Alerta de Seguridad Informática (2CMV-00020-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

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 del Gobierno de Chile (CSIRT), ha identificado una campaña de Phishing con el Malware Ursinf, un troyano que es conocido por el robo de credenciales bancarias y cuentas en línea.

A pesar que los correos electrónicos vienen en idioma italiano, se recomienda tener precaución. Los delincuentes buscan engañar indicando que existe una declaración que puede ser visualizado presionando el link adjunto. Cuando la persona hace clic en el hipervínculo es dirigido a una página web de Google Drive, que abre otra página falsa donde muestra un documento en formato PDF e incentiva a descargarlo. Al ser descargado se desencadena la infección ejecutando archivos Visual Basic.

Indicadores de compromisos

Url's:

https[:]//lloydsbankdocs[.]com/cvrpdy?ijf=2
https[:]//drive[.]google[.]com/file/d/1_Q5Lkoid9NcdQpIBswO2YQbzQRXvJOUJ/view
https[:]//drive[.]google[.]com/file/d/11vKk29GWmkOS-UX-WC4aB0vHAnuTQ1-S/view
https[:]//drive[.]google[.]com/file/d/14NeAnosm7k0vQkZXuyXnliaDUPzV1ZDX/view
https[:]//drive[.]google[.]com/file/d/14S5GemcsseoohRdKZNzhtZzwsoYemun-/view
https[:]//drive[.]google[.]com/file/d/15AHTraWOtG0gsXhK_WXZgJVyncRJcYRp/view
https[:]//drive[.]google[.]com/file/d/16X678tia_0tZflKfieDU_7-Yuu8_XMpY/view
https[:]//drive[.]google[.]com/file/d/191jtLZWuZQWRSmT5nXLsLcQwJofRZux9/view
https[:]//drive[.]google[.]com/file/d/1ABO3yKuyjFfb4xnTq6xiLa3fqq_sD_e2/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1ANDOq21XbiNX8JvUDQMscQlmyozdsqOC/view
https[:]//drive[.]google[.]com/file/d/1BKxqdNzTJIDvju6FhOQPQv6HS75al3xV/view
https[:]//drive[.]google[.]com/file/d/1BqdJGuBi8IbkkDQ7ygD_0B7EGh9aK75G/view
https[:]//drive[.]google[.]com/file/d/1bzXLzbvTNW9S619ojeoEF3MYd9yHqpZL/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1Cl3uyws5f8BwaI0AXiipy6NZNu9Mw0Ur/view
https[:]//drive[.]google[.]com/file/d/1CMte-uCMKP90_J61ML3PGNJdItyMH8nt/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1dOjE-5LzJKEJcQSMxURdVQhdtjbeyBmM/view
https[:]//drive[.]google[.]com/file/d/1dP6mte6dmQ_hMN67LK55LcL4wNry7SMz/view
https[:]//drive[.]google[.]com/file/d/1DYecZlU_RvdKuFDSAOd2jKV1IiwJboyk/view
https[:]//drive[.]google[.]com/file/d/1e9cHbR54Y4AHa4k_EGbE_WfelDBmiBN2/view
https[:]//drive[.]google[.]com/file/d/1F2wj8vxZ9JU_fgWHXqjT8NWqACe0PyYA/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1fpLbimtZRijR82qp7CiBducuy5bAqhCF/view
https[:]//drive[.]google[.]com/file/d/1Fv9FxCX7qC99J-6knmuQN82RdILDMTwZ/view
https[:]//drive[.]google[.]com/file/d/1FvIQh83NI5MoUWwJxs2neVmz9t5MPaWm/view
https[:]//drive[.]google[.]com/file/d/1hlrDIpWZf32aNIyi1ZzBr0toCsPR3EL6/view
https[:]//drive[.]google[.]com/file/d/1HWz773oga64XmnICq0VVnU6jb1MLJbUb/view
https[:]//drive[.]google[.]com/file/d/1JiAdyGeVjriku2-FDx94Z6avgGPmL8eO/view
https[:]//drive[.]google[.]com/file/d/1JwS5SP_2FPYPr-3K03e_km0eM4EWHs3i/view
https[:]//drive[.]google[.]com/file/d/1JXdQsuO9U_BEzRaZzGJ1cIySNeC9sxyD/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1K256YS9VugToSRV_Cyo_J2iXN1RGr3ZE/view
https[:]//drive[.]google[.]com/file/d/1Ki7qiSGEK0OENSkqJGI_gfzNCydxpFPH/view

