



## **Blocking Spyware** **infectionvectors.com** **July 2004**

### **The Problem**

The overwhelming presence of spyware/browser hijackers on host machines is a daily problem for security administrators. There is a fine line between spyware and Trojan, one that is often blurred so badly that it is impossible to distinguish one from the other. Infectionvectors.com treats the spyware as class of Trojans. Whether the software pipes unwanted ads into a host, redirects browsing, or transmits web activity back to a tracking site, it is a Trojan if it is installed without the user's explicit consent or enables routines not known to the user. In addition, these pieces of software are often extremely difficult to disable and remove; reappearing after a user has decided to remove the code from their system. They are installed in many cases without any warning through flaws in browser components, just as a network worm would infect a machine through an unchecked buffer in a network service.

At the very least, the presence of spyware that is allowed to transmit data outside of the organization is a covert channel, a means of moving information from the private network that is often unseen and unchecked by network administrators.

Legitimate adware is distinct from this category as it is often a required component of otherwise "free" software. Although the means of alerting a user that the adware is contained in the product is often shaky (buried in long user agreements with vague language), the use of advertisements to fund freeware products is separated from this discussion, which attempts to draw out the hijack code as belonging to the virus family.

### **Installation Routines**

These beasts are notoriously difficult to remove from an infected system. Some of the more well known, such as CoolWebSearch (CWS) and LOP, use random file names for the Trojans, making them impossible for a user to look up on the web to identify. In addition, they overwrite default files and use encrypted URLs/scripts. Many types of spyware hide installation files so that even if the user deletes the visible associated Registry keys once, they return the next time the browser is opened.

### **The Infection Mechanisms**

Infection vectors for browser hijackers include ActiveX controls, exploiting flaws in the Microsoft JVM, and accepting downloads by blindly clicking "OK" to requests. The first two are the only ones considered here; system administrators will have to deal with users

through education and training. Beyond intentionally installing “freeware” onto a machine, allowing scripts to run within the browser (and then the local machine) is the top cause of spyware installations. These visit-generated (or drive-by downloads) installations are the bane of home and enterprise users alike. The short list below reviews a few major install tactics and how they may be combated.

### **ActiveX Controls**

ActiveX refers to a large pool of controls based on the OLE and COM foundations that pervade Microsoft products. ActiveX controls allow for a wide range of applications to run within the browser window, greatly expanding the range a developer has when coding a website. However, as with any technology, there are nefarious uses for ActiveX as well. When packaged as an ActiveX object, a web surfer may download and execute a program unwittingly.

### **Microsoft Java Virtual Machine**

Posted as Microsoft Security Bulletin MS03-011, there is a flaw in the Microsoft VM builds through version 3809. This application allows Java code to run on Windows hosts. The Microsoft JVM is no longer supported and is not rolled out with Windows (as of SP1a for Windows XP). However, the widespread deployment of this tool (Windows 95 through XP had builds that are vulnerable, it also came with many versions of Internet Explorer), it is a popular target for spyware/hijack programs.

The vulnerability involves the ByteCode Verifier, which incorrectly checks the validity of malicious agents. Most antivirus companies include the exploit routines for this vulnerability in their scans.

An older vulnerability alert, released as MS00-075, describes another flaw in the VM, allowing unsigned applets to execute any control (even if it is labeled “unsafe”) from a malicious web page.

### **IE Holes**

Much attention has been given to unpatched vulnerabilities in Internet Explorer (a similar hole was recently discovered in Mozilla Firefox as well) that allow one to install objects onto the local machine. The hotfix released for the vulnerabilities simply disables the ADODB stream hooks, something that can be done without the software.

### **Email Messages**

Enticing a user to visit a web page that is waiting with the exploits noted above is certainly possible by compromising other sites. However, it is possible to target many more users through spam. Including the link for the exploit/Trojan in an HTML-based message is much more effective than lying in wait for visitors. Clients that are not protected against spam, routinely open email from unknown sources (or leave the

Preview pane on), and do not have the latest patches installed on their workstations are in jeopardy of having Trojans installed this way (both those that install backdoors and those that hijack web access).

### Blocking the Vectors

Automatic ActiveX execution can be disabled within Internet Explorer. Most sites will have little functionality lost without ActiveX. At the very least, “Prompt” should be selected, allowing the user to consider the source of the control before allowing it to execute.



The prompt to allow ActiveX controls.

Microsoft’s JVM can be removed entirely if not required from machines that still have it. Instructions for removing it (and replacing it with the Sun Microsystems’ version of the VM for Windows) can be found by following the link below.

The JVM can be patched to a level that is not affected by these vulnerabilities (but is also no longer supported) by installing the build 3810 (link below).

### Mitigation

Mitigating spyware once it is installed may be a laborious process that most (if not all organizations) do not have time to manage. To be completely successful, it would be necessary to block destinations for every unique spyware distributor, a difficult process indeed. However, it is possible to block a large number of the “well known” versions, which may at least limit what information is sent out of the organization a little.

All browsers allow for the possibility of spyware to be installed, as recent vulnerabilities in Firefox and Opera have shown. However, IE is still the favorite target of spyware creators. If IE is the browser of choice, it is also possible to disable the known “bad” ActiveX controls. Microsoft points out how to kill pieces of the ActiveX processing in KB 240797. An automatic tweak to the Registry can be found at <http://www.spywareguide.com/blockfile.php>. This tool (“blockfile”) sets the values of many ActiveX controls to prevent them from executing.

Dead listing spyware domains via DNS is another laborious but effective method of limiting how much data is collected and returned to the spyware servers. Unfortunately, spyware appears to be a technology that requires specialized tools, in the way of content

filters, traffic inspectors, and scanners/removers, to control. At the very least, this means constantly updating (via subscription service) the addresses/domains being blocked.

### **Resources**

An excellent review of the CWS variants written by the author of the best tool for removing them:

<http://www.spywareinfo.com/~merijn/cwschronicles.html>

Microsoft Advisory MS00-075

<http://www.microsoft.com/technet/security/bulletin/MS00-075.msp>

Microsoft Advisory MS03-011

<http://www.microsoft.com/technet/security/bulletin/MS03-011.msp>

Removing the Microsoft JVM

<http://www.winnetmag.com/Article/ArticleID/38206/38206.html>

KB 240797 – How to Stop and ActiveX Control from Running in Internet Explorer

<http://support.microsoft.com:80/support/kb/articles/q240/7/97.asp&NoWebContent=1>

Copyright © 2004 infectionvectors.com. All rights reserved.