

# Some new electronic gadgets come loaded with viruses

01:16 PM CDT on Saturday, March 15, 2008

**Associated Press**

From iPods to navigation systems, some of today's hottest gadgets are landing on store shelves with some unwanted extras from the factory – pre-installed viruses that steal passwords, open doors for hackers and make computers spew spam.

Computer users have been warned for years about virus threats from downloading Internet porn and opening suspicious e-mail attachments. Now they run the risk of picking up a digital infection just by plugging a new gizmo into their PCs.

Recent cases reviewed by The Associated Press include some of the most widely used tech devices: Apple Inc.'s iPods, digital picture frames sold by Target Corp. and Best Buy Co., and TomTom NV's navigation gear.

In most cases, Chinese factories – where many companies have turned to keep prices low – are the source.

So far, the virus problem appears to come from lax quality control – perhaps a careless worker plugging an infected music player into a factory computer used for testing – rather than organized sabotage by hackers or the Chinese factories.

It's the digital equivalent of the recent series of tainted products traced to China, including toxic toothpaste, poisonous pet food and toy trains coated in lead paint.

But sloppiness is the simplest explanation, not the only one.

If a virus is introduced at an earlier stage of production, when software is uploaded to the gadget, then the problems could be far more serious and widespread.

Knowing how many devices have been sold, or tracking the viruses with any precision, is impossible because of the secrecy kept by electronics makers and the companies they hire to build their products.

But given the nature of mass manufacturing, the numbers could be huge.

"It's like the old cockroach thing – you flip the lights on in the kitchen, and they run away," said Marcus Sachs, a former White House cybersecurity official who now runs the security research group SANS Internet Storm Center. "You think you've got just one cockroach? There's probably thousands more of those little boogers that you can't see."

Jerry Askew, a Los Angeles computer consultant, bought a new Uniek digital picture frame to surprise his 81-year-old mother for her birthday. But when he added family photos, it tried to unload a few surprises of its own.

When he plugged the frame into his Windows PC, his antivirus program alerted him to a threat. The \$50 frame, built in China and bought at Target, was infested with four viruses, including one that steals passwords.

"You expect quality control coming out of the manufacturers," said Mr. Askew. "You don't expect that sort of thing to be on there."

### **Accidental – so far**

Security experts say the malicious software is apparently being loaded at the final stage of production, when gadgets are pulled from the assembly line and plugged in to a computer to make sure everything works.

If the testing computer is infected – say, by a worker who used it to charge his own infected iPod – the digital germ can spread to anything else that gets plugged in.

The recent infections may be accidental, but security experts say they point out an avenue of attack that could be exploited by hackers.

"We'll probably see a steady increase over time," said Zulfikar Ramzan, a computer security researcher at Symantec Corp. "The hackers are still in a bit of a testing period – they're trying to figure out if it's really worth it."

Thousands of people whose antivirus software isn't up to date may have been unknowingly infected by new products, experts warn. And even protective software may not be enough.

Consumers can protect themselves from most factory-loaded infections by running an antivirus program and keeping it up to date. The software checks for known viruses and suspicious behaviors that indicate an attack by malicious code – whether from a download or a gadget attached to the PC via a USB cable.

One information technology worker wrote to the SANS security group that his new digital picture frame delivered "the nastiest virus that I've ever encountered in my 20-plus-year IT career." Another complained that his new external hard drive had malfunctioned because it came loaded with a password-stealing virus.

Monitoring suppliers in China and elsewhere is expensive and cuts into the savings of outsourcing. But it's what U.S. companies must do to prevent poisoning on the assembly line, said Yossi Sheffi, a professor at the Massachusetts Institute of Technology specializing in supply chain management.

"It's exactly the same thing, whether it happened in cyberspace or software or lead paint or toothpaste or dog food – they're all quality control issues," Mr. Sheffi said.

While manufacturing breakdowns don't happen often, they have become frequent enough – especially amid intense competition among Chinese suppliers – to warrant more scrutiny by companies that rely on them, Mr. Sheffi said.

"Most of the time it works," he said. "The Chinese suppliers have every reason to be good suppliers because they're in it for the long run. But it's a higher risk, and we've now seen the results of that higher risk."

### **Few details**

The companies whose products were infected in cases reviewed by The Associated Press refused to reveal details about the incidents. Of those that confirmed factory infections, all said they had corrected the problems and taken steps to prevent recurrences.

Apple disclosed the most information, saying the virus that infected a small number of video iPods in 2006 came from a PC used to test compatibility with the gadget's software.

Best Buy said it pulled its affected China-made frames from the shelves and took "corrective action" against its vendor. But the company declined repeated requests to provide details.

Sam's Club and Target say they are investigating complaints but have not been able to verify that their frames were contaminated.

Legal experts say manufacturing infections could become a big headache for retailers that sell infected devices and the companies that make them, if customers can demonstrate they were harmed by the viruses.

"The photo situation is really a cautionary tale – they were just lucky that the virus that got installed happened to be one that didn't do a lot of damage," said Cindy Cohn, legal director for the Electronic Frontier Foundation. "But there's nothing about that situation that means next time the virus won't be a more serious one."