Alerta de seguridad informática	2CMV22-00299-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de mayo de 2022
Última revisión	24 de mayo 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 indica falsamente a la víctima que se emitió una factura electrónica para su pedido. Para revisarla, el atacante adjunta dos archivos en formato PDF y XML. Al descargarlos y ser ejecutados, se 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

Asunto

✉ Tu factura está disponible - 23/05/2022

Servidor de correo

20.219.143.36	52.252.56.139	20.87.25.20	20.92.73.75
20.92.73.4	20.216.146.59	102.37.105.123	40.74.73.190
40.86.229.141	102.37.113.209	20.216.148.89	20.218.78.105
52.255.60.210	52.242.73.49	20.111.28.70	20.218.77.201
52.242.134.29	20.212.2.222	20.219.253.207	20.24.34.74
20.233.34.228	51.141.0.171	20.115.124.55	20.214.140.134
20.213.245.57	52.189.227.39	52.242.127.139	20.24.36.128
20.106.154.136	52.235.0.108	20.104.217.50	20.104.21.44
52.229.91.43	102.37.104.37	20.87.24.126	51.140.221.185
20.213.248.226	20.216.144.2	20.203.178.120	40.114.70.150
51.13.109.64	20.214.140.126	20.125.196.85	20.219.252.231
20.104.222.49	23.97.61.33	102.37.105.114	20.216.144.52
51.13.76.83	20.219.253.235	102.37.112.175	20.111.31.88
20.92.73.247	20.214.136.141	20.125.196.64	20.216.30.227
40.114.64.138	52.229.64.244	20.104.74.208	20.104.79.7
20.85.229.53	20.221.196.251	20.125.199.63	13.77.60.169
20.216.34.200	20.214.140.220	20.210.141.35	20.227.136.40
20.227.138.13	51.140.228.104	20.89.232.108	52.165.215.108
52.243.103.99	20.125.198.147	20.106.155.109	20.216.150.93
40.127.68.11	52.159.94.58	51.13.88.106	20.203.177.215
52.165.194.202	20.216.148.163	51.140.252.228	20.216.34.184
20.216.58.242	20.214.137.54	52.189.252.214	20.113.160.81
20.92.73.250	20.216.60.24	20.218.75.43	20.203.178.87
52.165.197.10	20.186.12.239	20.92.73.251	52.243.83.198
20.213.240.47	20.203.178.185	20.110.103.134	20.203.138.3
20.216.10.17	52.247.104.50	20.219.252.228	40.74.68.233
20.216.28.170	104.46.197.154	20.218.77.69	20.89.234.105
51.13.69.172	20.233.34.155	51.141.7.229	20.212.187.231
52.229.70.82	40.74.73.210	20.104.78.241	20.218.78.192
52.165.194.47	52.172.235.100	40.74.71.240	20.221.197.236
52.165.194.104	51.141.13.9	40.74.90.216	20.213.245.98
40.86.201.217	51.141.64.85	51.13.103.146	20.104.50.185
20.219.143.36	52.252.56.139	20.87.25.20	20.92.73.75

