Alerta de seguridad cibernética	2CMV21-00240-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de octubre de 2021
Última revisión	26 de octubre 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), 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	35056762755603176fdd69583d03f154c6b5a7dbac3ae758b9a1d4cd04ff4e32	MSOffice/Agent.GV!tr
2	134d2e46618207db5a72d7ca0fb39310491a5e3c4337dc459d623dbec2beaf06	MSOffice/Scam.2ED7!tr
3	a3d56f9820ec00991790b130b88f0b7fa36f9366b3ac287db58c70c5a4a5dc53	MSOffice/CVE_2017_11882
4	429200fcff319513ff946fae51d5bb4500f969e02f5dcc02bc7333506b77635b	MSIL/GenKryptik.FLEY!tr
5	4fe4931ff2df16ba3943c1380dd21e9c32ce29a708068b3190c10de20b5a1d99	PossibleThreat
6	fbf3874618c8de5a447f5d757b707e6680e83dd6a2edf4a11dcf566de65064e9	PossibleThreat
7	78efeb17c061e887abd631e616e44139a92ffc4d82f709c6cd062c23805cfcb7	
8	1151e2239b24e43cc43e43f1f3ef5241f7ea4831443e7fbf1981e7b2f7b116c8	
9	abd12aba01515d8829dba0e20a08420925265346bf63b0d0f25fa8dd72c33de9	
10	115239f3a4c673dbbcf990b8a81594c350a0e8c7c5216d1ffca4ffc7751d35b5	VBA/Agent.D795!tr
11	1845ebd6aaa37eb8a9665af93db7b53e6133a864ba613a376882107d2b1b582c	MSIL/Agent.AES!tr
12	02775b6ac6554e57854050cd6462a2bb1086a45607b6a5f22b6fb111e6880391	MSIL/Kryptik.ADCZ!tr
13	d3444dae388a8d1671d53edcd75a3ca92a427d0d7db8acfae89e2a92e264812b	MSIL/Agent.AES!tr
14	d7677d8ae3578e42bc4e7802420b14f63eb7ff9425f46c413c57eca2d8420e68	W32/Malicious_Behavior
15	7a4e256a50649d821899a58c8e401b205875027fbd871447f952e2582f4931c1	
16	df20110a040aae764dd95bdfb474fa2f9929d5e78f6280ddc6a9667d18da54cc	MSIL/Agent.AES!tr
17	741b738edb136abc66219d1ad8a4cbdbcc97f99d6ad85539a4881c39a0d62702	MSIL/Agent.AES!tr
18	61fa21c4f1d716dd406241273bd1763af497d919b8008c53f4c85bbbb48d1b64	MSIL/Kryptik.FVA!tr.dldr
19	069cf47ec8964fdae9009421489242faf2be3078b2f986874a3d4f0c67fda0a2	MSIL/Kryptik.FVA!tr.dldr
20	d2a3560a21206f97042705f8716f3b4e05088eaa202c601016d772b6afa73b79	

IoC nombre de archivo

Nombres de archivos con malware:

UOtBQlxt6rYmlyY.exe
SWIFT.rar
RPLTFL024962021.GZ
Proforma Invoice.pdf.z
PO-18102021.xlsx
PO # 11002021.zip
Order Confirmation & payment.,pdf.ppam
NEW ORDER AST 27-28 October.xlsx
Invoice.shtml
IMG_RFQ70103260100057.r12
HO-MA PO-7741.xlsx
HLG 21665-PSI-October -2021.zip
data24422.pif
Copy BL and Debit Note.rar
Bank slip.rar
ADNOC DOCUMENTS.rar
70654 SSEBACT.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.

N°	IP	Etiqueta de sistema autónomo
1	77.247.110.105	ABC Consultancy
2	165.232.135.241	DIGITALOCEAN-ASN
3	142.11.234.209	142.11.234.209
4	185.222.57.168	RootLayer Web Services Ltd.
5	185.222.57.214	RootLayer Web Services Ltd.
6	193.56.29.111	Web Hosted Group Ltd
7	195.242.110.72	Internet It Company Inc
8	212.193.30.87	Des Capital B.V.
9	37.221.113.41	M247 Ltd
10	45.137.22.144	RootLayer Web Services Ltd.
11	45.137.22.49	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: 2021.10.26 08:49:41 -03'00'