Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser | Mandiant

By Mandiant

Published: 2020-10-28 · Archived: 2026-04-05 13:04:10 UTC

First Seen	Server	Subject	MD5
12/12/19	140.82.60.155:443	CN=updatemanagir[.]us	ec16be328c09473d5e5c0
12/21/19	96.30.192.141:443	CN=cmdupdatewin[.]com	3d4de17df25412bb714fd
1/6/20	45.76.49.78:443	CN=scrservallinst[.]info	cd6035bd51a44b597c1e1
1/8/20	149.248.58.11:443	CN=updatewinlsass[.]com	8c581979bd11138ffa3a25
1/9/20	96.30.193.57:443	CN=winsystemupdate[.]com	e4e732502b9658ea33808
1/14/20	95.179.219.169:443	CN=jomamba[.]best	80b7001e5a6e4bd6ec795
1/16/20	140.82.27.146:443	CN=winsysteminfo[.]com	29e656ba9d5d38a0c17a4
1/19/20	45.32.170.9:443	CN=livecheckpointsrs[.]com	1de9e9aa8363751c8a71c
1/20/20	207.148.8.61:443	CN=ciscocheckapi[.]com	97ca76ee9f02cfda2e8e97
1/28/20	209.222.108.106:443	CN=timesshifts[.]com	2bb464585f42180bddccb
1/29/20	31.7.59.141:443	CN=updatewinsoftr[.]com	07f9f766163c344b0522e
1/29/20	79.124.60.117:443	C=US	9722acc9740d831317dd8
1/29/20	66.42.86.61:443	CN=lsassupdate[.]com	3c9b3f1e12473a0fd28dc3
1/29/20	45.76.20.140:443	CN=cylenceprotect[.]com	da6ce63f4a52244c3dced3
1/29/20	45.76.20.140:80	CN=cylenceprotect[.]com	da6ce63f4a52244c3dced3

1/30/20	149.248.5.240:443	CN=sophosdefence[.]com	e9b4b649c97cdd895d6a0
1/30/20	144.202.12.197:80	CN=windefenceinfo[.]com	c6c63024b18f0c5828bd3
1/30/20	149.248.5.240:80	CN=sophosdefence[.]com	e9b4b649c97cdd895d6a0
1/30/20	149.28.246.25:80	CN=lsasswininfo[.]com	f9af8b7ddd4875224c7ce
1/30/20	144.202.12.197:443	CN=windefenceinfo[.]com	c6c63024b18f0c5828bd3
1/30/20	149.28.246.25:443	CN=lsasswininfo[.]com	f9af8b7ddd4875224c7ce
1/30/20	45.77.119.212:443	CN=taskshedulewin[.]com	e1dc7cecd3cb225b131bdl
1/30/20	45.77.119.212:80	CN=taskshedulewin[.]com	e1dc7cecd3cb225b131bdl
1/30/20	149.28.122.130:443	CN=renovatesystem[.]com	734c26d93201cf0c91813
1/30/20	45.32.170.9:80	CN=livecheckpointsrs[.]com	1de9e9aa8363751c8a71c
1/30/20	149.248.58.11:80	CN=updatewinlsass[.]com	8c581979bd11138ffa3a25
1/30/20	149.28.122.130:80	CN=renovatesystem[.]com	734c26d93201cf0c91813
1/30/20	207.148.8.61:80	CN=ciscocheckapi[.]com	97ca76ee9f02cfda2e8e97
1/31/20	81.17.25.210:443	CN=update-wind[.]com	877bf6c685b68e6ddf23a4
1/31/20	31.7.59.141:80	CN=updatewinsoftr[.]com	07f9f766163c344b0522e4
2/2/20	155.138.214.247:80	CN=cleardefencewin[.]com	61df4864dc2970de6dcee6
2/2/20	155.138.214.247:443	CN=cleardefencewin[.]com	61df4864dc2970de6dcee6
2/2/20	45.76.231.195:443	CN=checkwinupdate[.]com	d8e5dddeec1a9b366759c
2/2/20	45.76.231.195:80	CN=checkwinupdate[.]com	d8e5dddeec1a9b366759c
2/3/20	46.19.142.154:443	CN=havesetup[.]net	cd354c309f3229aff59751

