TREND MICRO | research

Websites Hosting Cracks Spread Malware, Adware

Appendix

Indicators of Compromise (IoCs)

URL	Description
1a3a3b7817f44949[.]xyz	Malware Accomplice
24d19c52f04b13a5[.]xyz	Malware Accomplice
4alpha[.]xyz	Malware Accomplice
4everfeel[.]xyz	Malware Accomplice
4legand[.]xyz	Malware Accomplice
4pieces[.]xyz	Malware Accomplice
679814b72cfad5d5[.]xyz	Malware Accomplice
7001d44e3399cd85[.]xyz	Malware Accomplice
8343a51b3aec209e[.]xyz	Malware Accomplice
895ae68c0dd074b4[.]xyz	Malware Accomplice
92187dce3cfa5aa2[.]xyz	Malware Accomplice
9961786d6834d212[.]xyz	Malware Accomplice
9ff9585a4f95f00a[.]xyz	Malware Accomplice
a34e9523693ae52d[.]xyz	Malware Accomplice
allcrack[.]info	Malware Accomplice
allemz[.]xyz	Malware Accomplice
b[.]1p1eqpotato[.]com	Malware Accomplice
b2104237bc7d6c98[.]xyz	Malware Accomplice
bismil[.]xyz	Malware Accomplice
browsechost[.]xyz	Malware Accomplice
btrasd[.]xyz	Malware Accomplice
c[.]ewoss[.]com	Malware Accomplice
c3ecdd1fbb9a92c1[.]xyz	Malware Accomplice
c57caf2ae132d0b4[.]xyz	Malware Accomplice
c7b55e305871a2ec[.]xyz	Malware Accomplice
cache-check[.]net	Malware Accomplice
ced83f6fa144bab3[.]xyz	Malware Accomplice
cotraresi07[.]top	Malware Accomplice
crackkeys4u[.]com	Malware Accomplice
cracksarena[.]com	Malware Accomplice
cracksversion[.]com	Malware Accomplice
cracxpro[.]com	Malware Accomplice

crx24bac5[.]xyz	Malware Accomplice
daringman[.]xyz	Malware Accomplice
dedicatedcloud[.]info	Malware Accomplice
dream[.]pics	Malware Accomplice
dugdphost[.]xyz	Malware Accomplice
f5f5e40934718734[.]xyz	Malware Accomplice
feturen[.]xyz/	Malware Accomplice
freecrackdownload[.]com	Malware Accomplice
gandis[.]xyz	Malware Accomplice
gloriouhost[.]xyz	Malware Accomplice
hxxp://11sdhbvj[.]club	Malware Accomplice
hxxp://cnetdl[.]xyz/	Malware Accomplice
hxxp://download-files[.]work	Malware Accomplice
hxxp://file-download[.]info/	Malware Accomplice
hxxp://founanir[.]com/	Disease Vector
hxxp://komelix[.]xyz/	Malware Accomplice
hxxp://linkgame[.]info/go/aHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL2ZpbGUvZC8xZlpLOU5memVnMEZnMnhnRTNBVTVBXzA0V0NYYlNrTmovdmlldw==	Malware Accomplice
hxxps://4alpha[.]xyz/	Malware Accomplice
hxxps://4everfeel[.]xyz/	Malware Accomplice
hxxps://4legand[.]xyz/	Malware Accomplice
hxxps://4pieces[.]xyz/	Malware Accomplice
hxxps://brnomess[.]com/	Disease Vector
hxxps://cdncache-a[.]akamaihd[.]net/i/items/z7b85/js/z7b85[.]js	Malware Accomplice
hxxps://cnetdl[.]xyz/	Malware Accomplice
hxxps://daringman[.]xyz/	Malware Accomplice
hxxps://jupiters[.]xyz/	Malware Accomplice
hxxps://mycloudbook[.]xyz/	Malware Accomplice
hxxps://myroaster[.]xyz/	Malware Accomplice
hxxps://peafiber[.]xyz/	Malware Accomplice
hxxps://stronglly[.]xyz/	Malware Accomplice
hxxps://ziphost[.]online/	Malware Accomplice
hyporzfilez[.]xyz	Malware Accomplice
iadfna[.]xyz	Malware Accomplice

