



Disposable Victory
infectionvectors.com
July 2005

Overview

Recent research has pointed to two complementary trends in malware propagation: the increasing prevalence of spyware and worms on client devices and the proclivity of users to simply replace their desktops instead of trying to clean them. This report examines the issues surrounding these trends and the implications of disposing of malware-infected devices.

Recycled

Malware authors frequently reuse propagation methods in their code. Take for example, the continued use of the DCOM RPC (MS03-026) and LSASS (MS04-011) exploits in new malware. New infection strategies often lead to a flood of new applications, built around the same public exploit code. The average user rarely comes in contact with the technical specifications of patches for these flaws, a system that is encouraged by most OS vendors. The lack of technical awareness is not a problem in itself, as many PC owners allow automatic update programs to run in the background on their computers.

Replacement Parts

The difficulty in staying on top of spyware is apparent. Without making a technical case for how fast spyware develops, how it embeds itself into a system, and how difficult it is to remove, one can point to the inability of existing "anti-malware" software to clean a PC as the strongest measure of spyware's strength. Users that have anti-virus software installed and updated are the most

Why is spyware/adware cited as the reason people ditch PCs when worms have been around for much longer? There are two reasons that make the most sense. The first is that adware suffers from one "handicap" that traditional malware does not: it needs to alert the user that it is running on their system. Adware is not doing its job unless it can redirect the browser, display pop-ups, or otherwise take the user to advertising sites. Hijacking is one of the most-recognized attributes of spyware, something that is an immediate tip-off to a user. Although worms will often swallow system resources in their efforts to propagate, this may not be noticeable to a user, or may be accepted as the machine is "getting older." Worms are not subject to the same requirements of successful adware and are free to explore all types of stealthing mechanisms.

Once on a system, spyware is notoriously difficult to remove. The pain involved in identifying, locating, and removing infections is all but impossible for home users. The path of least resistance to a clean PC has become purchasing a new box for many people, as outlined by the PEW study. This represents a group of users completely lost by anti-spyware products and picked up by hardware manufacturers.

In addition to being a sales driver for PC makers, spyware infections can now be cited as a reason for a machine appearing "broken" to an end user. Much like a television, which for years now has been a disposable appliance (cheaper to replace than repair), a PC is now approaching scrap status when unusable. In earlier years, this was an expensive proposition; even a nasty viral infection would spur a cleaning process, not abandonment. The idea that a \$300 computer (the low-end limit for most vendors) investment is preferable to removal attempts will certainly lure anti-spyware makers (who rarely charge over \$100 for even their multi-application suite products).

Market Sharing

A few years ago, even in the face of declining hardware prices, it would have been inconceivable that PC makers would be the beneficiaries of spyware's success. Although the number of users that throw in the proverbial towel and buy a new computer is still relatively low, they do represent a loss in market share for spyware makers. As the price of PCs continues to drop and anti-malware products improve, spyware will have to improve its resource management - in terms of both processor cycles and user fatigue. It may well be that the spyware/adware creators will have to throttle the amount of ads they expect a user to view, in efforts of making their "products" more palatable. This may sound unlikely, and even futile; however, the goal of the spyware pusher is simply to make living with their software less painful than a new purchase or lengthy cleaning sessions.

Adware has proven to be a profit-generator for its owners. That at least provides an impetus for evaluating a means to keep it on as many machines as possible. Other malware writers have shown the ability to apply process and product improvement techniques to their wares (see infectionvectors.com reports on Mytob and Beagle for examples); spyware creators, already business focused, are likely to follow suit.

Future Cycles

The increasing base and speed of broadband connections could allow ISPs to offer full application hosting from central servers, bringing the thin client into homes. This was something that was inconceivable at the outset of Internetworking to residential clients (as was most everything that has happened on the Internet), but something that could vastly improve the security of home machines.

Security professionals routinely point to the human element as the weakest link in the chain when hardening a system. The introduction of client-side web exploits is proving this over and over. Web surfing with unpatched browsers (or patched software and bad

habits), without firewalls, without intrusion detection/prevention, and the inability to recognize changes in system performance are dangerous traits on today's Internet. A full-service ASP could monitor file transfers, network activity (mostly between virtual PCs in theory), and patch levels.

Users are calling for such a program with constant complaints regarding the bewildering nature of security advisories and their required action. Moreover, the cost of such a program would be attractive to anyone willing to purchase a new machine to solve their problem with spyware.

The benefits to users are numerous: their entire PC would be available anywhere in the world, they would be freed from the technical burdens of security bulletins, and their data would be safer.

A cheaper solution for the average person is to simply re-image their existing system, an option given with almost every new computer. System restores are also a foreign process to many people, an intimidating effort for many home users.

The final solution to spyware is yet to reveal itself, however, the improvement of existing cleaning software is all but assured. With the ever-expanding market of spyware-affected users shouting their willingness to spend hundreds of dollars to rid themselves of malware, the software companies will undoubtedly race to bolster their offerings. Whatever direction spyware itself takes, it is unlikely that the average user will ever find themselves ahead of the malware authors.

References

"Corrupted PC's Find New Home in the Dumpster" Matt Richtel and John Markoff, New York Times, 17 July 2005. <http://www.nytimes.com/2005/07/17/technology/17spy.html>

PEW Internet & American Life Project, <http://www.pewinternet.org/>.

PEW Spyware Report Sussanah Fox, PEW Internet and American Life Project, 5 July 2005. http://www.pewinternet.org/pdfs/PIP_Spyware_Report_July_05.pdf

"Bug busting: Getting Rid of Spyware" Sandi Hardmeier, 21 March 2005, Microsoft. <http://www.microsoft.com/windows/IE/community/columns/bugbusting.msp>

"Webroot Enlists Bots To Fight Spyware" Thomas Claburn, Security Pipeline, CMP 11 January 2005. <http://securitypipeline.com/57700512>