2/3/20	95.179.219.169:80	CN=jomamba[.]best	80b7001e5a6e4bd6ec795
2/3/20	140.82.60.155:80	CN=updatemanagir[.]us	ec16be328c09473d5e5c0
2/3/20	209.222.108.106:80	CN=timesshifts[.]com	2bb464585f42180bddccb
2/3/20	66.42.118.123:443	CN=conhostservice[.]com	6c21d3c5f6e8601e92ae1
2/4/20	80.240.18.106:443	CN=microsoftupdateswin[.]com	27cae092ad6fca89cd1b05
2/4/20	95.179.215.228:443	CN=iexploreservice[.]com	26010bebe046b3a33bacd
2/12/20	155.138.216.133:443	CN=defenswin[.]com	e5005ae0771fcc165772a1
2/12/20	45.32.130.5:443	CN=avrenew[.]com	f32ee1bb35102e5d98af81
2/14/20	45.76.167.35:443	CN=freeallsafe[.]com	85f743a071a1d0b74d8e8
2/14/20	45.63.95.187:443	CN=easytus[.]com	17de38c58e04242ee56a9
2/17/20	45.77.89.31:443	CN=besttus[.]com	2bda8217bdb05642c9954
2/17/20	95.179.147.215:443	CN=windefens[.]com	57725c8db6b98a3361e0d
2/17/20	155.138.216.133:443	CN=defenswin[.]com	c07774a256fc19036f5c8c
2/17/20	104.238.190.126:443	CN=aaatus[.]com	4039af00ce7a5287a3e564
2/17/20	144.202.83.4:443	CN=greattus[.]com	7f0fa9a608090634b42f5f
2/17/20	104.156.245.0:443	CN=comssite[.]com	f5bb98fafe428be6a8765e
2/17/20	45.32.30.162:443	CN=bigtus[.]com	698fc23ae111381183d0b9
2/17/20	108.61.242.184:443	CN=livetus[.]com	8bedba70f882c45f968c2d
2/17/20	207.148.15.31:443	CN=findtus[.]com	15f07ca2f533f0954bbbc8
2/17/20	149.28.15.247:443	CN=firsttus[.]com	88e8551f4364fc647dbf00

2/21/20	155.138.136.182:443	CN=worldtus[.]com	b31f38b2ccbbebf4018fe5
2/25/20	45.77.58.172:443	CN=freeoldsafe[.]com	a46e77b92e1cdfec82239f
2/25/20	45.77.58.172:443	CN=freeoldsafe[.]com	a46e77b92e1cdfec82239f
2/26/20	108.61.72.29:443	CN=myserviceconnect[.]net	9f551008f6dcaf8e6fe363c
2/27/20	216.155.157.249:443	CN=myserviceupdater[.]com	4c6a2c06f1e1d15d6be8c8
2/28/20	45.77.98.157:443	CN=topservicesbooster[.]com	ba4b34962390893852e5c
2/28/20	104.156.250.132:443	CN=myservicebooster[.]com	89be5670d19608b2c8e26
2/28/20	149.28.50.31:443	CN=topsecurityservice[.]net	77e2878842ab26beaa3ff2
2/28/20	149.28.55.197:443	CN=myyserviceupdater[.]com	0dd8fde668ff8a301390ee
2/28/20	207.246.67.70:443	CN=servicesecurity[.]org	c88098f9a92d7256425f78
2/28/20	63.209.33.131:443	CN=serviceupdates[.]net	16e86a9be2bdf0ddc896bc
2/29/20	45.77.206.105:443	CN=myservicebooster[.]net	6e09bb541b29be7b89427
2/29/20	140.82.5.67:443	CN=servicesbooster[.]org	42d2d09d08f60782dc4cd
2/29/20	108.61.209.123:443	CN=brainschampions[.]com	241ab042cdcb29df0a5c4f
2/29/20	104.156.227.250:443	CN=servicesbooster[.]com	f45f9296ff2a6489a4f39cd
2/29/20	140.82.10.222:443	CN=topservicesecurity[.]net	b9375e7df4ee0f83d7abb1
2/29/20	149.28.35.35:443	CN=topservicesecurity[.]org	82bd8a2b743c7cc3f3820e
2/29/20	207.148.21.17:443	CN=topserviceupdater[.]com	ece184f8a1309b781f912d
2/29/20	45.77.153.72:443	CN=topservicesupdate[.]com	8330c3fa8ca31a76dc8d78
3/1/20	140.82.10.222:80	CN=topservicesecurity[.]net	b9375e7df4ee0f83d7abb1

