Alerta de seguridad informática	2CMV22-00298-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2022
Última revisión	12 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 CSIRT de Gobierno. 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 de Gobierno) ha identificado una campaña de phishing con malware. El mensaje indica que se emitió una factura electrónica por un supuesto pedido. Para revisar en detalle el falso documento, el atacante adjunta enlaces para descargar la factura en formato PDF y XML. Al descargar el archivo y ser ejecutado, 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 - 12/05/2022

Servidor de correo

51.142.146.54	51.13.115.37	40.74.80.9	104.43.234.54
20.218.92.14	20.216.36.79	20.48.248.214	20.203.250.247
20.212.226.56	20.221.225.104	52.242.38.73	20.214.204.121
20.213.236.106	20.104.248.216	20.228.128.171	104.43.232.45
20.212.152.176	20.213.242.7	40.86.118.88	20.242.89.40
20.216.172.97	20.124.38.59	20.196.199.86	51.107.209.137
20.242.35.199	20.248.168.155	20.220.70.193	40.123.249.160
40.74.77.191	20.246.124.231	20.219.219.112	20.212.156.78
20.104.87.23	20.236.80.5	40.123.253.206	20.216.175.10
20.113.89.175	40.74.66.104	20.232.12.168	20.216.16.182
20.113.185.199	20.212.6.146	51.13.164.32	20.28.145.195
20.227.161.222	102.37.127.162	20.25.239.218	20.87.15.127
20.110.6.157	20.214.136.114	102.37.118.126	20.196.217.64
51.140.227.24	20.113.153.102	40.74.77.54	20.220.78.29
40.74.66.187	51.141.117.26	20.74.254.220	20.196.216.103
104.43.238.89	20.236.80.118	51.142.145.91	102.37.124.118
51.140.228.47	20.113.187.253	102.37.114.97	20.29.87.124
20.221.219.1	52.159.82.96	191.239.182.49	20.213.126.53
51.141.13.137	20.212.5.141	52.229.65.40	51.141.118.127
168.61.150.154	20.79.249.67	51.13.70.62	20.211.16.215
20.221.225.209	20.207.201.28	20.216.172.191	20.219.11.231
20.228.249.99	20.98.232.63	20.113.156.134	20.214.201.98
20.230.44.202	20.74.241.242	51.142.146.79	20.212.157.205
20.212.159.234	20.87.10.48	20.233.37.79	20.233.37.184
20.218.74.157	20.207.200.197	20.216.170.161	40.80.95.59
20.113.166.120	52.142.166.37	20.227.160.206	20.212.1.238
20.220.65.152	40.69.102.106	20.28.150.199	20.216.173.36
20.203.254.101	20.116.56.241	20.89.237.19	20.193.245.232
20.214.201.225	51.13.100.0	20.29.86.50	20.216.171.183
20.248.169.248	20.89.236.226	51.120.90.3	20.213.78.247
51.13.166.15	51.141.99.231	20.214.136.9	52.159.102.186
20.203.249.15	20.24.31.2	20.210.142.108	20.219.217.242
51.13.167.206	20.110.87.175	20.216.168.0	40.83.49.245

