Alerta de seguridad informática	2CMV21-00160-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Marzo de 2021
Última revisión	29 de Marzo 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de malware supuestamente proveniente de la empresa Siflex. El atacante busca persuadir a las personas para descargar el archivo adjunto ejecutarlo.

El mensaje del correo indica que se adjunta la factura proforma del nuevo pedido. El atacante adjunta un archivo comprimido con extensión .ZIP que contiene un archivo .EXE, que al ser ejecutado gatilla la infección del equipo.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Servidores Smtp
[37.26.26.71]

Correo Electrónico
mariaclaradable@gmail.com

Asunto
Solicitud de factura proforma

IoC Archivo Adjunto

Archivos que se encuentran en la amenaza

Nombre : Factura proforma, pedido nuevo.zip
SHA256 : 46772EF430645CB795EC68328B68AE2E3E380BB692596D4FE00DC0CC09F0C717

Nombre : Factura proforma, pedido nuevo.exe
SHA256 : B4B5E6482B3D938EE19066DEB66EE9E886404BE87DBF0C9BD74B5833CFAFB2E7

IoC Comunicación de Red

https://www.joomlas123[.]info/3nop/

bakecakesandmore[.]com
shenglisuoye[.]com
chinapopfactory[.]com
ynlrhd[.]com
liqourforyou[.]com
leonqamil[.]com
meccafon[.]com
online-marketing-strategie[.]biz
rbfxi[.]com
frseyb[.]info
leyu91[.]com
hotsmail[.]today
beepot[.]tech
dunaemmetmobility[.]com
sixpenceworkshop[.]com
incrediblefavorcoaching[.]com
pofo[.]info
yanshudaili[.]com
yellowbrickwedding[.]com
paintpartyblueprint[.]com
capricorn1967[.]com
meucarrapicho[.]com
wv0uoagz0yr[.]biz
yfjbupes[.]com
mindfulinthemadness[.]com
deloslifesciences[.]com
adokristal[.]com
vandergardetuinmeubelshop[.]com
janewagtus[.]com
cloudmorning[.]com
foresteryt01[.]com
accident-law-yer[.]info
rockerdwe[.]com
duftkerzen[.]info
igametalent[.]com
yoursafetraffictoupdates[.]review
jialingjiangpubu[.]com
maximscrapbooking[.]com
20sf[.]info
41230793[.]net
yoghurtberry[.]com
ubkswmpes[.]com
064ewj[.]info
rewsales[.]com
dealsforyou[.]tech
ziruixu[.]com
naehascloud[.]com
smokvape[.]faith
sunflowermoonstudio[.]com
stepgentertainment[.]com
tawbj[.]info
besthappybuds[.]net
koohshoping[.]com
ajikrentcarsurabaya[.]com
jkjohnsroofingfl[.]com
whatsnexttnd[.]com
yoyodvd[.]com
shadowlandswitchery[.]com
pmbnc[.]info
shoppingdrift[.]online
potashdragon[.]com
divorcerefinance[.]guru
wenxiban[.]com
589man[.]com

Imagen del mensaje

Saludos,

Envíenos la factura proforma del nuevo pedido adjunto para el pago por adelantado, haremos el pago lo antes posible,
Saludos

Marie Claire Dablé,
Siflex - Envases flexibles,
Dirección: El Totoral 700, Quilicura, Región Metropolitana, Chile
Número Phine: +56990018634
Correo electrónico: mariaclaradable@gmail.com

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: 2021.03.31 08:21:53 -03'00'