



Sunbelt Software

Network Agent

(Software Review)

**Sunbelt Software
Research Center**

April 23, 2006

Introduction/Overview

Network Agent (network.com) is a browser toolbar and add-on that enables users to perform searches on "keywords" ("networks") either through the toolbar itself or the browser URL address bar. Although users can define their own "networks" or "keywords" (which are then used as an alternative form of bookmarks), the search results returned for most "networks" are, in fact, paid-for advertising of one sort or another.

Distribution & Installation

Network is distributed only via Network's own web site (network.com). Sunbelt has received no reports of Network being installed at third-party web sites or with third-party applications. Users must initiate the installation, making it unlikely that Network would be installed without the knowledge and consent of the user. As discussed later, however, the potentially objectionable advertising functionality of the program is not fully disclosed to users during installation.

Advertising

While Network Agent itself does not display advertising on the user's desktop while the browser is closed (unlike so many other adware programs), the true function of the product is to put more advertising in front of users while they are browsing the web.

Browser pop-ups

Network Agent opens new ad-related browser windows when users perform searches through popular search engines like Google, Yahoo!, or MSN and the search terms match "networks" bought by customers of Network. These new browser windows -- which are effectively pop-ups -- open next to the user's original browser window on a landing page of the advertiser's choice.

While these pop-ups are limited in context to the use of popular search engines, they are nonetheless pop-ups spawned by the locally installed Network software, not the web pages actually visited by users.



Figure 1: Network "Demo"

Keyword search results

Network bills the product as an internet "keyword" application that allows users to perform searches on "keywords" either through the Network toolbar itself or the browser's URL address bar. What Network does not tell users beforehand, though, is that the "search results" returned are, more often than not, paid-for advertising of one sort or another.

Network returns two types of advertising-related "search results":

- 1) Overture PPC search results that are pulled through AltaVista - these search results are dominated by "Sponsored Matches," which are not as clearly distinguished from the organic search results as they could be.

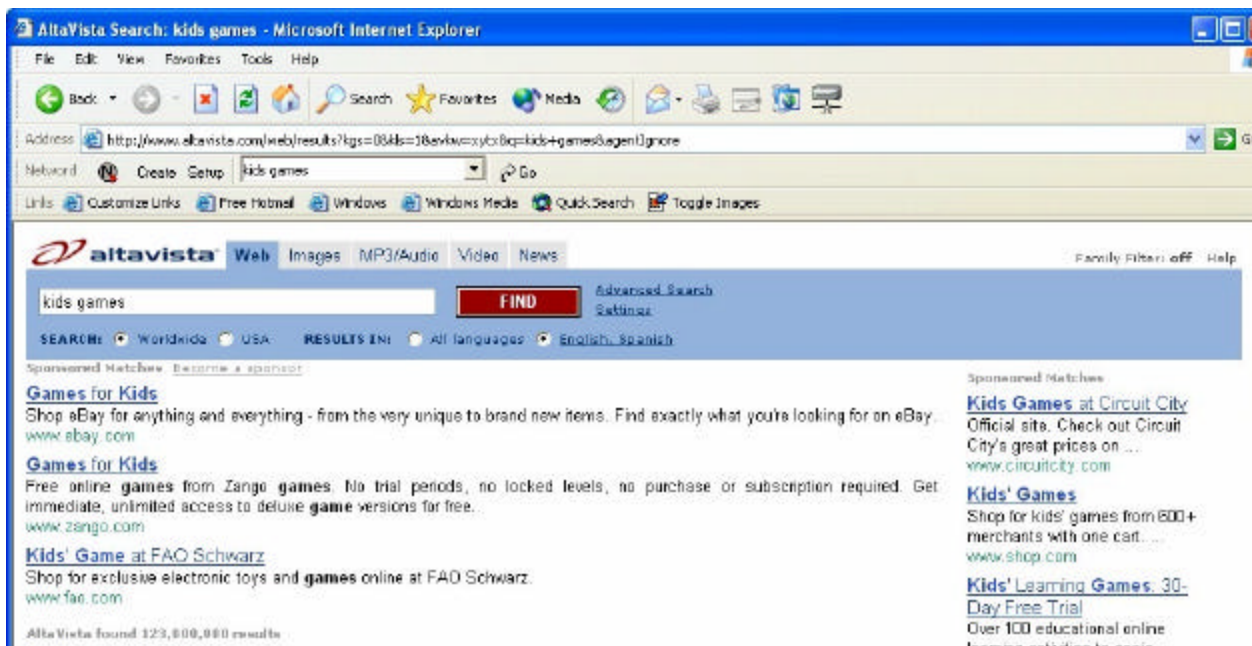


Figure 2: Overture/AltaVista PPC search results

- 2) Browser re-directs to advertising-related landing pages, many of which spawn pop-up advertising.

