Alerta de seguridad cibernética	2CMV21-00223-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de septiembre de 2021
Última revisión	27 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.

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:

N°	HASH	Tipo Malware
1	ce54e81125eb44ed53dec51f69f439d692ec3fcbfa99be82886163b5c869e74b	VBS/Agent.RHB!tr
2	d923ce5dbb6597b2273301a0b0dc647fca4f991ed56077ab79c27255236b9161	HTML/Agent.AQX!tr
3	595d62cc2f9ed1adb5942bbc6c00c1b5e57e005117d9242c7c2ddd40ae86cbe8	HTML/Agent.AQX!tr
4	c6ffb2a4f4431bf21036e943929bdfc08b7fd294078b58a12ee620185e02bdd1	HTML/Agent.AQX!tr
5	cc191eee507fc53308ddb782e027ad7f06067dafb3f0e29817e1e851bb6dc404	W32/Netsky.R@mm
6	8650d63541ab6adedffccf52b48bac6bea614b40b01bce5714a517cb58285233	Riskware/POC_Iframe_CID
7	9d501718380963810ff2c744984ae0b469acf79310208e54be06e89a4c274f43	HTML/Phish.D96E!tr
8	52143f691973b6e77f05a76d9d3acfe7c542160eaddc25f30a98d34924321a7a	Trojan.Zmutzy.812
9	e9112eae7f2de93d8e9722b06dc89ae78af80ff54bf8ff9466280c9be6181566	MSIL/GenKryptik.FLEG!tr
10	d93c8bb2a190934c96aae21f1e9a471cf13ed75a62ac339a307eaa6e00c6d70c	MSIL/GenKryptik.FLEG!tr
11	3fc3b61b78ef7b3133ae4350a591a56ee0cc7a0f0bdf6eaf40ea01f3c485dd04	MSOffice/Scam.2ED7!tr
12	135dedf906bbb8eef7aef3b5966f1b933e65725cef80e653031481feb7351d62	RTF/CVE_2017_11882.C!exploit
13	bec0f15ead1deb0d8761ae7c3946c5aa2547245b081fc5d2a9a84449f9c69fdf	MSOffice/Agent.GV!tr
14	d5e3e06abfafe1c34fe40609293e5c68124c8386fe176be8e4a9606ea7f1f6ba	Malicious_Behavior.SB
15	80076f3efa0ef7d925aea98f2dacc44218901df78131aa757fa17308d1b0c6ac	W32/Renamer.BQT!tr
16	94ccac8926a3631f24f90fdee44dba55012a296b1bd918ae206a1ca63290bd19	W32/PossibleThreat
17	4bec198c3b9044d9048d64b8f4910b1ece28a112a8574bbb3bde90c813c86375	W32/PossibleThreat
18	a0f83ac12ac70862e8d23f203dfacab3cb6b7db722caaf54a0316c9c036c67d4	MSOffice/CVE_2017_11882.DMP
19	333ea88cba349ca95118c5a3ea4e4f2f16cd403a933a1ee805d0763f629e07f5	HTML/Phishing.BTV!tr
20	d2328ee77375a61ce495f4ad6a18d4766588cd0d97cb17cc20eb6618ffe3ae96	PossibleThreat
21	c103b226304f25770133cc9f080bbb43c3a790eeaf542f581ecbdf37aff33b5e	HTML/Agent.AQX!tr
22	dfa4598a66fb4267bb2c51bf9e2dba6bc3c022cb2ad9838a6da7ff0f69077afc	W32/Agensla.FLEH!tr.pws
23	378e722690fc135e245b37d280aece03cad76ad95da7ac4af06293bb27bfd823	W32/Agensla.FLEH!tr.pws
24	dc7bc675429ac837433812650657f4e2712eaa1a9ed0ee15323c50c38a45930c	W32/Agensla.FLEH!tr.pws
25	f4a4a7d84f937fdaa9808d529e4541ae6ef330e77ed8bd42fc776ff088fa22fb	MSIL/Tiny.BGM!tr.dldr
26	4128ef1454b3c622904e02a72036174abcc26605d7204248f260441ab57efa4c	HTML/Redirect.1258!tr
27	de723989633a408ec0940236e4ae0a52d6fde55ba881d18aaf3366a28e3e2975	MSIL/GenKryptik.FLDA!tr

IoC nombre de archivo

Nombres de archivos con malware:

N°	Archivo Malware
1	bank details.XLXs.img
2	DEPARTAMENTO_INTERNACIONAL_DE_MOLOTERÃ□A..docx
3	dhlshipping.html
4	Doc1.pdf.rar
5	Document.zip
6	ðŸ“£_â,¬68__763__ID_2sVRGlvUKdyuCm540I3p8SdseMqgI6.html
7	IN00987656.pdf.exe
8	message18002.zip
9	NEW PRODUCT DETAILS.doc
10	New_Order_PO#960780_MT_Quote-MT.gz
11	Nuevo pedido # 86-55113,pdf.iso
12	OBL PN210700369.doc
13	Proforma Invoice-Bank Advice (PAID) Attached.pdf.zip
14	Quotation 200113893.pdf.img
15	QUOTATION INVOICE.html
16	REVISED ORDER.zip
17	RFQ indent.xlsx
18	Sept-PO-34482.html
19	Spare Parts KITO.XLXs.img
20	URGENT ORDER CURRENT LOUVOLITE PROJECT.doc

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	46.183.223.82	DataClub S.A.
1	172.96.11.222	UNREAL-SERVERS
1	88.30.17.247	Telefonica De Espana
1	192.119.110.154	HOSTWINDS
1	217.31.95.26	Hostserver GmbH
1	45.137.22.143	RootLayer Web Services Ltd.
1	45.137.22.48	RootLayer Web Services Ltd.
1	23.94.152.203	AS-COLOCROSSING
1	23.94.152.201	AS-COLOCROSSING
1	45.144.225.128	Delis LLC
1	84.38.130.219	DataClub S.A
1	67.207.82.148	DIGITALOCEAN-ASN
1	103.133.110.171	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
1	185.222.57.172	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: 2021.09.27 18:01:53 -03'00'