Alerta de seguridad cibernética	2CMV20-00072-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Agosto de 2020
Última revisión	07 de Agosto 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 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.

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

03040e27c1bf1606339ea64baf00d05a437368e203ff94dc4de84a6580b16c89
05b49d24c2dc263319238a138dc66dac72937c84bb7e8d9ce9d98966bb5763c6
08d0db663eee38e0d9f5b7a27d0ff3bfc9b2ccaefcf0b3347f4266295e4f16f4
0effb6a6fd452063873608c23dcffd0dc22ed6e84f273809dd8601d7a04ac3d8
129a59ef23cad9fdb25fa5b1a912c88a0856c5718576d8a158d54748dcde7b57
14ac0983d517a26f29b5bf82e476e9fe0ee494ad757956152c762d46eda7ed99
152bfe5cc08180a6865e85c4a2bbddafa9cd758e40c0cc296223761e5931ae2d
17d593021eca36c491e85a211c4634737d302dbc74456ed4de71a9c0d3a1e8fb
1bd34dabd0cc51323eb1db1e8ce1c4f1158778691b723c85315ed8f8778090bb
1c854aac6c58c6f6ea00c98ac569e1ca25382e1b7a898bccc4e069807180fcb4
1cc3fe55cd9952581cd54ff7b1a12d5a7a2aa90d760fda8b9a6b2ea8d010e1a7
268c4c958e4c17328ec2a8d5f589292fb6561e77f97915f5853ca116aea9ff97
26c00d468f7203957661f1f7802a750742ad5f9d0d1ed546ef4d899eba2c93b7
2786fc259332ce5c67ecec61cfcfb0a0a8f2e6db582d3f3cbb379b25834b7419
27cbaf5297dd6c9a9c490611f9fb563fd4a9de7f02758c6de86f90120b8935e2
2aaa85dd9ac60aea2f5746aaa7b925bdf4453f69fdf378f446da71cb35378c9a
2c5b7f8488ec8abc944d1a90f84293494cb7c6dea6cd23bad40fce8429f41442
2c6e3b78df9864cad8367f65bb7eab3d11cbcbcfd04ca28ecc21b0da188334b2
2cb9f4087e79b2b1fff438c9cb50fd3db33598843f31d58818129756a638f991
2f4f05ae11f110281616194a52c24c984e05139ad54df26d4a63863f6638e9eb
340d761bd35b05893677888fa972ebf76468a9cbfa0217257301a0965682ccae
34c34f5465ac4b1406c82fab5bfe36afc5519985e9d2141c9f4cd222169d112e
3a17dd818992725fb9bf1c2e0d4d18141f5b9fe15a184e7ebac32b935fe7e60f
3bf1a2f3fac51ede9efd841a8c10ff5da4af2add08f05fa7a88b49a5b4016dc8
416ce7a4ae6bb343dff5faa22163451d052b582aaf05f300876d3448ecb36b8c
420419cde08a92e989b226730033cf7b77c4d0650ad18aaba16226d48c328abf
47212fb8ff16b808717846fd7c601607cf65a9d515f602615c0d58cddc0fcba4
498ee7883a63f66a9237071033f525cf7cfdd8750fb001aa44a54d064bf5c21b
4c3a60e7e971b6096c36eb544d9d83d77f3af1bea6efbb5d3367c891d1fce46b
4d66b8fafcf69f590dc74a3383fa08576a6de54ef030b8d47bced68e03f63065
50fb657e98a84c410b26ceebc14745d70b30ddeab2f3836c8e7efdf751869f1e
5262f683ca04d27e286c1fa10577ad9306f7e1bb535c2f6b6884424feece32d6
538df0bf2b315adc42194d9c278ab23effb4326552c8ec20beb7a8af06a5682d

