

Beware of Link: E-Mail Virus Plays Havoc With Internet

By Jeremy A. Kaplan & Jana Winter
Published September 10, 2010

Here you have ... one heck of a mess.

An insidious e-mail virus remained in the top five Google searches Friday, a day after it snarled traffic and took down servers at ABC, NASA, Comcast, and Google -- and possibly even swamped the Department of Homeland Security's computers.

The Internet Storm Center, a free analysis and warning service that tracks malicious Internet activity, reported that the initial application that generated the vast cloud of spam clogging servers had been taken down, which should limit the spread of the virus Friday. And there were no new reports of infected servers Friday morning -- but the Web may not be out of the woods just yet.

"New variants may well follow," the Storm Center warned.

The virus, called "here you have" (or VBMania, though different security companies have different names for the same virus), is a simple Trojan Horse: An e-mail arrives in your inbox with the odd-but-suggestive subject line "here you have." The body reads "This is The Document I told you about, you can find it Here" or "This is The Free Download Sex Movies, you can find it Here."

Click the link in the message and you download and launch a program that spams the same Trojan Horse out to everyone in your address book, flooding and crippling e-mail servers.

Leading virus monitors such as **McAfee Labs** and **Symantec** are currently investigating the threat, and have already updated their website to push security products that could protect users.

"Stop or remove the virus with Norton Internet Security 2011," advises Symantec on the front page of its site Friday morning. The security companies describe "here you have" as especially challenging to monitor, since the virus may already have replicated into several new forms.

"It looks like multiple variants may be spreading and it may take some time to work through them all to paint a clearer picture," warned Craig Schmugar on McAfee's Threat Response page.

Difficult indeed.

In addition to a variety of major corporations, the virus appeared to take down internal servers at the Department of Homeland Security (DHS) on Thursday. Numerous sources told FoxNews.com that some DHS agencies that run on the Immigration and Customs Enforcement server crashed and were mostly disabled throughout Thursday.

But U.S. officials denied that issues with its servers were related to the virus, telling FoxNews.com that "neither DHS nor ICE were agencies that were affected."

"It's a phishing attack -- when you click on the link in an e-mail it goes into the address book. It was clogging a bunch of e-mail and that's it," officials told FoxNews.com. "It's too early to say how sophisticated it was, but a number of companies and agencies were affected."

DHS spokeswoman Amy Kudwa said that Homeland Security's experts were investigating the situation. She explained the U.S. Computer Emergency Readiness Team -- US-CERT, the agency tasked with preventing cyber attacks against the government -- was actively sharing its expertise with departments and agencies that had been affected, as well as private companies.

"US-CERT has received multiple reports from a number of federal agencies and private sector entities experiencing an email worm. A full assessment is being conducted -- US-CERT is in the process of collecting and analyzing samples of the malware and has developed and disseminated mitigation strategies."

"Basic cyber security practices and hygiene are essential to maintaining the security of networks and individual computers," Kudwa advised. She suggested that concerned Internet surfers should not trust unsolicited e-mail, treat all attachments with caution and (of course) never click links in unsolicited e-mails.

Hopefully , that advice makes its way back to NASA, where employees were hampered throughout the day -- and took to Twitter to complain about the problem.

Source: **FoxNews.com**