Security sleuths eye attack devices planted in packages

August 9 2019, by Nancy Cohen

Credit: CC0 Public Domain

How is this for irony. Everyone talks about security exploits getting more sophisticated. Yet an up and coming threat to the digital world, aka the hair-pulling mischief universe, could not be more elementary: hiding,

in a package, a low-cost, low-power computer designed for access attack and sending it off in the mail.

With millions of parcels en route to somewhere U.S., cyberattackers could take advantage of this seemingly innocent practice as an attack vector. The devices, tiny and lightweight, are attempts by criminals to hack into corporate or personal WiFi networks. Sleuths at IBM, in this day and age of e-commerce and package drops, call it warshipping.

"Once built, a warship device can perform wireless attacks simply by being shipped to someone and arriving on their desk or doorstep," according to *SecurityIntelligence*. "While in transit, the device does periodic basic wireless scans, similar to what a laptop does when looking for Wi-Fi hotspots. It transmits its location coordinates via GPS back to the C&C server."

IBM security researchers were in the news this week for testing these warshipping devices. What do these devices look like? Ather Fawaz sketched in the details for readers in *Neowin*.

"The device that needs to be deployed to the site is essentially made up of a single-board computer (SBC) that runs on a traditional cell-phone's rechargeable battery. Furthermore, with the off-shelf components, it costs just around $100 to make and looks more like a DIY project for a science exhibition at a school rather than a device that can be used to hack into networks."

IBM shows how shipping an exploitation device directly through the mail could allow attackers to hack into networks remotely with Charles Henderson, Global Managing Partner of IBM X- Force Red, at center-stage. That team has the ambitious title of "IBM X-Force Red" and their job is to uncover potential vulnerabilities in networks. In this instance, examining warshipping, "X-Force Red was able to infiltrate corporate

networks undetected. Our aim in doing so was to help educate our customers about security blind spots."

Through package deliveries to the office mailroom—or an individual victim's front door—packages can behave as an infiltrator.

Zack Whittaker, security editor at *TechCrunch*:

"Once the warship locates a Wi-Fi network from the mail room or the recipient's desk, it listens for wireless data packets it can use to break into the network. The warship listens for a handshake—the process of authorizing a user to log onto the Wi-Fi network—then sends that scrambled data over the cellular network back to the attacker's servers...With access to the Wi-Fi network, the attacker can navigate through the company's network, seeking out vulnerable systems and exposed data."

Whittaker said the team was not releasing proof-of-concept code so as to not help attackers.

"Think of the volume of boxes moving through a corporate mailroom daily," said Henderson in *SecurityIntelligence*. "Or, consider the packages dropped off on the porch of a CEO's home, sitting within range of their home Wi-Fi."

Actually, Henderson added, the malicious package does not have to be that recognizable but, as a 3G-enabled, remotely controlled system, "can be tucked into the bottom of a packaging box or stuffed in a child's teddy bear (a device no bigger than the palm of your hand) and delivered right into the hands or desk of an intended victim."

"In this warshipping project, " wrote Henderson, "we were, unfortunately, able to establish a persistent network connection and gain

full access to the target's systems."

"Would you let a visitor walk straight up to your chief financial officer's desk?" he asked. The same answer could apply for packages, especially if warshipping techniques were especially handy for cybercriminals during holiday seasons when package deliveries rise.

Businesses might consider best practices to avert warshipping attempts. Henderson had a number of suggestions in *SecurityIntelligence*. A scanning process for packages in mailrooms might be considered. Scanning could detect malicious devices in clothing or in books.