54b00033c30eff4f4585b45a9f04a22fb283856b5cfdaec0adadfa44645e2e4a
55d02808ea8031c7773affde46a28a40c347db186f9ff06b74d9941a06a8eaf1
56336192a4f8789f6eaeb22a57ca0f54bf0ff5ddaf7455af8864714c0d941e30
5a34b144f5f6df0a869e9f6d5805f310c0fcf4871128d792215a0c49f3b6fe48
5af88b2d9a192241b2b0e52aed733bdeb190a4af07eacc6940520f7441c04953
5b0be6394821d65cd709523f4aace411190349cf4dde98192b58d7c8ca65a69b
5c5b139f486c90ff9ba2c3f9ce53601d2d823de4fbb24f64cb7c26f76914df2a
5c616a2aa8edda1b20ef34c1b224865ef55afba4c27ff503fe109dc0839c117e
5cf9df63fc0062d8b9f461fd7d94bea278b4a18de25821a51d4933de73483a5f
5f69b9a201635edf0b717cde128fd0401cc1dd3b52f4ca2bc9d59f8d580ac0a6
60217e789634bd22ec28c52188c97a5a5cb8886661663fc79b59b9ffd33d73af
60e508e5b68a32f77e6b1b9cb14b36fec9a2d7e93d632eb0bc3ddafd07652f61
61407a2bb77dfa22827b5735f1e9ea42fe52799d2d5c0e1c2ac85290efbe9579
61ad770d6b0607489077c23465448db606602ff3fc0222077396e71692eda84a
62c944e88aa9a89db23e2db63e8744e0ec22dd0ccf46478bbcef7c688752b06a
6404a5a49751db7e1c82b5bdffadd5171eea2b5a4b43f9b77afb50b2095df09d
648d696cb8bce25f1b17691be0e9ed5f3b94320b6b489e2b77ad5f0e895e6786
69c1b7ace245b0f3a36b5f7ee854e98bbe4ae80fbfed72459200d88d1fb8dd4b
6c822bf85153ffff4d424e12352a19e60d31782008681d7287a00bf4750feb70
7052179b65c1bd330946e70e9a3716d321d3368d774ad1b578188bc94b992c0e
706fdc7d420cdb00957231e66056423617a36dbb164b61b2e24642e26c23311d
7086cd8aed7ec4f439758baeddefb114532304c3c614aed26cd0061fb95129e9
74826766f8e1e25f6cc5d42efd0e26f286fe713df51a702407b79bee122d667c
74b5a5e2f1ca9e2ce5b60eb11efe7430653d3bc4330800836b015f96c21916cf
76f38b42e6c5822d699f67b2b342f3657d7118ebd1c9a62f7e8c0e493ea10735
791aabe16af1e0700ec95a024dc76966d350bcc8d0cb3fdb0371bab88bcc1557
7b5c9eeb60ed37e862028376697fca4a2deaf5880032c884d3deb65a9d613387
7ce151a598299d6d4d24231e1311bd774a7bb03d010e3b46efd8c8bd833ee1a5
8187606140faf5d34070ee1f26650fb8d3b1549d3573e7c496a38d3bcea153b2
83199c3a1bbb38134c3c906319e4ac997003f912f7858649a8a6222d475fe002
84230df72a5032dd8173823050d14fe14769d543c5095c3f703fda250d72e2a6
890e6da8546d39ab79f0ea19fd80806ffb9b482e7a38da9553aee75f36049784
8aeb263a14ae386d1926b1885db7954af6e124fe1885cf9f3075ae7cd2025a16
9527b6ab531d291de7c1a88d344c4bb2770e73f860abf3ed702ceaf2e18cc905
98c92f9f7760480bc95e3c091adf4d40b14c4235b7940122ecaf52495a811524
9ae09a69d247b8bba8125e9ff88ded1645747e06003b7115abd793a458e11b04
9bb291ed5f1c331f49ffcce7f6a0780c4a790538b7fd0fffae09dc2c550d4cf7
9bba929ad5c1065794be4e8d4b6805e54340b3a4927b020cba7340b54973bcd3
9c66495d29ca493f2b453608d66cee148ed6afd4cac60b7909bb68087a574677
9db90751b23be0e9c4961bd7bede073eacdb33f765a559d40e68d0e6f4444973
9f0042355df96916dafb4a7e119ef22bfdd051653c32c759b005bf61a57e0324

