Gaining awareness to prevent social engineering techniques, attacks

by: Marcia Savage
Editor

Cybercriminals are using social engineering fueled by social media to attack users and break into companies.
On the surface, the email looked completely legitimate. It appeared to come from an employee within the U.S.-based Fortune 500 manufacturing firm and talked about a corporate initiative the CEO was pushing. Four high-level executives received the email; one clicked on a link embedded in the message. That was all the attackers needed. The unwitting click unleashed malware that infected the executive’s computer and gave them a foothold into the company’s network, where they sniffed for passwords and gained access to multiple systems.

Until the FBI notified it, the manufacturing firm -- which was negotiating to acquire a Chinese company -- had no idea the intruders were stealing data on a weekly basis. The stolen data was highly sensitive – critical emails with details of the negotiations. In the end, the company
scuttled its acquisition plans, says Frank Nagle, senior consultant at MANDIANT, an Alexandria, Va.-based information security firm that investigated the case.

The attack, which happened two years ago, is a stark example of the kind of social engineering techniques being used against companies today. Gone are days of the mass emails with misspelled messages. Criminals today are doing more reconnaissance than ever before – aided by social networks and all the personal information loaded onto them -- to craft targeted emails or instant messages that trick people into opening malware-rigged attachments or divulging passwords and sensitive information. Social engineering is a common technique used in advanced persistent threat activity – like the intrusion into the manufacturing firm -- raising the stakes as coordinated, state-sponsored groups infiltrate U.S. companies, hunting for corporate secrets.

Defending against today's social engineering attacks is difficult but not impossible, security experts say. It requires focusing on the human element of the equation with better security awareness training that gets employees to think twice about clicking on certain emails. Let's look at some of the social engineering ploys used against enterprises today, what's helping to fuel them, and strategies that can help a company fend off these attacks and protect its valuable data.

**SOCIAL NETWORKS: SOCIAL ENGINEERING GOLDMINE**

Social engineering is nothing new in the digital age, of course, but security experts say criminals are
using it more as companies have gotten better at securing their networks.

“Before it would have been easier to take advantage of unpatched systems,” says Mike Murr, a certified SANS instructor and author of the upcoming *Human Compromise: The Art of Social Engineering*. “Now it’s often easier for the attacker to get code running on a remote system by persuading a user using social engineering to click on a link, execute code, or enter their password.”

“We’re getting better at locking down the digital assets. We’re not perfect, but it’s to the point now where the attacker is getting more ROI on the user vector than some of the digital vectors,” he adds.

A common mistake enterprise security managers make is focusing on infrastructure and system defenses instead of people, says Shawn Moyer, managing principal research consultant with Accuvant LABS R&D team. “A lot of defenders still think in terms of an attacker on the Internet externally trying to find a way in. ...The reality is, if I’m the outside threat, I find an insider and that insider becomes your threat,” he says.

Targeting the insider has never been easier, thanks to the rise of social media like Facebook, LinkedIn, and Twitter, security experts say. Outsiders researching a company can search the sites to find out who works there, who the top executives are, what they’re talking about, and contact information: all data that can be used to personalize an attack, making it more effective.

“Information is much easier to mine,” says Moyer, who conducts penetration tests for clients. “I can find out who the IT security manager is much easier in 2011 than in 1991.”

Chris Nickerson, founder and principal consultant at Denver-based Lares Consulting, which provides
pen testing and other security services, says his tests for customers will use their Twitter or Facebook accounts to collect information and successfully social engineer employees. “These are corporate-sanctioned accounts. They’re huge attack vectors,” he says.

**Rules of engagement**

With social media helping to fuel social engineering attacks, companies can protect themselves by backing up their security educational efforts with policies for social media use, advises Frank Nagle, senior consultant at information security firm MANDIANT.

More and more companies are realizing it’s important to have rules for acceptable use of social networks, not only as protection from social engineering scams but also to protect their corporate reputation and image, he says.

“They can’t stop their employees from using social networks, but they can encourage them to use social networks in a responsible way that reflects on the company,” he says.

