

## Re: Update: UDP 770 Potential Worm

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-03/0013.html>

---

**From:** H C ([keydet89@yahoo.com](mailto:keydet89@yahoo.com))

**Date:** 03/02/02

Date: Fri, 1 Mar 2002 20:21:12 -0800 (PST)

From: H C <[keydet89@yahoo.com](mailto:keydet89@yahoo.com)>

To: Byrne Ghavalas <[security@gzone.org](mailto:security@gzone.org)>, [incidents@securityfocus.com](mailto:incidents@securityfocus.com)

Byrne,

Your post interested me greatly, and if you don't mind I'd like to ask a couple of questions that are inline to your quoted post below:

> *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.

> *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?

> *===Original Message===*

>

> *Hi All,*

>

> *I have gone through the archives and searched the*

> *'Net, but am*

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

- > *unable to locate any further information with*
- > *regards to these*
- > *strange packets – perhaps you fine people could be*
- > *of*
- > *assistance. :-)*
- >
- > *1. I was called in to analyse a customer's network.*
- > *They couldn't*
- > *understand why network connections kept failing and*
- > *machines*
- > *dropped out the network. They eventually found that*
- > *by removing*
- > *the MS-Proxy server from the network, the problems*
- > *were*
- > *'resolved'.*
- >
- > *2. They rebuilt the server using a different machine*
- > *and clean*
- > *media from original CDs. A day and a half later, the*
- > *problem*
- > *re-appeared – again corrected by unplugging the*
- > *machine from*
- > *the network.*
- >
- > *3. I analysed the machine, but found nothing*
- > *obvious. I decided*
- > *to sniff the TCP/IP traffic from the Proxy server*
- > *and found:*
- >
- > *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.

- > *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*

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

- > *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?

- > *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 systems respond to pings?

- > *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 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.

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 broken into again up being powered up.

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'.

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

---

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