

Unraveling Software Piracy

New counterfeiting exhibition at French Science and Industry Museum in Paris showcases Microsoft's use of intelligence and crime forensics to help dismantle the world's largest software counterfeiting ring.

PARIS — April 20, 2010 — Counterfeits are often associated with the images of cheap knock-offs offered at flea markets or low-quality fake designer goods sold out of someone's car trunk. These images are at odds with the real story behind software piracy. That story involves highly organized criminals operating sophisticated manufacturing plants to create near-exact replicas of genuine software.

These counterfeits are intended to deceive consumers into thinking they are buying the genuine article and are often sold at prices that are nearly the same as genuine software. However, while the counterfeit discs and packaging appear the same as legitimate software, the counterfeit software code itself can contain malware or viruses, or be stripped of critical security features that protect customers' information and technology systems. This faulty code leaves consumers vulnerable to system failures and, even worse, to cybercriminals who roam the Internet for potential victims.

This is a story in which Microsoft's David Finn and his team of piracy experts are playing a leading role by using cutting-edge intelligence and forensic techniques to track down the global criminal counterfeiting syndicates and support law enforcement in over 70 countries throughout the world. What's more, says Finn, who heads the company's anti-piracy investigations through its worldwide Legal and Corporate Affairs department, "We are increasingly collaborating with our own customers, who are providing critical information to help us identify software pirates, and addressing their concerns about the risks of using counterfeit software."

This week the story gains international attention through a new counterfeiting exhibition at the [Cité des Sciences et de l'Industrie](#) (French Science and Industry Museum) in Paris. Microsoft will be part of this broader exhibit that showcases how different industries are affected by piracy, and what the risks are that consumers face. The company will represent the software industry with a video documentary about how partnering with law enforcement across several continents led to prosecution of a Chinese criminal syndicate in what became the largest counterfeit case in history. In addition, a number of genuine and counterfeit Microsoft products will be displayed to help consumers distinguish genuine software from counterfeit. Also on display will be the company's latest technology used to identify and track down software pirates.

"This exhibition represents one of the largest combined efforts of government and industry coming together to speak out on the threats consumers face because of counterfeiting," says Blandine Savrda, commissioner at the Cite des Sciences et de l'Industrie. "If not for the collaboration of governments and private industry, the illegal trade of pirated products would continue to increase at an even higher rate."

The software piracy world today, says Finn, is a vast web of large and small criminal enterprises, seeking to profit in a variety of ways. Consumers are increasingly the victims of pirated software riddled with malware, viruses and malicious code by counterfeiters who are happy to take their money without regard to the quality and integrity of the product they are passing off as the real thing.

One key study by IDC in 2006* showed that one in four Web sites offering counterfeit software attempted to install unwanted or malicious code upon downloading. This rate is rising, as found by Media Surveillance, an anti-piracy solutions company based in Germany, when it recently downloaded

several hundred pirated copies of Windows and hacks and found that 32 percent contained malicious code.

The impact of harmful counterfeit software can be dramatic. Companies using pirated software are 73 percent more likely to experience a loss of data and 43 percent more likely to have computer failures lasting 24 hours or longer, accordingly to a Harrison Group study. “We are telling this story in order to underscore the fact that counterfeit products can be much more expensive than people think, putting people’s business and financial information at risk. And to make sure people understand that we are talking about criminal gangs — like the massive syndicate involved in the China case — who are behind the global manufacture and distribution of counterfeit software,” says Finn.

Unraveling Counterfeit Organizations

Donal Keating, Microsoft worldwide senior forensics manager, has devoted his career at Microsoft to developing technologies that uncover counterfeit software. Keating’s work has helped to unravel the mystery behind the world’s largest software counterfeiting crime syndicates and has helped lead to arrests, product seizures and convictions all over the world.

“As a rule, the software counterfeiting business is much like many legal big businesses in their level of organization, manufacturing expertise and sophistication,” says Keating. “The difference is that these organizations also employ many of the same tactics commonly used by criminal rings such as the use of violence and child labor, and the involvement in other types of crimes.”

