November 6, 2010
Chasing Pirates: Inside Microsoft’s War Room
By ASHLEE VANCE

AS the sun rose over the mountains circling Los Reyes, a town in the Mexican state of Michoacán, one morning in March 2009, a caravan of more than 300 heavily armed law enforcement agents set out on a raid.

All but the lead vehicle turned off their headlights to evade lookouts, called “falcons,” who work for La Familia Michoacana, the brutal Mexican cartel that controls the drug trade. This time, the police weren’t hunting for a secret stash of drugs, guns or money. Instead, they looked to crack down on La Familia’s growing counterfeit software ring.

The police reached the house undetected, barreled in and found rooms crammed with about 50 machines used to copy CDs and make counterfeit versions of software like Microsoft Office and Xbox video games. They arrested three men on the spot, who were later released while the authorities investigate the case. “The entire operation was very complicated and risky,” says a person close to the investigation, who demanded anonymity out of fear for his life.

The raid added to a body of evidence confirming La Familia’s expansion into counterfeit software as a low-risk, high-profit complement to drugs, bribery and kidnapping. The group even stamps the disks it produces with “FMM,” which stands for Familia Morelia Michoacana, right alongside the original brand of various software makers.

The cartel distributes the software through thousands of kiosks, markets and stores in the region and demands that sales workers meet weekly quotas, this person says, describing the operation as a “form of extortion” on locals.

The arrival of organized criminal syndicates to the software piracy scene has escalated worries at companies like Microsoft, Symantec and Adobe. Groups in China, South America and Eastern Europe appear to have supply chains and sales networks rivaling those of legitimate businesses, says David Finn, Microsoft’s anti-piracy chief. Sometimes they sell exact copies of products, but often peddle tainted software that opens the door to other electronic crime.

“As long as intellectual property is the lifeblood of this company, we have to go protect it,” Mr. Finn says.

Microsoft has adopted a hard-line stance against counterfeiting. It has set up a sophisticated anti-piracy operation that dwarfs those of other software makers; the staff includes dozens of former government intelligence agents from the United States, Europe and Asia, who use a host of “CSI”-like forensic technology tools for finding and convicting criminals.

But the hunt for pirates carries with it a cost to Microsoft's reputation.

The company's profit from Windows and Office remains the envy of the technology industry, and critics contend that Microsoft simply charges too much for them. In countries like India, where Microsoft encourages local police officers to conduct raids, the company can come off as a bully willing to go after its own business partners if they occasionally peddle counterfeit software to people who struggle to afford the real thing.

"It is better for the Indian government to focus on educating its children rather than making sure royalties go back to Microsoft," says Eben Moglen, a law professor at Columbia Law School and a leading advocate of free software.

Mr. Finn argues that Microsoft has no choice but to be aggressive in its fight, saying its immense network of resellers and partners can't make a living in areas flush with counterfeit software. He says consumers and businesses are being coaxed into buying counterfeit products that either don't work or do serious harm by clearing the way for various types of electronic fraud.

And, crucially, the counterfeit software cuts into Microsoft's potential profit. A software industry trade group estimated the value of unlicensed software for all companies at $51.4 billion last year.

The most vociferous critics of Microsoft and the overall proprietary software industry describe the anti-piracy crusade as a sophisticated dog-and-pony show. They say the software makers tolerate a certain level of piracy because they would rather have people use their products — even if counterfeit — than pick up lower-cost alternatives. At the same time, the critics say, the software companies conduct periodic raids to remind customers and partners that playing by the rules makes sense.

"It has always been in Microsoft's interests for software to be available at two different prices — expensive for the people that can afford it and inexpensive for those that can't," Mr. Moglen says. "At the end of the day, if you're a monopolist, you have to tolerate a large number of copies you don't get paid for just to keep everyone hooked."

Microsoft has demonstrated a rare ability to elicit the cooperation of law enforcement officials to go after software counterfeiters and to secure convictions — not only in India and Mexico, but also in China, Brazil, Colombia, Belize and Russia. Countries like Malaysia, Chile and Peru have set up intellectual-property protection squads that rely on Microsoft's training and expertise to deal with software cases.

As Mr. Moglen sees it, these efforts underscore a certain level of desperation on the part of American companies and the economy of ideas on which they have come to rely. "This is the postindustrial United States," he says. "We will make other governments around the world go around enforcing rights primarily held by Americans. This is a very important part of American thinking around how the country will make its living in the 21st century."

MICROSOFT'S pursuit of software counterfeiters begins in Dublin, at one of the company's 10 crime labs.

Donal Keating, a physicist who leads Microsoft's forensics work, has turned the lab into an anti-piracy playpen full of microscopes and other equipment used to analyze software disks. Flat-screen monitors show data about counterfeit sales, and evidence bags almost overflow with nearly flawless Windows and Office fakes. Mr. Keating serves as the CD manufacturing whiz on what amounts to Microsoft's version of the A-Team, clad in business-casual attire.

