NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2006/031306widernet-counterfeit.html

Targeting bogus goods

Technology gives merchants a fighting chance.

By Ann Bednarz, Network World, 03/13/06

Sometimes it's easy for Stacy Papachristos to spot a fake, such as a video of a classic WrestleMania match for sale online when World Wrestling Entertainment never released such a product.

The source? Counterfeiters and trademark infringers using the Internet to hawk products. "They'll be selling some of our older footage on DVDs, and it's footage I know we haven't produced on DVD," says Papachristos, who is associate counsel for intellectual property at WWE in Stamford, Conn.

Companies such as Tiffany, Oakley and Montblanc know the drill well. Counterfeiters have long created knockoffs of luxury goods from companies such as these. Auto parts makers, sporting goods suppliers and pharmaceutical manufacturers also are all too familiar with counterfeiters.

It's a problem that has grown since fraudsters began using auction sites and online marketplaces to sell counterfeit goods efficiently and in large volumes. The International Chamber of Commerce estimates that counterfeit goods account for 5% to 7% of world trade. In the IT industry, manufacturers lose about $100 billion to counterfeiters annually, according to research from KPMG and the nonprofit Alliance for Gray Market and Counterfeit Abatement (AGMA).

Fortunately for businesses, as counterfeit-related damages have multiplied, so too have the tools to fight back. Brandimensions, Cyveillance, GenuOne and MarkMonitor are among software makers with products that monitor for inappropriate or fraudulent use of a corporate name or identity on the Internet, including Web sites, domain names, chat rooms and auctions. (See related story about GenuOne customer Mitchell & Ness Nostalgia Company.)

In addition, vendors such as 3M, GenuOne and Texas Instruments offer security labels, some outfitted with RFID tags, others designed with photo-luminescent dyes embedded into labels and coatings, for example. These technologies can help companies better track and authenticate components and finished goods as they move through the supply chain, as well as make it harder to tamper with or copy packaging.

"E-commerce is playing a big role in counterfeit. The counterfeiters obviously want to get as close to the consumer as possible, and they don't want to have to rely on resellers and distributors," says Nick Tidd, president of AGMA.

A group of IT vendors formed AGMA to share ideas for tackling gray market issues. (Gray market activity refers to sales of authentic goods through an unauthorized channel.) The group has expanded its focus to include counterfeit IT gear.

"Counterfeit came on the radar screen about two and a half years ago. A number of our members found that their return rates were starting to increase, and that the quality of those returns was starting to become suspect," Tidd says.

Those are two indicators that can alert vendors to a counterfeiting problem - something not many IT buyers first

suspect, Tidd says. Consumers don't tend to think that IT gear, in its complexity, can be counterfeited, he says.

But Tidd has learned not to underestimate the tenacity of counterfeiters. "There's never a day that we don't just kind of shake our heads and say, 'Oh my gosh.' Even as our products get more complex, with things like surface mount technologies, and components get more miniaturized, they just find a way to copy it."

The allure of easy money is too strong. Jeffrey Unger, CEO of GenuOne, likens counterfeiting to selling illegal drugs. There's enormous economic incentive, but with less harsh penalties - a combination that has attracted the attention of organized crime, especially in Asia and Russia, he says. "It's a lot less risky to move counterfeit DVDs or routers or sneakers than it is to sell drugs. And the money is just as good."

Fighting the good fight

World Wrestling Entertainment has been using software from MarkMonitor for two years to help find knockoffs, after fans tipped off the company to the rash of unauthorized merchandise being sold on the Web.

"A lot of our fans started reporting infringements online to us," Papachristos recalls. The reports prompted WWE to dig deeper. "When we looked, we just saw an unbelievable amount of stuff on the Internet," she says.

WWE first deployed MarkMonitor's brand-protection software to find inappropriate uses of its corporate name, brands and logos. The company recently added the vendor's new Auction Monitoring module, which creates a daily snapshot of suspicious auctions and resellers so Papachristos doesn't have to manually scour the sites. She then decides whether to send a cease and desist letter, report the offense to the auction site, or request a suspension of the seller. "It saves me so much time," Papachristos says.

Detection speed is important, given how quickly fake wares proliferate. Counterfeiters work incredibly fast, whether they're copying a complicated piece of IT hardware or a simple DVD.

When a pay-per-view event airs, Papachristos knows to look for an unauthorized DVD version right away. "They'll have it up the next day," she says.

Sometimes the bad guys even beat WWE to market. When word gets out that WWE plans to release a new anthology of WrestleMania episodes, fake anthologies immediately start turning up on the Internet. "All of a sudden on eBay I'll see people trying to sell old WrestleMania footage," Papachristos says. "They'll make their own compilation and try to sell it because they know that ours is coming out."

The same goes for complex equipment. Before a product is released, there will be counterfeit versions, GenuOne's Unger says.

Outsourcing has increased the problem, he says. When companies are choosing a factory to outsource their manufacturing, they'll send samples of their products all over the world. If one winds up in the wrong hands, it will be reproduced and made available illegally before the company finishes its own production.

Using contract manufacturers can increase a company's exposure to counterfeiting. "Companies are taking their intellectual property, sending it to a third party, and teaching them how to make their product. There's leakage in that supply chain," Unger says.

In addition, as companies swap overseas factories, there's a risk production won't stop at the facility they vacated. "You've basically just left someone, somewhere, with the ability to make your product. Many of them, unfortunately, will keep making it."

One way to combat vulnerabilities in contract manufacturing is to better monitor outsourcers, supply chain partners and

distributors. "Folks have to be very diligent about watching the raw materials that are going into their factories, and they've got to watch the serial numbers very closely for duplication and fabrication," Tidd says.

Another anti-counterfeiting tactic is to make use of copy-resistant products and packaging, says Tidd, whose day job is head of 3Com's channel operations in North America. "At 3Com we've just started putting a four-dimensional holographic label on our switches," he says. "We're telling consumers of our product, 'Look for this label, which will help identify if this product is legitimate.'"

3Com also has been proactive in working with law enforcement to help orchestrate raids on sites where counterfeit 3Com products are being made. In some cases, law enforcement officials have gone in and seized the property and assets of the counterfeiters, Tidd says.

"When we do seize, it's often quite startling the amount of raw material that's there - everything from the components, right through to some of the finish goods," he says. "We might find our boxes and manuals. And that really is the only evidence we have as to the potential of that factory and what it could have produced against us from a revenue loss potential."

The Wider Net archive.