

Netsky and the Secrets to Success
infectionvectors.com
February 2005

Overview

Next month (March 2005) will mark the first anniversary of the release of Netsky.P, the most successful Netsky variant to date, and the most prevalent single virus of all of 2004. Although much has been written about the mass mailer and its “war” with Beagle, the information is generally focused upon the technical attributes of the worm and how to avoid/clean the code. This report examines the reasons this worm has found such success, even in the face of a number of obstacles and shortcomings that should have precluded its widespread distribution.

Based on the tremendous attention that Netsky.P has received, the usual review of the program is not part of the report proper. Anyone unfamiliar with the details of this worm, including how it works and propagates, should take a moment to review the Appendix.

The Netsky is the Limit

The first version of Netsky was distributed in February of 2004. That worm was a much simpler incarnation of the mass mailer than later variants. The original release had a single email message and a short, plain list of attachment names. Netsky.P was released on March 21, 2004, after a wave of variants spurred by a well-covered battle between Beagle and Netsky in which the participants used successive iterations of their respective worms to remove the others. As of this writing, Netsky.P continues to enjoy tremendous success, in terms of reaching a high number of users and infecting machines. As of February 21, 2005:

- Netsky.P remains a Level 3 (of 5, 5 being the highest) at Symantec’s Security Response
- CA Classifies the Threat as High; remains a Top Five reported threat
- Trend Micro’s Virus Map lists it as #2 in most infections in the last 24 hours (while it holds the top spot for infected files)
- Panda Software categorizes it as Threat Level 4 (highest)
- McAfee’s Top Threats list continues to hold Netsky.P
- Sophos proclaimed 2004, “
- Virus Bulletin’s compiled Virus Prevalence statistics show Netsky as the most reported piece of malware with over 50% of total reported instances

Many of the reports are likely due to the sheer number of copies Netsky makes of itself; a single infection can produce thousands of copies on a single machine (and routinely did so in lab tests). However, the long life of this mass mailer (which generally reach a peak quickly before trailing off) is not fully explained simply by the number of copies it creates.

How to Succeed at Virus Writing...

The reason Netsky.P has found its way onto so many machines is no secret at all: it combines a multitude of traits into a worm that exploits human curiosity, often referred to as social engineering. The previously mentioned “war” with Beagle also seems to have helped the virus writer (the admitted author, Sven Jaschen was arrested in the summer of 2004) develop his code. Many of the tricks employed by the worm were used by Beagle variants with great success. The following list outlines the most notable of these traits, in no particular order:

- 1) The worm uses the return address “lola@sexnet.com” sometimes instead of a randomly selected target address. Sex sells, anything with “sex” in the header is going to catch its share of curious recipients.
- 2) Many of the email messages the worm sends have a subject line that starts with a “Re:” and sometimes more than one. This trick makes people believe the message is a response to something they sent, or at least that the string was started by a human, not a virus. Similar tricks have been employed by other mass mailers, including Lovgate variants that actually did respond to messages with a copy of the worm.
- 3) Varied subject lines and message bodies are used liberally; this includes 30 pre-written messages and thousands of combinations of hard-coded message components. The tremendous variety prevents effective warnings based on specific attributes as the worm changes its wrapper so widely.
- 4) “Scanned by” line added to email messages gives many recipients comfort. The use of “+++Attachment: No Virus Found” and an AV vendor’s name snares a few more people.
- 5) Innocuous attachment names don’t raise the suspicions of anyone hoping to discern whether a file is malicious based on its title. Filenames such as “document05” and “game” are unlikely to trigger many alarms.
- 6) The use of double extensions (and placing blank spaces between the “harmless” extension and the executable extension) probably tricked a great many recipients.
- 7) Thousands of enticing file share copies helped draw in more people willing to execute the worm. Most of the filenames used are directed at those interested in viewing pornography or illegal software cracks, always helpful.

In Spite of Itself

There are also a few reasons that this code should not work quite as well as it has. These have obviously all been overcome by the worm.

- 1) The file dropped by the worm responsible for propagation has a static size. For all the work put into polymorphic code detection, it may seem that files with a constant size,

MD5 hash, etc. are not as threatening, however, Netsky proves that advanced coding techniques are not required for successful worms.

2) Netsky does not appear to have been “seeded” in the way that Beagle and MyDoom variants have been. The author needed to distribute the worm “manually” so to speak, finding his own means of delivering it to thousands of people.

3) The common name of Netsky.P in the anti-virus community. Researchers often point out that misaligned naming makes analysis and eradication difficult, however, the use of an agreed upon name has not helped remove Netsky.

4) It's removed by some pretty successful viruses. Given that most boxes infected with Netsky are not going to have current anti-virus software running and that their users are prone to opening suspicious email attachments, it would seem that widely distributed Beagle variants would be in a good position to remove Netsky.P (and prevent it from running).

U'l't'i'm'a't'i'v'e 'E'n'c'r'y'p't'e'd 'W'o'r'm'D'r'o'p'p'e'r' 'b'y 'S'k'y'N'e't'. 'C'Z'

Netsky's success is a testament how well a worm can do if it simply is given a few of the right tools. Namely, those tools include a wide variety of “wrappers” (subject lines, message bodies, and attachment names) and a convincing story (although short in the Netsky case, the message bodies are enticing enough to grab the attention of thousands of users).