The undercover operative of this group is Peter Anaman, a lawyer who was born in Ghana and educated in England; he taught hand-to-hand combat to soldiers during a stint in the French army and then taught himself how to write software. Mr. Anaman has applied his software skills and training to explore a shift in piracy from groups that make CDs to those that offer downloads online.

Through three online personas — two female and one male — Mr. Anaman chats with and sometimes befriends hackers in Russia and Eastern Europe who use stolen credit card numbers to set up hundreds of Web sites and offer products from Microsoft, Adobe and Symantec. "It is part of gathering human intelligence and tracking relationships," Mr. Anaman says.

Through an artificial intelligence system, Microsoft scans the Web for suspicious, popular links and then sends takedown requests to Web service providers, providing evidence of questionable activity. "The Web sites look professional," he says. "And some of them even offer customer support through call centers in India."

The counterfeiters, however, have automated systems that replace links that Microsoft deep-sixes. So the company has turned up the dial on its link-removal machine.

"We used to remove 10,000 links a month," Mr. Anaman says. "Now, we're removing 800,000 links a month."

He describes the groups behind these sites as "part of the dark Web," saying they have links to huge spam, virus and fraud networks. Microsoft's tests of software on some popular sites have shown that 35 percent of the counterfeit software contained harmful code.

Anthony Delaney, who started at Microsoft 25 years ago — driving a forklift to move boxes of its products for shipment — has worked his way up to become its piracy data guru.

On one of the flat screens, Mr. Delaney brings up a world map that lets users zoom into a city just as they would if hunting for directions online. But instead of highlighting landmarks and popular stores, the map illuminates Microsoft's retail partners. Hover a mouse over a shop in San Francisco, for example, and you can see how much software it sells, how often Office is sold in tandem with Windows, the failure rate for authentication codes and how many cease-and-desist letters have gone to suspicious sellers in the area.

According to the map, the area within a 50-mile radius of New York City accounted for more than 200 "actions" last year, including 165 cease-and-desist warning letters to companies suspected of selling pirated software.

"We can see that only 5 percent of your sales have Office attached to Windows," Mr. Delaney says. "If that's below the average for the area, we may go have a chat or conduct a test purchase."

This rather eclectic bunch is joined by about 75 other people, including former agents of the I.R.S., F.B.I., Secret Service and Interpol, and former prosecutors — all of whom work under Mr. Finn.

A former assistant United States attorney in New York, Mr. Finn directs this squad from a Paris office. He says Microsoft spends “north of $10 million” a year on its intelligence-gathering operations and an estimated $200 million on developing anti-piracy technology.

Mr. Finn talks at length about Microsoft’s need to refine the industry’s equivalent of fingerprinting, DNA testing and ballistics through CD and download forensics that can prove a software fake came from a particular factory or person. And his eyes widen as he thinks about advancing this technology to the point that Microsoft can emphasize the piracy issue directly to customers.

“Imagine the day when a consumer finds a link that says, ‘Click here if you would like a forensic examination of your disk,’ ” Mr. Finn says. “You put the disk in, the computer reads it and suddenly you see a map of everywhere that counterfeit has been seen all over the world. If people see it in a graphic and visual way, I think they are more likely to help.”

THE software thieves monitored by Microsoft come in various shapes and sizes.

College students, grandmothers and others have been found selling cheap, copied versions of software like Windows, Office, Adobe’s Photoshop and Symantec’s security software on eBay and other shopping Web sites.

And people unwilling to pay for discounted software, meanwhile, can find free versions of popular products online that offer downloads to all manner of copyrighted material.

Microsoft’s investigators, however, spend much of their time examining how large-scale counterfeiters produce copies at factories and then distribute their wares around the globe.

The biggest counterfeit software bust in history occurred in July 2007 in southern China. The Public Security Bureau there and the F.B.I. found a warehouse where workers assembled disks, authentication materials and manuals and prepared them for shipping. All told, investigators found $2 billion worth of counterfeit Microsoft software, including 19 versions of products in 11 languages. Software produced by this syndicate turned up in 36 countries on six continents.

As one means of trying to tell the genuine article from a fake, Microsoft embeds about an inch of a special type of thread in each “certificate of authenticity” sticker found on boxes of software and computers. The investigators spotted dozens of spools of counterfeit thread — 81 miles worth — at the Chinese warehouse.

Microsoft has found that operations of this scale tend to include all the trappings of legitimate businesses. Workers spend years building up contacts at software resellers around the globe, offering them discounted versions of software. Then they take the orders and send them off via shipping services, Mr. Keating says.

Many Microsoft products make users enter an activation code to register the software and have it work properly. The syndicates trade in stolen versions of these codes as well, and sometimes set up their own online authentication systems to give people the feeling they have a legitimate product. Groups in Russia and Eastern Europe, with various cybercrime operations in play, now use money gained from credit card fraud schemes to buy activation codes.

About a decade ago, only a few companies had the expertise or the $10 million needed to buy machines that could press CDs and DVDs. Today, someone can spend about $100,000 to buy second-hand pressing gear, says Patrick Corbett, the managing director at a CD plant owned by Arvato Digital Services, which produces Microsoft's retail software in Europe.

