



**Superbug:  
Antibacterial Soap & the Net  
infectionvectors.com  
June 2007**

**Overview**

The spring of 2004 may bring back fond memories for malware researchers. The rise of the “virus wars” between Bagle, MyDoom, and Netsky authors was responsible for a lot of headaches, but also glorious battle stories for worm warriors.<sup>1</sup> Although this notable period in malware history produced well-known malicious code, there were few who would have guessed that any specific worm would have remained successful a full three years later. However, that is the case for Netsky, whose variants continue to appear in top twenty lists for prolific malware.<sup>2</sup>

Of interest is what makes worms such as Netsky<sup>3</sup> successful, able to extend normal life expectancies into legendary infection periods. Are some worms just lucky, better engineered (whether technically or socially), or employing specific technical tricks that allow it to evade traditional defense mechanisms? In the physical world, researchers are concerned with the emergence of “superbugs,”<sup>4</sup> bacteria that survive floods of antibiotic treatments only to multiply, filling the void left by the weaker, succumbing germs. Superbugs evolve more quickly as a result of the very treatments that are intended to stop them. A correlation in the digital world is discussed in this report.

**The Diagnosis**

Netsky, which was, from a technical standpoint, the least impressive of the three families,<sup>5</sup> continues to insert the circa-2004 revisions of itself in the “most reported” malware lists. The worm does not take advantage of some powerful technical exploit – it depends wholly upon a recipient opening its attachment. The list of possible email subjects/bodies does not appear to be especially poetic, in context of other successful mass mailers, although, in Netsky’s favor is the fact that it’s “E” variant (Symantec) which is one of, if not the most, successful of the iterations, carries 80 possible subject lines and 261 messages. Some of these 261 message texts include:

```
-here is the document.  
-I've found your bill!  
-You are infected. Read the  
details!  
-<Transfer complete>  
-you cannot hide yourself! (see  
photo)  
-<Server Error>
```

One could see the use of so many subjects/messages as the result of awareness training: as companies, ISPs, and the media became efficient at spreading “watch lists” for worms like Melissa, the mass mailer writer responded by making it impossible. The countermeasure/reaction spiral continued with successive waves of malware. As signature-based products improved effectiveness malware coders used encryption and polymorphism with improved precision. Worms are released in 100 or 1,000 forms from day one, instead of waiting for infections to produce a new version of the code.

Of course, none of these “evolutionary” steps is indicative of the same process as that which produces drug-resistant bacteria/viruses.<sup>6</sup> “Superbugs” are the result of killing off the weaker (non-drug-resistant) bacteria and allowing drug-resistant (but not necessarily more resistant to heat, cold, antibodies, etc.)<sup>7</sup> strains to flourish. Although popularized during the “virus wars” of 2004, it is not especially common to find a worm that removes other worms from an infected machine. The impact of which is that multiple pieces of malware can easily exist on a single system; there is little (if any) competition in the cyber virus world. Just like antibiotic resistance, just because a worm dodges antivirus software does not mean it is stealthier, stronger, or more damaging than another. However, it will survive, have the opportunity to execute its payload, and spread.

### **Treatment**

Certainly, a direct correlation between Internet worm success and antivirus success is available. If a security product is effective at removing some worms, then what is left will dominate the “most seen” lists. This is not a function of the worm evolving though, but rather mathematical probability. If a polymorphic worm takes 1000 forms, and our detection engine can catch 999 of them, we would say that the success rate is a solid 99.9%, very effective. Yet, we know that there is a survivor, running its automated track across the net as fast as it is (programmatically) able.

Our current treatment for worm development is signature-based antivirus software, whether in the form of traditional client-based tools or intrusion

detection/prevention devices. Some “signatures” can catch lots of different virus strains, they can be thought of as the “broad spectrum antibiotics” of the Internet. If a coder beats those generic detections, is able to dodge the heuristic capabilities of the security community, he or she has gone a long way to ensure the longevity of the malware.

Returning to the example above, let us make an important note concerning an antivirus product that is 99.9% effective: effectiveness is based on the organism that employs the countermeasure. That is, an antibiotic is effective at killing bacteria, within one person. Antivirus software is effective, one machine at a time. If there was a means of applying anti-malware software to the whole of the Internet, worms such as Netsky would be much quicker to disappear.

Alas, it is not the malware that actually responds to its predator – at least at this point. Currently, a virus writer must observe what traits make successful malware strains and react accordingly. The Bagle worm writer noted the success of encrypting attachments, and sent ciphered copies of the code. Later, as antivirus companies reacted with an improved scanning mechanism (one that lifted the password from the accompanying email), the author made that an image file, thwarting decryption attempts.

