גירסה 1.00 - 28.6.2003

רשימת טרויאנים

מסמך זה הורד מהאתר http://underwar.livedns.co.il.
אין להפיץ מסמך זה במדיה כלשהי, ללא אישור מפורש מאת המחבר.
מחבר המסמך איננו אחראי לכל נזק, ישיר או עקיף, שיגרם עקב השימוש במידע המופיע במסמך, וכן לנכונות התוכן של הנושאים המופיעים במסמך. עם זאת, המחבר עשה את מירב המאמצים כדי לספק את המידע המדויק והמלא ביותר.

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.livedns.co.il

רשימת הטרויאנים

להלן רשימה של טרויאנים ידועים והפורטים אליהם הם מקשיבים.
ניתן להשתמש ברשימה כבסיס לזיהוי של טרויאנים המותקנים על מחשב.

במידה ואנו רוצים לראות את רשימת ה-ports הפתוחים על המחשב המקומי, נפתח Command Prompt, ונכתוב:

netstat -a

יש להדגיש כי הפורטים המצוינים כאן הם ברירת מחדל בלבד. בטרויאנים רבים קיימת האפשרות לשנות את הפורט ולבחור אחד אחר כלשהו במקומו.

Port	Trojan
2	Death
21	Back Construction, Blade Runner, Doly Trojan, Fore, FTP Trojan, Invisible FTP, Larva, MBT, Motiv, Net Administrator, Senna Spy FTP Server, WebEx, WinCrash
23	Tint Telnet Server, Truva Atl
25	Ajan, Antigen, Email Password Sender, Gip, Haebu Coceda (=Naebi), Happy 99, I Love You, Kaung2, Pro Mail Trojan, Shtrilitz, Stealth, Tapiras, Terminator, WinPC, WinSpy
31	Agent 31, Hackers Paradise, Masters Paradise
41	Deep Throat
48	DRAT
50	DRAT
59	DMSetup
79	Firehotcker
80	Back End, Executer, Hooker, RingZero
99	Hidden Port 2.0
110	ProMail Trojan
113	Invisible Identd daemon, Kazimas
119	Happy99
121	Jammer Killah V
123	Net Controller
133	Faranz, port 146 - Infector
146 *UDP*	Infector
170	A-Trojan
421	TCP Wrappers
456	Hackers Paradise
531	Rasmin
555	ini-Killer, NetAdmin, Phase Zero, Stealth Spy
666	Attack FTP, Back Construction, Cain & Able, NokNok, Satanz Backdoor, ServeU, Shadow Phyre
667	SniperNet
669	DP Trojan
692	GayOL
777	Aimspy
133	Faranz, port 146 - Infector
808	WinHole
911	Dark Shadow
999	Deep Throat, WinSatan
1000	Der Spaeher 3
1001	Der Spaeher 3, Doly Trojan, Silencer, WebEx
1010	Doly Trojan 1.35
1011	Doly Trojan
1012	Doly Trojan

1015	Doly Trojan 1.5
1016	Doly Trojan 1.6
1020	Vampire
1024	NetSpy, Psyber Streaming Server
1029	InCommand Access
1033	NetSpy
1042	Blah 1.1
1045	Rasmin
1050	Mini Command 1.2 Access
1080	WinHole
1081	WinHole
1082	WinHole
1083	WinHole
1090	Xtreme
1095	RAT
1097	RAT
1098	RAT
1099	BFevolution, RAT
1170	Psyber Stream Server, Streaming Audio Trojan, Voice
1200 *UDP*	NoBackO
1201 *UDP*	NoBackO
1207	Softwar
1212	Kaos
1225	Scarab
1234	Ultors Trojan
1243	BackDoor-G, SunSeven, SubSeven Apocalypse
1245	VooDoo Doll
1255	Scarab
1256	Project nEXT
1269	Mavericks Matrix
1313	NETrojan
1338	Millenium Worm
1349 *UDP*	BackOrifice DLL
1492	FTP99CMP
1509	Psyber Streaming Server
1524	Trinoo
1600	Shivka-Burka
1777	Scarab
1807	Spy Sender
1981	Shockrave
1966	Fake FTP
1969	OpC BO
1981	Shockrave
1999	TransScout, Backdoor
2000	Der Spaeher 3, TransScout, Insane Network 4, Milennium
2001	Der Spaeher 3, TransScout, Trojan Cow
2002	TransScout
2003	TransScout
2004	TranScout
2005	TransScout
2023	Ripper Pro, PassRipper
2080	WinHole
2115	Bugs