Correo Electrónico

root@urgencia57.id342032facturadisponible.com	root@urgencia78.id342032facturadisponible.com
root@urgencia12.id342032facturadisponible.com	root@urgencia58.id342032facturadisponible.com
root@urgencia410.id342032facturadisponible.com	root@contacto4.id342032facturadisponible.com
root@urgencia210.id342032facturadisponible.com	root@contacto97.id342032facturadisponible.com
root@urgencia62.id342032facturadisponible.com	root@urgencia21.id342032facturadisponible.com
root@urgencia84.id342032facturadisponible.com	root@contacto910.id342032facturadisponible.com
root@urgencia4.id342032facturadisponible.com	root@contacto94.id342032facturadisponible.com
root@urgencia79.id342032facturadisponible.com	root@contacto2.id342032facturadisponible.com
root@urgencia44.id342032facturadisponible.com	root@contacto7.id342032facturadisponible.com
root@urgencia1.id342032facturadisponible.com	root@urgencia53.id342032facturadisponible.com
root@urgencia91.id342032facturadisponible.com	root@urgencia710.id342032facturadisponible.com
root@urgencia38.id342032facturadisponible.com	root@contacto65.id342032facturadisponible.com
root@urgencia910.id342032facturadisponible.com	root@urgencia36.id342032facturadisponible.com
root@urgencia17.id342032facturadisponible.com	root@contacto96.id342032facturadisponible.com
root@urgencia71.id342032facturadisponible.com	root@contacto19.id342032facturadisponible.com
root@urgencia73.id342032facturadisponible.com	root@contacto41.id342032facturadisponible.com
root@urgencia81.id342032facturadisponible.com	root@contacto98.id342032facturadisponible.com
root@urgencia8.id342032facturadisponible.com	root@contacto92.id342032facturadisponible.com
root@urgencia25.id342032facturadisponible.com	root@contacto43.id342032facturadisponible.com
root@urgencia22.id342032facturadisponible.com	root@urgencia33.id342032facturadisponible.com
root@urgencia64.id342032facturadisponible.com	root@contacto46.id342032facturadisponible.com
root@urgencia810.id342032facturadisponible.com	root@contacto89.id342032facturadisponible.com
root@urgencia110.id342032facturadisponible.com	root@contacto88.id342032facturadisponible.com
root@urgencia68.id342032facturadisponible.com	root@urgencia76.id342032facturadisponible.com
root@urgencia5.id342032facturadisponible.com	root@urgencia99.id342032facturadisponible.com
root@urgencia86.id342032facturadisponible.com	root@contacto57.id342032facturadisponible.com
root@urgencia85.id342032facturadisponible.com	root@urgencia26.id342032facturadisponible.com
root@urgencia92.id342032facturadisponible.com	root@contacto29.id342032facturadisponible.com
root@urgencia45.id342032facturadisponible.com	root@urgencia18.id342032facturadisponible.com
root@urgencia63.id342032facturadisponible.com	root@contacto610.id342032facturadisponible.com
root@urgencia65.id342032facturadisponible.com	root@urgencia55.id342032facturadisponible.com
root@urgencia48.id342032facturadisponible.com	root@contacto23.id342032facturadisponible.com
root@urgencia98.id342032facturadisponible.com	root@contacto56.id342032facturadisponible.com
root@urgencia6.id342032facturadisponible.com	root@urgencia39.id342032facturadisponible.com
root@urgencia93.id342032facturadisponible.com	root@contacto84.id342032facturadisponible.com
root@urgencia51.id342032facturadisponible.com	root@contacto87.id342032facturadisponible.com
root@urgencia9.id342032facturadisponible.com	root@urgencia94.id342032facturadisponible.com
root@urgencia2.id342032facturadisponible.com	root@urgencia19.id342032facturadisponible.com
root@urgencia95.id342032facturadisponible.com	root@urgencia42.id342032facturadisponible.com
root@contacto91.id342032facturadisponible.com	root@urgencia56.id342032facturadisponible.com
root@urgencia75.id342032facturadisponible.com	root@urgencia32.id342032facturadisponible.com
root@urgencia37.id342032facturadisponible.com	root@contacto38.id342032facturadisponible.com
root@contacto39.id342032facturadisponible.com	root@contacto47.id342032facturadisponible.com
root@contacto79.id342032facturadisponible.com	root@contacto73.id342032facturadisponible.com
root@contacto210.id342032facturadisponible.com	root@urgencia89.id342032facturadisponible.com
root@urgencia61.id342032facturadisponible.com	root@contacto58.id342032facturadisponible.com

