TREND MICRO | research

Analysis: Abuse of Custom Actions in Windows Installer MSI to Run Malicious JavaScript, VBScript, and PowerShell Scripts

Appendix

Indicators of Compromise (IoCs)

Related hashes (SHA256):

	Detection name
88023bdf25eaa54bcf24f683494fdc6ad1f94741d4d932f5eb343949456dd77a	Trojan.JS.MSAIHA.A
7e043641534d64172d8d7222d602d6855aad1eef63f732fac824c3379cefe88b	Trojan.JS.MSAIHA.A
2c75e6c899238d9ed2e6a37bca9f4c714a913cb42e9b211f1180c4ad22e1a3e7	Trojan.JS.MSAIHA.A
cb4de06ae39da51760f16909ee24649b285d0aa9e62b422a01e79d81c6a6b171	Trojan.JS.MSAIHA.A
dd2058b16d3283cccb6ab97e9ce4c1e69828ab285b4888680c6d87f8c92f4390	Trojan.JS.MSAIHA.A
91c9916e741a3d829448f8271d4acdf7722501c2d46fed7c985fd95b533f6fad	Trojan.JS.MSAIHA.A
4f7e5495f48b2188d536e965067748863ce63681409b9beb11a39cc2fb84c85d	Trojan.JS.MSAIHA.A
25698b240b82852262b2de8e808d739f97339bca1666990dd682938ff7ff90fa	Trojan.JS.MSAIHA.A
2255bfeda16ed904f9ca1f8c872660ffa95365b5ae711ce92b9f957a2130e2fc	Trojan.JS.MSAIHA.A
9961be19eb1c17db21dc2f1d9cbf04ae35ffaf783d33b92f5afe2bb97058d3f2	Trojan.JS.MSAIHA.A
897a5b47811a78407ccdab3e570fba862033b5d4c076b4d2dc5d9f8a4e100280	Trojan.JS.MSAIHA.A
d9e4d80538b0b0a7608c0f1365f5811b6ed5173df5846660830b5d794e9cfad9	Trojan.JS.MSAIHA.A
eaf373d8d7dd5a0b799297bb8c8cd3610d0bdaf604a948915b432c94d32f6332	Trojan.JS.MSAIHA.A
2728c07f5026723e9d42391b3782aa59291834cde57e7ecd21ab094faf0257f8	Trojan.JS.MSAIHA.A

e3e90fbef6e8837f5c74f41bdb4208c89113197ba91826dbb517aea21718072a	Trojan.JS.MSAIHA.A
7155b055642f574210f631be707db2cf6625b2ee9a45b6e7866ecabd75c9590f	Trojan.JS.MSAIHA.A
b3e395bf18e392272953cefc25310839d1e78f1d92a3cb8c83e89062c19789e7	Trojan.JS.MSAIHA.A
d18b10a639545167477957c05bcc10b9d8df0061231d05faea242c7c557b053e	Trojan.JS.MSAIHA.A
de5e6bd022e2c05ea1a17e2cdd8d4cf745acdd92c36b3c84b564a4a48fdc696a	Trojan.JS.MSAIHA.A
d28acec373c669e201a54fa8d34afad9a6fa8470051c6aa6c6f80efefa11fb2d	Trojan.JS.MSAIHA.A
560a8a592196d9dfd32ce6d0e2ac498b3a64f5b791b176e36bb2e721d077f87e	Trojan.JS.MSAIHA.A
7ae252a7ddfa0fc57ab5d59ad2f49400b2f2a794e0fc24311c2fdcc26b072d16	Trojan.JS.MSAIHA.A
5d111482ea0b0b5065e00600d1618ace2e9ddd5f1d75cf0bcde4ef98e7d0f913	Trojan.JS.MSAIHA.A
13225b6bbf814361a120330a8b6e785f1be42c211202d9b544e93e5a86f9bfe8	Trojan.JS.MSAIHA.A
02d951e109115407fd93a5b5021e15d2d22a49cc78bb65faa0a1190732fe4ca1	Trojan.JS.MSAIHA.A
a2d24971430fe6ac17c0bae468401a92078d526e27af1883af61b5ebc5ef0689	Trojan.JS.MSAIHA.A
452b2a5f8ad4746d426f60601cfddacb8efac2609bc3e112d404c9668a5dd32f	Trojan.JS.MSAIHA.A
d1167bc7499d06b10027b96238a516dc1f20ca4a483efd75c8e2103f645f845d	Trojan.JS.MSAIHA.A
508061a79116c1a24e971a2682c5b703ca98c4e76d993eae19d26a3a16d2ae31	Trojan.JS.MSAIHA.A
b8f414006ab416e4d4c46d402199c71d12845c923d3b4e7a0da911ab15cd17f1	Trojan.JS.MSAIHA.A
0d4ce0706d018fe25c561c7fc5cf1436d5db2e80bf225c7ed99d57a7151be669	Trojan.JS.MSAIHA.A