Keating has traveled the world providing his expertise to law enforcement at counterfeit production sites under investigation by the police. “Seeing where counterfeit discs are manufactured has helped me see behind the curtain of what the crime syndicates are doing, which in turn has enabled us to develop innovative forensic systems and tools to develop evidence that helps bring them to justice,” he says.

“Ballistic” Forensics for Discs

In the early days, even if Microsoft was able to identify the counterfeiters, it was sometimes difficult to prove with certainty that a particular disc was counterfeit. Beyond that, it was quite difficult to prove the full extent of the criminal activity. These challenges motivated Finn and his team to develop more sophisticated forensic methods of analyzing counterfeit evidence. Microsoft also responded by developing more robust optical disc and print security features such as interactive holograms and embedded threads. “We are now able to match counterfeit discs to the machines that produced them through what I call ballistic forensics, much like police do with markings on bullets,” says Keating. “We are also able to ‘connect the dots’ between pieces of counterfeit to establish the distribution patterns of the crime rings.” These technology innovations led to the dismantling of the largest counterfeit ring in history in a case known as “Operation China Online.”

The China Syndicate

In a landmark case, Microsoft assisted China’s Public Security Bureau and the U.S. Federal Bureau of Investigation in an investigation that [led to raids in Southern China](#) of a criminal syndicate believed to have produced more than \$2 billion worth of counterfeit Microsoft software. Along with the use of forensic technologies, customers were a critical element in the investigation of this ring as more than 1,000 customers submitted counterfeit copies of their software to Microsoft, which Keating and his team were able to forensically link to the counterfeit syndicate. The counterfeit software came from 36 different countries and included 19 different versions of Microsoft products in 11 languages. Based in significant part on this powerful forensic evidence, a Chinese court convicted 11 members of the ring

and sentenced them to the longest prison terms ever handed down in a software counterfeiting case in China. This case made international headlines and will be featured at the [Cité des Sciences et de l'Industrie](#) beginning today.

“This case marked a milestone in the fight against software piracy, showcasing how governments, law enforcement and private companies can work together across borders to bring counterfeiters to justice,” said FBI agent Jason Smolanoff. “Unfortunately, software counterfeiting is a global, illegal business without borders. Criminals may be on the other side of the globe and may not even speak the same language, but they prey upon consumers all over the world.”

* “The Risks of Obtaining and Using Pirated Software,” IDC white paper sponsored by Microsoft, Doc # WP1006GRO, October 2006

Sidebar: How to Tell if Your Software Is Genuine

How do you know if the software you buy is genuine? Consider the following:

- Are you buying from a reputable reseller?
- Can your reseller confirm that its software would pass a Windows Genuine Advantage online validation test?
- Is the price too good to be true?
- Is a Certificate of Authenticity (COA) included?
- Is a hologram CD, DVD, or recovery media included?
- Are the product packaging and documentation high quality?
- Is an End User License Agreement (EULA) included?

If you've already purchased Microsoft software, you can find out for sure by visiting <http://www.howtotell.com>.

Related Links

- Press Releases
 - Microsoft and Consumers Take Action Against Global Software Piracy, Dec. 2, 2009, <http://www.microsoft.com/presspass/press/2009/dec09/12-02GlobalPiracyActionPR.mspx>
 - Raids in Southern China Target \$2 Billion Global Software Counterfeiting Syndicate, July 24, 2007, <http://www.microsoft.com/presspass/press/2007/jul07/07-24CounterfeitingSyndicatePR.mspx>
- Microsoft Resources
 - Microsoft How to Tell site, <http://www.microsoft.com/howtotell/>
 - Microsoft Worldwide Anti-Piracy Virtual Press Room, <http://www.microsoft.com/presspass/presskits/antipiracy/>
- Other Resources
 - [Cité des Sciences et de l'Industrie](#) (French Science and Industry Museum)