Issued 3/16/18

Researchers Find 29 Types of USB Attacks, Recommend Never Plugging into a USB You Don't Own

Research from Ben-Gurion University has exposed 29 types of USB attacks, and extends to your smartphone. It shows that you should never use a USB charger you find lying around or plug into a public USB port. Both can be compromised by attackers, as we talked about with one of the researchers on the project, Ran Yahalom. Yahalom is the co-author of a journal article (link) on the research with Dr. Nir Nissim, head of the Malware Lab of the Cyber Security Research Center at Ben-Gurion University, and Yuval Elovici, head of BGU's Cyber Security Research Center (CSRC). Yahalom said, "Microcontrollers can impersonate a USB peripheral. For example, you can program a teensy microcontroller or an Arduino [board] to act like a keyboard or a mouse. Once you program a keyboard and connect, it actually starts injecting key presses. It's actually like having someone working on your computer. Someone can use an off-the-shelf product to find a way to reprogram firmware, update firmware, a legitimate process, supported by our protocol. It does bidding. "We surveyed 29 attacks, updated last year. New methods of likely developed an d published attacks increase that number. The microcontroller, a reprogrammable microcontroller used to impersonate peripherals as well as an actually the firmware update. Academic circles call this 'bad USB.' It's a family of attacks based on reprogramming the firmware." He continued, "The other are electrical attacks. In 2015, showed how to generate or build an electrical component enclosed in a flash drive casing. It looks like a flash drive, but it's not a flash drive, it conducts a power surge attack once connected, and, fry the entire computer. New developments in this area of attack are also likely. "If you go into a coffee shop and use charger there, or an airport or a train station, any charger that is not your own, you don't know what

that piece of hardware really does," Yahalom stresses. "It may not be a charger, but a microcontroller hidden inside a charger casing. It could be something else. You don't know. Once put into your phone, anything could happen. I demonstrated how to connect a keyboard to a phone. But it doesn't look like a keyboard, it looks like a charger, but it's actually a microcontroller I reprogrammed. I programmed it to act as a keyboard, so it impersonates a keyboard and it looks like a charger. It's connected to the socket, but without an electrical part of that charger, it's just a microcontroller. I showed how to connect it to and lock the phone, a sort of 'ransomware.' that equates to if you want the pin number to unlock the device, then you must pay me, which can really happen. There are other types of attacks, where someone reprograms your phone and you wouldn't even know. You're carrying spyware, without knowledge of it, just because you injected something you weren't aware of." "The general rule of thumb is: treat technology as something you don't naturally trust. As users, we have a tendency to trust technology, to trust peripherals, i.e., you trust your flash drive, you trust your keyboard, but you trust it because you're not aware. Treat it as a syringe: You wouldn't find a syringe in the parking lot, pick it up, and inject it to yourself. Because you're aware you could be infected. You have no knowledge of what could happen, but are afraid because it could be dangerous. This is exactly the same thing." "Now that we're moving from the cyber world to the physical world, it becomes increasingly clearer and we must get the word out," he said.

• "Bring your own charger.
• "Use your own hardware.
• "Don't trust Wi-Fi networks.

"Educate yourself about different levels of security. For example, 3G is commonly believed to be more secure than Wi-Fi, since Wi-Fi's easier to hack." Just be careful. Don't trust anything."