20.219.217.12	51.13.99.172	51.120.89.125	20.48.248.47
20.220.68.124	20.213.246.74	52.229.105.212	52.242.35.190
20.233.7.107	20.216.27.66	20.216.32.223	20.248.175.18
20.233.7.196	20.113.167.241	20.213.243.221	40.74.80.10
20.221.217.44	20.227.162.55	20.214.185.84	20.113.160.89
20.227.163.102	20.25.221.33	52.243.102.255	20.113.92.74
20.196.202.243	20.116.56.255	52.189.220.124	20.124.209.32
20.232.132.213	20.199.111.240	20.216.34.1	20.203.177.232
52.242.20.35	20.89.239.15	52.165.234.105	20.220.78.168
20.228.250.56	20.214.187.88	20.115.15.41	102.37.120.175
40.123.252.87	40.122.240.30	51.13.72.116	20.120.3.79
40.74.77.180	20.242.118.63	20.25.114.36	52.165.39.67
20.216.169.72	52.142.146.239	20.74.249.252	20.214.186.168
13.73.107.244	20.221.218.71	20.29.86.149	20.203.180.44
20.242.7.123	20.242.96.115	20.207.206.207	20.207.201.150
51.120.81.193	51.141.121.98	20.207.202.2	20.116.58.147
20.228.251.208	20.24.155.235	20.104.227.196	20.216.19.65
20.213.244.157	52.229.64.138	102.37.103.37	20.212.188.221
20.212.0.110	51.141.106.10	20.196.221.156	20.196.204.160
20.212.153.92	20.219.14.118	102.37.122.112	20.227.162.219
51.142.166.104	20.199.110.121	20.74.240.26	20.216.38.160
20.208.43.12	51.141.124.195	20.220.72.179	20.25.222.177
20.203.254.63	20.110.135.255	20.210.138.146	20.248.174.96
20.214.204.119	20.104.230.209	20.213.245.252	20.28.151.9
20.113.165.192	20.87.14.196	20.120.111.9	20.228.254.253
20.214.200.47	20.216.172.76	20.207.200.66	13.77.46.213
20.212.156.78	20.219.51.199	20.119.252.145	20.25.219.220
20.25.12.135	20.233.3.174	40.69.132.18	20.213.246.74
40.87.42.132	51.13.67.35	20.203.252.164	51.141.110.211
40.69.98.32	20.25.114.5	20.213.232.155	20.116.57.93
13.70.134.177	20.233.4.37	20.104.226.249	20.203.178.75
20.227.163.240	20.220.75.230	20.196.204.204	20.232.118.31
20.242.64.149	20.29.83.121	102.133.190.149	20.227.162.223
20.212.153.254	20.220.77.175	20.203.126.197	20.216.172.15
20.214.200.13	20.236.82.148	23.101.237.156	20.220.75.35
51.142.146.160	20.89.237.143	20.231.120.66	20.230.21.102
20.242.71.134	20.214.138.224	20.104.251.234	20.219.8.117
102.37.114.41	40.69.141.99	102.133.190.149	20.113.166.175
20.248.171.87	20.212.3.120	40.74.77.252	20.236.81.66
51.140.205.87	20.213.235.5	20.203.249.53	20.116.69.90
20.216.169.7	20.115.8.103	20.220.66.126	20.248.184.105
20.113.166.162	20.89.248.238	20.219.220.180	20.211.16.229
20.74.254.193	20.214.185.95	20.213.236.84	20.214.136.114
40.74.68.214	20.203.248.63	52.242.24.134	20.113.134.65
20.212.113.145	40.112.61.180	20.219.216.239	
104.208.31.7	52.189.214.167	20.242.71.28	
40.123.251.114	20.213.245.136	20.109.121.195	
20.216.173.72	20.199.108.184	20.210.140.210	