436239f7edf52794c3079cfea89686e113831ab47978d1fcd34ffd5757582f6a	Trojan.JS.MSAIHA.A
2762b5d9bacc8ccf7c9d56bbbd9c20cf83dc672c8e3d2789cd52b795fe1594f1	Trojan.JS.MSAIHA.A
fc860e72caa015cefd24707e639f15ab7ed4337c0619f9fb801adaacc8128283	Trojan.JS.MSAIHA.A
4fe1dfe816420e42cf828d55d1327caada592aa48603f4a044bf05361958b0d7	Trojan.JS.MSAIHA.A
9530ae6ea114eb95f2ff7081e78c062b85d488fe936291e64e95e6240ee8249f	Trojan.JS.MSAIHA.A
9513e83096738e9a16c62b87064e4de3d7628104dde6ba9b9469780c06564793	Trojan.JS.MSAIHA.A
9826f960f36a4bad8cab9dda517060ea48e201c6a462def4407cc0a0c4e620c5	Trojan.JS.MSAIHA.A
b7e64fa27b78871c738c73c4021ec75db970fc055a0bdf7dd7e6355786b76686	Trojan.JS.MSAIHA.A
ecdee70ae5580f9f86f73a2a811236283da0660bd16af33cc7aac5ab1e8ba8d2	Trojan.JS.MSAIHA.A
e11176e221536c6990ad115552179727b01a62399403fc7be580c4b967c0258e	Trojan.JS.MSAIHA.A
ac914d4a899e1c2d5e5744c7560ea8d2096323f006831e33d08501ce3df1e545	Trojan.JS.MSAIHA.A
2830eedc5a95f292f51fee6ea8d58d0b68c9746069b36a016106426734ff516d	Trojan.JS.MSAIHA.A
02e3992b2f80dab38aefd6235068db61acc13d850e80c9bed4325f908b0210ed	Trojan.JS.MSAIHA.A
2821ebd6e20e68e63e9104f222f1ce31137c337a9eb14d0e35ef7d69fa91822d	Trojan.JS.MSAIHA.A
5dfba95b2bdefabe8919b3b754be9ed77dbe5c1ae2fdcec47154c85940ee1d36	Trojan.JS.MSAIHA.A
a4a791263ffefe05889df7b046b812e45e4b01f4fb677ffe373e015bfcb5a7be	Trojan.JS.MSAIHA.A
8d6642edb302a9a60e61deb82158ac159bb72937554af866e852b11d6d3e79c1	Trojan.JS.MSAIHA.A

