

EXHIBIT 107

Alan

From: Deven Parekh [DParekh@insightpartners.com]

Sent: Thursday, March 31, 2005 9:59 AM

To: Abram; Kaufman; Murray

Subject: At least we are not Ebola....interesting to also see the number of machines Claria is on....

<http://informationweek.securitypipeline.com/news/159908602.jsessionid=XFEKOWGF3VT2AQSNDBGCKH0CJUN>

This message may contain confidential and/or legally privileged information. If it has been sent to you in error, please reply immediately to advise the sender of the error and then destroy this message, any copies of this message and any printout of this message. If you are not the intended recipient of the message, any unauthorized dissemination, distribution or copying of the material in this message, and any attachments to the message, is strictly forbidden.

10/25/2005

DR302335
CONFIDENTIAL



CMP
United Business Media

Presented by **InformationWeek**
securitypipeline
FEATURING SECURE ENTERPRISE MAGAZINE

SEARCH

search [advanced search](#)

[Free Newsletter](#)

[Glossary](#)

[Contact Us](#)

[NEWS](#) | [TRENDS](#) | [HANDS ON](#) | [BLOG](#) | [PRODUCT FINDER](#) | [DESKTOP](#) | [NETWORK](#) | [INFRASTRUCTURE](#) | [PO](#)

news

March 30, 2005

CoolWebSearch, Dubbed Adware's "Ebola," Tops Spyware Threat List

By Gregg Keizer

Courtesy of [TechWeb News](#)

CoolWebSearch, adware that generates more than \$300 million a year for its maker, is the "Ebola" of adware, and easily the most significant spyware threat on the Internet, an anti-spyware security firm said Wednesday.

CoolWebSearch, which comes in multiple forms, can hijack Web search errors, usurp the browser's home page, and modify other Internet Explorer settings. Recent variants have taken to exploiting vulnerabilities in IE, such as those in the HTML Help system, to install on PCs.

"It's only purpose is to get on a PC, and stay on that PC, even at the cost of killing that machine," said Richard Stiennon, the vice president of threat research for Boulder, Colo.-based Webroot, which publishes the Spy Sweeper line of anti-spyware software.

According to Webroot, nearly half of the PCs it's audited for spyware or adware are infected with CoolWebSearch.

"It's the Ebola of the Internet," said Stiennon. "It's so malicious that it tends to break the ability of a machine to browse effectively, and therefore limits the number of ads and click-throughs that can be generated. Like Ebola, it kills its host before it can be productive."

Webroot's newest Top 10 list – it releases a list of the ten most significant spyware/adware threats every quarter – is based on the free [spyware](#) audits it conducts from its own Web site, and those it runs in cooperation with EarthLink, the Atlanta-based ISP.

"We rank programs on both prevalence and perniciousness," said Stiennon.

Second on Webroot's list is Gator/GAIN, adware that may display banners ads based on Web surfing habits. Gator is a long-time adware package that often gets on systems because it's bundled with free software, most notably the P2P file-sharing program Kazaa. By the SpyAudit scanning results, Gator/GAIN is on about 15 percent of all machines.

"If we take the leap and assume that the sample is representative of the

RELATED LINKS

- ☐ [Your IM Buddy, Or A Hacker? It's Get Tell](#)
- ☐ [FTC Nails Two Spyware Sellers For T](#)
- ☐ [Sober's Attack May Be Nothing To Sv](#)
- ☐ [Bank Of America Pushes Anti-Phishi Northeast](#)
- ☐ [Phishers Stay One Step Ahead](#)
- ☐ [Microsoft Promises To Patch Worsen Flaw](#)

[RSS](#) [Security Pipeline's Main RSS Feed](#)

[RSS](#) [Security Pipeline's Blog RSS Feed](#)



FEATURED MICROSITE:

Your IT peers

What's The Key To Small Biz Advantage?

Find out the keys to small and midsize suc and using the right mobile and desktop sol

Internet in total, we can estimate how many machines have Gator," said Stiennon. His best guess: 38.4 million PCs. Others on Webroot's list include (in descending order), 180search Assistant, ISTbar/Aupdate, Transponder, Internet Optimizer, BlazeFind, Hot as Hell, Advance Keylogger, and TIBS Dialer. Most are adware in composition – not that that means they're benign; they typically hijack search errors and re-direct them to another site, and/or blitz the PC with endless popups – but some are true spyware.

"We're finding keyloggers on about 15 percent of the machines audited," said Stiennon, "and Advanced Keylogger is the most prevalent right now. It's on relatively few machines – about 9,000 that we've found – but a keylogger on that many PCs is a scary concept in and of itself.

"Spyware writers are continuing to innovate and find new, more deviant ways to infiltrate systems," said Stiennon. "The increased presence of hijackers, dialers, and keyloggers demonstrates that the new trend for these threats is to go straight for the jugular."

Spyware/adware writers are doing that for one reason: money.

Stiennon, who has analyzed the spyware/adware economy, has come up an average cash flow per "customer installation" per year of \$2.40. For each system infected, then, he estimates that the adware author generates \$2.40 annually in pop-up fees, redirect fees, and other charges.

His cash-flow projection for the creator of CoolWebSearch – which using his formula may be on more than 127 million machines worldwide – is thus \$306 million. The company behind Gator/GAIN – the Redwood City, Calif.-based Claria – is bringing in around \$92 million a year, while 180search Assistant is raking in \$86 million.

"These guys make spammers look like two-bit back alley operations," said Stiennon. "No wonder there's a gold rush to get in on this."

