9 Tips To Block Hotel Wi-Fi Malware

May 11, 2012

The FBI issued an unusual warning this week to people traveling abroad: Beware malware attacks via hotel hotspots.

"Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel room," according to an advisory released by the Internet Crime Complaint Center (IC3), which is an FBI and National White Collar Crime Center partnership.

According to the advisory, the pop-up window prompts people to "update a widely-used software product." Clicking to accept the software update, meanwhile, would allow malware to be installed.

What can travelers do about these potential hotel Wi-Fi drive-by attacks? Focus on these nine information security essentials:

1. Update Before Leaving Despite the inevitable last-minute rush to get the bags packed, don't forget to install the latest application and operating system security updates onto your laptop, smartphone, and tablet before heading out. Also ensure that antivirus software is running on the device, and is likewise fully updated.

2. Block Pop-Ups Never, ever click on a pop-up window. "No major, reputable site requires a pop-up to work or function," said Kapil Raina, director of product marketing at Zscaler, via email. Preferably, configure your browser to block all pop-ups, so that no one using your computer--such as family members--can click on one.

3. Handle Free Wi-Fi With Caution The FBI advisory highlights the need to treat all free hotspots with caution. The problem, however, is that people often throw caution to the wind when presented with free stuff, such as USB keys or wireless access, and even if they're likely to be security-aware types attending a conference in the heart of Amsterdam filled with known hackers. That's what Steve Lord, a director at information security consultancy Mandalorian, discovered at this year's Black Hat Europe conference, when he installed a free Wi-Fi hotspot with the name "LEGITFREEWIFI." Sounds trustworthy, right? At least some of the attendees, who should have known better, used the hotspot with abandon.

4. Read Hotel Wi-Fi Directions Avoid connecting to fake hotspots by verifying which network actually belongs to the hotel. "If you must connect to a hotel Wi-Fi network, verify with the front desk the exact procedure (SSID name, process for payment, etc.)," said Zscaler's Raina. "You do not want to connect to a fake access point. Some hotels have direct connections (physical cables) you may opt for. In some cases, consider using your phone via 3G/4G as the connection point rather than Wi-Fi."

5. VPN Tunneling Secures Free Wi-Fi But Mandalorian's Lord, who deleted all data intercepted by his "weaponized hotspot," emphasized that he could have given his hotspot the same name as the hotel's hotspot, though didn't do so because he feared it would break the law. Of course, criminals would likely have no such compunctions. On that note, the best way to easily block such attacks is to use VPN tunneling. In fact, it's always a good idea--whether at home or abroad--to use a VPN whenever connecting to free Wi-Fi, since such hotspots, by their nature, aren't secure. Indeed, anyone can easily sniff wireless non-SSL traffic, unless it's routed via a VPN. Free, reputable VPN software is widely available for both PC and Mac (and in some cases, Linux), including Hotspot Shield from AnchorFree, the open source OpenVPN (Windows/Mac/Linux, Free), and Shrew Soft's VPN Client, as well as built-in VPN tools in both Apple OS X and Windows.

6. Download Software Updates Directly From Vendors While surfing the Web via hotel Wi-Fi, ignore all unsolicited software-update offers. "Download software updates directly from the software vendor's Web site if updates are necessary while abroad," according to the IC3 advisory. Anything else may be a scam. Also don't be afraid to verify security warnings by using another computer.

7. Beware Wired Hotel Connections Hotel hotspots aren't the only types of connections that can be compromised. According to news reports, systems at iBAHN--one of the world's largest providers of Internet services for hotels--were compromised last year. Although the company denied it had been hacked, any attacker who could successfully hack into that type of network would be able to serve up malware to anyone using a hotel network, even if they were connected via Ethernet cable.

8. Consider Using A "Burner" Laptop When traveling, one of the best ways to stay secure is simply to stay off the grid. If that's not an option, consider using a temporary, or "burner," laptop, such as an old laptop (personal) or extra machine (work). "Some companies now have policies where employees who travel abroad travel with a disposable laptop to ensure that no [intellectual property] or secrets available on their machines are stolen," said Rob Rachwald, director of security strategy at Imperva, in a blog post.

9. Don't Be Afraid To Hibernate Finally, if your computer has signs of infection, put it to sleep. "If you believe that you were hit, put your computer in hibernate or sleep mode until you can get expert help in repairing or restoring the system," said Raina at Zscaler. "Taking the system offline as fast as possible can prevent further data [exfiltration] and damage."

Source: http://www.informationweek.com/news/security/mobile/240000211