CERT Incident Note IN-2002-03: Social Engineering Attacks via IRC and Instant Messaging

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Social Engineering Attacks via IRC and Instant Messaging

Release Date: March 19, 2002

A complete revision history can be found at the end of this file.

Systems Affected Systems running Internet Relay Chat (IRC) or Instant Messaging (IM) clients

Overview

The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner.

I. Description

Reports received by the CERT/CC indicate that intruders are using automated tools to post messages to unsuspecting users of IRC or IM services. These messages typically offer the opportunity to download software of some value to the user, including improved music downloads, anti-virus protection, or pornography. Once the user downloads and executes the software, though, their system is co-opted by the attacker for use as an agent in a distributed denial-of-service (DDoS) network. Other reports indicate that Trojan horse and backdoor programs are being propagated via similar techniques.

Here is an example of one such message:

> *You are infected with a virus that lets hackers get into your machine and read ur files, etc. I suggest you to download [malicious url] and clean ur infected machine. Otherwise you will be banned from [IR C network].*

This is purely a social engineering attack since the user's decision to download and run the software is the deciding factor in whether or not the attack is successful. Although this activity is not novel, the technique is still effective, as evidenced by reports of tens of thousands of systems being compromised in this manner. See IN-2000-08: Chat Clients and Network Security for additional information.

II. Impact

As with any DDoS tool installation, the impact is twofold. First, on systems that are compromised by users running untrusted software, intruders may

- exercise remote control
- expose confidential data
- install other malicious software
- change files
- delete files

These risks are not limited to the installation of DDoS agents. In fact, any time a user runs untrusted software these same dangers are present.

The secondary impact is to the sites targeted by the DDoS agents. Sites undergoing a DDoS attack may experience unusually heavy traffic volumes or high packet rates, resulting in degradation of services or loss of connectivity altogether.

III. Solutions

Home users

Run and maintain an anti-virus product

The malicious code being distributed in these attacks is under continuous development by intruders, but most anti-virus software vendors release frequently updated information, tools, or virus databases to help detect and recover from the malicious code involved in this activity. Therefore, it is important that users keep their their anti-virus software up to date. The CERT/CC maintains a partial list of anti-virus vendors at

> *http://www.cert.org/other_sources/viruses.html#VI*

Many anti-virus packages support automatic updates of virus definitions. The CERT/CC recommends using these automatic updates when available.

Do not run programs of unknown origin

Never download, install, or run a program unless you know it to be authored by a person or company that you trust. Users of IRC and IM services should be particularly wary of following links or running software sent to them by other users, as this is a commonly used method among intruders attempting to build networks of DDoS agents.

Understand the risks

Users are encouraged to review our "Home Network Security" tech tip, which provides an overview of risks and mitigation strategies for home users.

> *http://www.cert.org/tech_tips/home_networks.html*

Sites

Site administrators are encouraged to review our report on denial of service attack technology trends, as well as our recommendations for managing the threat of denial-of-service attacks.

Trends in Denial of Service Attack Technology

> *http://www.cert.org/archive/pdf/DoS_trends.pdf*

Managing the Threat of Denial-of-Service Attacks

> *http://www.cert.org/archive/pdf/Managing_DoS.pdf*

Author(s): Allen D. Householder

Revision History

```
March 19, 2002: Initial release
```