And no wonder some adware firms are pushing anti-spyware vendors to "de-list" them from their detection and deletion scanners.

The most recent such move was by Computer Associates, which sells the PestPatrol anti-spyware line after acquiring the company in 2004. Last week, CA removed all Claria products – including Gator/GAIN – from its database under its [Vendor Appeal](#) program.

CA has been criticized in the past for de-listing software other anti-spyware vendors continue to list as malicious, and even [Microsoft](#) has backed down in at least one instance.

"One reason [Webroot](#) publishes the Top 10 list," said Stiennon, "is to help provide an idea of the scope of the whole spyware and adware issue, so that going forward, as the discussion of adware heats up and definition battles with the vendors begin, people will have some basic information about the extent of the problem."

[E-mail This Story](#)
[Print This Story](#)

FREE SECURITY
NEWSLETTER

Get the latest news, product info,
and trends every week.

apps.

Unleash the Power & Opportunity Computing

Experts will identify trends in grid computing examples and examine solution options.

Using Current Performance to Shape Future Results

Hear new strategies for improving business performance and results.

TECHWEBCASTS

Editorial and vendor perspectives
2005 enterprise server software: What's
new, what's different.
Put storage in order: New strategies
simplify regulatory compliance.

VENDOR RESOURCES

Avoid email danger & downtime with a
holistic email strategy.
Strategies for sustainable risk and
compliance management

FOCAL POINTS

(Sponsored links)

Boost performance for critical business
apps with dual-core.
Blade servers: Bigger isn't always better.

EDITOR'S PICKS

Why Linux Is More Secure Than Ever

A tech expert discusses open source security and how enterprises can ensure that their Linux is secured.

Opinion: Why Third-Party Patching Isn't Solution For Zero Day Exploit

Ride Along: Anatomy of a Break-In

Review: Spyware Detectors

Microsoft Plans To Patch Zero-Day Win

VOTING BOOTH

There is a third-party patch for the current Windows vulnerability but columnist [Rob I](#) doesn't recommend it. What's your take on third-party patches?

I think the third-party patch is a valuable remedy.

I'm not thrilled about third-party patches it's a good interim solution.

I agree with Enderle that third-party patches are more trouble than they're worth.

Vote

productfinder

In search of security products? Check out our [Product Finder](#) for a directory of anti-malware access control solutions, monitoring tools, and

SOA
Lets You

Subscribe!

SECURITY PIPELINE MARKETPLACE (sponsored links)

Authentication TCO White Paper

Discover how to secure multiple devices across your enterprise, plus reduce TCO and complexity by implementing a two-factor unified authentication solution. Leverage your existing infrastructure. Learn more.

Free Identity Management White Paper.

Learn how BMC's Identity Management Services can help secure your enterprise and give authorized users access they need to critical information, so they can deliver more consistent services. Register now for 'The Black Book on Corporate Security'

Policy Management vs Vulnerability Scanning

Which is right for you? Vulnerability scanning products test for known vulnerabilities. Policy management products are pro-active by locking the doors in advance of a possible attack. Click to request our white paper

Cost-Effectively Secure Sensitive Data

Encrypting data in servers and databases can address security gaps and privacy legislation. Ingrian DataSec Platforms offer granular encryption, seamless integration, and centralized security management. Combat data theft—with unprecedented ease and cost effectiveness. Download a white paper that outlines best practices for securing data.

How well are you defending your email network?

Defend with the best! The MX Logic Email Defense Service was awarded five stars from Veritest and provide 24 x 7 multi-layered protection against spam, viruses, worms, inappropriate content and SMTP attacks at the network perimeter.

Buy a Link Now

Top ten search terms from the TechWeb TechEncyclopedia.

How does your pay rate? Check the InformationWeek Salary Survey.

Mobilized Solutions Guide: Find and compare solutions for your business.

Top Requested White Paper Categories from TechWeb White paper Library.

Top ten search terms from the TechWeb TechEncyclopedia.

Sponsored Links: [White Papers](#), [Sponsor Resources](#), [WebCasts](#).

[News](#) | [Trends](#) | [Product Finder](#) | [Hands On](#) | [Blog](#) | [Desktop](#) | [Network](#) | [Infrastructure](#) | [Policy & P](#)
[Original Articles](#) | [Free Newsletters](#) | [Security Glossary](#) | [Contact Us](#) | [About Us](#) | [Privacy](#)

[The TechWeb Pipelines](#) | [TechWeb.com](#) | [InformationWeek](#) | [Optimize](#) | [Network Computing](#) | [IT Architect](#) | [Intelligen](#)
[Bank Systems & Technology](#) | [Wall Street & Technology](#) | [Insurance & Technology](#) | [IT Pro Downloads](#) | [Comm](#)
[Business Intelligence Pipeline](#) | [Compliance Pipeline](#) | [Desktop Pipeline](#) | [Developer Pipeline](#) | [InternetWeek](#) | [Linux](#)
[Messaging Pipeline](#) | [Mobile Pipeline](#) | [Networking Pipeline](#) | [Personal Tech Pipeline](#) | [Security Pipeline](#) | [Server F](#)
[Small Business Pipeline](#) | [SOA Pipeline](#) | [Systems Management Pipeline](#) | [Byte and Switch](#) | [Light Reading](#) | [Uns](#)

Copyright © 2005 CMP Media LLC. | SECURITY PIPELINE All rights reserved. [Privacy Policy](#) | [Your California Privacy Rights](#) | [Terms of Servi](#)