Alerta de seguridad cibernética	2CMV21-00200-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de junio de 2021
Última revisión	30 de junio 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 del Gobierno de Chile (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	2b41b43a834b2478d5847e662c060b21e3a4a379f2b474b7dc14b1fd5c4eeefb	MSIL/Kryptik.ABQV!tr
2	4473e22ad40e816cd3d172e45e06dbf5b7efb3fd3f7ea1c23e786051cad5756a	MSIL/Kryptik.ABQV!tr
3	f0e1abf821003b21880756b6697a96e818031a94653815f09869f29c704608da	MSIL/Kryptik.ABQV!tr
4	90786a6e788d4541051f2c754fc6b9dd803197de775959f7e76b67c02876c7d8	MSIL/Kryptik.ABQV!tr
5	0945ad2b9a16c4cee10805425ab4270095739f8f993e5b4a68730876fc60bd72	MSIL/Kryptik.ABOX!tr
6	00de32152d8bbc2f8b7c455964234418ef535750d11af0af3a5c7138274b6de2	MSIL/Kryptik.ABQV!tr
7	35e1132c4d5bd6ce3bb574fb61d0da63e98f3b473c72052c218cfa7d8927750a	MSIL/Kryptik.ABOX!tr
8	b18f41f963af2064d1cf3101631a1ae7426dfb327bfe6756b0d7cf16f7ebdd35	MSIL/Kryptik.ABQV!tr
9	222c5cbdc358ef41c0493d1f656a759e4dc0c7635148833901924490b43581db	MSIL/Kryptik.ABOX!tr
10	b0871e4ff17df03f7513bf5ed9aed71d6011c6542b3016324b4a15743f69d05b	MSIL/Kryptik.ABSG!tr
11	4189b55247d620166ed58da46949e5a4227c82748364fc61cd06ac83e8219417	MSIL/Kryptik.ABQV!tr
12	c44d428719c6f94f419fc91704c34bf27909d1daffee1baa17f97d873d3d46a4	HTML/MsPhishing.4231!tr
13	e913d86e60cb4ac0e0008015a78c78d780f5f210bb410e06fcded6fa0a22bc2b	HTML/MsPhishing.4231!tr
14	22a4bd616aa1cc32e51344ca9ccaba7fc38608ddd8e73ef7557ba05ed65d9008	HTML/Phish.70A6!phish
15	98baffb5cd3cda0c33648f487a7185a258589067b1f49adbc1d484032f6e95f5	HTML/Phish.70A6!phish
16	a9cc8cddb4c92d03e27ded9f766597de8d763bf537029b487952f43f3f7f837c	W32/Kryptik.EPLE!tr
17	71e3eb82dc3b703a8dba3b4d98b38485edf4ff8711b0cee42c9688323f7d6bb8	Malicious_Behavior.SB
18	1920fa7022ce82e956bef779d31f34e96c1a55769797545e55f8da8d093b671d	MSIL/Kryptik.ABQV!tr
19	a9f12b56f2057a88ccf7e9424fd158072e2ade913c2224c3c1106ea487449024	MSIL/Kryptik.ABOX!tr
20	d2782bda4b66e405aa6d987623f964aa1cc974cc134a63c964be47e53b473052	MSIL/Kryptik.ABOX!tr
21	3cea6bd93b9412c8b37dcddf638ee4a4c8a903fc6072fb14d72c0297bafd212e	MSIL/Kryptik.ABQV!tr

IoC nombre de archivo

Nombres de archivos con malware:

Invoice.zip
cotizaciÃ³n.pdf.gz
Product List.arj
datos bancarios y factura.pdf_____.gz
MV KOTOR.zip
_438590_23485.rar
Payment Advice.eml.zip
OC_5091372486.cab
299388384949111.LzH
Vsl Particulars Dohat Al Khaleej - V1.zip
New-po l48.html
VERIFICATION-PROCESS.HTML
Lista de ordenes de compra.zip
TFL_901307212161.img
SHIPPING ADVISE.lzh
PAYMENT.XLSX.zip
SKM_C335019110.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
103.232.55.10	VietServer Services technology company limited
198.251.79.80	1&1 Ionos Se
103.155.82.221	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
209.97.145.73	DIGITALOCEAN-ASN
81.21.172.152	Doruk Iletisim ve Otomasyon Sanayi ve Ticaret A.S.
103.167.84.243	VietServer Services technology company limited
192.185.46.187	UNIFIEDLAYER-AS-1
159.89.122.235	DIGITALOCEAN-ASN
86.122.125.173	RCS & RDS
165.227.27.58	DIGITALOCEAN-ASN
45.137.22.39	RootLayer Web Services Ltd.
66.154.111.172	PERFORMIVE
185.222.58.116	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: 2021.06.30 22:16:20 -04'00'