Alerta de seguridad cibernética	2CMV20-00084-02
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Septiembre de 2020
Última revisión	05 de Enero de 2021

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

035b6b3a5590a3549ca8ae3aee8a19e07ef40f00ee267afc49f5193df1d739d6
0404c5ba6bc30cd499925585296e268836aa69d56df0cc0cfc5fbb8d8b4cdb72
0652ccbe39403ce0a719d26d57155d72e04ef355cf1d151799daec8d9a57edeb
08d11ad93dda138d10de247269da92214f448b023b39515e9ba032852e67d571
0aaf77ddbd6733d57e90b7a839a8eec42c677c110577bd60b7cb99d0e92371a0
0b0ffa238ef619d9a4b8c0ceb5bbdd889e7ac69db6ef985e427280ddc7fdd113
0cb79454b96cfb3632acf8d5bb5c0a46ea56b09a8e0750cd72afc6f0ba281faf
0cc20101093fe0717a459f14250ba02273813050342e588fed50e77c5b9e52c7
0dcb1e942f7053380d0d8096d7163f69a2137985e9eeb871e6d53ce8379b6ef5
0ddcf0693e98920c63212e0c7c22756d6b89abde16ea579bc0b69e13bbef067e
0e8c650426f43e59e10f07c7b5c2149cb3e84a5ae8ea8ed94c98e8e685223f72
0fd1ea9df6c248cc1ef6ac65fc534db5ffb946cd912f8199503dd93fecbda5c0
10aea49fe96c99804e356b0933c857bf2ef02aef9098085070cd636983ea85c0
1696e01404af8e515a6ed2d5b48c04a659ac1ac279a678816278240d1ce7b9e7
16de0445d67ab1a72e451b4e21b90c287f22a6fdda0f7f7db1f07aae030a5782
177d7bb3166c95573855668f338f0187d49ae22dba0d9c9d3d47130c11ce8f5d
18eef10aade3987189bd4fc8110d9559a06486f8bed9772b3c5f6ce1a344aa84
1ad4af5b6ee1fcb28721dd82b054a45cc6198dca28ca68ccaaef5abd74636828
1af4d40526ef3bae6e86fdf3f6ec2ee8b72e9e8eadf0b2404e0c4fbcb7022d25
1b31be9d49fd6303c1d8a9a23f9c51c2fede70887153687264924c1e2827698d
1b861fc89bf8e49013023f4458519f13803bfabb2b4eff3e63cb209f31406192
1e9f8fefc37699da29bcd62be102f8ec29e40fc2344263266210301ce6feaa53
1ecd0bfbae520e676d9d934a4dd669c6236adf934383d76544e56791b375dc51
1f937adf2064797622d0c208d379a6afb1be8c34b826068ea42f6433ad2766e7
21396fd920983d75686b55c73d984b795d9a279fe6393b4b9de53e6836e0be76
21704f05a998612e83d730f45ddd56d7feaa3e332a5986a96a9c7bd924992903
226c6a5975ec56d38b6444325d3a4aabc3f5c9ff0f8de5cca0eccf3e2ad57f97
228f4f253488803c245aad64df1d3673fa7c72874fb54a9d60741e1cdac97b37
253d29ae952e29dfb3df338d3b57f7e2eee5487292a899a99cc1e1ab88861dcd
277b639551f761697d900d716ba951fb009a6946c9b45b9996d34445eb6bdd0f
27880572aefda24442d0e5517cb24b694a86e0438d5138d6f8a5ecfc42cfedc2
28852a0812d4c493c54382ee8489aef1695d1f07cedc122e9dff86a2ecd451ba

29727ccfff36705a0638c4b0127fc5ec22be60f05d542fd9e9f0f49f6827ef54
2b006308963f46f1dfb5287cd5a6b12dcb5856653ce7b98adbad16cc057baae3
2b4047b6169b9553f5a717b68bb9115896244cfbd2a0105b59e1cfed96f02958
2b8668a2cbfcf9b88c18995f1f415540b05b7668e8493f0ea171097b7e34261a
2c84fc7c7069d63cd2517e8448e92f997515ab241555282d6504ab9c3547595d
2e2b262bc0778dcdddb7424d66db431501072c798da9fa5192cf33af117f99d7
2ee162466a44a2c89434edbe3e3483c34136fcd57397d4782d4b7ebb2885dff5
2f8959d18d3051c0ceb18e1ea7fd567d15db4f00c0c26632a2202193540e668a
2fc990e3346409658a4fbc9a80a859dda1ab32781b1ee8343b1aff419aed2428
2ff4b7d7b02e82dce1df902e65b025fe06a6a66e3e4605ada4206d0eb2e33cd5
316329970083b915103bcc7de04a100c7288018f8c5683974b02f2ec150001bb
3497e1cf506b91bab9a901a99757f2115d1ad48386a00ca764dfd35aaea32e5d
34be158e660cc1cf8852b70f0fc715b8e915f5de83bfcc70bafeab8d84f8afa6
34fd9c4d643cf3cb0678e52d0d8f0c83d2f992ee6b56cfdf47c411a721821a2a
371c8a5719077a4a4972466a738c71da23f3a6fc87f6570aa04d1a0cea2bac6c
37e2718617c6c8c9fbbdf07608e6ea03b14b5d715a33a12c7e4605b573eb69d5
388b23c8be365ee8e2a0bb2a6d0bacfe55fb5e06ad2fd92fd48c6b7774561ff8
3b211810dcd8176df286ff6d29407b15b8977014c8a22899ef51874995c40462
3b43545a3e97a06cd721bc54eb46d1a9c2283029e8c2015ddc95c8e3c1e88344
3c1390aa1f70e293fac9e1291631e3ccd4e5c4cbdec08afad5131a5605cdae84
3c1cf5ad8e50053d609602b1aed8041565d9a173a1ab913f47ec3d719c816db2
3c58efa8a1ff50a1c91b091da3d10d88c300e014f0685c2d003132d3aa4b4fed
3c59f92dde33a4fe2cdb4ce3caaad42bae7cfed7a968b3616a33276ed5b24604
3d3ce21eb20a5c3ea022e9f6e9fd3a339ed2c4cb22c26bbc83e88d0cf7ab6cee
3f9968dbb3d21b0c64fbf4e6c7ec8fc1e458620e08cbfc640f9dce50c286ab07
4389f44d8e713a9bb096c31c1e74d1f52d1fbed209ed40b34e531425df5e6741
44cca8cba5ff51e2195e4c42279930fec3adf0cec60c38f0827e18f52070cd95
46086a9b833d843d14a1970ee32fbc800cdbcd58e151a358a917164ac7937972
49545b9e3e517aac716172240d7802e11573a8cd3b95a0e7775255215332c1e4
4ad77c7ff8d6fb6d360d9b8a09a5c50a6fd4847393e55351212e2f6e82f3f2b9
4b91fba1ab5d8983f62386771d0ef027518483ef95895a6f88bbeade5cace290
4d2bc1981d95dd0ab6a38d29c6485b8dad25387509e215d37990d8ac3709b7dd
501f7c90a7263d5bc31bb2a536885c14bad5f0a3b0ae29d3ebfdc7b901c76106
5215ec882e86e8604927d2f9da1a9ac3d0f6cb8cb2cf4b53441df2a10602bcfa
5257d16c0c4326698301dbc738acb3d3fd5f24040f48a7a022f8e00d4e5fe763
52cacf28b237a0c90d4a49fd44192565cda0c2ce66fcec9e082fc36bfd4ba4f4
5725c0f9cffd2f3f636860c6e2a9db32acb3488f44a10ff795be12fff64c88be
5740878873df3ee2ddd2e7a0024451f4b3a7a838262a63b40a601d3d57de8b6c
57b0f5d0c79f561bb2d78dc08e52608d1e7bd608a042fd6e941b0d545afa18f1
57de4681808130faf7d191373bbc8f8313104ee8723c748c6f0760eb0cc6be84
5890e9982eae03b04989d3f8f3281d0cc66e453b2911111075946a338f196e26

