



Catching the Lovsan Worm in Action! [8/11/03]

Laura Chappell, Sr. Protocol Analyst

Protocol Analysis Institute

www.packet-level.com; www.podbooks.com

Note: Check out a live infection online! Download lovsan-infection.zip (available in .cap/.dmp/.pkt formats) at www.packet-level.com > Library.

=====

You could hear the CPU screaming under the hood of my IBM Thinkpad. Suddenly, cruising the Internet was like wading through mud... at times it took up to 3 minutes to open up a simple Explorer window. Obviously, something was wrong...

Task manager indicated that *services.exe* process was taking up 99% of the processor time. Ugh – this appeared to be a virus. The *services.exe* has shown numerous problems with high utilization in the past, but this system was already patched (see MS doc Q328885).

I called my pal, Wally Rich at Network Associates to see if he had any clue what could be causing the strange behavior. He got right back to me with an upgraded alert on the Lovsan worm – he'd just received an internal alert from the McAfee guys – looks like my system matched the symptoms listed.

Downloading Stinger from www.mcafee.com (which had just been updated to wipe out Lovesan) fixed the problem quickly.

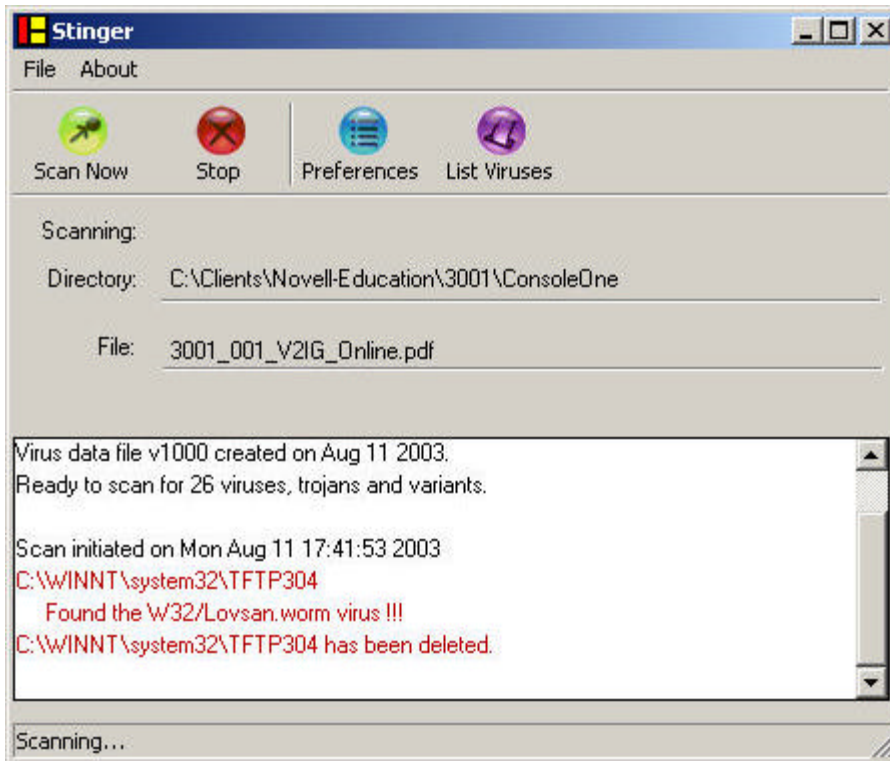


Figure 1: Stinger found Lovsan.worm virus and found the planted TFTP file it planted on my drive.

But that got my interested peaked – I wanted to catch this virus infecting a system and identify it's signatures on my drive.

When reading a bit about how this virus works, I noticed that the actual infection was done over port 4444.

