

**The Demise of the Mass Mailer?**  
**gordon@infectionvectors.com**  
**December 2004**

**Overview**

Since 1999 mass mailer worms have plagued Internet users everywhere. In each year following Melissa at least one mass mailer has grabbed the spotlight as the most prevalent and damaging virus of the year, from Nimda to MyDoom.<sup>0</sup> Some virus analysts have predicted that the mass mailer will decrease in popularity as a vehicle for malware in 2005 and has seen the peak of its life cycle. This article looks at the reasons given by the analysts and argues against their positions, positing instead that the mass mailer will continue to flourish in 2005 and will see additional improvements as a medium for transporting malcode.

**A Look at the Present**

To begin with, two quotes summarize the theory that the mass mailer is doomed in 2005. The position of Kevin Hogan (Symantec Europe) was presented in "The Register"<sup>1</sup>:

Mass mailing viruses will go the way of macro viruses and become much rarer next year. Viruses such as Sober and MyDoom are simply not as effective as they used to be, Kevin Hogan, a Symantec Europe manager, notes. "People know it's risky to double click on viruses. For virus writers there's no technical kudos. Also mass mailing viruses are noisy, bringing attention to themselves, and that goes against the trend of developing malware that hides its presence on infected systems," he said. December 9, 2004

Larry Seltzer predicted a similar fate early in the summer in an article that promotes the idea of an informed general user base refusing to open unsolicited attachments<sup>2</sup>:

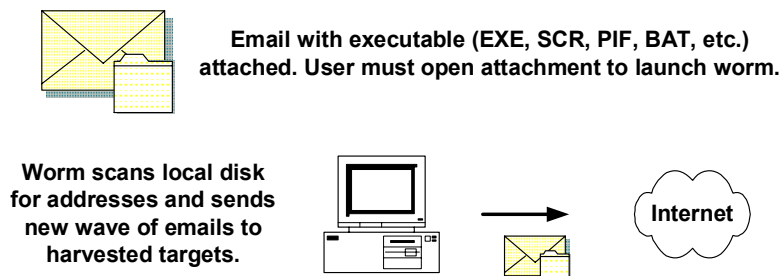
Since then [the Melissa worm], mass-mailer worms have undergone a variety of technical innovations and encountered a variety of countermeasures. But really, after the first one it should have been possible to tell any of them just by looking at them. But even if there are people who will never learn their lesson about these things, the era of the mass-mailer worm is coming to a close. June 7, 2004.

Although it is the position of this paper that these predictions are a bit early, both analysts above make excellent points about future virus releases and the challenges would-be malware authors will have. In fact, later in his article, Seltzer indicates the new firewall, antivirus, and mail client software will all contribute to the demise of email-borne worms. This is absolutely true, but the adoption of these technologies will not affect the number of email worm reports or infections next year, as the innovation on the worm coder's side will continue to improve as well. Seltzer does hit the one technology that will signal the end for mass mail of all kinds: SMTP authentication mechanisms. Although that is

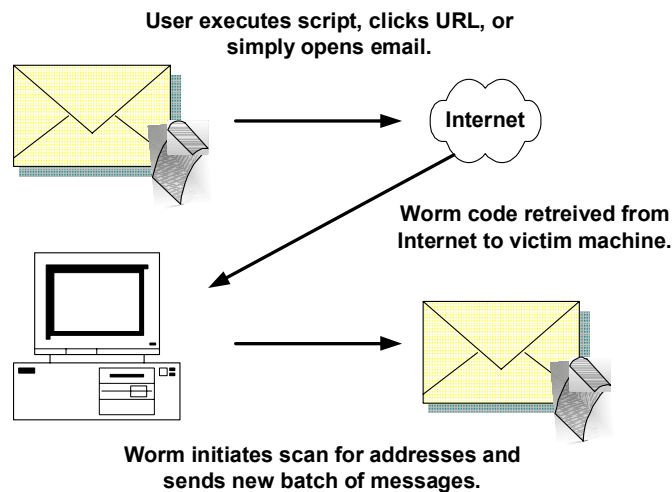
precisely the type of change that needs to occur to fight mail abuse on many fronts, its development and adoption has been slow.

### The Mass Mailer

Mass mail worms work by emailing malicious code to a user. Historically, the worm would be completely contained in the message, generally as an executable attachment.



Recent attempts to infiltrate PCs via email have included only a link or script file that kicks off a routine to retrieve additional code and execute it on a machine. The benefit of packaging exploits in this manner is that there is no attachment for a mail gateway to strip (a common means of defeating mass mailers). The diagram below describes the basic action of such mail-borne worms.



However a mass mailer infects a device, its goal is almost invariably the same: discover new targets by scanning the local hard disk or making network/Internet requests for email addresses so it can spread to additional machines. Each virus has a different set of routines it carries out after infection, however, each must propagate to new hosts in order to survive.

