


November 9, 2007

**PAGE ONE**

**DOW JONES REPRINTS**

 This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: [www.djreprints.com](http://www.djreprints.com).

- [See a sample reprint in PDF format.](#)
- [Order a reprint of this article now.](#)

# Web Scammer Targets Senior U.S. Executives

## Email Hoax Believed To Dupe Thousands; Mr. Stewart's Pursuit

By **CHRISTOPHER RHOADS**  
*November 9, 2007; Page A1*

MYRTLE BEACH, S.C. -- For months, a sophisticated hacker has been stealing the personal data of American corporate executives.

Hot on the hacker's trail is Joe Stewart. The former bass-guitarist-turned-cyber-sleuth stumbled onto the case in February. Since then, the 36-year-old Mr. Stewart has spent weeks in his office, in a nondescript building next to a half-abandoned strip mall here, virtually chasing the mysterious perpetrator across several continents. Mr. Stewart early on thought he had traced the scammer to China, then realized it was a false lead. Only when the perpetrator stumbled did Mr. Stewart get a break in the case.

Mr. Stewart, a top researcher for Atlanta-based Internet security firm SecureWorks Inc., says most of the scammed executives declined requests to discuss their experience. He says they include senior executives at Fortune 500 companies, working in industries from airlines and banks to manufacturing and pharmaceuticals. The number of those affected is likely in the thousands. In May, Mr. Stewart, who works closely with law enforcement, says he found one cache of data stolen by the scam from more than 1,400 executives.

News of the con, which specifically targeted intended victims with personalized emails, quickly swept through the nation's Internet security ranks. This scammer "knew your name, your title and your organization," says Jose Nazario, a researcher in the Ann Arbor, Mich., office of Arbor Networks Inc., an Internet security company.

## **1 CAST YOUR VOTE**

How secure do you feel your personal information is online? [Vote in the Question of the Day](#)<sup>2</sup>.

## **CAT AND MOUSE**

- [See the email that loaded malicious software onto executives' computers.](#)<sup>3</sup>
- [See the research Mr. Stewart posted as he studied the virus.](#)<sup>4</sup>



In the early days of the Internet, hackers broke into large computer systems just to prove they could. Later, mischief-makers created and blasted "virus" software world-wide, rapidly infecting millions of terminals within hours and slowing legitimate Internet traffic.

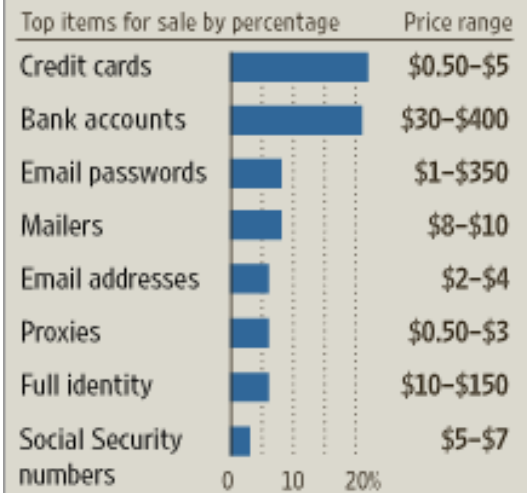
Over the years, Americans also became acquainted with the email scam, such as a sender posing as a bank and asking for account information. Such scams often were loaded with grammatical and spelling errors and lacked details tailored to the recipient. They were sent far and wide in hopes of hooking a few naïve victims.

But in the past two years, law-enforcement officials and Internet security experts say the global growth of broadband has fed a dramatic jump not only in the quantity but also the quality of cyber-attacks.

MessageLabs, a New York-based Internet security firm, says the number of hoax emails addressing recipients by their names and including their professional affiliation, among other personal details, has soared in recent months. In mid-September, the company discovered more than 1,100 such emails over a 16-hour period, and in late June more than 500 over two hours. Last year, it rarely saw more than one of these emails a day.

## Sneaky Business

Categories of stolen data sold online, as percentage of total.



One factor behind the change is the explosion in popularity of social networking Web sites like Facebook and LinkedIn, which give scammers access to information like a person's professional title and company affiliation. Mr. Stewart figures at least some of the targeted executives were found by the scammer searching for those with "C"s in their titles, like CEOs and CFOs. Corporate Web sites and news releases also provide helpful data for criminals.

What's more, since many executives answer email directly, they are directly accessible in ways their predecessors weren't.

Then there's the wide availability of illicit skills online. Criminals on the Web used to have to design and program their own viruses and scams. Now, such expertise can be purchased online for several hundred dollars.