root@urgencia46.id342032facturadisponible.com	root@contacto72.id342032facturadisponible.com
root@urgencia49.id342032facturadisponible.com	root@urgencia23.id342032facturadisponible.com
root@urgencia97.id342032facturadisponible.com	root@urgencia15.id342032facturadisponible.com
root@contacto44.id342032facturadisponible.com	root@contacto28.id342032facturadisponible.com
root@contacto63.id342032facturadisponible.com	root@contacto68.id342032facturadisponible.com
root@contacto6.id342032facturadisponible.com	root@contacto410.id342032facturadisponible.com
root@contacto93.id342032facturadisponible.com	root@contacto11.id342032facturadisponible.com
root@contacto67.id342032facturadisponible.com	root@urgencia11.id342032facturadisponible.com
root@contacto310.id342032facturadisponible.com	root@contacto110.id342032facturadisponible.com
root@contacto52.id342032facturadisponible.com	root@urgencia13.id342032facturadisponible.com
root@urgencia27.id342032facturadisponible.com	root@contacto83.id342032facturadisponible.com
root@urgencia41.id342032facturadisponible.com	root@contacto26.id342032facturadisponible.com
root@contacto99.id342032facturadisponible.com	root@contacto21.id342032facturadisponible.com
root@contacto5.id342032facturadisponible.com	root@contacto34.id342032facturadisponible.com
root@contacto75.id342032facturadisponible.com	root@contacto78.id342032facturadisponible.com
root@contacto37.id342032facturadisponible.com	root@contacto36.id342032facturadisponible.com
root@urgencia52.id342032facturadisponible.com	root@urgencia34.id342032facturadisponible.com
root@contacto71.id342032facturadisponible.com	root@contacto59.id342032facturadisponible.com
root@urgencia43.id342032facturadisponible.com	root@urgencia72.id342032facturadisponible.com
root@contacto48.id342032facturadisponible.com	root@urgencia59.id342032facturadisponible.com
root@contacto710.id342032facturadisponible.com	root@contacto3.id342032facturadisponible.com
root@contacto51.id342032facturadisponible.com	root@contacto1.id342032facturadisponible.com
root@contacto45.id342032facturadisponible.com	root@urgencia87.id342032facturadisponible.com
root@contacto42.id342032facturadisponible.com	root@urgencia310.id342032facturadisponible.com
root@contacto10.id342032facturadisponible.com	root@urgencia29.id342032facturadisponible.com
root@contacto74.id342032facturadisponible.com	root@urgencia10.id342032facturadisponible.com
root@urgencia88.id342032facturadisponible.com	root@urgencia610.id342032facturadisponible.com
root@contacto64.id342032facturadisponible.com	root@contacto8.id342032facturadisponible.com
root@contacto15.id342032facturadisponible.com	root@contacto17.id342032facturadisponible.com
root@contacto66.id342032facturadisponible.com	root@urgencia82.id342032facturadisponible.com
root@contacto62.id342032facturadisponible.com	root@contacto27.id342032facturadisponible.com
root@urgencia83.id342032facturadisponible.com	root@contacto18.id342032facturadisponible.com
root@contacto85.id342032facturadisponible.com	root@urgencia24.id342032facturadisponible.com
root@urgencia510.id342032facturadisponible.com	root@contacto16.id342032facturadisponible.com
root@contacto53.id342032facturadisponible.com	root@contacto86.id342032facturadisponible.com
root@contacto55.id342032facturadisponible.com	root@contacto810.id342032facturadisponible.com
root@urgencia69.id342032facturadisponible.com	root@contacto31.id342032facturadisponible.com
root@urgencia66.id342032facturadisponible.com	root@contacto25.id342032facturadisponible.com
root@contacto61.id342032facturadisponible.com	root@contacto49.id342032facturadisponible.com
root@contacto24.id342032facturadisponible.com	root@urgencia3.id342032facturadisponible.com
root@contacto22.id342032facturadisponible.com	root@urgencia31.id342032facturadisponible.com
root@contacto82.id342032facturadisponible.com	root@urgencia28.id342032facturadisponible.com
root@contacto54.id342032facturadisponible.com	root@urgencia47.id342032facturadisponible.com
root@contacto81.id342032facturadisponible.com	root@contacto69.id342032facturadisponible.com
root@contacto95.id342032facturadisponible.com	root@contacto76.id342032facturadisponible.com
root@contacto77.id342032facturadisponible.com	root@contacto9.id342032facturadisponible.com
root@urgencia74.id342032facturadisponible.com	root@urgencia16.id342032facturadisponible.com

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: myen8.zip
SHA256: 30f6ded6df72c217f2022e927d38643ac2f472b149c3317c8f3407e3728b4755

Nombre: taot0.msi
SHA256: af2f794adc6060e8c10fa32366d8be97bd3e4dd0a958978cb2315d035124f13e

Nombre: bisur.ahk
SHA256: 49d34cf73009f109860f8f5a3857f205240ecfcc5b1dbffe04a054090b45575e

Nombre: bisur.exe
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: JSON.ahk
SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f

Nombre: mole.ija
SHA256: cb76672f7442b725e4c39db6edb7cc7259469cdd38b3d0f4f90226d981a380a9

Nombre: izjiaybbox.28p
SHA256: 845b03ca416bbc07b1193fb2a678f70e19d4b4698a30ac0c0aba8c635d71eb52

Nombre: t8w1k00836cz8nllqvhhh
SHA256: 0a6af331a1d312b6b8563a5e4e8eaa83a5b933bd6f73f2b03168eb5e262b83d6

Nombre: o0pycr51102i1ll41ha62ggg
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

IoC URLS

hXXp://ip-72-167-45-95.ip.secureserver[.]net/.contacto/?hash=

hXXps://facturadisponible.japanwest.cloudapp.azure[.]com/?hash=

hXXps://www.opvn[.]info/modules/mole.ija

Imagen del mensaje

Imagen Descarga Malware

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.