Damming The Flood: A Current Threat

Scott Molenkamp
Senior Research Engineer
Computer Associates

Agenda

- Introduction
  - Background
  - History
- Functionality
  - mIRC
  - Bot
- Targets / Methods used
- Problems
- The Future

Overview

- 'Global Threat' bot
  - Rising trend in malware
  - Powerful scripting language
  - Open source
  - Worm like ability
    - Windows flaws
    - Weak security

Background

- IRC – Internet Relay Chat
  - Created in 1988 by Jarkko Oikarinen
  - Real time chat
- Defined by RFC1459 in 1993
  - RFC2810
    - Architecture
  - RFC2811
    - Channel management
  - RFC2812
    - Client protocol
  - RFC2813
    - Server protocol

Background (cont)

- IRC bot
  - Non human client
  - Programmed responses to events
  - Recently more nefarious associations

Background (cont)

- Bot-net
  - Gathered under control of a common overseer
  - IRC is the communication medium

History

- mIRC was originally unpopular
  - Must be running
- Worms exploited flaw
  - Rectified in 5.3 (12/1997)
- More expansive commands
  - IRC related commands
  - Run local files
- IRCII client also abused

History (cont)

- Subseven 2.1 (November 1999)
  - Controlled via IRC bot
- Common method used today
  - Backdoors
  - IRC bots
- Compromised user query
  - Oct 2000

mIRC Functionality

- mIRC scripting
  - Powerful language
  - Wide ranging functionality
  - React to IRC server events (remotes)
- Raw socket connections
  - Version 5.5 (01/1999)
  - TCP / UDP

mIRC Functionality (cont)

- Many other scripting capabilities
  - String manipulation
    - Regular expressions
    - Tokenizers
  - File manipulation
  - Timers
    - Execute repeatedly with delay
    - timer1 0 10 /msg #chan1 hello
    - timer2 5 10 /msg #chan2 hello

mIRC Functionality (cont)

- Variables (Prefixed by %)
  - /set /unset
  - %variable
- Identifiers (Prefixed by $)
  - Return specific values
  - $null
- . prefix
  - Forces no output display

mIRC Functionality (cont)

- Access levels
  - Events
  - Users
    - /auser /ruser
- Restrict / Allow
  - Access to events

mIRC Functionality (cont)

- TEXT event
  - on <level> : TEXT <pattern> : <messagesource> : <commands>
  - on *:TEXT : !hello : * : { commands }
  - on 10:TEXT: !bye : # : { commands }
  - on 10 : TEXT : * : * {
    if ($1 == !exit) { commands }
    }

mIRC Functionality (cont)

- Other events
  - CONNECT
  - INPUT
  - DNS
  - START / LOAD
- Usage
  - On * : CONNECT : { commands }
  - On * : START : { commands }

mIRC Functionality (cont)

- Raw sockets
  - sockopen
  - sockclose
  - sockread
  - sockwrite
  - socklisten
  - sockaccept
  - sockudp
    - udpread

mIRC Functionality (cont)

- Raw sockets example

```
sockopen httpsock www.aavar.org 80

on * : sockopen : httpsock :
{
   sockwrite –n $sockname GET / HTTP/1.0
}
```

mIRC Functionality (cont)

- OS interaction
  - Execute local files
  - DLL and COM object calls
    - Scripting.FileSystemObject
    - WScript.Shell
    - mIRC plugins

Bot Functionality

- Bounce (BNC)
  - Not necessarily malicious
  - Protect against Denial of Service
- Cloning
  - Multiple connections to same IRC server
  - Can be used to flood

Bot Functionality (cont)

- Flooding
  - mIRC script
  - External programs
- Port Scanning
  - Gather information
  - Used in immediate or later attacks

Target Systems

- Windows based
  - Dependency on mIRC
  - Originally no ability to automatically spread

Methods

- Social Engineering
  - Private messages via IRC
  - Deceptive web pages
    - Downloader
    - Installer package

Methods (cont)

- Server Message Block (SMB)
  - Sharing
    - Files
    - Printers
    - Serial Ports
  - Example protocols
    - TCP/IP
    - NetBIOS

Methods (cont)

- Prevalence of Windows XP
  - PsExec.exe
    - www.sysinternals.com
  - Weak Passwords
  - Fuelling the rise

Methods (cont)

- Exploit
  - IIS Web Server Folder Traversal (MS00-78)
- Trojan protocols
  - SubSeven
  - NetDevil

Components

- Minimal set
  - Copy of mIRC
    - Potentially modified packed or renamed
  - At least one malicious script
    - Probably named mirc.ini
  - Program to hide mIRC GUI
    - HideWindow

Components (cont)

- More expansive set
  - Many scripts
  - 3rd party programs
  - Other malicious programs
  - Servers
    - ftp
    - http
    - xdcc

Components (cont)

- Single install file
  - Setup Factory
  - Instyler
  - Install Wizard
  - PaquetBuilder*
  - GSFx Wizard*
  - NSIS
  - SFXMaker
  - RARSFx

Elements & Goals

- Resources
  - Diskspace
  - Anonymity
  - Illegal software / pornography distribution networks
  - Bandwidth

Elements & Goals (cont)

- Serv-U ftp server
- Vulnerability scanners
- Precompiled flooders
- Clean software
- Other non-malicious programs

Problems

- Many components
  - Some innocuous
- mIRC client
  - Renaming
    - Sanity check (mirc.exe, mirc32.exe)
  - Packing
  - Modification

Problems (cont)

- Modified mIRC client
  - Default loaded script name
  - mirc.ini found in non-standard directories may indicate compromise
  - Removal of resources
  - Registry key modification

Problems (cont)

- Categorising
  - Naming scheme
    - Open source
    - Reused
    - Modified
    - Rearranged
  - Varied platform prefix
    - Win32, BAT, VBS, IRC

The Future

- Prevalence is increasing
- Obfuscation
- Other spreading methods
  - SMTP
  - New exploits
- Coupled with
  - root kits
  - Firewall bypass / removal

Conclusion

- Rise in soft targets
  - Bandwidth to burn
- Immeasurable number of bot-nets
- Securing administrator accounts