Title: The Innocent Hill Walker

Les Ball and Natalie Coull

The observer

"So, I see that you like hillwalking? That is very interesting to me and you will be hearing from me soon". This is the opportunist thinking of the hacker and a starting point to the design and building of a creative attack on your personal data and identity. So how willing are you to share your private life with others, even though the disclosure might only be your seemingly innocent hobbies? Well beware, it may well be enough to catch you unaware.

The observed

The ubiquity of social media presents opportunities to express our private lives and who should gain access to them, as for example on Facebook. However, in our professional careers we are also under pressure to sell ourselves to raise corporate profiles. Some academics, for example, take great delight in expressing their interests online to enhance and personalise their university profile. Some companies and institutes also have lists of their employers' names and e-mails for ease of access. The competent cyber criminal will explore sites with such disclosures of data with the intent of exploiting them to form what is known in the trade as a spear phishing attack. The process is known as social engineering, or "the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in, or using technical hacking techniques (CSO Magazine, 2012)". In reality, social engineering feeds on the lethargy of the user regarding security and the aggression of the malicious hacker (Abraham and Chengalur-Smith, 2010).

The plot

The vulnerabilities of online users have been exposed by a team at the University of Abertay Dundee in a simulated attack on publicly available company data. Our purpose was to demonstrate how a malicious attacker, coupled with the appropriate use of software tools can harness and integrate theses open source data into the social engineering process to bring about a successful cyber-attack. Software tools were used to effectively search the company's website and to craft a weapon of attack. Maltego was used for data gathering and "drill down" searching, while the Simple Phishing Toolkit was used to construct an e-mail attack, which is essentially the confidence trick of the operational plot.

The hunt

Our simulated "hunt" is not yet fully automated and interoperable but could be in the future. It begins by extracting company date from the staff members who express various degrees of personal and work-related information. This vetted list is then input to Maltego, which can search for information related to the data in the list. It could for example produce alternative e-mails or other entities associated with any particular member of staff. More insightful is that the tool can produce a visualisation of interrelationships between all extracted entities. It is here that common interests amongst the staff members can be found. Hillwalking was the most popular pastime expressed online. A perfect place to catch prey!

The weapon
"Congratulations, you have won a prize, please click on the link below". Many of us are familiar with this type of e-mail landing in our inbox and delete it without a second thought. We have become savvy to this kind of junk-mail or attempted phishing attack. Now, however, the weapon of attack is the spear phish, which has a much more subtle and sharper point. The spear phish is intelligent and can design and construct an e-mail that will target you, psychologically court you and dupe you. It knows you like hill walking and will "scrape" details from websites related to your interest to increase its own credibility as a fellow hill-walker perhaps. "Hi, I'm Mark Smith, editor of the new "Walking Weekends" magazine …...I too am a keen hill walker and would like to offer you a free year's subscription to help promote our magazine……. if you fancy joining the merry crew go to our website ……… the offer closes this friday so do hurry ;-), warmest regards, Mark".

The kill
You went to the website? You fell for the warm and friendly invitation? Gotcha!

The aftermath
By visiting the bogus website malware is activated that can steal security by keystroke monitoring or from user activity on the company's server. Some of us may have fallen foul to the bogus website that appears to be your own online banking site. You know, the one that asks you to declare your financial details because they are updating their services or whatever. The spear phish never makes such a request to the individual to disclose their security information directly as the malware achieves this in lieu of the request. The victim has thus been undermined and security compromised.

The message
So what could any company or other venture do to secure the computing infrastructure from these types of creative attacks? Firstly, it is clear from this simulation that those staff members seeking professional and personal information are more vulnerable to a social engineering attack. The company should therefore provide the necessary education to its staff on security threats (Heikkinen, 2010) that can be engineered from public data and always question requests to click on links that were unexpected or unsolicited. Perhaps even less suspicious would be requests that are work-related and seem to follow the natural course of everyday working life rather than specific to personal interests. Taken further a company could design and implement policies that prevent their staff from posting personal details. Without such a policy in place the humanising effect ensues, which plays straight into the hands of the social engineer who is studying the psychological behaviour of its targets in order to mimic them in the attack. Lastly the company could take a more aggressive approach to actively spear phishing their employees explicitly in a harmless attack in order to test their awareness. It in effect becomes the company drill of a cyber-attack as a preventative measure and analogous to the fire drill exercise. In the same way, without education, policies and procedures in place the company may get its fingers burnt.

References

Abraham, S. and Chengalur-Smith, I., 2010. An Overview of Social Engineering Malware: Trends, Tactics, and Implications. *Technology in Society*, **32**(3): 183-196.

CSO Magazine, 2012. *The Ultimate Guide to Social Engineering.* [Online] Accessed 12/06/2012 at http://assets.csoonline.com/documents/cache/pdfs/Social-Engineering-Ultimate-Guide.pdf

Heikkinen, S., 2010. Social Engineering in the World of Emerging Communication Technologies. In *Proceedings of Wireless World Research Forum meeting #17, Nov 2006.*