نشانه‌های آلودگی (IoC)

سرورها و نشانه‌های URL

o4hlcckwlbcy7qhhohqswpqla6wx7c5xmsvk3k4rohknng4nofvgz5id[.] onion - port 5870 and 587
p2l44qilgm433bad5gbszb4mluxuejwkjaaon767m5dzuuc7mjqhcead[.]onion - port 42066
q2p4b6pprex5mvzxm2xdqgo4q3hy2p4if2ljq7fcoavxvab7mpk232id[.]onion - port 52566
3og7wipgh3ruavi7gd6y3uzhcurazasln55hb6hboiavyk6pugkcdpqd[.]onion - port 6697
bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws
can6dodp[.]servepics[.]com
ublock-referer[.]dev
hxxps://cloud-miner[.]de/tkefrep/tkefrep[.]js?tkefrep=bs?nosaj=faster.xmr2
hxxp[:]//can6dodp[.]servepics[.]com/setup.py
hxxp[:]//can6dodp[.]servepics[.]com/setup
hxxp[:]//can6dodp[.]servepics[.]com/py.exe
hxxp[:]//can6dodp[.]servepics[.]com/xmrig
hxxp[:]//can6dodp[.]servepics[.]com/xmrig1
hxxp[:]//ngiwge486ln9daoo[.]hopto[.]org/setup.py
hxxp[:]//ngiwge486ln9daoo[.]hopto[.]org/py.exe
hxxp[:]//bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws/setup.py
hxxp[:]//bp65pce2vsk7wpvy2fyehel25ovw4v7nve3lknwzta7gtiuy6jm7l4yd[.]onion[.]ws/py.exe

نمونه ها:

c3fe8058ab46bd21d22f920960caae1f3b22a7aeba8d5315fb62461f4e989a7d
8797ce228b32d890773d5dbac71cefa505b788cc8b25929be9832db422d8239b
bc2126c03f2242013f58b43eb91351fba15d300385252423c52a5b18ece6a54f
97ab2092f6b5b1986536a5ba45e487f19c97f52544ff494d43bb1baf31248924
c3fe8058ab46bd21d22f920960caae1f3b22a7aeba8d5315fb62461f4e989a7d
8130717a3d4053e2924a0393086511a41fc7777c045b45bb4f569bcbe69af8be
d65e874b247dda9845661734d9e74b921f700983fd46c3626a3197f08a3006bf
19c25ce4302050aec3c921dd5cac546e8200a7e951d570b52fe344c421105ea8
606258f10519be325c39900504e50d79e551c7a9399efb9b22a7323da3f6aa7a
2b77b93b8e1b8ef8650957d15aaf336cf70a7df184da060f86b9892c54eefb65
eb8b08e13aba16bd5f0d7c330493be82941210d3a6aa4856858df770f77b747d
80659cc37cb7fb831866f7d7b0043edc6918a99590bd9122815e18abb68daa35
19269ce9a0a44aca9d6b2deed7de71cf576ac611787c2af46819ca2aff44ce2a
a8bb386fa3a6791e72f5ec6f1dc26359b00d0ee8cb0ce866f452b7fff6dbb319
d58c3694832812bc168834e2b8b3bfcb92f85a9d4523140ad010497baabc2c3d
e884bd4015d1b97227074bcf6cb9e8134b7afcfb6a3db758ca4654088403430a
d6403b9c069f08939fc2f9669dc7d5165ed66a1cae07788c3b27fffb30e890a0
9d6171cf28b5a3572587140ef483739a185895ce2b5af3246a78c2c39beed7b8