

Re: what would cause this ??

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2007-10/msg00030.html>

- *From:* "Ant" <not@xxxxxxxxxx>
 - *Date:* Thu, 18 Oct 2007 21:08:37 +0100
-

"DrZaius" wrote:

supposedly, this person thinks someone they met online, deliberately aimed the attack at one specific machine (hers).

How so? It's just a link; there's no obligation to click it. And even if you do, Windows won't directly run the executable but will first ask what to do with it if subsequently, the scripted dialog on the page was clicked.

is there a way to find out who the site belongs to?
i tried the usual methods, but came up short.

The standard way is to use 'whois' but Windows doesn't have that application by default. There are several websites where you can do a whois lookup.

In any case, that was just the first link in the chain. there are a few domains and hosts involved before you get to the malware.

sajpj.eaqcfmc.cn (the host for the original link) -> runs a script at:
goodnserver.info -> loads a page at:
mystats.name -> redirects to:
themymoviessite.com -> loads the malware executable from:
videowebsoft.com

The domain eqqcfmc.cn is registered in China. I can't tell which registry because the name is in Chinese. sajpj.eaqcfmc.cn has IP address 217.20.112.28 which I find belongs to netdirekt in Germany.

goodnserver.info is registered through EstDomains (Estonia) and its IP (217.20.113.27) also belongs to netdirekt.

mystats.name gives no useful info about the registry or registrant but

Re: what would cause this ??

its hosted by 'Beyond The Network America' in the US at IP address 205.177.122.130.

themoviessite.com and videowebsoft.com are both registered through EstDomains and share the IP address 81.29.249.27. This is hosted by 'LLC GlobalWholesaleTrade' in Moscow, Russia.

All the EstDomains registrant (domain owner) details are unavailable. Looking at the providers and countries here, I wouldn't count on fast action in taking anything offline but you may be lucky.

Re: what would cause this ??