

# DShield.org

## Distributed Intrusion Detection System

Google

Web dshield.org Search

### IP Address Management

Rapid, scalable,  
policy-based  
allocation for  
GSM/UMTS  
networks  
[www.bridgewater-systems.com](http://www.bridgewater-systems.com)

### Noortech- Saudi Arabia

Access Control,  
Time &  
Attendance  
CCTV,  
Surveillance-IP  
Based Systems  
[www.noortech.com](http://www.noortech.com)

### Ip Video Surveillance

Find Suppliers of  
Network Security  
Cameras on  
Business.com.  
[www.business.com](http://www.business.com)

### BACnet Module

Add BACnet  
protocol to your  
Embedded  
Controller, Fast  
[www.ProtoCessor.com](http://www.ProtoCessor.com)

**Goto:** Forum List • Message List • New Topic • Search • Log In **Goto Thread:** Previous • Next

## Attackers botnet servers founded report .

Posted by: [ipsecurenetwork](#) (IP Logged)  
Date: May 6, 2006 08:01AM

Here i will post part of the list whit botnets founds attacking other networks around the world.

evidence for the FBI - CYBER - CRIME division.

Network services ]

\* Connects to "geo.argentinacorp.com" on port 7000 (IP).

\* Connects to IRC Server.

[ Security issues ]

\* Possible backdoor functionality [Authenticate] port 113.

[ Process/window information ]

\* Will automatically restart after boot (I'll be back...).

\* Attempts to open C:\WINDOWS\SYSTEM32\iexplore.exe mEITC:\SAMPLE.EXE.

Network services ]

\* Looks for an Internet connection.

\* Connects to "fenix.irc-argentina.com" on port 6667 (TCP).

\* Connects to IRC server.

\* IRC: Uses nickname SANDBOX803.

\* IRC: Uses username ezkie.

\* IRC: Joins channel #unc with password pass.

\* IRC: Sets the usermode for user SANDBOX803 to +xi.

Network services ]

\* Connects to "temple.irc-argentina.com" on port 6667 (TCP).

\* Connects to IRC server.

\* IRC: Uses nickname |80340.

\* IRC: Uses username ezkieya.

\* IRC: Joins channel #Msoft4 with password pretoriano.

\* IRC: Sets the usermode for user |80340 to +x.

\* IRC: Sets the channel mode for channel #Msoft4 to +nts.

Creates key "HKCU\Software\Microsoft\OLE".

\* Sets value "blah service"="evosys.exe" in key "HKCU\Software\Microsoft\OLE".

[ Network services ]

\* Connects to "temple.irc-argentina.com" on port 6667 (TCP).

\* Connects to IRC server.

[ Security issues ]

\* Possible backdoor functionality [Authenticate] port 113.

Connects to "temple.irc-argentina.com" on port 6667 (TCP).

\* Connects to IRC server.

\* IRC: Uses nickname NOR|80340.

\* IRC: Uses username ezkieya.

\* IRC: Joins channel #Msoft4 with password pretoriano.

\* IRC: Sets the usermode for user NOR|80340 to +x.

\* IRC: Sets the channel mode for channel #Msoft4 to +nts.

Network services ]

\* Connects to "temple.irc-argentina.com" on port 6667 (TCP).

\* Connects to IRC server.

[ Security issues ]

\* Possible backdoor functionality [Authenticate] port 113.

Network services ]

\* Looks for an Internet connection.

\* Connects to "elit.irc-argentina.com" on port 6667 (TCP).

\* Connects to IRC server.

\* IRC: Uses nickname tsyxyy.

\* IRC: Uses username tsyxyy.

\* IRC: Sets the usermode for user tsyxyy to +x.

\* IRC: Changes nickname to Lynx-176-1g2.

\* IRC: Joins channel #F&X.

\* IRC: Sets the channel mode for channel #F&X to +ntuk.

\* IRC: Sets the channel mode for channel #FX to +ntsk.

Network services ]

\* Looks for an Internet connection.

\* Connects to "fenix.irc-argentina.com" on port 6667 (TCP).

\* Connects to IRC server.

\* IRC: Uses nickname SANDBOX803.

\* IRC: Uses username ezkie.

\* IRC: Joins channel #unc with password pass.

\* IRC: Sets the usermode for user SANDBOX803 to +xi.

[ Network services ]

\* Looks for an Internet connection.

\* Connects to "run.ddosrules.com.ar" on port 6667 (TCP).

\* Connects to IRC server.

\* IRC: Uses nickname DDoS|803400248.

\* IRC: Uses username kagssjavmr.

\* IRC: Joins channel #@oot3d with password n0n3.

\* IRC: Sets the usermode for user DDoS|803400248 to -x+iB.

\* Attempts to delete share named "IPC\$" on local system.

\* Attempts to delete share named "ADMIN\$" on local system.

Creates value "Windows Config"="iexplore.exe" in key

```
"HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce".
* Creates value "Windows Config"="iexplore.exe" in key
"HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
[ Network services ]
* Connects to "haydee.ddosrules.com.ar" on port 7000 (IP).
* Connects to IRC Server.
[ Security issues ]
* Possible backdoor functionality [Authenticate] port 113.
Network services ]
* Looks for an Internet connection.
* Connects to "Goblins.Censor3d.Org" on port 6667 (TCP).
* Connects to IRC server.
* IRC: Uses nickname [ME]]803.
* IRC: Uses username ezkie.
* IRC: Joins channel #Eclipz3 with password eclipse123.
```

```
[ Network services ]
* Connects to "temple.censor3d.org" on port 6667 (TCP).
* Connects to IRC server.
* IRC: Uses nickname "[C]80340.
* IRC: Uses username ezkieya.
* IRC: Joins channel #Msoft5 with password pretoriano.
* IRC: Sets the usermode for user "[C]80340 to +x.
* IRC: Sets the channel mode for channel #msoft5 to +nts.
Network services ]
* Connects to "temple.censor3d.org" on port 6667 (TCP).
* Connects to IRC server.
* IRC: Uses nickname "[C]80340.
* IRC: Uses username ezkieya.
* IRC: Joins channel #Msoft5 with password pretoriano.
* IRC: Sets the usermode for user "[C]80340 to +x.
* IRC: Sets the channel mode for channel #msoft5 to +nts.
Network services ]
* Connects to "temple.censor3d.org" on port 6667 (TCP).
* Connects to IRC server.
* IRC: Uses nickname "[C]80340.
* IRC: Uses username ezkieya.
```

Personal information of the botnet owner.

names: Emilio Ribera  
Lastname: Ardiles  
adress 1: garibaldi 830  
Estate: Santiago del Estero  
Country: Argentina  
PHONE NUMBER: 4223457  
ZIP CODE: 4200

This information was provided by IPSecureNetWork abuse division.

**Options:** [Reply To This Message](#) • [Quote This Message](#) • [Report This Message](#)

**Goto:** [Forum List](#) • [Message List](#) • [Search](#) • [Log In](#)

Sorry, only registered users may post in this forum.

---

[ [Home](#) | [Login](#) | [What's New](#) | [Intro](#) | [Submit](#) | [Clients](#) | [Web Submission](#) | [All Reports](#) | [Mail Lists](#) | [Links](#) | [About](#) | [Privacy](#) ]

Contact [info@dshield.org](mailto:info@dshield.org) for more information.

last update: 10/Feb/2008 22:49  
DShield is a Servicemark of Euclidian Consulting