a10ccac3999b2563b8c2cd3970c382d631c9e040a9fed7b3e062c49b0d7c7341
a1668530748354caf4b83b007f729aa168414a2e53c2c87bc4043bdd0c7a3c06
a231b9e0cacf439e9d9e0522a3a7504fdd6a96d3d39e553ccc93b817db2e63ac
a2499afdc0cde0e9b047005e936a3e4f21d4b125714510c4090ece2a02013976
a381ceb779dc07557423184bcd01fa36433d8f400d912c67cdfa63300400f58f
a6742a79387898aaf809df6063957e85c4c87fd53f6fa8b8e05c208d1d85ada2
a9c2b4e4ad1eb3940862d0987157fd88ac5d292d01590ff8f3442a8bf389b624
acc38b0b18cd297c1ba29b4f19c6a13f6b6ac2f693bd3fbc65261d69820aa969
ad8d5522103a1694c39d1af9ab267e41522b348969e081dea22d39bdd7ea24a0
adb851e80e9be14bfe3061a9ca50f89247712ea6f24bfb21bd43b7a9ceebbb48
adf0c0b95460759ec00397aad0ac4ff47dd132b7b72cd4c13064f1d23c44b2c9
b05b7a5b7251a3088a61d778b36b9806d3c57425a15891696e1f447a258f08ff
b260d14fbf02a23cc5947fb0a5d22ced32d33b3b17a187d90c83d3906536cb3d
b35bcfa8fc444fb3ba341ffbdcbf424590e9ef72638b22881d70cc313330bb9f
b52a77bbbfcd54a2ea73e2249e6286d3f27eec330e25220cce1ddf097e3f9f14
ba8540360200ccce58d2b79cd48c1478ef917f68b460fcdc58f78d7cabb5e4d8
bb357017182090b9f1df33669c2f86cfe9d8bdf8e3d642d8d52d6c3478ed4347
bc4e6f2f51ea8d20050084adfd08a79cd489462c22f07695cb8a948511d1c572
c1d0be9adeba59340b82539e765938044a090c6fd548941c81793792e112da83
c2688db1ed1759520bd3d6d0e83a34b70f6582fe2c4ab812b274d2ece2fdbc37
c309e5627b9ce6c410f3ac385cdb9a54ed1af4d996fc9425fcc0b3f4b44b06d3
c67920a66134ea8d373af6d9b4c80251565b81b61ba4f8cd21e6b16979051c93
c98c4be3318c611e5a7ba96baed3a9da43243f367141d79a04924edf603ae9d6
cd464e843dca00b09b6541a7ccb05834ce98ece1eae8d609c542aa5304b90401
cdad26800b0cbf8b3c591cc545378d50c93a28c735fada99d6bbe4228f2ed6b0
ce537cebc52ef63cd5bf7f35abb10712d236835b821443089e3c40551d3cf481
d03048334da4159bce04cb387d58f785dd4b0ee96736f6582158481db2083c86
d1dea65be89ef46c53cd9518eabfcc4e965b45ce734b6cbab39e31fa8a3079e2
d21fb5ef05cc6d7375ad67529c3b74d7111dff2fd9a11ce6944a25e4dc2463c0
d65c86f358eed17035e99352ae03ffce23293409580c2f6c4a5e5ba5ec6e0280
d6a014a7283dd3276879843dd81369e4891a5f27287f84a5e5fa66dbfeeeb4fb
dd6ce80ece4bbbbd9b0a13664e10079dbc6594eef59c808295824adc0bcd61c9
ddc0264f82a81e5c3070a77887e7840f0fbde2949b742b74381fe8ec39daa9b8
df3276da854c3298c4b852a294ff1c0ba031ae27146e7534b3aef464d14af536
e036953eae1466c2e96a95c53b2a4febad81f74a776f22925eb746546269cb51
e0f9148635d301b40850b5a82e7c1d7c17161294e190d7b805efeb9e9b873cdb
e22a5a9d9261fb7c846f6df8f33afce0315af075f20771b5b8fe5fcd7361b1cf
e8ed2d9c5754d8f5ce8e8a293e600ecb9c125bb06b9f2388e1c8487158f4e254
e919c5503909e759af1d70a0d8a59fbb5c46a80b67f9a8039869b27035e77cda
e95ac77cf0fde9274d104fa3616149ea70b6f7e31d4cfb0c9b80103f83d05276
e99984f11ff3a6792d0a302968ae9f74774d3c66fb9e76ca0554858d3b576997

