



📁 stamparm / maltrail Public

🔔 Notifications

 Fork 1.1k

 Star 6.5k

<> Code

🔗 Issues 75

🔗 Pull requests 1

🔄 Actions

📁 Projects

📖 Wiki

🛡 Security

📈 Insights

📁 Files

🔗 3ea7045

🔍

🔍 Go to file

> 📁 core

> 📁 docker

> 📁 html

> 📁 misc

> 📁 plugins

> 📁 thirdparty

▼ 📁 trails

> 📁 custom

> 📁 feeds

▼ 📁 static

> 📁 malicious

> 📁 malware

▼ 📁 suspicious

📄 android_pua.txt

📄 anonymous_web_proxy.txt

📄 bad_history.txt

📄 bad_wpad.txt

📄 blockchain_dns.txt

📄 computrace.txt

📄 connectwise.txt

📄 crypto_mining.txt

📄 dnspod.txt

📄 domain.txt

📄 dprk_silivaccine.txt

📄 dynamic_domain.txt

📄 free_web_hosting.txt

📄 i2p.txt

📄 ipinfo.txt

📄 onion.txt

📄 osx_pua.txt

📄 parking_site.txt

📄 port_proxy.txt

📄 pua.txt

📄 superfish.txt

📄 suspended_domain.txt

📄 web_shells.txt

maltrail / trails / static / suspicious / crypto_mining.txt 

 MikhailKasimov Update crypto_mining.txt 0e3911e · last year  History

Code

Blame

1096 lines (812 loc) · 32.1 KB

Raw







1# Copyright (c) 2014-2023 Maltrail developers (https://github.com/stamparm/maltrail/)

2# See the file 'LICENSE' for copying permission

3

4# Reference: https://hackforums.net/printthread.php?tid=5655422

5# Reference: https://twitter.com/r3dbU7z/status/1347527548977242116

6# Reference: https://www.virustotal.com/gui/file/6cd557cb2582ab5cf8d0e77131479ab91c00bf

7

8107.191.47.239:3333

9176.31.105.53:3333

1045.32.233.191:3333

1151.144.104.161:3333

1251.144.119.120:3333

1354.37.7.208:3333

1494.23.251.22:3333

15107.191.47.239:7777

16176.31.105.53:7777

1745.32.233.191:7777

1851.144.104.161:7777

1951.144.119.120:7777

2054.37.7.208:7777

2194.23.251.22:7777

22minergate.com

23pool.minergate.com

24xmr.pool.minergate.com

25miningpoolhub.com

26minexmr.com

27pool.minexmr.com

28moneropool.com

29crypto-pool.fr

30dwarfpool.com

31xmrpool.eu

32prohash.net

33nanopool.org

34ethereumpool.co

35suprnova.cc

36siamining.com

37

38# Reference: https://www.virustotal.com/gui/file/7738ad1029f1709ec86c8ba24e04b3f71edf67