The modern era of email worms began with Melissa in 1999. Although there were other applications that proved the potential for mail as a virus medium (Happy99 for example, intended to look like a New Year's greeting), Melissa's global reach and slew of variants ushered in the use of email as a common attack vector. David Emm of Kaspersky Labs

noted that Melissa, “marked a quantum leap forward in terms of speed of infection.”<sup>3</sup> Over the next five years mass mailers would make great strides in both technical innovation and social engineering tricks. These improvements were not simply academic, the development of new mass mailers has led to an increasing number of successful infections; mass mailer worms account for thousands of compromised devices every year. In fact, in 2004 mass mailers took 9 of the top 10 spots for virus reports (Sophos 2004).<sup>4</sup> For November 2004, Viruslist.com shows all of the “Virus Top Twenty” entries are worms with at least their primary propagation routine involving email (Sober being the only “pure” mass mailer, the others such as LovGate also spread via file shares).<sup>5</sup> More relevant are actual infections (where a virus successfully installed itself on a machine), measured in part by Trend Micro’s worldwide compilation. Trend’s reports routinely show 7 of the top 10 infectors to be mass mailers.<sup>6</sup>

Mass mailer worms are successful for a number of reasons: the ease with which they are written, the curiosity of most users, and the insecure nature of SMTP. Mass mailers have taken many forms, from the VBS-constructed Anna Kournikova through the C++-based SoBig. Building a simple SMTP engine is not much of a task for someone familiar with any of these toolsets. In addition, there are plenty of pre-built mailers for any aspiring virus writer to use. Email can instantly mobilize any viral code, making it a quick way to give a Trojan/virus “legs” when releasing it onto the Internet. There are no advanced coding skills required to employ SMTP as the transport as there are with an Internet worm (where a carefully crafted and tested exploit is required to infect a machine).

User curiosity guarantees that attachments will be opened, sometimes just to “see what happens.” Although user ignorance or curiosity is often the focal point for security professionals, some credit must also be given to the well-designed messages that carry viral attachments. Some malware coders have made taken great care to make a message appear to come from someone the recipient knows, that the attachment was scanned with an antivirus program, or to send a mass mailer with no attachment at all (such as the exploit carried by Bofra).<sup>7</sup>

SMTP itself makes it relatively easy to reach a great number of targets. The mail protocol was not designed with much security in mind; the great majority of email systems still in use do not require authentication to relay mail to their users. The overwhelming spam issues that administrators face everyday all point to the simplicity of blanketing the Internet with email, whether it carries an advertisement or a virus. Mass mailers are easy to distribute (especially given the existing infrastructure of spam relays/compromised machines). Although many mailers peak quickly and then become quite rare (Netsky variants being the most noticeable exception this year), they still touch thousands of machines in a short time period. This allows a nefarious coder to exploit machines before users are notified about a specific worm or antivirus definitions are updated.

Email itself is a worldwide entry point for system access. In an instant an attacker (using the same successful tactics as a spammer) can get their code in front of thousands of users in their target audience. Internet worms rely on a system being connected at the very instant an infected machine is scanning for hosts (even with the proliferation of worms

like Blaster and Sasser that seem to be ubiquitous across the Internet), this is not true for mailers that happily sit on mail servers waiting to be processed. A user may recognize the ploy, there may be an antivirus application running on the targeted machine, or the target may be using the wrong operating system to allow infection. In either case, these mitigating circumstances are not unique to mass mailers, they affect viruses of all types.

### **The Reports of the Mass Mailer Demise...**

Hogan and Seltzer each point to user awareness as a reason that email-borne worms will begin to die off. However, years after some of the most widely reported mass mail outbreaks (such as ILOVEYOU), worms like SoBig were able to infect countless machines. Even after newspapers and news broadcasts around the world picked up the “war” between Netsky and Beagle both worms continue to dominate “most reported” lists on antivirus sites. Furthermore, even if users begin deleting attachments, the latest trend in mail worms is to deliver only a link or exploit to an Inbox (see Beagle variants from the summer of 2004 and the Bofra worm).

The idea that mass mailers bring too much attention to their respective authors would be a deterrent if the attention was unique to that type of worm. However, the authors of some of the most damaging worms, such as MyDoom, Beagle, Sober, and LovGate are no closer to being arrested than the day the first version of each was released. Arrests from 2004 (which saw numerous high profile arrests) were split between mail worms and non-mass mailer malware. Although arrests for Sven Jashan (for Sasser netted a mass mail coder when it was confirmed that he wrote Netsky) and Magold author Laszlo K (as well as the author of Lasku) were reported, the arrest of the alleged Agobot creator, Blaster.F distributor, and other Trojans around the world indicate that any virus coding risks detection and imprisonment; mass mail is not inherently any noisier than an Internet worm.

Hogan points to the lack of stealth involved with mass mailers; these worms swallow a great deal of resources on local systems and increase the chances that they will be caught. Although this may be true of most mail-borne worms, it is not intrinsic to mailer functionality. Further, sending small email messages such as those sent by Bofra is not especially resource intensive, especially for high-powered machines now appearing in homes around the world. If detected, the mass mailer is likely to have already begun the dissemination of new messages, allowing the worm to spread. Even with the greater chance of detection, there is still a high return on investment for a mass mail author: the simplicity and speed of hitting a very high volume of targets affords some leeway when it comes to detection by an end user. It is the attacker that invests months in research and exploit development to hit a single target that cannot afford detection, not a mass mailer.

