



Just in Time: Microsoft Vector Exploit Time January-April 2005
infectionvectors.com
April 29, 2005

Much is made about the security bulletins released by Microsoft each month (except for March this year, which saw no new alerts) and the impact the respective flaws will have on the integrity of Windows devices. The 23 bulletins of 2005 represent more than were released at this time last year (April saw reports 11-14 from Microsoft). On April 30 of last year Sasser was released, based upon the vulnerability reported earlier that month, MS04-011 (a patch that contained fixes for LSASS among 13 others). One of the most revolutionizing cases for patch management was back in 2003, when the Blaster worm was released a mere 3 weeks after the MS03-026 DCOM RPC Buffer Overflow report was made public. That event forever raised the bar for delivering patches speedily, much to the dismay of configuration management teams everywhere. This year, there have not been any worms written for vulnerabilities within the same time period as Blaster.

The bulk of the malware that has received attention this year points to the trend in infection vectors: allowing a user to open a malicious file and infect their own machine. Even with the release of alerts for MSN Messenger, the worms that have "targeted" this application (such as Bropia and Kelvir) do not exploit them. These worms simply send a copy/link to users and ask them to open them. The same is true of another worm receiving attention: Mytob. This malware mass mails itself and uses familiar buffer overruns in RPC DCOM (MS03-026) and LSASS (MS04-011).

Although Internet worms have not developed, a good deal of malware still exists for the first four months worth of Microsoft bulletins. In one case, as seen in the table below, malware was out well before the patch. The malicious code that exists is in the form of directed exploits, generally applications that would be considered Trojan Horses.

Last year, Bill Gates made the following statement in regard to times to exploit:

"The time to exploit about a year and a half ago was typically 60 to 90 days. Time to exploit now we've seen anywhere from three to 21 days. We haven't seen a single case where there has been a six-month time to exploit a known security vulnerability. I wish people were waiting six months to do the exploits."

Certainly, the test for each of these is still to be proven, a worm could be written for any of these bulletins later in the year of next year and be effective. For example, Wallon, although not released until May of 2005, exploited two flaws discovered in the first four months of the year. However, the amount of existing malware for a particular entry point is very important to configuration management specialists, security managers, etc.

The table below shows the Microsoft Security Bulletin and related malware through April's alerts (PoC = Proof of Concept code exists for this exploit).

Vulnerability (Date Released)	Description	Malware (Date Discovered)
MS05-001 (11 January 2005)	HTML Local Zone Security Bypass	Phel (27 December 2004) Magise (21 March 2005)
MS05-002 (11 January 2005)	Malformed Cursor/Icon	Globe (12 January 2005) Hebolani (27 January 2005) Anicmoo (16 February 2005)
MS05-003 (11 January 2005)	Indexing Service	N/A
MS05-004 (8 February 2005)	ASP.NET Path Validation	N/A
MS05-005 (8 February 2005)	Link Processing	PoC (8 February 2005)
MS05-006 (8 February 2005)	Sharepoint Services	N/A
MS05-007 (8 February 2005)	Windows Info Disclosure	N/A
MS05-008 (8 February 2005)	Windows Shell	N/A
MS05-009 (8 February 2005)	WMP/Messenger PNG	PoC (10 February 2005)
MS05-010 (8 February 2005)	License Logging Overrun	PoC (8 February 2005)
MS05-011 (8 February 2005)	SMB Vulnerability	N/A
MS05-012 (8 February 2005)	OLE/COM Vulnerability	N/A
MS05-013 (8 February 2005)	DHTML Editing/ActiveX	N/A
MS05-014 (8 February 2005)	IE Cumulative Update	N/A
MS05-015 (8 February 2005)	Hyperlink Object Library	N/A
MS05-016 (12 April 2005)	Windows Shell	VBS_RUNEXPLT (22 April 2005)
MS05-017 (12 April 2005)	Message Queuing	N/A
MS05-018 (12 April 2005)	Windows Kernel	N/A
MS05-019 (12 April 2005)	TCP/IP – ICMP Vuln	N/A
MS05-020 (12 April 2005)	IE Cumulative Update	PoC (18 April 2005)
MS05-021 (12 April 2005)	Exchange	PoC (19 April 2005)
MS05-022 (12 April 2005)	MSN Messenger 6.2	N/A
MS05-023 (12 April 2005)	MS Word Vulnerability	N/A

Microsoft Security Bulletins and Related Malware January – April 2005.

To consider the six-month range mentioned by Gates, it is necessary to examine the 7 patches released in November and December of 2004. Although there are examples of code that targets the flaws in IE, no major worms were developed for those vulnerabilities. The WINS flaw that allows remote code execution (MS04-045) was considered one of the more likely vulnerabilities to spawn a worm. As of April 2005, there are two: Poxdar (Doxpar) released in February 2005, and Kelvir.W, released in mid-April. There are also examples of Trojans that exploit this hole, such as Winser.

Overall, the malware that exists continues the trend of simply delivering an exploit to a user and relying on social engineering to infect a machine. The Beagle worm showed tremendous success with this model, as has newer code such as Brodia and MytoB. The use of the web-based vectors via the IE flaws reported in 2004 and 2005 is also evidence for the increase in “passive malware,” code waiting for users to compromise their machines through “drive by” web-based infections or by opening attachments/links from sheer curiosity. Much of the malware of 2005 may well be described as “venus flytraps,” attractively lying in wait for their next victims.

This is the first of the 2005 reports in regards to Microsoft security bulletins, which are closely monitored by infectionvectors. For additional information on the bulletins or on malware defense, please see <http://www.infectionvectors.com/>.

References

Bropia Report on Symantec's Site

<http://securityresponse.symantec.com/avcenter/venc/data/w32.bropia.html>

Kelvir Report on Symantec's Site

<http://www.symantec.com/avcenter/venc/data/w32.kelvir.aw.html>

Sasser Report on Symantec's Site

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>

Wallon Report on Symantec's Site

<http://securityresponse.symantec.com/avcenter/venc/data/w32.wallon.a@mm.html>

Bill Gates' Quote Concerning Time to Exploit:

"Gates dishes out security promises" Tech News on ZDNet.

http://news.zdnet.com/2100-1009_22-5250003.html

Microsoft Security Bulletin November 2004

<http://www.microsoft.com/technet/security/bulletin/ms04-nov.msp>

Microsoft Security Bulletin December 2004

<http://www.microsoft.com/technet/security/bulletin/ms04-dec.msp>

Sophos' Winser Analysis

<http://www.sophos.com/virusinfo/analyses/trojwinsera.html>

Poxdar Report on Symantec's Site

<http://securityresponse.symantec.com/avcenter/venc/data/w32.doxpar.html>

Kelvir.W Report on Symantec's Site

<http://securityresponse.symantec.com/avcenter/venc/data/w32.kelvir.w.html>