Di seguito sono presenti le regole, da inserire nel firewall, per configurare le porte per bloccare l'attacco alla ricerca dei programmi Troiani. In questo modo è possibile capire se un segnale di allerta del firewall è un vero attacco o una normale attività della rete. E' evidente che le impostazioni di queste regole variano a seconda del firewall utilizzato ed inoltre non tutti i firewall permettono di aggiungere nuove regole.

Per ogni singola regola presente nella Tabella sotto indicata bisogna:

Bloccare ogni applicazione

Per il servizio Remoto -----> Blocca tutti i servizi

Per gli indirizzi Remoto e Locali -------> Blocca tutti gli indirizzi

Blocco in Entrata	**Protocollo**	**Porte e/o Servizi locali (Proprio PC)**
Back Orifice 2000	TCP o UDP	Back-Orifice, Back-Orifice-2000,Back-Orifice-2000-1
NetBus	TCP	NetBus-Pro, NetBus, NetBus-2
GirlFriend	TCP	21554
WinCrash	TCP	2583,3024,4092,5742
DeepThroat	TCP o UDP	2140, 3150, 41, 60000,6670,6771,999
Hack 'A' Tack	TCP o UDP	31785,31787,31788,31789,31791,31792
FC Infector Trojan	TCP o UDP	146
Dmsetup Troian	TCP	58
Stealth Spy Troian	TCP	555
FireHotcker Troian	TCP	5321
Attack FTP Trojan	TCP	666
Dark Shadow Troian	TCP	911
Silencer Troian	TCP	1001
Block Netspy Trojan	TCP	1024
RASmin Trojan	TCP	1045,conference
Extreme Trojan	TCP	1090
Ultor's Trojan	TCP	1234
Whack-a-Mole Trojan	TCP	Porta da 12361 a 12363
WhackJob Trojan	TCP	12631
FTP99CMP Trojan	TCP	1492
Shiva Burka Trojan	TCP	1600
Spy Sender Trojan	TCP	1807
Blook ShockRave Trojan	TCP	1981
Remote Explorer Trojan	TCP	2000
Trojan Cow Trojan	TCP	2001
Trojan Ripper Trojan	TCP	2023
Blook Bugs Trojan	TCP	2115
Striker Trojan	TCP	2565
Phinneas Phucker Trojan	TCP	2801
Rat Trojan	UDP	2989
Filenail Troian	TCP	4567
Sokets de Trois v1. Trojan	TCP	5000,5001
Blade Runner Trojan	TCP	Porta da 5400 a 5402
SERV-Me Trojan	TCP	rmt
BO-Facil Trojan	TCP	Porta da 5556 a 5557

Robo-Hack Trojan	TCP	5569
The Thing Trojan	TCP	6400
Indoctrination Trojan	TCP	6939
GateCrasher Trojan	TCP	6969,6970
Priority Trojan	TCP	6969
Remote Grab Troian	TCP	vdolive
ICKiller Troian	TCP	7789
iNi Killer Troian	TCP	9989
Acid Shivers Trojan	TCP	10520
COMA Trojan	TCP	10607
Senna Spy Trojan	TCP	11000,13000
Progenie Trojan	TCP	11223
GJammer Trojan	TCP	12076
Keylogger Trojan	TCP	12223
Proziack Trojan	TCP	22222
EvilFTP, UglyFTP Trojan	TCP	23456
Delta Source Trojan	TCP o UDP	26274
QaZ Trojan	TCP	7597
TrinOO DDoSTrojan	UDP	34555
Block SubSeven 2.1/2.2 Trojan	TCP	27374,2774
NetBlOS Networking	TCP o UDP	nbsession
Backdoor/SubSeven	TCP	1999,2773,54283,7215,Backdoor-g-1, Backdoor-g-3
Master Paradise	TCP o UDP	31,3129,40421,40422,40423,40426
Bla	TCP o UDP	1042,666
Portal of Doom	TCP o UDP	10067,10167,3700,9872,9873, 9874,9875
NetSphere	TCP	Porta da 30100 a 30102
NetMonitor	TCP	7300, 7301,7306, 7307, 7308
TransScout	TCP	Porta da 1999 A 2005
Doly	TCP	1010 1011 1012 1015
Donald Dick	TCP	23476,23477

Autore: Andrea Signorini

Web site: Sicurezza in Rete - http://digilander.libero.it/andreaing/