eb2fa7da4134ccab3547e41ac3ebf79e61dd4643cd65c429287126908ef8e69a
f6e608de417c7e4e4e693353a1a84920591e872cefcb27e0d93ef6b97a133481
fac5fe709d65e53860aae4c70e10e47bc3a4bde2b4f8aaa91e3ddb4cdb612570
fc494d4b419e758620c30b412bd21901780dc1089750439d2d25bf94bc52def2
fef330d48bed61c5c87bbce7eb9124c4e46b9fa8b5a070ae1f2dd1d061bb16e0

IoC Descarga malware Urls

hxxp//swiftlogisticseg[.]com/wp-admin/available-rEvbQDJne-2vpsDkD7vW/gw8-wdwzcwgjc-warehouse/MjQYHI8i-9idjejg79jfvq/
https://116[.]125[.]120[.]88/bFfFX0W/jgrqLS/NqmbC25ks8PM/WXZEJREWwz3qGM5p/
hxxp//webstack[.]com[.]au/wp-includes/U890802/
hxxp//mobiletech[.]net/images/TnpY/
hxxp//mx2interests[.]com/gulf/dhcWCM/
hxxp//rouxweb[.]com/sea/IOm310/
hxxp//sallyabbeyarts[.]com/SALLY_ART_2014/UqN4k/
hxxp//novellogic[.]de/ad_o_2ig/2mnnXLTp-kpH5QsjR-array/5crrar1nezbbe-t8r7v9-portal/8442kCcp-7fwyN6pjuItv/
hxxp//brizboy[.]com/site/closed-5062759-oBrty78DTTZ/verified-area/yhRwLP0s-KuosHc2onimj1t/
hxxp//82[.]76[.]111[.]249/Koy6u/Y8Uv7SdtF/QFwEoDICyk1bBI1/ToIWPKz1CsOABI/g9tyx3Z/63twmDbt9qGGbzwSwq/
hxxp//www[.]ncsu[.]org[.]ng/wp-content/3_tcn_pc/
hxxp//204[.]197[.]146[.]48/etZfdOsqGN/xAlHTIQ/5Ioj3QMLGGkSR/dRAxsrkHxE/iim66MlIQ/
hxxp//paletas[.]org/cgi-bin/besxXuq/
https://78[.]189[.]60[.]109/7CqVO1plp1i1N/LF9oQV1/
hxxp//198[.]57[.]203[.]63:8080/UvauZAaDWUa2/
hxxp//lindnerelektroanlagen[.]de/pages/closed_array/corporate_Qvt1WRAIL_wizVz4iwC2/Mb2cyxZUJuX_et9L1IppzGs5/
hxxp//psyberhawk[.]com/cgi-bin/personal-JrOFJw-R3R1sEMo7S/mBHrF-RYaUiC8fo-warehouse/RQfOw-g5t05f7juq0/
hxxp//pstanford[.]co[.]uk/wp-content/personal-section/verifiable-space/la6JqK-14glq1ys0fje/
hxxp//whistledownfarm[.]com/wp-admin/Qkqig0vqd685w76/
hxxp//47[.]146[.]32[.]175/5X3YOu/O42fq24hH/liUhOOiYcp35/ImTI/CoUu7qxQCbz9/
hxxp//driftaway-holidays[.]co[.]uk/wp-content/wf_gmc_c1tk6o1/
hxxp//umphrey[.]us/ww12/qo_s1mq_p4o/
hxxp//dkeventmarketing[.]com/tasteofnj/aqr8_xsa_53/
hxxp//fon-gsm[.]pl/87/n4o2_fl5_kw0f36a/
https://fsastudio[.]com/zp_m_j4/
hxxp//www[.]spektrondesigns[.]com/cgi-bin/3vzc_oj94_q3v42ns4nb/
hxxp//buybywe[.]com/payment/4ots_c9x_ty/
hxxp//haverkatejuristen[.]nl/libraries/HmSZqoH3Xo-uCOohtqIdMJIEB-box/external-profile/HYBMewyjjYG-Nffqbq8Jd90htq/
hxxp//tvsanmiguel[.]com/ww4w/y_mm_n8/
hxxp//dgreitkelis[.]lt/ww12/gmei_ksa_vb/
hxxp//techlh[.]com/old_whmcs/jd_elc_1e/
hxxp//tedbrengel[.]com/wp-admin/gg_p_njyjdpr/
hxxp//teldesign[.]com/stats/szv5_kv_vaf4016v/