Looking at a system that had just been infected, I opened up the DOS box and checked out active connections.

```

C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   CHADWICK:epmap          CHADWICK:0             LISTENING
TCP   CHADWICK:microsoft-ds  CHADWICK:0             LISTENING
TCP   CHADWICK:1025           CHADWICK:0             LISTENING
TCP   CHADWICK:1027           CHADWICK:0             LISTENING
TCP   CHADWICK:1115           CHADWICK:0             LISTENING
TCP   CHADWICK:1116           CHADWICK:0             LISTENING
TCP   CHADWICK:4444           CHADWICK:0             LISTENING
TCP   CHADWICK:5679           CHADWICK:0             LISTENING
TCP   CHADWICK:1115           unknown.Level13.net:http ESTABLISHED
TCP   CHADWICK:1116           unknown.Level13.net:http ESTABLISHED
UDP   CHADWICK:epmap          ***
UDP   CHADWICK:microsoft-ds  ***
UDP   CHADWICK:1026           ***
UDP   CHADWICK:isakmp        ***
UDP   CHADWICK:1036           ***

```

Figure 2. An active connection on port 4444 may indicate a Lovesan.worm virus infection had just occurred.

FILTERING FOR LOVSAN

Great! I can catch that easily – I built a filter looking for all traffic to and from port 4444 as follows:

Source Port field (offset 0x22)/value 4444 (0x115C in hex)

Destination Port field (offset 0x24)/value 4444 (0x115C in hex)

Note: Sniffer wants hex values, while EtherPeek prefers decimal – I'll show you both filters.

Here's what the patterns looks like:

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	11	5c														
2																

Name: Source Port 4444 (0x115c)

Figure 3: The first pattern looks at the source port number.

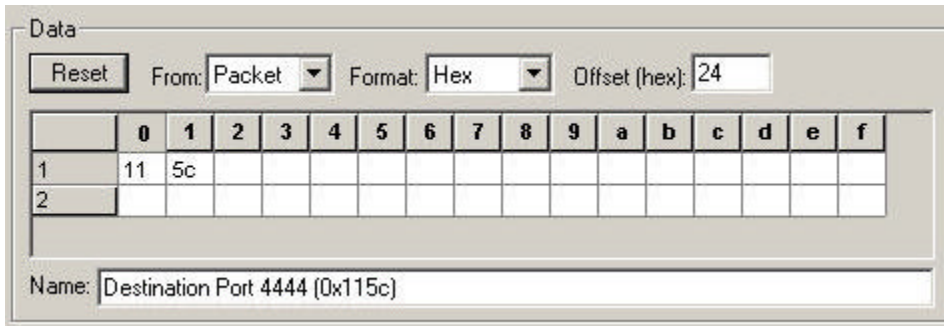


Figure 4: The second pattern looks at the destination port.

