proofpoint

Indicators of Compromise

21de75a8d9d38f342b508015d7a9a7021cea85c29d2f7fabd1ec29be545806b6	SHA256	CryptoWall/H1N1 Loader Document
4de3f3789c70eef3a8eeb0f8934e6b2dfcc27dd7e0c38be428f45f6d7ee2d58e	SHA256	CryptoWall/H1N1 Loader Document
f135871e5d8a2455db8f6c961f701a4f3ba61e9c17698f8f7821679825e12ce2	SHA256	CryptoWall/H1N1 Loader Document
e099d716b97b694468e99419e62151a11ac2ad4858677c3faa1fb31c68d4fe50	SHA256	CryptoWall/H1N1 Loader Document
31181877c62da67b7e4f8805e9054d35aa00f79cef01340fde6262aff2c9607a	SHA256	CryptoWall/H1N1 Loader Document
040ddf1e583eb33531e41017cfdb7337c436697ee493d77827ba8ee50f11125e	SHA256	CryptoWall/H1N1 Loader Document
8fc3fad15e02a8c865c9c73e27d983cf8bface6575b3b3775222a558ac1d5205	SHA256	CryptoWall/H1N1 Loader Document
524495ca590a960f3710622431120f52866fed0e633a5b0e128069e80717fac4	SHA256	CryptoWall/H1N1 Loader Document
1bad34fdbfc2fdf9f4486ef2ab5cca2348a44a3eb1c59885062fcf8b627f2f60	SHA256	CryptoWall/H1N1 Loader Document
51d1452fd0537f0d241ad74d1bcbf42804e15a8a2df33b84258d3a0e290e1369	SHA256	CryptoWall/H1N1 Loader Document
d51191890c6d9c4a524c41ed611a0d9f956b73b8d9068d59772b4bbb818be2eb	SHA256	CryptoWall/H1N1 Loader Document
ddb2975dfd45053c3ca68cdf6131639bf662a4b43ce44e004cc17b5ef4f08acf	SHA256	CryptoWall/H1N1 Loader Document
da5f1a08d01c09ee1d942ffa92dff20ff758af9c71fea0f699bb0223b1bc85e4	SHA256	CryptoWall/H1N1 Loader Document
928051dc3460670008132fe98f325c2688f1c68ebfe25a97137d9259a96cbb60	SHA256	CryptoWall/H1N1 Loader Document
19e9d53a16f6094f44dc909a6239e5d03d16b98878e3fa3806908b817d3074f7	SHA256	CryptoWall/H1N1 Loader Document

f49b264cb0db37e492095f87caca1db9c44c92138ef4ddc841ce50198f3cc07f	SHA256	CryptoWall/H1N1 Loader Document
144e781370a53e027770c58a0bc8c491a038ecee0b63f0e3ba15cc7cbbddabc6	SHA256	CryptoWall/H1N1 Loader Document
bb1c2d771c7dc2aa9d9e799946107d34c5935ba6fe627d8e454d0648c20e19ed	SHA256	CryptoWall/H1N1 Loader Document
c9d175bb2420753fb679896219cdd581109c1404899a3cff195c4a8b795fcbbd	SHA256	CryptoWall/H1N1 Loader Document
661c1825c1818c781281eda993e5684c0597d9547d01ccb4b68d034cf58bbfc0	SHA256	CryptoWall/H1N1 Loader Document
dccc3a03103dcd3523fef6cdc9e2d02508060bbf1cd72deb6b65ba106341d76d	SHA256	CryptoWall/H1N1 Loader Document
b8a6cf0d62bc0a933c19f70ec6e265ada2c9dcd161345721653574aec121bd9f	SHA256	CryptoWall/H1N1 Loader Document
d584665d1d77b2052857188a44891ec389f123d8ce11ab6640689032c96e6ee0	SHA256	CryptoWall/H1N1 Loader Document
df5ce6f870c6a48c806ec8db43a0e1c4b3492e04b7308342480e7016f9da543b	SHA256	CryptoWall/H1N1 Loader Document
df97bdf25b8a7247ac30b9215ec17f757b981bf0cd498c579e341361aebd09bf	SHA256	CryptoWall/H1N1 Loader Document
b38968437a93214ade3fdca50075d9247c587502ea209f06b4feeb54f87069d5	SHA256	CryptoWall/H1N1 Loader Document
e51eb50026de6fa3f57906e71d9ce856b53dae9d7a84dd6e95b17a3d52cb3794	SHA256	CryptoWall/H1N1 Loader Document
51d52d5dac1a9e6cdef7f07d3322911bce8cd93acf5bcc46687eb51811e5a999	SHA256	CryptoWall/H1N1 Loader Document
13894603776bc7a0e96e504de5b4505322a8e50483f0a7b56fe647b97116400d	SHA256	CryptoWall/H1N1 Loader Document
bdcfa45c64988dbf3ce482e9a004c987df5748540f0575531c46dd4b156af4e7	SHA256	CryptoWall/H1N1 Loader Document
9bb6a2e798b6b8b520590a198f18bfad9fc2fb5fdfd24bc5c255d44eb22775a6	SHA256	CryptoWall/H1N1 Loader Document