https[:]//drive[.]google[.]com/file/d/1kJfFvE2uwxI4BwgPKOKKcedqx-pii534/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1KOL-qV5airJyp_XOxRuuI6HG2LSalGVr/view
https[:]//drive[.]google[.]com/file/d/1kqMAAbyaQ6ocZNGO8Q8JEfTWuGs-Owdn/view
https[:]//drive[.]google[.]com/file/d/1LDS5Z5qFlPmGI9rIs03nCr8qrx3i-y6u/view
https[:]//drive[.]google[.]com/file/d/1MJ-f7lnuNt7Hg2yDqHjjmi9o82WieixH/view
https[:]//drive[.]google[.]com/file/d/1mqP6odmy6rLF2flOQD-5vG2Q02pJwCHJ/view
https[:]//drive[.]google[.]com/file/d/1N75--pFvPJ0ioJ0B8qUce-rLR8BPpMq0/view
https[:]//drive[.]google[.]com/file/d/1ocw1saK5JnRPnubspwtjZLAgKU7WS4y1/view
https[:]//drive[.]google[.]com/file/d/1OVi-JDvFTZIa8hQbDuZ8x4fAx1VV18-C/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1PaNr6n-6t0h6otOXjDF1089WMnzmDG6g/view
https[:]//drive[.]google[.]com/file/d/1pCZBj5k2zBH7YfPOqHE2tpCYLBs1olD8/view
https[:]//drive[.]google[.]com/file/d/1PupBY4-UzrR7vFaJIEP6nqnkOhY-rtR9/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1SnQWFHdp4uz_luR8GORyR38Gal22cLpP/view
https[:]//drive[.]google[.]com/file/d/1soMy-uY_QfO6Jd4jmLiVaXxNeBgjJiCO/view
https[:]//drive[.]google[.]com/file/d/1SRHL-OiV3ReLr3r4_25BzcQOWLvic44C/view
https[:]//drive[.]google[.]com/file/d/1TUckjTX561892lSqoF9bSW2FwUI5avms/view
https[:]//drive[.]google[.]com/file/d/1usDKqih1yf-HuHWdcudNhecHLeEi7Vad/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1vA-7OHAuTE88Nw55I58R_dU0d7cKxbEI/view
https[:]//drive[.]google[.]com/file/d/1XEbshjpK77jlqicB1J_Wt3d7emyNROwE/view
https[:]//drive[.]google[.]com/file/d/1xjEmoXAEhrwxJzi1AVZ5CVpefUc8OB_W/view
https[:]//drive[.]google[.]com/file/d/1Ybw86E6eApHHfeSiku6OdE1x0KTBuh20/view
https[:]//drive[.]google[.]com/file/d/1yEAI3i9LYlBWZvkm0KOGbAW8L_GX03Ik/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1YgJkLtYI3DKxkRmkYCCHfAGma2GIpVJA/view
https[:]//drive[.]google[.]com/file/d/1ZA9uZJ0b9ZrUIXQ0iU-LpP3lJ9jA-uET/view
https[:]//drive[.]google[.]com/file/d/1ZksPjL-lGuAuWpkTnK-Q2wfkif-ofoyd/view?usp=sharing/
https[:]//drive[.]google[.]com/file/d/1ZS4MIF7_FV3dxSwYhkoSnqv4MzoFTIKI/view
https[:]//drive[.]google[.]com/file/d/1ZVsN9SAlQWkRy8fCR7D44EhX4V02OlPY/view