He cites the IBM Social Computing Guidelines as an example of a corporate acceptable use policy extended to social media. They include protecting personal privacy, not disclosing IBM confidential data, and respecting copyright laws.

People generally have become aware of broad-based social engineering attacks like spam or 419 scams, so attackers have turned to social networks to create more targeted emails, says MANDIANT’S Nagle, who is also a PhD candidate at Harvard. They’ll also send messages on the social networks themselves to exploit the trusted environment they provide. “Attackers started tailoring
these messages so they’re no longer poorly spelled and generic,” he says.

In the case of APT, attackers are particularly adept at such reconnaissance to craft targeted attacks, Nagle says: “They do their homework better.”

For example, someone wanting to break into a defense contractor could first identify five to 20 employees to target, then research those people, says Lance Spitzner, director of SANS Securing the Human Program. From publicly available information on the Internet, they could find out that those employees recently attended a conference and create a spear phishing email that pretends to be a follow-up from the conference.

“By customizing the email, two things happen: They’re far more likely to click on it and by having a small number [of targets] it’s more likely to slip through. It goes under the radar of the antivirus companies because they don’t have signatures [for it],” he says.

**ATTACKS ON CORPORATE DATA**

Social engineering played a role in this year’s attack on RSA, the security division of EMC. The APT began with two different spear phishing emails with the subject line “2011 Recruitment Plan” sent to two small groups of employees, according to Uri Rivner, head of new technologies, identity protection and verification at RSA. “The first thing actors like those behind the APT do is seek publicly available information about specific employees – social media sites are always a favorite,” Rivner wrote in a blog post. One employee clicked on the spreadsheet attached to the email, which contained a zero-
day exploit; attackers then were able to infiltrate RSA and steal information related to its SecurID products.

Social engineering also factored into two other high-profile breaches over the past 18 months: The attack by the “Anonymous” group on security firm HBGary Federal earlier this year, and the attack on Google, which the company disclosed in January 2010. In February, HBGary founder Greg Hoglund told investigative reporter Brian Krebs that the attackers tricked a network administrator into giving up access to Rootkit.org, a research website maintained by Hogland; from there, they gained access to systems containing sensitive emails and other data.

The attack on Google’s intellectual property, which put APT into the popular lexicon of the security
industry, started with reconnaissance that targeted specific Google employees. As described by Heather Adkins, information security manager at Google, during a presentation at the Forum of Incident Response and Security Teams (FIRST) Conference 2010 last year, the attackers gathered information posted by the employees on social networks like Facebook and LinkedIn, set up a Web server hosting a phony photo website, then sent emails containing links that appeared to come from people the employees trusted. Clicking on the links sent them to the website, which downloaded malware and ultimately gave the criminals an opening to infiltrate Google servers.

“Spear phishing in and of itself is not a particularly sophisticated form of attack, but its exploitation of a person’s trusted relationships can make it quite effective,” Adkins says in an email this year. “Relatively simple spear phishing can also be a gatekeeper to more complex operations like APT and others.”

APT attackers usually rely on targeted email and instant messages to trick employees into downloading a malicious link or attachment, Nagle says. Another common tactic in APT is to hack into one person’s account and use that person’s contacts to send an email or instant message and try to break into another company. That tactic “drastically increases the chances that the second victim will click on the infected PDF file or whatever it is they send,” he says.

In one MANDIANT investigation, APT attackers who had infiltrated a company looked through its emails and intercepted an exchange with someone who worked at another company in the same industry. The attackers then added a malicious payload to a document that was included in that email exchange.

“The second company clicked on it because it was coming from someone they already talked to, it was
related to a subject they already talked about, and it was a version of a document they already opened,” Nagle says. “That’s not uncommon... If the APT is interested in that industry, once they’ve compromised one company in that industry, they’ll use that as leverage to go after other companies in that industry.”

He’s also seen cases in which attackers will intercept IMs to break into other companies or other parts of an enterprise. “They’ll use contacts on MSN Messenger, then jump into a conversation that people are having” and add a malicious link, he says.

