EXHIBIT 3

ngrBot v1.1.0.0 - (Updated 16.05.2011) Thread Options

03-01-2011, 04:56 AM (This post was last modified: 05-16-2011 02:46 AM by edditer.) Post: #1

edditer
take a knee spaceman, take a knee..

Posts: 1,214
Joined: Jun 2010
Vouch:

As a member of the ngrBot development team, I'm proud to present you...

v1.1.0.0 (May 15th 2011)

Information

ngrBot's core is an advanced ring3 (usermode) system-wide injection and hooking engine. The system uses techniques similar to those of ZeuS and SpyEye. (This is not a banking bot!)

The bot will run on Windows 2000, XP, Vista, 7, Server 2003 (and R2) and Server 2008 (and R2). It also supports 64-bit operating systems, but currently can only inject into 32-bit processes.

Change Log / Updates

v1.1.0.0 (16.05.2011)

v1.0.3.0
Spoiler (Click to View)

Installation

The bot is designed to install silently and successfully on a Windows Vista/7 system on a limited account with UAC enabled. It installs to the user's Application Data directory with a pseudo-randomly generated filename and creates a registry key to ensure the bot runs at startup. The bot fully supports Unicode characters and will therefore run on Asian and Eastern European systems.

IRC Nickname Generation

Code:
```
<new>{<COUNTRY>|<OPERATING SYSTEM><user type>}<random letters>
```

An example would be: n{RU|XPa}abcdefg

Modules & Features

ROOTKIT
- The rootkit module will attempt to hide the bot's registry startup key as well as the bot file.

RUSKILL
- The Ruskill module will, if enabled for a download command, monitor the downloaded file as it executes. Ruskill will flag any files that it copies itself to or creates to be deleted at the next system reboot.

PROACTIVE DEFENSE (PDEF+)
- The PDef module is an advanced threat detection and removal system. It monitors a range of file and networking APIs to detect and neutralize other threats that are running on the system. Currently this module can detect, block and remove malware that spreads via USB drives, browser exploit packs, and bots that use IRC to communicate.

DNS MODIFIER
- This module can block domains from being accessed and redirect domains/IP addresses to others.

SLOWLORIS
- This module is for webservers running Apache HTTPd. It is designed to use low bandwidth and to maintain connections as long as possible, thus consuming all available resources.

SYN FLOOD
- The syn flood module is good for webservers that Slowloris fails to take down.

UDP FLOOD
- This module is ideal for taking home connections offline.

INTERNET EXPLORER LOGIN GRABBER
- This module hooks wininet.dll and analyzes POST requests made by the IE web browser to capture usernames and passwords on the fly.

FIREFOX LOGIN GRABBER
- This module hooks nspr4.dll and analyzes POST requests made by the Firefox web browser to capture usernames and passwords on the fly.

FTP LOGIN GRABBER
- The FTP module hooks ws2_32!send to grab the FTP logins as they are used.

USB SPREADER
- Waits for USB drives to be inserted and then attempts to infect them using multiple .lnk methods and obfuscated autorun.

MSN SPREADER
- This module hooks ws2_32!send to detect MSN messages being sent. It will then monitor outgoing messages and wait for the spoofed number of messages to be sent before replacing one with the set spread message. It has been tested with the msnp10 and msnp21 protocols with msnmsgr.exe, wlcomm.exe, pidgin.exe, and msnmsgs.exe.