

Re: Update: UDP 770 Potential Worm

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-03/0016.html>

From: H C (keydet89@yahoo.com)

Date: 03/02/02

Date: Sat, 2 Mar 2002 06:43:50 -0800 (PST)

From: H C <keydet89@yahoo.com>

To: Byrne Ghavalas <security@gzone.org>, incidents@securityfocus.com

Byrne,

Thanks for the response.

- > *I am still investigating this issue. In the network*
- > *capture there*
- > *were no packets indicating some form of replication.*
- > *However,*
- > *my capture was limited due to the switched*
- > *environment.*

Hhhhhmmm...okay, doesn't sound like a worm, then.

- > *I have*
- > *an image of the original disk and am in the process*
- > *of setting up*
- > *a lab to conduct further controlled testing. I*
- > *would like to see if*
- > *it is possible for this problem to self-replicate*
- > *(worm-like) and if so, how.*

I assume by "self-replicate", you mean that you'd like to see if the problem occurs on the test network, using the dup'd image...correct? Again, that wouldn't be 'worm-like' behaviour at all.

Please understand, I'm not trying to be nit-picky...just clear in the terminology. I teach an incident response course for NT/2K/XP, and these sorts of things fascinate me. However, there can be a lot of confusion if things aren't referred to correctly.

- > *After analysing the network capture, I noticed that*
- > *the UDP*
- > *packets were being originated from a variety of*
- > *hosts, not just the proxy.*

Re: Update: UDP 770 Potential Worm

SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

I think that this is a very important point. Are the UDP packets originating from systems within the network? Are any of the source IP addresses located outside the network in question?

- > *This could be the result of a*
- > *variety of things,*
- > *one of which could be a worm that has propagated*
- > *itself*
- > *around the network. I don't know this for sure and*
- > *need to*
- > *conduct further analysis of the host(s).*

I agree. As a note of caution, until further investigations have been conducted, I would strongly recommend against referring to this as a worm or trojan in any way. Doing so tends to spread FUD and confusion, as the connotation is that an automated piece of software is capable of compromising multiple boxes, potentially through a known or perhaps a 'zero day' exploit. The final analysis may show this to simply be a configuration issue.

- > *I'm not sure if you received the attachment that I*
- > *sent in with*
- > *the message, if not, let me know and I will forward*
- > *it to you.*

Please do.

- > *I have sniffed the traffic and conducted an analysis*
- > *of the*
- > *packet. Please take a look at the file and you*
- > *should see what I mean by the above.*

Okay.

- > *Good question. Sorry for not being clearer in the*
- > *original*
- > *post. The proxy had already been isolated from the*
- > *network,*
- > *so my first steps were to check for obvious trojans*
- > *and*
- > *strange services. Nothing was revealed in 'netstat'*
- > *that was*
- > *out of the ordinary.*

I'd be very interested in seeing the information you collected. The reason I say this is b/c in the course I teach, I have several labs that are set up using trojans that look like normal services and processes.

Re: Update: UDP 770 Potential Worm

SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

For example, what tools did you use to collect the services information? I wrote a tool (available at my web site...<http://patriot.net/~carvdawg/perl.html>) that collects all service information, including the service executable name and account it runs under (I know it's Perl, but I've compiled most of the tools into stand alone executables for use in IR).

Further, what tools did you use to collect volatile information from the system regarding processes? Netstat may not show anything out of the ordinary, b/c it doesn't show any of the endpoint information in relation to processes...unless the system you're investigating is XP.

This leads to another question. Going back over your first post, it isn't clear what type of system (outside of MS-Proxy) that you're working with. I apologize if I missed this, but what OS and Service Pack/hotfix level are you working with on the proxy? How about the other hosts that have exhibited similar behaviour (you stated above that the strange UDP source port 770 datagrams originate from multiple hosts)?

> *I then plugged a cross-over cable between my laptop
> and the
> proxy to sniff any attempted communication. This is
> when I
> noticed the strange pattern of UDP packets.
> Believing it may
> be normal and the result of an application or
> service on the
> machine, I proceeded to stop all of the services and
> apps
> on the machine to see if the problem disappeared –
> it didn't.*

Can you be specific? I mean to say, if you stopped all services, to include the Server and Browser services, Workstation service, etc, wouldn't the box have eventually just stopped all together?

> *My next step was the use of fport.exe to find the
> process
> causing this problem. There was nothing listening
> on UDP
> port 770. Odd. (I intend investigating this further
> once the
> lab is properly set up.)*

SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

Have you tried using TDIMon from SysInternals as a backup? What other process information did you collect? Did you use PSLIST and LISTDLLS from SysInternals?

> *With the clients permission, I plugged my laptop in to the network and sniffed the packets. No UDP packets with a source of 770.*

What was the time period of the capture? Also, where in the network were you...you said this was a switched environment. Did you use the management port on the switch at this point?

I ask b/c you'd stated that the strange datagrams were originating from multiple hosts.

> *The next step was to plug the proxy server in to the network and observe the effects. Immediately, UDP packets with a source port of 770 began to travel across the network. My laptop was plugged in to a hub on the network, which linked to the backbone switch. As such I was only able to see some local traffic and broadcast traffic.*

I know you said this started immediately after you plugged the proxy back into the network, but was the proxy the source of these datagrams you observed?