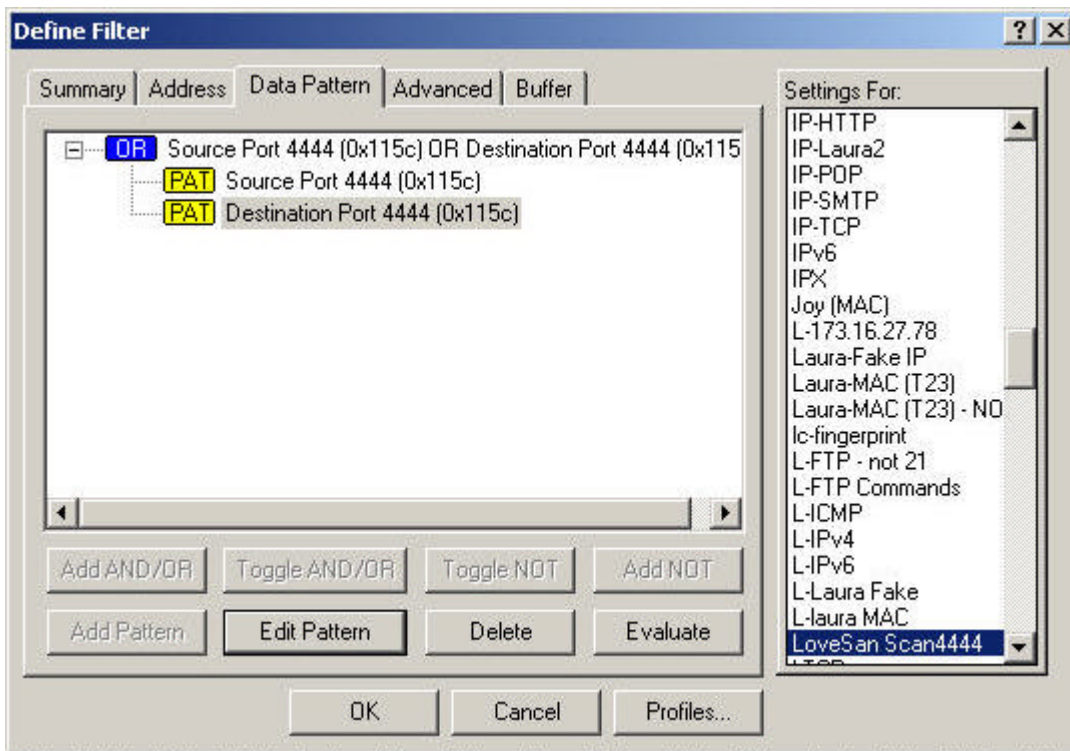


Figure 5: Simply 'OR' the two patterns together to look at traffic to/from port 4444.

In EtherPeek I could enter the decimal value 4444 and away I went.

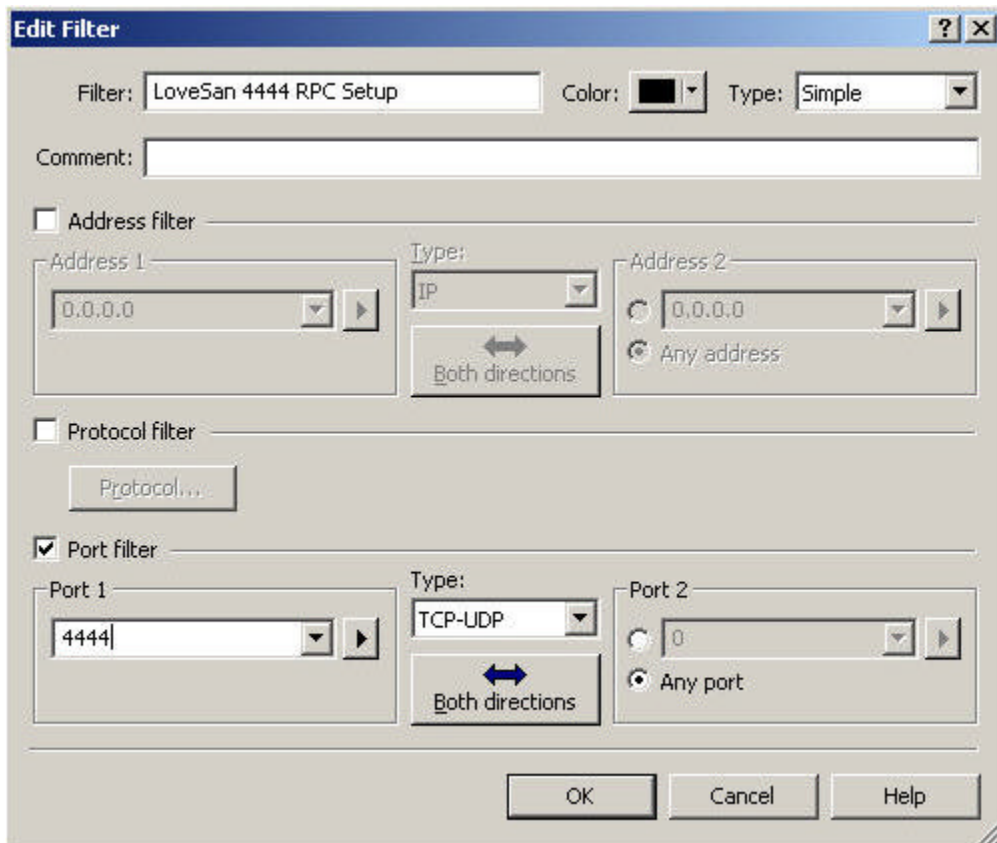


Figure 6: Simply enter the decimal value 4444 in EtherPeek and away you go!