iibex[.]xyz	Malware Accomplice
jscontent[.]net	Malware Accomplice
jupiters[.]xyz	Malware Accomplice
kamalsas[.]xyz	Malware Accomplice
kellyfight[.]com	Malware Accomplice
kincofilez[.]xyz	Malware Accomplice
komelix[.]xyz/	Malware Accomplice
lotrihost[.]xyz	Malware Accomplice
metriq[.]xyz	Malware Accomplice
munikar[.]xyz	Malware Accomplice
mycloudbook[.]xyz	Malware Accomplice
myroaster[.]xyz	Malware Accomplice
ovagames[.]net	Malware Accomplice
oysfob[.]com	Malware Accomplice
pandalytics[.]xyz	Malware Accomplice
peafiber[.]xyz	Malware Accomplice
photoa5260bc7[.]xyz	Malware Accomplice
pizbaserver[.]xyz	Malware Accomplice
ppae8oe4eku9[.]com	Malware Accomplice
pprq7[.]com	Malware Accomplice
procrackey[.]com	Malware Accomplice
ps4ux[.]com	Malware Accomplice
qdatasales[.]com	Malware Accomplice
rabil[.]xyz	Malware Accomplice
range6d109e83[.]xyz	Malware Accomplice
remotefilez[.]info	Malware Accomplice
rismz[.]xyz	Malware Accomplice
ryuuf[.]xyz	Malware Accomplice
s[.]dcbap[.]com	Malware Accomplice
s[.]hklmm[.]com	Malware Accomplice
s[.]igmhb[.]com	Malware Accomplice
s[.]lm15d[.]com	Malware Accomplice
s[.]pmddby[.]com	Malware Accomplice
sahiltech[.]gujworks[.]com	Malware Accomplice
secure[.]trkkrd[.]com	Malware Accomplice
serialfull[.]info	Malware Accomplice

siteprerender[.]com	Malware Accomplice
stronglly[.]xyz	Malware Accomplice
subhans[.]xyz	Malware Accomplice
sygdf[.]xyz	Malware Accomplice
tadive[.]xyz	Malware Accomplice
technicalcomputersolution[.]com	Malware Accomplice
thecracksetup[.]com	Malware Accomplice
thepcgaming[.]com	Malware Accomplice
tonia[.]xyz	Malware Accomplice
tukiodrft[.]xyz	Malware Accomplice
tursd[.]xyz	Malware Accomplice
uvi4-servers[.]xyz	Malware Accomplice
uyhfd[.]xyz	Malware Accomplice
vimxhost[.]xyz	Malware Accomplice
www[.]alfygame[.]com	Malware Accomplice
www[.]freepcgames51[.]com	Malware Accomplice
www[.]freepcgames52[.]com	Malware Accomplice
www[.]gujworks[.]com	Malware Accomplice
www[.]icoregames[.]net	Malware Accomplice
www[.]interestvideo[.]com	Malware Accomplice
www[.]serialkeysoftware[.]com	Malware Accomplice
www[.]softfiler[.]com	Malware Accomplice
www[.]thegamesdownload[.]net	Malware Accomplice
yahsia[.]xyz	Malware Accomplice
yairs[.]xyz	Malware Accomplice
yiaris[.]xyz	Malware Accomplice
ytr556[.]xyz	Malware Accomplice
ytsda[.]xyz	Malware Accomplice
ziaris[.]xyz	Malware Accomplice
ziphost[.]online/	Malware Accomplice

Figure 1. Pay-per-install (PPI) websites that spread malware and adware.

SHA256	Detection
251EC73E864627D26DFE2ED8D857E029916285E0AD8E1FA1DD864AB4C42E1564	Adware.JS.BrowsJack.AA

4BB676D8B5B61940A613DF0B7909CA4C8FAAE0BBBA69EABE1328E30FCF815B1A	
68AF9E29178C8FE652D42FC889B1C2CA7D2C2C2784B215A806A1314BDE0F1161	
A861BF4A01F4680C5292A217AA401C0C7BBBE4F8D5B7985C9C39F1879B7C6F0D	
AA00DB31980B4811E1539723F5F4508E71227202E3AB3AA6D07859CA9C9709BD	
B661A3058767AEC51967F1B4AD9944CC344B92F0079FF0E031E19DCBD30DE72F	
B9FE0F691DC60593BD6FA97C244CD32A6772203CBA404702A5B1F22A0111197D	
DDDA97623B89D2143445A41589594297C568DC2EFB56651DD86B4BE7E52B75B8	
EEBFB2078FAB96CF24BA9B10BAFACB8D7EA317DA484DA067F9C44DF2072124FB	
F8CE61FBF61531C9340C239F54CA9BEE99A0E98B7D5E25484CA3C0C5E69A0939	Adware.JS.LNKR.AA
7A20A7DA7A71A18B7318AFA3ADFBAC70957FFEF170A196ECD346B6AAB8AC8603	Coinminer.JS.COINHIVE.QSVBWMT
3C1F7AF5E69A599268BCB3343B8609006A255090234D699C77922C95743E9E98	Trojan.Win32.SMOKELOADER.BR
6537843B21462F2F851D8B73CAA6BA1310177082991F40A74AAB3D19D7774ABB	
8E4A1C18E20FE4C941C2BA41817D9A594EB61BD78205C5249600B80053D1C6B8	
9902A7FDAAC2E764B8E50ADBD9EBCA4D8D510C2DF9AF6C5C6A19C721621DD873	
B8943FC714223B6C3802BBCF298374FA2558977122129D14EFCAD50A44D97CED	
C1A900D7A0C9C1FC5A5016DA37BF9A630AE4479D8679DA3B2A5E4AAC6E48E6D1	