hxxp//scanfone[.]com[.]br/dianetica/Scan/yt8946095680333222ia5ivz5lawkt4nhv/

IoC nombre de archivo

Nombres de Archivos con Malware

WH991522.doc
10 08072020 9141192.rtf
1orden_de_compra_20013.7z
5338566.doc
759 2334.rtf
9013_08_06_20204133.doc
AQ3010625132RE.doc
BA9946426520SJ.doc
BH3162835518GT.doc
BW6168754833KI.doc
BX2362746997JL.doc
County Report - August.doc
Data 08072020 205108.doc
DE9000213228UE.doc
DETAILS 08_07_2020 YAZ70941.rtf
DETAILS_0807202006116.doc
Details-08_07_2020.rtf
DKF-080120 SXO-080720.doc
doc_08072020.rtf
doc_08072020364385.doc
doc_8228.docm
DRK-080120 WHD-080720.doc
DY6765085277OC.doc
EFF-080120 TVT-080720.doc
Estimate 0144518.doc
Export10032885_Mahler-Besse_8_6_2020_1209.xlsm
F_3 -08072020-58510.rtf
FILE 08062020.docm
File0414392.doc
Form - Aug 07, 2020.doc
FXI-080120 FCI-080720.doc
FYX-080120 NJI-080720.doc
GVS3477533964519.docm
GXJ-080120 FVO-080720.doc
HN3670027088OE.doc
Invoice P09535234.doc
Invoice.doc
Invoice.docm
J16 invoicing.doc
JM9576022055PR.doc
JMG-080120 HOB-080720.doc
KN3277964455SM.doc
KQ1516818623LB.doc
LHB-080120 JFT-080720.doc
list_080620207664406.doc
LJ8153565055RA.doc
LK0986516733MR.doc
LL4793387485ZG.doc
LOM-080120 OPQ-080620.doc
MAIL 08072020039580.rtf
MAIL-08_07_2020-NV327663.docm
MAJDALANI INOX S.A Pedido 050820.r01
MES.rtf
MES_3245.docm
MES567.doc
Message 08_06_2020.doc
message_08072020.rtf
message055713.docm
MI9629904859XX.doc
MNA-815302 08072020 FPC513.docm
MYK-080120 PFQ-080620.doc
natmass.ace
natori.ace
New Order PDF.zip
OA6577113723PZ.doc
OC_Y7039184652.cab
OE7767714096RA.doc
Outstanding invoice.doc
pack46253479.docm
PJI-080120 ZLO-080720.doc

Image001.pdf.gz
INFO 08072020 3341.docm
info 08072020 AFL477501.docm
Info09.docm
inquiry.gz
INV #55232 FOR PO #4020757790.doc
Inv G932.rtf
Inv. 8131928811.doc
Invoice 261563.doc
Invoice 841512.doc
Invoice A01332.doc
VNI_2 56233.docm
VO8440754389CR.doc
VTT-080120 COH-080620.doc
WGL-080120 JKY-080720.doc
WZ9755203681PA.doc
XA-8256 Medical report p2.doc
YFN-080120 BWH-080620.doc
PO# 08072020.doc
PO# 08072020Ex.doc
RE1922819421DP.doc
Ref08062020.gz
Relief International Award Notification..pdf
REN#42159.jar
RFQ 866645 Airox Nigen.rar
SCAN-08_07_2020-GIN2592.doc
Scan-a1uUFPSajiFP5Ts - xlsx.gz
ScanMT103 sanc Ltd.rar
shipping document.html
SW7022200463MD.doc
Swift_transfer_copy.html
TA0541856315YZ.doc
UQG-080120 OKO-080720.doc
UWI-080120 BZD-080720.doc
VB0591943926NA.doc
YQ-8072 08_07_2020.doc