It is the second form of advertising that is of most concern, as these browser re-directs occur without warning and land users on pages that can spawn aggressive pop-up advertising. In our testing, for example, we performed a search on the term "spyware." The browser was re-directed without warning to a landing page at spyware.com, which spawned advertisements for various products of dubious quality, including WinFixer and WinAntivirus, both of which are well known rogue security products with track records of aggressive deceptive advertising. (1) Indeed some of the pop-up advertising took the form of deceptive "warnings" that our test PC might be afflicted with "spyware" or "critical" errors (see Figure 3 below).

Another search on the term "registry" saw the browser re-directed to registry.com, which spawned a blizzard of pop-ups that blanketed the desktop. Still another search on the term

"smileys" caused the browser to re-redirect to a web page for Smiley Central.

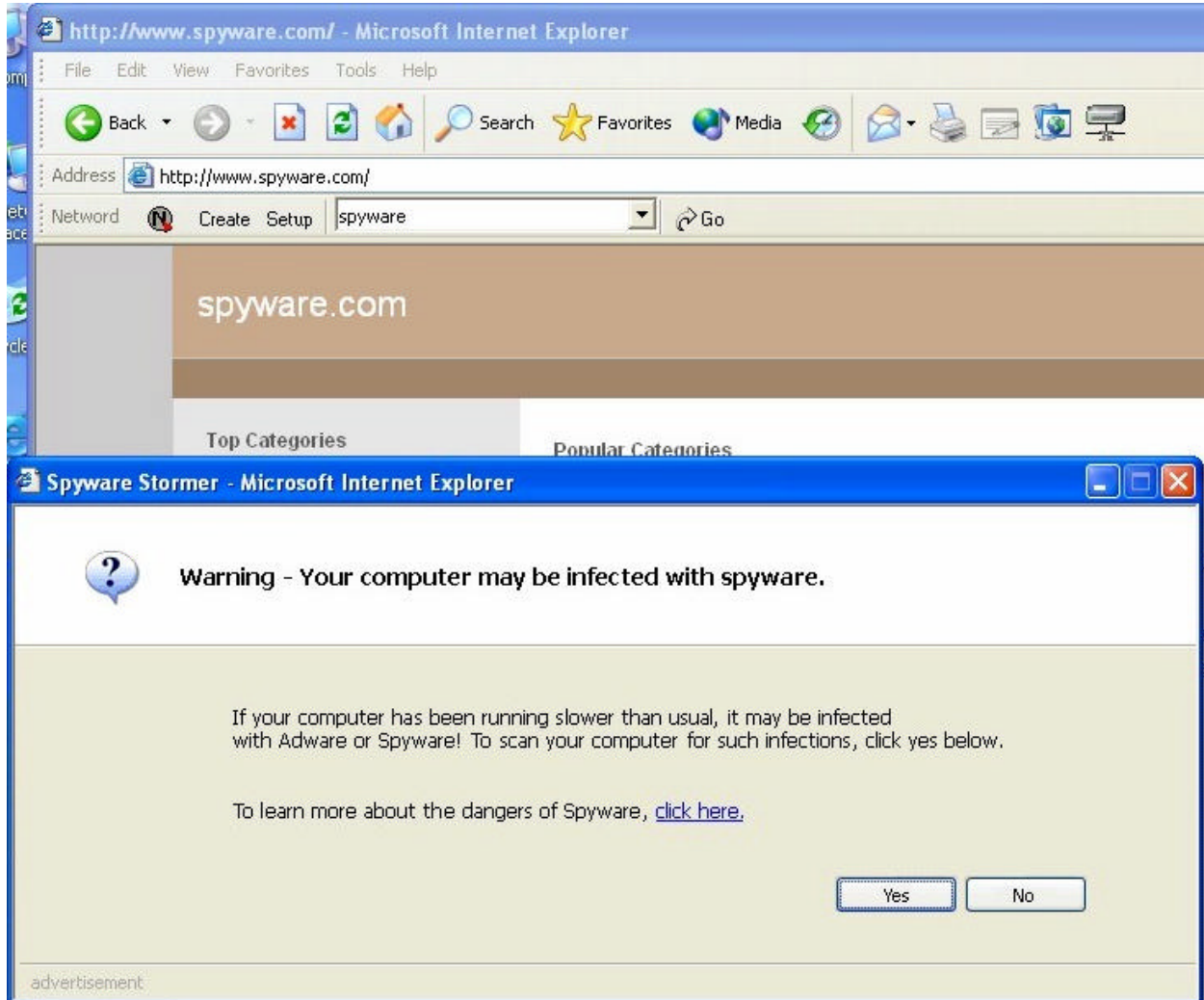


Figure 3: deceptive pop-up advertising spawned by Network re-redirect

Given that most popular browsers already allow for "keyword" searching from the URL address bar, and given that the toolbar has little other functionality beyond "keyword" searching and matching of one sort or another, the primary purpose and function of the Network Agent would seem to be the replacement of the browser's own native "keyword" searching with Network's own heavily ad-driven "network" search functionality. And although users can define their own "networks," they cannot define "networks" that have already been purchased by advertisers. (2)

System Reconfiguration

Network Agent adds a BHO and toolbar to Internet Explorer. These browser add-ons effectively replace or take over the browser's own "keyword" searching functionality. They also allow users to define "networks" of their own, which function as an alternative form of bookmarks. No other significant system modifications by Network were observed in testing.

Data Collection, Transmission, & Sharing

Network does collect some data about users and their use of the product. During setup, users are requested to provide their ZIP code. Users who want to define their "networks" are required to register with Network. This registration process requires users to supply an email address. The Network privacy policy states (3):

The Company does not collect any personal information on or about specific Navigating Web Users, nor does it monitor the navigating behavior of such users.

As part of the Networks redirection process certain data is collected at the Company computer server level. Such data may include Networks used, IP addresses, and timing and browser information. This information is used on an aggregated level, both for internal data performance purposes and as part of the business planning process.

Given that none of the data collected appears to be tied to a unique ID number or personally identifiable information (PII) of any kind, the privacy implications of Network Agent are negligible.