2140	Deep Throat, The invasor
2155	illusion Mailer
2283	HVL Rat 5
2300	Xplorer
2565	Striker
2583	WinCrash 2
2600	Digital Root Beer
2716	The Prayer 2
2773	SubSeven
2801	Phineas Phucker
2989 *UDP*	Rat
3000	Remote Shutdown
3024	WinCrash
3128	RingZero
3129	Masters Paradise
3150	Deep Throat, The invasor
3459	Eclipse 2000, Sanctuary
3700	Portal Of Doom
3791	Eclypse, Totaleclipse 1.0
3801 UDP	Eclypse
4000	Psyber Streaming Server, Skydance
4092	WinCrash
4242	Virtual Hacking Machine
4321	BoBo, SchoolBus 1.0
4444	Prosiak, Swift remote
4567	File Nail
4590	ICQTrojan
5000	Bubbel, Back Door Setup, S ockets de Troie, Socket 23
5001	Back Door Setup, Socket de Troie
5010	Solo
5011	One Of The Last Trojans (OOTLT), OOTLT Cart
5031	NetMetropolitan 1.0/1.04
5032	NetMetropolitan
5321	Filehotcker
5343	wCrat
5400	Blade Runner, Back Construction 1.2/1.5
5401	Blade Runner, Back Construction
5402	Blade Runner, Back Construciton
5512	illusion Mailer
5521	illusion Mailer
5550	Xtcp, Xtcp2
5555	ServeMe
5556	Bo Facil
5557	Bo Facil
5569	RoboHack
5637	Crasher
5638	Crasher
5714	WinCrash
5741	WinCrash
5742	WinCrash
5882 *UDP*	Y3K RAT
5888	Y3K RAT
6000	The Thing

6006	The Thing
6272	Secret Service
6400	The Thing
6666	TCPShell (*NIX Backdoor)
6669	Vampyre
6670	Deep Throat
6711	SubSeven
6712	SubSeven
6713	SebSeven
6723	Mstream
6771	Deep Throat
6776	BackDoor-G, SubSeven
6838 *UDP*	Mstream
6883	DeltaSource
6912	ShitHeep
6913	ShitHeep Danny
6939	Indoctrination
6969	GeteCrasher, Priority, IRC 3
6970	GeteCrasher
7000	Remote Grab, Kazimas
7001	Freak88
7215	SubSeven
7300	NetMonitor
7301	NetMonitor
7302	NetMonitor
7303	NetMonitor
7304	NetMonitor
7305	NetMonitor
7306	NetMonitor
7307	NetMonitor
7308	NetMonitor
7309	NetMonitor
7424	Host Control
7424 *UDP*	Host Control
7789	Back Door Setup, ICKiller
7983	Mstream
8080	RingZero
8787	BO2K
8879	Hack Office Armageddon
8988	BacHack
8989	Rcon
9000	Netministrator
9325 *UDP*	Mstream
9400	InCommand
9872	Portal Of Doom
9873	Portal Of Doom
9874	Portal Of Doom
9875	Portal Of Doom
9876	Cyber Attack, RUX
9878	TransScout
9989	ini-Killer
9999	The Prayer 1
10067	Portal Of Doom

