TREND MICRO | research

Shifting Tactics: Breaking Down TA505 Group's Use of HTML, RATs and Other Techniques in Latest Campaigns

Appendix

Indicators of Compromise (IoCs)

Related hashes (SHA-256):

	Detection name
920dc539dc6d018864ab2d1ce1955c4efc1bb70cfb4f31837349bdd198b202b0	Backdoor.Win32.FLAWEDAMMY.AH
a1e8b9e0b10a9fa979ac90f08721b237d6d2c000313855442f1a88aca43e709a	Backdoor.Win32.FLAWEDAMMY.AI
ffa564c01110a8d3350624b12dc67703fc00644f87b3e5b599013837c33854d9	Backdoor.Win32.FLAWEDAMMY.AJ
c24ab9d90ba0dd363de5cac13a27758a9951f5f60dd7ecbf3f458d9d80cee432	Backdoor.Win32.FLAWEDAMMY.AJ
0d51f0fa172718b5e462fd8f2b077285f3cf28a6132933858293af4051f025b9	Backdoor.Win32.FLAWEDAMMY.AK
9de446b29f7ac43609a4026a89e240809cd98cf33963387a708a4fd3d72bce6b	Backdoor.Win32.FLAWEDAMMY.AK
3ded9c7772a9a7a63e78e4f78e2b652351be8185863f23cbff369e2faff1d9a1	Backdoor.Win32.FLAWEDAMMY.AK
8e5a7ca13f217a7acf9cdeb38f1c2e926dcebaaeb32e145bd079e44d7be9d92c	Backdoor.Win32.FLAWEDAMMY.AK
50f300bf2e87a2063eee32867b1d7f41f55f67cec0b2f26d2d6766dcf7c459a6	Backdoor.Win32.FLAWEDAMMY.AL
388769cfe8894c84cce9de27ea27f31fdeec5178db3c27cb6e969225e7bc4669	Backdoor.Win32.FLAWEDAMMY.AL
2ca22859ea8a28e55502b5c7da12f3df33552ab0b94373a75c7f4c9c62eb3cd9	Backdoor.Win32.FLAWEDAMMY.AL
c97e51b5e19206a8b0181aab52c427473d221422ec22a3a4c8dcd25fb5f441bb	Backdoor.Win32.FLAWEDAMMY.AL
834d3c93e4e19bf609ea0af2fca9355c46a05050df8647027ff788287e93d259	Backdoor.Win32.FLAWEDAMMY.AL
31f4a30317b6d6eea7829750a706366528ec13e57abfa1ecaef88ca4e570ff07	Backdoor.Win32.FLAWEDAMMY.AL

25dda542bcae4694bd1e9c0d7f768d2f92f3264451511 24b8ce5b58c46975b80	Backdoor.Win32.FLAWEDAMMY.AL
e2cb3ede6e6cfd774ba1ff8460530461cac2085c664d3288 338eb565e1556016	Backdoor.Win32.FLAWEDAMMY.AL
aacc4be830debbbe0695cf2da6a97662050030734e3cdee 1507735ffbe464b79	Backdoor.Win32.FLAWEDAMMY.AL
29d909f3fc2691c1e144d07666644ed34663ee35feff38de2 8855f5652646b55	Backdoor.Win32.FLAWEDAMMY.AL
70eb8455c7f785dd0e2b2d99f49855209af1336b63b2d469 d4374a23d61db61b	Backdoor.Win32.FLAWEDAMMY.AL
a71868b9a251b7986841b2adf10e4e6e0d3a53e1ba08a8f e5ce0ff8d5c954748	Backdoor.Win32.FLAWEDAMMY.AL
35c4636bc2298f6d61cbf656930b984e30a5767bc45d140 d7517ca3b6a5fb30f	Backdoor.Win32.FLAWEDAMMY.AL
bd89300f5e2ab6a7aaeb339870f526465a5d3ec2f8f8fa6c9 69a9a7635406a22	Backdoor.Win32.FLAWEDAMMY.AL
2527295523f67e0a87c7e6049f2b7954f494b33e18254618 ae02528e1f9b1d4b	Backdoor.Win32.FLAWEDAMMY.AL
ae570d4a4127838a19daa4cc44ebb7528905be9e75c8a1 cf3545ea231f4d7d6e	Backdoor.Win32.FLAWEDAMMY.AL
f3df565c41cc26604a19b2d27406fa5ec94e6f876ef5f40b6 4bf2e3d28696e76	Backdoor.Win32.FLAWEDAMMY.AL
5d121e2a5a4ce3bbb96152af8dd529a06a969e2b405f79af 038e02f2ae862c31	Backdoor.Win32.FLAWEDAMMY.AL
e0c1c2ab82ff668a2310652b46a340738b2e7c2cdec90d1 97ec57b874b0de6dc	Backdoor.Win32.FLAWEDAMMY.AL
c76e57800aa901071a462a0fe0bb5dddb6433cba5cf2cc2 6337dc10625409d51	Backdoor.Win32.FLAWEDAMMY.AL
c7bd34c293757db133003b926be050bbeabc8cabfae4a2c ac1e58ae528594aec	Backdoor.Win32.FLAWEDAMMY.AL
8235712093c3d4d8e6ace925ce65654bb6d68673cfcfb8f3 808f40b67bbdf65d	Backdoor.Win32.FLAWEDAMMY.AM
c8fb3160afb8cc0f6bded6b4d27c5557e25df3aa6379d053 ba82a5ee216ea29c	Backdoor.Win32.FLAWEDAMMY.SMA

