

Re: Scanning a Mapped Drive on a LAN

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-02/1064.html>

From: Leythos (void_at_nowhere.com)

Date: 02/25/04

Date: Wed, 25 Feb 2004 15:45:57 GMT

In article <QP2%b.1501\$Er4.28@fe2.columbus.rr.com>, jaygreg90@hotmail.com says...

> *Leythos, you seem to be a bit more analytical than "Shoot from the hip"*
> *johns. What's you're take on my situation please. I have the original issue*
> *resolved; the Colonel made sense and I've decided to simply schedule my*
> *scans of one machine with reminders on my Outlook calendar. But that leaves*
> *me with the issue of these other programs I think I need – or something*
> *better if I find it; SpyBot and Ad-Ware. Got a comment or recommendation?*

I'm not sure I understand the "reminders on my OL calendar" bit? If you do a live-update every day, and run a full scan every evening, and leave the AV product active all the time, you can't really ask for more.

As for SB and AW, I've only used SBS&D from www.safer-networking.net, there is a clone-type Spybot that's a rip-off of SBS&D, so make sure you have the real one.

I've found that SBS&D finds about 95% of the things out there that don't like you, but, since it's a free application I can't complain about it.

What I do is run it about 4 times, making sure I've downloaded the updates before I run it. I boot to safe mode on the last scan and check again – this is on customers systems, not one my own systems.

I also edit the registry to remove items from the RUN, RUNONCE sections that are not needed and I also search for items in the registry that may be hidden.

I run NAV Small Business Edition 8.1 on my computers – smaller foot print, faster, never failed me yet.

> *Regarding the misread by "johns", I was told long ago I had little to be*
> *concern with as a simple home LAN user with my machines behind a router. Two*
> *of the machines run firewalls, the WIN95 doesn't. In your opinion, an I*
> *reasonably well protected? IF not, I'd appreciate hearing something*
> *constructive in a straightforward manner. Use polysyllabic words to*
> *disguise the conversation from "johns" if you wish.*

alt.computer.security: Re: Scanning a Mapped Drive on a LAN

In the old days I had a simple Linksys Router BEFSR41 and a good NAV product (not NIS or NPF) running on my computers, never had a problem. When I started a server farm I bought a WatchGuard Firebox II unit and I've removed the BEFSR41. I also run Wall Watcher on one of the systems that sits behind the Linksys units – this lets me see all in/outbound so that I can tell if a machine has been compromised based on traffic.

Since I have a block of IP's I setup a couple development areas where I attach a BEFSX41 router to an IP and then have several servers and workstations behind that. This lets me build applications without the risk of compromising my LAN (the FB II network) should something go wrong. Again, each system in running a licensed copy of SBE 8.1 full time.

It doesn't make any difference what OS you run, Linux, Windows, MAC, etc... there are things out there that, once they reach you, will compromise your machine. A border device like a router with NAT is a first step in blocking intruders from even gaining access to your computers. A second step is a quality AV product. A final step is to understand the issues with your use of the internet, browsing, usenet, email, etc...

As an example, I use IE 6 because I write .Net code and need IE 6 for some of the features, but I secure IE 6 in a manner that I feel safe in using it on the generic web – I do not visit warez sites or porn sites or other places that are high-risk areas. For usenet I use Gravity and feel very secure using it. For email I use MS Outlook, BUT, I have my own email servers and all in/out bound email is scanned, stripped of unapproved attachments, virus's removed, and any files that are unknown in the attachments are removed. I also don't open email from people I don't know.

Here is something I sent to customers and friends about IE the other day:

The easiest way to clean a machine is to download SpyBot Search and Destroy from <http://www.safer-networking.org/index.php?page=download> and the update and run it several times (download button is about half-way down the page).

Once you get your machine cleaned, you can make the following changes to your Internet Explorer settings to help keep web sites from installing bad things on your computers.

There are a couple simple things that you can do if you are using IE, they make browsing a little more of a challenge, but they make it more secure and still provide full ability on sites you trust:

- 1) Open IE, select TOOLS, Internet Options
- 2) Select Security TAB
- 3) Select "Internet" globe

Re: Scanning a Mapped Drive on a LAN

alt.computer.security: Re: Scanning a Mapped Drive on a LAN

- 4) Click DEFAULT LEVEL, then SELECT HIGH
- 5) Select "Custom Level"
- 6) Select "Scripting – Active Scripting – Prompt"
- 7) Click OK
- 8) Select "Trusted Sites Check Mark Circle"
- 9) Select "SITES", uncheck "Require Server Verification" – you will be adding the normal and secure sites in here that you trust, if you don't uncheck this you can't enter non-secure sites in this list.
- 10) Type "<http://v4.windowsupdate.microsoft.com>" in the ADD box and click ADD
- 11) Type "<http://Windowsupdate.microsoft.com>" in the ADD box and click ADD, click OK to close window
- 12) Click "Default Level" then change to "Medium".
- 13) Select "Privacy" tab, set to MEDIUM HIGH
- 14) Select "General" tab, select "Temporary Internet Files – Settings"
- 15) Select "Every visit to the page"
- 16) Select 20MB for the temp internet files size, click OK
- 17) Select "Advanced" Tab
- 18) Uncheck both "Enable Install On Demand" items
- 19) Uncheck "Enable third-party browser extensions"
- 20) Uncheck "Play Animations, sounds, videos in web pages"
- 21) Select/Check "Empty Temporary Internet file folder..."
- 22) Click OK to close the settings window

Now, when you browse to a site you want to trust, it's not going to work, you are going to have to ADD the site to the TRUSTED SITES in the OPTIONS / SECURITY tab. This can be a real pain, but it can save your butt when it comes to sites that can compromise your system.

You will find that after the first week that you are not adding sites to the list any more and that you're experience is a lot nicer, less pop-ups, and less chance for something to hack your browser.

Don't forget, you should only ADD TRUSTED SITES to the list. Even if you make a mistake, we set the TRUSTED SITES to MEDIUM in stead of it's default LOW, but you really want to limit the ones you add to verifiable commercial quality sites.

--
--

spamfree999@rrohio.com
(Remove 999 to reply to me)