

Alerta de seguridad cibernética	2CMV20-00096-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Octubre de 2020
Última revisión	15 de Octubre 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 afectada 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.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), comparte una serie de Indicadores de Compromiso (IoC) obtenidos del análisis realizado a múltiples campañas de phishing con archivos adjuntos que contienen malware, los que están circulando en el ciberespacio nacional y representan un riesgo para los sistemas informáticos, así como para los usuarios en general. CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

## Observación

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

## IoC hash

Hash SHA-256

```
064adbd5640ef3fda23824886ee23921c5a3e50d8e7a2906bdd636e1c982aa9a
bf8ee01a9c299fdfaa7fa6f61e9e04bb31b5f56300c4570228e524796c8a45ab
4e2c7d269a6ac0822ab6f3045c0352299c4cc28a7cb08bcb3d1fd3bcfed4d7aa
9cdefce35cdb78bfad530dc47d20a2497159cfaff4df8e163843ece18a16396c
a1c53669a74c641f7a0eed1bbec5529242618aa390c71a3072d430a21d3fee06
b8f2d69f5d20a8093f4818f97e7132a4f3f2c13efe56bde8c964e774476a81ba
e6656ed1edab164c4265d570612ec29b3b6cf3ba3dece150fd79b6c72eae5915
2c625a1699cdcee6b7e861b1efac690e1b8ee1b2e3c48531c114f51c26cff0d2
b39fcf25539085d53a8b25521c1575252fc848d771f07c6a47b301ddd0de8eb0
946bf30ffb29a1059ae80c7e097b0de738bebd31f464fb6b49e90e1ccc896ddb
6aa6dd4f298a8a76d5fab78b73d4f6cad58a2433dfea5cc8c73e6843beb55fb2
f312e194afb25bbe4a19df14123d1943d11f6157322f6cfc6a8652debe57cb01
2cf0dd02b4ac5b4a4eb95e478c1e145f0434764848f7d553620a139e5592e768
4305a26fa817354b7d255344e4f38a4ffa90dd777e2b2d36fbd1474a5948f082
b880aa0040b5f386b895c23af6b05c18473eb9db95ec3942e713fc454c6f4cef
baa4377dd7c181c1972988831c2937f2b580c824001330acf0ca30a2fbf6c629
2cc4dd8780ab90a62026b5a0a1f381f8f85ea4c95b7d9ded566c11def61abadc
02125959734adf9a58e54d61f5f552653d516427221e9cacd06fe64764afb6d6
587b89a514b829530288000449bcbcc41ab09583a07d1a88bc7f4b039d6318a4
1ff7fe031157a4aa850e07c245724cb4b195b180027a60e672dd38964972255a
c47b8924773dd748e6368815239ac9ddba31aaf0d4ce309edf74427137ef61d5
40a0260a9aa72cb24c10efec5a8715c35a647b5b580a64a6672acdf3ecd44280
7397def823ca9bcfdb5fd0de99d9a21b4d8673041883877e52753ba3186d1538
3afb8b0d508b9c991684aca6b9a84832947be2e6e4cf5bf4ab56ad279a729c4c
dade6e39f4c9cdabbb12d2b5216fa5a1a84a2d375074484d57a728997cc372d4
```

## IoC Descarga malware Urls

Urls que son disparadas por la infección inicial del malware, podrían existir otras urls no detectadas

hxxp://savetheboom[.]com/admin\_access/xht/  
hxxps://dakwahwisata[.]net/wp-admin/c/  
hxxps://popcornv[.]com/wp-includes/KHKX/  
hxxps://dusitserve[.]com/gethits/o3A/  
hxxps://asc-kl[.]com/v2/Ztf/  
hxxp://gaashaan[.]com/cgi-bin/O/  
hxxp://inmaainv[.]com/site/cLDOJFI/  
hxxp://wynn838[.]com/wp-content/ZhG/  
hxxp://ladsbarbearia[.]com/wp-content/PI/  
hxxp://syracusecoffee[.]com/customer/jf/  
hxxps://mrveggy[.]com/erros/PO/  
hxxp://givingthanksdaily[.]com/5Q/  
hxxp://buesink[.]com/Pics-shower/ScE/  
hxxp://hottco[.]com/stats/lX/

## IoC nombre de archivo

Nombres de Archivos con Malware

Datos 2020 WNY_053989.doc	CEI-100120 MTV-101420.doc
PO# 10142020.doc	TH_0439_14_lokakuuta_20.doc
invoice #164828.doc	FI_673262_141020.doc
Untitled_71888885.doc	Order1008202009.xz.zip
60907.xls	IMG MT103 4564734 OWA_JPG.GZ
Fakturierung_2020_10_1453358224.doc	New order.xlsx
factura fiscal 5101846 14.10.doc	New order list.xlsx
HE57104918G_COVID-19_SARS-CoV-2.doc	recibo de pago.zip
info 981846-562799597.doc	ORDEN DE COMPRA 1692020.zip
Mensaje 1410 PPN_1973.doc	payment in euro.exe
717520440796202.doc	msg11390.pif
fatura 74914800 14 10 20.doc	FI_59012_14_lokakuuta_20.doc
Bank Details .xlsx	

## IoC servidor smtp

Direcciones IP del servidor Smtip de donde fue enviado el correo

196.46.192.26      202.66.174.108  
66.146.0.201      66.84.15.151  
41.221.32.207      202.66.173.167  
51.75.202.197      210.134.165.80  
65.254.254.80      185.222.57.73  
199.168.188.91    210.56.11.43  
109.205.64.52      47.88.189.81  
64.69.218.92      212.39.90.97  
184.106.54.106    185.222.57.174  
109.205.64.59      94.46.167.170  
89.40.4.85

## IoC Correo Electrónico

Correo electrónico de donde fue enviado

uczsynod@zamnet.zm	altamira@jrlojero.com
service@metroinfiniti.com	robikris22t@gmail.com
venance.kalulunga@pct.co.tz	sawijama5iweq@gmail.com
ops@fastunisia.com	renato@pontuallogistica.com
d.hernandez@corporacionurimar.com	sales@drpgroups.com
mariaisabel.avila.f@dihego.com	elena.zeiss@cultura.gob.cl
ore@ore-peinture.fr	doripama101ufy@gmail.com
(nvaldecchy@chilexpress.cl)	info@esi-seafood.com
andresdiaz@automotrizval.cl	info@b-account.com
sabrina.consul@redebrasil.com.br	mgesrl@infovia.com.ar
info@sparkserve.live	almuhaidb.jarir@ewaahotels.com
t.endo@nexus-thai.com	chutikhan@pro-connect.co.th
ankitshukla@ndsbl.in	accountstaff@umbalpln.com
info@eurasia3.com	noreply@mbienes.cl
koepketemi17pdxtg@gmail.com	sawijama5gyviz@gmail.com
garcee@constructoraatlas.com.pe	westelle638ineyl@gmail.com
michhyma42fvts@gmail.com	

## 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.