3/1/20	207.148.21.17:80	CN=topserviceupdater[.]com	ece184f8a1309b781f912d
3/1/20	108.61.90.90:443	CN=topservicesecurity[.]com	696aeb86d085e4f6032e0a
3/1/20	45.32.130.5:80	CN=avrenew[.]com	f32ee1bb35102e5d98af81
3/2/20	217.69.15.175:443	CN=serviceshelpers[.]com	9a437489c9b2c19c304d9
3/2/20	155.138.135.182:443	CN=topservicesupdates[.]com	b9deff0804244b52b1457(
3/2/20	95.179.210.8:80	CN=serviceuphelper[.]com	bb65efcead5b979baee5a2
3/2/20	45.76.45.162:443	CN=boostsecuritys[.]com	7d316c63bdc4e981344e8
3/4/20	108.61.176.237:443	CN=yoursuperservice[.]com	7424aaede2f35259cf040f
3/4/20	207.246.67.70:443	CN=servicesecurity[.]org	d66cb5528d2610b39bc3c
3/6/20	188.166.52.176:443	CN=top-servicebooster[.]com	f882c11b294a94494f75de
3/7/20	149.248.56.113:443	CN=topservicehelper[.]com	2a29e359126ec5b746b1c
3/8/20	199.247.13.144:443	CN=hakunamatatata[.]com	e2cd3c7e2900e2764da64a
3/8/20	95.179.210.8:443	CN=serviceuphelper[.]com	bb65efcead5b979baee5a2
3/8/20	207.246.67.70:443	CN=servicesecurity[.]org	d89f6bdc59ed5a1ab3c1ec
3/9/20	194.26.29.230:443	CN=secondserviceupdater[.]com	c30a4809c9a77cfc09314a
3/9/20	194.26.29.229:443	CN=firstserviceupdater[.]com	bc86a3087f238014b6c3a(
3/9/20	194.26.29.232:443	CN=fourthserviceupdater[.]com	3dc6d12c56cc79b0e3e8c(
3/9/20	194.26.29.234:443	CN=sixthserviceupdater[.]com	951e29ee8152c1e7f63e8c
3/9/20	194.26.29.235:443	CN=seventhserviceupdater[.]com	abe1ce0f83459a7fe9c728
3/9/20	194.26.29.236:443	CN=eighthserviceupdater[.]com	c7a539cffdd230a4ac9a47

