Windows Platform

SHA-256

06f6ca3feaabfe07aa370d502bc00782df88fa0584c870fc31e642808f0f3924 - Trojan.Win64.DLOADR.AUSURC
0cc36dd25e099cc6f1798dabe1d6a3e2d8c3883aa0e0d7296e94d035cdb74f3c - Trojan.Win64.DLOADR.AUSURC
119c0a8258cc1ff958e6ec9ec8eae9d8e73a50833e01aa6565395464b8e33f7a - Trojan.Win64.DLOADR.AUSURC
1d8cef17a8588c216a9e69f3b4acd55dad1b9c69b25b344452ade112eaa96cb5 - Trojan.Win64.DLOADR.AUSURC
29969986180a89ab00f6578ffe0748749d4fbd767ee0d09f516458bf47380514 - Trojan.Win32.PLUGX.ENM
2c403e390f59b2c2bfafde476dc18000b0ad1bbc8ac9ee0670662c48ba5b748f - Trojan.Win32.PLUGX.ENM
2ecb9e6f123aef47a0650fbd76da8d57408bc43413959750f46b47645e58f88e - Trojan.Win32.PLUGX.ENM
3210460b6afa2b0219895685d12de570a711cce64d1fc2f9fec3dac2918543a7 - Trojan.Win32.PLUGX.ENM
354fed4072f0c12b9a7e40f48feb32c043481d0a87fbff599ce36fd2e323d379 - Trojan.Win32.DLOADR.TIOIBEPQ
369e74a8e1f686896f82d92ee2467ca6736bc44b06faab9db9ea6473aef4c397 - Trojan.Win32.DLOADR.TIOIBEPQ
3c873ed23fe64445168382cd59a3a9eef08b3be19a660999afc474b890e57959 - Trojan.Win32.DLOADR.TIOIBEPQ
3d57b604db0023cc57de8f224ad5b211a0a5250de68671fc61c55e1b354ceb38 - Trojan.Win32.DLOADR.TIOIBEPQ
401d0b1f1a94df6a70818ef2bad80d139bb258c0e7746612066599aa43456dad - PUA.Win64.FlashServ.AA.component
44f80cb1d774bbdee01281f621b8f42d2facee8db1678828db9e9b3a00fa2a63 - PUA.Win64.FlashServ.AA.component
4d591853294dcc8afc8c646fffddc8b0efaeb44f120145011b83a6c63463e18d - PUA.Win64.FlashServ.AA.component
50f4c8cf2b50fb75e7fc32860207e7d13e88a813bf7c96ed12a6953bd5fe71f5 - PUA.Win64.FlashServ.AA.component
5ead238621bef7cc4c4f58ac5eb614dd16acbcfd30c75169ff5f16d7905243a5 - Trojan.Win32.COBALT.BF

