BLIND SPOT —

Researchers devise iPhone malware that runs even when device is turned off

Research is largely theoretical but exposes an overlooked security issue.

DAN GOODIN - 5/17/2022, 4:20 AM

Classen et al.

SUBSCRIBE SIGN IN

When you turn off an iPhone, it doesn't fully power down. Chips inside the device continue to run in a low-power mode that makes it possible to locate lost or stolen devices using the Find My feature or use credit cards and car keys after the battery dies. Now researchers have devised a way to abuse this always-on mechanism to run malware that remains active even when an iPhone appears to be powered down.

It turns out that the iPhone's Bluetooth chip—which is key to making features like Find My work—has no mechanism for digitally signing or even encrypting the firmware it runs. Academics at Germany's Technical University of Darmstadt figured out how to exploit this lack of hardening to run malicious firmware that allows the attacker to track the phone's location or run new features when the device is turned off.

This video provides a high overview of some of the ways an attack can work.

[Paper Teaser] Evil Never Sleeps: When Wireless Malware Stays On After Turning Off iPhones.

The research is the first—or at least among the first—to study the risk posed by chips running in low-power mode. Not to be confused with iOS's low-power mode for conserving battery life, the low-power mode (LPM) in this research allows chips responsible for near-field communication, ultra wideband, and Bluetooth to run in a special mode that can remain on for 24 hours after a device is turned off.

"The current LPM implementation on Apple iPhones is opaque and adds new threats," the researchers wrote in a paper published last week. "Since LPM support is based on the iPhone's hardware, it cannot be removed with system updates. Thus, it has a long-lasting effect on the overall iOS security model. To the best of our knowledge, we are the first who looked into undocumented LPM features introduced in iOS 15 and uncover various issues."

Advertisement

They added: “Design of LPM features seems to be mostly driven by functionality, without considering threats outside of the intended applications. Find My after power off turns shutdown iPhones into tracking devices by design, and the implementation within the Bluetooth firmware is not secured against manipulation.”

The findings have limited real-world value since infections required a jailbroken iPhone, which in itself is a difficult task, particularly in an adversarial setting. Still, targeting the always-on feature in iOS could prove handy in post-exploit scenarios by malware such as Pegasus, the sophisticated smartphone exploit tool from Israel-based NSO Group, which governments worldwide routinely employ to spy on adversaries.

FURTHER READING
iPhones of US diplomats hacked using “0-click” exploits from embattled NSO

It may also be possible to infect the chips in the event hackers discover security flaws that are susceptible to over-the-air exploits similar to this one that worked against Android devices.

FURTHER READING
New Attack exploiting serious Bluetooth weakness can intercept sensitive data

Besides allowing malware to run while the iPhone is turned off, exploits targeting LPM could also allow malware to operate with much more stealth since LPM allows firmware to conserve battery power. And of course, firmware infections are already extremely difficult to detect because of the significant expertise and expensive equipment required to do so.

The researchers said Apple engineers reviewed their paper before it was published, but company representatives never provided any feedback on its contents. Apple representatives didn’t respond to an email seeking comment for this story.

Ultimately, Find My and other features enabled by LPM help provide added security because they allow users to locate lost or stolen devices and lock or unlock car doors even when batteries are depleted. But the research exposes a double-edged sword that, until now, has gone largely unnoticed.

“Hardware and software attacks similar to the ones described, have been proven practical in a real-world setting, so the topics covered in this paper are timely and practical,” John Loucaides, senior vice president of strategy at firmware security firm Eclypsium. “This is typical for every device. Manufacturers are adding features all the time and with every new feature comes a new attack surface.”

READER COMMENTS 90 SHARE THIS STORY

Join Ars Technica and

Get Our Best Tech Stories

DELIVERED STRAIGHT TO YOUR INBOX.

Email address

SIGN ME UP

By signing up, you agree to our user agreement (including the class action waiver and arbitration provisions), our privacy policy and cookie statement, and to receive marketing and account-related emails from Ars Technica. You can unsubscribe at any time.

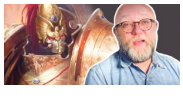
DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

Advertisement

Unsolved Mysteries Of Quantum Leap With Donald P. Bellisario



Unsolved Mysteries Of