67255c29a1b2fcc1f9067f08fcf575a2d654e4f8d235a5a583ff2605b7728455	Trojan.JS.MSAIHA.A
3dc2eaea450dfcf7ea0029e9796b8515bce76fe2c9edc92d86f0ac9c5f2d8fe2	Trojan.JS.MSAIHA.A
b805a4e04d0d16ff945b2e4e2286d83622c3db7e9fe1d01ee0fdc88ab628a69e	Trojan.PS1.MSAIHA.A
1b40ceddad5ef4571f423540be1ee2511014b739b490a559cedd7f20df797c19	Trojan.PS1.MSAIHA.A
c5fc03b0d86e01e98eeab8cdabbf08787f41e1faceb34ec1637ce69a811a84a8	Trojan.PS1.MSAIHA.A
78f7713ee80344fc092c3d09bfe8fe3dc649d5c983b36d5d05d0cc2e7139769f	Trojan.PS1.MSAIHA.A
66749f150d28d86b2574e14ff3d5ded39a4522751ff2a64bdca5badb2a9b04e9	Trojan.PS1.MSAIHA.A
9358eaa61d8528eb6ea55af2cface9a24a960e246cc2860b09ba4c950a10b370	Trojan.PS1.MSAIHA.A
63971d10612d590d53206fd6923b4158b1cffff5fab502812d7b47c698f52154	Trojan.PS1.MSAIHA.A
afaff57a1818658009aa0e68cf18909c025d9d67975e92e958e3791e581aa9a4	Trojan.PS1.MSAIHA.A
b4f1ebd93c9fd6c7139e2362e017428e75ff99bda2a552ad970d88a6ff0912a7	Trojan.PS1.MSAIHA.A
5830c011314d4c445d80dc9cd1fc589c37a2ab1ab374ff1705601cfca3080d6b	Trojan.PS1.MSAIHA.A
8207973672f13b9543ba33baaf62b29ebe10ad4276c8502c014d7e0c813fc7df	Trojan.PS1.MSAIHA.A
68e90538ab20f24a06b0dffbc6c533f9da8de9c5355cda19096d0b875a385d03	Trojan.PS1.MSAIHA.A
7c5351fc5b7597780a848a9656d6e1b834d533f1aa0366123240ca86ba6c5d2f	Trojan.PS1.MSAIHA.A
a5c91b61a3a44ff921cf5a7116af260fc0127fbe99f6f7dc85f827095be69317	Trojan.PS1.MSAIHA.A
f04cf75053e627949cf2efe27ce944fbce9a3d7d6428874b881b469a9639744b	Trojan.PS1.MSAIHA.A

a4fee646c3677ce62f28146aa64b62879635b73d9d3b4e2c74e410674e6821c9	Trojan.PS1.MSAIHA.A
5c4ba034435fada5ca982c89225295a3d9bb1c1792217b76dafa0a612899a6ea	Trojan.PS1.MSAIHA.A
234ea038ea2825ee0867cd7cd590caca6a09d3dd9ff0acada89f1d72f25b3de2	Trojan.PS1.MSAIHA.A
805c80994473ffbac05fdb73585b28fd4ffab6cd0399a6d03eb75cf8706f7445	Trojan.PS1.MSAIHA.A
f7f2a56045731e4892a72819754128d4cd181c22975c83e1ce1c1739213ad279	Trojan.PS1.MSAIHA.A
3768b90d3404f6b2dec3186f4697debe211ad11a93238f047f1c3ed5e49e26a3	Trojan.PS1.MSAIHA.A
877ca4ad7f965251eefe2a3e736ac4d1e443f8c0178d116f611cce01babc7465	Trojan.PS1.MSAIHA.A
59bdfdb074f1e542a881d19c1e3b93981f9dead259a6177a3d6c200b3b429558	Trojan.PS1.MSAIHA.A
52219cf6a8ccbcfba4c65f1a30763e94dbb6df77a8caab87c3dbb4f9daedacb1	Trojan.PS1.MSAIHA.A
ff78197646d3599045783feb35e55ca37726db9ad8e1e1acb6d7b1afd64ff9d8	Trojan.PS1.MSAIHA.A
989284d0d02909ae9f53350cc11cd501ddd2a8c292d0e4a00572e4be249cc683	Trojan.PS1.MSAIHA.A
a5484ced2f8132bf44b757420372b6231638e8dca96fc55129e11817cbd3c561	Trojan.PS1.MSAIHA.A
f708f155bf1fcdb5c3c1dc4d8b387a788fffb27a71ece5c7f110cd5d569f31f7	Trojan.PS1.MSAIHA.A
e3f3c3ead469d0b525f17555e204195785cc50eb8599df07eb1c82edb8f3bfec	Trojan.PS1.MSAIHA.A
cf098a64d7539980c64c749c4a38e98662a29e8370dd0995a04b6ebf69f6b010	Trojan.PS1.MSAIHA.A
1f2576d30303b5853202a151ce8bdfdfc09dfac94e97be8a5a315359d8c20240	Trojan.PS1.MSAIHA.A
490a844877e4bb7070bb19bf6899fd2eb13f5e5f3ee6ec62d1bc6c2c668f7633	Trojan.PS1.MSAIHA.A