Correo Electrónico

root@comprobante58.id7099237facturaeletronica.org	root@factura93.id7099237facturaeletronica.org
root@comprobante22.id7099237facturaeletronica.org	root@factura86.id7099237facturaeletronica.org
root@comprobante37.id7099237facturaeletronica.org	root@comprobante42.id7099237facturaeletronica.org
root@factura3.id7099237facturaeletronica.org	root@factura32.id7099237facturaeletronica.org
root@comprobante33.id7099237facturaeletronica.org	root@factura10.id7099237facturaeletronica.org
root@comprobante3.id7099237facturaeletronica.org	root@factura710.id7099237facturaeletronica.org
root@comprobante66.id7099237facturaeletronica.org	root@factura110.id7099237facturaeletronica.org
root@comprobante83.id7099237facturaeletronica.org	root@comprobante65.id7099237facturaeletronica.org
root@factura37.id7099237facturaeletronica.org	root@comprobante410.id7099237facturaeletronica.org
root@comprobante25.id7099237facturaeletronica.org	root@comprobante86.id7099237facturaeletronica.org
root@comprobante21.id7099237facturaeletronica.org	root@gobierno36.id420238facturaeletronica.com
root@factura4.id7099237facturaeletronica.org	root@gobierno94.id420238facturaeletronica.com
root@comprobante68.id7099237facturaeletronica.org	root@gobierno78.id420238facturaeletronica.com
root@comprobante51.id7099237facturaeletronica.org	root@gobierno29.id420238facturaeletronica.com
root@comprobante89.id7099237facturaeletronica.org	root@gobierno53.id420238facturaeletronica.com
root@factura66.id7099237facturaeletronica.org	root@gobierno47.id420238facturaeletronica.com
root@comprobante52.id7099237facturaeletronica.org	root@gobierno210.id420238facturaeletronica.com
root@comprobante49.id7099237facturaeletronica.org	root@gobierno42.id420238facturaeletronica.com
root@comprobante54.id7099237facturaeletronica.org	root@gobierno38.id420238facturaeletronica.com
root@factura68.id7099237facturaeletronica.org	root@gobierno26.id420238facturaeletronica.com
root@comprobante41.id7099237facturaeletronica.org	root@factura55.id420238facturaeletronica.com
root@factura74.id7099237facturaeletronica.org	root@gobierno64.id420238facturaeletronica.com
root@comprobante64.id7099237facturaeletronica.org	root@factura89.id420238facturaeletronica.com
root@comprobante34.id7099237facturaeletronica.org	root@gobierno96.id420238facturaeletronica.com
root@comprobante29.id7099237facturaeletronica.org	root@factura52.id420238facturaeletronica.com
root@comprobante26.id7099237facturaeletronica.org	root@gobierno59.id420238facturaeletronica.com
root@factura410.id7099237facturaeletronica.org	root@factura48.id420238facturaeletronica.com
root@comprobante19.id7099237facturaeletronica.org	root@factura35.id420238facturaeletronica.com
root@comprobante76.id7099237facturaeletronica.org	root@factura91.id420238facturaeletronica.com
root@factura16.id7099237facturaeletronica.org	root@gobierno85.id420238facturaeletronica.com
root@factura92.id7099237facturaeletronica.org	root@gobierno55.id420238facturaeletronica.com
root@comprobante11.id7099237facturaeletronica.org	root@gobierno31.id420238facturaeletronica.com
root@factura96.id7099237facturaeletronica.org	root@gobierno62.id420238facturaeletronica.com
root@factura54.id7099237facturaeletronica.org	root@factura92.id420238facturaeletronica.com
root@factura48.id7099237facturaeletronica.org	root@factura3.id420238facturaeletronica.com
root@factura82.id7099237facturaeletronica.org	root@factura810.id420238facturaeletronica.com
root@factura81.id7099237facturaeletronica.org	root@gobierno22.id420238facturaeletronica.com
root@comprobante47.id7099237facturaeletronica.org	root@factura9.id420238facturaeletronica.com
root@factura8.id7099237facturaeletronica.org	root@gobierno44.id420238facturaeletronica.com
root@comprobante72.id7099237facturaeletronica.org	root@factura37.id420238facturaeletronica.com
root@factura75.id7099237facturaeletronica.org	root@gobierno8.id420238facturaeletronica.com
root@factura41.id7099237facturaeletronica.org	root@gobierno810.id420238facturaeletronica.com
root@factura78.id7099237facturaeletronica.org	root@gobierno76.id420238facturaeletronica.com
root@comprobante98.id7099237facturaeletronica.org	root@factura69.id420238facturaeletronica.com
root@comprobante81.id7099237facturaeletronica.org	root@gobierno61.id420238facturaeletronica.com
root@comprobante2.id7099237facturaeletronica.org	root@gobierno510.id420238facturaeletronica.com

