

## Re: Update: UDP 770 Potential Worm

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-03/0017.html>

---

**From:** Byrne Ghalalas ([security@gzone.org](mailto:security@gzone.org))

**Date:** 03/02/02

From: "Byrne Ghalalas" <[security@gzone.org](mailto:security@gzone.org)>  
To: "H C" <[keydet89@yahoo.com](mailto:keydet89@yahoo.com)>, <[incidents@securityfocus.com](mailto:incidents@securityfocus.com)>  
Date: Sat, 2 Mar 2002 07:48:12 -0000

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hi H C,

Thank you for your comments. I have replied to your questions in-line.

> > *I still believe that the packets may be the result*  
> > *of some kind of*  
> > *worm / trojan, with the goal of knocking machines*  
> > *off the network.*  
>  
> *Other than the fact that systems were falling off of*  
> *the network immediately after the 'attack', what other*  
> *evidence have you collected to support this? A worm*  
> *replicates itself...none of the traffic you described*  
> *supports this. I'm wonder what I've missed in your*  
> *analysis...any elaboration would be appreciated.*

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. 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.

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

Re: Update: UDP 770 Potential Worm

## SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

> > *My analysis revealed that the final destination of*  
> > *these strange packets*  
> > *was UDP 138, however I was not fortunate enough to*  
> > *sniff any of*  
> > *these packets and so am not sure of the payload of*  
> > *these final packets.*  
>  
> *You'll have to forgive me, but this makes little sense*  
> *to me. Perhaps it's some gaps in my understanding of*  
> *IP, but how can you know that a UDP datagram is*  
> *destined to port if you haven't sniffed it somehow?*

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. 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.

> > *3.1 Intermittently, 5 UDP packets were sent with*  
> > *Source port of*  
> > *770 and consecutive destination ports, with a*  
> > *directed-broadcast*  
> > *address as the destination.*  
>  
> *Are you meaning to state here that the source address*  
> *of the UDP datagrams is the IP address of the proxy?*  
> *If so, what does the output of 'netstat -a' tell you?*  
> *Since it's an MS machine, what does fport.exe or*  
> *TDIMon tell you about the process that is utilizing*  
> *the source port?*  
>  
> *I apologize if the above question regarding the source*  
> *IP address seems stupid, but for all of the*  
> *specificity in your post, the one thing that you never*  
> *specifically stated was that bit of info. I simply*  
> *wanted to be clear on it.*

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 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.

## SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

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.)

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

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 have included the output of two of the 'conversations' that were captured in the attachment that was sent with the original message. You will notice that some packets have a unicast source address while others have a broadcast source address.

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

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.

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

> > *3.5 When the proxy is plugged on to the network, I  
> > noticed that  
> > it ARP'ed for it's own IP address, after which a  
> > barrage of packets  
> > hit the network. (I was sniffing a switched network,  
> > plugged in to  
> > a  
> > hub – so only saw local traffic and the broadcast  
> > traffic.)  
>  
> What tool were you using to sniff?*

Ethereal 0.9.0. Win2k, SP2. Winpcap 2.2

> > *After a few  
> > minutes, machines started to drop off the network!  
>  
> What does 'drop off the network' mean? Were any  
> errors noted on the systems themselves? Did the*

Re: Update: UDP 770 Potential Worm

## SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

> *systems respond to pings?*

Sorry – again I could have been clearer. The machines can still be pinged, but stop responding to normal SMB requests. The only thing I could find in the event logs was that the redirector timed out – but there was only one message and it was only on one of the boxes... So not much to support the fact that the redirector failure was a result of the UDP packets.

This is something that I will be investigating once I have the lab in place.

Sorry that there isn't much to go on at the moment.

> > *3.7 Some of the machines appeared to have a*  
> > *'conversation'*  
> > *between themselves and the broadcast address.*  
>  
> *What does this mean? What ports were involved? What*  
> *can you tell us about the contents of the packets?*  
> *Was this normal NetBIOS traffic?*

I would like to refer you to the original attachment that I sent with the message. I think it does a reasonable job of answering this question ;–)

> > *I would appreciate any comments / suggestions, and*  
> > *useful*  
> > *insights. If you require any further information,*  
> > *let me know and I will see what I can do.*  
>  
> *From what you've posted, I would say that there is*  
> *quite a bit that that hasn't been done. Running a*  
> *port-to-process mapping tool on the proxy (assuming*  
> *that the proxy is the source of the UDP traffic) would*  
> *have been something done almost immediately. After*  
> *all, if something is using port 770, one should be*  
> *able to find it.*

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.

> *You stated that the proxy was rebuilt from clean*  
> *media, on fresh equipment. What steps were taken to*  
> *secure the box? Was any data loaded from backup? Was*  
> *any monitoring of the box done after the new one was*  
> *powered on? In order to support the theory of a worm*  
> *or trojan, the new box would have to have had been*  
> *subjected to tainted media, or it was immediately*

Re: Update: UDP 770 Potential Worm

## SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

> *broken into again up being powered up.*

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.

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

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.

> *Have any searches of the MS site, particularly TechNet  
> been conducted? According to several documents there,  
> UDP port 770 is the source port for something called  
> 'cadlock'.*

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

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.)

The only information I could find about Cadlock is that it is an application used for securing CAD drawings. There may be more to this, but no luck so far.

Finally, the only other piece of information I could find was here: <http://www.sans.org/y2k/021201-0930.htm>

If you look 3/4 down the page you should see:

```
Server used for this query: [ whois.ripe.net ]
inetnum: 217.56.35.0 – 217.56.35.31
netname: PERMEDICA-S-P-A-
descr: PERMEDICA S.P.A.
country: IT
```

Feb 8 09:11:23 217.56.35.2:53 -> z.y.w.98:53 UDP

Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58943 UDP

Re: Update: UDP 770 Potential Worm

SecurityFocus Incidents: Re: Update: UDP 770 Potential Worm

Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58942 UDP  
Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58941 UDP  
Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58940 UDP  
Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58939 UDP  
Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58938 UDP  
Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58937 UDP  
Feb 8 09:11:23 217.56.35.2:770 -> z.y.w.98:58936 UDP

You'll notice that it closely matches what I have found (A few minor differences). You will also notice that it is a year old... This is what prompted me to contact Incidents.org.

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

Kind regards,

Byrne Ghavalas

-----BEGIN PGP SIGNATURE-----

Version: PGPfreeware 7.0.3 for non-commercial use <<http://www.pgp.com>>

iQA/AwUBPICDqV9b3++bhmFHEQLrPgCgn19rck+SPaPA9244K7AgmmXA/ZAAoNB+  
+FsOxE0DJbtDPRVCGy0czP5B  
=SPsX

-----END PGP SIGNATURE-----

---

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:** [H C: "Re: Update: UDP 770 Potential Worm"](#)
- **In reply to:** [H C: "Re: Update: UDP 770 Potential Worm"](#)
- **Next in thread:** [H C: "Re: Update: UDP 770 Potential Worm"](#)
- **Reply:** [H C: "Re: Update: UDP 770 Potential Worm"](#)
- **Reply:** [H C: "Re: Update: UDP 770 Potential Worm"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)