

Re: RootKit Revealer Tool

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-02/24035.html>

From: Dan (*spamyou_at_user.nec*)

Date: 02/23/05

Date: Wed, 23 Feb 2005 06:19:11 -0700

Please tell me how you keep your system(s) secure and I will try to the best of my ability to help you solve your problem(s) or questions.

Security on Electronics is my Passion

GodSpeed!!!

"R. McCarty" <PcEngWork-NoSpam_@mindspring.com> wrote in message news:zs_Sd.4949\$Ba3.211@newsread2.news.atl.earthlink.net...

: Yes, it's a little on the cryptic side. What I don't understand is how
: RootKits can get past Windows File Protection. I would assume it
: doesn't change the identifier that WFP monitors. Still, it seems like
: a big challenge, since the normal checks-&-balances for locating &
: removing Malware don't apply.

: On my system it picks up about 8 items that I'm researching a little
: more to determine what is going on. Maybe we need a different form
: of WGA (Windows Genuine API's).

:
:

: "Melelina" <Melelina@medscape.com> wrote in message

: news:ecPk2\$ZGFHA.936@TK2MSFTNGP12.phx.gbl...

: >I ran it already. Hard to understand the output. If you have KAV 5.0 you
: > can't use the tool as it identifies all files as being discrepancies.

: >

: > "R. McCarty" <PcEngWork-NoSpam_@mindspring.com> wrote in message

: > news:HhZSd.4767\$Ba3.12@newsread2.news.atl.earthlink.net...

: >> For anyone who's been reading up on the potential, newest threat to
: >> Windows (Rootkits). SysInternals has created/posted a tool that will
: >> scan your system.

: >> <http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml>

: >> (on a Technical Savvy scale of 10 - this one is about 8.5)

: >>

: >> Rootkits is basically a way for Malware, etc to "Hide" itself within
the

: >> OS, so normal scanning tools and detectors are unable to locate them.

: >> If I understand it correctly, the Malware actually hooks into system
code

microsoft.public.windowsxp.general: Re: RootKit Revealer Tool

: >> making it almost invisible to normal scanning methods. In one article it
: >> indicates the only removal process will be a full system re-install !
: >>
: >> It worthwhile to spend some time researching this issue, as it won't be
: >> long before this threat becomes more prevalent.
: >>
: >>
: >>
: >
: >
:
: