

Forum:[Hack Forums](#)

Thread: [CurrPorts Monitor Open TCP/IP connections](#)

MonacoSquad - November 16, 2013, 4:37 am

Maybe you guys heard of this tool already but its a great tool to monitor all traffic on windows systems.

You can see if someone has infected your pc and is sending information to remote address. Or you can see that the crypter you just bought on the marketplace is actually rooted and sending back your information to the FBI ;)

<http://www.nirsoft.net/utils/cports.html>

Other great uses are checking what update ip/domains anti-virus programs use and block them.

Great tool to have.

Smurb - November 18, 2013, 10:54 am

My cousin told me alot about this.

Thanks for the share, will be useful for other people on here.

Jagster™ - November 20, 2013, 10:00 am

This program has been around for awhile, and yes OP you're correct if you use it correctly then it is a great tool to monitor your system's traffic!

Gary™ - November 25, 2013, 5:28 pm

Can anyone give me a bit of help with this? I ran CurrPorts and I'm currently seeing the following:

Code	System	784	TCP	135	epmap	0.0.0.0	0.0.0.0	Listening	25/11/2013
23:48:06	NT AUTHORITY\NETWORK SERVICE				RpcEptMapper, RpcSs				26/11/2013
01:21:23									

System	4	TCP	139	netbios-ssn	192.168.1.65	0.0.0.0	Listening	N/A
26/11/2013	01:21:23							

System	4080	TCP	554	rtsp	0.0.0.0	0.0.0.0	Listening	25/11/2013
23:50:25	NT AUTHORITY\NETWORK SERVICE				WMPNetworkSvc			26/11/2013
01:21:23								

System	484	TCP	49152		0.0.0.0	0.0.0.0	Listening	25/11/2013
23:48:03	NT AUTHORITY\SYSTEM							26/11/2013 01:21:23

System	560	TCP	49153		0.0.0.0	0.0.0.0	Listening	25/11/2013
23:48:04	NT AUTHORITY\SYSTEM				KeyIso, SamSs			26/11/2013 01:21:23

System	552	TCP	49154		0.0.0.0	0.0.0.0	Listening	25/11/2013
23:48:03	NT AUTHORITY\SYSTEM							26/11/2013 01:21:23

System	2296	TCP	49164		0.0.0.0	0.0.0.0	Listening	25/11/2013
23:48:24	NT AUTHORITY\NETWORK SERVICE				PolicyAgent			26/11/2013
01:21:23								

System	3928	TCP	49204		192.168.1.65	80	http	72.249.47.77	ns1.inputsafe.com
--------	------	-----	-------	--	--------------	----	------	--------------	-------------------

Close Wait 25/11/2013 23:49:29 Gary-PC\Gary 26/11/2013 01:21:23

System 836 TCP 49316 192.168.1.65 80 http 91.199.212.171 download.comodo.com Close Wait 25/11/2013 23:48:06 NT AUTHORITY\SYSTEM cmdAgent 26/11/2013 01:21:23

System 836 TCP 49317 192.168.1.65 80 http 178.255.82.1 downloads.comodo.com Close Wait 25/11/2013 23:48:06 NT AUTHORITY\SYSTEM cmdAgent 26/11/2013 01:21:23

System 1548 TCP 49761 192.168.1.65 80 http 72.249.47.77 ns1.inputsafe.com Close Wait 25/11/2013 23:49:05 Gary-PC\Gary 26/11/2013 01:21:23 Program Manage

System 924 TCP 52106 192.168.1.65 80 http 217.32.28.222 Established 2 5/11/2013 23:48:07 NT AUTHORITY\NETWORK SERVICE CryptSvc, Dnscache, LanmanWorkstation, NlaSvc 26/11/2013 01:21:23

System 4 TCP 445 microsoft-ds 0.0.0.0 0.0.0.0 Listening N/A 26/11/2013 01:21:23

System 4 TCP 2869 iclap 0.0.0.0 0.0.0.0 Listening N/A 26/11/2013 01:21:23

System 4 TCP 5357 wsd 0.0.0.0 0.0.0.0 Listening N/A 26/11/2013 01:21:23

System 4 TCP 10243 0.0.0.0 0.0.0.0 Listening N/A 26/11/2013 01:21:23

System 4 UDP 137 netbios-ns 192.168.1.65 N/A 26/11/2013 01:21:23

System 4 UDP 138 netbios-dgm 192.168.1.65 N/A 26/11/2013 01:21:23

System 420 UDP 500 isakmp 0.0.0.0 25/11/2013 23:48:08 NT AUTHORITY\SYSTEM AeLookupSvc, Appinfo, BITS, Browser, EapHost, gpsvc, IKEEXT, iphlpsvc, LanmanServer, MMCSS, ProfSvc, SENS, ShellHWDetection, Themes, Winmgmt 26/11/2013 01:21:23

System 1676 UDP 1900 ssdp 127.0.0.1 25/11/2013 23:48:14 NT AUTHORITY\LOCAL SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23

System 1676 UDP 1900 ssdp 192.168.1.65 25/11/2013 23:48:14 NT AUTHORITY\LOCAL SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23

