

Re: [Full-Disclosure] Rootkit For Spyware? Hide your adware from all Adware removers and Anti-viruses

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-09/0951.html>

From: GuidoZ (uberguidoz_at_gmail.com)

Date: 09/23/04

To: "macmanus@gmail.com" <macmanus@gmail.com>

Date: Thu, 23 Sep 2004 13:04:11 -0700

I guess my comment further down was overlooked:

GuidoZ said:

> *To save someone else from saying this, I'll reply to my own comment. =)*

>

>> *I've yet to find a rootkit, spyware, or malware that is*

>> *COMPLETELY hidden, in every aspect, from the user.*

>

> *Well, DUH. How could you find it if it was COMPLETELY hidden? ;)*

> *Clarification: The user and a sysadmin that has a clue are two very*

> *different people.)*

--

Peace. ~G

On Thu, 23 Sep 2004 14:34:33 -0400, macmanus@gmail.com

<macmanus@gmail.com> wrote:

> Because you have never seen it means it doesn't exist? If it was

> "COMPLETELY hidden", maybe you just never found it.

>

>

>>> It is quite possible to hide processes, reg keys and files, and is often
>>> done by various malware.

>>

>> Aye. I didn't word my statements correctly. (Was tired... =P) You are
>> very much correct.

>>

>> I guess I was trying to speak along the lines of AV detection and
>> forensics. I've yet to find a rootkit, spyware, or malware that is
>> COMPLETELY hidden, in every aspect, from the user. There is always a
>> way to find it. Granted, they can bypass the "usual means" (regedit,
>> taskmanager, etc) in Windows, however there are specialized tools
>> (process viewers for example) that show hidden processes. What I meant
>> to express is they seem to claim being able to hide from everything.
>> (Even if an AV solution detected the very program they use as an
>> installer.) That, I doubt.

>>

>>

>> To save someone else from saying this, I'll reply to my own comment. =)

>>

Re: [Full-Disclosure] Rootkit For Spyware? Hide your adware from all Adware removers and Anti-viruses

Full-Disclosure: Re: [Full-Disclosure] Rootkit For Spyware? Hide your adware from all Adware removers and Anti-viruses

```
> > > I've yet to find a rootkit, spyware, or malware that is
> > > COMPLETELY hidden, in every aspect, from the user.
> >
> > Well, DUH. How could you find it if it was COMPLETELY hidden? ;)
> > Clarification: The user and a sysadmin that has a clue are two very
> > different people.)
> >
> > --
> > Peace. ~G
> >
> >
> > On Thu, 23 Sep 2004 14:38:34 +1000, Matt <matt@systemlinux.net> wrote:
> > > GuidoZ wrote:
> > > > Interesting indeed. Although, I imagine this was a spam email, and I
> > > > never believe (nor buy) anything from spam. I wonder how credible this
> > > > really is. If there was such a way to do what they claim, don't you
> > > > think it would have been big news? >One would think you wouldn't
> > > > first
> > > > hear about it through spam.
> > > >
> > > > It is quite possible to hide processes, reg keys and files, and is often
> > > > done by various malware.
> > > >
> > > > Also - nice website they have. http://www.randexsoft.com Simply says:
> > > >
> > > > Access Forbidden -- Go away.
> > > >
> > > > I love a company who is customer friendly.
> > > >
> > > > --
> > > > Peace. ~G
> > > >
> > > >
> > > > On Wed, 22 Sep 2004 20:10:28 -0700 (PDT), Will Image
> > > > <xillwillx@yahoo.com> wrote:
> > > >
> > > >>I recieved this in my inbox today:
> > > >>how long do you think this company will last?
> > > >>
> > > >>
> > > >>>Date: Wed, 22 Sep 2004 19:02:44 -0400
> > > >>>From: Jacques Tremblay <jacques.tremblay@gmail.com>
> > > >>>To: xillwillx@yahoo.com
> > > >>>Subject: Hide your adware from all Adware removers
> > > >>>and Anti-viruses
> > > >>>
> > > >>>To: Business development manager
> > > >>>
> > > >>>Subject: Hide your adware from all Adware removers
> > > >>>and Anti-viruses
> > > >>>
> > > >>>
> > > >>>Hi,
> > > >>> Adware removers are gaining in popularity and
> > > >>>they cause a big
> > > >>>revenue threat to adware based businesses, as we see
> > > >>>our software
> > > >>>installations get desinstalled after a period of
> > > >>>time that is shorter
> > > >>>and shorter, we see our revenues get smaller and
> > > >>>smaller.
```

Re: [Full-Disclosure] Rootkit For Spyware? Hide your adware from all Adware removers and Anti-viruses

Full-Disclosure: Re: [Full-Disclosure] Rootkit For Spyware? Hide your adware from all Adware removers and Anti-virus

```
> > _____  
> > Full-Disclosure - We believe in it.  
> > Charter: http://lists.netsys.com/full-disclosure-charter.html  
>  
>  
>  
> _____  
> Full-Disclosure - We believe in it.  
> Charter: http://lists.netsys.com/full-disclosure-charter.html  
>  
--  
Peace. ~G
```

```
_____  
Full-Disclosure - We believe in it.  
Charter: http://lists.netsys.com/full-disclosure-charter.html
```

Re: [Full-Disclosure] Rootkit For Spyware? Hide your adware from all Adware removers and Anti-viruses