IoC servidor smtp

201.76.49.136	66.96.189.5	196.29.32.34	178.250.64.59	163.44.196.28
201.76.49.126	89.32.144.184	201.76.49.122	177.185.201.34	113.23.214.191
201.76.49.75	167.99.145.121	201.76.49.132	167.99.78.107	200.74.193.140
201.76.49.9	203.78.107.146	201.76.49.71	189.126.112.76	69.89.18.3
54.38.207.33	207.248.85.19	201.76.49.4	201.76.49.130	213.135.0.95
150.95.183.80	150.95.20.134	179.185.61.131	201.76.49.2	91.244.162.210
54.38.207.0	201.76.49.79	78.47.188.13	180.250.242.212	185.216.113.100
195.78.211.239	201.76.49.135	190.210.9.178	113.23.215.130	112.109.90.80
54.38.206.98	201.76.49.74	65.99.248.165	207.148.123.206	83.103.43.63
54.38.207.1	201.76.49.125	189.113.174.76	75.98.233.2	88.135.38.169
201.76.49.140	201.76.49.7	95.216.241.201	137.59.125.200	88.135.38.169
201.76.49.80	201.76.49.78	139.162.220.238	189.126.112.74	103.15.48.223
54.38.207.2	201.76.49.139	109.203.103.246	201.76.49.129	110.4.44.145
201.151.206.8	103.15.48.224	201.76.49.180	201.76.49.70	195.13.167.102
43.229.85.232	209.59.180.124	201.76.49.137	202.71.144.54	81.88.40.216
201.76.49.123	104.152.177.36	217.169.223.125	213.238.175.13	213.142.132.174
201.76.49.138	201.76.49.73	31.47.196.212	201.76.49.147	88.255.249.220
201.76.49.133	201.76.49.134	139.162.220.238	82.223.132.68	216.230.137.116
201.76.49.5	201.76.49.124	103.232.66.27	189.126.112.10	81.19.78.4
201.76.49.72	201.76.49.6	191.252.30.34	201.76.49.128	139.162.30.33
196.61.224.140	103.129.15.238	190.106.132.26	189.126.112.247	195.91.130.22
179.188.7.168	201.76.49.77	187.45.181.45	103.77.163.28	193.56.28.147
91.108.157.12	203.154.100.69	189.126.112.77	103.215.136.36	222.146.32.177
209.126.127.4	216.245.212.3	201.76.49.131	200.6.186.181	45.112.124.77
185.22.84.10	201.76.49.76	201.76.49.10	109.74.192.34	154.66.66.118
41.77.232.33	69.167.160.14	201.76.49.3	189.126.112.205	95.161.226.166
177.185.203.199	200.49.145.154	109.237.142.230	201.76.49.243	116.202.86.111
201.76.49.127	45.147.231.73	154.72.196.227	189.126.112.9	50.31.152.126
189.126.112.246	186.155.200.186	152.171.50.169	113.161.38.148	192.254.163.242
162.241.131.240	177.70.124.126	190.117.54.180	113.23.212.191	62.138.137.170
201.76.49.226	209.239.121.100	103.217.93.32	74.116.246.162	82.69.164.126
41.33.197.58	191.252.30.25	179.7.225.116	91.244.162.210	202.69.36.36
89.32.144.184	200.215.171.86	191.113.191.120	189.216.97.85	177.185.201.188
23.83.212.26	190.237.162.21	66.96.189.6	201.76.49.217	103.15.48.236
190.252.193.68	181.46.66.203	189.8.78.163	200.123.26.167	103.82.198.114
162.214.66.66	191.252.14.18	119.15.167.212	46.26.190.2	201.76.49.244
182.23.49.37	189.126.112.162	45.73.34.118	200.60.67.202	81.21.81.35
150.95.20.20	150.95.29.34	59.124.246.15	177.185.202.209	59.124.24.181

