



Adworms
infectionvectors.com
May 2005

Overview

The security community has accepted the idea that a virus could be used to generate revenue at this point. Worms like SoBig¹ and Beagle² point to the profit-motivated virus developer as a real threat to the Internet. The extensive use of spyware to snare referral commissions and deliver users to advertisers provides additional evidence of the problem: money is a tremendous motivator, and legality/ethics won't be an obstacle.

Years Ago...

A report surfaced years ago about a company, ViruSystems, which intended to sell computer viruses on the open market, creating and customizing malicious code for its customers. The idea was that advertising space could be sold within the virus and all of the targets could be seen as consumers.

This, of course, was a hoax³ that circulated via email for quite a while, and may still be circulating. If it is, however, it is likely not viewed with the same surprise and outrage it once was. Consider the following passages from the hoax, which was designed as a fake interview with the CEO of ViruSystems:

Q: Ad space? Who would buy an ad in a virus?

A: How about the anti-virus makers such as Symantec and McAfee? There is real synergy. In a single email, you get a virus and an offer to buy the vaccine. It is so obvious, I don't know why nobody has thought of it before."

Certainly no antivirus vendor has attempted such a thing, however, there are numerous accusations of extortion just like the example above in the spyware world.⁴

Q: Hence your marketing slogan.

A: Yes. 'When computer viruses are outlawed, only outlaws will have computer viruses.'

Q: The gun lobby would be proud.

A: The parallels are undeniable. Like gun makers, we produce and sell weaponry. But remember, we also have an additional revenue stream: we sell advertising space on the bullets.

Again, the “drive-by infection” techniques used by a great many spyware samples (and the creation of a breed of malware some refer to as adware/spyware) is much like putting an ad on the bullet. Although most people are greatly annoyed with adware tactics and attempt to remove the applications, the advertisements themselves are still reaching their targets and spyware companies still reap the referral-per-click revenue.

Q: OK, let me ask you this: viruses are free, so assuming the 'virus collector market' is not fiscally material, why would nihilistic programmers actually spend money on what they now make or get for nothing?

A: Virus creators are cost-conscious, that is true. But they are also conscious of technology and outcome. If they can build or download a free virus that wipes out a few jpeg files, or buy an outrageous virus that erases a hard drive, we think they will choose the latter.

Worms such as Mytob have shown the advantages of taking code from multiple successful places and combining it into a revenue generator rather than attempting to create completely new code. Taking the MyDoom propagation mechanism and the functionality of Sdbot allowed malware producers to turn profits without sinking a tremendous amount of capital into program development. Granted, kits such as Agobot are free, however, there are cases of people selling custom versions of bots as well as the compromised zombie networks for malicious purposes.

Although the original “warning” was a hoax, would there really be anything surprising about a spyware company that solicited customers? Most users would likely agree, as security professionals have seen, that this probably already exists.

Some companies that believe their products are far from “spyware” have sued anti-spyware organizations, having the incorrect categorization corrected.⁵ The effect this will have on the spyware cleaning products in the long term has yet to be seen, however, software that carries an end user license agreement (EULA) may well be immune from automatic removal.

Build a Better Mousetrap

With the line between adware/spyware and an Internet worm as blurry as ever (if one ever believed there was a difference), it should be no surprise that successful worms are being enlisted to install adware. The Opanki worm⁶ released in April of 2005 takes the worm/spyware links to new levels, using the infection vectors and methods of an instant messaging (IM) worm like Bropia⁷ or Kelvir⁸ and the payload of the average spyware application. Opanki attempts to retrieve 9 separate families of spyware (a total of 14 different packages for Opanki.B) or a bot client (SDBot retrieved by Opanki.C⁹).

Additionally, Nemog¹⁰, a Trojan that establishes a spam relay on an unsuspecting user’s machine has been found to travel with an unusual partner (not the MyDoom derivatives it originated with), the most reported worm of the last year, Netsky. Recently, Symantec offered evidence of such a team-up with the description of Netsky.AI.¹¹

As source code for successful worms finds its way to the public sphere it is likely that repeat examples will be found. The release of such code is not required. There are plenty of coders talented enough to create a network worm capable of retrieving additional applications from the Internet.

The challenge for spyware-removers will be to remove what they legally can when a worm drops it. Once the EULA is removed completely from the equation, there should be no restriction on what can be cleaned from system.

Spyware distributors have already shown a proclivity to use forced installations (via “drive-by” vectors through web browsers), hidden files, random filenames, and a host of other obfuscation tactics to prevent users from identifying and removing software. It is not technical prowess that limits the installations of these programs, only the motivation to adopt the exact same strategies of most worms; the inclusion of exploits such as the Windows LSASS overflow (MS04-011).

Consider the vectors already adopted by spyware distributors:

- Web Browsers/Active Content (so-called “drive-by” installs)
- Email (via links that are mass mailed and lead to content like that noted above)
- Passive Links/Banner Ads
- IM Worms
- Attached to Unrelated Software (such as the traditional Trojan Horse)

Others are sure to follow as long as the operation is profitable.

Ad in a Virus?

To answer the fictional question from the ViruSystems hoax, there are considerable buyers for such an advertising medium. Most already exist, although they may not know how the message is being delivered. The continued profitability of spam, adware, browser hijackers, and spyware will propel the underground empire of malicious code to new levels. One day the idea that there was separate categorization for adware and spyware may seem ridiculous to end users, as the daily threats will be dominated by such code.

Malware defense of all types, from user awareness to technical mitigation efforts are still the best protection against all types of unwanted code. For more information, please see the resources available at <http://www.infectionvectors.com>.

References

1. SoBig Information
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?vname=worm_sobig.a
2. Beagle Information
<http://infectionvectors.com/malagents/beagle.htm>
3. The ViruSystems Hoax
<http://www.symantec.com/avcenter/venc/data/virus.business.html>
4. Spyware Extortion
http://spywareblog.com/index.php/2004/10/11/the_ftc_alleges_spyware_extortion_1
5. "See you later, anti-Gators?" Paul Festa, 22 October 2003. CNET News.com.
http://news.com.com/2100-1032_3-5095051.html
6. Opanki.B
<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FOPANKI%2EB&Vsect=T>
7. Bropia Information
http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?idvirus=57910
8. Kelvir Information
<http://www.sophos.com/virusinfo/analyses/w32kelvira.html>
9. Opanki.C
<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FOPANKI%2EC>
10. Nemog.D
<http://securityresponse.symantec.com/avcenter/venc/data/backdoor.nemog.d.html>
11. Netsky.AI
<http://www.symantec.com/avcenter/venc/data/w32.netsky.ai@mm.html>