af8d87c144265ab2f056802b128af06eb8b548ed0761161f7a4a5b39fd0d2165	Backdoor.Win32.FLAWEDAMMY.SMA
aed93518018d50c2d41d9d8a3c07207512205a17a0978a208deb28e4d88fc38a	Backdoor.Win32.FLAWEDAMMY.SMA
322a5c41e47e2d311d7535f407df803d9a56b2ec90c5948b7a9236edd0ff276b	Backdoor.Win32.FLAWEDAMMY.SMA
4066c65958d09f36a453f5a3fd794f46e886fcd878aac4c589ae9264eb070457	Backdoor.Win32.FLAWEDAMMY.SMKAT
103d73ff58511b8f67b83507afba8262c145e006647264423bb2ed8fb77e13d7	Backdoor.Win32.FLAWEDAMMYY.AC
7ad161d420780db1b14358cd60d50482e3bd9964ad8a9cb33942e698bdbf0d9e	Backdoor.Win32.FLAWEDAMMYY.AC
f74bedcb4ac33f7343fbbabec0f636b887d92c06e156ac765f345732cf6cbce8	Backdoor.Win32.RABASED.AB
17b20aa770ccf250b5aded470fbbaa329856543022ba21f993d5fa02ebb670c7	Backdoor.Win32.RABASED.AB
8c738710cff8cecb1f2e22c4255764e2288981b1d0d78f1d9afd715ab0188abc	Backdoor.Win32.RABASED.AC
35b3ae3b68e7019a47ce375d3953da2b29bd8b6a8100a98003d873dfb48a601f	Backdoor.Win32.SERVHELPER.A
fd2516f5a8dd9eaddac65f4bd8ae4ed6cba9e115ebe88c3f6d2f5e2cdd5e20a6	Backdoor.Win32.SERVHELPER.A
64d48cde2de91849a414a86ad342a157288e7f6e58d7e58de1d077b9737e6dd8	Backdoor.Win32.SERVHELPER.A
988f4869e55317fb97aad3bde4fdb89180148ea7dd6eba7d84f8d1a3d5fb027b	HackTool.Win32.RMS.AA
609b0a416f9b16a6df9b967dc32cd739402af31566e019a8fb8abdf3cb573e30	PUA.Win32.RManSys.AA
59d825f5965b4cfecdc67f6afec973d41b5fb2ee3f2c2fe5575b5cca4eddbf1d	Trojan.BAT.STARTER.TIAOOAAP
ea9a0f4ec69452e85dad7d18396d5471e8edc4109e5ce2e4602a6fa097c466f2	Trojan.BAT.STARTER.TIAOOAAQ
a5f35a93fbf95308cef5131ba208810e12585f2e4dd15c88630b3adfafa8dc32	Trojan.HTML.FLAWEDAMMYY.A