3/9/20	194.26.29.237:443	CN=ninethserviceupdater[.]com	1d1f7bf2c0eec7a3a0221f
3/9/20	194.26.29.225:443	CN=seventeenthservicehelper[.]com	6b1e0621f4d891b8575a2
3/9/20	194.26.29.227:443	CN=nineteenthservicehelper[.]com	38756ffb8f2962f6071e77
3/9/20	194.26.29.242:443	CN=thirdservicehelper[.]com	3b911032d08ff4cb156c06
3/9/20	194.26.29.244:443	CN=tenthservicehelper[.]com	a2d9b382fe32b01391972
3/9/20	194.26.29.226:443	CN=eighteenthservicehelper[.]com	4acbca8efccafd92da9006
3/9/20	194.26.29.243:443	CN=ninthservicehelper[.]com	0760ab4a6ed9a124aabb8
3/9/20	194.26.29.201:443	CN=secondservicehelper[.]com	d8a8d0ad9226e3c968c58
3/9/20	194.26.29.202:443	CN=thirdservicehelper[.]com	0d3b79158ceee5b6ce859
3/9/20	194.26.29.220:443	CN=fourservicehelper[.]com	831e0445ea580091275b7
3/11/20	207.246.67.70:80	CN=servicesecurity[.]org	d89f6bdc59ed5a1ab3c1ec
3/13/20	165.227.196.0:443	CN=twentiethservicehelper[.]com	977b4abc6307a9b373222
3/14/20	45.141.86.91:443	CN=thirdservice-developer[.]com	edc2680e3797e11e93573
3/14/20	194.26.29.219:443	CN=firstservisehelper[.]com	6b444a2cd3e12d4c3feade
3/14/20	45.141.86.93:443	CN=fifthservice-developer[.]com	60e7500c809f12fe6be568
3/15/20	45.141.86.90:443	CN=secondservice-developer[.]com	de9460bd6b1badb7d8314
3/15/20	45.141.86.84:443	CN=firstservice-developer[.]com	6385acd425e68e1d3fce38
3/17/20	45.141.86.96:443	CN=eithtservice-developer[.]com	e1d1fb4a6f09fb54e09fb2
3/17/20	45.141.86.92:443	CN=fourthservice-developer[.]com	5b5375bf30aedfa3a44d75
3/18/20	45.141.86.94:443	CN=sixthservice-developer[.]com	4d42bea1bfc7f1499e469e

3/18/20	108.61.209.121:443	CN=service-booster[.]com	692ed54fb1fb189c36d2f1
3/18/20	134.122.116.114:443	CN=service-helpes[.]com	ad0914f72f1716d810e7bc
3/18/20	209.97.130.197:443	CN=helpforyourservice[.]com	00fe3cc532f876c7505ddb
3/18/20	192.241.143.121:443	CN=serviceshelps[.]com	e50998208071b4e5a7011
3/18/20	45.141.86.95:443	CN=seventhservice-developer[.]com	413ca4fa49c3eb6eef0a6cl
3/18/20	198.211.116.199:443	CN=actionshunter[.]com	8e5bedbe832d374b56585
3/18/20	45.141.86.155:443	CN=sexyservicee[.]com	cca37e58b23de9a1db9c38
3/19/20	194.26.29.239:443	CN=eleventhserviceupdater[.]com	7e0fcb78055f0eb12bc841
3/19/20	45.141.86.206:443	CN=servicedhunter[.]com	fdefb427dcf3f0257ddc534
3/19/20	45.141.86.92:443	CN=service-updateer[.]com	51ba9c03eac37751fe06b7
3/19/20	134.122.116.59:443	CN=servicedbooster[.]com	db7797a20a5a491fb7ad0c
3/19/20	134.122.118.46:443	CN=servicedpower[.]com	7b57879bded28d0447eea
3/19/20	134.122.124.26:443	CN=serviceboostnumberone[.]com	880982d4781a1917649ce
3/20/20	45.141.86.97:443	CN=ninethservice-developer[.]com	e4a720edfcc7467741c582
3/20/20	178.62.247.205:443	CN=top-serviceupdater[.]com	a45522bd0a26e07ed1878
3/20/20	159.203.36.61:443	CN=yourserviceupdater[.]com	7b422c90dc85ce261c0a65
3/20/20	134.122.20.117:443	CN=fifthserviceupdater[.]com	99aa16d7fc34cdcc7dfceal
3/23/20	165.22.125.178:443	CN=servicemonsterr[.]com	82abfd5b55e14441997d47
3/24/20	69.55.60.140:443	CN=boostyourservice[.]com	7f3787bf42f11da321461e
3/24/20	45.141.86.98:443	CN=tenthservice-developer[.]com	eef29bcbcba1ce089a50ae