> *Further information which I probably should have included; The packets included in the analysis are not from the proxy. The proxy server's IP address is 172.22.1.31*

Yes, that would tend to have an effect on any analysis conducted.

> *I don't know why the packets start when the proxy is plugged in to the network, and stop when it is removed. The capture does not make this obvious.*

More specific information regarding the particular hosts...say, simply identifying them...would be

Re: Update: UDP 770 Potential Worm

SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

useful. For example, if you could link particular IP addresses to the type of system...proxy, f/w, workstation, and even your system...the analysis would probably go much more smoothly.

- > *I am happy to provide the full set of packet*
- > *captures to you or*
- > *anyone that would like them. (TCPDUMP format.)*

Sure. Send one or two my way. Just be forewarned that Yahoo has a size limit on attachments.

- > *Ethereal 0.9.0. Win2k, SP2. Winpcap 2.2*

Good. I have that exact setup on my system. If you can archive and send me one or two of the captures, with information regarding each host, I'll see what I can discover.

- > *An initial check was performed, as explained earlier*
- > *in this*
- > *post, but I agree that indepth analysis is required.*
- > *I will*
- > *post the results of my analysis in the lab*
- > *environment as soon as I have them.*

I look forward to what you find.

- > *Again, all good points. As I was called in after*
- > *the second*
- > *proxy had caused problems for the client, certain*
- > *controls*
- > *were not put in place to aid in finding the source*
- > *of the*
- > *problem. The client, did not perform any steps to*
- > *secure*
- > *the box. They installed Win2K, SP2, MSProxy & Patch.*
- > *They also installed SurfControl.*

I'm sure you interviewed the client...were you able to determine whether any data had been reloaded from a backup?

Also, you've stated the make-up of the system...very good to know. What is the version of MSProxy used? What is the "patch" that was installed? Were any hotfixes beyond SP2 installed?

- > *As mentioned before, there were no problems for*
- > *about*
- > *a day and a half.. This leads me to believe that*

Re: Update: UDP 770 Potential Worm

SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

- > *something*
- > *had to have occurred on the box. Perhaps, if this is*
- > *a worm,*
- > *the box was eventually re-infected. Alternately the*
- > *box has*
- > *been compromised by someone.*

I'm curious about this last statement. Do you mean to say that the box "may have been compromised by someone"? If not, and you are sure that it has been, what evidence do you have to support this? I'm curious, b/c the statement is very emphatic...you seem sure of the fact. I think that this information would have an overall impact on the investigation.

Again, please don't take my questions as flames, and please understand that I am in no way trying to disprove anything you've said. I am simply trying to get more information to attempt to answer your question. I spent quite some time as a network security manager for a large telecomm, and I wrote the incident response policy for that telecomm. I dealt with many folks during my tenure who would state emphatically that they'd been 'hacked' with no real evidence to support that.

Also, I hear similar statements from the attendees of my IR course...the purpose of the course is to teach them how to root these things out.

- > *At the moment I am*
- > *unable*
- > *to answer either question. I will have a better*
- > *indication of*
- > *whether or not this is a worm after examining the host*
- > *in a controlled lab.*

Perhaps if you told me what sorts of things you've already checked (you can contact me directly w/o posting to the list, if you like), I can recommend other areas that may need to be examined.

- > *Due to the current security architecture, it is not*
- > *possible to*
- > *determine the current method of entry, if this is*
- > *the case.*
- > *Additional investigation and measure would be*
- > *required.*

At this point, I'd agree with you completely.

SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

- > *Indeed! I have scoured the net to find anything that*
- > *would relate to this problem.*

Odd. I didn't find anything either...but then, I didn't look very hard.

- > *Patrick Nolan from Incidents.org was kind enough to*
- > *suggest that I investigate ICP, unfortunately this*
- > *doesn't*
- > *seem to be right... (If you would like to know more*
- > *about*
- > *this – mail me direct.)*

Oddly enough, Patrick and I have been in contact, as well. He made a comment about your conversation, and when I asked for more information...I was curious at that point...he refused, citing the confidentiality necessary between analyst and client. In his defense, he hasn't provided any specific information, but I assumed based on what little he did say, that you were the one he was talking about.

- > *I trust this makes things a little clearer. Any*
- > *further questions or suggestions are welcome.*

If there is anything you can send me to assist in the analysis, please do. Also, let me know what you've collected from the Proxy (and any other system from which this traffic is originating) with regards to process information...perhaps I can suggest some other things. These items are required for a complete analysis.

Carv

Do You Yahoo!?

Yahoo! Sports – sign up for Fantasy Baseball

<http://sports.yahoo.com>

This list is provided by the SecurityFocus ARIS analyzer service. For more information on this free incident handling, management and tracking system please see: <http://aris.securityfocus.com>

- **Previous message:** [zaire: "Re: Large Attack"](#)
- **Maybe in reply to:** [Byrne Ghavalas: "Update: UDP 770 Potential Worm"](#)
- **Next in thread:** [H C: "Re: Update: UDP 770 Potential Worm"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)