Uninstallation

Network can be uninstalled through the Add/Remove Programs Control Panel applet. The Network uninstaller performs a reasonably clean and complete uninstallation of the product.

Malware

Network Agent is not malware itself, does not install malware, and is not known to be installed by malware.

Notice, Disclosure, Choice, & Consent

As noted earlier, the installation process for Network ensures that users must know and be aware of the installation of the product. The problem, however, is that the advertising-related nature of the product is not properly disclosed to users before or during installation, and users could very well think that they are getting a substantial upgrade to their browser's own native "keyword" searching capability when in fact that capability is effectively being downgraded to a more advertising-oriented "keyword" searching replacement.

Although the download page for Network does mention "Network Advertising in all Major Search Engines," the fact that this advertising will take the form of pop-up advertising is not clearly disclosed. And although the Network home page does offer a short video tour ("demo")

of the product, the video downplays the advertising functionality of the product. Moreover, the information in this "demo" is never affirmatively presented to users during installation.

Finally, the browser re-directs performed by Network will likely be entirely unexpected by users, and the pop-up advertising spawned by some of the Network-chosen landing pages could prove a very unwelcome surprise.

Sunbelt's Listing Criteria

Network Agent does trip at least four of Sunbelt's published Listing Criteria (4):

Distribution & Installation

- installs on users' PCs after providing only substandard, inadequate notice and disclosure, and thus failing to secure users' full, meaningful, and informed consent

Advertising

- displays third-party advertising in pop-ups and windows that the software opens on the users' desktops and which are not part of internet content that users directly choose to visit or view without first providing sufficient notice and choice to users and securing their full, meaningful, and informed consent, or without offering users a means for permanently removing or opting out of the advertising short of purchasing a "pro" version of the product and/or incurring a fee
- displays, opens, or embeds advertising using other methods or means that most reasonable persons would find objectionable, unfair, misleading, deceptive, or coercive

Notice, Disclosure, Choice, & Consent

- fails to clearly, conspicuously, and meaningfully disclose key terms related to advertising, system reconfiguration, and data collection / transmission practices

Recommendations

Network Agent is currently classified by Sunbelt Software as an "Adware" program, with a Threat Level of "Elevated" and a default action of "Quarantine." Given that the software is not installed without users' knowledge and does not engage in any severely objectionable practices, this classification is unwarranted.