45.79.219.4	162.144.73.176	160.242.142.180	149.72.192.247	199.250.217.29
189.126.112.158	162.241.42.151	178.211.62.44	213.142.132.174	95.211.208.40
177.154.132.147	80.15.54.216	210.245.107.253	162.144.126.34	69.89.18.3
72.29.89.6	181.56.189.18	201.76.49.108	190.227.13.2	82.223.214.121
60.242.20.166	91.193.107.48	201.76.49.109	67.227.156.212	177.185.201.133
197.242.145.198	175.107.198.121	201.76.49.98	185.222.57.157	154.0.172.73
62.77.50.54	77.75.123.178	219.94.129.96	80.85.157.233	
200.43.175.130	200.73.113.14	37.230.106.98	41.219.127.69	

IoC Correo Electronico

ABlanco_srl@arnetbiz.com.ar
acc@pipasps.co.id
account.mk@melilea.com
account@sindbadtravel.az
adauto@eletrodataengenharia.com.br
adm@depositocasaramos.com.br
admin@asc-ga.org
adnan.yousaf@synergyav.com
ag_336.01@pec.agentivittoria.it
ahmed.beram@fasttrack-sd.com
ahmed@landmasters.com.qa
ale@natufood.com.br
alfonso@casagaillard.com
ali.haider@gerrys.com.pk
ana@beercompany.com.br
andre@homemdaterra.com.br
andrew@autovalve.co.za
Anna.Odoherty@btl-group.co.uk
annelize@ellis-engineering.co.za
aprendizgh@mercapava.com.co
arego@tel.inf.br
ariel.intimone@distrimedjujuysrl.com.ar
assist_drcossio@corazonymedicina.com.mx
atendimento@gruposomoscia.com.br
ayazma@emlakyonetim.com.tr
ayto@cenicero.org
blends.redsea@blends.com.sa
bookingota@haidanggroup.com
botifarma@arnetbiz.com.ar
caceres@recicladoscaceressur.com
cadastro@grupomovimente.com.br
celiaquedas@casadosconstrutores.com.br
celso.davi@jagua.com.br
chughtai@amsco.pk
cida@interya.com.ar
claudio.banhara@amarabrasil.com.br
cobranzas@brurin.com.ar
ketoanmpv@mpv.com.vn
khh@protour.com.tw
khoald@giangnam.com.vn
kleber.carvalho@grupocobra.com.br
kosit@nci.co.th
lady.hr@gmart.my
latif@ablenet.com.my
lcampelo@amarabrasil.com.br
linda.suarez@b2bkeyz.com
linda@beger.co.th
ljurado@grupocva.com
logistica@transilvana.net
lpmoreira@tel.inf.br
ludene@excelmachinemoving.co.za
m.abyat@ksc.ir
mai.vuongngoc@goldsunpackaging.vn
marceloalvarez@andesmar.com.ar
marco.roberti@ldm.it
maruyama@sanwa-con.co.jp
Masis@harkadir.am
mbatista@galvezcentromedico.com.ar
mertoglu@caravelle.com.tr
metzerplas-ecuador@metzerplas.com.ec
mhernandez@taboada.com.co
michelecarvalho@nassau.com.br
miza@gisbtraining.com
mmata@eigbox.net
mohamed.morsy@be-group.com
murat.guven@cinarecza.com
mustafa.yilmaz@akcadag.com.tr
muzammil@ag-gigi.com.pk
n.lukman@avisena.com.my
nagy@landmasters.com.qa
najam.abbas@alshamsfoods.com
natalia@log-an.pl
news.sustentareseguros.com.br
newtenders@tenderadvisor.com