Smtp Host

[113.170.62.182]
ppp-191[.]pool-002[.]spbnit[.]ru
[37.114.153.15]
[222.252.111.243]
[77.35.235.116]
[14.232.132.239]
[132.255.16.7]
[123.21.178.91]
[37.114.134.200]
[14.231.137.74]
[117.0.193.37]
[171.243.79.123]
[14.184.151.234]
[116.111.163.208]
a16[.]sub225[.]net78[.]udm[.]net
[138.97.94.29]
[14.186.30.224]
[113.173.166.171]
[113.188.132.167]
[111.95.18.88]
[27.73.13.33]
[123.21.121.46]
[113.167.172.97]
[191.54.228.253]
95-55-55-59[.]dynamic[.]avangarddsl[.]ru
[123.27.155.189]
[121.202.81.45]
[27.76.151.25]
[123.20.94.73]
[95.53.55.220]

[177.8.222.42]
[205.217.246.141]
[192.141.234.66]
[14.234.4.220]
[113.172.226.8]
[14.231.37.135]
[178.46.192.44]
[190.120.99.106]
[123.22.95.16]
[201.221.61.219]
[123.21.225.164]
[113.172.139.5]
[111.95.21.124]
[36.183.128.139]
[121.203.203.141]
[14.186.5.241]
[171.234.74.135]
[171.237.74.74]
[117.1.199.120]
[183.14.25.253]
mm-16-224-212-37.grodno.dynamic.pppoe.byfly[.]by
[37.114.167.107]
[129.205.22.204]
[171.242.70.176]
[14.164.137.3]
[123.27.183.167]
[93.178.79.125]
[42.57.224.200]
[27.66.103.6]
[113.169.43.37]

From: (Original)

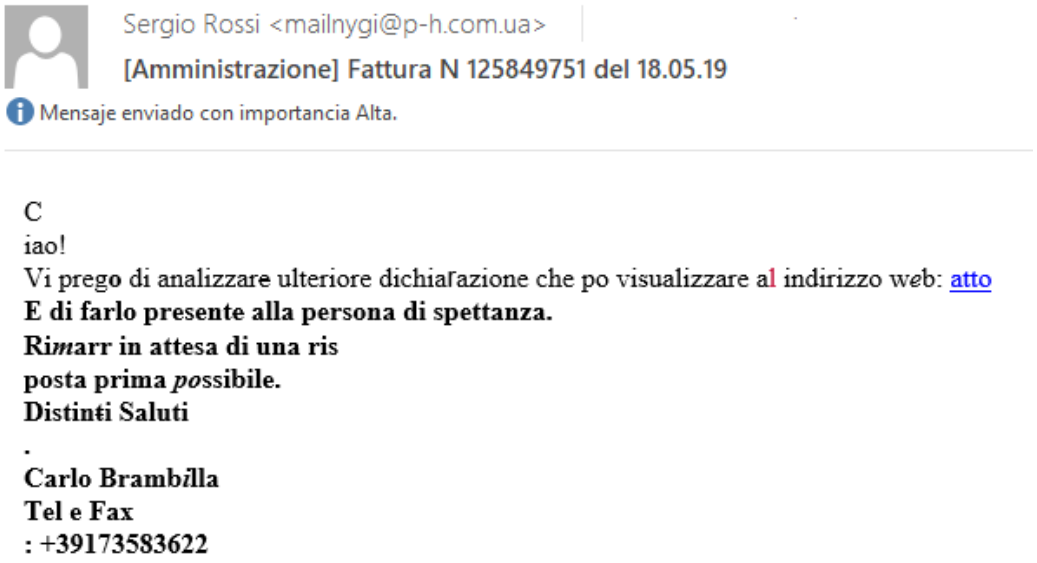
simonetta_justina@wiuh[.]com
barberi_flavio@wbiu[.]com
abella_primo@antu[.]com
vittori_michelle@utgd[.]com
broggi_nuncio@ycnb[.]com
gaetani_santo@psql[.]com
troia_biondello@bkvd[.]com
todora_speranza@vkfz[.]com
corsini_fortino@auhf[.]com
scola_venecia@mjfh[.]com
grosso_giovanna@nipo[.]com
mailnygi@p-h[.]com.ua
mailru@p-w-e[.]com
mailyoujp@pa.uc3m[.]es
borgese_attilio@pacific-tour[.]com
cianciolo_honorius@pacificexhibitions[.]com
petralia_zanipolo@p-art.co[.]jp
genua_marietta@pacific-time[.]com
tancredi_gino@p-p-o[.]net
corallo_giordana@pabsttheatre[.]com
monetti_maury@pacificedgebistro[.]com
iacobelli_borachio@pac-data[.]com
riotto_vesuvio@pabucunkarnesi[.]com
micheli_braulio@pacetek[.]com
galdi_eriberto@p-enerji[.]com
quattrucci_amerigo@p-l-b[.]com
vitanza_cajetan@pacificescort[.]com
stefano_mariabella@p30land[.]com
paonessa_deusdedit@p-gunma[.]com
salvatori_speranza@pa-saiyo[.]com
giannuzzi_maurizio@paceshipping[.]net
cicconi_giordana@p-honey[.]com