Armed with such tools, scammers can target specific groups of people, such as wealthy executives. The emails are sophisticated enough to dupe even discriminating Web users.

One morning in May, such an email landed in the inbox of Scott Foernsler, head of global sales at Air2Web Inc., an Atlanta mobile messaging and marketing company. It informed him that a Better Business Bureau complaint had been filed against him and asked him to click an attached link to respond.

The email featured the Better Business Bureau's familiar torch logo running across its top on a blue background. It addressed Mr. Foernsler by name and also provided the name of his firm as well as a case number. The sender's email address: consumer-complaints@bbb.org.

The email looked so professional that Mr. Foernsler, an executive with 22 years of sales experience, never suspected a thing. "Anything about our customers I want to take action on," he says. He clicked on the link

and was informed he would be contacted again. Mr. Foernsler then received another email informing him that the complaint had been resolved. He gave the matter no further thought until early June, when SecureWorks notified him that his computer was infected.

By clicking on the bogus complaint link, he had downloaded software that was sending anything he then inputted online -- such as passwords, credit-card numbers, usernames, banking information and personal browsing -- to a Web site controlled by a criminal.

Mr. Foernsler has since changed all his passwords and usernames and had the software removed. But like the other executives scammed, he has no idea what information was stolen -- or what criminals may be doing with it.

One of a handful of Web sleuths to proactively go after bad guys, Mr. Stewart is chasing this con artist largely on his own. With Internet service providers more focused on signing up subscribers and law enforcement only recently bulking up on resources, policing the Web relies heavily on a loosely coordinated community of obscure university researchers, volunteers and security experts of varying backgrounds and expertise.

"It's like the Old West when there was very little law enforcement for a large territory," says Mr. Stewart.

A dogged gumshoe, Mr. Stewart almost never got into computers. He taught himself programming languages on his sixth-grade teacher's computer after school, but abandoned the hobby several years later, assuming there were few interesting careers in the field. It was the late-1980s, before the existence of the commercial Internet. Mr. Stewart turned his attention to radio broadcasting in college, but dropped out when he ran out of money for tuition.

With a wife and two young boys to support, Mr. Stewart stocked shelves at a Lowe's Home Improvement store during the day and at night alternated between stacking shoes in a shoe store and mopping floors at a Pizza Hut restaurant.

In 1996, Mr. Stewart's mother gave him her old computer. He scrounged up enough money to get online and began programming again, occasionally fixing computers for friends. That led to a job as an analyst with an Internet security firm in town, which was eventually acquired by his current company SecureWorks.

Mr. Stewart quickly gained notice for his willingness to post his findings online, in order to make others aware of new threats and to share his various techniques. Many experts demur out of fear of retribution. After Russian hackers described by Mr. Stewart attacked his personal Web site, SecureWorks decided to remove the company sign from the Myrtle Beach office. The gray, one-story building is surrounded by a barbed-wire fence, with a security camera at the gate.

Mr. Stewart first became aware of the Better Business Bureau scam last February, when a colleague forwarded him the email. Mr. Stewart was impressed with the email's professional appearance and its tactic of striking at the recipient's desire to keep customers happy.

## **Server in China**

He gave chase. Mr. Stewart found the attack was hosted on a new domain name registered on a server located in China, under the name Li Hu. The registrar that sold the domain name did business only in Chinese. At one point the attack was collecting 70 megabytes of data every day.

The attacks escalated. By the beginning of June, the virus was unleashing nearly 43,000 fake emails a day on SecureWorks clients alone.

But Mr. Stewart began to believe the scam did not originate from China. The typical Chinese scams involve extracting trade secrets from companies and governments. Moreover, Chinese computers are often enlisted in attacks by scammers trying to conceal their location. Since a high number of Chinese computers use pirated software, security measures are low, making them particularly vulnerable to enlistment in cyber armies controlled by others.

Realizing the Chinese connection was a decoy, Mr. Stewart began looking for clues in the cache of stolen data. Before Mr. Stewart found it, the scammer had moved the stolen data with increasing frequency. Mr. Stewart tracked it to Web sites hosted on a server in Dallas, then Philadelphia, Toronto and back to Dallas.

In late-June, Mr. Stewart discovered the perpetrator had made a costly mistake. Combing through the stolen cache of data he had found, Mr. Stewart noticed one infected computer had accessed a familiar Web site address -- the same one used to host the scam. Mr. Stewart concluded the scammer had mistakenly infected his own computer. Now he had the scammer's computer address, a numerical address attached to every computer.

Public sources available online show the Internet service provider where every computer online in the world is registered. Law enforcement can use that information to identify -- and in some cases eventually arrest -- the suspect.

