Alerta de seguridad cibernética	2CMV21-00191-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de junio de 2021
Última revisión	07 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.

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:

ID	Hash	Tipo Malware
1	48e5957d0051766804f0f0a6503e08ad1748404621e2cc40000a351acb7bf049	MSOffice/Agent.GV!tr
2	de7aa2a14d5e0f7c115416ca88f33b2aefac4e4d9dfb941643a64db60b6f45eb	MSIL/Kryptik.ABHT!tr
3	e479cc72a5c8500bef39e159b9f3b90ba9629a180028f0f80a02274b17a3801c	MSOffice/Agent.GV!tr
4	2f7f1a43ce097e9b4ffaae162eaa6b20f87b4f7b873d7951864978636eedf421	MSOffice/CVE_2017_11882.C!exploit
5	0cd70fd04a01dcb095dac96b68bbffc6a47dc6651030656893f6744278c8926f	Malicious_Behavior.SB
6	8b3499872ce31886294713b699a5c3051ba3ede9bcaaf2a8e54df114725d6308	HTML/Phish.D799!tr
8	c3e1008f5f5bdaa71c41e8fe0ae9615b0de342ddbeac28a0d409b5b004b84a68	Malicious_Behavior.SB
9	07ffbabb575117c731872d2d6cda388f2343fdee55d700f8357263a48c0edabc	HTML/Agent.TA!tr
10	5b52135e0a170eafb2b9479fecbe0591cc14fc3d7cbe6e10d69ab4dd15637dfb	HTML/Phish.BJQ!tr
11	857a20f05d51fb0346fa09c106e7eadb4037f27888e65c56f9688b7cdd00b71f	Malicious_Behavior.SB

IoC nombre de archivo

Nombres de archivos con malware:

POI_0610_36_31.xlsx
PAYMENT FOR MS FOB 3-2027.zip
IMG_0520177609.xlsx
Contract.xlsx
DHL Delivery Documents.pdf.z
DHL Global.html
PO#70877A05777.cab
Purchase Order #0637621.docx
New_Order_Details_BSTWY051221.htm

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
143.244.159.175	DigitalOcean, LLC
143.244.159.163	DigitalOcean, LLC
103.232.53.185	VietServer Services technology company limited
185.222.57.86	RootLayer Web Services Ltd.
128.199.119.198	DigitalOcean, LLC
165.232.146.180	DigitalOcean, LLC
188.166.113.55	DigitalOcean, LLC
162.245.190.75	Quadranet-Global

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: 2021.06.07 10:56:49 -04'00'