giovanini_falito@p-h-v[.]com
blanco_fortino@p3mc[.]com
scalone_mia@p-d-a[.]net
marcolini_gratiano@pabitos[.]com
manca_carlotta@pabellondelfuturo[.]com
baldo_tancredo@p21forum[.]com
lippi_maurizio@pacificdivingacademy[.]com
argento_braulio@p90x-lean[.]com
muscato_demarco@pacificexpresscourier-cargouk[.]com
giarraputo_vittorio@p2collars[.]net
leandro_vesuvio@p-i-o[.]com
rosi_quorra@pacific-sports[.]com
sano_hortensio@p6s4resx6.xorg[.]pl
ruggiero_proculeius@pabaseball[.]com
verona_ilaria@p7z[.]com
girone_nek@pacificfishworks[.]com
zappala_contessa@p2e[.]de
patella_cajetan@pablosplayanegra[.]com
spano_uberta@p-c-e[.]de
bertolino_giovanna@p-d-v-r[.]com
montelongo_ettore@pa-equipment[.]com
leone_fleance@pacificchina[.]com
broggi_falito@pacharge[.]com
guerino_nek@pacasolaire-innovation[.]com
mariano_tancredo@pabbo[.]com
farinacci_deusdedit@p-q-h[.]com
casaletto_paris@pacemakerhelp[.]com
marzo_massimo@p-de[.]jp

Subject:

[Amministrazione] Fattura N
Fattura n.

Imagen Correo


Sergio Rossi <mailnygi@p-h.com.ua>
[Amministrazione] Fattura N 125849751 del 18.05.19
Mensaje enviado con importancia Alta.

C
iao!
Vi prego di analizzare ulteriore dichiarazione che po visualizzare al indirizzo web: atto
E di farlo presente alla persona di spettanza.
Rimarr in attesa di una ris
posta prima possibile.
Distinti Saluti
.
Carlo Brambilla
Tel e Fax
: +39173583622

Paolo Serritella <Borgese_Attilio@pacific-tour.com>

[Amministrazione] Fattura N 9328 del 15/06/2019

Cia
o!
Vi prego di analizzare ulteriore dichiarazione che po visualizzare al indirizzo web: sc
ar
icare
E
di farlo presente alla persona di spettanza.
Rimarr in attesa di una risposta prima possibile.

