An invitation to crime: How a friendly click can compromise a company

March 13 2010, By Byron Acohido

"Hey Alice, look at the pics I took of us last weekend at the picnic. Bob". That Facebook message, sent last fall between co-workers at a large U.S. financial firm, rang true enough. Alice had, in fact, attended a picnic with Bob, who mentioned the outing on his Facebook profile page.

So Alice clicked on the accompanying Web link, expecting to see Bob's photos. But the message had come from thieves who had hijacked Bob's Facebook account. And the link carried an infection. With a click of her mouse, Alice let the attackers usurp control of her Facebook account and company laptop. Later, they used Alice's company logon to slip deep inside the financial firm's network, where they roamed for weeks. They had managed to grab control of two servers, and were probing deeper, when they were detected.

Intrusions like this one -- investigated by network infrastructure provider Terremark -- can expose a company to theft of its most sensitive data. Such attacks illustrate a dramatic shift under way in the Internet underground. Cybercriminals are moving aggressively to take advantage of an unanticipated chink in corporate defenses: the use of social networks in workplace settings. They are taking tricks honed in the spamming world and adapting them to what's driving the growth of social networks: speed and openness of individuals communicating on the Internet.

"Social networks provide a rich repository of information cybercriminals

can use to refine their phishing attacks," says Chris Day, Terremark's chief security architect.

This shift is gathering steam, tech security analysts say. One sign: The volume of spam and phishing scams -- like the "LOL is this you?" viral messages sweeping through Twitter -- more than doubled in the fourth quarter of 2009 compared with the same period in 2008, according to IBM's X-Force security research team. Such "phishing" lures -- designed to trick you into clicking on an infectious Web link -- are flooding e-mail inboxes, as well as social-network messages and postings, at unprecedented levels.

An infected PC, referred to as a "bot," gets slotted into a network of thousands of other bots. These "botnets" then are directed to execute all forms of cybercrime, from petty scams to cyberespionage. Authorities in Spain recently announced the breakup of a massive botnet, called Mariposa, comprising more than 12 million infected PCs in 190 countries.

Three Spanish citizens with no prior criminal records were arrested. Panda Security, of Bilbao, Spain, helped track down the alleged ringleader, who authorities say has been spreading infected links for about a year, mainly via Microsoft's free MSN instant messenger service.

"It became too big and too noticeable," says Pedro Bustamante, senior researcher at Panda Security. "They would have been smarter to stay under the radar."

What happened to Bob and Alice, the picnickers at the financial firm, illustrates how social networks help facilitate targeted attacks. As a rule, tech-security firms investigate breaches under non-disclosure agreements. Honoring such a policy, Terremark used pseudonyms for

the affected employees in supplying USA Today with details of what happened at the financial institution.

Investigators increasingly find large botnets running inside corporate networks, where they can be particularly difficult to root out or disable. "Social networks represent a vehicle to distribute malicious programs in ways that are not easily blocked," says Tom Cross, IBM X-Force Manager.

The attacks run the gamut. In just four weeks earlier this year, one band of low-level cyberthieves, known in security circles as the Kneber gang, pilfered 68,000 account logons from 2,411 companies, including user names and passwords for 3,644 Facebook accounts. Active since late 2008, the Kneber gang has probably cracked into "a much higher number" of companies, says Tim Belcher, CTO of security firm NetWitness, which rooted out one of the gang's storage computers.

"Every network we see today has a significant problem with some form of organized threat," Belcher says. The Kneber gang "happened to focus on collecting as many network-access credentials as possible."

Stolen credentials flow into eBay-like hacking forums where a batch of 1,000 Facebook user name and password pairs, guaranteed valid, sells for $75 to $200, depending on the number of friends tied to the accounts, says Sean-Paul Correll, researcher at Panda Security. From each account, cyberscammers can scoop up e-mail addresses, contact lists, birth dates, hometowns, mothers' maiden names, photos and recent gossip -- all useful for targeting specific victims and turning his or her PC into an obedient bot, Correll says.

