Striker Pierce Summary of Social Hacking Investigation

The Tale of Two Insiders: Social Hacking to Get Corporate Secrets

WASHINGTON, DC, USA, January 26, 2015 /EINPresswire.com/ -- Striker Pierce Summary of Social Hacking Case: Published in Frontline Security Magazine

"A Tale of Two Insiders:
How current and former employees can unwittingly fall prey to aggressive CI agents"

by Brian O'Shea
© FrontLine Security 2014 (Vol 9 No 3)

Larry and his company were the victims of aggressive competitive intelligence collection utilizing social engineering (including social hacking and escalated recruitment). He needed to identify the leaks and any third parties involved, and prevent further loss of proprietary intelligence.

> Social Hacking is the oldest method of intelligence collection in the world, and remains the most effective
> *Brian O'Shea, CEO, Striker Pierce*

The Investigation
After a deep investigation and an aggressive "social hacking" penetration test, it was revealed that two employees had been responsible for leaking competitive intelligence to Larry's most aggressive competitor. One employee had left the firm a year ago, the other still worked for the company. Here is what the investigation revealed.

The Former Employee:
Employee #1, who we will refer to as "Mike," had left the company roughly a year before. He had been offered a more lucrative offer from a start up in New York and could not resist the opportunity. As it turned out, the startup company soon began having financial and product problems. Mike's salary was cut twice, and now that he lived in Manhattan, he realized his expenses were swallowing his income, and his bills were mounting. He updated his professional social media profile and advertised "Small Business Consulting" as an attempt to bring in more income. One day, he received a phone call from an "investment firm" seeking his expertise in the industry he had just left. He would be paid an hourly rate in the high three-figures and all consultations were over the phone. "Why not," Mike thought, and began having weekly paid phone calls with the "investment firm" immediately. He never questioned it… they never asked specifically about Larry's company and certainly never asked for detailed company data. They simply wanted to know about the industry and (generally) how companies in that industry dealt with the challenges of pricing, development, and go-to-market issues.

Mike received his first cheque and was hooked. After the first few weeks, he was providing flow charts and outlines for strategies. Mike felt fine with this, he told our interviewers, and insisted he had never revealed anything specific about Larry's company. He truly had no idea just how much damage he had caused.

The Current Employee:
Employee 2, who we will refer to as "Linda," had been with Larry's company for many years and was considered a "Superstar" by management and colleagues alike. She had no plans to leave, and she wanted to eventually be offered an equity partnership. Larry had personally served as her mentor and had adjusted her position to put her on the partner track. However, it was revealed that the more of a "Superstar" Linda became, the more she reflected this in social circles, in her professional social media profile, and on her resumé, which she updated every time she finished a project. Linda had been giving the competitors information for months without even realizing it.
The two employees, one current and one former, had been aggressively and successfully targeted by a third party firm that had been hired by Larry's competitors to collect primary data about Larry's company and certain product lines.

First, they had targeted Mike for recruitment to serve as an unwitting source to reveal internal processes and methodologies. Then they targeted Linda to confirm Mike's information and to collect timely updates on projects, programs, key personnel, and internal company organization management.

Methodology
Corporate Espionage is almost impossible to detect in cases like this, but not impossible to prevent. There are currently hundreds of companies across the U.S. and internationally that specialize in this type of collection – and falls into the "grey area" in terms of legality. They are not hacking networks, nor are they paying current employees for information. They are simply using social engineering and deception for collection purposes. Ironically, this is the oldest method of intelligence collection in the world, and remains the most effective.

Prevention
How do you stop them? Here are a few recommended steps to lessen the likelihood of losing important intelligence to outside collectors.

Quarterly social hacking penetration testing. This is the best way to detect leaks prior to them causing too much damage. Firms who offer this service will essentially mimic the behaviors of competitive intelligence firms of this nature in order to provide early detection of intelligence leaks. Any employee discovered to be inadvertently revealing company data can be evaluated and counselled accordingly.

Pre-Publication review of all resumes and social media. Ensure your employees have their professional profiles and resumes reviewed by either a third party counter-intelligence provider or counter-intelligence trained HR personnel prior to public release. This will help you manage what your current employees and even formers are revealing online about your company.

Monitor. All computer, phone, and printer use should be monitored and recorded. Additionally, this data should be reviewed regularly by your counter-intelligence provider for detection of questionable activity.

Training. Having great company morale and excellent corporate communications is just the first step. Have your company receive quarterly counter-intelligence training in a fun and entertaining way that can double as Team building.

Invest where it counts
Larry did everything right, but not everything he could have. Your employees and former employees are the two best sources of intelligence. It is important to invest the resources to protect them as much as it is important to protect your cyber-based data. The Two Insiders of this story, though unwitting, could have destroyed Larry's business and would have never even known they were responsible.

Remember, your best assets could be your competitors' best sources.

Brian O'Shea
Striker Pierce LLC
571-451-4833
email us here