1b388a55b353cf90bc00febe00ae4e1f266eb226283c3bdaec8d68f3998b52fa	Trojan.HTML.FLAWEDAMMYY.C
24bc7e6dee566098d17bdae0e3ce6df2c60ca76fae76abbe3d63ab1d1e54e0dc	Trojan.HTML.FLAWEDAMMYY.C
1fb8f6448df0ce9f9536dbc6a1d2036bae49b05bafbc56c64dc0fd80700ca063	Trojan.HTML.FLAWEDAMMYY.C
3de9ccaeafd0089e6c32523f8cf7139655444ec0c9ce1a7f1238219ddfa9557c	Trojan.HTML.FLAWEDAMMYY.C
450a09fa7a12ba5657911f3c1028abbcbc1fd47177305dab3ef29f24e2f93bf6	Trojan.HTML.FLAWEDAMMYY.C
5ff54cc46c23ba26b41cb1823799c6f2d6fea8a8b617cdd448b5a9d6b9f908ba	Trojan.HTML.FLAWEDAMMYY.C
84fbcd3639d632906f4d3d3424420da6671101d373a6da9f01113c90db0b1ca5	Trojan.HTML.FLAWEDAMMYY.C
1920a8e211c6e24833d589e6d7efad49939e739f2bbf8ce9cb4545be42a68a10	Trojan.HTML.FLAWEDAMMYY.C
f9f9f584e7a2b168ec2ef04454bd26e454c4ebff9bf1d460f852553c98a5d1f2	Trojan.HTML.FLAWEDAMMYY.C
2f1d905a265a5c0c5f106f23e6f03cf1c90750a8e72f7073c6bac7bf31a91408	Trojan.HTML.FLAWEDAMMYY.C
d3388f28952da55e94e93be6e045342410e93f4ed78218104d1128238cbfd632	Trojan.HTML.FLAWEDAMMYY.C
2cff860b685244cd1a1d6869d73b093ebfb5b5d1b35a8fe4a6083b5ecdf57ff2	Trojan.HTML.FLAWEDAMMYY.C
cab8d1102680c3c3d5b8b292a939043b7f3c1a0d186f2b984a17a7811ce4b760	Trojan.HTML.FLAWEDAMMYY.C
76bf02986d7ddba3ed148e366834b0c6a0fbef98623fefbed3c46f9fe56559c1	Trojan.HTML.FLAWEDAMMYY.C
4b6f43c8793ae495bca15a32fe56527bc771b3c0df0e9c78f780d8f3e91f13c7	Trojan.HTML.FLAWEDAMMYY.C
eab7dd64511ceb8ed7b4b5ec19ef0c2f60d4c9865f81b7525d1cd34d3c20940a	Trojan.HTML.FLAWEDAMMYY.D
cf31eba83fd2a0090a77d348e611ae0674f9dea48c307977a5af4e487c184217	Trojan.HTML.FLAWEDAMMYY.D

73ce6aeebcf448edad10e676b9c4bf3f7f1d57eab3e5e52c75102ed889744dda	Trojan.HTML.FLAWEDAMMYY.D
7326adda68bb55bea76d3d088e5d5279df9e4da732ba1049880b2661e92ea297	Trojan.HTML.FLAWEDAMMYY.D
85ef20c4e3a3122debf9c3a2898452b5d88af3b1dd995e9bce88ce17f8c934cc	Trojan.HTML.FLAWEDAMMYY.D
080715e7ddabc2f8bceaa1a5c6e64609e1e1b679adb2a7852a862a5683dba899	Trojan.HTML.FLAWEDAMMYY.D
8addd86846c2cadba3285ea9916b264e17a6b14a85bb14e7af74c26d7c55092e	Trojan.W97M.DEDEX.F
55b7642b852989a8f297b249ac7decfcd5570e86ca3eb06449abdbf70ca20208	Trojan.W97M.DEDEX.F
e023484127089d609bad7be875d5cdf1111a7c4c92acbff8b1d0e5dfad803d08	Trojan.W97M.DEDEX.F
8639a2981e880c6e3eb9db9be149b26d56c550b9eaea5593a6dce63feb07636b	Trojan.W97M.DEDEX.F
eb2b7103f20d75306c534cce183fb4aa359e371d2cb9bf09dfc75b4bb164a362	Trojan.W97M.DEDEX.F
38ba4b8c499f04750da95e195614e3bbc9152270739a80fc5f33d143ec62b84c	Trojan.W97M.DEDEX.F
ec6097c4fdbe0736e416b58be0a4dd042c46a9cf7eef997b3eb72384609cbca9	Trojan.Win32.AMADEY.A
6389e82e1674e56d006c2c58e36641db661c35eba3a7a418e5577c71497459dc	Trojan.Win32.FLAWEDAMMY.AB
4777235644a753cd6f0cfdf20d003d2a46be75bf0a1c8bdc3b7e3aef7713b002	Trojan.Win32.FLAWEDAMMY.AB
7edc56dd709d0af1c2f54cda7d8808c1748fa3370aa9319945dca85943d46710	Trojan.Win32.NECURS.USWE
f4cd8c0da6b2da44c43ec5c9a35155f0b47a2636954cb0329c8c14d66f4ecd5e	Trojan.Win32.RABASED.A
cc81dd1eba5b887d09b0eecb8443916dea82dc58e1cf847f1653413fb804210c	Trojan.Win32.STARTER.TIIBHAO
f485eefaa8022eaed3f55a9eac4edfdebdae4a6a2f7658f40d5c5f7bde5f9604	Trojan.X97M.DEDEX.AFJV