root@factura29.id7099237facturaeletronica.org	root@gobierno45.id420238facturaeletronica.com
root@comprobante62.id7099237facturaeletronica.org	root@gobierno610.id420238facturaeletronica.com
root@factura91.id7099237facturaeletronica.org	root@gobierno57.id420238facturaeletronica.com
root@factura77.id7099237facturaeletronica.org	root@gobierno33.id420238facturaeletronica.com
root@factura5.id7099237facturaeletronica.org	root@factura410.id420238facturaeletronica.com
root@comprobante38.id7099237facturaeletronica.org	root@gobierno54.id420238facturaeletronica.com
root@comprobante35.id7099237facturaeletronica.org	root@factura57.id420238facturaeletronica.com
root@comprobante55.id7099237facturaeletronica.org	root@gobierno5.id420238facturaeletronica.com
root@comprobante15.id7099237facturaeletronica.org	root@gobierno52.id420238facturaeletronica.com
root@comprobante110.id7099237facturaeletronica.org	root@gobierno69.id420238facturaeletronica.com
root@comprobante710.id7099237facturaeletronica.org	root@factura33.id420238facturaeletronica.com
root@comprobante210.id7099237facturaeletronica.org	root@gobierno98.id420238facturaeletronica.com
root@comprobante79.id7099237facturaeletronica.org	root@gobierno10.id420238facturaeletronica.com
root@comprobante32.id7099237facturaeletronica.org	root@factura58.id420238facturaeletronica.com
root@factura73.id7099237facturaeletronica.org	root@factura86.id420238facturaeletronica.com
root@factura71.id7099237facturaeletronica.org	root@factura96.id420238facturaeletronica.com
root@factura45.id7099237facturaeletronica.org	root@factura76.id420238facturaeletronica.com
root@factura28.id7099237facturaeletronica.org	root@factura82.id420238facturaeletronica.com
root@factura9.id7099237facturaeletronica.org	root@factura45.id420238facturaeletronica.com
root@comprobante69.id7099237facturaeletronica.org	root@factura62.id420238facturaeletronica.com
root@comprobante36.id7099237facturaeletronica.org	root@factura41.id420238facturaeletronica.com
root@comprobante77.id7099237facturaeletronica.org	root@gobierno410.id420238facturaeletronica.com
root@comprobante59.id7099237facturaeletronica.org	root@gobierno89.id420238facturaeletronica.com
root@comprobante61.id7099237facturaeletronica.org	root@gobierno710.id420238facturaeletronica.com
root@comprobante96.id7099237facturaeletronica.org	root@factura65.id420238facturaeletronica.com
root@factura13.id7099237facturaeletronica.org	root@gobierno37.id420238facturaeletronica.com
root@comprobante53.id7099237facturaeletronica.org	root@factura1.id420238facturaeletronica.com
root@comprobante5.id7099237facturaeletronica.org	root@factura75.id420238facturaeletronica.com
root@comprobante28.id7099237facturaeletronica.org	root@gobierno81.id420238facturaeletronica.com
root@factura89.id7099237facturaeletronica.org	root@gobierno73.id420238facturaeletronica.com
root@comprobante87.id7099237facturaeletronica.org	root@gobierno110.id420238facturaeletronica.com
root@comprobante310.id7099237facturaeletronica.org	root@factura72.id420238facturaeletronica.com
root@factura61.id7099237facturaeletronica.org	root@factura26.id420238facturaeletronica.com
root@comprobante95.id7099237facturaeletronica.org	root@factura4.id420238facturaeletronica.com
root@comprobante8.id7099237facturaeletronica.org	root@gobierno7.id420238facturaeletronica.com
root@factura53.id7099237facturaeletronica.org	root@factura13.id420238facturaeletronica.com
root@comprobante74.id7099237facturaeletronica.org	root@factura18.id420238facturaeletronica.com
root@comprobante31.id7099237facturaeletronica.org	root@factura74.id420238facturaeletronica.com
root@factura85.id7099237facturaeletronica.org	root@gobierno11.id420238facturaeletronica.com
root@factura51.id7099237facturaeletronica.org	root@factura46.id420238facturaeletronica.com
root@comprobante39.id7099237facturaeletronica.org	root@gobierno97.id420238facturaeletronica.com
root@comprobante6.id7099237facturaeletronica.org	root@factura73.id420238facturaeletronica.com
root@factura52.id7099237facturaeletronica.org	root@factura68.id420238facturaeletronica.com
root@comprobante10.id7099237facturaeletronica.org	root@gobierno71.id420238facturaeletronica.com
root@factura15.id7099237facturaeletronica.org	root@gobierno16.id420238facturaeletronica.com
root@comprobante45.id7099237facturaeletronica.org	root@factura54.id420238facturaeletronica.com
root@factura58.id7099237facturaeletronica.org	root@factura36.id420238facturaeletronica.com
root@factura64.id7099237facturaeletronica.org	root@factura85.id420238facturaeletronica.com

