

Re: Ping Malke

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-06/0121.html>

From: David H. Lipman (DLipman~nospam~_at_Verizon.Net)

Date: 06/08/05

Date: Wed, 8 Jun 2005 11:00:22 -0400

From: "Zvi Netiv" <support@replace_with_domain.com>

| "David H. Lipman" <DLipman~nospam~@Verizon.Net> wrote:

|

>> *Hi Malke:*

|

| Would you mind for others' comments? ;-)

|

>> *I have a NEW utility. It combines; Trend Sysclean, the McAfee Command Line Scanner and*

>> *the Sophos Command Line Scanner all in one menu driven utility.*

>>

>> http://www.ik-cs.com/programs/virttools/Multi_AV.exe

>>

>> *After you execute and extract the files, look at the PDF help file.*

>> *"C:\AV-CLS\Multi AV Command Line Scanner.PDF"*

>>

>> *Let me know what you think and how it can be improved.*

|

| Nice!

|

| A couple of comments, to consider for further versions:

|

| I personally hold that cleaning under Windows should be conducted from self
| boot, from the installed OS. Yet since you mention the option of clean booting
| for Win 9x/Me, by aid of boot disk made from www.bootdisk.com, then be aware
| that there exists a free (for private use) bootdisk to NTFS from DOS, with full
| read-write access, from <http://www.datapol-technologies.com/dpe/recovery/ntfs/>

|

| In your instructions (PDF file), I would recommend that anything you suggest
| running from safe mode, be run from safe mode WITH COMMAND PROMPT instead.

| The reason is that many malware load by injecting through Explorer, that loads
| in safe mode just as well. You have my permission to include the ToggleMode
| utility in your package, if required. You may need it to start Win 9x/Me in
| safe mode with command prompt (a mode they lack inherently). From
| www.invincible.com/item/80

|

| Regards, Zvi

| --

microsoft.public.security.virus: Re: Ping Malke

| NetZ Computing Ltd. ISRAEL www.invincible.com www.ivi.co.il (Hebrew)
| InVircible Virus Defense Solutions, ResQ and Data Recovery Utilities

Hi Zvi:

I relish your comments. Thanx !
I'll look into those ideas you have provided.

You mentioned -- "...malware load by injecting through Explorer..." The script will look at the "shell=explorer.exe" directive of the Registry in NT and in SYSTEM.INI in Win9x/ME. If there is malware being chained off of explorer such as...

shell=explorer.exe malware.exe

When you run the script in Normal Mode to update the Command Line Scanner (CLS), it will properly set the shell= directives back to "shell=explorer.exe" and should not load the malware again when rebooted into Safe Mode.

--

Dave

<http://www.claymania.com/removal-trojan-adware.html>

<http://www.ik-cs.com/got-a-virus.htm>