On the high end, the Koobface worm, initially set loose 19 months ago, continues to increase in sophistication as it spreads through Facebook, Twitter, MySpace and other social networks. At its peak last August,

more than 1 million Koobface-infected PCs inside North American companies were taking instructions from criminal controllers to carry out typical botnet criminal activities, says Gunter Ollmann, vice president of research at security firm Damballa.

In another measure of Koobface's ubiquity, Kaspersky Labs estimates that there are 500,000 Koobface-controlled PCs active on the Internet on an average day, 40 percent of which are in the U.S., 15 percent in Germany and the rest scattered through 31 other nations. "The personal information employees post day-by-day on Facebook is turning out to be a real gold mine," says Stefan Tanase, a Kaspersky Lab senior researcher.

Facebook, the dominant social network, with 400 million members and therefore the biggest target, says recent partnerships with Microsoft and security firm McAfee to filter malicious programs help keep compromised accounts to a small percentage. "We are constantly working to improve complex systems that quickly detect and block suspicious activity, delete malicious links, and help people restore access to their accounts," says spokesman Simon Axten.

Still, social networks have grown popular because they foster open communication among friends and acquaintances, which plays into the bad guys' hands, says Eva Chen, CEO of anti-virus firm Trend Micro.

"These new communication platforms are where people go, so that's where the hackers are going," Chen says.

Meanwhile, discussions about restricting workplace use of social networks and training employees to be more circumspect are just beginning to percolate at venues like the big tech security trade show held the first week of March in San Francisco sponsored by RSA, the security division of EMC. "Most larger businesses simply ask employees

to watch their time spent on social-networking sites," says Ollmann.

Each infected PC in a corporate network represents a potential path to valuable intellectual property, such as customer lists, patents or strategic documents. That's what the attackers who breached Google and 30 other tech, media, defense and financial companies in January were after. Those attacks -- referred to in security circles as Operation Aurora -- very likely were initiated by faked friendly messages sent to specific senior employees at the targeted companies, says George Kurtz, McAfee's chief technology officer.

The attack on the picnicking co-workers at the financial firm illustrates how targeted attacks work. Last fall, attackers somehow got access to Bob's Facebook account, logged into it, grabbed his contact list of 50 to 60 friends and began manually reviewing messages and postings on his profile page. Noting discussions about a recent picnic, the attackers next sent individual messages, purporting to carry a link to picnic photos, to about a dozen of Bob's closest Facebook friends, including Alice. The link in each message led to a malicious executable file, a small computer program.

Upon clicking on the bad file, Alice unknowingly downloaded a rudimentary keystroke logger, a program designed to save everything she typed at her keyboard and, once an hour, send a text file of her keystrokes to a free Gmail account controlled by the attacker. The keystroke logger was of a type that is widely available for free on the Internet.

The attackers reviewed the hourly keystroke reports from Alice's laptop and took note when she logged into a virtual private network account to access her company's network. With her username and password, the attackers logged on to the financial firm's network and roamed around it for two weeks.

First they ran a program, called a port scan, to map out key network connection points. Next they systematically scanned all of the company's computer servers looking for any that were not current on Windows security patches. Companies often leave servers unpatched, relying on perimeter firewalls to keep intruders at bay. The attackers eventually found a vulnerable server, and breached it, gaining a foothold to go deeper.

A short time later, the attackers were discovered and cut off. One of Bob's Facebook friends mentioned to Bob that the picnic photos he had sent had failed to render. That raised suspicions. A technician took a closer look at daily logs of data traffic on the company's network and spotted the vulnerability scans.

Terremark's Day says two or three collaborators, each with different skill sets, most likely worked together to pull off the attack. "They were noisy about how they went about this," says Day. "Had they been quieter they would've gotten much further."