root@factura36.id7099237facturaeletronica.org	root@gobierno310.id420238facturaeletronica.com
root@factura46.id7099237facturaeletronica.org	root@comprobante73.id7099237facturaeletronica.org
root@factura18.id7099237facturaeletronica.org	root@factura7.id7099237facturaeletronica.org
root@comprobante88.id7099237facturaeletronica.org	root@factura87.id7099237facturaeletronica.org
root@comprobante27.id7099237facturaeletronica.org	root@comprobante46.id7099237facturaeletronica.org
root@comprobante23.id7099237facturaeletronica.org	root@factura17.id7099237facturaeletronica.org
root@comprobante810.id7099237facturaeletronica.org	root@comprobante78.id7099237facturaeletronica.org
root@factura35.id7099237facturaeletronica.org	root@factura610.id7099237facturaeletronica.org
root@factura43.id7099237facturaeletronica.org	root@comprobante610.id7099237facturaeletronica.org
root@factura76.id7099237facturaeletronica.org	root@factura94.id7099237facturaeletronica.org
root@factura62.id7099237facturaeletronica.org	root@comprobante91.id7099237facturaeletronica.org
root@comprobante71.id7099237facturaeletronica.org	root@comprobante4.id7099237facturaeletronica.org
root@factura49.id7099237facturaeletronica.org	root@factura84.id420238facturaeletronica.com
root@factura55.id7099237facturaeletronica.org	root@factura17.id420238facturaeletronica.com
root@comprobante93.id7099237facturaeletronica.org	root@gobierno910.id420238facturaeletronica.com
root@factura72.id7099237facturaeletronica.org	root@gobierno72.id420238facturaeletronica.com
root@factura98.id7099237facturaeletronica.org	root@factura43.id420238facturaeletronica.com
root@comprobante44.id7099237facturaeletronica.org	root@gobierno77.id420238facturaeletronica.com
root@comprobante97.id7099237facturaeletronica.org	root@gobierno93.id420238facturaeletronica.com
root@comprobante85.id7099237facturaeletronica.org	root@factura610.id420238facturaeletronica.com
root@factura88.id7099237facturaeletronica.org	root@factura15.id420238facturaeletronica.com
root@comprobante57.id7099237facturaeletronica.org	root@gobierno56.id420238facturaeletronica.com
root@comprobante92.id7099237facturaeletronica.org	root@factura14.id420238facturaeletronica.com
root@factura27.id7099237facturaeletronica.org	root@factura56.id420238facturaeletronica.com
root@factura44.id7099237facturaeletronica.org	root@gobierno68.id420238facturaeletronica.com
root@factura910.id7099237facturaeletronica.org	root@factura69.id7099237facturaeletronica.org
root@comprobante7.id7099237facturaeletronica.org	root@comprobante18.id7099237facturaeletronica.org
root@comprobante24.id7099237facturaeletronica.org	root@factura1.id7099237facturaeletronica.org
root@comprobante510.id7099237facturaeletronica.org	root@factura38.id7099237facturaeletronica.org
root@factura83.id7099237facturaeletronica.org	root@comprobante75.id7099237facturaeletronica.org
root@comprobante1.id7099237facturaeletronica.org	root@comprobante910.id7099237facturaeletronica.org
root@factura7.id420238facturaeletronica.com	root@factura810.id7099237facturaeletronica.org
root@factura110.id420238facturaeletronica.com	root@factura25.id7099237facturaeletronica.org
root@gobierno87.id420238facturaeletronica.com	root@factura79.id7099237facturaeletronica.org
root@factura63.id420238facturaeletronica.com	root@factura34.id7099237facturaeletronica.org
root@factura93.id420238facturaeletronica.com	root@comprobante84.id7099237facturaeletronica.org
root@gobierno79.id420238facturaeletronica.com	root@comprobante12.id7099237facturaeletronica.org
root@gobierno88.id420238facturaeletronica.com	root@factura47.id7099237facturaeletronica.org
root@gobierno2.id420238facturaeletronica.com	root@factura57.id7099237facturaeletronica.org
root@factura910.id420238facturaeletronica.com	root@factura2.id7099237facturaeletronica.org
root@factura49.id420238facturaeletronica.com	root@factura42.id7099237facturaeletronica.org
root@factura87.id420238facturaeletronica.com	root@factura56.id7099237facturaeletronica.org
root@factura8.id420238facturaeletronica.com	root@comprobante63.id7099237facturaeletronica.org
root@gobierno75.id420238facturaeletronica.com	root@gobierno63.id420238facturaeletronica.com
root@factura24.id420238facturaeletronica.com	root@gobierno86.id420238facturaeletronica.com
root@factura27.id420238facturaeletronica.com	root@gobierno24.id420238facturaeletronica.com
root@factura81.id420238facturaeletronica.com	root@factura16.id420238facturaeletronica.com
root@factura66.id420238facturaeletronica.com	root@factura710.id420238facturaeletronica.com