Less than 30 seconds later I caught a live infection.

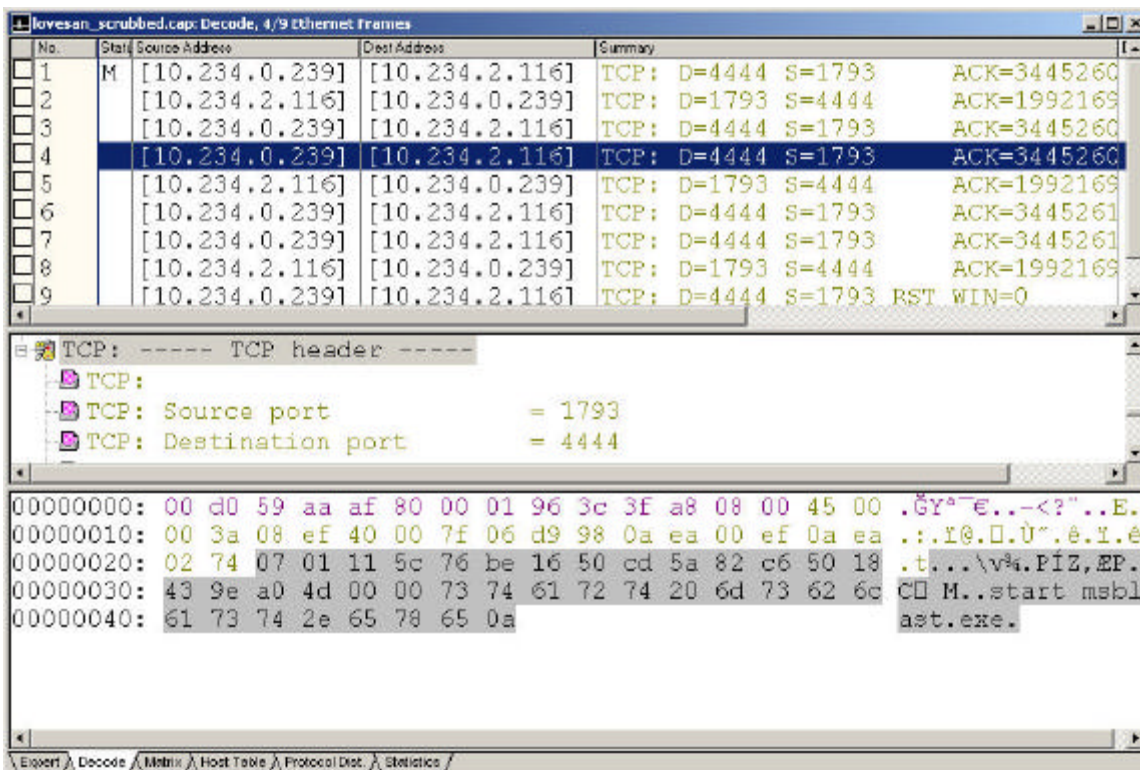


Figure 7: Sure enough – the trace indicated the attacker was launching msblast.exe.

This trace file is online at www.packet-leve.com in the Library section. It is called lovsan-infection.zip (available in .cap/.dmp/.pkt formats).

Now – it appears that Lovsan puts a tftp### file in the \WINNT\SYSTEM32 directory (where ### is a random set of 3-digits). Stinger found the tftp304 file immediately and deleted it (see Figure 1).

A quick search of the drive before Stinger was run found the file as well.