934553d6d71df95909a79011e7fe54c02ed36db6d91b1118810809ee2e45977d	SHA256	CryptoWall/H1N1 Loader Document
219e6cc0b503c5155d6343db57afc520e8e92a9660fe7215c9fdf68ef4a2e16c	SHA256	CryptoWall/H1N1 Loader Document
b0b33d0b9e8ab14d6f32fe9969f8a95154a12e9d6f86af30944fbb9c0b995fae	SHA256	CryptoWall/H1N1 Loader Document
23ad10b10cb54c3de5b72f685ab1c650a69c97a972788987a9143cc227908027	SHA256	CryptoWall/H1N1 Loader Document
960be0b5eb436de2f09425c17f94dd65fd71661c66898945d56187f783d1bd8d	SHA256	CryptoWall/H1N1 Loader Document
cfec9a8f9ab1369b410dfecc307188fcd319c1a171b5e18c6bb064de3074457a	SHA256	CryptoWall/H1N1 Loader Document
7a0dc4ab55694a368f2094d7c96544664a65d4fecca64065fdf8e386b6fd1e74	SHA256	CryptoWall/H1N1 Loader Document
7afe159eae74acfb3ab66955f8c4548fc8c122e61c3bb6eb1eff315a2ed370b2	SHA256	CryptoWall/H1N1 Loader Document
04804b92f283fc0bad586b08a169eb334a398abdf2c0659006d4a7cefef27a7e	SHA256	CryptoWall/H1N1 Loader Document
6e5afb86904adb80ed96d5582304483a13c72208ccfbee67303cceb8d6da1cf5	SHA256	CryptoWall/H1N1 Loader Document
1824e68470e75996a2b3d6f5978541d82019b4b4e8de3274a893af9c107369d1	SHA256	CryptoWall/H1N1 Loader Document
beb396e8694369d6e81a9f83dfaa7ff323a03937f20620d2901b77ceba87af3e	SHA256	CryptoWall/H1N1 Loader Document
90719326061afef4751138778c76804d7d15f893317ea36ce6d9eb9df90919d2	SHA256	CryptoWall/H1N1 Loader Document
cce9ea89d0957457beaa71415337b54d4e07aa0a17acac07fcb778363db963a9	SHA256	CryptoWall/H1N1 Loader Document
3167d7613c7b6942fab73e35f7c05a278a4488687fa4aaaa825b2aaad8ee2d4e	SHA256	CryptoWall/H1N1 Loader Document
482a83f9066b95f567c1e0caf95ae034160723f0db15c358ba0aebcbee5b386f	SHA256	CryptoWall/H1N1 Loader Document

6ba845b1e3433c380b03d71c70af9d8e24fb4bf0b0997df3c543e022071634ce	SHA256	CryptoWall/H1N1 Loader Document
408a53621f34427388c71c7343544e9794a0c1d85fcada4c3cbf2fbd39801ec7	SHA256	Dridex 222 Document
2db470dd06252bf860e78096ed255b317ae7f7b8074a93d81ff518f293ea9fde	SHA256	Dridex 222 Document
0259e653a9c17b04bad98e0e8cb4835f418f1256a7603807ba09a3b97a583d70	SHA256	Dridex 222 Document
9540f1f53a0b515e25e5907b43890aef4f3b6964662461c2951b85d91d407fc9	SHA256	Dridex 222 Document
a5d38e043acbad58247b641429fc7764a2ce6d9b0d7953b6d458946f76050e6c	SHA256	Dridex 222 Document
629736be158503075b66ac368ea040258a584a6163fd0138392630f1259a966	SHA256	Dridex 222 Document
6a33288612dd7f74d0ae1704219864506553 82915d4371321d4d4d4a6507fcf5	SHA256	Dridex 222 Document
e234a209004b76c2374057929eff1605efc32cbddbf5a1b6faff1fc2893fe8af	SHA256	AU Ursnif Document
10372e472b35b03a8d32372c0d07d271c085 47f57adb405d21bdaf30a4af8d87	SHA256	AU Ursnif Document
33449ed6e99286f1b8c6d9ed0480ca8893d70 10f6e1997180b3f28c74bb3b7e2	SHA256	AU Ursnif Document
f115df5fa948e0228f208855b860911864c0b2 6b7601010c9ec23cf32e9c7f31	SHA256	AU Ursnif Document
c0407c207b17179241ddd1ac38cd57de3e2b b4bd1c1e6e093af9ffcd87f28fab	SHA256	AU Ursnif Document
72fb0752bbe4024b05baa71b8d26b9529b39 531f4e4f88eef9049604462d6b7a	SHA256	AU Ursnif Document
65d9979b11885e44567799f69258492f6e699 22c66858e03b03a21790d031cee	SHA256	AU Ursnif Document
7bb439a5221f667fd30b6fca2ed9ba48ac986a 1998d4d8fe167b0c08e9e59c35	SHA256	AU Ursnif Document