594ff02ece537d5b89d332028897434d386cef4d6ffd2975df20bafa25dcc73a
5a5e616ef0e077c753837492dbeb00f61df923acd5103b9401b1cde6b30dffde
5b34fdfd16c49176f9e6e5cdeb255aa73c18c4ef0648c89118cb1b17b52c8f13
5f03d2d47de2cae1093e06e63de209ffdc8f2e6d6a2cb119cbe47fdf9b1b7169
606156582d173b7c78124288f7397c6eea3a60712afe55af650f3eeb0f10e909
615ddef68be422aa6be121057665944efe51c39e2bbfdc7bcbe3c9d67eaec6c9
62074e14407f4bc511eaef884985e46bd1162b0131bb672df2221c834291cd56
63b43136ec0bf182f4b07471caca8638ca1fc5697c472b6ec14bd98cca7f83d2
64aeec8e232831a373a4309f94521b986bc12a571cc5db634e70faf06cc7faf2
6baff2f6cfd1547dcbdd72cdc5427d9010e3181e9dbb6883b06f9560ac6269fe
6c9b8b1ff33f3dbec13757ab9b93ad6af34e331c0e0b324e5f4fca5975c721fe
6ce84223848fd5a242a71345717844b20ae65bf855fce533773310b7553d40c2
6d05fd0835601d3f58f7c6d342cd98e5fe3a9f4a1c2ccbc91fa80fb44c61eec9
6df6c61d3a907e743390d59b2a85a7a93bcf497756edaeffa71689d01f5df30e
6e10a01cd9dec093dcf1eb9caa2d4a8209d2d6059899c938b397b75bf04efffa
6eb7889d705322ae1a17f1b7bb05f17e5d428836248afe4463b8e43c29d8deb9
6f48e567e4349e2e25489ac1fd73e0bd367bb1bf61d973ae804ba7fade17a481
71d15488aee41d34d93a37d7f1fd6847fe8afb33a854c5faa19f11862e182a41
73818082e7c7778d880b9ab188d76faa85c61122b5d6a9707879cbfffb52d2aa
73a937492cd19dfb7896e882b4fcf2c4cc02afcac92432f465fda3b227bdd71b
7a4ed17db69f38f93cbc1e7c8bfcdc6a59bed09817dcb5543bced7dd857d5d20
7afc19b6ab1b98ad6468214d6c6f8f5c11672b1fc14c3ad0c02fc6482d1ba13d
7eb224c51850844c03666301bce5552e5f0c837cf25dfc9c61e6f6fe26901fc4
80d8e37e856ada6bc31bdd15d3ef46e47cf2163c6394c78aba7ee026b55a6b2b
8339aaf949af73763c5e6a70a93671acb34144ada73118e2c9b12df9e39fe517
851c250b817a29f5f838f1a745426959e37cea8ce0acacb1d5d7b0a5a90e88cc
8908af6cd4fc4011189cfcaacd849be1d040e14bb47a091709fbbeb01f6e99e0
8bed569623a29053b4afa3b4ae87a4a315e6d7c539495d01cdae226ded6c226b
8cc1181adf15de80334aa3655aa002208d8c486aab3c6ec298ef37524dfced01
8d253d477a880e88aa5e56dfcc9d55b92d6ed74e03c314896fd41624e12e3f77
8d87385c8850b320c8270e97d6701ccf59828b90fc7555fae005424eeabe521a
8e3e1eba03e7086b3a74183de400fca7066e591371698fe294955c546f4d47f0
8e9e1b69bd5522b98140c1a3bc03dc2ce6df4197d6048c61483eeefde45fd116
8ef853df2f6e1f34b1edaf59de47855922e5e0f5032b155b476d81f3d0a8dac0
8efdee7070d9a95a4a5315be53cad8260bed0bc29c7b9acffcdb3c948d2ee9d4
8f0c6aee074c9853dfe141cd9443619a2f571751616d3b57fc77a2d3da045f08
8f982fbabf310f38727905fdd82669e0209986538c035ae98a940599e389bbfa
90c07df000d1bc052aff867da662729ef779053087f39f5e82f4243e8f4cb537
91679c7c3a43531ce40e2ee77fbb7b2c662476e838fd142c669818dd48c4aaef
9222032952132f172b53f0ab9565c80a876b29cd95fcbe30ddaa3e6e839333f0
94686192ec7dd8e3efdf8c623a8e225207db68a24a91f1dae2cc94f659ffa4af

