Alerta de seguridad cibernética	2CMV21-00171-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de abril de 2021
Última revisión	15 de abril 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 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 y sus usuarios.

El CSIRT de Gobierno 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:

0acc507306ecd1611dd25529edfc2700e540691a6134fbc4ed7f60a4f39c55c7
15766952153a9e11676b5e11bfdd1c456a8b3e4cbd198ed7103f41d974147c33
1f5eab05d75803151d380e314f83814132be888c7a985f403ef7430b2c2e5b2a
21dd819d9eb7c012ab9cf32789bcabcc23cefb43a985b752e1df1b4d4bfc77d3
36f496f8ef4c2987ce15ce583eca5c02c87e15bc58372b5d12e3679ea639915c
5d5010a70fffdbc9a2e229f3cdb33d49d8a37a07f56835a9d4e16b2af8b604e9
69194d64960f6ddbdcc748818b968edeedfc68540ad179a3cb4f3f13f2368f06
7bff738ef69a4dd506b2756139505771dfb37290f256a9f77ce9a5403ce90e2b
9c345ffc9965f975a5c357720e6ee0b95bc07dfc37e61d9ad987476b5c25efd8
ba7935cac92628b2817a4f5722e6b3e639d532e282d9ec3877a3170fb77e41d3
d277995849e24f93dd53f665c59f06d16539d56a11a2e6bebb2397b61c35cdf0
d6d47c457f5d2c398322b919b3af8f635b5f261c255088e2d474922a94302728
db23e995afa20a9f2d33773e61a9983abbc990ff4ab81ae07e9410eb3f9fa4ad
db793419bfd833fe3372878bb5d037daefb29de2b6686b978c84c3c1de6820f2
de1e9817130936360966c279d3455f06d6f2e8168a392530a97a618306d89c0f
f2b3eaa3cb510f72e8ba0b9634dac29624ccfe7a467c78531f77c65a7de5b64b
f53dce28d8632d54070cd42aa0ad8cc7af986aa25588a9f5ab2b90a0400a7f59
f7b378f89cddd83d1629f8eea60468d1d9855221c1e652bacebba1f429a90140

IoC nombre de archivo

Nombres de archivos con malware:

transferenciaPDF.arj
Transferencia140421.zip
doc5566797500PDF.arj
Doc5566797500.zip
AWB_600595460.zip
SPECIFICATION OF REQUIREMENT FOR PORT AGENTS.xlsm
purchase order.html
PURCHASE LIST.zip
Port Agency Team Compliance Standalone Issue.doc
po_5467_FROM Art-Sea Industrial Company Limited
LIST OF PRODUCTS NEEDED.zip
ISS BPS HUB INSTRUCTION TO AGENTS.doc
IMG 8754567778 PDF.rar
HSSE FORM V 1.0.xlsm
Enquiry 042021 Emine INCE_PDF.gz
DHL Delivery Documents.ace

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
89.163.242.168	Myloc managed it ag
84.38.130.192	Dataclub s.a.
62.193.52.152	Celeste sas
45.144.225.82	Des capital b.v.
45.144.225.201	Des capital b.v.
45.137.22.118	Rootlayer web services ltd.
212.159.66.160	British telecommunications plc
206.189.48.231	Digitalocean-asn
185.247.34.165	Flex network sarl
185.121.120.217	Des capital b.v.
168.205.125.1	Brasil digital servicos de informatica e comercio
168.167.3.66	Btc-gate1
164.163.56.8	Pala pablo federico
103.99.1.145	Vietnam posts and telecommunications group

IoC Correo Electrónico

Correo electrónico de donde fue enviado:

ygarcia@macoma.cr
waleed@mageneet.com
urdinola@pollofelizsaltillo.com.mx
redessociales@acciona.com
phlau@art-sea.com
iss.cpsp@iss-shipping.com
info@ic-eg.com
docusign@aw-engineering.com
chusui@tzdegree.com
castro.malu.7@gmail.com
ashkansmk@yahoo.com
admins@support.com
admin@nskmicro.co.jp

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: 2021.04.15 16:25:21 -04'00'