proofpoint

9a292db2300c48234ee8e1ac7530349a9870 9a73aeea743f83d5099b355335af	SHA256	AU Ursnif Document
62060f13d9fdeb2f1cde97a9147aa563b9e87 899d9158757389af66a65206859	SHA256	AU Ursnif Document
c1e07f81e5fb7fac5c03594aed528b6f3adbc0 bb028d5f1b341b3eb51b653afe	SHA256	AU Ursnif Document
37169162b12198e88066880d0de061f6071bf f793d637776cbeb308f38dd86b1	SHA256	AU Ursnif Document
e9ec5b3483d6592da5b7657baae3240dc67e 7519bb5210e8cf6e8ae2cdb63f69	SHA256	AU Ursnif Document
9617039aae8471d927726cadb1d15d21e219 d7eb9d1d5ed5b582cfd94d3f4966	SHA256	AU Ursnif Document
2752dc5294d39f7f0e89f7128cf5c1d05cde96f 2f55bb19ad13263a10a5bd290	SHA256	Nymaim Document
4d0c14edfa616c0a5618b312f5ca90b3a2918 8288f35c5d8c1c2ae37ef11371f	SHA256	Nymaim Document
4e97e6fc3cd28237c2a108a0a76fa03a4c5aaf abaa71f6c39c5abcdb390fd204	SHA256	Nymaim Document
6e3dfd88c29db4928d8776477536970428d9 0aa574e5f481115d1d47a0d8f650	SHA256	Nymaim Document
7fade2990becf491aad48812f465363c7a9d4e e9995e008bed2fad31735c632f	SHA256	Nymaim Document
80525692d12c1c25a92cccd75d3325ba039b b7f45babc0cf5db932449c7774bb	SHA256	Nymaim Document
b211d879a44a5eb0452b8785bbcbd929b1a4 a74641d4c020c1c954cd379bd31a	SHA256	Nymaim Document
a1770a7671679f13601e75a7cb841fea90c7a dd78436a0bea875ce50b92afc33	SHA256	Fileless Ursnif Document
340f82a198aa510159989058f3f62861de741 35666c50060491144b7b3ec5a6f	SHA256	Fileless Ursnif Document
f204c10af7cdcc0b57e77b2e521b4b0ac0466 7ccffce478cb4c3b8b8f18e32a2	SHA256	Fileless Ursnif Document

proofpoint

0661c68e6c247cd6f638dbcac7914c826a5fe ee1013e456af2f1f6fd642f4147	SHA256	Fileless Ursnif Document
a8663becc17e34f85d828f53029ab110f92f63 5c3dfd94132e5ac87e2f0cdfc3	SHA256	Fileless Ursnif Document
30cd5d32bc3c046cfc584cb8521f5589c4d86a 4241d1a9ae6c8e9172aa58ac73	SHA256	Fileless Ursnif Document
83e305724e9cd020b8f80535c5dd897b2057c ee7d2bb48461614a37941e78e3a	SHA256	Fileless Ursnif Document
f45bf212c43d1d30cc00f64b3dcae5c35d4a85 cacd9350646f7918a30af1b709	SHA256	Fileless Ursnif Document
1e746ba37c56f7f2422e6e01aa6fde6f019214 a1e12475fe54ee5c2cf1b9f083	SHA256	Fileless Ursnif Document
7e22ea4e06b8fd6698d224ce04b3ef5f00838 543cb96fb234e4a8c84bb5fa7b3	SHA256	Fileless Ursnif Document
815bd46e66f1d330ed49c6f4a4e570da2ec89 bcd665cedf025028a94d7b0cc1e	SHA256	Fileless Ursnif Document
910c697647b3c9179427184630c125634532 467cd24f0f40699962d7d0a7e31a	SHA256	Fileless Ursnif Document
74ec24b5d08266d86c59718a4a476cfa5d220 b7b3c8cc594d4b9efc03e8bee0d	SHA256	Fileless Ursnif Document
90a7951683a5a77a21d4a544b76e2e6ee04e 357d2f5bfcff01cd6924906adf77	SHA256	Fileless Ursnif Document
2c21dafcb4f50cae47d0d4314810226cba3ee 4e61811f5c778353c8eac9ba7dc	SHA256	Fileless Ursnif Document
247511ab6d7d3820b9d345bb899a7827ce62 c9dd27c538c75a73f5beba6c6018	SHA256	Fileless Ursnif Document
708374a4dfaaa8e44ee217ca5946511cacec5 5da5eabb0feb1df321753258782	SHA256	Fileless Ursnif Document
136379754edd05c20d5162aed7e10774a956 57f69d4f9a5de17a8059c9018aa6	SHA256	Fileless Ursnif Document
5d215ef3affe320efe4f5034513697675de40b a8878ca82e80b07ad1b8d61ed8	SHA256	Fileless Ursnif Document