Armed with his first real clues, Mr. Stewart was then able to obtain files from other Web site hosting services associated with the address. He began piecing together the person's identity, tracing his online activity back several years. He found connections between this scam and others that used the same Web server and employed similar coding techniques, leading to additional email addresses, online aliases and Web sites most likely used over the years by the same person.

Those included a Web site for what initially appeared to be a legitimate investment company, called Ronald West, and another for a company called Beitel Electronics. Both turned out to be bogus names used as part of his criminal operation. Mr. Stewart found an older version of the Beitel Electronics site under the name Trispective. A Google search of that name led to an array of postings dating back several years from a young Romanian male.

Those postings provided additional details: The person is fluent in English; born on July 21, 1982; and often goes by the online alias "Raynor," a reference to a character from the online game Starcraft.

Professional criminals on the Web rarely leave clues, but there is a point in their lives when they are just entering the field and still learning how to conceal themselves. That formative period -- still traceable on the Internet -- can provide tidbits of information critical to unlocking the person's identity.

Using the variety of names he had collected, he found one posting from late 2002 under the name Trispective, showing that the individual at the time owned and wanted to sell the domain name thegov.org. Using an archival Web tool, Mr. Stewart in mid-June found an actual photo of "Raynor" attached to the site at the time.

It shows a glowering young man standing in what appears to be a computer room, with tiled walls and a bank of computer terminals behind him. He has dark, heavy eyebrows, jet-black bangs hanging over his face and a holstered gun strapped over his shoulder. Mr. Stewart forwarded his collected evidence to the Federal Bureau of Investigation. The agency in recent years has stationed agents in Romania and more than 60 other countries to follow up on such leads.

"We are in an electronic arms race," says Shawn Henry, deputy assistant director of the FBI's cyber-crime division. "Every time our technology catches up with the latest [malicious software], the bad guys come up with another way to get in." He declined to comment on whether the agency is investigating Raynor. The person using that screen name did not respond to an email seeking comment.

The scam is still circulating -- one week last month SecureWorks detected 8,323 such emails -- though it is likely being done by copycats. The scam has also taken other forms, including an email that purported to be from the Internet Revenue Service informing recipients they are being investigated for tax fraud. Another version sent a phony invoice for services rendered.

### **Raynor's Advantage**

Raynor's biggest advantage: lack of awareness, since most of its victims are too embarrassed to go public. Patrick Boegel, an executive with an advertising company in Albany, N.Y., called Media Logic, discovered the scam software on his computer after Mr. Stewart contacted him.

Mr. Boegel didn't believe it at first, but eventually was able to determine that several things were compromised, including log-in information for email and other Web sites, including a photo gallery site. Initially willing to discuss his experience, Mr. Boegel later declined, citing "company policy."

Mr. Boegel was lucky. His data was found by Mr. Stewart, and he was told what was happening. Nobody -- except perhaps Raynor -- knows how many executives were ensnared, how much data stolen, or the financial toll.

Mr. Stewart's pursuit continues. Late last month, Mr. Stewart found the Romanian had come up with a new idea: sending infected emails purportedly from the Equal Employment Opportunity Commission telling recipients a harassment complaint was filed against them. This week, Raynor was sending as many as 1,000 such emails to SecureWorks clients each day.

**Write to** Christopher Rhoads at [christopher.rhoads@wsj.com](mailto:christopher.rhoads@wsj.com)<sup>5</sup>

**URL for this article:**

<http://online.wsj.com/article/SB119456922698387317.html>

**Hyperlinks in this Article:**

- (1) <http://forums.wsj.com/viewtopic.php? t=974>
- (2) <http://forums.wsj.com/viewtopic.php? t=974>
- (3) [javascript:OpenG\('http://online.wsj.com/public/resources/documents/info-flash08.html? project=BETTERBUSINESS'\)](javascript:OpenG('http://online.wsj.com/public/resources/documents/info-flash08.html? project=BETTERBUSINESS'))
- (4) <http://www.secureworks.com/research/threats/bbbphish/>
- (5) <mailto:christopher.rhoads@wsj.com>

**Copyright 2007 Dow Jones & Company, Inc. All Rights Reserved**

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit [www.djreprints.com](http://www.djreprints.com).

**RELATED ARTICLES AND BLOGS**

---

**Blog Posts About This Topic**

- [Will an Internet "Jihad" Be More Tha A Hiccup For The U.S.](#) [www.wakeupamericans-spree.blogspot.com](http://www.wakeupamericans-spree.blogspot.com)
- [Domain Names Hosting](#) [aidinc.org](http://aidinc.org)

**More related content** *Powered by Sphere* 