Years after the “virus wars,” the tactics of virus writers remain largely the same: polymorphism (both manual and automatic), widespread distribution, and encryption. In January 2007, Peacomm included wide spamming as its delivery mechanism (using another mass mailer to travel), rootkit technology to hide

from the digital antibodies, and advanced communications techniques (in the form of a peer-to-peer network).<sup>8</sup>

More recently, we've seen malware develop in places we didn't previously have defense mechanisms at all. In May of 2007, TIOS.Tigraa, a virus written for Texas Instruments calculators was catalogued.<sup>9</sup> Infecting undefended operating systems is another conscious evolution of the malware ecosystem, directed by very security-aware coders.

### Scrub Up

Instead of attempting to kill every bug, medical professionals have said that washing germs away as often as is possible will reduce one's exposure to germs significantly enough to reduce risk – without risking superbug development (unless, of course, we're talking about antibacterial soap...). A correlation for the Internet doesn't truly exist, as detection and destruction are virtually the same – unless one is speaking of virtual execution.

Conceivably, an intelligent antivirus detection system could execute a piece of malware in a sandbox and deliver any outbound communication that occurs as part of its installation routine. Of course, any installation routines would be dumped (along with spamming, DoS, etc.). The potential benefit of such a scheme would be to fool the command and control arm of the malware outfit – making it look like a full army of bots existed when in fact there was a much smaller set of zombies awaiting the (for-profit) directives. If those paying for leased bot nets could not be sure there was going to be a return on their investment, less of an investment may be

made. The idea of a virtual infection could be replicated across countless virtual machines inside honeypots – in theory flooding the command (or peer-to-peer nets) with junk.

If a particular strain of bacteria is resistant to penicillin, another antibiotic is used. If an Internet worm dodges a host's antivirus, it is not likely that another product would be used, as most infections are not obvious as they were in the days of Stoned.<sup>10</sup> As malware changes its traits, maybe it is necessary for antivirus programs to do the same. "Polymorphic antivirus," could take the form of a scan engine that uses variable names, signature sets, and means of reading files. The scanning program could itself hide from the computer it is installed on (rootkit-style technologies), employ both local and web-based scanning, and various virtual environments (as noted above).

Technological advances are equally possible on both sides. Whenever a coder makes a better antivirus, a malware developer will produce a new attack. Keeping a system free of germs is a matter of good practice – running your data environment in a professional manner. Although we have tried to come up with the most complete set of heuristic capabilities, the universal advice for email scanners is to block all EXE attachments. We have accepted that certain things present too much risk when compared to their benefits. Good awareness programs, sound filtering, minimal reliance on the client antivirus program, and process-based incident response still dominate professional practices. Virus protection advice for systems on the Internet is best summarized as, "wash your hands."

## References

1. Michelle Delio, "At the front in the virus war." Wired, 18 February 2004.  
<http://www.wired.com/techbiz/it/news/2004/02/62324#>
2. The Viruslist.com Virus Top Twenty for April 2007,  
<http://www.viruslist.com/en/analysis?pu bid=204791937>  
Netsky takes 4 of top 20 spots, including #1.
3. Netsky.T (Viruslist) was catalogued in June of 2004.  
Email-worm.Win32.NetSky.t  
<http://www.viruslist.com/en/viruses/encyclopeda?virusid=48821>
4. A discussion of "superbugs" is in order for those interested. See, Tamar Nordenberg. "Miracle Drugs vs. Superbugs" FDA Consumer Magazine (November-December 1998).  
[http://www.fda.gov/fdac/features/1998/698\\_bugs.html](http://www.fda.gov/fdac/features/1998/698_bugs.html)
5. Certainly, any successful piece of malware is somewhat impressive; Netsky, however, did not include the technical tricks or professional development cycle of its competitors like Bagle and MyDoom – preferring the straight-ahead tactics of many earlier worms (i.e., "here's an email attachment, open it"). For more information on these practices, please see [http://www.infectionvectors.com/library/years\\_of\\_the\\_beagle.pdf](http://www.infectionvectors.com/library/years_of_the_beagle.pdf).
6. The concept of evolving virus code was examined in the infectionvectors.com paper: Viroolution.  
<http://www.infectionvectors.com/vectors/viroolution.htm>.
7. Which begs the question as to how super a superbug really is; if it is resistant to antibiotics, we have given it elevated status – when maybe the bacteria is easier to kill with a vitamin supplement, or heat/cold, or any of an infinite number of possible treatments.
9. TIOS.Tigraa at Symantec  
[http://www.symantec.com/enterprise/security\\_response/writeup.jsp?docid=2007-060115-3305-99&tabid=2](http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-060115-3305-99&tabid=2)
8. Peacomm at Symantec:  
[http://www.symantec.com/security\\_response/writeup.jsp?docid=2007-011917-1403-99](http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99).  
Known as Small.DAM at F-Secure:  
[http://www.f-secure.com/v-descs/small\\_dam.shtml](http://www.f-secure.com/v-descs/small_dam.shtml).
10. Information on the Stoned virus:  
<http://www.ciac.org/ciac/bulletins/a-28.shtml>.

Copyright © 2007 infectionvectors.com.  
All rights reserved.