9503ed618a0ae3dfc72db64539e74857e4c29fca168b195918f810b247540b57
967415ea771ff1e6fbce4550f16b452266f68cbffca120254022093ec6813741
96e9194d08285c4dae093f6075771fe0f21778e87b190999a06e84e9d5aef3ec
9751102a45867f2bf42c69dc2e61e3843954e705252fc2856093f418e74b7148
9922b76bfdc024016dde4bbdb94099ac4a6ed95e4843cad3a7c5e1869dbdaef8
9c7dce6ea718136519452bae2af91e745b1c1baa77475d5eeb82f2d1c7c205d9
9d5212a6e90a26a6d1bfc33a3ec46e8d8860b7e396506da8765ebba958194d2c
9e04d1f3e7ca23ced9aabfac6051d0ae653073493eabc78c1d97b79d46f2d750
a05f2c13588ffde0a65432ce0177f37ed19997d77abd2cc98ce71e57022337e6
a08de510f35e7e06ad165ed35d4292990a37f575efd818a6bc06d5edf736fabf
a4b9c4f58b25faa69a49df7b077ad40d8327bb7835bd3ae4093912aad1ec1fc2
a6063a4ddac83a0c12c64756371c74eb6058afc6a91c6cb770e017a52b2abb07
a795784ae28a452a8da93e531ffd1f4430d0357d0ea2760983510f54e19b1bee
a8c47069d1686730953338d5065bf694f4f8534c60147d2f0467cdbdd6e25388
a9db4b5c07b7e20a5ea8b7f523c48a4f0b50bb0936cb2b258a3156a6b96b6ab8
ad27b63b09b63bca658f4014efa2edd009e3879615ee758b53462fb4439ba907
ad848d29b187bc9c72cb49ccecede8093af394820696e7d66dd04d1b4039e5c1
ade05da2338046eb060e4e1170f8bb541ee72cc86fb4118cd7f354062f36aa6a
ae3ab485a1a0a83ecf01ecce2ab33128457ef98a645b15e72aeebf31d50eebc4
b0aaf7d0504bd566433908707857b937b6cb0cc8f4715d8e911eaaba70292b26
b1519746d2c2a349f5fd48d89760bc67161a6474005f9060909bcf2e2c3fa1c2
b1f6dfdb8a754e9280de2ad50b4a86db25ef11e5d38aaeab93c2bb98fa3a80e0
b2c3e64ab3ab1c28a62b304818675d4cceb67883945d05bf39f03b926622d1c9
b36a5693fea5bc4698bd119f82cb58f7614afc7c7c25667fd0ca41554bfa7923
b3c6abf670480a16083371fbbe54e43aae5e790eff0aa861813e51e44ca2c975
b5c594f80d5f76a189ece1257e4d352cd66bbf5e048a214779208e9b9a56e8f9
b8db6f6f7f6e805570cf9ab2031cf820598bf6022457e4235fefe96dada54a0c
ba542af180c3dd6d9a2f2edc5ca201438c0281d1a72aeee0f79607634d3b80c2
bd27f3269d193854a58fbb75d13f3c26ce089bc43d37942ffafbe72c1bf2f68f
bed3f7b320f76cf9f8d681db435aff657da5b036930ff7f54878be6f996f5165
bf086d97fb5c70dcd8f11cf3a5ac6362b9efa523ea55165fd138a87e7058662b
bfd08fb445d1a3818d100a3bc111884821d8ede6460a5f284ef48d6809e2d33d
bfffa800271c615eddc3de34cde6e40c5b59a1c179317743f602e37ec3d081c8
c0e363fe981075690c469fcd067c287d4a29b8dbb091f490ab9c69046c5198a0
c1094cca429221fbcfa2032992dfa4749cd578c84436dd5067ee3aa7ee1b8f15
c37840edb6dddf8301b40eb8ccbe9d9cb46c4627e61351a113e1a2719aec7bdf
c3c7d714e005649cdcbcc10f9c220ef8758360eb6a83439a30dd8bd8342137b0
c73755adfaaec6c30f8aa60297c3ecf9ee9138406ce7d4b72da49d19fcd59d58
c78cbb2242b3c4f7e0e1aea3289c5e8baf9b3f93f4ad92f59d21a6a16c7b6563
c912d0b0fa0ef94d96426995e018e84d44e32f9e3779579e59a5086ea553d63f
c9c354820f02ae6dfc24e0ec2bffe39a23788c33f0a7022088bfdb17980038e0

cb08b8c0588f2fa00b3a5e8242355dbfa727dbf7d5cb0961ff817b1cc2646351
ccd58bef2cbb06d866583c3f7730f7b732668135ac3af082f2e85e38de77e380
cd45e23f088267245341834d20d8dde8179ebd93a8499ee11630fd0e85822f62
d22e0f5cf4f0cd9ab2121bc4d93499f817db516480f38b3d0c231c96b6325fd4
d35467f531f8b4d92138f73118c7a577c5759318b0105e124a68d78a3e9688cc
d40f20372cab8614ed65f313a01d0a06b4cd4e81435fe53211462f130f65ce46
d56df5f427f91252fe323ebdb721f7cdaea54a6c253d3ba23e1eb89d770e3f64
d56f5d0a5b2da4fe33822477a8b491f2f80616acb779be2f6632a43119d34ec6
d5c82fa7b506c1ac8ed30c7a75bf6a742bed00c05ea6a867e9e07b0efa121abd
d61eed6495d66ec5c0af991b418af8f8feaba83378a99261c374e11c7e64f98c
d79a5ecc027e2a8e22c0696042098611e5c8fa56c0d1f84f7a9efdea0278dec3
d8309de59f7718d33b5c2d1da381e60e2be4adea2758e3e804d73730b976d85b
d896e1c310d5d774a45055fe335049d9c8178aee0362110b45fe96dbe3a587bc
da62bcbaf979d67943395094d8cd54a2f02041a0edd3822ce83c46f4ca52b2f7
da97628d24588e7fb6a878c4c97eef5adce978ee1df4edc4ce4f1e717ec5e399
db18e8e273721a438d28a0af0729005b92df1544c25418e5aec74b0395c1a5c1
dd95d433ad338cad9e92a60a6b770d719d2c252aaa1086ba0ac513be240d639c
ddb93bc7fb5a09a4f332bb2efdcc51671521c6034d87119f68917c18592aaadd
de5ff2a86b9b97821a627ee23d91fecfc32dcb3d5db129604ca5c47f4feb102b
dfeaa43aef65196242d0b83e285cc19d0466c5569071aa03c90b760efeeddd47
e0b4a8200e1aa5f0fb554fec161b466f3d9a6e49b7d5ea436b1c72f7fe9376df
e159458d4bc5114c9261dfedaff530c0bea0b0d109555197f3fb7747692e538e
e1f1cce4d268ef9cffda9704ca7c421bc9efd109c50cb3c9b1491423481da4be
e2128d842ea9c4bab5165962173991eb6ff5d3b4f867cd40b4e7c3795e710917
e230a0e4fd7e475cabd49337e97a876bd4a8d060abc7ff1543c2205f28f9b639
e34317bb799040db5ac6d4821d19f6d0b9dba1ed1151217f3af0cd4ff1cde887
e944c16047fadc8d0a07b5dbb4be4f7d8c809533eb993835ed2ca4ee77627253
e9dddb9c45be4bdea8979c858ffcd44610b0e57e6270b3839ec1f9578862c5f3
eb90ac416eaab1746f3abdd17df32808b9d46a647b8bc1d2513dffb37364a508
efa0c6db8eeb3d6afe3393e68ffa3e026db22ef4bca549f37cf270969db12f56
f0e0bd710b0178b6000d573906078f6906c0cc4781b7634a9e0dd95d33785aa9
f4b770344e78791146677dc8e1fa4d56fcb574605948de9381aeaab6a0b9bf74
f5aa4f4153127a7f9f370caec764490889225ee2d1be6302a80ca1821c5c2804
f69d80723388387365060c795e3574955dfe37329979dfb222f64217e4077b63
fafd66b6d56510fd6afacd580ecb8bac519930d60e8e2b981a1caf91ab25f3d4
fb202daec090f66e34ad0172964a1a88d0787c1ce5caa29fb7793fa5df8b760e
fbc43602b9ab1be7385409ab752e3cfd45ee7acb0cf67d66f5d357019bbe3bed
fce230cc51f22d3300a491125869d2d269a62848b60d641218f36cd92e7ec261
fd8d355ef99846ef00d7fd6db12f7a93667aded995b8d7feb5fb27a5853b8714
fe0adfcbe96e41a03d65dd47514b5db3b216690ca8d3c1680a913e6927e27195
fec4e874fea735e68d8d2416e64a3246c9f7075c27e3fb037291430f092d9192

