Apple AirTag Bug Enables ‘Good Samaritan’ Attack

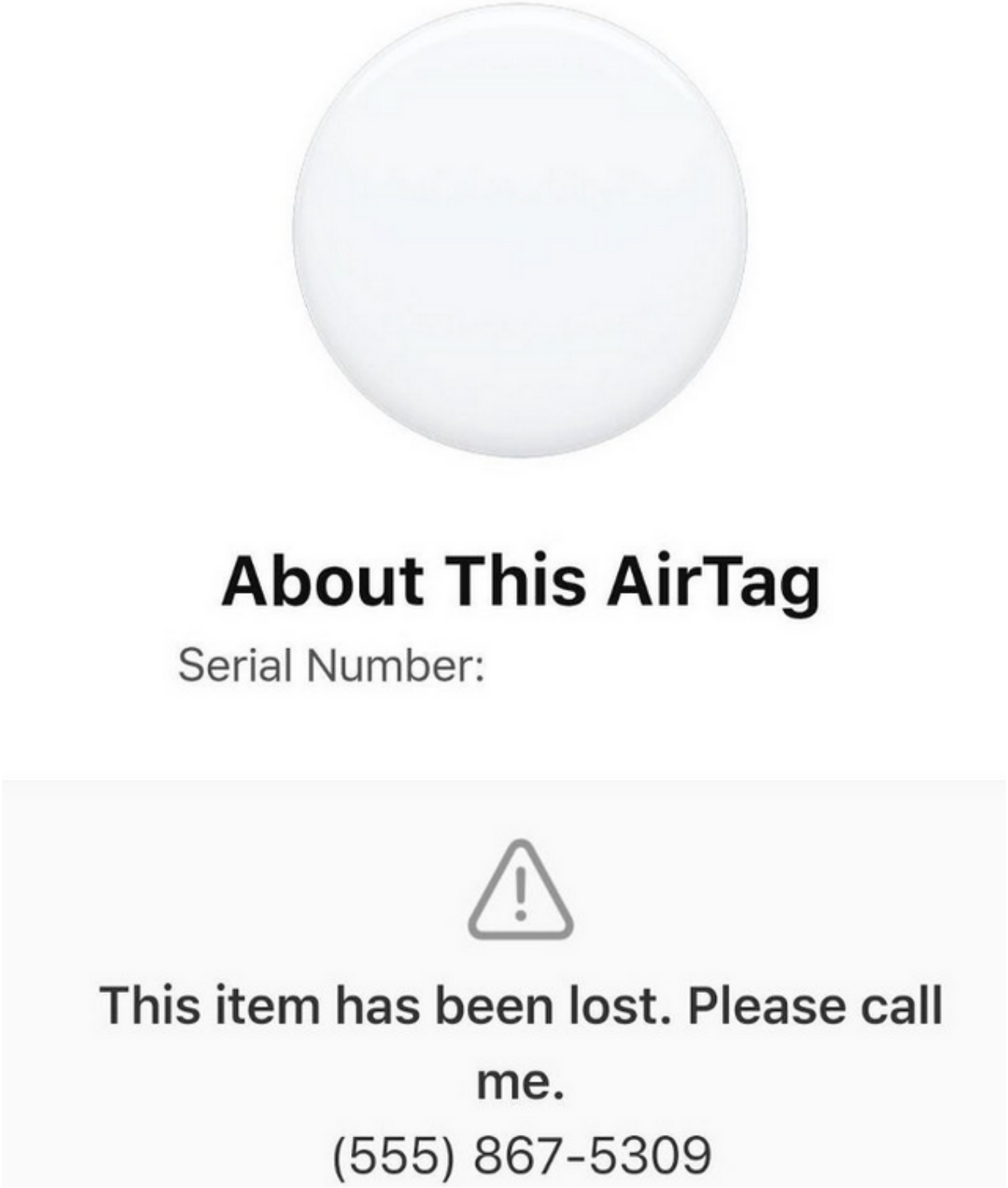
The new $30 **AirTag** tracking device from **Apple** has a feature that allows anyone who finds one of these tiny location beacons to scan it with a mobile phone and discover its owner’s phone number if the AirTag has been set to lost mode. But according to new research, this same feature can be abused to redirect the Good Samaritan to an iCloud phishing page — or to any other malicious website.

The AirTag’s “Lost Mode” lets users alert Apple when an AirTag is missing.

Setting it to Lost Mode generates a unique URL at https://found.apple.com, and allows the user to enter a personal message and contact phone number. Anyone who finds the AirTag and scans it with an Apple or Android phone will immediately see that unique Apple URL with the owner's message.

When scanned, an AirTag in Lost Mode will present a short message asking the finder to call the owner at at their specified phone number. This information pops up without asking the finder to log in or provide any personal information. But your average Good Samaritan might not know this.