3/26/20	178.79.132.82:443	CN=developmasters[.]com	5cf480eba910a625e5e52e
3/26/20	194.26.29.247:443	CN=thirteenthservicehelper[.]com	2486df3869c16c0d9c23a8
5/4/20	159.65.216.127:443	CN=info-develop[.]com	5f7a5fb72c6689934cc5d9
9/22/20	69.61.38.155:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gtrsqer[.]com	d37ba4a4b1885e96ff54d1
9/22/20	96.9.225.144:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=hakunaman[.]com	4408ba9d63917446b31a0
9/22/20	96.9.209.216:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=caonimas[.]com	d921dd1ba03aaf37d5011(
9/22/20	107.173.58.176:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=chalengges[.]com	dfeb6959b62aff0b93ca20
9/22/20	96.9.225.143:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=reginds[.]com	05c03b62dea6ec06006e57
9/22/20	69.61.38.156:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=errvghu[.]com	c14a892f8203a04c7e3298
9/22/20	45.34.6.229:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=harddagger[.]com	7ed16732ec21fb3ec16dbb
9/22/20	45.34.6.226:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=getinformationss[.]com	1788068aff203fa9c51d85
9/22/20	45.34.6.225:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gameleaderr[.]com	0fff2f721ad23648175d08
9/22/20	107.173.58.185:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=razorses[.]com	b960355ba112136f93798
9/22/20	107.173.58.183:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nomadfunclub[.]com	a3d4e6d1f361d9c335effd
9/22/20	107.173.58.175:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bouths[.]com	e13fbdff954f652f14faf11
9/22/20	185.184.223.194:443	C=US,ST=CA,L=Texas,O=lol,OU=,CN=regbed[.]com	67310b30bada4f77f8f336
9/22/20	109.70.236.134:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=vnuret[.]com	ae74cbb9838688363b792
9/23/20	64.44.131.103:443	C=US,ST=TX,L=Texas,O=serviceswork,OU=,CN=serviceswork[.]net	af518cc031807f43d646dc
9/23/20	69.61.38.157:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=moonshardd[.]com	c8fd81d6d3c8cbb8256c47
9/23/20	193.142.58.129:443	C=US,ST=TX,L=Texas,O=zapored,OU=,CN=zapored[.]com	5a22c3c8a0ed6482cad0e2

9/23/20	45.34.6.223:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=hurrypotter[.]com	bf598ba46f47919c264514
9/23/20	107.173.58.179:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=biliyilish[.]com	1c8243e2787421373efcf9
9/23/20	45.34.6.222:443	C=US,ST=TX,L=Texas,O=dagger,OU=,CN=daggerclip[.]com	576d65a68900b270155c2
9/23/20	107.173.58.180:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=blackhoall[.]com	69643e9b1528efc6ec9037
9/23/20	107.173.58.182:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=checkhunterr[.]com	ca9b7e2fcfd35f19917184
9/23/20	45.34.6.221:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=check4list[.]com	e5e0f017b00af6f020a28b
9/24/20	213.252.244.62:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=ayiyas[.]com	8367a1407ae999644f25f6
9/24/20	185.25.50.167:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=chainnss[.]com	34a78f1233e53010d29f2a
9/30/20	88.119.171.75:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=martahzz[.]com	eaebbe5a3e3ea1d5992a4d
10/1/20	88.119.171.74:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=jonsonsbabyy[.]com	adc8cd1285b7ae6204547
10/1/20	88.119.171.55:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=tiancaii[.]com	bfe1fd16cd4169076f3fba
10/1/20	88.119.171.67:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=cantliee[.]com	c8a623eb355d172fc3e083
10/1/20	88.119.171.76:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=realgamess[.]com	0ac5659596008e64d4d0d
10/1/20	88.119.171.68:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=maybebaybe[.]com	48003b6b638dc7e79e75a
10/1/20	88.119.171.69:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=saynoforbubble[.]com	5c75a6bbb7454a04b9ea2
10/1/20	88.119.171.73:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=chekingking[.]com	e391c997b757424d8b239
10/1/20	88.119.171.77:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=wondergodst[.]com	035697cac0ee92bb4d743
10/1/20	88.119.171.78:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=zetrexx[.]com	fc133bed713608f78f9f11
10/1/20	213.252.244.38:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=mountasd[.]com	8ead6021e2a5b9191577c
10/1/20	107.173.58.184:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=pudgeee[.]com	1c9949d20441df2df09d13