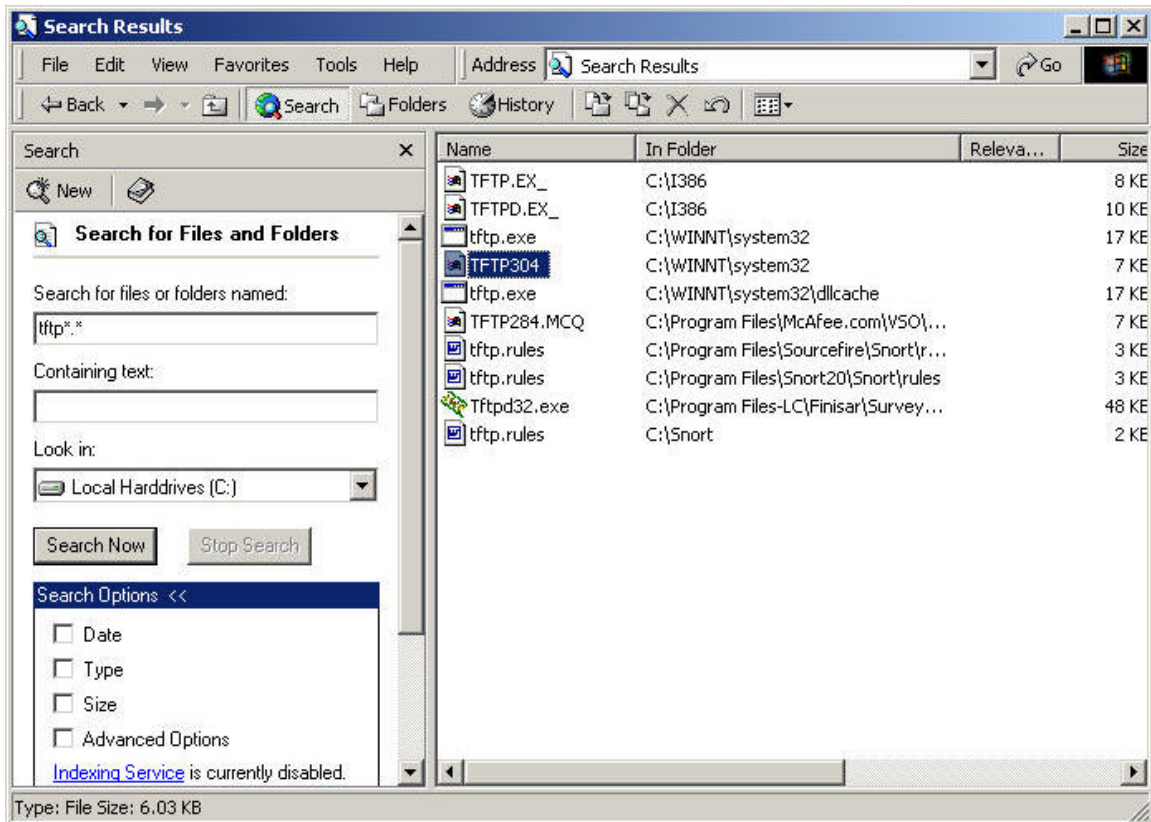


Figure 8: Searching for tftp*. * found the culprit file quickly.

PROTECTING AGAINST LOVSAN

Lovsan takes advantage the RPC Interface Buffer Overflow vulnerability in Windows systems. (See http://vil.nai.com/vil/content/v_100499.htm for more information.) Apply the MS03-026 patch to protect your systems against this vulnerability.

Although being nailed by a virus is no fun at all, it is great to have tools such as Sniffer and EtherPeek and Stinger to capture and eradicate the virus. Special thanks to Wally Rich of Network Associates and kudos to the Avert team (vil.nai.com) for catching this so quickly and updating Stinger today to nail this sucker!

Laura Chappell is the Sr. Protocol Analyst for the Protocol Analysis Institute. She can be reached at lchappell@packet-level.com. See www.packet-level.com or www.podbooks.com for more resources for the protocol analyst.