root@gobierno6.id420238facturaeletronica.com	root@factura28.id420238facturaeletronica.com
root@factura77.id420238facturaeletronica.com	root@gobierno41.id420238facturaeletronica.com
root@factura98.id420238facturaeletronica.com	root@gobierno58.id420238facturaeletronica.com
root@factura78.id420238facturaeletronica.com	root@factura38.id420238facturaeletronica.com
root@factura83.id420238facturaeletronica.com	root@gobierno18.id420238facturaeletronica.com
root@factura61.id420238facturaeletronica.com	root@factura79.id420238facturaeletronica.com
root@factura53.id420238facturaeletronica.com	root@factura10.id420238facturaeletronica.com
root@factura51.id420238facturaeletronica.com	root@gobierno1.id420238facturaeletronica.com
root@factura31.id420238facturaeletronica.com	root@factura47.id420238facturaeletronica.com
root@gobierno95.id420238facturaeletronica.com	root@gobierno65.id420238facturaeletronica.com
root@gobierno74.id420238facturaeletronica.com	root@factura510.id420238facturaeletronica.com
root@gobierno92.id420238facturaeletronica.com	root@gobierno21.id420238facturaeletronica.com
root@factura88.id420238facturaeletronica.com	root@gobierno48.id420238facturaeletronica.com
root@factura44.id420238facturaeletronica.com	root@factura31.id7099237facturaeletronica.org
root@gobierno84.id420238facturaeletronica.com	root@factura65.id7099237facturaeletronica.org
root@factura5.id420238facturaeletronica.com	root@comprobante17.id7099237facturaeletronica.org
root@factura71.id420238facturaeletronica.com	

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: factura.zip
SHA256: e8fd3f933680a7e12ef159da9eaec83ad885fe2ac9361336dcc6a4ff60dbf3a6

Nombre: nenz7.msi
SHA256: 1bb3877853e6b68409b2c8b5c95c8a580fd1504d16a089ffe08d60f8b6dbceb7

Nombre: JSON.ahk
SHA256: bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f

Nombre: plpl09.exe
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: plpl09.ahk
SHA256: af91374748aca3eefc61de4fedb6595c5ce09e09295c740498238e2b0d25f765

Nombre: serpes0909.goq
SHA256: c012d97f6084740fd35b7b927445364e2e2c2e1b5ff0d6836698b4fffb073ef7

Nombre: ET1oYl7ZJvRigu1zggg
SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4

Nombre: cQOTDjyiEt.asx
SHA256: fd69295a7000348f1dead438a522424db213a1765bbc4679e03040474223a5f2

Nombre: hvh4046M87Q2m4jdqDC5hhh
SHA256: 4a493c35de59fdd1b5f102b2925fea869df8a1510db0cadcd053070a97a9b945

IoC URL

hXXps://www.upec.edu[.]ec/subsitios/ciden/modules/idcliente/

hXXps://fi-ac[.]it/modules/mod_up/.factura/

hXXps://special.arabi21[.]com/russiaWP/serpes0909.goq

Imagen del mensaje

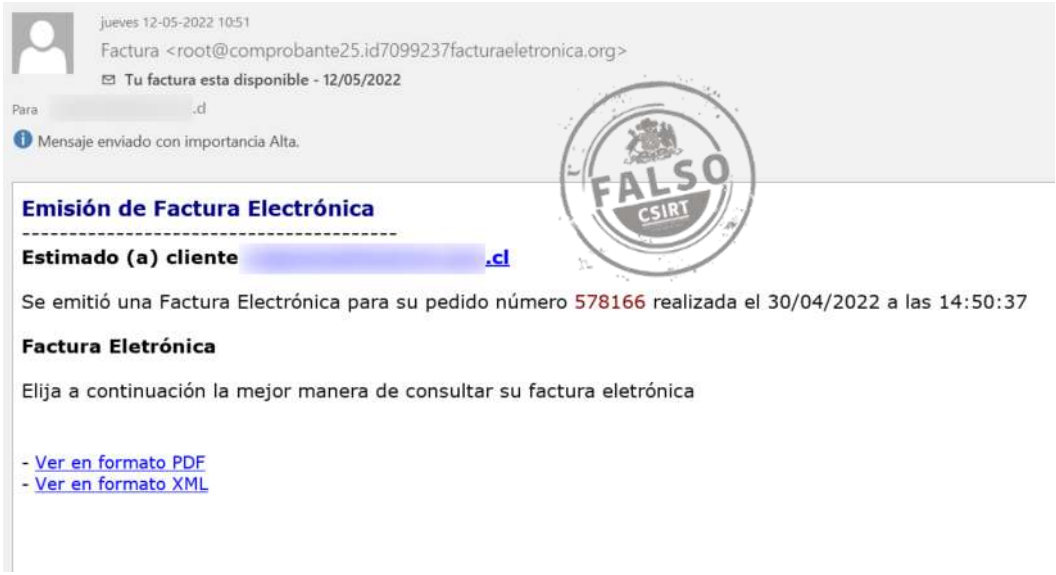

Imagen descarga malware

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.