



Just in Time: Microsoft Time to Exploit 2

May – August 2005

infectionvectors.com

August 2005

This report continues to monitor the development of malware based on vulnerabilities detailed in Microsoft Security Bulletins in 2005. Part 1 is available at http://www.infectionvectors.com/vectors/jit_exploit_time.htm. In the previous report, 3 of the 23 advisories had directly attributable malicious code associated with them. 5 more advisories had publicly available proof-of-concept code. Note that this was produced right after the August advisories and will be updated at the end of the year.

Since the writing of the first portion of this report, new malware has been discovered for MS05-020, specifically, the DHTML race condition memory corruption flaw. The associated Trojan, named Helemoo by Symantec, was found in late July 2005, three and a half months after the bulletin was released. The exploit had proof-of-concept code available one week after the vulnerability was disclosed by Microsoft.

From May through August 2005, twenty new advisories were published, for a year-to-date total of 43. For comparison, in August of 2004, the 26th advisory was released.

The relatively quiet spring and summer for malware is due in large part to the lack of serious outbreak among Windows-based worms. The table below shows the release of bulletins from May through August as well as associated malware/proof-of-concept (PoC) code, where applicable.

Vulnerability (Date Released)	Description	Malware (Date Discovered)
MS05-024 (10 May 2005)	Explorer Web View (W2K)	PoC (May 2005)
MS05-025 (14 June 2005)	IE Cumulative Update	N/A
MS05-026 (14 June 2005)	HTML Help	Phel.Q (3 July 2005)
MS05-027 (14 June 2005)	SMB Validation	N/A
MS05-028 (14 June 2005)	Web Client Service	N/A
MS05-029 (14 June 2005)	OWA Cross Site Scripting	PoC Available (15 June 2005)
MS05-030 (14 June 2005)	Outlook Express Update	PoC (21 June 2005)
MS05-031 (14 June 2005)	Interactive Training	N/A
MS05-032 (14 June 2005)	MS Agent Spoofing	N/A
MS05-033 (14 June 2005)	Telnet Information Disclosure	N/A
MS05-034 (14 June 2005)	Cumulative Update for ISA Server	PoC Available (10 June 2005)

MS05-035 (12 July 2005)	Word Font Parsing	N/A
MS05-036 (12 July 2005)	Color Management Module	PoC (21 July 2005)
MS05-037 (12 July 2005)	JVIEW Profiler	Jevprox (12 July 2005)
MS05-038 (9 Aug 2005)	Cumulative IE Update	PoC Available (Aug 2005)
MS05-039 (9 Aug 2005)	Plug and Play Flaw	N/A
MS05-040 (9 Aug 2005)	TAPI Vulnerability	N/A
MS05-041 (9 Aug 2005)	RDP Flaw	PoC Available (9 Aug 2005)
MS05-042 (9 Aug 2005)	Kerberos Disclosure/Spoof	N/A
MS05-043 (9 Aug 2005)	Print Spooler	N/A

In addition to exploits released soon after the bulletin (those that inch ever closer to the “zero day” fears of many analysts) it is interesting to note the malware created well after the bulletin. There have been few new additions to the Microsoft product-based malware from the first quarter of the year, which is consistent with the relatively quiet year 2005 has been overall for malware.

Of the recent alerts, security professionals have shown great concern over the Plug and Play flaw (MS05-039), publicly stating that the hole could have “Sasser”-like implications for malware. That is a pretty big statement, one that will be proven or disproven over the next few months. Sasser came out almost exactly one month after the flaw was announced.

Since the release of the first part of this document, Microsoft has used its Honeymonkey system to unearth numerous drive-by exploits. The tool acts much like an active honeypot, scanning web sites for malicious software that is pushed to unsuspecting browsers. The Honeymonkey investment is an innovative direction for the software company, distinct from flaw identification and patches.

Microsoft’s Security Business and Technology unit VP, Mike Nash, was quoted at a security conference this summer touting the advancements they have made with the XP SP2 release. He noted that users of the release are “13 to 15 times less likely to be infected by some of the most prevalent malicious software” as opposed to users of prior versions of Windows.

Overall, although the total number of vulnerabilities is slightly higher than 2004, the first two thirds of 2005 have been much quieter in terms of malware infections for Windows users. This is, of course, due in large part because of the absence of a Sasser or “war” between mass mailers as was seen in the spring last year. The last part of this report is due to be published in December of 2005.

References

MS05-026

Phel.Q Trojan 3 July

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=VBS%5FPHEL%2EQ&VSect=T>

MS05-029

PoC

<http://www.securiteam.com/windowsntfocus/5WPOF1FG1W.html>

MS05-037

Jevprox downloader Trojan 12 July

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.jevprox.html>

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=JS_JAPROX.A

MS05-032 Trojan out in July of 2005

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.helemoo.html>

MS05-020 Trojan, Helemoo

<http://securityresponse.symantec.com/avcenter/venc/data/pf/trojan.helemoo.html>

PoC for MS05-030

<http://www.frstirt.com/exploits/20050624.MS05-030-NNTP.c.php>

Alarm Over Plug and Play Vulnerability

Curt Woodward, "Microsoft trying to fix security hole." Business Week, 9 August 2005.

http://www.businessweek.com/ap/financialnews/D8BSKH180.htm?campaign_id=apn_home_down&chan=db

Honeymonkey

Robert Lemos, "Flies swarm around MS Honeymonkey." SecurityFocus, 9 August 2005.

http://www.channelregister.co.uk/2005/08/09/ms_honeymonkey/

Mike Nash

Sean Michael Kerner, "Has Microsoft Made Security Strides?" Internetnew.com, 11 July 2005.

<http://www.internetnews.com/security/article.php/3519246>