"Just five years ago, there were five sites in China that supplied the whole country," Mr. Corbett says. "Now these machines are commonplace."

A prized object in the factory is the stamper, the master copy of a software product that takes great precision to produce. From a single stamper, Arvato can make tens of thousands of copies on large, rapid-fire presses.

Crucially for Mr. Keating, each press leaves distinct identifying markers on the disks. He spends much of his time running CDs through a glowing, briefcase-size machine — and needs about six minutes to scan a disk and find patterns. Then he compares those markings against a database he has built of CD pressing machines worldwide.

This system allows Microsoft to follow the spread of CDs from factories like the ones in China. The company conducts test purchases of software — online and in stores — and receives copies from some of the 300,000 people who have complained about running into counterfeits over the last four years.

Microsoft keeps tight controls over its partners that produce CDs. But counterfeiters get around these measures by stealing stampers and presses, presenting factories with fake paperwork from Microsoft or printing in a factory when it isn't doing official business — a practice known in the industry as producing "cabbage."

To make life harder for the counterfeiters, Microsoft plants messages in the security thread that goes into the authenticity stickers, plays tricks with lettering on its boxes and embosses a holographic film into a layer of lacquer on the CDs.

To the untrained eye, the counterfeit software in Microsoft's labs appears to be exact replicas, right down to the boxes. Chinese counterfeiters mimic the built-in hologram simply by placing a holographic sticker across the entire surface of a CD; then they use other machines to erase some of the unique identifiers found at microscopic levels.

Such tactics have pushed Microsoft to create a new type of digital fingerprinting technology that scans a disk's software code for special defects. The same techniques allow Microsoft to find malicious code that may have been injected in its products.

THE grand question surrounding Microsoft's anti-piracy razzle-dazzle is whether it's worth the cost.

The piracy problems tend to run highest in regions where there is less money to pay for Microsoft's products. Backers of free software like the Linux operating system take aim at these areas, and Microsoft also faces growing competition from Google, which gives away its Office rival to consumers and sells a business version at prices far below what Microsoft typically receives.

"We love Microsoft's heavy-handedness," says Jim Zemlin, the executive director of the Linux Foundation, a nonprofit organization. "We want 100 percent of the people using Windows to pay for it, because in those places where you have a lot of pirated use of Windows, we don't have any cost advantage."

Microsoft's critics portray its behavior as reactionary, saying the company is trying to protect old business models as new devices and services arrive.

"If people are going to steal something, we sure as hell want them to steal our stuff," says Michael Simon, the chief executive of LogMeIn, a company whose software is used in smartphones and tablets. "When you have a saturated market like Microsoft and have no growth in these devices, then it might be different."

The anti-piracy tactics employed by Microsoft rub many people in the software industry the wrong way as well.

The Business Software Alliance, which is financed in part by Microsoft and conducts audits and investigations on its behalf, spends about $50 million a year going after counterfeiters and offers rewards to people who report the use of pirated software in their companies. The alliance also finances the oft-cited annual study performed by the research firm IDC that comes up with a dollar amount tied to piracy losses.

Robert J. Scott, a lawyer at Scott & Scott in Dallas, contends like many others that the alliance's figure is too high and that the group draws imprecise conclusions about the purchases that people would have made if they weren't pirating software.

"I don't put much stock in those reports," says Mr. Scott, who advises businesses being audited by the alliance and other software companies.

The alliance defends its numbers, and Mr. Finn at Microsoft says the group's figures are accurate. He plays down the central accusation that Microsoft would face less of a piracy threat if it just lowered prices. "We have seen no connection between piracy rates and price," he says, citing the company's own pricing experiments. "I think it's a canard."

Meanwhile, Microsoft-sponsored raids and customer audits sometimes have a public relations fallout.

Two years ago in India, Microsoft hired Anup Kumar, a 10-year veteran of the Central Bureau of Investigation, in part to teach the company how to push software piracy cases through the local bureaucracy. When raids followed, many local software sellers chided the government in the local press, saying it bowed to Microsoft's will.

And, last month, Microsoft altered its policies in Russia after a spate of incidents in which local security services seized computers of advocacy groups and opposition newspapers, using the pursuit of stolen software as justification. Microsoft said it would provide a blanket software license for advocacy groups and media outlets, and offer legal aid to such groups caught up in software inquiries.

The protection of intellectual property has become a high-stakes political game where countries that do Microsoft's bidding expect some kind of return on their effort, according to Joseph Menn, author of "Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet."

"It's part of the geopolitical process," he said, "and Microsoft has a level of clout that a lot of other folks don't in Washington and in other countries."

Mr. Finn argues that Microsoft's anti-piracy efforts and training of law enforcement are a benefit to countries that want to build out their tech sectors and show they value intellectual property.

"Intellectual property is a critical engine of economic growth," Mr. Finn says. "That's not just for large companies, but also for small businesses and entire countries. We work with governments that are realizing this is in their best interests."

Miguel Helft contributed reporting.

More in Technology (2 of 29 articles)
Tag-Along Marketing

Read More »
Close