618e38e0e5ccdefbd4bc4987f60c40f1c2f733c2441ed2026d1530910d7196bd - Backdoor.Win32.ZEGOST.AYHHM
68feab7ef7a2bd4754620b3a5a511988d18384bbd42d100e528cc5b876a1d771 - Backdoor.Win32.ZEGOST.AYHHM
6aa3fa0fc477966c81ff15725ae3f8d687f847256ab20833802e983a510d5ff9 - Backdoor.MSIL.QUASAR.X
6ab71022f268885c67e7251e52fab62c163820c67988cf579e76a383a0f6f8dd - Backdoor.Win32.ZEGOST.AYHHM
6b8ae6f01ab31243a5176c9fd14c156e9d5c139d170115acb87e1bc65400d54f - Backdoor.Win32.ZEGOST.AYHHM
74d93253090f999977fa8e32b03b94bb8d35f59a8390545fd10da0f7fb1fcd13 - Backdoor.Win32.ZEGOST.AYHHM
76d008d9955509d3db6e190acfa58fdf12fc64253884ac6981187a3e5ffdeb20 - Trojan.Win32.DROPPER.TIOIBEPN
784ceff596d94ef365ae261ae43a83c43d52e04dc46b09a8fb5960772bca4a00 - Trojan.Win64.DROPPER.AUSURB
794991233088eb8c9ecc2d63df97041f5dc63f8169e2da8a42f07366c6fb215f - Backdoor.MSIL.ASYNCRAT.BD
7afd418750824969fd6d0c6db949456998f792c97d6a69669051e1c90a458a5b - Trojan.Win64.ORAT.AS
7d0ff5125ace6fc49103c71fdab7f430c20741ce36b54e0379c71a6841962e0f - Trojan.Win32.HELLOBOT.AA
7de8be300fc35f81a316a61d07840c9963b5590b16296fde54c70ac88de6e837 - Trojan.Win32.DROPPER.ERA
81d2be1565c05f77e829e1296d17d9456ae672459e4283315cdd0dfae01626a9 - Backdoor.Win32.TROCHIL.B
825b2e89cec971074819bafde889208dea729997d8b71599017e3277d5f32523 - PUA.Win32.Mimi.B
844a3992b2a4f0b81f813175650135b2571825fc0dbfac7e3ebea8370be74748 - Trojan.Win64.PLUGX.AC
86fb171f52fef167ba8dd202c6b6530d3fe3def1158a4d3385bef3258650724d - Trojan.Win32.PLUGX.ENM
89fb709ed5ac5cc3342b9894af039dcbb1988848c87063ba15b4ab69399ae77d - Trojan.Win64.PLUGX.AC
8e101eb365d5f7a2f66f253a7ca7736f1a7ae9e71567da3436615be105f0844e - Trojan.Win64.PLUGX.AC
9217518710b77766d9dc3397c3ce9bd88734c71c8b80a2dd1e9ed1312efacd9c - Trojan.Win32.PLUGX.ENM
9bf4ab66bc119ccbf13ac3b0374c39de4c27e0f2aae4fc4383fe7ec0c7246ec5 - Trojan.Win64.PLUGX.AC
9d72cb7c95bcec88f7bf4bfffdb2b0ebe5902f3da943d03794e8a6f586f0c1a3 - Trojan.Win32.PLUGX.ENM

a3d3a7aac4b42cd7a295a44d23ef457fb4dc74113912f3d3270649c10bedd0b4 - Trojan.Win64.PLUGX.AC
aefaaa2c69a2f275d05c2d319877f321c617b337e3c67e3e9acfbaeffdd1c3eb - Trojan.Win32.PLUGX.ENM
b0d62e927975627c720fcf734ea7bb49ebe0790defa6d1085ff93e4b39c74f57 - Trojan.Win64.PLUGX.AC
b7d91f0e15cf0258fc857699171b6627337d511ecca9ab22adf668e0918eec50 - Trojan.Win32.PLUGX.ENM
b85955932ef6c04f92cdddf9c2f9d6f4693b2a35f6fa2be252fef93cb44c73c0 - Trojan.Win64.PLUGX.AC
be213cfb0795e8a645d50eec7e55520e952279963dcef4e11b49c022ec283129 - Trojan.Win32.PLUGX.ENM
c664a816771b8d058796bdddbc0554510c430cc7fc98bae5153a21b1797bf39c - Trojan.Win32.PLUGX.ENM
d4140f016eba287d34182ae4ff29f52349d8c0b151eb2d253e5838ca6f662053 - Backdoor.Win32.PLUGX.EYSGVP
d6a97f90030a981a1495196f2fdf99f70d333abe165eecafc5b08302f70a6ea3 - Backdoor.Win32.PLUGX.EYSGVP
ddd19d60f37f04e33fb74f6ef2e45f24be1bab8423aba608987804eed9316567 - Backdoor.Win32.PLUGX.EYSGVP
e0395231a9c1fdb9299ab3803a50405e095f25671b5435712562cd5619f6fc1d - Backdoor.Win32.PLUGX.EYSGVP
e2451144e007e588ac81cbf76573a1ab5279b1f8ddc9d2ea6066c33c2691284e - Backdoor.Win32.PLUGX.EYSGVP
eb17f6e4b31656887640fdadd17958ac9dfb5de8c1128258618bd8c63921f2f4 - Backdoor.Win32.PLUGX.EYSGVP
eb9ffe12dff87a143ea188fc6c16f2b3f44e43c2ae20506c4a69c23c3c74e6c2 - Backdoor.Win32.PLUGX.EYSGVP
ebfc2b62ea889cf96c4eb0b649672c6b713ad163fd5818c2f46a9b5726dd80fb - Backdoor.Win32.PLUGX.EYSGVP
f3de33eac07bebd2ce91ec7603b7d021c5e5e68d6b39a3615ee27134b008942c - Backdoor.Win32.PLUGX.EYSGVP
f78d5fd3c8e680a25f0372a82c19866bf1c9fcb131612301f5988128011ce91f - Backdoor.Win32.PLUGX.EYSGVP
f8720cc2747a3518d13193a2fe9cb791be7e37396fbc448f63a8227d5f552e52 - Backdoor.Win32.PLUGX.EYSGVP
fadd3aebdcdf61da44bccf7b71f30312c807c432514b761010aef10ddaf93270 - Backdoor.Win32.PLUGX.EYSGVP
fb765bb69ceb6e63fbb5aaf0bf5be2373d1043507dc4aa41819b84c4d6c9a83e - Backdoor.Win32.PLUGX.EYSGVP
fc1e2a0ed20ef3cb8a543b65cc0db5d05f5e107a6c43bf6f1c0b581e6167a59f - Backdoor.Win32.PLUGX.EYSGVP

