Social-media tools used to target corporate secrets

April 5 2011, By Byron Acohido

Not long after airstrikes began in Libya earlier this month, certain attorneys at four U.S. law firms, known for having high-profile clients in the oil industry, each received a personally addressed e-mail message.

Each message carried an Adobe PDF attachment, purportedly an analyst report describing the effect of Libya's uprising on oil futures. Each lawyer clicked on the attachment.

But the PDF was actually pre-set to deliver a quick-acting computer intrusion, says Chris Day, chief security architect at data security company Terremark, who watched the attack unfold. Within a few seconds, the PC of each attorney who clicked on the attachment began sending a silent beacon to a command server controlled by the intruders.

Terremark alerted law enforcement, and the law firms were notified, cutting off yet another persistent intrusion-a distinctive type of hack that has quietly become a staple of the cyberunderground.

"We're seeing criminal gangs using these tactics against commercial enterprises simply because they work so well," says Day.

Such so-called spear-phishing attacks, which often enlist social-media tools to meticulously wedge into corporate networks, are increasingly used in computer thefts that pinpoint valuable corporate data, according to a report released today by IBM's X-Force cybersecurity team.

"Cybercriminals have become more focused on quality of attacks, rather than quantity," says Tom Cross, X-Force threat intelligence manager.

Elite cybercriminals are tapping into search engines and social networks to help them target specific employees for social-engineering trickery at a wide range of companies, professional companies and government agencies.

They wait patiently for an opportune moment to seed an infection, knowing they need only infect one well-placed PC to gain a foothold inside a company network. They then proceed to stealthily probe deeper over many months.

"It's become very common for advanced groups to be in systems for a year or longer without being detected," says Kim Peretti, forensics director at PricewaterhouseCoopers.

The booty of choice: intellectual property.

Proprietary intellectual property is generally considered twice as valuable as day-to-day financial and customer data, according to Forrester Research. A thriving criminal market has evolved for converting stolen trade secrets into cash, say security experts and law enforcement officials. Demand is being driven by Asian companies looking to undercut Western rivals, and by scam artists seeking to game stocks and commodities markets. Persistent intrusions keep stolen company secrets flowing into this underground market.

Cybercriminals have "shifted their focus to trade secrets and product planning documents," says Simon Hunt, chief technology officer of McAfee's Endpoint Security division.

Yet, only a minority of persistent intrusions are being detected, and

fewer still are disclosed publicly, as companies are loath to announce that they've been breached. McAfee estimates that just three in 10 organizations report all data breaches.

Even so, a spate of high-visibility hacks that have recently come to light gives a glimpse at the scale and profitability of persistent intrusions.

Earlier this year, companies participating in Europe's carbon registries lost some $50 million to an Eastern European gang that infiltrated their trading systems. Nasdaq last month admitted that intruders roamed undetected for at least a year deep inside its cloud-based collaboration service, called Director's Desk, whose users are senior executives and board members of big public companies.

In a typical month, threat-detection company Mandiant is busy investigating some 30 to 40 persistent intrusions in organizations around the world. It's just one of several security companies that specialize in such investigations.

"There have been thousands of compromised organizations in the United States alone over the last five years," says Kevin Mandia, CEO of Mandiant. "In the last 18 months, we've responded to approximately 100 different organizations in North America and throughout the world who were hacked by criminals operating out of Asia."

Criminal gangs in China, Russia and Ukraine, in particular, appear to be in the vanguard of such attacks, Mandia says. They've quickly and astutely moved to take full advantage of the corporate sector's embrace of Internet-based technologies.

For instance, many attacks Mandiant has investigated began with the criminals doing reconnaissance on Google, Facebook, LinkedIn, Twitter and other popular Internet services to find companies to target-and

pinpoint specific executives, researchers, analysts, engineers or key administrative assistants to attack.

The next step is to craft a spear-phishing lure designed to entice a specific employee to click on a viral attachment or Web page link, using information gleaned during the reconnaissance phase to make the attachment or link seem trustworthy. In 2010, criminals increasingly used e-mail, instant messages and social-network posts to spear phish targeted employees, says IBM's Cross.

One enterprising gang recently put a twist into spear phishing by noticing that more than a few executives have a penchant for using Google Alert in connection with their names. Google's free service will email a Web link to the executive every time the search engine indexes a Web page containing a fresh news article mentioning the executive.

The intruders figured out how to inject an infection onto such Web pages at just the right moment, so the infection has a low chance of being detected and a high chance of appearing as part of a Google Alert arriving in the executive's in-box, says Mickey Boodaei, CEO of security company Trusteer. One way they do this is by putting up an infectious Web page that redirects to a legitimate Web page carrying a news article about the executive; the link between the bad and good sites is enabled just after Google indexing has occurred. "These targeted attacks are very powerful and should be taken very seriously," Boodaei says.

Once an initial infection takes hold, persistent intruders seek to gain wider and deeper access to an organization's network. This typically means pilfering a system administrator's user name and password to gain escalated privileges; there are myriad proven techniques for accomplishing this.

With escalated privileges, the intruders can map the layout of the

network and make note of key servers that control e-mail and store data. They also routinely disable antivirus protection and install "multiple backdoors with different configurations," setting up options for re-infecting the network should they be detected, says Mandia.

In one case, a company discovered 100 infected computers, took them off line, and hired Mandiant to confirm its network was clean. Investigators found the intruders used backdoors to freshly infect 20 workstations and servers. By quickly removing the 100 infected PCs, the company alerted the intruders, who changed tactics. "The problem with immediately removing compromised systems is that it typically alerts the attacker and lets them know an infected system has been identified," says Mandia.

Another pitfall for companies is not knowing what's been stolen. Borrowing techniques developed in the cyberespionage world, persistent intruders can easily hide their tracks.

Few details have been disclosed about the Nasdaq breach last month, other than that "suspicious files" were found lurking for an extended period on a server supporting Directors Desk. Think of Directors Desk as a no-nonsense social network for very privileged users. Nasdaq describes it as a "complete turn-key, fully-hosted online board (of directors) technology solution, with over 5,000 users representing more than 175 organizations worldwide, including many Fortune 500 companies."

Nasdaq quickly issued a statement saying "there is no evidence that any Directors Desk customer information was accessed or acquired by hackers."

Nicholas Percoco, who heads SpiderLabs at data security firm Trustwave, and Uri Rivner, head of new technologies, identity protection

and verification at RSA, security division of EMC, say it seems most plausible that whoever inserted the suspicious files used a classic persistent-intrusion attack.

"Whoever did this was definitely targeting the Holy Grail of insider information," Rivner says. "In the past year, we've seen more and more evidence of cybercriminals targeting specific individuals in private-sector corporations."

Percoco says the intruders were "probably going after very valuable, company-confidential information, such as financial results prior to their being announced, mergers and acquisitions under consideration, company plans, product roadmaps, IPOs, all those types of things that would be available to members of a board."

The quickest route to profits would be for the intruders to harvest insider information, then make trades to game the stock market. But it could take months or years for cyberforensics and market experts to ferret out evidence.

McAfee and Science Applications International recently surveyed 1,000 senior information technology professionals in the U.S., United Kingdom, Japan, China, India, Brazil and the Middle East. Roughly 25 percent of organizations participating reported they had a merger, acquisition or product roll-out "stopped or slowed by a data breach or the credible threat of a data breach." And 62% of respondents expressed concern that securing company secrets is going to get more problematic with the rising use of Internet-connected smartphones, tablet PCs and e-readers in workplaces .

"Criminals are attacking corporate intellectual capital, and they are often succeeding," says McAfee's Hunt.