hxxp://vascoboiblog[.]space/update/KB25421[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://officewithout[.]space/KB998394[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://updatesarecoming1000[.]space/usa/kb37892[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://kotoberlin[.]com/wp-includes/office[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://batiatus[.]net/wp-includes/office[.]php	URL	CryptoWall/H1N1 Loader
hxxp://mastfm102[.]com//wordpress/wp-includes/asalam[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://audio-hacks[.]com/wp-includes/salam[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://laasciidle[.]com/wp-includes/office[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://mariannmahoney[.]com/wp-includes//office[.]exe	URL	CryptoWall/H1N1 Loader
hxxp://phdfashion[.]com/wp-includes//calc[.]exe	URL	CryptoWall/TinyLoader
hxxp://divasasbysa[.]com/wp-includes//kb[.]exe	URL	CryptoWall/TinyLoader
hxxp://pretenlignesansenquetedecredit[.]com/wp-includes/kis[.]exe	URL	SmokeLoader/TVSpy
hxxp://galaxysportsonline[.]com/system/logs/office[.]exe	URL	TinyLoader
hxxp://31[.]192[.]105[.]24/1[.]exe	URL	TVSpy
hxxp://cuentosparahacertefeliz[.]com/wp-includes/notepad[.]exe	URL	Dridex 222
hxxp://forexonlinebusiness[.]info/wp-includes/kbe[.]exe	URL	Dridex 222

hxxp://usatraveldeals[.]net/wordpress/wp-includes/load4[.]php?prot=secrete	URL	Dridex 222
hxxp://pdfviewapp[.]com/?filename=CHEXXiNC%20Payment%20Advise_ID00589884[.]pdf	URL	Dridex 222
hxxp://pdfviewapp[.]com/?filename=CHEXXiNC%20Payment%20Advise_ID00589884[.]scr	URL	Dridex 222
hxxp://www[.]kiryanaking[.]com/system/logs/putty[.]exe	URL	AU Ursnif
hxxp://gitafashion[.]com/image/flags/putty[.]exe	URL	AU Ursnif
hxxp://ug-stroy[.]com/image/flags/tg[.]exe	URL	AU Ursnif
hxxp://satellite-rent[.]com/image/data/logo[.]exe	URL	AU Ursnif
hxxp://spartanleather[.]com[.]au/image/flags/rsa[.]exe	URL	AU Ursnif
hxxp://brightapparel3[.]com/image/data/msoffice[.]exe	URL	AU Ursnif
hxxp://dsmartbuy[.]com/image/data/office[.]exe	URL	AU Ursnif
hxxp://abettermindset[.]com/images/office[.]exe	URL	AU Ursnif
hxxp://antalyanalburiye[.]com/image/payment/client[.]exe	URL	AU Ursnif
hxxp://galleryamjadi[.]ir/image/flags/he[.]exe	URL	Nymaim
hxxp://krovlya-nova[.]com/image/flags/bf[.]exe	URL	Nymaim
hxxp://stickerplug[.]com/image/flags/config[.]exe	URL	Nymaim
hxxp://raximpex[.]com/image/data/office[.]exe	URL	Nymaim

hxxp://naipeclandestino[.]com[.]br/image/data/office[.]exe	URL	Nymaim
hxxp://tribudellusato[.]altervista[.]org/image/templates/office[.]exe	URL	Nymaim
hxxp://sociallyvital[.]com/images/office[.]exe	URL	Nymaim
hxxps://github[.]com/consfw/msfw/raw/master/README	URL	Fileless Ursnif
hxxps://github[.]com/consfw/msfw/raw/master/TODO	URL	Fileless Ursnif
hxxps://supratimewest[.]com/README	URL	Fileless Ursnif
hxxps://supratimewest[.]com/TODO	URL	Fileless Ursnif
hxxps://github[.]com/minifl147/flue/raw/master/memo	URL	Fileless Ursnif
hxxps://github[.]com/minifl147/flue/raw/master/adv	URL	Fileless Ursnif
hxxps://github[.]com/flowsdem/found/raw/master/rost	URL	Fileless Ursnif
hxxps://github[.]com/flowsdem/found/raw/master/virst	URL	Fileless Ursnif
hxxp://www[.]starwoodhotels[.]pw/install/Instrdrive	URL	Fileless Ursnif
hxxp://www[.]starwoodhotels[.]pw/install/Workflow2	URL	Fileless Ursnif
hxxp://rabbitons[.]pw/cache	URL	Fileless Ursnif
hxxp://rabbitons[.]pw/css	URL	Fileless Ursnif
hxxp://supratimewest[.]biz/img/green	URL	Fileless Ursnif
hxxp://supratimewest[.]biz/img/captcha	URL	Fileless Ursnif
20338201ea3cbb697dd74ac709cf2574e5feedbe6306592706aa8c276c8bf40c	SHA256	CryptoWall hash
7CC33C1C5B760A6525C414796F37175BC887DCD99318CAA8A622855A598B13AE	SHA256	CryptoWall hash

