From brand new laptop to infected by pressing 'on' (Update)

September 13 2012, by Richard Lardner

A customer in Shenzhen, China, took a brand new laptop out of its box and booted it up for the first time. But as the screen lit up, the computer began taking on a life of its own. The machine, triggered by a virus hidden in its hard drive, began searching across the Internet for another computer.

The laptop, supposedly in pristine, super-fast, direct-from-the-factory condition, had instantly become part of an illegal, global network capable of attacking websites, looting bank accounts and stealing personal data.

For years, online investigators have warned consumers about the dangers of opening or downloading files emailed to them from unknown or suspicious sources. Now, they say malicious software and computer code could be lurking on computers before the bubble wrap even comes off.

The shopper in this case was part of a team of Microsoft researchers in China investigating the sale of counterfeit software. They suddenly had been introduced to a malware called Nitol. The incident was revealed in court documents unsealed Thursday in a federal court in Virginia. The records describe a new front in a legal campaign against cybercrime being waged by the maker of the Windows operating system, which is the biggest target for viruses.

The documents are part of a computer fraud lawsuit filed by Microsoft against a web domain registered to a Chinese businessman named Peng

Yong. The company says it is a major hub for illicit Internet activity. The domain is home base for Nitol and more than 500 other types of malware, making it the largest single repository of infected software that Microsoft officials have ever encountered.

Peng, the owner of an Internet services firm, said he was not aware of the Microsoft lawsuit but he denied the allegations and said his company does not tolerate improper conduct on the domain, 3322.org. Three other unidentified individuals accused by Microsoft of establishing and operating the Nitol network are also named in the suit.

What emerges most vividly from the court records and interviews with Microsoft officials is a disturbing picture of how vulnerable Internet users have become, in part because of weaknesses in computer supply chains. To increase their profit margins, less reputable computer manufacturers and retailers may use counterfeit copies of popular software products to build machines more cheaply. Plugging the holes is nearly impossible, especially in less regulated markets like China, and that leaves openings for cybercriminals.

"They're really changing the ways they try to attack you," said Richard Boscovich, a former federal prosecutor and a senior attorney in Microsoft's digital crimes unit.

And distance doesn't equal safety. Nitol, for example, is an aggressive virus found on computers in China, the United States, Russia, Australia and Germany. Microsoft has even identified servers in the Cayman Islands controlling Nitol-infected machines. All these compromised computers become part of a botnet—a collection of compromised computers—one of the most invasive and persistent forms of cybercrime.

Nitol, meanwhile, appears poised to strike. Infection rates have peaked,

according to Patrick Stratton, a senior manager in Microsoft's digital crimes unit who filed a document in the court case explaining Nitol and its connection to the 3322.org domain.

For Microsoft, pursuing cybercriminals is a smart business. Its Windows operating system runs most of the computers connected to the Internet. Victims of malware are likely to believe their problems stem from Windows instead of a virus they are unaware of, and that damages the company's brand and reputation.

But more than Microsoft's image is stake when counterfeit products are tainted by malware that spreads so rapidly, Boscovich said. "It's more than simply a traditional intellectual property issue," Boscovich said. "It's now become a security issue."

The investigation by Microsoft's digital crimes unit began in August 2011 as a study into the sale and distribution of counterfeit versions of Windows. Microsoft employees in China bought 20 new computers from retailers and took them back to a home with an Internet connection.

They found forged versions of Windows on all the machines and malware pre-installed on four. The one with Nitol, however, was the most alarming because the malware was active.

"As soon as we powered on this particular computer, of its own accord without any instruction from us, it began reaching out across the Internet, attempting to contact a computer unfamiliar to us," Stratton said in the document filed with the court.

The laptop was made by Hedy, a computer manufacturer in Guangzhou, China, according to the court records. The company, reached by phone, declined to answer questions.

Stratton and his colleagues also found Nitol to be highly contagious. They inserted a thumb drive into the computer and the virus immediately copied itself onto it. When the drive was inserted into a separate machine, Nitol quickly copied itself on to it.

Microsoft examined thousands of samples of Nitol, which has several variants, and all of them connected to command-and-control servers associated with the 3322.org domain, according to the court records.

"In short, 3322.org is a major hub of illegal Internet activity, used by criminals every minute of every day to pump malware and instructions to the computers of innocent people worldwide," Microsoft said in its lawsuit.

Peng, the registered owner of 3322.org, said he has "zero tolerance" for the misuse of domain names and works with Chinese law enforcement whenever there are complaints. Still, he said, his huge customer base makes policing difficult.

"Our policy unequivocally opposes the use of any of our domain names for malicious purposes," Peng said in a private chat via Sina Weibo, a service like Twitter that's very popular in China. "We currently have 2.85 million domain names and cannot exclude that individual users might be using domain names for malicious purposes."

But past warnings by other online security firms have been ignored by Peng, Boscovich said. 3322.org accounted for more than 17 percent of the world's malicious web transactions in 2009, according to Zscaler, a computer security firm in San Jose, California. In 2008, Russian security company Kaspersky Lab reported that 40 percent of all malware programs, at one point or another, connected to 3322.org.

U.S. District Judge Gerald Bruce Lee, who is presiding in the case,

granted a request from Microsoft to begin steering Internet traffic from 3322.org that has been infected by Nitol and other malwares to a special site called a sinkhole. From there, Microsoft can alert affected computer users to update their anti-virus protection and remove Nitol from their machines.

Since Lee issued the order, more than 37 million malware connections have been blocked from 3322.org, according to Microsoft.