

Re: Is secedit.exe left by a hacker?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-11/10780.html>

From: Jim Matthews (jim_matt@swbell.net)

Date: 11/02/02

From: "Jim Matthews" <jim_matt@swbell.net>

Date: Sat, 2 Nov 2002 08:51:27 -0800

The Linksys I am using is a BEFSR11.
The Firmware revision is 1.38.5 from April 12, 2001.

I am also looking into the other programs you mentioned
to scan my computer.

I will post my findings here for anyone who is interested
and following this.

>-----Original Message-----

>

> "Jim Matthews" <jim_matt@swbell.net> wrote in message
> news:0c9601c281d1\$737a7b70\$39ef2ecf@TKMSFTNGXA08...

>> Recently I noticed a lot of net activity on my LAN from
>> my W2K system. When I looked to see what was going
on, I

>> found a program called secedit.exe running out of
>> WINNT\System32. When I looked further, I saw a file
>> called secedit.sdb. I also found a file called 445.txt
>> which seems to contain a list of IP addresses that were
>> tested on port 445.

>>

>> There are times when I have restarted my computer, I
>> have noticed a command window with a title of secedit.

>>

>> I have a Linksys router that I use as a firewall to my
>> DSL connection so I thought I was pretty safe.

>>

>> Can anyone tell me if this is legitimate or has a
hacker

>> gotten in? Also, is there anything I need to set on
the

>> Linksys that is not a default setting?

>

> You don't mention which Linksys you are using. Some of
them don't do much

>to block outbound traffic, so that if you are infected
by a virus or worm or
>irc worm or trojan, a hacker can remotely control your
computer despite your
>firewall.
>
>You may want to download a free syslog client to capture
the logs from your
>firewall. By default, Linksys logs disappear after
about 10 minutes, which
>isn't very good if you've been hacked
a tool to look for
>open ports, such as Vision or Fport from
www.foundstone.com/knowledge or
>Pstools / Pslit from www.sysinternals.com
>
>For more extensive information about looking for
Trojans, backdoors and
>other hacker tools, see the section in this FAQ
entitled "How can I tell if
>I've been hacked?"
>
>=====

>
>Which firewall should I choose? Which firewall is the
best?
>
>A: The answer to this question varies depending on your
computer systems,
>your security requirements and your personal
preferences. Below are some
>firewalls and other forms of firewall-like packet
filtering:
>
>NO MATTER WHICH FIREWALL YOU CHOOSE...
>No matter which firewall you choose, you should
seriously consider
>downloading and installing MyNetWatchman or Dshield.
These are free programs
>that work with your firewall software or hardware to
automatically report
>hacking attempts to the hacker's ISP. You get to see
information about
>whether that IP address has been used to scan or hack
other computers, or
>whether it might be targeting just your computer. You
also get to see
>whether the ISP has responded or taken action against
the offending user.
>You can get this software at one of the links below:
>

>www.mynetwatchman.com
>www.dshield.org
>
>*Also, no matter which firewall you choose, the lists below of port numbers*
>*for common software services may be helpful when configuring your firewall*
>*or when trying to monitor the firewall logs for signs of intrusion:*
>
>www.iana.org/assignments/port-numbers
>www.iisfaq.com/default.asp?View=P106
>
>
>**FIREWALL SOFTWARE:**
>www.sygate.com [*free for non-commercial use, also works like a sniffer*]
>www.kerio.com [*free for non-commercial use*]
>www.agnitum.com [*free for non-commercial use*]
>www.zonealarm.com [*free for non-commercial use, also blocks pop-ups*]
>www.iss.net [*Black Ice*]
>www.symantec.com [*Norton*]
>www.webattack.com
>www.download.com
>www.tucows.com
>[*Windows XP users can also consider using the ICF firewall that comes with*
>*XP, more info below*]
>
>**FIREWALL DEVICES [HOME / SOHO]:**
>www.linksys.com [*starts around \$70 US*]
>www.netgear.com [*starts around \$70 US*]
><http://search.ebay.com/search/search.dll?query=firewall>
>[*prices on new and*
>*used firewalls*]
>
>
>
>
>
>
>
>
>
>