**SECURITY AWARENESS**

Security experts acknowledge that targeted social engineering attacks can be tricky for companies to combat. Keepings systems patched and updated is critical, of course, but technology only goes so far, making effective employee security awareness training essential, they say.

“Employees in these social engineering attacks are really on the front lines,” Nagle says. “When email is really targeted, it’s tough to come up with technical means so you need to rely on employees to be educated and on alert for those types of things.”

It’s important to train users to trust their instincts on any email that seems at all suspicious, experts say. “Organizations would do well to caution employees to be wary of unexpected messages or unsolicited links, even if they appear to come from friends or co-workers,” Google’s Adkins says. “A quick phone confirmation in suspicious cases is a much better option than becoming a victim of spear
Lares Consulting’s Nickerson says there are usually always signs that expose an email as a phishing attack. For example, phishers don’t understand tonality; it’s usually easy to tell if someone you know wrote an email from the tone. Users can also mouse over a link to identify it; if it looks suspicious, don’t click on it, he says.

“Pay attention to the details, like the email address it’s coming from, the links you’re being sent to, and the tone of the email,” Nickerson says.

**Social engineering demo**

A social engineering contest at last year’s DefCon18 targeted 17 companies, including Walmart, McAfee, Cisco, and Apple, and all failed. Contestants were each assigned to one target and managed to get a piece of information using social engineering.

That shows that enterprise security awareness programs aren’t working, says Chris Hadnagy, lead developer of Social-Engineer.org, which hosted the Social Engineering Capture the Flag event. Companies should pay heed to the report produced after the CTF – and the report from this year’s upcoming contest – to improve their programs, he says.

Last year’s final report was downloaded more than 300,000 times, and prompted requests from companies on how to use it. “We worked with companies to improve their security awareness programs,” Hadnagy says. “We accomplished our goal, which was to raise awareness of the threat social engineering poses to corporate America and to provide something that companies can use as a tool for improving their awareness programs.”

In the CTF event, contestants have two weeks to collect information and build a profile of the target company. At DefCon, they’re given 25 minutes to call their target and collect as many “flags” as possible: information
such as VPN software, type of browser, employee schedules, and food supplier. No directly sensitive information such as passwords, IP address, Social Security numbers or credit card numbers is targeted.

This year’s contest at DefCon19 in August in Las Vegas will have 15 targets, including two “premier targets,” which Hadnagy says are companies that have agreed to work with SocialEngineer.org and be used as social engineering targets. Contestants this year will be given an actual professional audit report they can mimic in their information gathering. Also, a new target ranking system will be introduced; organizers won’t list the data extracted from the targeted companies but will rank how they fared overall, Hadnagy says.

Part of the problem is that companies have fallen short when it comes to security awareness training, which often ends up being a cursory exercise for compliance purposes, says Spitzner. “We’ve done tremendous work to secure computers but nothing to secure the human operating system. That’s why these social engineering techniques are so prevalent,” he says. “To change human behavior, you need to educate and train employees, not just once a year but continuously. Like you continually patch computers and applications, you’re continually training and patching human operating systems.”

Employees who are trained to be security aware are more likely to realize if they’re victimized by a spear phishing email and quickly call the security team, Spitzner says. That speeds response, which is particularly critical with APT, he adds.

Chris Hadnagy, aka loganWHC and operations manager for Offensive Security, says companies need to create a program that makes security awareness personal for employees with hands on training that demonstrates how easy it is to profile them online or how easy it is to crack their password.

“I’ve heard employees say, ‘What do I care, it’s not my data.’ Now, security awareness has become
personal for them. It’s not just about protecting their employer’s data but their life,” says Hadnagy, who also is lead developer of Social-Engineer.org and author of *Social Engineering: The Art of Human Hacking*.

Dave Marcus, director of security research and communications at McAfee Labs, agrees: “If you show them how easy it is to mine their own data, they’ll get it.”

Pen testing is another step companies can take to help protect their employees and their data against social engineering attacks, experts say.

