

Re: MAKING YOUR COMPUTER SYSTEM SECURE AFTER IT'S BEEN COMPROMISED

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-08/0911.html>

From: CyberDroog (*DoILookLikeIWantSpam?_at_duh.net*)

Date: 08/13/03

Date: Wed, 13 Aug 2003 07:32:20 GMT

On Wed, 13 Aug 2003 04:54:36 +0400, Tracker
<"snailmail(remove)222000"@yahoo.com> wrote:

>Copyright 2003 by Debbie X. All rights Reserved. No part of this
>publication may be reproduced in any form or by any means, or stored in
>a data base or retrieval system, without prior written permission of the
>publisher. You may pass along this information, but give credit where
>credit is due.

Debbie, please get a clue. Usenet IS a data base and retrieval system. I hope you gave EasyNews written permission since I just pulled your post from their system.

And you know what? I'm about to quote your copyrighted work at will.

>I highly recommend keeping the hacked hard drive and purchasing a new
>one.

Yeah, like *you* could afford to do that. Perhaps you should upgrade from Windows 95 first...

>Of course you could mirror the drive, but you still need a
>replacement drive to perform this task. You can't produce the same
>results by replicating files versus viewing the actual hard drive
>itself. If your system was used to attack and crash a Network, or
>System, you have proof for the FBI or any Law Enforcement Agency. This
>would show you were not involved in any illegal activities until you
>discovered your system was hacked.

Jesus Debbie, have you never heard of Ghost? You can make a bit for bit copy if the hard drive.

Oh God, now she *has* heard of Ghost... I hope I'm not responsible for a new chapter of drivel in her "book".

>The proper method is to re-format your hard drive, and install from

*>original CD-ROM. To safe guard against software manufacturer employee
>malicious activity always virus check your CD-ROM. Not too long ago, I*

Virus check your CD-ROM with what? A CD from a software vendor? What if the virus scanner vendor has a malicious employee?

Frankly Debbie, you personally would probably do better to scan your *vibrator* for viruses, bacteria, lice and ticks. Some little critter has burrowed under your skin and is messing with your mind.

*>Virus check all floppy disks because hackers DO install a Backdoor,
>Trojan Horse, or Virus on disks. They enjoy doing this especially when
>you're online using your computer, with a floppy in the drive. My
>preference is to obtain a replacement CD-ROM if your software
>applications are on a floppy. What concerned me most is a Backdoor was
>planted in a .zip file and unopened. Norton's Anti-virus application
>couldn't detect it. Let's one day you come along and for no reason, you
>decide to open this .zip file, voila, the Backdoor is unleashed.*

Debbie, get yourself a copy of Norton Anti-Virus before you talk about it. You could be sued for libel. Norton can scan .zip files, and it will detect viruses/trojans if an attempt is made to extract the files.

*>A number of Internet Service Providers allow free dial-up access with
>DSL and Cable connections. Note: Hackers are taking advantage of your
>canceled accounts even when they were closed. Until certain Internet
>Services Providers and Telecommunication Companies correct their major
>error; telecon your ISP and ask them to change your password since
>malicious hackers are abusing your canceled account, holding you liable.*

You aren't liable if your account is canceled moron. In case you didn't know, you aren't liable for everything done with every old phone number you ever had either.

*>Disabling all unnecessary Window Services will assist in making your
>computer system secure. How to accomplish this task is presented under
>"Windows Services you might want to disable". If running any type of
>Server, update the latest application patches.*

Like you have ever even seen a server...

*>Once you are able to view all Hidden Files and Folders, it would be
>smart to make a backup copy of your registry. To perform this, do the
>following:*

- >*
- >A. Select Start, Run, type in Regedit, and press enter.*
- >B. Then Select Registry, Export Registry File*
- >C. In the box, type a name like "3-21-02.txt"*
- >D. Select Save.*

>

>You can open this file in any text editor. What you want to do first is

>check the bottom of the file. Hardware/Application/Device Driver

The bottom of the file? That is insane. A registry is composed of hives and keys. It isn't a linear format.

--

FAITH, n. Belief without evidence in what is told by one who speaks without knowledge, of things without parallel.

- Ambrose Bierce