Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	2CMV22-00303-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2022
Última revisión	29 de junio 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 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
1	d69450df6cd1f5533347c2578c54c49d858c38348ac107c561c5c09f3d07b400	XF/CoinMiner
2	248afc87ac9723820d97227bcf7bf8d621805a7b6fb7044324b90e3d8be0655c	RTF/CVE_2017_11882
3	dc51417399862b1fef10dc05222266931c00bc44c65c8510a9561de0cfa1b300	MSExcel/CVE_2017_11882!exploit
4	5660ee546c3a75b373af637a20ba9daa2ed6f52201b4aaa8c42596004235e835	MSExcel/CVE_2017_11882!exploit
5	97b2a411f2ea38e77a03f9bb502a7a2c123edbfa20adc56b4dfc672c24add829	PossibleThreat
6	3ca51efbc492b4b519050419b8b68b62f74b07ae8d1066aef540c10d5791058d	Malicious_Behavior
7	26b14b79c80d395141bceb2294b3ce8badd977b789158a5890743f2f359c3bd2	Malware_Generic
8	61548e27d883de30704f2569a58b1a2b1be69f8360234f99be013a3a3516b7ec	MSIL/Agent.MJJ!tr
9	22ffaee9a79a9b1537a7195f2460a6156634b6396c757a73b72c76af6d7c3fe5	MSIL/GenKryptik
10	618bbbba4ca1ee491b9a5ed62847124ba166215905a302312e2177cdd700b76b	MSIL/GenKryptik
11	84caa576cdfea20e6e44c709699714026b87dc02c01ec75935a537462be66a57	PossibleThreat
12	af64d169c79c34397382c4a2ec4d8a7db3caa07b2ab3ba40c1c9b1bfb438b46a	XF/CoinMiner
13	d958fe80b1ba071fe95b6c549639070c7a871e743a8a82859734a300dca74915	MSIL/GenKryptik
14	e6bcf73dfd9fb1622830ed694be2c0aea6bac3e1443bb7ce01718cf33cffeff0	HTML/Phishing
15	a8f295b6346e094a388df74c39eec95d5de375729e7d17553b2a0e58dff08182	HTML/Phishing
16	e480a896b459dd9476175411d6bf759cf7e7a962880405deb5f90b0fc6390a99	HTML/Phishing
17	43a817ce7cb5019d22ad0ea7ff45bf56d822d5eb68664a563fcce564f85c1a1b	MSIL/Kryptik
18	588d2be55b6cbc691b19ab1a51b33fe5ad1618c3f5dcc038dd2171a6599cf295	VBA/Agent
19	a96b8cb2c893b776384cae4be4afbf545f3410223724c5a507fe470387035d8a	HTML/Phish
20	d5417dce5fa94a66256cd146db74e502569ab35f3cb7eaf8dd1876958454cc4d	MSIL/GenKryptik
21	c8a2d7fe935322abe5bb782f87bebde4c41c4dfbf655958ee1bedad09bc05474	MSIL/GenKryptik
22	efd7419b4d206b430ac72ba668439db4fa4e593441c0f493bc0945d1b737910e	MSIL/GenKryptik

IoC nombre de archivo

Nombres de archivos con código malicioso:

N°	Nombre
1	mensaje 2135453.xls
2	Escanear_28062022.xls
3	detalles_3142030441.xls
4	R 2806.xls
5	informe_047.xls
6	LYN 2043354.xls
7	archivo 646113.xls
8	paquete_2806.xls
9	PO NO865.doc
10	Mensaje 90365798.xls
11	documento_2806.xls
12	LATCO_773464.xlsx
13	DATOS 2806.xls
14	ESCANEAR 400.xls
15	archivo 0.xls
16	informe_2806.xls
17	ESCANEAR-28062022.xls
18	Info-64808469685.xls
19	Correo_2806.xls
20	DETALLES_2806.xls
21	Info_0657125509.xls
22	102Q_34544.xls
23	detalles_85798133049.xls
24	detalles 2806.xls
25	adjuntos-863134497.xls
26	AWB # Ref 0926317468.pdf.iso
27	lista-2806.xls
28	83 335644216.xls
29	PO_87910219.zip
30	25644022.xls
31	sin ttulo_2806.xls
32	Purchase Order 28th June.img
33	detalles_28062022.xls
34	adjunto-892.xls

35	RZZJY-299.xls
36	nrle-28062022.xls
37	comentarios 021533.xls
38	DOCUMENTO 28062022.xls
39	ARCHIVO-3.xls
40	DHL0038747896.7z
41	04427208.xls
42	cotizaciÃ³n y nuevo pedido.pdf.001
43	Quotation Request28June2022Phnom Penh, Port to EU NGC92728.gz
44	Escanear_38263.xls
45	PO 28.06.2022.xlsx
46	DocuSign_INV089881.htm
47	New Order.rar
48	shipping document.xlsx
49	mp3wav010_Prochilenl_soundmp3_.html
50	vsl particulars & packing list.zip
51	NEW_ORDER_LIST.IMG

