BUSINESS: THE 8TH LAYER

HACKING SOCIAL NETWORKS

By Lynn Greiner

The more users trust the community the more they risk having their trust compromised.

If you're a gregarious creature, chances are you indulge that tendency on one or more social networking websites. Whether it's Facebook, MySpace, Xing, Orkut, Friendster, LinkedIn, or even Twitter, such services provide the answer to a fundamental human need: belonging.

However, these online communities are composed of the same mix of interests as their physical counterparts. There are village idiots and smart alecks, jerks and nice people, good guys and, alas, bad guys.

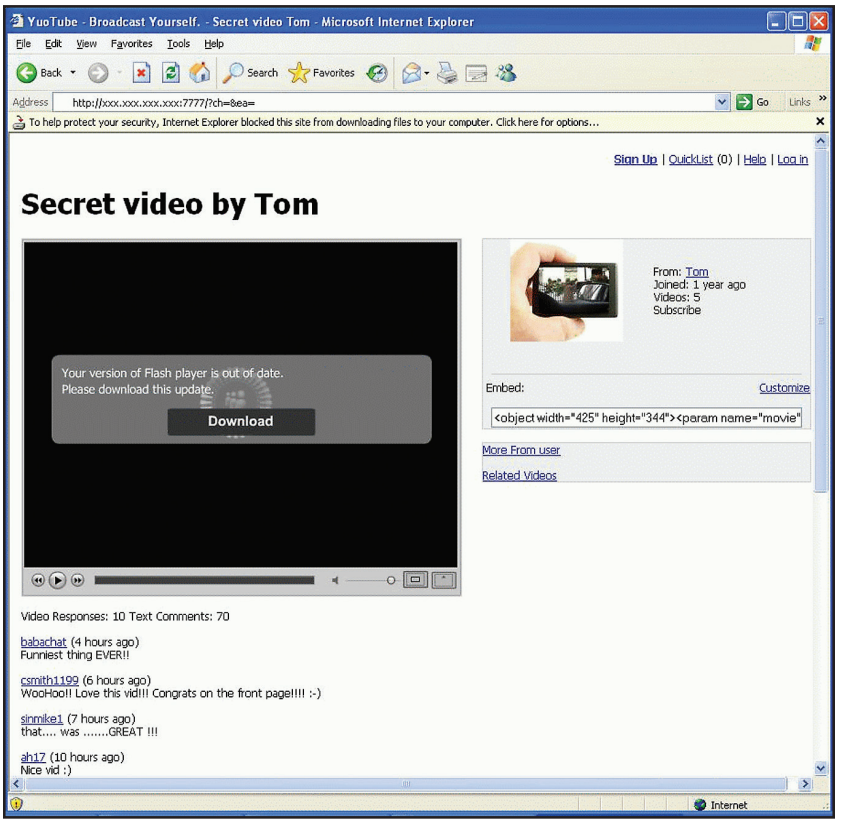
According to researchers at Moscow-based anti-malware vendor Kaspersky Lab, the bad guys are having a field day dreaming up nefarious and lucrative ways to exploit the trust people have in their online networks. Senior malware analyst and social network specialist Sergey Golovanov says he's been seeing increased buzz on hacker forums, with bad guys sharing ways to compromise social-networking sites.

Last January, CNN reported, Facebook user Bryan Rutberg's status update suddenly became a plea for assistance, and one of his online friends received a direct message saying that Rutberg was visiting the U.K., had been robbed, and needed funds to get home. That friend wired $1,143 to Rutberg's London address, to help his buddy.

There's one thing wrong with this heartwarming picture of friend helping friend; the whole time, Rutberg was sitting safely at home in Seattle, unaware of the goings-on. His Facebook account had been hacked, and the $1,143 is now in the pockets of person or persons unknown.

Hacking social network user accounts can be disturbingly easy, Golovanov says, because of our innate tendency to trust our friends. If someone you know posts a message on your Facebook wall, telling you that embarrassing pictures of you are posted at a particular location, you're apt to click the link to find out how embarrassing the photos really are (and possibly figure out how to get even with the person who posted them).

Malware authors take advantage of that trust to compromise accounts. Consider, for example, the malware called Koobface. Infesting both Facebook and MySpace in recent months, it



The Koobface virus prompts users to update Flash with a (bogus) file.

masquerades as a message from a friend and directs victims to a supposedly funny video. That link pops up an alert that a Flash Player update is required for viewing while kindly pointing you to the necessary file.