UDP	
10085	Syphillis
10086	Syphillis
10101	BrainSpy
10167 *UDP*	Portal Of Doom
10520	Acid Shivers
10528	Host Control
10607	Coma
10666	Ambush
10752	LINUX mounts Backdoor
11000	Senna Spy
11050	Host Control
11051	Host Control
11223	Progenic Trojan
12076	Gjamer
12223	Hack 99 KeyLogger
12345	NetBus, GabanBus, X-Bill, Pie Bill Gates
12346	NetBus 1.0, GabanBus, X-Bill
12361	Whack-a-Mule
12362	Whack-a-Mule
12623 *UDP*	DUN Control
12624	Buttman
12631	Whack Job
12701	Eclipse 2000
12754	Mstream
13000	Senna Spy
13010	Hacker Brazil
13700	Kuang 2 The Virus
15092	Host Control
15104	Mstream
16484	Mosucker
16660	Stracheldracht
16772	ICQ Revenge
16959	Subseven DEFCON8 2.1
16969	Priority, Portal Of Doom
17166	Mosaic
17300	Kaung 2 The Virus
17777	Nephron
18753 *UDP*	Shaft
19864	ICQ Revenge
20000	Milennium
20001	Milennium
20002	AcidkoR
20034	NetBus 2 Pro
20203	Logged!, Chupacabra
20331	Bla
20432	Shaft
20432 *UDP*	Shaft
21544	Girl Friend, Kidterror, Schwindler 1.8, Schwindler 1.82
22222	Prosiak
23023	Logged
23432	Asylum

23456	Evil FTP, Ugly FTP, Whack Job
23476	Donald Duck
23476 *UDP*	Donald Duck
23477	Donald Duck
26274 *UDP*	Delta Source
26681	Spy Voice
27374	SubSeven 2.1
27444 *UDP*	Trinoo
27573	SubSeven
27665	Trinoo
29104	Host Control
29891 *UDP*	The Unexplained
30001	TerrOr32
30029	AOL Trojan 1.1
30100	NetSphere
30101	NetSphere
30102	NetSphere
30103	NetSphere
30103 *UDP*	NetSphere
30133	NetSphere Final 1.31.337, Trojan Spirit 2001a
30303	Sockets de troie, Socket 23, Socket 25
30974	Intruse
30999	Kaung 2
31335 *UDP*	Trinoo
31336	BO Whack, ButtFunnel
31337	Baron Night, BO Client, BO2, BO Facil
31337 *UDP*	Back fire, Back Orifice, Deep BO
31338	NetSpy DK, ButtFunnel
31338 *UDP*	Back Orifice, Deep BO
31399	NetSpy DK
31554	Schwindler
31666	BoWhack
31785	Hack a Tack
31787	Hack a Tack
31788	Hack a Tack
31789 *UDP*	Hack a Tack
31791 *UDP*	Hack a Tack
31792	Hack a Tack
32100	Peanut Brittle, Project nEXT
32418	Acid Battery 1.0
33333	Blakharaz, Prosiak
33577	PsychWard
33777	PsychWard
33911	Spirit 2001a
34324	BigGluck, TN, Tiny Telnet Server
34555 *UDP*	Trinoo - Windows

35555 *UDP*	Trinoo - Windows
37651	Yet Another Trojan
40412	The Spy
40421	Masters Paradise, Agent 40421
40422	Masters Paradise
40423	Masters Paradise
40426	Masters Paradise
41666	Remote Boot
41666 *UDP*	Remote Boot
43210	SchoolBus 1.6/2.0
44444	Prosiak
47262 *UDP*	Delta Source
49301	Online KeyLogger
50505	Sockets de Troie
50766	Fore, Schwindler
50776	Fore, Remote Windows Shutdown
51996	Cafeini
52317	Acid Battery 2000
53001	Remote Windows Shutdown
54283	SubSeven
54320	Back Orifice 2000
54321	Back Orifice 2000, SchoolBus 1.6/2.0
54321 *UDP*	Back Orifice
57341	Netraider
58339	ButtFunnel
60000	Deep Throat
60068	Xzip 6000068
60411	Connection
61348	BunkerHill
61466	TeleCommando
61603	BunkerHill
63485	BunkerHill
65000	Devil 1.03, Stacheldracht
65432	The Traitor
65432 *UDP*	The Traitor
65535	RC