

Exploitable mirc, or a trojan ?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2002-02/1008.html>

From: -=JinXsta=- (JinXy@dna.ie)

Date: 02/27/02

From: "=-JinXsta=-" <JinXy@dna.ie>
To: <security-basics@securityfocus.com>
Date: Wed, 27 Feb 2002 19:20:29 -0000

I lurk alot here and I know a fair amount about computer security although I still thought I would hit you with this question.

I have a friend on mirc that is being "penetrated" in someway. This goes as follows...

The person quits with a quit message of (I am lame, I bow down to the master...")

This message is not generic as it has happened on two occasion with both different quit messages.

The user is also unaware that this is happening, he just sees a disconnect message.

After this has happened, his computer seems to function correctly, until when he reboots his "c: drive is inaccessible" , his only "layman" solution is to reinstall windows.

He is on windows98 incidently, although it also happened with WindowsME

The first time this ocured, I told him not to install any third party services, such as icq etc. and just have his mirc – which again I told him to download 6.1 in case it was the mirc service that was being comprimised. I also told him not to use any canned nukes/programs as they are usually infected within themselves.

However, he followed my advice and it happened to him again. My first thought is that is a trojan, especially after the TCP probes(shown below), his walls (zone alarm pro and neo watch) logged just before this happened. But, it must be a relatively advanced trojan as its getting past his wall and due to the random nature of the probes it seems that the person is not directly connecting to the trojan server and is unaware of what server they are actually connecting to. I suspect the person is a big script kiddy, but I cannoy confirm this.

SecurityFocus BASICS: Exploitable mirc, or a trojan ?

I have also suggested to him, to get filemon and regmon on his system so as he can see when anything is being changed that he is unaware of, which he is going to do now.

I also checked the IP of the probes and they seem to be coming from a shell account, so I am also guessing that they may be running a sploit or scanner from a shell.

he is also running NortonAntivirus2002 , msn

So.. I ask you...

What other possibilities are there of the comprmise?

How could he detect the comprmise?

How could he prevent the comprmise?

What is this P+P bug within all versions of windows?

-tom

1 The firewall has blocked Internet access to your computer (HTTP) from 66.28.178.10 (TCP Port 2165) [TCP Flags: S].

Time: 2/25/02 12:23:06

2 The firewall has blocked Internet access to your computer (TCP Port 1080) from 63.169.40.130 (TCP Port 4833) [TCP Flags: S].

Time: 2/25/02 12:30:14

3 The firewall has blocked Internet access to your computer (HTTP) from 63.169.40.130 (TCP Port 1506) [TCP Flags: S].

Occurred: 2 times between 2/25/02 12:30:58 and 2/25/02 12:31:32

4 The firewall has blocked Internet access to your computer (TCP Port 3128) from 63.169.40.130 (TCP Port 2293) [TCP Flags: S].

Occurred: 4 times between 2/25/02 12:31:44 and 2/25/02 12:32:18

5 The firewall has blocked Internet access to your computer (TCP Port 8080) from 63.169.40.130 (TCP Port 3452) [TCP Flags: S].

Time: 2/25/02 12:32:30

6 The firewall has blocked Internet access to your computer (TCP Port 81) from 63.169.40.130 (TCP Port 4571) [TCP Flags: S].

Time: 2/25/02 12:33:16

Exploitable mirc, or a trojan ?

SecurityFocus BASICS: Exploitable mirc, or a trojan ?

7 The firewall has blocked Internet access to your computer (TCP Port 8081) from 63.169.40.130 (TCP Port 1609) [TCP Flags: S].

Time: 2/25/02 12:34:02

8 The firewall has blocked Internet access to your computer (Telnet) from 63.169.40.130 (TCP Port 2558) [TCP Flags: S].

Time: 2/25/02 12:34:48

9 The firewall has blocked Internet access to your computer (TCP Port 1562) from irc.adultchatnetwork.com (64.38.226.9) (TCP Port 7000) [TCP Flags: AP].

Occurred: 2 times between 2/25/02 12:43:14 and 2/25/02 12:45:36

10 The firewall has blocked Internet access to your computer (TCP Port 1563) from irc.adultchatnetwork.com (64.38.226.9) (TCP Port 7000) [TCP Flags: AP].

Occurred: 2 times between 2/25/02 12:44:46 and 2/25/02 12:45:08

11 mIRC tried to send data to the Internet (64.38.226.9), but was denied access by the Internet Lock

-
- **Previous message:** Chris Chandler: "RE: The Best Network Scanner?"
 - **In reply to:** jrd@gerdesas.com: "Re: O-Mail, Or How Paranoid Are We Today."
 - **Next in thread:** Demitrious S. Kelly: "RE: O-Mail, Or How Paranoid Are We Today."
 - **Messages sorted by:** [date] [thread] [subject] [author] [attachment]