Alerta de seguridad cibernética	2CMV22-00268-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2022
Última revisión	18 de enero de 2022

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) 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	79390d74ac5d9e1a37e5ec40d8a9ebd4e51d9598c188904d04556fca5dd4e059	W32/GenKryptik
2	5b0d065a71763b3b4d10e9698b0a52ffac6449dcb5ec164e05ea51f29601d09f	HTML/FishForm
3	b0952410c39724104693f4eb208970f63fce89906412e4b5490285df21f59716	W32/Kryptik
4	322be40c4ec58a0942b584e96e0519acc3387c8f168aa18f366f605ca8849c7c	HTML/FishForm
5	86321a6dc43410bccf207514622720dd9158712ef66d41a19349ab746c6571ac	W32/Agent
6	08f1362639e69b136f04156aa4802a82578a6cb814538b9bd1c28ed94a1b0556	MSIL/GenKryptik
7	ba7ced035fbffe4cba8bdb77fb53afdad9bc238a055b83ac1b6d99cf420001e3	MSIL/GenKryptik
8	04290d8a6419d1015f6808108d0079f39e6e4ca072e41cfbdedcf0ef58c3f54d	FSA/RISK_HIGH
9	7bb1a94f6fd0454907445ac27b8dd60194ed82487ca0d3599e18a3f33880ec32	FSA/RISK_HIGH
10	9a5fed7c3354d80e30b123cb7a3f97be804664e1bc9df62c1f9c2c8735ee06cb	FSA/RISK_HIGH
11	a8f1bc063be81555d043190546e682a81ddd41e6ab3ffe2a773bf31b188e4b26	MSIL/GenKryptik
12	c8acbbd19c3e64861646818a93f77c9f9a66e57e696705375b566280b00584c9	MSIL/GenKryptik
13	0b4d74ec7b25671c083dedc0c3aca60caa8baa7891e1fe670dda1de025c280db	MSIL/Kryptik
14	4338680aa46cc18856d018bf2c8c317fd30749a19ba0fdf578f30fb9a545a7cd	W32/Agent

IoC nombre de archivo

Nombres de archivos con código malicioso:

N°	IP	Etiqueta de sistema autónomo
1	104.168.245.54	HOSTWINDS
2	5.196.78.142	OVH SAS
3	212.192.246.247	AS-SERVERION
4	103.138.109.15	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
5	103.149.13.211	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
6	45.87.62.110	Hyonix LLC
7	64.225.75.252	DIGITALOCEAN-ASN
8	185.222.57.80	RootLayer Web Services Ltd.
9	2.56.59.182	AS-SERVERION

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	88.30.17.247	Telefonica De Espana
2	45.137.22.60	RootLayer Web Services Ltd.
3	45.137.22.124	RootLayer Web Services Ltd.
4	212.193.30.66	Delis LLC
5	212.192.246.74	AS-SERVERION
6	212.192.246.31	AS-SERVERION
7	212.192.241.70	AS-SERVERION
8	200.66.65.23	Megacable Comunicaciones de Mexico, S.A. de C.V.
9	192.227.191.17	AS-COLOCROSSING
10	192.227.191.16	AS-COLOCROSSING
11	185.222.57.93	RootLayer Web Services Ltd.
12	185.222.57.168	RootLayer Web Services Ltd.
13	170.39.212.175	TIER-NET
14	165.22.67.71	DIGITALOCEAN-ASN
15	103.166.183.38	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
16	103.156.93.66	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
17	103.156.91.24	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP
18	212.192.246.250	AS-SERVERION
19	212.192.246.202	AS-SERVERION
20	23.235.223.116	INMOTION

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).
- 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: 2022.01.18 12:41:47 -03'00'