81122d5e5c58b260fb5c9ccda6eed02c798698dca583cffabe307af6492f0bc4	Trojan.X97M.DEDEX.AFJV
506459056f4129de2990735fd20c627f06c55ce6fd911d0edc090a72ab6b2ca6	Trojan.X97M.DEDEX.AFJV
a56efcd89af7d93655160ea8720082e635f4b2c073cb4c1517e2f21733035938	Trojan.X97M.DEDEX.AFJV
eebdc75696b9bc1e32067b49c20403a374dd127d8e3f968a6d837a0ab9867dc6	Trojan.X97M.DEDEX.AFJW
5fea84068cb70b5ef6d7fdfc0c9e6424ce88aa1b14103aa89ef506e956551d4f	Trojan.X97M.DEDEX.AFJW
9ec25cfed79d1193f3d65e1669fe291856cd6d51f6da2cf2888af9aa983a9280	Trojan.X97M.FLAWEDAMMY.AB
080f4870f8ca4f50d1be57d8c529b7a2a3df52790171c2464674bc134b58a9e6	Trojan.X97M.FLAWEDAMMY.AB
70d46db11c64062ff93111137c530d180668685d1a19997365156876723ed7ee	Trojan.X97M.FLAWEDAMMY.AB
443d45c29f035af7dbe086068eda6b22b85ad862a74bc7e0e02ba65f63e9d912	Trojan.X97M.FLAWEDAMMY.AB
a46dae2f891fef5744b110751f0037a8db04a15d183d05a11c31c79de9c4e6dc	Trojan.X97M.FLAWEDAMMY.AB
be3e8f4518163790fa9dccafd510ed752617b28dfe0a8833ec38b493d6630dc2	Trojan.X97M.FLAWEDAMMY.AB
5c5c457c7debe90dc57beb33deadb973fea6e400990fd11899dd003b10e4d54e	Trojan.X97M.FLAWEDAMMY.AB
4da4d6917d07d7eb9021ffb8de669720c9f51a86b9fbb5ce99ebe2afd1441cf5	Trojan.X97M.FLAWEDAMMY.AC
d5347f95512be99c463877af379c9a7ceff4166bab4567f79a0fbe043af072f2	Trojan.X97M.FLAWEDAMMY.AC
fb51e4be53d9cee67b7001f4b7f0f84b23f42e809f44c5b679a2bc5f31e3f80d	Trojan.X97M.FLAWEDAMMY.AC
15811bd40a1a8b80c16db43a03d129835b386aef791c487208b31117da952d98	Trojan.X97M.FLAWEDAMMY.AC
8658d105354b4cabe349788894fb56ba6fa375632d450df8e21b82e85f0f0d3e	Trojan.X97M.FLAWEDAMMY.AC

