EXHIBIT 107
Alan

From: Devion Parekh [DParekh@insightpartners.com]
Sent: Thursday, March 31, 2005 9:56 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/156608602/sessionid=XE-KC5T63YTPRQA%SGBGC3KBG-76

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

By Gregg Keizer

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 lookup the browser's home page, and mimic other Internet Explorer settings. Recent variants have been targeted 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 stability 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 current Top 10 list - it releases a list of the ten most significant spyware/adware threats every day - 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 track programs on both prevalence and perniciousness," said Stiennon.

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

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


11/10/2006
"We’re finding keyloggers on about 15 percent of the machines audited," said Silverman. "And advanced keylogging is the most pervasive right now. It’s on relatively few machines — about 800 that we’ve found — but a keylogger on that many PCs is a scary concept in and of itself.

"Spyware writers are trying to innovate and find new, more devious ways to infiltrate systems," said Silverman. "The increased prevalence of hijackers, drivers, and keyloggers demonstrates that the new trend for these threats is to go stealth for thepopup costs, redirect fees, and other charges.

"There are a number of factors that are making the threat more difficult to detect," said Silverman. "First, the companies are using more sophisticated methods to hide their activity from users. And with the increasing popularity of adware and spyware programs, it’s becoming more difficult to detect these threats.

"One reason is the way in which these programs are designed," said Silverman. "They are designed to be difficult to detect and remove, and they often use complex, multi-layered communication channels to hide their activities from users. In addition, these programs can be difficult to remove because they often rely on operating system components that are not visible to users.

"Another factor is the way in which these programs are distributed," said Silverman. "Many of these programs are distributed through legitimate sources, such as software distribution services and websites. This makes it difficult for users to detect and remove these programs.

"The final factor is the way in which these programs can be easily installed," said Silverman. "Many programs are designed to be installed without user intervention, and they can be installed in the background without the user’s knowledge. This makes it difficult for users to detect and remove these programs.

"In conclusion, the threat of spyware and adware is a serious problem that requires a comprehensive approach to detection, removal, and prevention. Users should be aware of the risks associated with these programs and take steps to protect their systems. By being aware of the risks and taking these steps, users can reduce their risk of being infected by these programs.

"Security Pipeline, a weekly newsletter from CoolWebSearch, provides timely and accurate information on the latest developments in the spyware and adware field. The newsletter is designed to keep users informed about the latest threats and provides tips and techniques for protecting against these threats. Subscriptions are available for $20 per year.
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 proactive by locking the doors in advance of a possible attack. Click to request our white paper.

Cost-Effectively, Securely Sensitive Data
Encrypting data in servers and databases can address security gaps and privacy legislation. Ingrain 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 Veritas and provides 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.


Top Requested White Paper Categories from TechWeb Whitepaper Library.

Top ten search terms from the TechWeb TechEncyclopedia

Sponsored Links: White Papers | Sponsor Resources | Webcasts


The TechWeb Pipelines | TechWeb.com | InformationWeek | Optimize | Network Computing | IT Architect | Intelligent Bank Systems & Technology | Web Street & Technology | Insurance & Technology | IT Pro Downloads | Commit Business Intelligence Pipeline | Compliance Pipeline | Desktop Pipeline | Developer Pipeline | InternetWeek | Linux Messaging Pipeline | Mobile Pipeline | Networking Pipeline | Personal Tech Pipeline | Security Pipeline | Server E Small Business Pipeline | SOH Pipeline | Systems Management Pipeline | Style and Sketch | Light Reading | Usr

Copyright © 2006 CMP Media LLC. SECURITY PIPELINE All rights reserved. Ebola Policy | Your California Privacy Rights | Terms of Use


1/10/2006