Distinti Saluti.
&
nb
sp;

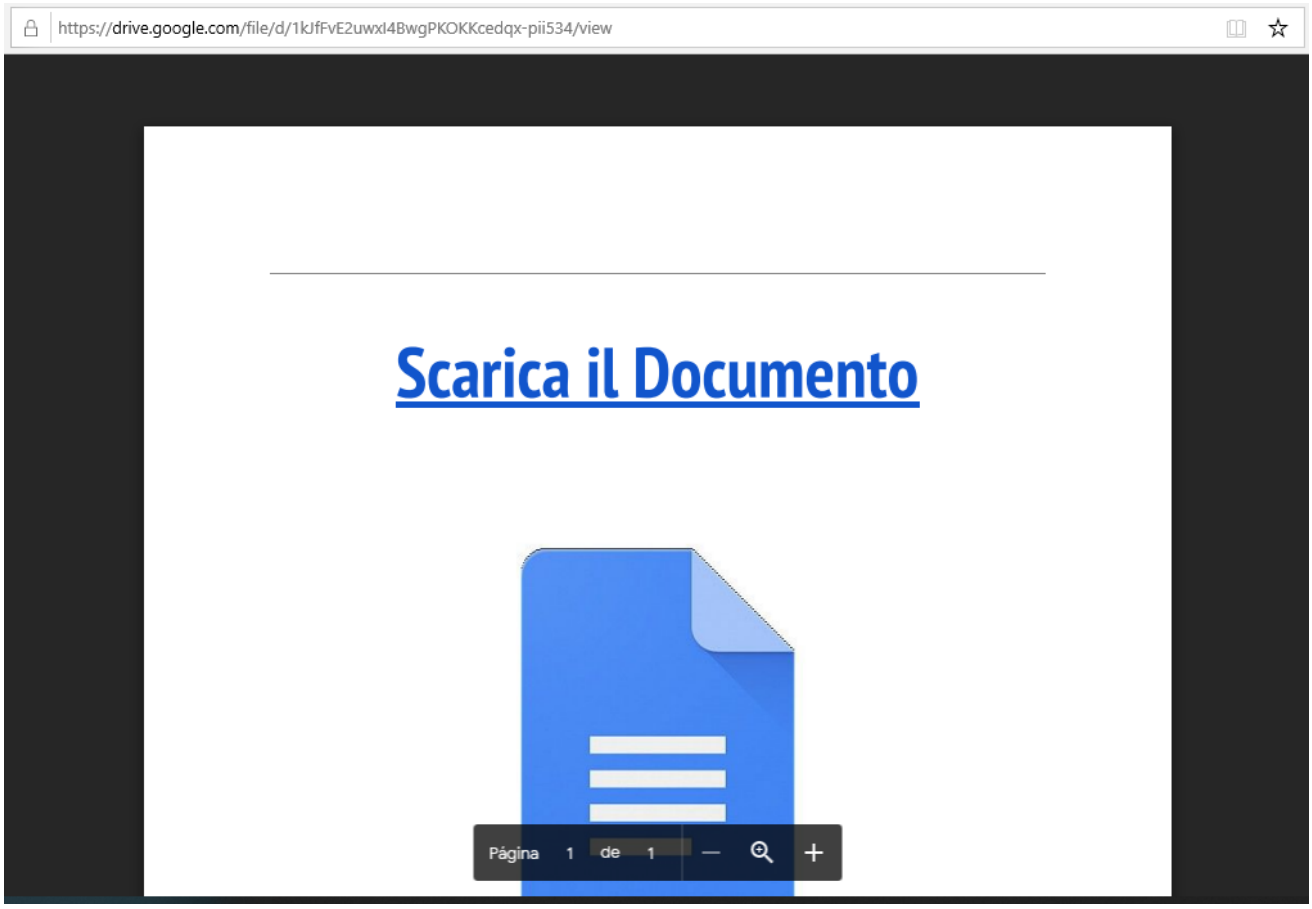
Giovanni Busetto
Tel e Fax : +39173583622

Zanipolo Luchetti <Simonetta_Justina@wiuh.com>

Fattura n. 026 del 28.06.19

FATTURA N. 041 DEL 25.06.19 GESTIONE ORIZZONTI .
C
ordiali Saluti
Antonio Bruzzone

Imagen Urls



- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.17 18:33:52 -04'00'