a0cce7cb98e88da35b219fc071cce889921e88d4042fa706eb8a84b96891a238	Trojan.X97M.FLAWEDAMMYY.A
f0a934abc38094c052662ccb878693633c012f59b611b3b653ba76c717899e51	Trojan.X97M.FLAWEDAMMYY.A
6837b198cfd6f30df59ce07c5f7267b59f0d1bef0163b4ab0136d9888dd35988	Trojan.X97M.FLAWEDAMMYY.A
714a4f83585ed7da31211e697d0ff6056215420248b783165848b46de222edbb	Trojan.X97M.FLAWEDAMMYY.A
c146486576db4515b181b8754a2788edf0d5b4a2733f7c18dd5ce3d34433c125	Trojan.X97M.FLAWEDAMMYY.A
bbcaa05900f9180fa5eb9291fd01cefb5370804beedac605cba07996948b5ad3	Trojan.X97M.FLAWEDAMMYY.A
ea367af7f8f23bc6a8c16eaf184bf7ab36c37de8e1d39fb44b66e64f9c0f2401	Trojan.X97M.FLAWEDAMMYY.B
55a4f8d7a7c019c256d3d0eb92772b45dbc11f34f497e423279114503a38ac21	Trojan.X97M.POWLOAD.NSFGAIEH
3e434ba1fbb43191917fa8ebbb2537d6e005cf68a78d9dbbc0da2a73619e8057	Trojan.XF.DEDEX.F
74ed4411cfd7b4679a7d77af0e5899ab0a88a1a5c806453da3ad4ff6cf41b689	Trojan.XF.DEDEX.G
5ee78d7fede5af18b7040d3f8403f6fd16b49867ef832c803be0f1542d56e5c8	Trojan.XF.DEDEX.H
07150d594e393f44f318d6cdc4128ffcfcfad78a2afc1726400b5cee61777518	Trojan.XF.DEDEX.I
bbaa46c930ae342cc50925ce71ad8b29230141c3cda617a5b411f529c00746ee	Trojan.XF.DEDEX.J
e30862c6a935955bf58907f698dc3b42bdfc14390e48e899adee8fb4281535d5	Trojan.XF.DEDEX.K
9a8946578f9f66bd1dd468abb6d777f3efb998a15810360ec0ef798d446efc56	Trojan.XF.DEDEX.K
502b64555b0e1fe72c78c0979993d2418c8494a828ab327959b58b744a4b7774	Trojan.XF.DEDEX.K
a913e031787fad730358523c0eebd2f0d6ed24b12ced3664857af1aa9103f910	Trojan.XF.DEDEX.K

fb3c0a4449b1d97aa759c2d47bfbe6d82c0466c6b5bf58a5bd8637314bc2a871	Trojan.XF.DEDEX.K
214999b07cd3293c329c63a4c1ca88fab182a090942a7a31883860b588502c39	Trojan.XF.DEDEX.K
e82db6a27d20f09e3023fe4d2d4a5f1ba0c2cde7e88bcfb158244919e805e0ed	Trojan.XF.DEDEX.K
559210d28dcbff8517f3bdddc8e298d188d543785adc9fdf96ced005a29b72ba	Trojan.XF.DEDEX.K
f7a615eb750b37c381b3d8a563a2d2a810659094e2548fdba95ced82fa390707	Trojan.XF.DEDEX.K
2774105b340fb22a59c23a8c843ec229ac1e478c91f31ff37dac5bcb8cfc5b6f	Trojan.XF.DEDEX.K
dd2b4e71cda845cdbef1b05a840b19acd23aadacf1d401551d1dc6e7c2a982bb	Trojan.XF.DEDEX.K
a84dac2e91d85fe5081209813b576b6ab067629f4ed125c825afb7c7f012f639	Trojan.XF.DEDEX.K
da866de4a50f546bf90eb7b413477e282d3b3d69d72ee777c00befff0651fafa	Trojan.XF.DEDEX.K
f1ba97f80aa1b424db809d7271ae50a3378302fc29d5849ac786ab4aa43f4a08	Trojan.XF.DEDEX.K
8870d88040d227887e616fc48d59caf920c238dcdedc0e9c3b6669a7337ae819	Trojan.XF.DEDEX.K
d87b7af7958b2c0b69ab1280add7b0493e33c7652ec5084d7a45659cf0037f8f	Trojan.XF.DEDEX.K
0832b77f91fe8eebe80e29780c0a34444d4e19edf60e710069c3a4fb7d07c290	Trojan.XF.DEDEX.K
0808c07168acd57e1927f2d8aa8aa6f46415503462f71a8c3308f5cfec1eeead	Trojan.XF.DEDEX.K
337a4048a92fd86f7122a9b3fce3f54e74932e6e82aec819124d831f84d7c481	Trojan.XF.DEDEX.SMNH3
5b2aada3f4d3b5f4d007bae0eb5a36398921183f977be2e3820f09eda58cfbf5	Trojan.XF.DEDEX.SMNH3
b3b28087fa0163ed1194fa51bce2565ed9b3be6f370167442e2734d0ec4fbce1	Trojan.XF.DEDEX.SMNH3

b069ce6b1de9040473b57ca67650b49355d4c31ee7fd5d96ed243ea1e88936d5	Trojan.XF.DEDEX.SMNH3
aaa8c954fdc03e1d7658a8ad7f1cda39474614a1c6187642d7f904da2623cdc7	Trojan.XF.DEDEX.SMNH3
7220b264a52dc98a207210155e55e1993b0c96914e635b643805821461d8aa1a	Trojan.XF.DEDEX.SMNH3
5516e1eca41f22d3330a64543e66b73885593bf47db09bc1fcfb4f50e7719b7f	Trojan.XF.DEDEX.SMNH3

