

Re: Malware Triangle

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-12/0043.html>

From: Ant (*not_at_home.today*)

Date: 12/02/04

Date: Thu, 2 Dec 2004 01:16:53 -0000

"kurt wismer" wrote:

> *Ant wrote:*

>> *"kurt wismer" wrote:*

>>> *Ant wrote:*

>>>

>>>> *The <script> tag says "here's a script, you can run it if you like".*

>>>

>>>> *that's an embellishment... it says "here's a script", i'll give you*

>>>> *that, but that's about it...*

>>

>> *And those embelishments contribute to the whole, and are the problem*

>> *with respect to malware issues.*

>

> *i actually meant that it was an embellishment on your part, not the*

> *designers part, nor html's part...*

Ok, the capable browser says "Ooh look, a script tag! That means I can run what's inside. Oh well, if you insist...", or words to that effect.

>>>> *... tags don't instruct, they describe...*

>>

>> *The effect is the same, as far as a permissively configured browser is*

>> *concerned, when it interprets html with embedded executable content.*

>

> *browsers don't define html...*

I know.

> *the 'effect' may very well be the same*

Yes.

> *but the fact is that html does not have instructions, it has tags... if*

> *tags were instructions they'd be called instructions...*

Indeed.

alt.computer.security: Re: Malware Triangle

>> *Html has evolved to allow all sorts of constructs and active content*
>> *which we might think inappropriate for a text markup language, but*
>> *was thought necessary to enhance hypertext for the web experience.*
>
> *i reiterate – those are *not* part of html...*

I know.

> *what html has is the*
> *ability to act as a container for non-html content, nothing more... it*
> *is no different than an archive format in that respect...*

It is different, in that the intention is for a browser to run that content. I don't expect that when I open an archive.

>> *An html text file with the "embellishments" effectively becomes one*
>> *script containing not only layout and display descriptions, but*
>> *references to executable objects, and program source code which will*
>> *be interpreted and run in a suitably configured browser. Perhaps I*
>> *should not have called this conglomeration "html" in my original post*
>> *to this thread.*
>
> *that conglomeration is an html document, but it is not html...*

The whole thing is effectively one script for a web browser to interpret and act upon as it sees fit.

> *here's an obvious distinction – it is possible to have a browser that*
> *fully complies with the html standard and yet does not (even can not)*
> *execute the additional content contained within html documents they*
> *display (think lynx, or maybe arachne),*

True, but they are not as widely used as the ones that do. Many people using popular browsers do not have them (or their operating system) configured safely.

> *just as there are email clients*
> *that do not (even can not) execute the additional content contained*
> *within the emails they display...*
>
> *would you condone emails being called programs*

I'm not comfortable with calling email or html documents "programs", but was suggesting they should be treated as such because of the way they are mostly handled.

> *in spite of the fact*
> *that the specifications for email do not include mention of*
> *instructions to be carried out when encountered in the email body?*

alt.computer.security: Re: Malware Triangle

Email specs don't say a lot of things. When companies such as MS seek to redefine email, enable processing of rich and executable content in their email clients, and encourage users to accept this paradigm, we have a problem when their software is so widely used.

> *why should html documents be considered any different?*

Perhaps they shouldn't (because of the way emails are often handled). However, the difference for me is that I expect and want to run active content in some trusted webpages, but I never do with emails.

> *they are containers*

> *of arbitrary content and their respective readers may be (often are)*

> *configured to execute some of that content automagically...*

They are containers, but any executable content is in them for the purpose of being run. You might say that an exe file is a container of machine code and data. If I open it with a loader it will be run. If I open it with a debugger I can choose to run some of it, and display the data within (bitmaps, etc.). If I open it with dependency walker it won't be run. Granted, you will always expect an exe to be run when loaded by the OS, but you won't necessarily expect that for the scripts in an html document loaded by a browser.