CDA45D5FA94378384FB24ACB08D8876276589395BFEB3BB1F1C238DCBEDA4D02	
D10748BD42FF423687616BB1A36CA3CC829B37AF4013382CEB18B2C80263300D	
57AD792C2B88E32003582F2B8A7ECA4FF5A5FD13A691C797DEC9CFA2C93A9D97	Trojan.Win32.AZORULT.WLEE
8BB0482999B0F6C1BC5B7A9EA4B156D95B2330390DB26E01883DC3A2B832A5F9	Trojan.Win32.POISON.AD
13BF5C5D7F20410B0B87060AD144BF78047A02E3DA8E292723040EDE4AF3B5B0E	
25124012F44F5D838C0C924D074729AB612F240785A305C8955376D1AECDB077	
2ADD6E9481830BDF25FCB67C5902A29EFF674A52377D77AB1459F561F08426FBF	
6D7E441B7451F644C533DFA2B34B14662B12F3EB61CC43B332E60E3D821C1AB0	
7F37C38D208A5AEB6DF1B932AA6819904D89AA62166A3C2D7B04E9A68C8BD386	
D36FFF0B9D62C5E2BB707CBB94283F64FCD8AD7BA8A67CAFAD72A0D620821F39	
CF2B678C818250017178507080B51F6B34EE4D642FA022AFADD82D741EF59540	Trojan.Win32.MINGLOA.A
C948F55D1FB5F492E726CE561A1836A37840E86D2B3F90050E496DDE27B49615	
D4D3127047979A1B9610BC18FD6A4D2F8AC0389B893BCB36506759CE2F20E7E4	
479DB7DBF43EF8A762678EA30F8D589176FE6610C5CD825FA1A202CE9BB6B12A	Trojan.Win64.FOXSTLR.A

E7C02D9F66BBC38625F659FF3FBED32A125B402D8196621D08637F57A8F33B05	Trojan.Win32.FOXSTLR.A
3CFDEC895F96DAE3DCDC86F803F0AF499877B38A462A6CD0AC48F25266F7398D	Trojan.JS.MALINK.AM
B0D675F1E5D4F772CD90E59A2D64D24CF682A1C966FECCA50C87C985F64E4136	Trojan.Win32.EXTENBRO.AB
8F538ED9E633D5C9EA3E8FB1354F58B3A5233F1506C9D3D01873C78E3EB88B8D	Adware.JS.ExtenBro.B
D35FBD13C27F0A01DC944584D05776BA7E6AD3B3D2CBDE1F7C349E94502127F5	
0189D710AD69B80F18E165AA80E623341D930B1B80FDBAEF6F5F7E3EA5D4CA63	Adware.JS.Lnkr.AA
8B860E41AA3C0E704799CBE488AE40764B8A347A2774EF7E2D2C0E8A3A474F0C	
049A37075D98969F1329129023B46109DAC41A86459B55A53A22E08EF18874E0	Adware.JS.Akamaihd.A
1AF707773DA58ACE84AF3A9FE659C77D64AE3528A998CC32C5F8D9703E3EDB39	
46FB1FEAE76905B3EAEE831239C3BE27D4EFB75BB122FF82A6C31F4090A6CFF3	
546968800386EF86BF9B673F4405144084E23094268D7C9C1FCB8B6B2A66954D	
56AA3FFFDB47FA4DA0571684F9A551DDB13D71AF97FFEDBD4537026E2AAE7521	
5ED56A69BB277EB788D538F7328EEFC1D599129B8D18B4F2F452BAEE0A858CB6	
97B27132E344610184D3A370FF254089F6DB80BDC819AB1E68DB4E4CF858D6C0	

98C1362C75F7C9F7447430D392E0AC0619FDFDE64BB85816103F2A03F206A913	
9FA19D7AC57DBB893EB4F7DCAAA3E87AB58C8BB0C4475B5B6576070E3AFE5017	
A4B956D347873245A669069CDF76FCC5613E9ACFD1ABCB43AC146EC779895942	
A9E940EAED37BDFEB9469BD53E3C485FFC8BDB983BB29AC8288C47E5DE4890E8	
B33E1023127464D1F62830A6A10AB09B40F16724EC86FF6578692820E4378875	
B5CAFF60D722FD23963A8A8BE0B4527BF3CE58EDD559EB2BC180064C74BD6779	
BC2E0AFD718443AB0D807B487647D67912C18A5E48000EAC85700F0008D6BD87	
C4DDB0000582576F17F103A7C652C689932D0065612E0A783998951CD461F135	
C865576100A0634C78EF56181EA4798BCF0168DFBB214963740552F618A15C69	
CA893BAE32773CB9A638CE4035116D591E51B4510E07EF571E20732FA51C4B42	
E34B4FD2057A647BD1E3E06581AE9A0C55C07348D509CC9E5339F85ACBD040D6	
EF6A409ED7123EE10AD9FF0A68847BC19B7977611A9CD5A3C3294FA7A7888A4F	
F26EA9BC43E7F3BF8D5DA284E298DD262E084475CE5FA252D35EEEF11CE11E79	
FCE80A44A3677C0C797BDBD5ACD3F0E5590192181C507538D9E8245225F11E54	

FF076B5C76558318602642F4D239DAD9EC89DA70E77D029186CD3F708801E3F0	

Figure 2. Malware and adware detections

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