631b0dbe0f6aa0c061b27154e0accfa24c1ba05b06a408bdd01c0780dc876e9c	Trojan.PS1.MSAIHA.A
5d2d0b36c81c3303560b5b1f2828ffcc6acbc3f5325bf2ac107817fa1b259aa1	Trojan.PS1.MSAIHA.A
a5484ced2f8132bf44b757420372b6231638e8dca96fc55129e11817cbd3c561	Trojan.PS1.MSAIHA.SM
c5fc03b0d86e01e98eeab8cdabbf08787f41e1faceb34ec1637ce69a811a84a8	Trojan.PS1.MSAIHA.SM
f7f2a56045731e4892a72819754128d4cd181c22975c83e1ce1c1739213ad279	Trojan.PS1.MSAIHA.SM
326452a45f62957651f834c480a28a12f5ddecbebfd393fd77284366887cb84d	Trojan.VBS.MSAIHA.A
56d37082a02b6b4bd08e55060945fbcdf4fee3bc372062b4caaa04133cd8d398	Trojan.VBS.MSAIHA.A
08d289adaea9b6ebe0de7e0961a0919ca9b66441c5fcf4aa9a3238a5d4782fa4	Trojan.VBS.MSAIHA.A
96f163247ac719e2f3c23329d72c5919aaaff510021edfa4a9fe3a91ea501fda	Trojan.VBS.MSAIHA.A
75602afffbfba49f81c576959d9c4a87a850cf49c9e47252f6d9662d28edf480	Trojan.VBS.MSAIHA.A
93a4672abfc5af99be639a64720bca442b4884211695cf1e530f8517515daacb	Trojan.VBS.MSAIHA.A
46acf4ff0f2e1d40022cf0e13ffc52e7574fc0bdf7b04468ddf9fc60658a5759	Trojan.VBS.MSAIHA.A
fa71e1c2b50eceb47177e7427e41cccb0fcfb6d69043fc026a0944a211a53f3b	Trojan.VBS.MSAIHA.A
ec85138598c57c6a6bdb5ed470614f582d3b5a8c6b243eb2f41b9970ea13d130	Trojan.VBS.MSAIHA.A
70691084372a08973d9456294d9eb83f6b1c5a7e1265c96eec15dc108f9fa223	Trojan.VBS.MSAIHA.A
1c17cf7af862cdb0af2f5540391ac3d0b427bd6369cf1a5fbb8d82fb80964d1c	Trojan.VBS.MSAIHA.A
30b05b0ea020a8168e1052a17ddb0b2b9a249d54866a1ccb5b78d0b0a575793b	Trojan.VBS.MSAIHA.A

6c23f8d96b2e840567644418099f458640fd60b6d9ac6f752c30b7bc55166c04	Trojan.VBS.MSAIHA.A
3416f2430480f1e8b79f8f64b42f76bfec83b69fdaf055cebc1209b87d149d28	Trojan.VBS.MSAIHA.A
65677dbe3b686c6c07026ada7575ae020d7d1648b302afb3a454fa1dc40c0fe4	Trojan.VBS.MSAIHA.A
f708f155bf1fcdb5c3c1dc4d8b387a788fffb27a71ece5c7f110cd5d569f31f7	Trojan.PS1.MSAIHA.B
234ea038ea2825ee0867cd7cd590caca6a09d3dd9ff0acada89f1d72f25b3de2	Trojan.PS1.MSAIHA.B
8cd927f9e6abf3ce1cdba7c1abd2d9417509e41c9eb3831685964a341cb6ac3e	Trojan.PS1.MSAIHA.B
18797de8c4ea36572c6a2d5f1f41044bbf924893f5393ab619646fe3dd002b6c	Trojan.PS1.MSAIHA.B
dcef0f78d6cc93a818ba512fcf0a6f25d1533d081c6754b96adf9e4d9066e5c9	Trojan.PS1.MSAIHA.B
f03fb0970be1a728e8ad1632c1d3d1c16af8fa298e0d9984795934478dfdf4d1	TrojanSpy.Win32.CASBANEIRO.XLB
8c0fc11afb2500dd987642cca9d2a092ee978cfe0b6a5d1456402e04e04b6055	TrojanSpy.Win32.CASBANEIRO.XLB
c60ce678c4deab3425f3731809ae069875bdc529b55be9fe77e3c310b1aef37e	Trojan.AutoIt.AUTINJECT.AA