10/1/20	88.119.174.109:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=loockfinderrs[.]com	c0ddfc954aa007885b467f
10/1/20	88.119.174.110:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=puckhunterrr[.]com	ee63098506cb82fc71a4e8
10/1/20	88.119.174.114:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=voiddas[.]com	422b020be24b346da8261
10/1/20	88.119.174.116:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sibalsakie[.]com	8d8f046e963bcd008fe4bb
10/1/20	88.119.174.117:443	C=US,ST=TX,L=TExas,O=lol,OU=,CN=rapirasa[.]com	c381fb63e9cb6b0fc59dfa
10/1/20	88.119.174.118:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=raidbossa[.]com	add6b742d0f992d56bede7
10/1/20	88.119.174.119:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=lindasak[.]com	9bbd073033e34bfd80f658
10/1/20	88.119.174.121:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bithunterr[.]com	9afef617897e7089f59c19
10/1/20	88.119.174.120:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=giveasees[.]com	3f366e5f804515ff982c15
10/1/20	88.119.174.107:443	C=US,ST=TX,L=Texas,O=office,OU=,CN=shabihere[.]com	c2f99054e0b42363be915
10/1/20	88.119.174.125:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=tarhungangster[.]com	4ac8ac12f1763277e35da0
10/1/20	88.119.174.126:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=imagodd[.]com	7080547306dceb90d809c
10/1/20	88.119.174.127:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=raaidboss[.]com	03037dff61500d52a37efd
10/1/20	88.119.174.128:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sunofgodd[.]com	959bed7a2662d7274b303
10/1/20	213.252.244.126:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=hungrrybaby[.]com	1d28556cc80df9627c203
10/1/20	213.252.244.170:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=loxliver[.]com	85e65803443046f921b9a0
10/1/20	213.252.246.154:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicegungster[.]com	9df6ba82461aa0594ead03
10/5/20	5.2.64.113:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=qascker[.]com	18aadee1b82482c3cd5ebe
10/7/20	5.2.79.122:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=cheapshhot[.]com	94bc44bd438d2e290516d
10/7/20	88.119.171.94:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=havemosts[.]com	f0ede92cb0899a9810a67c

10/7/20	5.2.64.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=mixunderax[.]com	e0f9efedd11d22a5a08ffb9
10/7/20	5.2.64.135:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bugsbunnyy[.]com	4aa2acabeb3ff38e39ed1d8
10/7/20	5.2.72.202:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sweetmonsterr[.]com	c04034b78012cca7dcc4a0
10/7/20	88.119.175.153:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=zhameharden[.]com	2670bf08c43d995c74b4b8
10/7/20	213.252.245.71:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=serviceboosterr[.]com	127cc347b711610c3bcee4
10/7/20	213.252.246.144:443	C=US,ST=TX,L=Texas,O=US,OU=,CN=servicewikii[.]com	b3e7ab478ffb0213017d57
10/7/20	5.2.64.149:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=sobcase[.]com	188f603570e7fa81b92906
10/7/20	5.2.64.144:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=unlockwsa[.]com	22d7f35e624b7bcee7bb78
10/7/20	88.119.174.139:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=serviceupdatter[.]com	12c6e173fa3cc11cc6b09b
10/7/20	88.119.174.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-boosterr[.]com	28435684c76eb5f1c4b48b
10/7/20	88.119.175.214:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=dotmaingame[.]com	9c2d64cf4e8e58ef86d16e
10/7/20	5.2.72.200:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=wodemayaa[.]com	f6f484baf1331abf55d067
10/7/20	5.2.79.10:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=hybriqdjs[.]com	d8eacda158594331aec3ac
10/7/20	5.2.79.12:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gunsdrag[.]com	29032dd12ea17fc37ffff1e
10/7/20	5.2.79.121:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=gungameon[.]com	eaf32b1c2e31e4e7b6d5c3
10/7/20	5.2.64.174:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=quwasd[.]com	442680006c191692fcc3df
10/7/20	5.2.64.172:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=remotessa[.]com	0593cbf6b3a3736a17cd64
10/7/20	5.2.64.167:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=secondlivve[.]com	38df81824bd8cded4a8fa7
10/7/20	5.2.64.182:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=luckyhunterrs[.]com	99dbe71ca7b9d4a1d9f722
10/7/20	88.119.171.97:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicesupdater[.]com	7d7199ffa40c50b6e5b025