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	ASN
1	98.142.233.71	TERRA-NETWORKS-MIAMI	AS 40260
2	94.46.23.48	Almouroltec Servicos De Informatica E Internet Lda	AS 24768
3	92.223.159.2	Fastweb	AS 12874
4	89.252.151.33	Kapteyan Bilisim Teknolojileri San. ve Tic. A.S.	AS 207429
5	86.35.15.78	Orange Romania Communication S.A	AS 9050
6	69.174.99.150	ASN-QUADRANET-GLOBAL	AS 8100
7	45.83.122.239	IT WEB LTD	AS 200313
8	45.61.171.224	Hyonix LLC	AS 213122
9	216.59.16.169	IMMEDION	AS 15085
10	212.36.80.195	OGIC Informatica S.L.	AS 15699
11	207.180.218.28	Contabo GmbH	AS 51167
12	202.55.133.137	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	AS 63737
13	201.76.49.98	Locaweb Servicos de Internet SA	AS 27715
14	201.76.49.49	Locaweb Servicos de Internet SA	AS 27715
15	201.76.49.48	Locaweb Servicos de Internet SA	AS 27715
16	201.76.49.242	Locaweb Servicos de Internet SA	AS 27715
17	201.76.49.224	Locaweb Servicos de Internet SA	AS 27715
18	201.76.49.199	Locaweb Servicos de Internet SA	AS 27715
19	201.76.49.198	Locaweb Servicos de Internet SA	AS 27715
20	201.76.49.177	Locaweb Servicos de Internet SA	AS 27715
21	201.76.49.176	Locaweb Servicos de Internet SA	AS 27715
22	201.76.49.159	Locaweb Servicos de Internet SA	AS 27715
23	201.76.49.149	Locaweb Servicos de Internet SA	AS 27715
24	201.76.49.142	Locaweb Servicos de Internet SA	AS 27715
25	201.76.49.131	Locaweb Servicos de Internet SA	AS 27715
26	201.76.49.123	Locaweb Servicos de Internet SA	AS 27715
27	201.76.49.116	Locaweb Servicos de Internet SA	AS 27715
28	201.76.49.115	Locaweb Servicos de Internet SA	AS 27715
29	200.80.10.72	Locaweb Servicos de Internet SA	AS 27715
30	200.14.80.165	Locaweb Servicos de Internet SA	AS 27715

N°	IP	Etiqueta de sistema autónomo	ASN
31	200.1.126.24	Locaweb Servicos de Internet SA	AS 27715
32	194.87.84.98	Delis LLC	AS 211252
33	189.126.112.58	Locaweb Servicos de Internet SA	AS 27715
34	189.126.112.56	Locaweb Servicos de Internet SA	AS 27715
35	189.126.112.51	Locaweb Servicos de Internet SA	AS 27715
36	189.126.112.33	Locaweb Servicos de Internet SA	AS 27715
37	189.126.112.31	Locaweb Servicos de Internet SA	AS 27715
38	187.95.145.190	Horizons Telecomunicacoes e Tecnologia S.A.	AS 262318
39	185.32.188.2	Sampling Line-servicos E Internet, Lda	AS 62416
40	177.36.34.54	BRASIL TECNOLOGIA E PARTICIPACOES SA	AS 262907
41	164.163.56.10	PALA PABLO FEDERICO	AS 265781
42	154.0.169.134	Afrihost	AS 37611
43	152.89.247.36	combahton GmbH	AS 30823
44	146.190.56.140	DIGITALOCEAN-ASN	AS 14061
45	143.90.14.67	SoftBank Corp.	AS 4725
47	142.44.204.137	OVH SAS	AS 16276
48	120.50.33.23	M1 NET LTD	AS 17547
52	103.167.84.102	VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED	AS 63737
53	103.118.24.195	NSS INTL CO., LTD.	AS 131626
54	200.201.195.236	DC MATRIX INTERNET SA	AS 10733
55	200.195.200.141	Horizons Telecomunicacoes e Tecnologia S.A.	AS 262318
56	195.248.231.195	Data Rush IT Services, S.L.	AS 199581
57	189.126.112.208	Locaweb Servicos de Internet SA	AS 27715
58	189.126.112.164	Locaweb Servicos de Internet SA	AS 27715
59	189.126.112.116	Locaweb Servicos de Internet SA	AS 27715
60	185.102.170.127	Des Capital B.V.	AS 213035

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.