Operation indiscriminately infects iPhones with spyware

August 31 2019, by Frank Bajak

This Sept. 12, 2018, file photo shows an Apple iPhone XR on display at the Steve Jobs Theater after an event to announce new products, in Cupertino, Calif. Suspected nation-state hackers used malware-laden websites to infect iPhones with spyware in what security researchers are calling the worst general security failure yet affecting the Apple devices. Announced late Thursday, Aug. 29, 2019, by Google researchers, the vulnerabilities were quietly fixed by Apple in February but only after thousands of iPhone users were believed exposed over more than two years. (AP Photo/Marcio Jose Sanchez, File)

Researchers say suspected nation-state hackers infected Apple iPhones with spyware over two years in what security experts on Friday called an alarming security failure for a company whose calling card is privacy.

A mere visit to one of a small number of tainted websites could infect an iPhone with an implant capable of sending the smartphone owner's text messages, email, photos and real-time location data to the cyberspies behind the operation.

"This is definitely the most serious iPhone hacking incident that's ever been brought to public attention, both because of the indiscriminate targeting and the amount of data compromised by the implant," said former U.S. government hacker Jake Williams, the president of Rendition Security.

Announced late Thursday by Google researchers, the last of the vulnerabilities were quietly fixed by Apple by February but only after thousands of iPhone users were believed exposed over more than two years.

The researchers did not identify the websites used to seed the spyware or their location. They also did not say who was behind the cyberespionage or what population was targeted, but experts said the operation had the hallmarks of a nation-state effort.

Williams said the spyware implant wasn't written to transmit stolen data securely, indicating the hackers were not concerned about getting caught. That suggests an authoritarian state was behind it. He speculated that it was likely used to target political dissidents.

Sensitive data accessed by the spyware included WhatsApp, iMessage

and Telegram text messages, Gmail, photos, contacts and real-time location—essentially all the databases on the victim's phone. While the messaging applications may encrypt data in transit, it is readable at rest on iPhones.

Google researcher Ian Beer said in a blog posted late Thursday that the discovery should dispel any notion that it costs a million dollars to successfully hack an iPhone. That's a reference to the case of a United Arab Emirates dissident whose iPhone was infected in 2016 with so-called zero-day exploits, which have been known to fetch such high prices.

"Zero day" refers to the fact that such exploits are unknown to the developers of the affected software, and thus they have had no time to develop patches to fix it.

The discovery, involving 14 such vulnerabilities, was made by Google researchers at Project Zero, which hunts the security flaws in software and microprocessor firmware, independent of their manufacturer, that criminals, state-sponsored hackers and intelligence agencies use.

"This should serve as a wake-up call to folks," said Will Strafach, a mobile security expert with Sudo Security. "Anyone on any platform could potentially get infected with malware."

Beer said his team estimated that the infected websites used in the "indiscriminate watering hole attacks" receive thousands of visitors per week. He said the team collected five separate chains of exploits covering Apple's iOS system as far back as version 10, released in 2016.

Apple did not respond to requests for comment on why it did not detect the vulnerabilities on its own and if it can assure users that such a general attack could not happen again. Privacy assurance is central to the Apple

brand.

Neither Google nor Beer responded to questions about the attackers or the targets, though Beer provided a hint in his blog post: "To be targeted might mean simply being born in a certain geographic region or being part of a certain ethnic group."

Security manager Matt Lourens at Check Point Software Technologies called the development an alarming game-changer. He said that while iPhone owners previously compromised by zero days were high-value targets, a more widespread seeding of spyware at a lower cost per infection has now been shown possible.

"This should absolutely reshape the way corporations view the use of mobile devices for corporate applications, and the security risk it introduces to the individual and/or organization," Lourens said in an email.

In his blog post, the Google researcher Beer warned that absolute digital security can't be guaranteed.

Smartphone users must ultimately "be conscious of the fact that mass exploitation still exists and behave accordingly;" he wrote, "treating their mobile devices as both integral to their modern lives, yet also as devices which when compromised, can upload their every action into a database to potentially be used against them."