In the war against viruses, we continue to see that a well- (socially) engineered worm can have a dramatic impact on the Internet, even a year after its release.

Appendix: Netsky.P Infection and Propagation

Netsky.P arrives as an email attachment or through a file sharing application. A user must execute it to infect a machine. Once opened, the worm does the following:

Copies itself to the Windows directory as FVProtect.exe (which launches the virus) and userconfig9x.dll (which holds the propagation routine code). In addition, it hooks the Registry with a startup entry, executing FVProtect.exe each time Windows is launched. It then drops 3 MIME-encoded copies of itself, a Uuencoded copy, and a ZIP archive of itself in the Windows directory. The two applications (FVProtect and userconfig9x) have different mutex names, 'D'r'o'p'p'e'd'S'k'y'N'e't' and _-oO]xX|-S-k-y-N-e-t-|Xx[Oo- _ respectively.

Netsky.P, like its relatives, then removes Registry entries associated with Beagle and MyDoom.

The program then drops multiple copies of itself in any folder whose name includes any of the following strings: bear, donkey, download, ftp, htdocs, http, icq, kazaa, lime, morpheus, mule, my shared folder, shar, shared files, upload. The file is copied with the following names:

```
1001 Sex and more.rtf.exe
3D Studio Max 6 3dsmax.exe
ACDSee 10.exe
Adobe Photoshop 10 crack.exe
Adobe Photoshop 10 full.exe
Adobe Premiere 10.exe
Ahead Nero 8.exe
Altkins Diet.doc.exe
American Idol.doc.exe
Arnold Schwarzenegger.jpg.exe
Best Matrix Screensaver new.scr
Britney sex xxx.jpg.exe
Britney Spears and Eminem porn.jpg.exe
Britney Spears blowjob.jpg.exe
Britney Spears cumshot.jpg.exe
Britney Spears fuck.jpg.exe
Britney Spears full album.mp3.exe
Britney Spears porn.jpg.exe
Britney Spears Sexy archive.doc.exe
Britney Spears Song text archive.doc.ex...
Britney Spears.jpg.exe
Britney Spears.mp3.exe
Clone DVD 6.exe
Cloning.doc.exe
Cracks & Warez Archiv.exe
Dark Angels new.pif
Dictionary English 2004 - France.doc.ex...
DivX 8.0 final.exe
Doom 3 release 2.exe
E-Book Archive2.rtf.exe
Eminem blowjob.jpg.exe
```

Eminem full album.mp3.exe
Eminem Poster.jpg.exe
Eminem sex xxx.jpg.exe
Eminem Sexy archive.doc.exe
Eminem Song text archive.doc.exe
Eminem Spears porn.jpg.exe
Eminem.mp3.exe
Full album all.mp3.pif
Gimp 1.8 Full with Key.exe
Harry Potter 1-6 book.txt.exe
Harry Potter 5.mpg.exe
Harry Potter all e.book.doc.exe
Harry Potter e book.doc.exe
Harry Potter game.exe
Harry Potter.doc.exe
How to hack new.doc.exe
Internet Explorer 9 setup.exe
Kazaa Lite 4.0 new.exe
Kazaa new.exe
Keygen 4 all new.exe
Learn Programming 2004.doc.exe
Lightwave 9 Update.exe
Magix Video Deluxe 5 beta.exe
Matrix.mpg.exe
Microsoft Office 2003 Crack best.exe
Microsoft WinXP Crack full.exe
MS Service Pack 6.exe
Netsky source code.scr
Norton Antivirus 2005 beta.exe
Opera 11.exe
Partitionsmagic 10 beta.exe
Porno Screensaver britney.scr
RFC compilation.doc.exe
Ringtones.doc.exe
Ringtones.mp3.exe
Saddam Hussein.jpg.exe
Screensaver2.scr
Serials edition.txt.exe
Smashing the stack full.rtf.exe
Star Office 9.exe
Teen Porn 15.jpg.pif
The Sims 4 beta.exe
Ulead Keygen 2004.exe
Visual Studio Net Crack all.exe
Win Longhorn re.exe
WinAmp 13 full.exe
Windows 2000 Sourcecode.doc.exe
Windows 2003 crack.exe
Windows XP crack.exe
WinXP eBook newest.doc.exe
XXX hardcore pics.jpg.exe

Netsky.P then harvests email addresses by scanning the local hard disk. The addresses are plugged into two types of messages: some randomly crafted from lists of subjects, bodies, etc. and some that are composed in the worm code. The attached code is also named in a similar fashion, by combing strings with numbers.

References

Trend Micro's Virus Map and Statistics

<http://www.trendmicro.com/map/>

CA Virus Information

<http://www3.ca.com/securityadvisor/virusinfo/default.aspx>

Panda Software Virus Information

http://www.pandasoftware.com/virus_info/

McAfee Virus Information

<http://vil.nai.com/vil/default.asp>

Virus Bulletin's Virus Prevalence statistics

<http://www.virusbtn.com/resources/malwareDirectory/prevalence/index.xml?current>

The F-Secure 2004 Review provides great details on Netsky's reach and the arrest of Sven Jaschen "F-Secure Corporation Data Security Summary for 2004"

<http://www.f-secure.com/2004/>

"Year of the Netsky" note by Sophos "War of the Worms"

<http://www.sophos.com/pressoffice/pressrel/uk/20041208yeartopten.html>