

Version 1.2

Updated: 2005-09-28

Preface

The Internet suffered from the 376 byte long worm which goes by the name Sapphire SQL Worm, slammer etc.

While preparing for a presentation I thought it would be fun to publically show the newest worm to the public, and boy it was easy.

Using an iBook and an Acer Aspire 1300 I connected them using a cross-over Ethernet cable and had some good clean network fun.

Use this if you like

You need

Target which you make vulnerable - almost any Windows PC should do

Evil hacker machine with the worm.pl which you can download from http://www.digitaloffense.net/worms/mssql_udp_worm/ - thank you guys for making this easy (you also need netcat the nc program, but surely you have this already installed)

worm.pl is a Perl script which has the worm code which allow you to send it through netcat to another machine

Disclaimer: I am lazy, so I didn't verify this code - use with care even if this IS the original code you are sending this to a machine which is vulnerable - watch out for side effects.

A TEST-NETWORK - YES! You need to do this on a dedicated network, unless you're the BOFH network-admin and wants to play games to get more funding for your gamer-pc.

How to do it

Infect the target machine using some variant of SQL server. I used the Microsoft Office XP CD, which have MSDE2000 - the standalone version of SQL Server. After a quick reboot I had a running MSSQLSERVER service.

Connect the setup using a hub or cross-over cable. Then configure the two machines using for instance the addresses

- 10.0.0.1 hacker machine
- 10.0.0.2 target machine, use 10.0.0.1 as the default GW

Start the worm

```
perl worm.pl | nc -u -v -v -v server 1434
```

Then use your favourite network monitoring program to watch tcpdump, netstat, ethereal etc.

Being kewl!

if you're a REALLY COOL guy or girlie you can then make screen dumps or go show this to management - they will LOVE THIS!

I made this screendump

This picture shows how the worm behaves when started in a small test environment - CLOSED NETWORK using a crossover cable and two laptops, and the worm.pl code provided by digitaloffense.net

The command used to start the worm is highlighted

The network is immediately saturated with traffic!

Tcpdump in the lower left is running so fast the screen dump is almost

unreadable - show the sending of the worm to random hosts

netstat in the lower right shows the bytes sent, -w 5 means wait 5 seconds between samples

nc is the netcat program being used to send the worm to the 'server', which is just an alias to the vulnerable host

What happens

You send 376 bytes in an UDP packet Then the server is infected by this worm, and starts sending out UDP packets to random IP addresses - at FULL network speed. About 25000 packets and 10Mbytes of data is wasted pr second in my setup.

Side effects

Note: On purpose I didn't set my hacker/router to actually try to forward packets - it just drops all these. I wanted to know how many packets my machine would send out, had it been a vulnerable server on the Internet.

On the real Internet several things might have/did happen

- The infected machine would receive ICMP unreachable packets from actual machines which existed, but didn't have the port open: Example sending worm to machine without MS SQL: # tcpdump -i en0 host 192.168.1.52
tcpdump: listening on en0 14:32:41.028357 192.168.1.51.49257 >
hlk.kramse.dk.ms-sql-m: udp 376 14:32:41.030282 hlk.kramse.dk >
192.168.1.51: icmp: hlk.kramse.dk udp port ms-sql-m unreachable
- routers would try to find machines on their local segments - multiple ARP packets to find these machines
- routers would try to lookup non-existing networks in their routing tables - those not assigned, in-use yet

In general I expect these side effects to have had some influence.

Questions/feedback

Questions which I haven't investigated:

- Does SQL server try to lookup the addresses when the worm is received?
- More side effects than above?

[Please send any feedback to me](#)

Quotes about this worm

from CSIRT.dk - danish Computer Security Incident Response Team "Ormen er i sig selv ikke farlig, men den spreder sig så hurtigt og så massivt, at internetforbindelsen kan tabe pusten. CSIRT.DK har i weekenden måttet hjælpe en kunde på en 32 Mbit-linje, hvor 98-99% af kapaciteten var udnyttet af ormen."

Best regards
Henrik
hik@kramse.dk