

PCWorld » Business Center » Security

Recommend: 10 19 1 29 0 Comments

As Targeted E-mail Attacks Proliferate, Companies Wince

By [Jeremy Kirk, IDG News](#) Aug 5, 2011 2:50 pm

The strange e-mails arrived in executives' inboxes around the same time that the Australian oil company was negotiating a deal with a Chinese energy company.

The e-mails had the same structure and format as those sent around the company and were baited with text that appeared to refer to a supposed continuing discussion between executives. The messages looked authentic from a nontechnical perspective, just part of normal electronic communication within a company.

But the corporate IT administrator felt something wasn't quite right. Upon closer examination, the administrator found the e-mails, while appearing to come from internal company servers, were actually coming from other domains not authorized to send e-mail for the company.

The e-mails contained a malicious link that would redirect the person who opened it to a website of another energy company whose Web pages had been hacked in order to deliver malicious software designed to steal data. Victims would have no indication they'd been attacked.

It became clear that hackers were on a campaign to find out more about the pending deal.

"This was just their [the hackers] idea of due diligence," said the Australian IT administrator, who did not want himself or his company to be identified in this story due to the sensitivity of the intrusion.

The situation that faced the Australian company is one that is confronting companies and organizations worldwide regardless of their industry: hackers are getting a lot better at breaking through the defenses designed to keep information safe.

The attacks these days are "getting worse," said Alex Lanstein, a network and systems architect at security vendor FireEye, which makes systems designed to thwart Web-based attacks.

On Tuesday, McAfee -- a major security vendor now owned by Intel -- said it had gained access to a server that had logged intrusions into 72 companies, nongovernmental organizations and governments, including the U.N., U.S. defense contractors and the World Anti-doping Agency, among many others.

Dubbed "Operation Shady RAT" (remote access tool), McAfee heralded the operation as one of the most significant examples of "advanced persistent threats," or cyberattacks that are undetected for a long time.

Some of the most frequently targeted organizations are financial institutions, energy companies, defense contractors and pharmaceutical companies, but hackers are also expanding their remit to other areas, such as law firms, Lanstein said.

Law firms are always at the core of many business transactions, ranging from mergers and acquisitions to patent negotiations and more. And their computer security practices are not quite as good as more frequently targeted organizations, Lanstein said.

"There are always lawyers involved and they always have the most sophisticated information," he said.

Governments are a frequent target. William Hague, the U.K.'s foreign secretary, said in a speech in February that three of his staff were sent e-mails from a purported colleague outside the Foreign Office, the U.K.'s equivalent of the U.S. State Department.

"The e-mail claimed to be about a forthcoming visit to the region and looked quite innocent," Hague said. "In fact it was from a hostile state intelligence agency and contained computer code embedded in the attached document that would have attacked their machine. Luckily, our systems identified it and stopped it from ever reaching my staff."

Cisco's ScanSafe division, which specialized in products that scan Web traffic for malicious activity, [released a report earlier this week](#) that looked at how frequently employees of enterprises encounter malicious software on the Internet. It found employees as a group ran into malware an average of 335 times per month for the first half of this year.

Companies in pharmaceutical, chemical, energy and oil industries are at the highest risk for encountering malware on the web, the report said.

In response to the targeted attacks against the Australian oil company, the IT administrator said he built a tool that automatically strips out links in e-mails that come from outside his company. That may be inconvenient for some users, but "we can do without the links but we can't do without security," he said.

Fundamentally, the administrator said many executives still regard computer security as a hindrance and that "these geeks are just trying to make their life hard."

ULTIMATE ENTERTAINMENT



Learn to use your computer network as a next-generation entertainment hub.

[Get started.](#)

HOME NETWORKING ZONE



Answers to your home networking questions.

[Get in the Zone](#)

Similar Articles:



['Massive' Epsilon E-Mail Breach Hits Citi, Chase, Many More](#)



[How to Monitor Your Employees' PCs Without Going Too Far](#)



[Epsilon E-Mail Breach: 4 Unanswered Questions](#)



[Must-Have Tools and Tricks](#)



[Cybercrime Fight Costing Companies More This Year](#)



[More than E-mail at Stake in Google Gmail Attack](#)

Best Prices on Security Devices

[Most Popular](#)[All Categories](#)

[RV220W Firewall Appliance](#)

\$257.75 and up [See All Prices](#)



[ProSafe FVS318G Firewall](#)

\$118.00 and up [See All Prices](#)



[RV 120W Wireless VPN/Firewall - 4 Port - VPN Throughput: 25 Mbps - IEEE 802.11n draft](#)

\$135.88 and up [See All Prices](#)



[NetDefend DFL-210 VPN/Firewall](#)

\$312.00 and up [See All Prices](#)

[See all Best Prices on Security Devices »](#)

See also: [Best Prices on Antivirus Software](#), [Best Prices on Security Software](#)

Subscribe to the BizFeed Newsletter - weekly

[See All Newsletters »](#)

"I still think they think this is a nuisance and that the security guy will take care of it," the IT administrator said. "They are not elected [to the board] for IT savvy. They're old-school business people."

Send news tips and comments to jeremy_kirk@idg.com

Would you recommend this story? YES | 2 NO | 0

Recommend: Like 10 19 1 29 Email 0 Comments Print

Comments



Leave a comment

Submit Comment

Once you click submit you will be asked to sign in or register an account if you are not already a member.

Editors' Picks



Dropbox Cloud Was a Haven for Data Thieves, Researchers Say



Tech Deals Led IPOs in Second Quarter



ICANN C to Step I

Home

Products

- Android App Reviews
- iPhone App Reviews
- Business Center
- Cameras
- Camcorders
- Cell Phones & PDAs
- Consumer Advice
- Desktop PCs
- E-Readers
- Gadgets
- Gaming
- HDTV
- Home Theater
- Laptops
- Macs & iPods
- Monitors
- Printers
- Software
- Spyware & Security
- Storage
- Tablets
- Tech Industry
- Tech Events
- Upgrading
- Windows 7

Network Sites

- PCWorld Business Center
- Search for Tech Jobs
- Careers at IDG
- Macworld
- MacUser
- Mac OS X Hints
- iPhone Central

About PCWorld

- About Us
- Advertise
- PCWorld Content Works
- Terms of Service Agreement
- Privacy Policy
- Site Map

Resources

- Newsletters
- FAQ
- Contact Us
- RSS Feeds
- Magazine Customer Service
- Community Standards

Visit other IDG sites:

© 1998-2011, PCWorld Communications, Inc.

Try 2 risk-free issues



Name City

Address 1 State Zip

Address 2 E-mail (optional)

[Click Here](#)

Canadian Residents | Foreign Residents | Gift Subscriptions
Customer Service | Privacy Policy