Alerta de seguridad informática	2CMV20-00057-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Marzo de 2020
Última revisión	25 de Marzo de 2020

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 a través de un correo electrónico que utiliza el nombre de la compañía de Defontana. El mensaje del correo indica que fue generado por la emisión de una factura electrónica. En el cuerpo del correo se dispone de un enlace para la descarga de dicha factura, pero al seleccionar el enlace es dirigido a la descarga de un archivo ZIP, el cual contiene un archivo Html que, al ser ejecutado, direcciona a otro sitio descargando de forma automática otro archivo ZIP, el cual al ser descomprimido, permite obtener otro archivo con extensión MSI. Al ser ejecutado, se gatilla un script y se procede a la descarga del malware.

INDICADORES DE COMPROMISOS

Servidor Smtp

[52.228.69.44]
[52.228.64.110]
[52.228.66.239]
[52.228.65.107]
[52.228.57.93]
[13.88.226.51]
[52.228.57.155]
[52.228.23.114]
[52.228.57.234]
[13.88.235.183]

Sender

root@alphafox17[.]borawebservicioscl1[.]com
root@alphafox35[.]borawebservicioscl1[.]com
root@alphafox36[.]borawebservicioscl1[.]com
root@alphafox51[.]borawebservicioscl1[.]com
root@alphafox04[.]borawebservicioscl1[.]com
root@alphafox21[.]borawebservicioscl1[.]com
root@alphafox55[.]borawebservicioscl1[.]com
root@alphafox51[.]borawebservicioscl1[.]com
root@alphafox43[.]borawebservicioscl1[.]com

Asunto

Chilexpress - Tenemos un pedido en nuestro deposito en su nombre

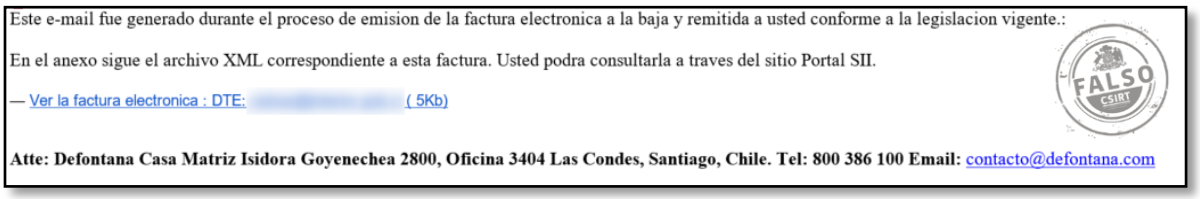
Url's

https[:]//deportes[.]ulpgc[.]es/misc/--/https[:]/www[.]defontana[.]com/cl/?cliente=
https[:]//www[.]ctc[.]com[.]sg/travelclub/sites/acessos/0019203/

Hash MD5

c00f05300eab399ac2ac6a448714aae5
f54c6fa901539fc160b1a7d2e35e3243
0cf3090dd6de2f23bf520f7fea43389c
c9e5ddc25b5651363a41fb89d94aa3d3

IMAGEN DEL MENSAJE



Este e-mail fue generado durante el proceso de emision de la factura electronica a la baja y remitida a usted conforme a la legislacion vigente.:

En el anexo sigue el archivo XML correspondiente a esta factura. Usted podra consultarla a traves del sitio Portal SII.

— Ver la factura electronica : DTE: [redacted] (5Kb)

Atte: Defontana Casa Matriz Isidora Goyenechea 2800, Oficina 3404 Las Condes, Santiago, Chile. Tel: 800 386 100 Email: contacto@defontana.com

RECOMENDACIONES

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- 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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.25 13:01:50 -03'00'