IoC Descarga malware Urls

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

hxxp://khoweb[.]xyz/wp-includes/OaozkN/
hxxp://amarettobh[.]com[.]br/sys-cache/eXhf8Nc/
hxxp://caorauducvan[.]vn/wp-admin/PCsGWi/
hxxp://sehitgazihaberleri[.]com/wordpress/W5e1D/
hxxp://oggisivola[.]it/5doedb3/3Nk/
https://hauizone[.]com/c4ccx/sD/
hxxp://zhaniyasoft[.]ir/wp-content/file/ANEbg/
hxxp://51[.]254[.]140[.]91:7080/vqSGfDP3PPYUjJYiu/wn0iwMDz7/wPwmPrdi/HM9S4/
hxxp://162[.]144[.]42[.]60:8080/7PAHmBBn/mMJS/RrJuwpfHs/
https://blueyellowshop[.]com/wp-includes/mihae8A/
hxxp://kingsalmanquran[.]com/wp-content/wuPyeI/
https://dagranitegiare[.]com/wp-admin/Z21r6R/
hxxp://acontarborreguitos[.]com/acontarborreguitos/I/
hxxp://atenaclinicaesegurancadotrabalho[.]com/cgi-bin/NlMH/
hxxp://digitalbazar[.]com/wp-admin/RVEzrK/
https://byc-center[.]com/wp-admin/Z4r/
hxxp://castlestudios[.]com/images/Z/
hxxp://khoweb[.]xyz/wp-includes/OaozkN/
hxxp://amarettobh[.]com[.]br/sys-cache/eXhf8Nc/
hxxp://caorauducvan[.]vn/wp-admin/PCsGWi/
hxxp://sehitgazihaberleri[.]com/wordpress/W5e1D/
hxxp://oggisivola[.]it/5doedb3/3Nk/
https://hauizone[.]com/c4ccx/sD/
hxxp://personalizzabili[.]com/images/lvyX7QK/
hxxp://www[.]bismarjeparamebel[.]com/u/qkhyf/
hxxp://agenciatabletshouse[.]com[.]br/erros/1PM/
hxxp://desk4succes[.]nl/stats/cNFjYB/
hxxp://westerndata[.]com[.]au/wp-includes/3jp/
hxxp://graphicom[.]it/cgi-bin/HsPkL/
hxxp://oneinsix[.]com/test/1F4c/
hxxp://academiadotrader[.]net/wp-content/f/
hxxp://whitegoldinitiatives[.]org/wp-admin/d/
https://lifeadvicer[.]com/wp-content/L/
hxxp://intc[.]solutions/wp-content/qi6/
hxxp://sanatcifiyatlari[.]net/dup-installer/5/
https://www[.]letslearntech[.]com/wp-content/u/

https://sublimatransfer[.]com/backup28082020/Ir/
https://blueyellowshop[.]com/wp-includes/mihae8A/
hxxp://kingsalmanquran[.]com/wp-content/wuPyeI/
https://dagranitegiare[.]com/wp-admin/Z21r6R/
hxxp://acontarborreguitos[.]com/acontarborreguitos/I/
hxxp://atenaclinicaeseguranca dotrabalho[.]com/cgi-bin/NlMH/
hxxp://digitalbazar[.]com/wp-admin/RVEzrK/
https://byc-center[.]com/wp-admin/Z4r/
hxxp://academiadotrader[.]net/wp-content/f/
hxxp://whitegoldinitiatives[.]org/wp-admin/d/
https://lifeadvicer[.]com/wp-content/L/
hxxp://intc[.]solutions/wp-content/qi6/
hxxp://sanatcifiyatlari[.]net/dup-installer/5/
https://www[.]letslearntech[.]com/wp-content/u/
https://sublimatransfer[.]com/backup28082020/Ir/
hxxp://castlestudios[.]com/images/Z/
hxxp://khoweb[.]xyz/wp-includes/OaozkN/
hxxp://amarettobh[.]com[.]br/sys-cache/eXhf8Nc/
hxxp://caorauducvan[.]vn/wp-admin/PCsGWi/
hxxp://sehitgazihaberleri[.]com/wordpress/W5e1D/
hxxp://oggisivola[.]it/5doedb3/3Nk/
https://hauizone[.]com/c4ccx/sD/
hxxp://personalizzabili[.]com/images/lvyX7QK/
hxxp://www[.]bismarjeparamebel[.]com/u/qkhyf/
hxxp://agenciatabletshouse[.]com[.]br/erros/1PM/
hxxp://desk4succes[.]nl/stats/cNFjYB/
hxxp://westerndata[.]com[.]au/wp-includes/3jp/
hxxp://graphicom[.]it/cgi-bin/HsPkL/
hxxp://oneinsix[.]com/test/1F4c/
hxxp://kinotheque[.]com/wp-includes/os/
hxxp://vandamebuilders[.]com/wp-includes/Ess/
hxxp://raintoday[.]org/wp-admin/wm/
https://intenswel[.]com/wp-content/qM1/
https://himosaandnasa[.]com/lfnwz/um/
hxxp://buygrowtogether[.]com/amfxn/G4/
https://xn--mgbao2hg[.]net/cgi-bin/1/
hxxp://nehircim[.]com/lunkx/rH/
hxxp://cialisuqol[.]com/zaf1hlz/jNf/
hxxp://tarun[.]pro/cgi-bin/bdV/
hxxp://deletegoogle[.]club/wp-includes/Ub/
https://kamagorder[.]com/wp-admin/Di/