Related malicious URLs:

hxxp[:]//3[.]91[.]64[.]111/index[.]php

hxxp[:]//35[.]247[.]253[.]135/initId[.]php

hxxp[:]//35[.]247[.]253[.]135/initId[.]php

hxxp[:]//35[.]247[.]253[.]135/initId[.]php

hxxp[:]//45[.]77[.]17[.]129/coringa/fsdgtrgerhet[.]php

hxxp[:]//149[.]56[.]244[.]167/~postosao/xxx/xperiencies/

hxxp[:]//149[.]56[.]244[.]167/~postosao/xxx/contador/

hxxp[:]//149[.]56[.]244[.]167/~postosao/xxx/contador/

hxxp[:]//149[.]56[.]244[.]167/~postosao/xxx/contador/

hxxp[:]//149[.]56[.]180[.]167/cont1/

hxxp[:]//177[.]153[.]227[.]196/~mudeagoracom/atualizacao/xxxx/AAAAAxxMonnMX[.]zip

hxxp[:]//177[.]153[.]227[.]196/~capitalefigeniac/eletros/xxx/aLPdtQRnMPPz9[.]zip

hxxp[:]//177[.]153[.]227[.]196/~postosaoangeloco/clinicas/pacientes/

hxxp[:]//177[.]153[.]227[.]196/~mhphostcom/team/best/kJ8HFswn[.]zip

hxxp[:]//177[.]153[.]227[.]196/~postosaoangeloco/clinicas/pacientes/

hxxp[:]//177[.]153[.]227[.]196/~postosaoangeloco/clinicas/pacientes/

hxxp[:]//191[.]252[.]109[.]43/initld[.]php

hxxp[:]//191[.]252[.]109[.]43/initld[.]php

hxxp[:]//alcoolismo[.]com[.]br/sMCVxxMoMX[.]zip

hxxp[:]//barbosaoextra[.]com[.]br/fonts/initld[.]php

hxxp[:]//barbosaoextra[.]com[.]br/dados/noticia/7/imagem/initld[.]php

hxxp[:]//beppo[.]com[.]br/yaya/

hxxp[:]//capitalefigenia[.]com[.]br/nuvens/AAAAAxxMonnMX[.]zip

hxxps[:]//capitaltotal[.]com[.]br/vestiarios/modelos/

hxxps[:]//casanov309[.]online/jurtfgd/kjhgdrftejk[.]zip

hxxps[:]//casanov309[.]online/mod9087/cumpy7[.]zip

hxxps[:]//casanov309[.]online/yainc/gtflux[.]zip

hxxp[:]//clinicasaoangelo[.]com[.]br/atualizacao/mLPxTsMCVxxMoMX[.]zip

hxxp[:]//clinicasaoangelo[.]com[.]br/atualizacao/mLPxTsMCVxxMoMX[.]zip

hxxp[:]//clinicasaoangelo[.]com[.]br/atualizacao/mLPxTsMCVxxMoMX[.]zip

hxxps[:]//cntusestudos[.]site/bargihudon/xmaoim2m[.]zip

hxxps[:]//cntusestudos[.]site/ariegua/sewdeaq[.]zip

hxxps[:]//cntusestudos[.]site/bargihudon/xmaoim2m[.]zip

hxxps[:]//coringa[.]painelcoringav5[.]site/mortolino/Gerador/Load/msi/idfasnfhsaifudhasfklasfjaksljkgjlkjlkgjlk[.]php

hxxp[:]//www[.]cupom100[.]kinghost[.]net/semestre/initld[.]php

hxxp[:]//dyar[.]com[.]br/rpm/

hxxp[:]//dyar[.]com[.]br/rpm/

hxxp[:]//focustributos[.]com[.]br/mxwjMiBNRKnx[.]zip

hxxp[:]//hnhu[.]gob[.]pe/portal/documentos/wp-content/plugins/hello_dolly/5s6pa4ljc[.]zip