Related malicious URLs:

159.69.48.50:5655

169.239.129.103:8080

94.156.133.183:8080

hxxp://103[.]73[.]66[.]137/01[.]dat

hxxp://109[.]234[.]38[.]177/dom4

hxxp://116[.]203[.]180[.]29/01[.]dat

hxxp://158[.]255[.]208[.]175/da2.dat

hxxp://160[.]202[.]162[.]147/1[.]tmp

hxxp://163[.]172[.]84[.]54/filename[.]php

hxxp://167[.]179[.]119[.]235/02[.]dat

hxxp://169[.]239[.]128[.]168/dynhost

hxxp://169[.]239[.]128[.]169/dynhost

hxxp://172[.]104[.]104[.]166/01[.]dat

hxxp://172[.]104[.]104[.]166/m1

hxxp://172[.]104[.]104[.]166/m2

hxxp://172[.]104[.]117[.]15/02[.]dat

hxxp://195[.]123[.]227[.]20/dashost

hxxp://27[.]102[.]118[.]143/dom1

hxxp://45[.]76[.]206[.]149/01[.]dat

hxxp://45[.]76[.]223[.]177/02[.]dat

hxxp://45[.]77[.]16[.]211/01[.]dat

hxxp://5[.]149[.]254[.]25/1[.]tmp

hxxp://66[.]42[.]45[.]55/02[.]dat

hxxp://66[.]42[.]45[.]55/m3

hxxp://66[.]42[.]45[.]55/m4

hxxp://92[.]38[.]135[.]134/dom2

hxxp://92[.]38[.]135[.]88/da[.]dat

hxxp://amenyan[.]zouri[.]jp/20190706_866384[.]xls

hxxp://angelmariotti[.]xyz/xsmkld/index[.]php

hxxp://billyjimmyer[.]top/xsmkld/index[.]php

hxxp://canyoning-austria[.]at/dashost

hxxp://citroenmehari[.]dk/20190706_066381[.]xls

hxxp://dannysannyer[.]top/xsmkld/index[.]php

hxxp://datdepot[.]net/nzt1

hxxp://fjiisiis33[.]icu/jquery/jquery[.]php

hxxp://furhatsth[.]net/q1

hxxp://furhatsth[.]net/q2

hxxp://globe-trotterltd[.]com/dashost

hxxp://gohaiendo[.]com/ppk/index[.]php

hxxp://govhotel[.]us/p[.]exe

hxxp://homeone[.]co[.]kr/eTaxInvoice_476543853[.]xls

hxxp://houusha33[.]icu/jquery/jquery[.]php

hxxp://ianhennessee[.]com/eTaxInvoice_776347534[.]xls

hxxp://kabatas[.]ch/~erhan/eTaxInvoice_467523[.]xls

hxxp://kupitorta[.]net/lsadat1

hxxp://kupitorta[.]net/lsadat2

hxxp://kupitorta[.]net/lsadat3

hxxp://lecmess[.]top/tmp

hxxp://losabetos[.]com[.]sv/eTaxInvoice_8466345[.]xls

hxxp://profan[.]es/dashost

hxxp://slemend[.]com/cykom1

hxxp://slemend[.]com/cykom2

hxxp://statesdr[.]top/q3

hxxp://statesdr[.]top/q4

hxxp://tommyhalfigero[.]top/xsmkld/index[.]php

hxxp://topdalescotty[.]top/xsmkld/index[.]php

hxxp://traveser[.]net/tmp

hxxp://tunnelview[.]co[.]uk/ES_2[.]exe

hxxp://vairina[.]top/20190706_089785[.]xls

hxxp://vairina[.]top/20190706_125803[.]xls

hxxp://vairina[.]top/t1

hxxp://vairina[.]top/t2

hxxp://velquene[.]net/mshost1

hxxp://velquene[.]net/mshost2

hxxp://waiireme[.]com/20190706_077345[.]xls

hxxp://waiireme[.]com/20190706_983782[.]xls

hxxp://waiireme[.]com/t3

hxxp://waiireme[.]com/t4

hxxp://www.kerrison[.]com/dashost

hxxp://zonaykan[.]com/lsadat1

hxxp://zonaykan[.]com/lsadat2

hxxp://zonaykan[.]com/lsadat3

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