

microsoft.public.security.virus: Re: attachment and e-mail where to report these security issues?

Re: attachment and e-mail where to report these security issues?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-03/1926.html>

From: Phil Weldon (*notdisclosed_at_example.com*)

Date: 03/26/04

Date: Fri, 26 Mar 2004 18:21:49 GMT

No, you still don't get it. The receiver need not "look up" ANYTHING.... they really can't in most cases. THAT is why the ENTIRE headers should be sent to the originating ISP, so the ISP can look up the correct originating account. Also be aware that one of the ways the swen worm spreads is to send a fake "infected email received from you" messages that contain the infective package as an attachments purporting to be the rejected message. Responding to that type of message is, of course a waste of time. Some organizations and ISP's DO have antivirus scanning of email, unfortunately some of these scanners are set to notify the harvested email address rather than the originating ISP. And certainly no ISP will act on a report that does NOT include the headers... it is hard enough to get them to act on a report that DOES include the headers.

--

Phil Weldon, pweldonatmindjumpdotcom

For communication,

replace "at" with the 'at sign'

replace "mindjump" with "mindspring."

replace "dot" with "."

"D.Currie" <dmbcurrie.nospam@hotmail.com> wrote in message

news:c40hsq\$2be6gs\$1@ID-193095.news.uni-berlin.de...

> If somebody wants to go through the trouble of looking up the sender

> properly, that's one thing, but most folks aren't going to bother with

> much

> more than the name it's coming from. Why bother with messy headers when

> they

> can simply report the person to their ISP? And if the viruses are coming

> en

> masse like swen did, few people are going to bother with much more than

> cleaning out the junk.

>

> Like people who bounce spam back, not realizing that the return addresses

> are often fake.

>

> Of course, you're correct that the instructions were the right way to

> report

> the virus, but I doubt most people will go through all of that for every

> virus email they get.

>

> If you read the way the OP phrased it -- wanting to report the "twit" who

> sent it, you can see that people tend to want to blame the person whose

> name

Re: attachment and e-mail where to report these security issues?

microsoft.public.security.virus: Re: attachment and e-mail where to report these security issues?

> is on the email, rather than understand that the sender is also a victim,
> and the name is likely to be false.
>
>
>
>
> "Phil Weldon" <notdisclosed@example.com> wrote in message
> news:lv08c.1150\$Dv2.840@newsread2.news.pas.earthlink.net...
> > No, you don't understand. These infected messages use harvested
email
> > addresses in the "From" field in the headers, but the IP address in
the
> > headers is the actual IP address the infected system used for its
> connection
> > to the internet. If you follow the directions Veronica Loell gave, the
> ISP
> > will have the information necessary to locate the account with the
> infected
> > system, even if the IP address were dynamically assigned. And if the
> > "From" email address WERE correct (which it never is - after all the
virus
> > writers don't want the infected systems tracked down), then it would be
a
> > GOOD a thing, not a bad thing, to let the ISP know. After all, if
someone
> > has an infected system, don't you think they would like to know about it
> and
> > get help? Think about it; if your system were spreading a virus you
would
> > like to know about it as soon as possible, I hope.
> >
> > --
> > Phil Weldon, pweldonatmindjumpdotcom
> > For communication,
> > replace "at" with the 'at sign'
> > replace "mindjump" with "mindspring."
> > replace "dot" with "."
> >
> > "D.Currie" <dmbcurrie.nospam@hotmail.com> wrote in message
> > news:c4087c\$2dserh\$1@ID-193095.news.uni-berlin.de...
> > > Unfortunately, if you report the sender, you're either reporting some
> poor
> > > fool whose computer is infected (and he's either fighting it or
doesn't
> > know
> > > he has it) or you're reporting some innocent third party whose address
> is
> > > being spoofed by the virus because the infected computer has that name
> in
> > > the address book. Most likely it's going to be the innocent third
party
> > > because that's the way most of the newer viruses work these days.
> > >
> > > So not only does it do no good, it also can harm an innocent person if
> the
> > > ISP does take some action and/or it ties up the ISP who get these
> reports.
> >
> >
> >
> >