



April 23, 2007

Pg. 1

Cyberspies exploit Microsoft Office

By Byron Acohido, USA TODAY

SEATTLE — Cyberspies have a new secret weapon: tainted Microsoft Office files.

A rising number of cyberattacks are taking aim at specific individuals at critical government agencies and corporations — enticing them to unwittingly open a corrupted Word, Excel or PowerPoint file sent as an e-mail attachment.

Clicking on the file relinquishes control of the PC without the user's knowledge. The attacker then uses the compromised PC as a base from which to roam the organization's internal network.

Federal agencies and defense and nuclear contractors are under assault. Security firm MessageLabs says it has been intercepting a series of attacks from PCs in Taiwan and China since November.

"The bad guys know which organizations have data worth stealing and are picking them out one by one," says Alex Shipp, senior technologist at MessageLabs.

In early 2006, security experts detected one or two such attacks a week. Last month, MessageLabs intercepted 716 e-mails carrying corrupted Office files aimed at 216 different agencies and companies.

Assaults are coming from China and perhaps other countries in the hunt for military, trade and infrastructure intelligence, says Alan Paller, research director at The SANS Institute, a security think tank. The goal: strategic advantage over the USA. "The attacks are working," says Paller. "Penetrations are deep and broad."

Some attacks could be "on-demand," at the behest of companies that hire cybergangs to pilfer data from rivals, says Righard Zwieneberg, chief researcher at Norman Data Defense Systems.

At a congressional hearing last week on cybersecurity, Donald Reid, a senior State Department official, described how an employee in May clicked on a Word document corrupted via a security hole for which Microsoft had no patch. A fix wasn't available until eight weeks later. Microsoft has issued 10 patches for security holes in Office programs since January 2006, including a handful delivered only after crooks began using newly discovered flaws in their attacks. The best protection: keeping Office security patches updated.

The Office file attacks are "very targeted and very limited," says Mark Miller, Microsoft's director of security response, who called on workers "to absolutely extend extreme caution" when opening Office files in e-mail.

Microsoft has been slow to patch security holes in Office programs, says Zwieneberg. "But the cybercriminals are getting smarter and smarter."

http://www.usatoday.com/tech/news/computersecurity/2007-04-22-cyberspies-microsoft-office_N.htm