5e5068078df417637f0c38d19658587f5	HTML/Phishing.BEK!tr
46	cb1493c7e850d97fd843c1a00f11a481baf5fbd3892d22ae83efaecd532776d8	HTML/Phishing.BEK!tr
47	884832a7270da0513e77c376564423f0e10236818c121f1630ebd4cb9304828a	HTML/Phishing.BEK!tr
48	1915c34909dac35ee5fa31fe8ffbbc762b01a906b4ac21964c24dcd2560f1348	HTML/Phishing.BEK!tr
49	eb75baa713c06b6a6fb1557d91a9ac1ec2b1bc9bcda4ad1253d09fbdf6c487fc	HTML/Phishing.BEK!tr
50	f14dad1ab1bf4da70481bdcbcdf31fa0642a2f85c5176c405ba9f783f6002763	HTML/Phishing.BEK!tr
51	16fcc6562a9b381d646605065e2c0d07d4313703752ad75aafd2cb98b721e4f9	HTML/Phishing.BEK!tr
52	23ea4752dc2df4d8087579e950e670753347e6fda7b82d3a2a044013e9c77c0d	HTML/Phishing.BEK!tr
53	5f725d2e82b54b288198dbf25495ac5b017f6fbe1ba927ade0352ec20ea76122	HTML/Phishing.BEK!tr
54	7b2f0e5b8c504207bd11299908c0c8e254a4583923dbad4428928dad8f5b140a	RTF/CVE_2017_11882.C!exploit
55	f8e5931926034fb027649ebd98867c41315b44bd05c7bb56f5f506a170162010	MSOffice/Agent.GV!tr

N°	HASH	Tipo Malware
56	4b2be6731f01d01fca26a96260020ee62a266f018d081d170c30043c0191fe76	W32/Injector.EQGK!tr
57	87ef5fdc453362f2a6472c66db59645a6efae8b1f67ba95cfb2b5c9184c0eee5	PossibleThreat.PALLASNET.H
58	401ca80a6909af5525501f14a2deedc569ab3ba4e276c77ca1b6fc2e820a5c53	W32/Injector_AGen.AG!tr
59	b277c57c94e4063b679e9d6e181a58aa82697773f98e40a5f68fa4db785e1986	Malware_Generic.P0
60	fe50b5d75c26eb3d727b32a031f726df6f6447a97340cba0ac89ace8e812ab23	Malware_Generic.P0
61	3b895f545a3e92575e0b7971e061c929ad1f3913c1d3db3acc8a58e3e25a45be	W32/Injector.EQAC!tr
62	d610a9f285980c3838bbc11fbef2c5b999b20f81149328a809d41e6bf97b54cb	W32/Injector.EQGK!tr
63	033372113246279f04ccac1fab6748a2bfd2ed9b9c5cb980534f444dac558af8	MSOffice/Agent.GV!tr
64	80658759ad67edd23bc4cbfaba5e2add421ff794772ddffe24174b6f25904087	Java/GenericGB.29230!tr
65	d09bc5f5e58e844d5739c655830b27c55e2b784d4b65d3f676df60383a8eae27	MSIL/Kryptik.ACTW!tr
66	40bf30e02d39fb1cca08b9cc64005f86c33b181628fcf6c50b3f21d00eef37da	Malicious_Behavior.SB
56	4b2be6731f01d01fca26a96260020ee62a266f018d081d170c30043c0191fe76	W32/Injector.EQGK!tr
57	87ef5fdc453362f2a6472c66db59645a6efae8b1f67ba95cfb2b5c9184c0eee5	PossibleThreat.PALLASNET.H
58	401ca80a6909af5525501f14a2deedc569ab3ba4e276c77ca1b6fc2e820a5c53	W32/Injector_AGen.AG!tr
59	b277c57c94e4063b679e9d6e181a58aa82697773f98e40a5f68fa4db785e1986	Malware_Generic.P0
60	fe50b5d75c26eb3d727b32a031f726df6f6447a97340cba0ac89ace8e812ab23	Malware_Generic.P0
61	3b895f545a3e92575e0b7971e061c929ad1f3913c1d3db3acc8a58e3e25a45be	W32/Injector.EQAC!tr

IoC nombre de archivo

Nombres de archivos con malware:

Price Inq 01.xls.zip
SOA.UUE
Swift copy.r15
Invoice0012.iso
Remitance Aowl internationa co.limited SWIFT-$ 111,480.GZ
REMITTANCE-54324.rar
Purchase order.r15
Shipping documents.xlsx
DHL PARCEL.HTML
SOA.lzh
Payment_MT103.r09
New Purchase Order.img
AWB 101221_pdf.rar
Documents.html
PI- 202110088.doc
TransportLabel_1189160070.xlsx
signed copy.rar
First enquiry.zip
Nueva lista de pedidos.zip
file31.cab
SOA.xlsx
BANK INFORMATION.r15

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	62.113.202.103	23M GmbH
2	77.247.110.172	ABC Consultancy
3	103.232.55.238	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED
4	134.209.231.21	DIGITALOCEAN-ASN
5	138.197.163.80	DIGITALOCEAN-ASN
6	143.198.71.50	DIGITALOCEAN-ASN
7	162.144.153.50	UNIFIEDLAYER-AS-1
8	176.61.147.211	Domios S.A
9	185.222.57.88	RootLayer Web Services Ltd
10	185.222.58.136	RootLayer Web Services Ltd
11	185.222.58.154	RootLayer Web Services Ltd
12	188.126.94.39	GleSYS AB
13	212.193.30.112	Des Capital B.V.
14	45.137.22.137	RootLayer Web Services Ltd
15	45.137.22.38	RootLayer Web Services Ltd
16	45.137.22.60	RootLayer Web Services Ltd
17	45.137.22.70	RootLayer Web Services Ltd
18	45.137.22.90	RootLayer Web Services Ltd
19	64.44.168.170	NEXON

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: 2021.10.14 08:53:38 -03'00'