Sploitcast

Technology, Information Technology

Sploitcast The new fishing Trojan that delivers stolen information back to the attacker via ICCP packets was a very interesting topic to me. I was surprised that this information was not sent back using HTT post or emailing. The part that was not that surprising was that the Trojan installs itself as an Internet Explorer help tool; this is a common way to infect a computer because it is the least suspecting way of attack. The Trojan actually appears to be doing the opposite that it was created for. A Trojan has never taken advantage of this way to export personal users' information before. It is scary to know that system administrators may not be used to seeing ICMP ping packets going outbound from a network. This new way of hacking information is not really surprising to me because hackers are always coming up with new methods to hack information. System administrators are usually the ones tasked to prevent this kind of activity, but if the information is not sent through using HTT post or emailing, then they likely won't notice it. Also, it is interesting to know that firewalls stop any incoming ICMP ping packets, but do not do so going out. Because these packets are unique, then it is likely that some software could be made to detect any malicious ICMP ping packets.

I also learned that the company Immunity has a new product that is a handheld penetrative testing tool. This product may come in handy against these malicious kinds of attacks because it can scan all the computers on a wireless network and then give details about any file shares or anything of interest.

One thing that I did not previously know about was Offensive Computing, which was launched by a pair of independent researchers. It is an open source search engine that contains information and analysis on 40, 000

hostile files from around the security industry. This could be helpful in identifying files that may be malware. IT departments can work together to combat the threat of viruses and malware. The female on the tape said that this type of collaboration may negatively affect anti-virus software, and I agree that it could be a problem in the future.

Another thing that I learned was how easy it is to get information off a laptop because it is relatively unprotected. I agree that corporate policy, such as not allowing sensitive information to be stored on a laptop, and hard drive encryption, such as encrypting files that contain sensitive information, are some of the ways to combat this. Databases should not be stored on laptops and instead on a server. Security policies should be implemented to help protect valuable information from being stolen. Users with laptops should only access vital information remotely from the server and no important information left on the laptop. Penalties are a way to encourage employees with laptops to follow company policy.

The discussion about the susceptibility of laptops to hackers was of particular interest to me because I very often use a laptop in public areas. While I may not have sensitive information, it is still a risk that others may take advantage of.