System 1676 UDP 3702 ws-discovery 0.0.0.0 25/11/2013 23:48:14 NT AUTHORITY\LOCAL SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23

System 420 UDP 4500 ipsec-msft 0.0.0.0 25/11/2013 23:48:08 NT AUTHORITY\SYSTEM AeLookupSvc, Appinfo, BITS, Browser, EapHost, gpsvc, IKEEXT, iphlpsvc, LanmanServer, MMCSS, ProfSvc, SENS, ShellHWDetection, Themes, Winmgmt 26/11/2013 01:21:23

System 4080 UDP 5004 0.0.0.0 25/11/2013 23:50:25 NT AUTHORITY\NETWORK SERVICE WMPNetworkSvc 26/11/2013 01:21:23

System 4080 UDP 5005 0.0.0.0 25/11/2013 23:50:25 NT AUTHORITY\NETWORK SERVICE WMPNetworkSvc 26/11/2013 01:21:23

System 924 UDP 5355 llmnr 0.0.0.0 25/11/2013 23:48:07 NT
AUTHORITY\NETWORK SERVICE CryptSvc, Dnscache, LanmanWorkstation,
NlaSvc 26/11/2013 01:21:23

System 1676 UDP 53384 192.168.1.65 25/11/2013 23:48:14 NT
AUTHORITY\LOCAL SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013
01:21:23

System 1676 UDP 53385 127.0.0.1 25/11/2013 23:48:14 NT AUTHORITY\LOCAL
SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23

System 1676 UDP 58227 0.0.0.0 25/11/2013 23:48:14 NT AUTHORITY\LOCAL
SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23

System 784 TCP 135 epmap :: :: Listening 25/11/2013 23:48:06 NT
AUTHORITY\NETWORK SERVICE RpcEptMapper, RpcSs 26/11/2013 01:21:23

System 4 TCP 445 microsoft-ds :: :: Listening N/A 26/11/2013
01:21:23

System 4080 TCP 554 rtsp :: :: Listening 25/11/2013 23:50:25 NT
AUTHORITY\NETWORK SERVICE WMPNetworkSvc 26/11/2013 01:21:23

System 4 TCP 2869 icslap :: :: Listening N/A 26/11/2013
01:21:23

System 4 TCP 5357 wsd :: :: Listening N/A 26/11/2013
01:21:23

System 4 TCP 10243 :: :: Listening N/A 26/11/2013
01:21:23

System 484 TCP 49152 :: :: Listening 25/11/2013 23:48:03 NT
AUTHORITY\SYSTEM 26/11/2013 01:21:23

System 560 TCP 49153 :: :: Listening 25/11/2013 23:48:04 NT
AUTHORITY\SYSTEM KeyIso, SamSs 26/11/2013 01:21:23

System 552 TCP 49154 :: :: Listening 25/11/2013 23:48:03 NT
AUTHORITY\SYSTEM 26/11/2013 01:21:23

System 2296 TCP 49164 :: :: Listening 25/11/2013 23:48:24 NT
AUTHORITY\NETWORK SERVICE PolicyAgent 26/11/2013 01:21:23

System 420 UDP 500 isakmp :: 25/11/2013 23:48:08 NT
AUTHORITY\SYSTEM AeLookupSvc, Appinfo, BITS, Browser, EapHost, gpsvc, IKEEXT,
iphlpvc, LanmanServer, MMCSS, ProfSvc, SENS, ShellHWDetection, Themes,
Winmgmt 26/11/2013 01:21:23

System 664 UDP 546 dhcpv6-client fe80::8890:1c:b538:50c5 25/11/2013
23:48:09 NT AUTHORITY\LOCAL SERVICE AudioSrv, Dhcp, lmhosts, wscsvc 26/11/2013
01:21:23

System 1676 UDP 1900 ssdp ::1 25/11/2013 23:48:14 NT AUTHORITY\LOCAL
SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23

System 1676 UDP 1900 ssdp fe80::8890:1c:b538:50c5 25/11/2013 23:48:14 NT
AUTHORITY\LOCAL SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013
01:21:23

System 1676 UDP 3702 ws-discovery :: 25/11/2013 23:48:14 NT
AUTHORITY\LOCAL SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013
01:21:23

System 420 UDP 4500 ipsec-msft :: 25/11/2013 23:48:08 NT
AUTHORITY\SYSTEM AeLookupSvc, Appinfo, BITS, Browser, EapHost, gpsvc, IKEEXT,
iphlpvc, LanmanServer, MMCSS, ProfSvc, SENS, ShellHWDetection, Themes,
Winmgmt 26/11/2013 01:21:23

System 4080 UDP 5004 :: 25/11/2013 23:50:25 NT AUTHORITY\NETWORK
SERVICE WMPNetworkSvc 26/11/2013 01:21:23