https://sabai-massage-thai-nc[.]com/tmzcc4d/SJZ/
https://youxel[.]com/sys-cache/r/

IoC nombre de archivo

Nombres de Archivos con Malware

RFQ#F44E0741.rar	2586 ZWB-0399943.doc	SBA-090120 HJI-091420.doc
Asif Professional CV.xlsx	Misin Cena de liderazgo comunitario Invitacin a reunin.doc	YJ 96-27639.doc
$9,424.08.zip	ID9333182404UY.doc	KKI-090120 LLM-091420.doc
RE CITÄ€TS.arj	Todos deben venir a la reunin maana..doc	Arch_092020_26-91785.doc
INVOICE.pdf.gz	320480-SHA_08935290.doc	DP3022309911TN.doc
20201409_82-0-97844379.doc	Datos 9_911661.doc	50%_swiftoutput.zip
Alb. 12-5-5596794.doc	Documento 092020.doc	OAA-090120 NDG-091420.doc
ISCINV0477061-VIACO-update.zip	Siguiente junta.doc	UTA-090120 ZNJ-091420.doc
doc_35225.doc	Documentacin 0920.doc	Documento 1409 41881.doc
IM-1736 Medical report Covid-19.doc	mensaje-1409-2020-31605.doc	TC6455881314AR.doc
Shipment Document BL,INV and packing list.jpeg.ace	PO# 09142020.doc	0926-86-0446208.doc
NK2361910606YN.doc	nuestra reunin del mircoles 28 de sept..doc	facturas vencidas y datos bancarios.img
PO# 09152020.doc	informe 14.09.20.doc	Declaracin de nmina de septiembre 2020.doc
Datos-SN-5057316.doc	orden de compra.r00	Informe de nmina de septiembre.doc
TAX CLEARANCE CERTIFICATE M.html	FILE A_7668.doc	po n-9685#.doc
Prxima reunin de finanzas.doc	55_1409_K-2812.doc	PO.pdf.z
FA# 09142020.doc	Alb. 99-8-0901297.doc	Payment Reciept Number 3939.iso
Facturas de septiembre.doc	3094.doc	dhl_doc876567686756.zip
FILE-45-9956.doc	Adjunto 092020.doc	Galmon Order and Specification.rar
RST-090120 RJU-091520.doc	INV_83082.doc	36 1409 092020 E_3805.doc
Shipping_Document.pdf.html	6504436_092020.doc	Mensaje_092020_22_4478

75.doc

YKG-090120 WSW-091520.doc
Quotation.iso
FILE_1509.doc
Todos deben asistir a la reunin de maana.doc
Protocolo de la reunin..doc

Nuestra reunin el viernes.doc
Reunin de emergencia.doc
Form - Sep 15, 2020.doc

{:REGEX: 20.doc
BX9560261563UU.doc

Factura 1509.doc
INV_8552.doc
Datos_2020_ZZC_807744.doc
Info 15 77-96651.doc

Archivo-2020-7660.doc
Factura para mes de septiembre.doc
Documento_092020.doc
N.237494 15.09.2020.doc
816582.doc
Copy invoice #4922.doc
FA# 09152020.doc
Prxima reunin el viernes.doc
factura 15.09.20.doc
La reunin se llevar a cabo el viernes..doc
2020-09-15 Fra. 62302.doc
20201509_PE65-492
IN65591311.doc
Prxima reunin ordinaria el viernes.doc

reunin regular el viernes.doc
Alb. 55-7-321483.doc

Declaracin de septiembre.doc

Correccin de la nmina de septiembre.doc
2020-09-14 Fra. 261807.doc
DG5219605610AM.doc

INFO 14 092020 933-80638.doc
VNS-090120 LQC-091420.doc

Factura 0920.doc
Documento_2020_X-2276.doc
KC2432_092020_66-3910.doc

Arch 092020 492-4120824.doc
4359 factura septiembre.doc
Archivo_1409_092020_SN-8863.doc
5160_2020_059-33030.doc
ZYS84512_2020_00132268.doc
info-2020.doc

Form - Sep 14, 2020.doc

XSF-090120 UFJ-091420.doc
MHM-090120 DCP-091420.doc
INV_89542.doc
494388.doc
INV_790171.doc
Adjunto-092020-29586.doc
0151500 2020.doc
NL 39-3856242.doc

FILE_CY-43975.doc
Datos_2020_PC_905246.doc

Adjunto 7_53554.doc

QJV-090120 YBU-091420.doc

ESZ229620_14_2020.doc
RG0739548771SE.doc
Attachments-20200914-1260642.doc

893-2020.doc
attachments.zip
Invoice payment.pdf.z

MK1106319A.xlsx
MK1106319A.zip
Nueva orden de compra de DIXION,pdf.iso
mensaje_T-54557.doc
Adjunto_1409.doc
pedidos estndar #5688_3456,pdf.iso
57024 2020.doc

OY0582403269GT.doc
94126 3-8008.doc
Arch-1409-O-1172271.doc
DAT-60424865.doc
NKR-090120 PTU-091420.doc

Invoice 2020.docx
message12845.pif
file-092020-10-7379.doc
Arch_14_228-0413.doc
Alb. 11-3-6594559.doc
Alb. 276_00078.doc
Proforma Invoice - Copy.zip
Produc_listing_787.img