96358524e91b428980e2c041b7da7c40caee4cc4ba2089c23353e25c3ffde3f8	SHA256	CryptoWall hash
A0EF6BD2842658695BE4F1F84F0C62D010A8AA406E3A31E9DE5EF8662A058D80	SHA256	H1N1 Loader hash
B1ACB11DBEDD96763EE00DD15CE057E3259E1520294401410D8C42CFA768A50A	SHA256	NeutrinoBot hash
BCDB7ED813D0D33B786AE1A4DFA09A2CB3A0B61CE1BB8DB01DBDF7D64EC4B4A0	SHA256	Pony hash
21B96966DB9395C123C4620FD90C142F6080DBA038BD65F6A418293BA3104816	SHA256	TinyLoader hash
FAFE60C1A92EA059E89FED7AF763468698BAE2B1E127291F8A66AF20EC2CAEF6	SHA256	TinyLoader hash
affa76507118deef34d20a9dde224fbce7bdcf5633e7ff529e5b291cfc2bce8c	SHA256	SmokeLoader hash
e70e34fb85894d27e0711f56e1d57b9d126c4bb22a62454cc38f39fc3cd2c37d	SHA256	TVSpy hash
92BB0544F1AD7661BF2A77F5305EC439B10FB005CCA3545FAEC2B8DE5887110E	SHA256	Dridex 222 hash
55F53DD1351BFA6CE3D0AA83D8F32C473A933CF3EC27E92A71A406AFDB636891	SHA256	Dridex 222 hash
2cba464f6454b598809063e58beed60d7a322f87720567997dda5f685ec5936a	SHA256	AU Ursnif hash
2f2f6de08d9fed80a1bcdee7cdf3b82aa002deeeb340b041d70767df7b448fa2	SHA256	AU Ursnif hash
22085dc5212df9f732881f18d4bf757abf6073524f23f60b39f8653150f7e19d	SHA256	AU Ursnif hash
cf3dff8bcd402f8c6f38239a9b800d76df2bfa57411a9a4768135ce11876e56a	SHA256	AU Ursnif hash
aa76d3af03b44639148d190785eab9720471ffc28c71468182b786ed0b0eb	SHA256	AU Ursnif hash
A51BE357ABB2BB1CDF977EBE05BEEB85943FAEFDA16855F0345EDFEE915C0CDB	SHA256	Nymaim hash

72D246767B58ED8FFD39D6CEA8B44E48AF578CC0DD725BDEDF83163EEF28A31F	SHA256	Nymaim hash
ED7A5B229299FBD58DC3F0E9A7096177E0268B125F70048D9A970266E531DC01	SHA256	Nymaim hash
A3326D8C59CEAAAE4798303B0653716794300ABC8202EAC3784D432CA3D74A5B	SHA256	Nymaim hash
AC73097A37BF4EFFD54FF65CAEC9FE6A46BE9DB18D1D1602CCD26D6B9944A048	SHA256	Nymaim hash
8928cfbc77cd2987c7ed66c507b6cbcd2b3e727be384f96fbdc0b98452308d39	SHA256	Nymaim hash
5A499D04E5298BE9F1C2F8164D2432BC301471E48D4DE1BFF348F68993805A60	SHA256	Nymaim hash
d6b818c6ed3fd3be9f113d19cde7e43a2d4d46c2377ee91236986342ec00a828	SHA256	Fileless Ursnif hash
db13dd332ad7c2be03e3be2c4f3eeece29682f6c7a717c820b4d8a858e030f82	SHA256	Fileless Ursnif hash
hxxp://acie[.]edu[.]np/DFQvsZ[.]php	URL	CryptoWall c2
hxxp://acmm[.]org[.]au/idjFbx[.]php	URL	CryptoWall c2
hxxp://ahtubafishing[.]com/CXjq48[.]php	URL	CryptoWall c2
hxxp://all-4-music[.]nl/yBDEMc[.]php	URL	CryptoWall c2
hxxp://allescorts4u[.]com/dfgOwA[.]php	URL	CryptoWall c2
hxxp://anilyildirim[.]net/zn9mur[.]php	URL	CryptoWall c2
hxxp://apartment[.]od[.]ua/I35pl6[.]php	URL	CryptoWall c2
hxxp://apexminerals[.]com[.]au/k8HqvL[.]php	URL	CryptoWall c2
hxxp://apptitudes[.]fr/eC2F1f[.]php	URL	CryptoWall c2
hxxp://arcticbear[.]net/MRGKAC[.]php	URL	CryptoWall c2
hxxp://ariixhouse[.]nl/iMVfC4[.]php	URL	CryptoWall c2
hxxp://artistblip[.]com/QJ9HzW[.]php	URL	CryptoWall c2
hxxp://asiamaster[.]kz/vUn1wz[.]php	URL	CryptoWall c2

