The only people happy with this news will be the local system builders...

Microsoft's digital crimes division tells the court **malware is being installed on PC machines in China before they're even released from the factories.**

What? That's right, your customers who import direct from China may be buying Trojan Horses. Even European importers who bring in unknown Chinese brands could be affected-- unless the importer (like many larger distributors already do) sets up his own security control.

Microsoft investigating counterfeit software in China purchased 20 new computers via retail only to discover malware pre-installed on 20% of the machines tested, with pirated Windows versions present on each of the tested machines.

According to Microsoft's Patrick Stratton, a manager in the company's digital crimes unit and the author of the court testimony, the discovery of a machine pre-loaded with the malware Nitol was the most disturbing.

"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," he wrote. As soon as a thumb drive was plugged into the machine, Nitol copied itself onto that drive and then, when that drive was attached to another machine, copied itself onto the new machine as well.

All this news comes from a lawsuit filed by Microsoft against a man behind a web domain used by the malware-- a Chinese businessman known as Peng Yong. The lawsuit alleges "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."

Peng denies any wrongdoing but security firm **Zscaler** pinpoints 3322.org as responsible for more than 17% of malicious web transactions in the world in a single year.

Why this matters is that ecommerce lets Asian makers direct compete with local system builders. Tablets touted on the internet at cheap prices can be had by the public. But **no one is verifying the security of their supply chains.**
An Asian maker need not be directly involved: a handy bribe could inspire a factory worker.

Indeed this could happen in Europe as well... but at least when discovered here the consumers would have strong local recourse for damages. The ancient Romans had it right: Caveat emptor or "Let the buyer beware."

Go **Read Microsoft's Frightening Testimony on Unsecured Supply Chains**