PO#904600 140920.doc
202011 HM.doc

941.doc

message.pif
AMI-090120 KBR-091420.doc
VX000080.doc
2020-09-14 Fra. 18255_00063.doc

DAT 2020.doc	Copy invoice #096837.doc	PAYMENT TRANSFER COPY.zip
INFO-1509-2020.doc	3181289.doc	N.2886541 14.09.2020.doc
Estimativa BZ003924.doc	Alb. I0004667.doc	Documento-1409-2020-14932.doc
CONTRATO 14_09_20.doc	Factura 14.09.2020.doc	Adjunto 849849.doc
JT 91-7604885.doc	N.55 ZR 14.09.2020.doc	755.doc
36645_0001 factura septiembre.doc	FQQ-090120 QMW-091420.doc	7325_8-645621.doc
FACT - Sep 14, 2020.doc	UAI-090120 YZP-091420.doc	mensaje-2275.doc
WNK-090120 ZNZ-091420.doc	Inv_66623.doc	QUOTE 2020.pdf.gz
LJI-090120 ICX-091420.doc	NCE-090120 VPY-091420.doc	MG00057539 factura septiembre.doc
TZP-090120 UME-091420.doc	UNTITLED-2020.doc	IB88-521 DR2967.doc
FILE H-8924.doc	79899208_14_2020_EB-1079.doc	DAT-14.doc
737220-14-518311.doc	ORDER ITEM#914_2020_PDF.gz	Vessel particulas.zip
PO4299832205MA.doc	20201409_0076.doc	CONTACT DETAILS.zip
BL-DOC-20200716-07594-PL#04829.pdf.gz	NAMRU6.xlsx	XHL-090120 PSY-091420.doc
Bank_Payment_pdf.iso	Proforma Invoice CWUSKRUDH.pdf.z	JLF-090120 ZCX-091420.doc

IoC servidor smtp

Direcciones IP del servidor Smtp de donde fue enviado el correo

172.93.184.181	61.126.24.28	185.58.73.24	182.163.127.209
185.161.209.150	103.241.128.174	103.195.184.175	103.10.223.16
156.96.119.22	162.241.53.22	46.101.170.190	95.217.102.131
82.223.70.126	219.109.143.134	197.221.10.75	198.54.114.159
219.99.208.167	165.73.140.14	153.120.17.84	67.23.248.122
202.216.97.31	212.68.61.41	67.222.108.72	200.147.35.75
173.203.187.69	176.119.210.162	54.64.242.132	197.189.201.235
196.25.187.130	204.93.178.28	43.228.184.227	198.199.82.141
197.112.2.6	65.49.80.89	119.92.116.77	66.34.138.227
45.143.222.16	148.245.131.94	190.61.250.131	66.34.138.227
103.3.168.19	203.1.69.2	203.160.58.6	31.186.28.24
178.18.200.13	202.155.27.140	46.30.212.0	31.186.28.28
51.255.213.114	219.118.68.207	200.45.0.217	173.255.227.24
162.144.145.178	202.221.162.11	200.45.48.8	37.59.252.58

60.250.159.100	202.221.162.39	154.70.144.70	210.163.51.33
178.20.231.225	203.160.56.35	195.8.59.49	72.18.132.9
150.95.255.196	210.131.4.98	195.200.78.249	95.111.224.35
105.28.118.129	133.242.215.93	189.113.175.11	96.44.174.200
170.249.203.90	129.232.148.98	104.148.61.187	41.221.32.206
23.111.165.178	116.12.55.236	72.34.16.20	23.111.139.228
193.106.246.3	207.180.197.156	210.140.74.85	104.148.61.174
62.210.78.57	67.23.234.103	62.108.227.185	51.91.64.57
103.133.106.134	103.14.99.61	200.63.192.27	195.201.5.112
31.186.28.23	210.230.216.239	195.29.150.135	66.96.189.7
210.233.81.2	210.131.0.50	103.142.214.6	34.192.101.164
203.147.156.18	203.152.216.226	108.166.43.94	205.251.155.65
210.224.185.225	198.23.53.43	220.247.222.58	190.116.55.180
210.130.137.3	59.106.165.164	159.65.161.32	194.126.4.66
112.213.90.59	65.254.253.50	122.219.254.44	194.126.4.79
113.34.78.228	59.106.171.96	49.212.235.95	192.64.78.30
79.98.29.209	60.43.152.181	195.62.175.162	202.22.232.43
211.5.114.131	183.81.155.98	54.38.80.178	167.99.191.201
118.82.81.163	178.79.190.7	162.241.157.244	216.194.164.187
82.145.32.99	202.216.97.12	64.140.165.106	203.146.237.187
197.242.151.110	190.14.159.6	139.138.58.140	136.243.124.198
111.221.40.221	23.227.134.218	79.98.39.243	72.249.60.194
118.69.170.246	189.113.175.56	27.34.154.55	118.97.118.130
200.29.96.35	69.16.233.137	156.96.47.119	210.152.9.52
197.189.201.235	104.244.124.160	195.182.87.11	219.99.208.197
78.142.63.48	50.28.79.140	210.152.150.114	219.109.138.62
62.108.227.193	80.85.33.13	123.200.0.5	196.46.192.45
175.177.0.6	219.99.208.66	193.142.58.11	149.72.163.198
62.149.156.105	62.171.130.71	103.125.191.145	151.252.56.182
197.189.198.114	210.226.44.22	104.168.237.188	188.165.178.14
145.14.14.25	152.89.233.10	167.88.160.229	210.131.159.96
200.147.34.34	191.101.165.202	200.63.192.9	148.251.90.100
198.23.59.142	200.58.101.11	103.130.100.16	185.222.57.201
80.77.147.178	200.58.101.136	162.241.104.29	83.65.238.15
95.216.149.58	91.148.168.28	59.125.10.91	80.85.33.13
51.15.151.169	186.225.1.9	217.18.4.10	210.134.90.8
203.205.250.101	186.1.31.37	209.59.140.28	161.35.2.157
187.51.211.5	85.10.225.200	72.52.252.138	81.91.177.62
202.66.175.38	94.127.7.149	208.80.12.126	50.116.124.69
194.24.250.131	95.110.193.164	104.43.18.9	192.185.194.16
91.230.192.160	91.148.168.28	209.58.149.74	210.152.9.52

