Alerta de seguridad cibernética	2CMV22-00267-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2022
Última revisión	17 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	32d44eccf7bc0c54b56a06ae8613fb336acb58d45bc901e0a6f73c9aad25ed74	MSIL/Kryptik
2	0ced157a9989624a11b713d3f20b9bbaf6d110258d0a5540b69a785263f1b99d	MSIL/CoinMiner
3	654ee607a193d7d3bf2ece94aa9af3478dc4bcc220b54872f3db69ae7dc7fd6f	MSIL/GenKryptik
4	a1578bda0b28e1f7964f006c7b873543114cd0ab6c4e22cae5419ed74a9798a3	MSIL/GenKryptik
5	4f235e7d96f7caf333c0a2cff4f6a860ac7ffca62918e2ddddb64cd10ed3ca94	MSIL/GenKryptik
6	c1391e445b4c4888009f79c513da19ae1f846faaafa2bd4779aa96f8301496bd	MSIL/GenKryptik
7	afaf29e3caa6f81224cc42933d966bf27481c040a8ed88fe9ebb9ba130f668cd	MSIL/CoinMiner
8	e6471b3bf587c95aecd1bb4d4fa6b341797f3e41402c68b91eebd514c1cc2869	MSIL/GenKryptik
9	d40dda28eb3ae29bfb4b88992d3f93dd11c6f909210ddcadfcf9f2aacb196b98	Malware_Generic
10	3c200afc123f4ec9fea4c8e52de22de7229ca0d92c2771db597428c333b28712	MSIL/GenKryptik
11	c9773c2c3db8a09f33f5ba35afee2d036283b0a302cfda97835e721d3e4ac7af	W32/Kryptik
12	3bfedf5f7c37324a394a535d912f3dcb91c5934e843e4b610587906363db3223	MSIL/GenKryptik
13	abfda6109651f6dcfcd50655890aaee6ff1a3ced119d925d20af186677098ccd	Riskware/POC_Iframe_CID
14	e34317bb799040db5ac6d4821d19f6d0b9dba1ed1151217f3af0cd4ff1cde887	W32/Netsky
15	86c54c0fe5904c2fc1991cfc5e286c00f7a399c2ff6a479c9d0193beb4abbb35	Malicious_Behavior
16	7433e1df9f8d45fe6cc344aabee0f86d1d4968b8f910032e2c33fa8a2cf07ddf	HTML/Phishing
17	095f1af7b4e88e0ab825190478738d0e02744cd553ec0e56989c8453a3607520	HTML/Phishing
18	ac53397794de90ff6d4a3f0dca9fe0461e4b84aaa836bd70a94d418f6de7eaca	HTML/Phishing
19	5b72fc57cf22b55a088f83fbf915cf63ff052a40cda34c589ed9e3fa53bbaa28	MSIL/GenKryptik
20	31e8cba4a858778fefd770d93f4e5d41852248c43aae3d264f9f4c75e6d4a31c	HTML/Phishing
21	20f0cfdf5c92f5b86cebde96452ea43997ba12148c2873c7c0c8141aa63e5f44	HTML/Phishing
22	277f40f9cc9dfaba9ec68c0831973f287ff802c47c49d3278aaff86030c63b5a	HTML/Phishing
23	380293b9c765ae6d40351bd50a9bba8e85fcdd8f4f7fe133f422488847f0d158	HTML/Phishing
24	af888cc7c0eddb88526d5445743ad61a669d6c88d94d874eef4f8a876689dad6	MSIL/GenKryptik
25	af246e9ccbefacfb89655a929007c1d2fe37aaefbbe537c020f48e41f2b692d6	MSIL/GenKryptik
26	8a0961654c71edaffd006ad55de0d0c753f160402ad71c6cb89c220907a105ad	MSOffice/CVE_2017_11882

IoC nombre de archivo

Nombres de archivos con código malicioso:

N°	Archivo Malware
1	awb purchase order.html
2	CIEhA8T5.zip
3	CV.7z
4	DJ.arj
5	Document.rar
6	El nuevo pedido esta en la lista..zip
7	IMG_9787.zip
8	Invoice Ref#17-01-2022.rar
9	mail10929.pif
10	message.pif
11	New Oder 2022.gz
12	pago.lzh
13	PO#85012457.gz
14	Purchase order docs. pdf.....zip
15	Purchase Order.xlsx
16	shipping documents.zip
17	SWIFT007_010012022.r00
18	SWIFT007_010012022.r15
19	Tax Inv for Jan-2022 (FS).xlsx
20	update status of order 07G050.r00
21	XVS022-012022.xlsx

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).
- 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.