The FBI has recently issued an advisory warning companies that hackers are increasingly targeting law firms and public relations companies with a sophisticated e-mail scheme that breaks into their computer networks to steal sensitive data. They note that these attacks are often linked to large corporate clients doing business overseas. However, this is not a new situation. Cybercrime experts in the US and UK say this began as far back as two years ago but has grown dramatically over the past 6 months.

Tony Campbell, one of the publishers of online cybercrime journal, Digital Forensics Magazine said "Spear phishing is probably the most common form of attack. These come through spam e-mails that easily slip through common defences, appearing harmless because they seem relevant and from a trusted source.”As is often the case with cybercrime it can be difficult to tell whether hackers are working on behalf of a country's government, located in that country, or simply routing computer traffic through that country,” commented Campbell.

While some computer network attacks have been linked to countries, such as China, in many cases they are orchestrated by independent cybercrime groups. Such a group was recently convicted in the UK after investigation by a joint task force, set up between the financial industry and the Police Central e-Crime Unit (PCeU). The task force was set up in direct response to criticism that the UK government wasn't doing enough to tacking the rising problem of cybercrime. UK police are hailing the sentencing of four people who used a Trojan to siphon money out of online bank accounts.

“It doesn’t surprise me that hackers are going after law firms”, said Campbell, “they will often target companies that are involved in major international business - anything from seeking a patent on a sensitive new technology to opening a factory in another country. Often they are looking for sensitive documents, and legal companies have plenty of those. It’s probably the most effective way to obtain economic, personal and personal security related information about your target”.

While opening a "spear phishing" email itself does not pose a danger, they often contain web links or attachments that when clicked or opened will infiltrate the network or install malicious programs.Once the hacker is in the network, they often plant a computer program that searches for, collects and copies files and sends them to a computer server, usually in another country. The program also may create a backdoor that will allow hackers to come back later.

Digital Forensics Magazine can help keep cybercrime and computer forensics experts up-to-date with the latest developments and advances in forensic techniques. It is available as both an online magazine and in print and is published quarterly. For more information, please visit www.digitalforensicsmagazine.com

++ENDS++

If you would like to advertise in the magazine, or for more information, please visit www.digitalforensicsmagazine.com/media