The Hacking Threat You've Probably Never Considered

August 10, 2016 - We warn our readers constantly about using safe computer habits when surfing the web or looking at email. Don't click on links in email messages from unknown sources. Stay away from shady websites. Make sure your anti-virus definitions are up to date and that you are running anti-virus software. But there is a threat out there that we have never considered before and which is apparently quite affective when it comes to luring new hacking victims.

Tech.co ran a story on Monday that made me wonder whether or not my computing practices were as safe as they should be. The author, George Diab, relayed a story from the BlackHat 2016 conference in Las Vegas. At the conference, I Google executive pondered whether dropping an infected USB drive in a parking lot would be an effective way to gain access to someone's computer. Put another way, if you found a USB flash drive in a parking lot, would you pick it up and plug it into your own computer?

It turns out that there was a study done on this topic. A research team planted nearly 300 USB drives around a college campus. 48% of the drives were eventually connected to the computers of the people who found them.

In this case, the USB drives were only infected with a program that got them to phone home and let the researchers know that the drives were active. But what if they had been dropped in the employee parking lot at a bank? Or a hospital? Or a brokerage house? Or on a military base? And what if they contained malware that would immediately infect computer systems when they were attached to a computer? That's a real possibility. There is no need for the person falling for this "prank" to be forced to click on a link or open a file.

This is actually a very frightening scenario. A plan this simple could bring a company to its knees very quickly. It could also damage national security if used in the right environment.

We're urging our readers to talk about this scenario with their employers and employees. It should be included in any data security training that your company does. And it should be included in your employee policy manuals because all of your network security procedures can be rendered useless by one unthinking act; an employee who finds a flash drive and who just has to find out what's on it.

byJim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow me on Twitter:

Follow ACCESS