

Re: Download freeware RKR scanning software (detect Sony rootkit & others)

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-11/0524.html>

From: karl levinson, mvp (levinson_k_at_despammed.com)

Date: 11/20/05

Date: Sun, 20 Nov 2005 08:39:01 -0500

<pamelafiischer@yahoo.com> wrote in message
news:1132469140.484946.192840@g14g2000cwa.googlegroups.com...

- > C:\Documents and Settings\Administrator\Local Settings\Application
- > Data\Mozilla\Firefox\Profiles\p72bk7em.default\Cache\33084D91d01
- > 11/19/2005 10:24 PM 16.84 KB Visible in directory index, but not
- > Windows API or MFT.
- > C:\Documents and Settings\Administrator\Local Settings\Application
- > Data\Mozilla\Firefox\Profiles\p72bk7em.default\Cache\9ED97802d01
- > 11/19/2005 10:24 PM 37.73 KB Visible in directory index, but not
- > Windows API or MFT.

All of the registry nulls look OK to me. I would focus first on hidden files than on hidden registry values. The two hidden files above were the only ones that might merit further investigation. I'm not positive these two files are signs of anything important.

Note that there are supposedly root kits that can disable Rootkit Revealer and make it fail to detect hidden files. For a second opinion, you might also search for rkdetect in www.google.com and run that as well. I think it's a little harder to run than just double-clicking on it, I think you have to may run it at the command line. Using the same method to find and run Hijack This! and post the logs to their web site may also be helpful.

- > Note that I removed the numbers for fear they may have contained
- > personal identification information (what are those 8-4-4-4-12
- > character numbers anyway?).

Depending on where they are in the registry, those numbers generally uniquely identify a program, user or other object. Here they are CLSID or Class ID numbers, which Microsoft defines as:

<http://www.microsoft.com/technet/prodtechnol/host/proddocs/appint/asdefclassid.msp>

A universally unique identifier (UUID) that identifies a COM component. Each

microsoft.public.security: Re: Download freeware RKR scanning software (detect Sony rootkit & others)

COM component has its CLSID in the Windows Registry so that it can be loaded by other applications.