10/7/20	88.119.171.96:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicemount[.]com	f433d25a0dad0def0510cd
10/7/20	96.9.209.217:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=fastbloodhunter[.]com	e84c7aa593233250efac90
10/7/20	69.61.38.132:443	C=US,ST=CA,L=Mountainvew,O=Office,OU=,CN=kungfupandasa[.]com	e6e80f6eb5cbfc73cde408
10/13/20	45.147.230.131:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bakcup-monster[.]com	4fdeab3dad077589d5268
10/13/20	45.147.229.92:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bakcup-checker[.]com	b70cdb49b26e6e9ba7d0c
10/13/20	45.147.229.68:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup-simple[.]com	57024c1fe5c4acaf30434b
10/13/20	45.147.229.52:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup-leader[.]com	ec5496048f1962494d239
10/13/20	45.147.229.44:443	C=US,ST=TX,L=Texsa,O=lol,OU=,CN=backup-helper[.]com	938593ac1c8bdb2c52565
10/14/20	45.147.230.87:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nasmastrservice[.]com	cced46e0a9b6c382a97607
10/14/20	45.147.230.159:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-leader[.]com	e912980fc8e9ec1e570e20
10/14/20	45.147.230.141:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-checker[.]com	39d7160ce331a157d3ecb
10/14/20	45.147.230.140:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-simple-helper[.]com	d9ca73fe10d52eef695232
10/14/20	45.147.230.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-leader[.]com	920d04330a165882c8076
10/14/20	45.147.230.132:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=boost-servicess[.]com	771463611a43ee35a0ce0
10/14/20	45.147.229.180:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=elephantdrrive[.]com	1e4a794da7d3c6d0677f7
10/14/20	45.147.230.159:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-leader[.]com	9c7fe10135f6ad96ded28f
10/15/20	45.147.230.132:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=boost-servicess[.]com	a78c0e2920e421667ae73
10/15/20	45.138.172.95:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-hellper[.]com	a0b2378ceae498f46401aa
10/16/20	108.62.12.119:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top-backuphelper[.]com	e95bb7804e3add830496b
10/16/20	108.62.12.105:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=best-nas[.]com	8d5dc95b3bd4d16a3434b

