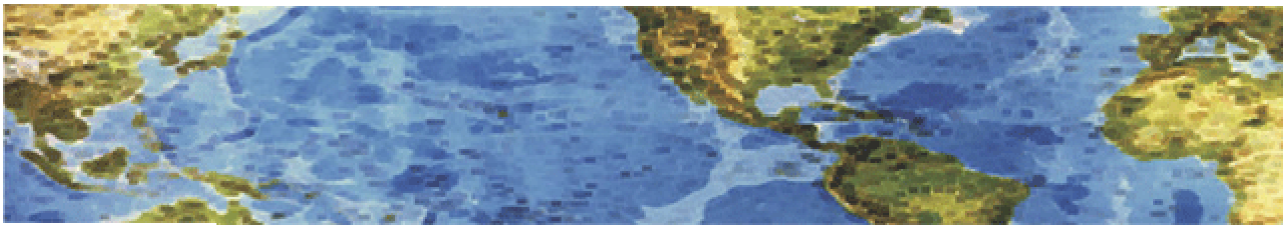
HALL ASSOCIATES



Risk-Based Decision Making Commentary
27 September 2013 Newsletter

Beta Bot: A New Trend in Cyber-Attacks

"I don't think most banks are aware of these latest scams that are replacing Zeus, SpyEye and other financial Trojans, in terms of popularity and usefulness to the criminals," says an analyst at the consultancy Gartner. "This particular Trojan is using techniques that I've seen before, so I'm not sure if it's that unique. **But Beta Bot is most definitely indicative of the new trend in cyber-attack vectors."**

Beta Bot's Attack

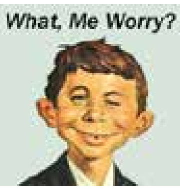
The Internet Crime Complaint Center and the Federal Bureau of Investigation recently issued an advisory about Beta Bot, the new malware that targets e-commerce sites, online payment platforms and even social networking sites to compromise log-in credentials and financial information. When Beta Bot infects a system, an illegitimate but official-looking Microsoft Windows message box named "User Account Control" pops up, asking the user to approve modifications to the computer's settings. "If the user complies with the request, the hackers are able to exfiltrate data from the computer," the advisory states. "Beta Bot is also spread via USB thumb drives or online via Skype, where it redirects the user to compromised websites." **Beta Bot defeats malware detection programs** because it blocks access to security websites and disables anti-virus programs, according to IC3.

Mitigating Risks

IC3 and the FBI warn that if consumers see what appears to be an alert from Microsoft but have not requested computer setting modifications from the company, they have likely been targeted for a Beta Bot attack. If infected, running a full system scan with up-to-date anti-virus software is recommended. And if access to security sites has been blocked, then downloading anti-virus updates or a new anti-virus program is advised. This trend of continual compromise of login credentials, which compromises standard online authentication practices, should be concerning to banking institutions. **And they should be taking steps to educate their customers**. Financial institutions should be proactively alerting their customers to this new threat.

This is a good example of how criminals' methods are constantly evolving. They are coming up with sophisticated methods that appear so convincing, even people who typically would not fall for their schemes may do so.

http://www.govinfosecurity.com/beta-bot-new-trend-in-cyber-attacks-a-6099/op-1



The Basics of Social Engineering

A recent study indicates that 30% of Americans will open e-mails, even when they know a message is malicious. One in eleven admitted that they have infected their IT systems by opening a malicious e-mail attachment. The reasons given for doing this are telling. For women, messages containing invitations from social networks are the most alluring. For men, messages with suggestions of money, power and/or sex were the most tempting.

So, you have all the bells and whistles when it comes to computer and network security and you have invested in all the latest technology. **But a social engineering attack can bypass all those defenses.**

Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology rather than breaking in or using hacking techniques. For example, instead of trying to find a software or operating system vulnerability, a social engineer might call an employee or family member and pose as an IT support person, trying to trick the employee or family member into divulging their passwords.

Social engineering has proven to be a very successful way for criminals to get inside your organization or your family. Criminals often take weeks or months getting to know a place before coming to the door or making a phone call. Such preparation includes finding a company phone book and an organizational chart, and researching employees on social networking sites like LinkedIn or Facebook.

People fall for these cons every day because they have not been adequately warned about social engineering cons and invariably want to be helpful. Human behavior is ALWAYS the weakest link in any security program. Without the proper education, most people won't even recognize a social engineer's tricks because they are increasingly very sophisticated. Four basic principles in misleading people:

- They project confidence. Instead of sneaking around, they proactively approach people and draw attention to themselves.
- They give you something. Even a small favor creates trust and a perception of indebtedness.
- They use humor. Its endearing and disarming.
- They make a request and offer a reason. Psych 110 research shows people are likely to respond to any reasoned request.

Awareness is the number one defensive measure. Employees and family members should be aware that social engineering exists and also be aware of the most commonly used tactics. A lot of information is available on these tactics. One website to check out is csoonline.com. It has numerous articles about social engineering. Some of the best ones are (can contact me for copies) :

Social Engineering – The Basics
How to Rob a Bank: A Social Engineering Walkthrough
Four Signs of an Easy Victim on Social Networks
What It's Like to Steal Someone's Identity

Hi Amy, This is Joe, from IT...I'm working from home today...