

**SEATTLE POST-INTELLIGENCER**

[http://seattlepi.nwsourc.com/business/351670\\_picframevirus18.html](http://seattlepi.nwsourc.com/business/351670_picframevirus18.html)

**Chinese PC virus may have hidden agenda**

*Last updated February 17, 2008 10:07 p.m. PT*

**By DEBORAH GAGE**  
SAN FRANCISCO CHRONICLE

An insidious computer virus recently discovered on digital photo frames has been identified as a powerful new Trojan Horse from China that collects passwords for online games -- and its designers might have larger targets in mind.

"It is a nasty worm that has a great deal of intelligence," said Brian Grayek, who heads product development at Computer Associates, a security vendor that analyzed the Trojan Horse.

The virus, which Computer Associates calls Mocmex, recognizes and blocks antivirus protection from more than 100 security vendors, as well as the security and firewall built into Microsoft Windows. It downloads files from remote locations and hides files, which it names randomly, on any PC it infects, making itself very difficult to remove. It spreads by hiding itself on photo frames and any other portable storage device that happens to be plugged into an infected PC.

The authors of the new Trojan Horse are well-funded professionals whose malware has "specific designs to capture something and not leave traces," Grayek said. "This would be a nuclear bomb" of malware.

By studying how the code is constructed and how it's propagated, Computer Associates has traced the Trojan to a specific group in China, Grayek said. He would not name the group.

The strength of the malware shows how skilled hackers have become and how serious they are about targeting digital devices, which provide a new frontier for stealing information from vast numbers of unwary PC owners. More than 2.26 million digital frames were sold in 2007, according to the Consumer Electronics Association, and it expects sales to grow to 3.26 million in 2008.

The new Trojan also has been spotted in Singapore and Russia and has 67,500 variants, according to Prevx, a security vendor headquartered in England.

Grayek said Mocmex might be a test for some bigger attack, because it's designed to capture any personal, private or financial information, yet so far it's only stealing passwords for online games.

"If I send you a package but it doesn't explode, why did I send it?" he said. "Maybe I want to see if I can get it out to you and how you open it."

The initial reports of infected frames came from people who had bought them over the holidays from Sam's Club and Best Buy. New reports involve frames sold at Target and Costco, according to SANS, a group of security researchers in Bethesda, Md., who began asking for accounts of infected devices on Christmas Day. So far the group has collected more than a dozen complaints from people across the country.

The new Trojan isn't the only piece of malware involved. Deborah Hale of SANS said the researchers also found four other, older Trojans on each frame, which may serve as markers for botnets -- networks of infected PCs that are remotely controlled by hackers.

There is W32.Rajump, which deposits the same piece of malware that infected some of Apple's video iPods during manufacturing in October 2006. It gathers Internet Protocol addresses and port numbers from infected PCs and ships them out, according to Symantec. One destination is registered to a service in China that allows people to conceal their own IP addresses.

Then there is a generic Trojan; a Trojan that opens a back door on PCs and displays pop-up ads; and a Trojan that spreads itself through portable devices like Moxmex does.

How all this malware got onto the photo frames and what it's doing there is unclear. Trojans can download other Trojans, which is part of how botnets are controlled.

While SANS is investigating the infections, the retailers are saying little.

Sam's Club said it has found no infected frames, and its distributor, Advanced Design Systems, did not return calls.

A few Target customers complained about frames distributed by Uniek, a store spokesman said. Target is no longer selling those frames, but that's because they didn't sell well over the holidays, he said. Target has found no infections, he said, but is watching for them.

Best Buy said one line of its Insignia frames -- also now discontinued -- was infected during manufacturing but would not provide details.

Costco did not return calls seeking comment.

## **VIRUS PROTECTION**

Protecting against these new computer viruses, which so far are aimed at PCs running Windows, is hard -- and sometimes impossible. Updated antivirus software works unless the malware writers get ahead of the antivirus vendors, which is what happened with the new Trojan. Computer Associates, for example, just began protecting against it in the past two weeks.

While some advise disabling Autorun in Windows, which allows devices to run automatically when they're plugged into a USB port, it's not a fail-safe. Doing so requires some computer expertise, and this Trojan re-enables Autorun if it's turned off, according to Brian Grayek of Computer Associates. "If you plug in (the frame), you're already infected," he said.

Deborah Hale at SANS suggested that PC users find friends with Macintosh or Linux machines and have them check for malware before plugging any device into a PC.

She also recommended backing up data with an online service such as Mozy.com that offers free backup for home users with less than 2 gigabytes of data. But it does not back up the operating system, she warned. If you're attacked and your PC fails, you'll have to reformat and reload all of the programs.

If you think you bought an infected device, e-mail SANS at [info@sans.org](mailto:info@sans.org) and call your retailer.

- Best Buy: 877-467-4289
- Sam's Club: 888-746-7726
- Target: 800-591-3869

- Costco: 800-955-2292

© 1998-2008 *Seattle Post-Intelligencer*