102.22.81.39	62.149.156.120	81.42.224.67	219.99.208.197
191.252.30.3	185.80.1.136	87.253.233.125	219.109.138.62
104.247.79.212	51.91.30.65	87.253.233.139	196.46.192.45
46.245.193.175	184.106.54.113	203.167.7.62	149.72.163.198
158.69.184.120	184.106.54.115	210.255.115.36	151.252.56.182
50.116.76.140	93.89.232.210	45.138.172.120	188.165.178.14
191.252.30.19	109.245.241.198	104.148.61.184	210.131.159.96
45.76.59.173	192.185.50.45	128.199.30.176	148.251.90.100
160.119.100.127	41.217.220.14	212.200.253.238	185.222.57.201
103.132.144.86	192.175.105.166	103.252.255.69	83.65.238.15
190.105.225.25	63.143.40.2	140.227.244.23	80.85.33.13
197.189.247.38	162.254.149.196	80.85.33.13	210.134.90.8
203.130.9.13	154.0.161.22	210.233.73.163	161.35.2.157
177.101.150.117	192.185.148.104	211.13.204.74	81.91.177.62
178.162.212.203	217.70.240.137	192.185.144.80	50.116.124.69
185.194.124.36	210.172.192.97	69.89.23.191	192.185.194.16
46.105.41.134	192.185.46.225	195.222.0.3	203.29.125.101
67.227.227.189	192.185.184.48	129.232.238.146	192.185.51.196
185.221.216.58	203.138.209.188	37.48.85.204	144.76.38.75

IoC Correo Electrónico

Correo electrónico de donde fue enviado

purchase@fluidcontrols.com	eduardo.mendes@edr.com.br	jzgelbolingo@crestcebu.com
0111@yotutuzi.com	egle.skeiviene@telsiai.lt	kapistec@eurofarm.com.mk
056.fi@torrescorzonissan.com	ermanes@rcmloc.com.br	kawan@sankyoo.co.jp
316sawamura@seikyo-seki.jp	eservices@firs.gov.ng	keiribu@marutama-net.co.jp
4.fiorentina@afmarezzo.it	ewinmedical@micro.co.bw	ketcdutj170goauc@gmail.com
a.balikci@kayaden.com	exinsts@gmail.com	kimgarr459ypx@gmail.com
A.poursaddami@rayavin.com	express@sf-express.com	kkato@e-matsunaga.com
Accountant@maximixe.com	facturacion@jjinternacional.com	kotake@saito-shoji.com
accountingdxb@splendid-travel.net	faeza@apexautoshield.co.za	koueki@g-shakyo.or.jp
accounts.kampala@freightreach.com	faisal@ibd.net.bd	koujibu@yotutuzi.com
accounts.mahabubnagar@renault-india.com	fanie@dekockandcronje.co.za	k-yashima44@goda-s.co.jp
accounts@abchina.com	farouk.ayub@mushko-ps.com	kzaman@adroitbd.com

accounts@turtlenest.in
admin.bpn@josuabersaudara.com
admin@chosenengine.co.za
admin@glplastering.com
admin@greendropfarms.com
admin@maxmeen.com
administrador.07@fincaprimavera.com
adminsteelpoort@rkdengineering.co.za
advokat@advokat.co.ke
aji@kiaceramics.com
akhan@ialpak.com
al@nixusedcars.com
alalbayt@inco.com.lb
ali.akpinar@regormakina.com
amadorcarballal@wanadoo.es
amasundu@vodamail.co.za
amedo@wpi.com.pg
andersonkingsrol@gmail.com
andrea.martins@victoriaarmazens.com.br
angelica.hernandes@key.com.mx
anittiff04lvjai@gmail.com
antonio.arroyo@corcimex.com
anything@507.maxzizo.ga
arapoti@transval.net.br
areti.siozou@sevpde.gr
ashwani_sharma@owmnahar.com
b_sadiwa@megamasterlink.com.ph
backmt@easyautomotive.com.br
barve@pirh.si
biserka.radovanovic@ilincic.rs
faturas@paranalatex.com.br
fax2@anmaki.jp
fbraun@cpachile.cl
fernando.palafox@mazdavalle.com.mx
fernando@mosmail.co.za
finance.bali@rsp.co.id
financeiro@altoeadvocare.adv.br
financeiro@omggraduados.com.br
florjone348nz@gmail.com
gacem.n@ems.dz
gaofei@cn-alloys.com
geracore539tyz@gmail.com
geral@iautocarcenter.com
gerencia@cemac.org.ar
gerencia@gruponacsa.com
gerenteventas@fomtexcentroamerica.com
gestionh@traatlas.com
gujranwala@cliveshoes.com
gunnclar77yiryo@gmail.com
h.badali@turbinemachine.com
haberes@villaregina.gov.ar
haider@supernetesolutions.com.pk
hakan@aep.com.tr
hayashi@ishikawakensa.co.jp
heisei-mitutosi@world.odn.ne.jp
henning@timetrucking.co.za
hgonzalez@mazdalastorres.com.mx
hoantk@c21.com.vn
imran.wali@bilfinger.com
info@abc-tool.co.jp
lab2@greenvina.com
labodega@grupambasori.cat
laboratorio@redimat.com.ar
lalan.maulana@dls.co.id
linda.chee@galmon.com
lisa@g4.co.za
lneshuku@napwu.org.na
loan@kpwoodworking.com
lorence@shy-blind.com
m.rus@pharmconsult.com.pl
m_oohira@ask-s.co.jp
macabel@dunkindonuts.ph
magali.bottemer@toulon-avocats.eu
magsardegna@ltsolution.it
maheen.r.s@dadabhoy.edu.pk
maintenance@medicaids.com
manutencao@biasiconstrutora.com.br
maponce@rigbapromo.com
markbrown@semesearchtechnologies.com
marketing@turustour.com
martineza@human-resources.com.mx
matheus@cantuvda.com.br
mecanico@frivasa.mx
meice.moura@grupomouraam.com.br
melville@dtamaritime.com
metafora@metaforikos.gr
mfg@swanindia.com
michhyma42eseq@gmail.com
michhyma42xm@gmail.com
milagros.cifuentes.ln@mail.co

