3 iOS 0-days, a cellular network compromise, and HTTP used to infect an iPhone

Getty Images

reader comments

23 with

Apple has patched a potent chain of iOS zero-days that were used to infect the iPhone of an Egyptian presidential candidate with sophisticated spyware developed by a commercial exploit seller, Google and researchers from Citizen Lab said Friday.

The previously unknown vulnerabilities, which Apple patched on Thursday, were exploited in clickless attacks, meaning they didn’t require a target to take any steps other than to visit a website that used the HTTP protocol rather than the safer HTTPS alternative. A packet inspection device sitting on a cellular network in Egypt kept an eye out for connections from the phone of the targeted candidate and, when spotted, redirected it to a site that delivered the exploit chain, according to Citizen Lab, a research group at the University of Toronto’s Munk School.

A cast of villains, 3 0-days, and a compromised cell network

Citizen Lab said the attack was made possible by participation from the Egyptian government, spyware known as Predator sold

by a company known as Cytrox, and hardware sold by Egypt-based Sandvine. The campaign targeted Ahmed Eltantawy, a former member of the Egyptian Parliament who announced he was running for president in March. Citizen Lab said the recent attacks were at least the third time Eltantawy's iPhone has been attacked. One of them, in 2021, was successful and also installed Predator.

"The use of mercenary spyware to target a senior member of a country's democratic opposition after they had announced their intention to run for president is a clear interference in free and fair elections and violates the rights to freedom of expression, assembly, and privacy," Citizen Lab researchers Bill Marczak, John Scott-Railton, Daniel Roethlisberger, Bahr Abdul Razzak, Siena Anstis, and Ron Deibert wrote in a 4,200-word report. "It also directly contradicts how mercenary spyware firms publicly justify their sales."

The vulnerabilities, which are patched in iOS versions 16.7 and iOS 17.0.1, are tracked as:

- CVE-2023-41993: Initial remote code execution in Safari
- CVE-2023-41991: PAC bypass
- CVE-2023-41992: Local privilege escalation in the XNU Kernel

Advertisement

According to research published Friday by members of Google's Threat Analysis Group, the attackers who exploited the iOS vulnerabilities also had a separate exploit for installing the same Predator spyware on Android devices. Google patched the flaws on September 5 after receiving a report by a research group calling itself DarkNavy.

"TAG observed these exploits delivered in two different ways: the MITM injection and via one-time links sent directly to the target," Maddie Stone, a researcher with the Google Threat Analysis Group wrote. "We were only able to obtain the initial

renderer remote code execution vulnerability for Chrome, which was exploiting CVE-2023-4762.”

The attack was complex. Besides leveraging three separate iOS vulnerabilities, it also relied on hardware made by a manufacturer known as Sandvine. Sold under the brand umbrella PacketLogic, the hardware sat on the cellular network the targeted iPhone accessed and monitored traffic passing over it for his phone. Despite the precision, Citizen Lab said that the attack is blocked when users turn on a feature known as Lockdown, which Apple added to iOS last year. More about that later.

There’s little information about the iOS exploit chain other than it automatically triggered when a target visited a site hosting the malicious code. Once there, the exploits installed Predator with no further user action required.

To surreptitiously direct the iPhone to the attack site, it only needed to visit any HTTP site. Over the past five years or so, HTTPS has become the dominant means of connecting to websites because the encryption it uses prevents adversary-in-the-middle attackers from monitoring or manipulating data sent between the site and the visitor. HTTP sites still exist, and sometimes HTTPS connections can be downgraded to unencrypted HTTP ones.

Once Eltantawy visited an HTTP site, the PacketLogic device injected data into the traffic that surreptitiously connected the Apple device to a site that triggered the exploit chain.

Enlarge / Network diagram showing the Spyware Injection Middlebox located on a link between Telecom Egypt and Vodafone Egypt.

Predator, the payload installed in the attack, is sold to a wide array of governments, including those of Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia. Citizen Lab has said that Predator was used to target Ayman Nour, a member of the Egyptian political opposition living in exile in Turkey, and an Egyptian exiled journalist who hosts a popular news program and wishes to remain anonymous. Last year researchers from Cisco’s Talo security team exposed the inner workings of the malware after obtaining a binary of it. https://arstechnica.com/?p=1970625