39

4094.130.143.162:45700

41

42# Reference: https://www.multipool.us/

43

44multipool.us

45

46# Reference: https://mining-help.ru/

47

48mining-help.ru

49

50# Reference: https://xmrminer.cc/

51

52xmrminer.cc







53

54# Reference: https://www.monero.how/tutorial-how-to-mine-monero

55

56supportxmr.com

57monero-hackvault.com

-  xenarmor.txt
-  __init__.py
-  mass_scanner.txt
-  mass_scanner_cidr.txt
-  .gitattributes
-  .gitignore

```
57  monero.nashvaulc.pro
58  monerohash.com
59  monero.crypto-pool.fr
60  xmrpool.net
61  poolmining.org
62  pool.xmr.pt
63  xmr.prohash.net
64  xmr.poolto.be
65
66  # Reference: http://www.gandalph3000.com/
67
68  gandalph3000.com
69
70  # Reference: https://pangolinminer.com/
71
72  pangolinminer.com
73
74  # Reference: https://hellominer.com/
75
76  hellominer.com
77
78  # Reference: https://github.com/keraf/NoCoin/blob/master/src/blacklist.txt
79
80  # coinhive.com
81  # coin-hive.com
82  # jsecoin.com
83  # reasedoper.pw
84  # mataharirama.xyz
85  # listat.biz
86  # lmodr.biz
87  # minecrunch.co
88  # minemytraffic.com
89  # crypto-loot.com
90
91  # Reference: https://www.virustotal.com/#/file/179c5390ba2023402283104fd85d6394033976bc
92
93  sparechange.io
94
95  # Reference: https://blog.talosintelligence.com/2018/08/rocke-champion-of-monero-miners
96
97  8282.space
98  3389.space
99
100 # Reference: https://github.com/xmrig/xmrig/blob/master/src/net/strategies/DonateStrate
101
102 fee.xmrig.com
103
104 # Reference: https://www.securityhome.eu/malware/malware.php?mal_id=7994909645aa0b75fc0
105
106 donate.xmrig.com
107
108 # Reference: https://isc.sans.edu/forums/diary/What+is+going+on+with+port+3333/23215
109
110 mine.moneropool.com
111 pool.cortins.tk
112 pool.supportxmr.com
113 xmr.crypto-pool.fr
114 xmrpool.eu
115
116 # Reference: https://unit42.paloaltonetworks.com/mac-malware-steals-cryptocurrency-exch
117
118 koto-pool.work
```




1023
1024 # Reference: <https://www.virustotal.com/gui/ip-address/51.254.84.37/relations>
1025
1026 mine.lesliejust.is

1027

1028 # Reference: <https://www.virustotal.com/gui/ip-address/34.98.99.30/relations>

1029

1030 monerpool.org

1031 cbd.monerpool.org

1032 cbdv2.monerpool.org

1033 daili01.monerpool.org

1034 linux.monerpool.org

1035 moner.monerpool.org

1036 moner1min.monerpool.org

1037 xiazai.monerpool.org

1038 xiazai1.monerpool.org

1039 xmr.monerpool.org

1040 xmr1min.monerpool.org

1041 xx11m.monerpool.org

1042 xx11mv2.monerpool.org

1043

1044 # Reference: <https://www.virustotal.com/gui/file/82d54b01efce5dd7f9cc36e77e9663a545c834>

1045

1046 142.202.242.45:5555

1047 nbminer.com

1048 dl.nbminer.com

1049 lhr.nbminer.com

1050 lhr3.nbminer.com

1051

1052 # Reference: <https://twitter.com/SecureSh3ll/status/1614755430651105281>

1053

1054 141.94.96.144:5555

1055

1056 # Reference: <https://www.virustotal.com/gui/file/00869be6a840dbdd657bb91cd6afb5c24e512e>

1057

1058 141.95.206.77:8443

1059

1060 # Reference: <https://www.virustotal.com/gui/file/854edb1e3d27ceddd528cd604883c9f08cea19>

1061

1062 51.68.190.80:14433

1063

1064 # Reference: <https://www.cadosecurity.com/redis-miner-leverages-command-line-file-hosti>

1065 # Reference: <https://otx.alienvault.com/pulse/64020be7e20c783ba85177f5>

1066

1067 herominers.com

1068 xmrfast.com

1069 pool.xmrfast.com

1070 monero.herominers.com

1071 pool.gntl.co.uk

1072 ca.monero.herominers.com

1073 xmr.pool.gntl.co.uk

1074

1075 # Reference: <https://www.crowdstrike.com/blog/crowdstrike-discovers-first-ever-dero-cry>

1076 # Reference: <https://otx.alienvault.com/pulse/6414cd3690659d2c4d446f91>

1077 # Reference: <https://www.virustotal.com/gui/file/021a6ac6cac28e6d9527ef0fcbc09d3d225162>

1078 # Reference: <https://www.virustotal.com/gui/file/124281b20b6c97ebbc902d5dde5dc958a2dcc>

1079

1080 15.204.9.209:10300

1081 15.235.184.172:10300

1082 167.235.7.72:10300

1083 172.86.75.2:443

1084 45.61.137.195:58282

1085 community-pools.mysrv.cloud

1086

1087 # Reference: <https://www.virustotal.com/gui/file/0dba10ee3fede85677e79f64f863e2e05ce8e9>

1088

1089 94.130.9.194:45700

1090 bcn.pool.minergate.com

1091 bcn.vip.pool.minergate.com

1092 fcn-xmr.pool.minergate.com

1093 mro.pool.minergate.com

1094 xmc.pool.minergate.com

1095 xmo.pool.minergate.com

1096 xmr.vip.pool.minergate.com