hxxp://ask-us-anything[.]tk/PsdO76[.]php	URL	CryptoWall c2
hxxp://aspectdesigns[.]com[.]au/0rTVlG[.]php	URL	CryptoWall c2
hxxp://australianmotorinns[.]com/9ctKlH[.]php	URL	CryptoWall c2
hxxp://avazuinc[.]com/D04m5N[.]php	URL	CryptoWall c2
hxxp://balustradydrewniane[.]pl/Fcb7VZ[.]php	URL	CryptoWall c2
hxxp://behejbrno[.]com/MixtUZ[.]php	URL	CryptoWall c2
hxxp://bem-bakery[.]com/HPINRS[.]php	URL	CryptoWall c2
hxxp://budni[.]info/zYNKoq[.]php	URL	CryptoWall c2
hxxp://bulksmsdealer[.]com/vR3BEX[.]php	URL	CryptoWall c2
hxxp://calsalumni[.]iastate[.]edu[.]staging[.]sites[.]flyinghippo[.]com/ScXajM[.]php	URL	CryptoWall c2
hxxp://campaignforyoungamerica[.]org/LT3YRB[.]php	URL	CryptoWall c2
hxxp://centralescorts4u[.]com/XqVFBm[.]php	URL	CryptoWall c2
hxxp://conseils-finance[.]com/kJsnUb[.]php	URL	CryptoWall c2
hxxp://daddysground[.]cz/zTVoGb[.]php	URL	CryptoWall c2
hxxp://dentiste-paris-20[.]fr/IhfweE[.]php	URL	CryptoWall c2
hxxp://dermalightcr[.]com/tHja9Z[.]php	URL	CryptoWall c2
hxxp://dineroexperto[.]pe/zOesbw[.]php	URL	CryptoWall c2
hxxp://dining-bar[.]com/BQ_Ln4[.]php	URL	CryptoWall c2
hxxp://directoryassistanceamerica[.]com/XeBUDN[.]php	URL	CryptoWall c2
hxxp://dolphinworld[.]org/MaB54K[.]php	URL	CryptoWall c2
hxxp://dorisbociort[.]ro/6sZTLc[.]php	URL	CryptoWall c2
hxxp://dunwoodypress[.]com/DJHMXS[.]php	URL	CryptoWall c2
hxxp://e-minunat[.]ro/ZeNpML[.]php	URL	CryptoWall c2
hxxp://ecocity[.]kz/7_9SR6[.]php	URL	CryptoWall c2

hxxp://ecoinfo[.]kz/LUoMqa[.]php	URL	CryptoWall c2
hxxp://edlenimaging[.]com/be5AmR[.]php	URL	CryptoWall c2
hxxp://emotionwerbung[.]de/389Tak[.]php	URL	CryptoWall c2
hxxp://empiredigitalmarketing[.]com/09LihY[.]php	URL	CryptoWall c2
hxxp://en[.]theolympiaschools[.]edu[.]vn/FCfXeB[.]php	URL	CryptoWall c2
hxxp://europartners[.]it/Dd6VPR[.]php	URL	CryptoWall c2
hxxp://event-travel[.]co[.]uk/3K6Psd[.]php	URL	CryptoWall c2
hxxp://fiyaskobirlik[.]com/UxAK5e[.]php	URL	CryptoWall c2
hxxp://funzone-veza[.]sk/Owm50c[.]php	URL	CryptoWall c2
hxxp://ggvidrosautomotivos[.]com[.]br/KMYz1s[.]php	URL	CryptoWall c2
hxxp://giaohang[.]org/lCs_PE[.]php	URL	CryptoWall c2
hxxp://giosposa[.]com/Zoe2aN[.]php	URL	CryptoWall c2
hxxp://golcukrehberi[.]com/6JQEva[.]php	URL	CryptoWall c2
hxxp://goldenangels[.]com[.]tr/l4Fw8D[.]php	URL	CryptoWall c2
hxxp://grafitti-photo[.]com/IGHOYq[.]php	URL	CryptoWall c2
hxxp://granrio[.]com[.]br/4A0Hw5[.]php	URL	CryptoWall c2
hxxp://hand-made[.]by/rQWftY[.]php	URL	CryptoWall c2
hxxp://hatha[.]it/6tnLEG[.]php	URL	CryptoWall c2
hxxp://highclassescorts4u[.]com/Snuxg7[.]php	URL	CryptoWall c2
hxxp://ifawindow[.]co[.]uk/0w5MVI[.]php	URL	CryptoWall c2
hxxp://igotocd[.]com/rklVaO[.]php	URL	CryptoWall c2
hxxp://ihadthat[.]com/1NEnbi[.]php	URL	CryptoWall c2
hxxp://indonesiandomains[.]com/e9vsxj[.]php	URL	CryptoWall c2