hxxp[:]//ilfratello[.]com[.]br/rdr/mLPxTsMCVxxMoMX[.]zip

hxxp[:]//joaovicente[.]com[.]br/pnl/

hxxp[:]//krika[.]com[.]br/lpot/xzolXmjLumOdy[.]zip

hxxp[:]//krika[.]com[.]br/pnl/

hxxp[:]//krika[.]com[.]br/lpot/

hxxp[:]//macil[.]com[.]br/mLPxTsMCVxxMoMX[.]zip

hxxp[:]//macil[.]com[.]br/mLPxTsMCVxxMoMX[.]zip

hxxp[:]//menegatti[.]net[.]br/nHh5Uz[.]zip

hxxp[:]//mktcomunicacao[.]com[.]br/cn/

hxxp[:]//mktcomunicacao[.]com[.]br/cn/

hxxp[:]//mudeagora[.]com[.]br/atualizacao/xxx/sMCVxxMoMX[.]zip

hxxp[:]//nevesai[.]com[.]br/cnt/

hxxps[:]//s3[.]eu-west-2[.]amazonaws[.]com/stocksoftbr/ModPumMs2003[.]zip

hxxps[:]//s3[.]eu-west-3[.]amazonaws[.]com/abrilgeralll/ModPmAbrilzada[.]zip

hxxps[:]//s3[.]eu-west-2[.]amazonaws[.]com/stocksoftbr/Mod1803xrd[.]zip

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/mortobas/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/frezzado/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/zebriudo/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/zebriudo/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/caddeeaotk/image2[.]png

hxxps[:]//s3-us-west-2[.]amazonaws[.]com/stacklayer/AbrilModPum[.]zip

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/coringaudo/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/cadiadorls/image2[.]png

hxxps[:]//s3-us-west-2[.]amazonaws[.]com/stacklayer/AbrilModXr[.]zip

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/coringaudo/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/frezzado/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/mortobas/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/cadiadorls/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/robootiza/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/gjueuirzebrakkjsda/image2[.]pn

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/hkjtrobotsjd/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/riejardalkj/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/lkjrcadeadfikjg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/gsdjrmortosdfa/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/cofge5hrtyheujhsgrfdsg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/gsdjrmortosdfa/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/zebthdergeh54eghe5rye5hr56/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/cagf4yh5rtjyek796l78jrhrdhg65e/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/jarhfgjr56t5ghrtdfggherhjd/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/robtjkl86ol6i7rhtdsvfsfegd/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/mou56ytsdgsgbdt6jdfg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/cofge5hrtyheujhsgrfdsg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/mou56ytsdgsgbdt6jdfg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/cagf4yh5rtjyek796l78jrhrdhg65e/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/robtjkl86ol6i7rhtdsvfsfegd/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/jarhfgjr56t5ghrtdfggherhjd/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/robtjkl86ol6i7rhtdsvfsfegd/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/jtruy56ygdfx/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/cagf4yh5rtjyek796l78jrhrdhg65e/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/jarhfgjr56t5ghrtdfggherhjd/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/mou56ytsdgsgbdt6jdfg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/mou56ytsdgsgbdt6jdfg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/bdthertyhed6/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/fgdh65yeghfg/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/hr6tur5ysdgh/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/gsdgrjtyityh/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/bdthertyhed6/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/hr6tur5ysdgh/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/jtruy56ygdfx/image2[.]png

hxxps[:]//s3-eu-west-1[.]amazonaws[.]com/hkjtrobotsjd/image2[.]png

hxxp[:]//sertaomax003[.]kinghost[.]net/yak1009/hfmacttpo[.]zip

hxxps[:]//sistemadecontagems-com[.]umbler[.]net/nova/

hxxp[:]//soot[.]com[.]br/compactador[.]zip

hxxp[:]//sppdms[.]com[.]br/mrw/procedimento/investigatorio/intimacao/compactador[.]zip

hxxp[:]//topgretr[.]com[.]br/initld[.]php

hxxp[:]//topgretr[.]com[.]br/initld[.]php

hxxp[:]//topgretr[.]com[.]br/initld[.]php

hxxp[:]//topgretr[.]com[.]br/initld[.]php

hxxp[:]//topgretr[.]com[.]br/initld[.]php

hxxp[:]//tupiratinsnaweb[.]com[.]br/comeco2123/compactador[.]zip

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

©2019 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.