fc8ee97fd67dbcd47780713f076c36bedf7c29be0ba6f1912635b0557fc3764f - Backdoor.Win32.PLUGX.EYSGVP
fcf56480bc8bb87af97cdc5dbd7aba94e0178eb5af98f4a2fb813b89b228b63e - Backdoor.Win32.PLUGX.EYSGVP

In-the-wild URLs

http://27[.]255.79.17/ieboxs.exe
http://27[.]255.79.17/rdpclip.exe
http://adobe[.]name:8080/7v9v
http://hk[.]whoamis.info/list.exe
http://www[.]adobe.name/Download/flashplayerpp_install_cn.exe
http://www[.]whoamis.info/dllhost8080.exe
https://adobe-flash[.]wiki/Download/flash_install_cn.exe
https://mmimdown[.]oss-cn-hongkong.aliyuncs.com/windows/mimi-setup-1.1.6.3.exe
https://update[.]adobe.wiki/Download/Flash_Installer.exe
https://www[.]adobe.name/Download/flashplayerpp_install_cn.exe
https://www[.]adobe.name/Download/Updater.exe

C&C

12371829hkdanm[.]fbi.am
149[.]28.31.166:29527
149[.]28.31.166:443
1qw6etagydbn2peifj8hf[.]fbi.am
45[.]76.199.119/g.pixel
45[.]77.22.215:83
adobe[.]name:83
agph[.]ivi66.net:443
agph[.]ivi66.net:53
caonimade[.]11i.me:443
caonimade[.]11i.me:53
darwin[.]github.wiki:53
fbi[.]fuckbc.com:29527
flash[.]wy886066.com
fuckeryoumm[.]nmb.bet:443
fuckeryoumm[.]nmb.bet:53
fuckyou[.]fbi.am:8080
helloword[.]11i.me:443

helloword[.]daj8.me:443
huaidan[.]fbi.am:443
huaidan[.]fbi.am:53
localhost[.]11i.me:443
localhost[.]11i.me:53
rc[.]dajuw.com:443
steam[.]dajuw.com:53
tools[.]daji8.me:443
tools[.]daji8.me:53
win[.]googie.ph
www[.]whoamis.info
www[.]whoamis.info:5237