hxxp://inicc[.]yucatan[.]gob[.]mx/UIagAy[.]php	URL	CryptoWall c2
hxxp://international[.]woptimo[.]com/YglxHK[.]php	URL	CryptoWall c2
hxxp://itt-pushkino[.]org/D2BE6m[.]php	URL	CryptoWall c2
hxxp://itvsoft[.]asia/rRwKxj[.]php	URL	CryptoWall c2
hxxp://jadwalpialadunia[.]in/rG4Rdi[.]php	URL	CryptoWall c2
hxxp://jameswbos[.]com/v10aAJ[.]php	URL	CryptoWall c2
hxxp://jjcampbell[.]com/1wK5Iy[.]php	URL	CryptoWall c2
hxxp://jlprotect[.]ca/_poxuV[.]php	URL	CryptoWall c2
hxxp://jogos[.]testeqi[.]com[.]br/4t1E7X[.]php	URL	CryptoWall c2
hxxp://kadr37[.]pl/fFe_xr[.]php	URL	CryptoWall c2
hxxp://kskillsmobility[.]eu/ludO0_[.]php	URL	CryptoWall c2
hxxp://larosa[.]com[.]au/8beYcC[.]php	URL	CryptoWall c2
hxxp://lazycranch[.]us/PtAg1I[.]php	URL	CryptoWall c2
hxxp://liberal[.]com[.]mx/0My2EZ[.]php	URL	CryptoWall c2
hxxp://london-escorts-agency[.]org[.]uk/fdnmyD[.]php	URL	CryptoWall c2
hxxp://loved[.]kz/yMZFGp[.]php	URL	CryptoWall c2
hxxp://lptech[.]sk/g3lfoj[.]php	URL	CryptoWall c2
hxxp://macphoto[.]nl/7NBUqj[.]php	URL	CryptoWall c2
hxxp://mangohills[.]net/RxIoCE[.]php	URL	CryptoWall c2
hxxp://mastertrade[.]tk/12fDze[.]php	URL	CryptoWall c2
hxxp://maxicarga[.]co/L8HU29[.]php	URL	CryptoWall c2
hxxp://mehmetekinci[.]biz/Hg3V8b[.]php	URL	CryptoWall c2
hxxp://monicasalvador[.]com[.]ar/btWiaQ[.]php	URL	CryptoWall c2
hxxp://morainecare[.]com/eQRvWp[.]php	URL	CryptoWall c2

hxxp://muel[.]altervista[.]org/z1ho2W[.]php	URL	CryptoWall c2
hxxp://myteaminspired[.]com/mzTOIv[.]php	URL	CryptoWall c2
hxxp://neoad[.]de/NXy1mb[.]php	URL	CryptoWall c2
hxxp://noahwilbanks[.]com/PtXsO_[.]php	URL	CryptoWall c2
hxxp://ofertarelampago[.]com[.]br/4jiPBG[.]php	URL	CryptoWall c2
hxxp://otkritka[.]com[.]ua/MVc9hg[.]php	URL	CryptoWall c2
hxxp://otkritka[.]com[.]ua/tjhW2B[.]php	URL	CryptoWall c2
hxxp://pc[.]all-to-all[.]com/Ryfq7Y[.]php	URL	CryptoWall c2
hxxp://premierdisneyvilla[.]com/QXeHOy[.]php	URL	CryptoWall c2
hxxp://quadparticle[.]com/fZ1Y8M[.]php	URL	CryptoWall c2
hxxp://raincchina[.]com/NSrcQE[.]php	URL	CryptoWall c2
hxxp://ronikagp[.]ir/U_ABoi[.]php	URL	CryptoWall c2
hxxp://silstop[.]pl/Si0cCJ[.]php	URL	CryptoWall c2
hxxp://sohbetodalari[.]net/GnOLXh[.]php	URL	CryptoWall c2
hxxp://sowellness[.]be/fYvA5U[.]php	URL	CryptoWall c2
hxxp://sowellness[.]be/isB2Ac[.]php	URL	CryptoWall c2
hxxp://stevesyachtrepair[.]com/S8bJFl[.]php	URL	CryptoWall c2
hxxp://t-firma-en[.]itech-websolutions[.]com/U2Ac7i[.]php	URL	CryptoWall c2
hxxp://taftee[.]in/JnGQ1s[.]php	URL	CryptoWall c2
hxxp://tbraille[.]com[.]br/XAT7zH[.]php	URL	CryptoWall c2
hxxp://telecom-sa[.]com/azRXqt[.]php	URL	CryptoWall c2
hxxp://thebeautythesis[.]com/UaEigq[.]php	URL	CryptoWall c2
hxxp://thebesttshirtsonline[.]com/CF9iM8[.]php	URL	CryptoWall c2