“Red team penetration testing is important. Not just getting a vulnerability scan to pass an audit, but engaging in open scope attack simulation,” Moyer says, acknowledging his bias on this front. Generic network pen tests have specific methodologies and are designed as one-size-fits all, he says. “Real hacking is a creative exercise. Whenever you have a rigid set of rules of engagement, it doesn’t leave the door open for creativity. Not that a red team will find every single path into an environment, but it will find paths that your standard methodology did not.”

---

**PEN TESTING TECHNIQUES**

One social engineering tactic that pen testers are using with a lot of success to break into companies is what Nickerson calls “polo shirt attacks.” Testers will use intelligence gathered about the client and impersonate a representative from a cleaning crew, auditing firm or other service organization by wearing a polo shirt with a logo. The shirts are easy to have made, Hadnagy says.
“I can show up at your building, say I’m from such-and-such waste management. I heard one of your
Dumpsters is damaged and I need to go on site,” he says. “Who is going to stop the dude with the
clipboard and shirt with the logo? You find the Dumpster, pull out papers and discs and load the car.”

Nickerson says he’s seen a number of companies experience asset losses, theft and even corporate
espionage when criminals have used this kind of impersonation scheme. “Impersonation happens at all
levels, and in my opinion, is responsible for a great deal of loss in many businesses, he says. Clients are
beginning to strengthen their defenses by checking for identification of service providers, having
processes for calling the normal service representative to see who was sent for the job, and not
accepting unscheduled visits, he says.

When he’s on a red team case, Moyer starts out with the domain name and domain name registration
of the company to collect information about a company. Other tools include the American Registry for
Internet Numbers (ARIN), the company’s website (especially the “About Us” page), and Web forums.
The most valuable piece of information he digs up is the company’s email naming convention. From
there, he constructs a scenario specific to the company.

For example, in a case involving a retail company, he found employees chatting on a Web forum. One
worker mentioned that the company didn’t offer an employee discount. Moyer created a fake
employee discount program by registering a separate domain name. Then he sent emails to about 20
employees telling them they were enrolled in private early testing of the discount program and asked
them to forward the message to five co-workers they’d like to participate. “Once I have that first click,
I can pivot into the environment from that victim’s machine,” he says.

“I got an understanding of the employees and tailored a scenario specific to them,” Moyer adds. “Most
companies aren't thinking of an attacker specifically targeting them.”

Hadnagy describes another case in which his team gathered data from social media sites and Internet forums to create a successful spear phishing email. The client company had just upgraded its firewall and IDS systems; three IT workers discussed a problem they were having with the firewall configuration on sites like LinkedIn and Twitter. “Now, I'm the secretary to the CIO, here’s a PDF that’s a solution to that. Personal phishing attacks are very successful with the use of social media,” Hadnagy says. “It makes your whole story line credible because you know something personal about them.”

**LESSONS LEARNED**

After cases involving APT and a social engineering attack, MANDIANT often sees companies step up their awareness efforts, Nagle says. They won’t divulge the details of the attack to employees, but they’ll caution them to be on alert for suspicious emails. In the case of the manufacturing firm, remediation included boosting the company’s ability to monitor its internal network, something Nagle says many businesses neglect.

He’s seen heightened awareness really pay off, with employees spotting suspicious emails and forwarding them to IT, which sends them to MANDIANT for analysis. “We’ll confirm it’s malicious. That to me is great because it’s education working,” he says.

Marcia Savage is editor of Information Security. Send comments on this article to
Dig deeper on Security Awareness Training and Internal Threats

- Applying insider threat detection during the hiring process
- Pretexting: How to avoid social engineering scams
- Mitigate malicious apps with mobile device security training
- Risk versus hype: What is the real impact of insider security threats?
0 comments

Share your comment

Register or Login

E-Mail

email@techtarget.com

Username / Password

Username
Network Penetration Test
pwnieexpress.com
Bolster Your Security While Meeting Compliance Requirements.

CSA to closely monitor enterprise cloud data privacy issues in 2015
The Cloud Security Alliance says cloud data privacy has emerged as a top issue for industry amid Microsoft’s battle with the U.S....

**An introduction to Docker and its effect on enterprise cloud security**

Docker provides improvements for application virtualization, but what does it mean for security? Expert Ed Moyle offers an intro ...