As for the trends in virus coding, they continue to support the use of mass email messages as a quick transport for malware. Graham Cluley accurately describes the reality for the global virus scene: “Virus writing has become more about trying to generate money than creating mass mailing worms”.<sup>8</sup> It isn’t that mass mailers themselves are doomed to extinction, it’s that the trend is away from creating chaos

through mass mail. The mailer still has a prominent place as virus medium, but now it is being refined to exploit its strengths: quick, worldwide dissemination.

### **Is the End in Sight?**

The greatest threat to email viruses is the improvement in anti-spam technology. As spam is controlled, with either secure SMTP implementations or gateway filtering, mass mailers will suffer and lose their place as a viral transport.

Mass email will continue to have its share of the virus market throughout 2005, and probably 2006. Innovations like those seen with 2004's Beagle worm will push the medium to new heights.<sup>9</sup> The simplicity and public availability of mass mail engines ensures its survival as a popular worm mechanism. The curiosity of most users will ensure that mass mail enjoys success for years to come. The traditional definition of a mass mail worm will continue to evolve as well, looking much more like the latest versions of Bofra than the self-contained grandfathers of the mail worm like Melissa or Sircam. Mass mailers will continue to be the launching point for worms like LovGate and the infamous Nimda, using email as the way into a system so that other propagation mechanisms like file share copying and network vulnerabilities can be used as infection vectors.

Finally, the success and popularity of mass mail worms will only fall off as unique threats to unauthenticated global mail delivery are in place. The indicators noted by the analysts above (user education, attention to coder, risk of discovery/removal) are far from new; they have all existed since 1999 and should have caused the death of the species long ago. Until fundamental changes occur across the Internet, mass mail worms will continue to enjoy great success.

## Citations

0. It is at least arguable that the list looks like this: 2000: ILOVEYOU, 2001: Nimda, 2002: Klez.H, 2003: SoBig, 2004: MyDoom/Netsky/Zafi.
1. “The strange death of the mass mailing virus” John Leyden, December 9, 2004.  
[http://www.theregister.co.uk/2004/12/09/symantec\\_virus\\_forecast\\_2005/](http://www.theregister.co.uk/2004/12/09/symantec_virus_forecast_2005/)
2. This article points to a lot of the reasons viruses as a whole should be on the decline and why mass mailers will eventually have to make tremendous adjustments.  
“The End of the Mass-Mailer Worm Era” Larry Seltzer, June 7, 2004.  
<http://www.eweek.com/article2/0,1759,1607743,00.asp>
3. “Traditional antivirus solutions – are they effective against today’s threats?” David Emm, Kaspersky Labs, October 17, 2004.  
<http://www.viruslist.com/en/analysis?pubid=153595662>
4. Sophos 2004 Virus Review  
<http://www.sophos.com/pressoffice/pressrel/uk/20041208yeartopten.html>
5. Viruslist November Top 20  
<http://www.viruslist.com/en/analysis?pubid=155727022>
6. At the time this was written, it was difficult to find anywhere in the world not covered with reports of mass mail worms.  
Trend Micro Virus Detection Map  
<http://www.trendmicro.com/map/>  
  
Additional evidence of actual infections can be found at Panda Software’s site, which provides statistics in a similar fashion.  
[http://www.pandasoftware.com/virus\\_info/map/map.htm](http://www.pandasoftware.com/virus_info/map/map.htm)
7. Bofra Technical Details  
<http://www.viruslist.com/en/viruses/encyclopedia?virusid=65410>
8. “‘White collar’ virus writers make cash from chaos” John Leyden, December 7, 2004.  
[http://www.theregister.co.uk/2004/12/07/sophos\\_av\\_review\\_2004/](http://www.theregister.co.uk/2004/12/07/sophos_av_review_2004/)
9. “The Beagle Worm History” Parts 1 and 2, Jason Gordon, 2004.  
<http://www.securityfocus.com/guest/24228> & <http://www.securityfocus.com/guest/24231>

### **Additional References**

“Worming the Internet – Part 2” Katrin Kocheva, November 2001.  
[http://www.virusbtn.com/magazine/articles/features/2001/11\\_01b.xml](http://www.virusbtn.com/magazine/articles/features/2001/11_01b.xml)

“The Year of the Worm” Bill Hayes, August 16, 2001.  
<http://www.securityfocus.com/infocus/1291>

“MyDoom.A: Fastest Spreading Virus in History” Jay Munro, February 3, 2004.  
<http://www.pcmag.com/article2/0,1759,1485719,00.asp>

“Virus arrests across the world” July 4, 2004.  
<http://www.viruslist.com/en/news?id=1815104>

Beagle.AN (Beagle without attachments as referenced above)  
<http://www.viruslist.com/en/viruses/alerts?alertid=2140045>