hxxp://timeaddedon[.]com/CBRrYv[.]php	URL	CryptoWall c2
hxxp://tugay[.]com[.]tr/prkdzF[.]php	URL	CryptoWall c2
hxxp://turbosol[.]asia/l7xydO[.]php	URL	CryptoWall c2
hxxp://uzmankirala[.]com/KhVRbv[.]php	URL	CryptoWall c2
hxxp://vancouverdispensarycoalition[.]ca/euqUb5[.]php	URL	CryptoWall c2
hxxp://verybigloan[.]com/1vR9hu[.]php	URL	CryptoWall c2
hxxp://villisplace[.]info/fJQ_3v[.]php	URL	CryptoWall c2
hxxp://vinastudio[.]at/8TkXUJ[.]php	URL	CryptoWall c2
hxxp://vladoveverka[.]sk/6RGZgC[.]php	URL	CryptoWall c2
hxxp://wallpapersau[.]net/igrHKY[.]php	URL	CryptoWall c2
hxxp://winika[.]com[.]br/SGJ_Fr[.]php	URL	CryptoWall c2
hxxp://yardstickglobal[.]in/Y37Jux[.]php	URL	CryptoWall c2
hxxp://zhahan[.]kz/TSOXQL[.]php	URL	CryptoWall c2
hxxp://zolty[.]eu/bnFKET[.]php	URL	CryptoWall c2
hxxp://zuiyougou[.]com/Pfy2Qs[.]php	URL	CryptoWall c2
179[.]43[.]160[.]47:20010	IP	TinyLoader c2
50[.]7[.]124[.]170	IP	TinyLoader c2
hxxp://www[.]vascoboiblog[.]club/0x00/gate[.]php	URL	H1N1 c2
hxxp://5[.]45[.]179[.]179/ajax[.]php	URL	NeutrinoBot c2
hxxp://5[.]45[.]179[.]179/p/ajax[.]php	URL	Pony c2
hxxp://wearesorryfortheinconvenience[.]com	URL	Smoke Loader c2
hxxp://31[.]192[.]105[.]24/mtv/gate[.]php	URL	TV Spy c2
128[.]199[.]186[.]92:643	IP	Dridex 222 Loader c2

180[.]235[.]132[.]105:8843	IP	Dridex 222 Loader c2
5[.]56[.]61[.]62:666	IP	Dridex 222 Loader c2
37[.]34[.]52[.]185:444	IP	Dridex 222 Worker node
89[.]46[.]196[.]61:443	IP	Dridex 222 Worker node
212[.]183[.]20[.]78:444	IP	Dridex 222 Worker node
41[.]79[.]173[.]47:443	IP	Dridex 222 Worker node
95[.]170[.]95[.]81:5445	IP	Dridex 222 Injects c2
146[.]0[.]40[.]33:8843	IP	Dridex 222 Injects c2
151[.]248[.]121[.]167:1743	IP	Dridex 222 Injects c2
95[.]213[.]192[.]83	IP	AU Ursnif c2
93[.]170[.]141[.]22	IP	AU Ursnif c2
notallowallownothingaal[.]me	domain	AU Ursnif DGA domain
agentclientmediap[.]me	domain	AU Ursnif DGA domain
notallowallownothingaal[.]me	domain	AU Ursnif DGA domain
aljsccliclientheaseenot[.]me	domain	AU Ursnif DGA domain
mediapartnerssays[.]me	domain	AU Ursnif DGA domain
seeuserjdisallowclient[.]me	domain	AU Ursnif DGA domain

sofficeraclientagent[.]me	domain	AU Ursnif DGA domain
jscsasaysallowalsaswal[.]me	domain	AU Ursnif DGA domain
jscdisallowsaauser[.]me	domain	AU Ursnif DGA domain
jherecliallowalclient[.]me	domain	AU Ursnif DGA domain
agentofficer[.]me	domain	AU Ursnif DGA domain
aljsccliclientheaseenot[.]me	domain	AU Ursnif DGA domain
mediapartnerssays[.]me	domain	AU Ursnif DGA domain
seeuserjdisallowclient[.]me	domain	AU Ursnif DGA domain
sofficeraclientagent[.]me	domain	AU Ursnif DGA domain
jscsasaysallowalsaswal[.]me	domain	AU Ursnif DGA domain
au-tda[.]com	domain	AU Ursnif injects c2
au-tdc[.]com	domain	AU Ursnif injects c2
http://apngwen[.]com/yvovgw65u/index[.]php	URL	Nymaim c2
http://apngwen[.]com/rqgbfhq/index[.]php	URL	Nymaim c2
http://apngwen[.]com/xk0ktpadlj/index[.]php	URL	Nymaim c2
http://uvflerpoqgj[.]com/mwk2ntlx/index[.]php	URL	Nymaim c2
http://ykyru[.]com/eipqcxxb/index[.]php	URL	Nymaim c2
http://ykyru[.]com/oslhhtx/index[.]php	URL	Nymaim c2
http://mbcqjsuqsd[.]com/fa7vi1df/index[.]php	URL	Nymaim c2

31[.]184[.]234[.]21	IP	Nymaim Ursnif injects c2
162[.]244[.]32[.]157:8458	IP	Nymaim Ursnif VNC
oklinjgreirestacks[.]biz	domain	Fileless Ursnif c2
brookmensoklinherz[.]org	domain	Fileless Ursnif c2
mletterinklandoix[.]net	domain	Fileless Ursnif c2