That's important because Apple's Lost Mode doesn't currently stop users from injecting arbitrary computer code into its phone number field — such as code that causes the Good Samaritan's device to visit a phony Apple iCloud login page.



A sample "Lost Mode" message. Image: Medium @bobbyrsec

The vulnerability was discovered and reported to Apple by Bobby Rauch, a security consultant and penetration tester based in Boston. Rauch told KrebsOnSecurity the AirTag weakness makes the devices cheap and possibly very effective physical trojan horses.

"I can't remember another instance where these sort of small consumer-grade tracking devices at a low cost like this could be weaponized," Rauch said.

Consider the scenario where an attacker drops a malware-laden USB flash drive in the parking lot of a company he wants to hack into. Odds are that sooner or later some employee is going to pick that sucker up and plug it into a computer — just to see what's on it (the drive might even be labeled something tantalizing, like "Employee Salaries").

If this sounds like a script from a James Bond movie, you're not far off the mark. A USB stick with malware is very likely how U.S. and Israeli cyber hackers got the infamous Stuxnet worm into the internal, air-gapped network that powered Iran's nuclear enrichment facilities a decade ago. In 2008, a cyber attack described at the time as "the worst breach of U.S. military computers in history" was traced back to a USB flash drive left in the parking lot of a U.S. Department of Defense facility.

In the modern telling of this caper, a weaponized AirTag tracking device could be used to redirect the Good Samaritan to a phishing page, or to a website that tries to foist malicious software onto her device.

In the modern telling of this caper, a weaponized AirTag tracking device could be used to redirect the Good Samaritan to a phishing page, or to a website that tries to foist malicious software onto her device.

Rauch contacted Apple about the bug on June 20, but for three months when he inquired about it the company would say only that it was still investigating. Last Thursday, the company sent Rauch a follow-up email stating they planned to address the weakness in an upcoming

update, and in the meantime would he mind not talking about it publicly?

Rauch said Apple never acknowledged basic questions he asked about the bug, such as if they had a timeline for fixing it, and if so whether they planned to credit him in the accompanying security advisory. Or whether his submission would qualify for Apple's "bug bounty" program, which promises financial rewards of up to $1 million for security researchers who report security bugs in Apple products.

Rauch said he's reported many software vulnerabilities to other vendors over the years, and that Apple's lack of communication prompted him to go public with his findings — even though Apple says staying quiet about a bug until it is fixed is how researchers qualify for recognition in security advisories.

"I told them, 'I'm willing to work with you if you can provide some details of when you plan on remediating this, and whether there would be any recognition or bug bounty payout'," Rauch said, noting that he told Apple he planned to publish his findings within 90 days of notifying them. "Their response was basically, 'We'd appreciate it if you didn't leak this.'"

Rauch's experience echoes that of other researchers interviewed in a recent *Washington Post* article about how not fun it can be to report security vulnerabilities to Apple, a notoriously secretive company. The common complaints were that Apple is slow to fix bugs and doesn't always pay or publicly recognize hackers for their reports, and that researchers often receive little or no feedback from the company.

The risk, of course, is that some researchers may decide it's less of a hassle to sell their exploits to vulnerability brokers, or on the darknet — both of which often pay far more than bug bounty awards.

There's also a risk that frustrated researchers will simply post their findings online for everyone to see and exploit — regardless of whether

the vendor has released a patch. Earlier this week, a security researcher who goes by the handle "illusionofchaos" released writeups on three zero-day vulnerabilities in Apple's iOS mobile operating system — apparently out of frustration over trying to work with Apple's bug bounty program.

Ars Technica reports that on July 19 Apple fixed a bug that llusionofchaos reported on April 29, but that Apple neglected to credit him in its security advisory.

"Frustration with this failure of Apple to live up to its own promises led illusionofchaos to first threaten, then publicly drop this week's three zero-days," wrote **Jim Salter** for Ars. "In illusionofchaos' own words: 'Ten days ago I asked for an explanation and warned then that I would make my research public if I don't receive an explanation. My request was ignored so I'm doing what I said I would.'"

Rauch said he realizes the AirTag bug he found probably isn't the most pressing security or privacy issue Apple is grappling with at the moment. But he said neither is it difficult to fix this particular flaw, which requires additional restrictions on data that AirTag users can enter into the Lost Mode's phone number settings.

"It's a pretty easy thing to fix," he said. "Having said that, I imagine they probably want to also figure out how this was missed in the first place."

Apple has not responded to requests for comment.

Update, 12:31: Rauch shared an email showing Apple communicated their intention to fix the bug just hours *before* — not after — KrebsOnSecurity reached out to them for comment. The story above has been changed to reflect that.