comercial@consei.com.br
compras@farmapaulo.com.br
compras@formulazero.com.br
compras@garcitassa.com.ar
compras@papelariaperpetuosocorro.com.br
compras@pluralmack.com.br
creditoshn@vitatrac.com.gt
daliborka.calic@lukadunav.co.rs
david.helsel@systoleads.com
deo.rolla@zainretail.com
dp@atacadaodastintas.com.br
dwi.hermansyah@pmt.co.id
e.poggi@agentevittoria.it
e.ville@cnode.io
eduardo.romero@estructuras.com.ar
elie@mtcmobile.com.na
ElshankinaEN@serconsrus.com
emaraiwai@nasinu.com.fj
engenharia@redesiminternet.com.br
ertekesites@veszpremzoo.hu
etirco@arnetbiz.com.ar
express@dhl.com
faerber@medizinrecht-suedwest.de
faturamento@hondafaberge.com.br
felipe@dogmarepresentacoes.com.br
finance@madya.co.id
finance@mayrig.sa
fiscal@baratela.com.br
frotapc@cplog.com.br
fsobindura@zol.co.zw
g.pacino@assoretipmi.it
garcitas@garcitassa.com.ar
gerencia@eigbox.net
glandy.auma@uhrc.ug
gterribile@tecarga.com.ar
gyoum@kimuchi.gr.jp
hien.nt.2@pg.mesa.vn
hr@gingernco.com
hseq@bosquessuelosyaguas.com
noreply@dhl.com
norlaily@celestial.com.my
norzalinah@jlpw.com.my
NTV1309@cmsbando.com
of-cuentas@redcopmaco.com.ar
omid.hakimi@1tv.af
operations@acmclearing.co.zw
operations2@newtide.nl
pantacorte@pantanalferro.com.br
pbngda-yan@shi.co.jp
pedidosvc@cas-svegliati.com.ar
pelitli2@emlakyonetim.com.tr
phillipr@dulytrucks.co.zw
phuongdtl@mescoelevator.vn
pin2405@rambler.ru
presidencia@eigbox.net
principal@stthomasschoolranchi.com
product.development@megasyariah.co.id
prvs=1487c9a37f=jakarta.mds@amarishotel.com
purchase@airoxnigen.com
qltb@ssic.com.vn
rachael@lorimak.co.zw
ranjiv.shakya@sysnetglobal.com
recursodeglosa@tommasi.com.br
rifat@flasreklam.com
rmoron@maref.com.ar
s_sawitree@beger.co.th
sakti@transvision.co.id
sale.mgr@powerheatseal.com
sales3@eigbox.net
sarphan@emlakyonetim.com.tr
sarthak.bar@ceasefire.in
sergio.logistica@platerostrucking.com.mx
seyyam.nasir@mmpakistan.com
shahid.ashraf@eigbox.net
shaikh.anis@dawnnews.tv
sidney.dhlamini@kobwa.co.za
sius@abltrading.com
supaporn.s@weltronroyaltech.com

hue.ht@phucbinh.com.vn
ilacson@femco.com.sa
info@centroufficionet.it
info@chohogroup.com
info@classicpalace.ae
info@corralconsultors.com
info@f-tec-elektro.com
info@hotelminiatureistanbul.com
info@oracltransport.com
info@quoctekimhung.com
info@schlosserei-pollinger.de
info@wallada.com
info1@riccione.com.ar
infocaty@catyhotel.com
isinda@femco.com.sa
jhonatan@commcell.com.br
jnahuwo@easternproduce.co.mw
josejuan.r@multiorder.net
jovelyn.r@neb.ae
joyce.flores@aquiresz.com
joyce.flores@b2bkeyinfo.com
joyce.flores@gobusinessmerge.com
kamcheong_ha@cohl.com
Karabo@ndra.co.za
supervisao.recepcao@vitalsaudeocupacional.com.br
suzieta@vast.com.my
tamecsa@arnetbiz.com.ar
tatieli.gomes@fulltimesolucoes.com.br
tecnico@sscrosoppi.com.ar
televendas08@baratela.com.br
thabo@nyapotseinc.co.za
thayna@camarc.com.br
thidarath@beger.co.th
tito.gamarra@testekndt.com
todocasa@arnetbiz.com.ar
tuncaycebe@servisgrup.com
unvanzyl_mrs@ri.org
van_serefiye1@emlakyonetim.com.tr
vendasgov@compactatecnologia.com.br
ventas@majdainox.com
ventassps_01@ainsahn.com
viniciuslima@perfectaprint.com.br
w_metee@beger.co.th
wandee@atmgreenhealth.com
wiono@justintime.co.id
wiwat_ch@sirieakluck.co.th
zodwa@fdf.co.sz

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.