10/16/20	108.62.12.114:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top-backupservice[.]com	d5de2f5d2ca29da172473
10/16/20	108.62.12.116:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=bestservicehelper[.]com	9c7396ecd107ee8f8bf552
10/16/20	45.147.230.141:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-checker[.]com	1134a6f276f4297a083fc2
10/16/20	45.147.230.140:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-simple-helper[.]com	2150045f476508f89d9a3
10/16/20	45.147.230.133:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=nas-leader[.]com	f4ddc4562e5001ac8fdf0b
10/19/20	74.118.138.137:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top3-services[.]com	75fb6789ec03961c869b5
10/19/20	74.118.138.115:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=simple-backupbooster[.]com	9f5e845091015b533b59f
10/19/20	108.177.235.53:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=best-backup[.]com	4b78eaa4f2748df27ebf66
10/19/20	74.118.138.138:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topbackup-helper[.]com	bcccda483753c82e62482
10/21/20	45.153.241.1:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup1helper[.]com	672c66dd4bb62047bb836
10/21/20	45.153.240.240:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=checktodrivers[.]com	6825409698a326cc319ca
10/21/20	45.153.240.194:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver1master[.]com	7f9be0302da88e0d322e5
10/21/20	45.153.240.138:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=boost-yourservice[.]com	2c6a0856d1a75b303337a
10/21/20	45.153.240.136:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup1master[.]com	6559dbf8c47383b7b4935
10/23/20	45.153.240.157:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver1updater[.]com	7bd044e0a6689ef29ce23e
10/23/20	45.153.240.178:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1updater[.]com	9859a8336d097bc30e6e5
10/23/20	45.153.240.220:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driverdwl[.]com	43fb2c153b59bf46cf6f67
10/23/20	45.153.240.222:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=viewdrivers[.]com	22bafb30cc3adaa84fef747
10/23/20	45.153.241.134:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backups1helper[.]com	31e87ba0c90bb38b986af2
10/23/20	45.153.241.138:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver1downloads[.]com	f8a14846b7da416b14303

10/23/20	45.153.241.146:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicehel[.]com	01abdaf870d859f9c1fd76
10/23/20	45.153.241.153:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service-hel[.]com	c2eaf144e21f3aef5fe4b15
10/23/20	45.153.241.158:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=servicereader[.]com	de54af391602f3deea19cd
10/23/20	45.153.241.167:443	C=US,ST=TX,L=Texas,O=US,OU=,CN=view-backup[.]com	5f6fa19ffe5735ff81b0e79
10/23/20	45.147.231.222:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=top3servicebooster[.]com	ff54a7e6f51a850ef1d744c
10/23/20	45.153.241.141:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1view[.]com	4cda9d0bece4f6156a8096
10/26/20	74.118.138.139:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topbackupintheworld[.]com	e317485d700bf5e8cb8eea
10/26/20	108.62.12.12:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topservice-masters[.]com	e0022cbf0dd5aa597fee73
10/26/20	108.62.12.121:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=topservicebooster[.]com	44e7347a522b22cdf5de65
10/26/20	172.241.27.65:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backup1services[.]com	cd3e51ee538610879d6fa7
10/26/20	172.241.27.68:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backupmaster-service[.]com	04b6aec529b3656040a68
10/26/20	172.241.27.70:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=backupmasterservice[.]com	200c25c2b93203392e1ac
10/26/20	45.153.241.139:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driver-boosters[.]com	9d7c52c79f3825baf97d13
10/27/20	45.153.241.14:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1update[.]com	5bae28b0d0e969af2c0eda
10/28/20	190.211.254.154:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=driverjumper[.]com	a1e62e7e547532831d0dd
10/28/20	81.17.28.70:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=service1boost[.]com	67c7c75d396988ba7d6cd
10/28/20	81.17.28.105:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivehepler[.]com	880e59b44e7175e62d751
10/28/20	179.43.160.205:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivedownload[.]com	cdea09a43bef7f1679e9cd
10/28/20	179.43.158.171:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivefinder[.]com	512c6e39bf03a4240f5a2d
10/28/20	179.43.133.44:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivedwn[.]com	87f3698c743f8a1296babf

10/28/20	179.43.128.5:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idrivecheck[.]com	6df66077378c5943453b3
10/28/20	179.43.128.3:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idriveupdate[.]com	9706fd787a32a7e94915f9
10/28/20	81.17.28.122:443	C=US,ST=TX,L=Texas,O=lol,OU=,CN=idriveview[.]com	0e1b0266de2b5eaf427f59

FireEye detects this activity across our platforms. The following table contains several specific detection names from a larger list of detections that were available prior to this activity occurring.