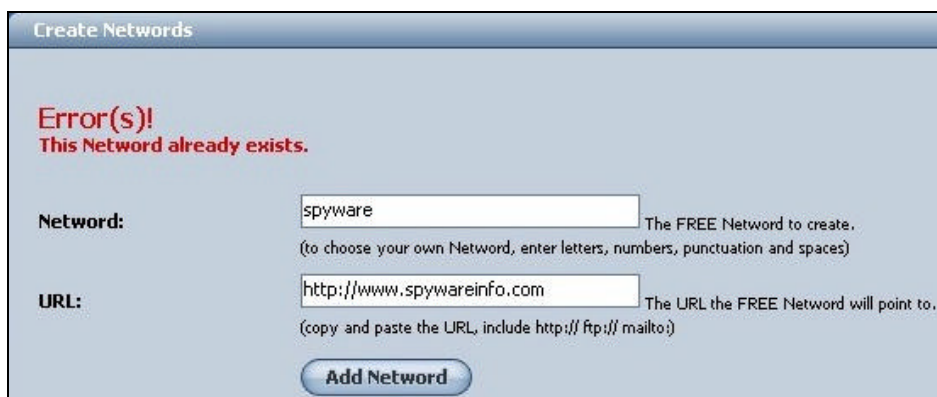
Nonetheless, Sunbelt is concerned with the advertising-related functionality of the product's keyword searching and limited pop-up functionality as well as the fact that this advertising behavior is not clearly disclosed to users' prior to or during installation. As it is entirely possible that users could install the product without knowing that keyword searches could cause browser re-directs to pop-up infested landing pages or that searches at popular search engines could spawn pop-ups, Sunbelt is entirely justified in offering this program as a detection to its users.

The Sunbelt Research Team therefore recommends that Sunbelt re-classify Network Agent as a "Low Risk Adware" program, with a Threat Level of "Low" and a default action of "Ignore."

With this classification, Sunbelt CounterSpy will continue to detect Network Agent, however, users will be forced to affirmatively elect to remove the program by changing the action in the scan results screen from "Ignore" to "Quarantine" or "Remove." Users who wish to keep Network Agent will be able to do so without fear that CounterSpy will automatically remove the program.

Notes:

1. See: "Rogue/Suspect Anti-Spyware Products & Web Sites." *SpywareWarrior.com* <http://www.spywarewarrior.com/rogue_anti-spyware.htm>.
2. We attempted to define our own "netword" for the term "spyware," however, we were informed that the term was already taken.



The screenshot shows a web form titled "Create Networks". At the top, there is a red error message: "Error(s)! This Network already exists." Below the error, there are two input fields. The first is labeled "Network:" and contains the text "spyware". To its right, there is a small text label: "The FREE Network to create. (to choose your own Network, enter letters, numbers, punctuation and spaces)". The second input field is labeled "URL:" and contains the text "http://www.spywareinfo.com". To its right, there is a small text label: "The URL the FREE Network will point to. (copy and paste the URL, include http:// ftp:// mailto:)". At the bottom of the form, there is a blue button labeled "Add Network".

Figure 4: Failed attempt to define "spyware" as "netword"

3. Network Privacy Policy. <<http://netword.com/consumer/privacy-policy.html>>.
4. Sunbelt Software Listing Criteria. <http://research.sunbelt-software.com/Listing_Criteria.cfm>.

About Sunbelt Software

Headquartered in Tampa Bay (Clearwater), Fla., Sunbelt Software was founded in 1994 and offers products to protect and secure systems from costly inefficiencies including spam and spyware; as well as enterprise solutions to protect against system downtime and security vulnerabilities.

Sunbelt Software is part of the Sunbelt International Group, which includes Sunbelt Software, Inc. and Sunbelt System Software in Europe. The Sunbelt System Software group has offices in the UK, France, Netherlands, Sweden and Germany.

Primary Media Contacts

Laurie Murrell
lauriem@sunbelt-software.com
888-NT UTILS (688-8457)
Marketing Communications Manager
Sunbelt Software

Heather Kelly
heather@sspr.com
719-634-8274
S&S Public Relations for Sunbelt Software

Jason Ovitt
jovitt@sspr.com
847-415-9326
S&S Public Relations for Sunbelt Software