System 4080 UDP 5005 :: 25/11/2013 23:50:25 NT AUTHORITY\NETWORK
SERVICE WMPNetworkSvc 26/11/2013 01:21:23

```

System 924 UDP 5355 llmnr :: 25/11/2013 23:48:07 NT AUTHORITY\NETWORK
SERVICE CryptSvc, Dnscache, LanmanWorkstation, NlaSvc 26/11/2013 01:21:23
System 1676 UDP 53382 fe80::8890:1c:b538:50c5 25/11/2013 23:48:14 NT
AUTHORITY\LOCAL SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013
01:21:23
System 1676 UDP 53383 ::1 25/11/2013 23:48:14 NT AUTHORITY\LOCAL
SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23
System 1676 UDP 58228 :: 25/11/2013 23:48:14 NT AUTHORITY\LOCAL
SERVICE FDResPub, SSDPSRV, upnphost 26/11/2013 01:21:23
Unknown 0 TCP 51875 192.168.1.65 80 http 213.120.162.226 Time
Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51883 192.168.1.65 80 http 216.239.120.39 phx2-ss-3-lb.cnet.co
m Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51891 192.168.1.65 80 http 23.74.85.109 a23-74-85-109.deploy.
static.akamaitechnologies.com Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51892 192.168.1.65 80 http 23.74.85.109 a23-74-85-109.deploy.
static.akamaitechnologies.com Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51893 192.168.1.65 80 http 23.74.85.109 a23-74-85-109.deploy.
static.akamaitechnologies.com Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51894 192.168.1.65 80 http 23.74.85.109 a23-74-85-109.deploy.
static.akamaitechnologies.com Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51928 192.168.1.65 80 http 173.194.34.187 lhr14s22-in-f27.1e10
0.net Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51929 192.168.1.65 80 http 173.194.34.187 lhr14s22-in-f27.1e10
0.net Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51930 192.168.1.65 80 http 173.194.34.187 lhr14s22-in-f27.1e10
0.net Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51931 192.168.1.65 80 http 173.194.34.187 lhr14s22-in-f27.1e10
0.net Time Wait N/A 26/11/2013 01:21:23
Unknown 0 TCP 51941 192.168.1.65 80 http 178.236.4.159 Time
Wait N/A 26/11/2013 01:21:23
Unknown 0 TCP 51942 192.168.1.65 80 http 178.236.4.159 Time
Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51950 192.168.1.65 80 http 173.194.34.188 lhr14s22-in-f28.1e10
0.net Time Wait N/A 26/11/2013 01:21:23

Unknown 0 TCP 51951 192.168.1.65 80 http 173.194.34.188 lhr14s22-in-f28.1e10
0.net Time Wait N/A 26/11/2013 01:21:23
Unknown 0 TCP 51952 192.168.1.65 80 http 69.172.216.58 Time
Wait N/A 26/11/2013 01:21:23
Unknown 0 TCP 51953 192.168.1.65 80 http 69.172.216.58 Time
Wait N/A 26/11/2013 01:21:23

```

Unknown	0	TCP	51962	192.168.1.65	80	http	216.239.120.246	phx2-dw-cbsi-xw-lb
.cnet.com	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	51978	192.168.1.65	80	http	107.23.6.176	ec2-107-23-6-176.com
pute-1.amazonaws.com	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	51979	192.168.1.65	80	http	217.32.28.223	Time
Wait	N/A						26/11/2013 01:21:23	
Unknown	0	TCP	51980	192.168.1.65	80	http	217.32.28.223	Time
Wait	N/A						26/11/2013 01:21:23	
Unknown	0	TCP	51994	192.168.1.65	80	http	217.32.28.230	Time
Wait	N/A						26/11/2013 01:21:23	
Unknown	0	TCP	52003	192.168.1.65	80	http	50.112.170.89	ec2-50-112-170-89.us
-west-2.compute.amazonaws.com	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52010	192.168.1.65	80	http	107.23.13.87	ec2-107-23-13-87.com
pute-1.amazonaws.com	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52019	192.168.1.65	80	http	173.194.34.186	lhr14s22-in-f26.1e10
0.net	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52020	192.168.1.65	80	http	173.194.34.186	lhr14s22-in-f26.1e10
0.net	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52021	192.168.1.65	80	http	173.194.34.186	lhr14s22-in-f26.1e10
0.net	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52022	192.168.1.65	80	http	173.194.34.186	lhr14s22-in-f26.1e10
0.net	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52023	192.168.1.65	80	http	173.194.34.186	lhr14s22-in-f26.1e10
0.net	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52061	192.168.1.65	80	http	2.16.115.231	Time
Wait	N/A						26/11/2013 01:21:23	
Unknown	0	TCP	52062	192.168.1.65	80	http	31.13.72.1	edge-star-shv-03-lhr2.fac
ebook.com	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52063	192.168.1.65	80	http	31.13.72.1	edge-star-shv-03-lhr2.fac
ebook.com	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52087	192.168.1.65	80	http	23.35.209.224	a23-35-209-224.deplo
y.static.akamaitechnologies.com	Time Wait	N/A					26/11/2013 01:21:23	
Unknown	0	TCP	52103	192.168.1.65	80	http	23.23.235.140	ec2-23-23-235-140.co
mpute-1.amazonaws.com	Time Wait	N/A					26/11/2013 01:21:23	

Is there anything here I should be alarmed by, or better closing? Bit of a noob when it comes to this side of things.. Any help is appreciated,

:)