m

bitval@datanet.ee	info@afriqueinfinity.co.za	miyabe@dcorp.co.jp
bjreddy@designtreeconsultants.com	info@amicidellavalcolla.com	miyama.daiju@garde-intl.com
boksburg@thomastyres.co.za	info@aria-one.co.jp	mohamadkhani@khorshidbarsava.ir
brasta@manovonia.lt	info@arvindproduct.com	monica.alvarez@coralsa.com.gt
brian@edisondialysiscentre.co.za	info@askinberbersigorta.com.tr	morita@asahi-electric.com
brucomac@latrobe.net.au	info@breeze-bell.com	mrodriguez@confecielito.com
bube4@maler-buchholz.de	info@comune.sestola.mo.it	nagano@sg-sogo.co.jp
budiman-hrd@greentextile.co.id	info@dunlopillo.nl	nandipa@executiveplacements.com
buencillo.doris@ct-bond.com	info@enkayhomes.com	n-hirata-psd@pp.em-net.ne.jp
c25@hahncollections.co.za	info@eteria-al.com	nigel@pbrands.co.za
c46@hahncollections.co.za	info@fujita-senzai.co.jp	n-iwao10000@kdsgr.co.jp
carinayacanto@caja-abogados.com.ar	info@hasansoltani.ir	nks-eto@aso.ne.jp
Cary@KatahdinLLC.com	info@irsce.org	no_reply@dhl.com
cdarequipa@corporacionadc.net	info@ishikawakensa.co.jp	nobari@sakoogroups.com
Chipo@surteegroup.co.za	info@j-s-m.jp	noeochoa@cue.satnet.net
claiton.santos@redebrasil.com.br	info@kingoriadvocates.co.ke	non710@ictv.ne.jp
clipperturismo@uol.com.br	info@neimarine.com	nour.safetli@protechgroup.me
comprastallerlm@constructoragusa.com	info@nitto-reform.jp	nurse@thedoctors.com.au
comptabilite@eijc.nc	info@olympiaeurope.com	nuwaraeliya@kreston.lk
comunicado@sys-prontius.com	info@omke.gr	office@nfvoe.at
contabilidad@focatransport.com	info@pandaga.us	office@timelektro.com.mk
contact@aduanaylogisticamx.com	info@pasticceriavarriale.it	ogawa@morimatu.co.jp
contadorlt@mazdalastorres.com.mx	info@pibajio.com	onex2@ushibuka-cci.or.jp
corinna.li@dhl.com	info@trasaadria.hr	opscni5@cargomen.com
countersales@boltboyz.co.za	infocr@asopwc.com	orcamentos@pedro-moreira.com
creditoycobranza1.ags@torrescorzonissan.com	infomation@katokogyo.co.jp	order@brightoman.org
dandung.setyoko@bnimultifinance.co.id	infopajak@99teknologi.id	organic@atlasfoods.org
dang@prudential.com.np	inplant.cajaplax@tergum.com.mx	otiscatr45koho@gmail.com
daphne@indomaguro.co.id	isendana0pg@gmail.com	patrhoyt29t@gmail.com
dety_acct@koinbaju.co.id	ithelpdesk@sharpsight.in	paul@rcfcmb.com

dkollias@eggs.gr
dte@clinicalasacacias.cl
dumvadi@visikatli.lv
dysonkizz7fawus@gmail.com
edp.service@tanishford.in
edp@veeyesfoundry.com
eduardo.borges@agrofava.com.br
swang@oceanlandchb.com
t_takeuchi@sakaigumi.jp
talento.hh4@tvcable.net.ec
tamar.todua@toduaclinic.ge
tanaka-syou@sincol.co.jp
teodora.halacheva@aquachim.bg
thomas@optima-lift.com
tram@phanthietgarment.com.vn
trichardt@jayteetrading.co.za
t-sengoku@yokoban.co.jp
tufail@gegcc.com
unrecognized.mail@dobipress.bg
vendas1@actioil.com.br
vendas3@milainox.com.br
ventas.gt@fernandezsera.com
ventas@puertonuevoantofagasta.cl
ventas2@hierrosur.com.uy
vespucio_100@sade.cl
vessel-it@marfret.fr
vgclemente@arnet.com.ar
vipechi@gmail.com
voraisai2dry@gmail.com
voraisai2e@gmail.com
ivan.markovic@wdconcordwestdoo.com
jaider@activezipper.net
jayden@panocean.com
jayson-salario@wellbemedic.com
jonespatr72iocwa@gmail.com
jp.humbert@villette-sur-ain.fr
judivalo036raeeo@gmail.com
sales@dixion.de
sales@hzafl.com
sales@tyen-axle.com
sat-rijeka@ri.t-com.hr
secretaria@transur.net
sekisaikan@shibasan.co.jp
serviceacte@huissier-77.fr
shafiulalam.impl@ifadgroup.com
sheila@mukongoloadvocates.co.ke
shimoura@art-shimoura.com
shinsei@seisakusha.co.jp
shipping@dhl.com
simone.gori@simetlc.com
siraj@durranilaw.pk
smisg@superad2.com.sg
smu@george.ph
sparcapelsebrug@despar.info
sparkroeze@despar.info
stanley.tonui@pct.co.tz
stavros@wonderland.gr
sumon@fizbd.com
suvimol@pg.co.th
suzana.ksela@mobilehouses.eu
payroll@ganada.co.id
pecas@evolutioncar.com.br
peme1.support@supercare.com.ph
psmain_acctng@bhf.com.ph
pyledary522dzidi@gmail.com
qualidade@augemm.com.br
quality@albarakahdatesfactory.com
ralpzand8mvios@gmail.com
realchimaltenango@pizzapizza.com.gt
reception@mreales.com
reception@nissanec.co.za
revai@ascodan.co.zw
rh@bmwaguascalientes.mx
richard@serengetiestates.co.za
rnivo_vp@vivetic.com
robert@questmerchandise.ie
roddorva8spuu@gmail.com
rogelio.miranda@tropper.mx
rokunohe55sho2008@r15.7-dj.com
rosiane@eletricasenior.com.br
rosy.arce@grupocadena.mx
s47daiwa@pear.ccjnet.ne.jp
sales.sd@bharatheatersindustries.com
www.1234.www@iris.eonet.ne.jp
y_takano@kyotokango.ac.jp
yarngodown-zta2@libertymillslimited.com
yoshida@yamaguchiseito.co.jp
yuxianzhao@yinlun.cn
zzzzrzs_beograd@mojdoktor.gov.rs
wsAccountsPayable@wsgc.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.