That file is not, however, a Flash update but a Trojan that promptly installs a proxy and a backdoor, preparing the victim's machine for future mischief. Oh, and it also takes advantage of the user's logged-on state to blast out its phony message to all of his or her contacts, starting yet another infection cycle.

Members of a 20 million strong Russian social network similar to Facebook, Vkontakte.ru, were hit last October with a scam that combines several media. According to Golovanov's colleague Denis Maslennikov, who monitors mobile malware, members receive a message, again supposedly from a friend, saying they can get a credit to their mobile-phone account by installing an application. The link they click installs a program that actually sends an SMS message to a premium number, netting the crook the usage fee. Multiply even a few dollars per victim by a user base of that size, and you're talking big money.

Compromised accounts are bought and sold online, much like stolen credit card numbers (they can be purchased by the hundred, if you know where to look), providing cyber-crooks an unending supply of potential nodes for their botnets, along with victims for their scams. In fact, if you want to acquire a particular "friend," such access can be had too, for a price.

Social networks have to pay their bills like everyone else, so enterprising malware purveyors have yet another venue for profit—advertising. No, they don't buy ads. What they do buy are tools that let them hack legitimate banner ads based on Adobe Flash, enabling them to install malware when clicked.

Other hacks aren't so high-tech but can be equally destructive. Social engineering on social networking sites need not involve malware—only trusting victims and people who, for whatever reason, want to take advantage of them.

Take, for example, the story (again from CNN) of the 18-year-old Wisconsin student who created a female persona on Facebook to persuade his teenage classmates to send "her" pictures of themselves in the nude. He then allegedly used the photos to blackmail the young men into performing sex acts with him. The only malware involved here was inside the perpetrator's head; he has since been arrested and faces a dozen charges ranging from possession of child pornography to sexual assault of a child under 16.

He's not the first, nor will he be the last, to pretend to be someone else online for some sort of profit. MySpace has reportedly found and removed 90,000 known sex offend-

ers from its rolls over the past couple of years.

Perhaps sadder was the case of the Missouri mother who pretended to be a 16-year-old boy on MySpace to, she later claimed, discover what a former friend was saying about her teenage daughter. Again, no tech was involved, aside from the social network itself. The victim, a 13-year-old girl struggling with depression and self-esteem problems, was completely taken in by this apparently nice "guy" and his interest in her, and when the "boy" dumped her and then posted insulting, publicly viewable comments about her, she hanged herself in her bedroom and died the next day.

Parents with more responsible motives are actually the fastest-growing demographic on Facebook. Whether they want to keep an eye on their offspring or simply catch up with their own old friends, enough members in the over-35 set have become social networkers that Stanford University is offering a four-part lecture series called "Facebook for Parents." It teaches the basics, as well as ways for parents to protect their kids.

There may be times, however, when you really do want to hack a social network, so to speak. I use "hack" in a very broad sense here, but sometimes you need to influence how, and how often, you show up in searches. LinkedIn, a predominantly business-oriented social network, actually scores your profile and advises you on ways to improve your chances of being found when you want to be.

Post a photo, it says. Complete your profile. Get people to recommend you. And recommend other people to create cross-links between profiles.

For those with a nefarious goal, the more information about yourself you post online, the more attractive you are. Young people often, sometimes inadvertently, give away their location, the name of their school, and enough other information to put themselves at risk from predators. Adults who should know better post enough information about upcoming vacations that it makes burglars drool and sharpen their crowbars. And all age groups forget that not just pals will see those naughty pictures from last week's party; the boss (or a potential boss) might be online too.

Yet there's something about social networking that's liberating to many; that's what makes it so hackable. Average folks wouldn't think of dancing naked down Main Street, but that's effectively what they do online, posting their deepest thoughts and fears (not to mention that funny but compromising cellphone photo), while trusting their friends to do them no evil. It's what being part of a community is all about.

Which makes hackers very happy, and sometimes very rich.

COMPROMISED ACCOUNTS ARE ACTUALLY BOUGHT AND SOLD ONLINE, MUCH LIKE STOLEN CREDIT CARD NUMBERS (YOU CAN PURCHASE THEM BY THE HUNDRED, IF YOU KNOW WHERE TO LOOK), PROVIDING CYBER-CROOKS WITH AN UNENDING SUPPLY OF POTENTIAL NODES FOR THEIR BOTNETS, ALONG WITH VICTIMS FOR THEIR SCAMS.

Lynn Greiner (lynng@ca.inter.net) analyzes the business of technology from Toronto.

DOI: 10.1145/1516035.1516038