Alerta de seguridad informática	2CMV22-00304-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2022
Última revisión	29 de junio de 2022

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 phishing con malware. El mensaje proviene, supuestamente, por una persona del equipo de trabajo de la víctima, quien adjunta un archivo en formato Excel. Al ejecutarlo, se descargan archivos .dll que son parte del malware que gatilla la infección del equipo.

Familia de malware: Emotet

Observación

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

IoC archivo

Archivos que se encuentran en la amenaza

Nombre: DOCUMENTO_2806.xls
4_29062022.xls
541 375578.xls
958_981664777223.xls
ARCHIVO_28062022.xls
DETALLES_28062022.xls
doc_37.xls
documentación-28062022.xls

SHA256:
d69450df6cd1f5533347c2578c54c49d858c38348ac107c561c5c09f3d07b400

Otros IoC en relación a la amenaza

Nombre: OdUQ1aKjficWdcW[.]dll

SHA256:
c62d72b1a9be3b574d734d3d88bf85d1654b1475e808c8a7f9a2aa0892a65e18

Dominios/URL:

http://kairaliagencies[.]com/data_winning/kWV0fTwakEvHJUKF/

http://corporateissolutions[.]com/administrator/xOEXwASH3uUe/

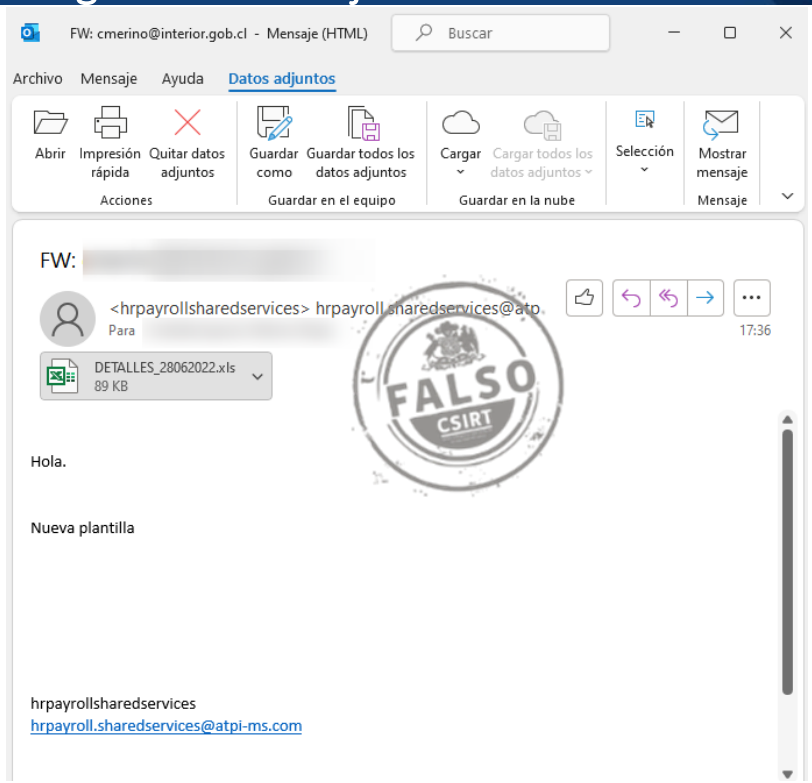
https://curite[.]net/cgi-bin/1IXkx/

https://decorusfinancial.com/wp-content/4E3HMlzDpriI3MZ0fp/

188[.]165.79.151:443
5[.]253.30.17:7080
46[.]101.234.246:8080
157[.]245.111.0:8080
103[.]56.149.105:8080
198[.]199.70.22:8080
93[.]104.209.107:8080
103[.]224.241.74:8080
128[.]199.242.164:8080
139[.]196.72.155:8080
202[.]29.239.162:443
88[.]217.172.165:8080
83[.]229.80.93:8080
37[.]44.244.177:8080
196[.]44.98.190:8080
175[.]126.176.79:8080
36[.]67.23.59:443
104[.]248.225.227:8080
165[.]232.185.110:8080
104[.]244.79.94:443
78[.]47.204.80:443
178[.]62.112.199:8080
37[.]187.114.15:8080
85[.]25.120.45:8080
210[.]57.209.142:8080
103[.]254.12.236:7080
202[.]28.34.99:8080
103[.]41.204.169:8080
116[.]124.128.206:8080
195[.]77.239.39:8080
202[.]134.4.210:7080
128[.]199.217.206:443
165[.]22.254.236:8080
103[.]85.95.4:8080
190[.]107.19.179:443

85[.]214.67.203:8080
118[.]98.72.86:443
54[.]37.228.122:443
190[.]145.8.4:443
139[.]59.80.108:8080
43[.]129.209.178:443
157[.]230.99.206:8080
62[.]171.178.147:8080
46[.]101.98.60:8080
87[.]106.97.83:7080
103[.]71.99.57:8080
103[.]126.216.86:443
188[.]225.32.231:4143
54[.]37.106.167:8080
64[.]227.55.231:8080

Imagen del mensaje



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: 2022.06.29
10:22:24 -04'00'