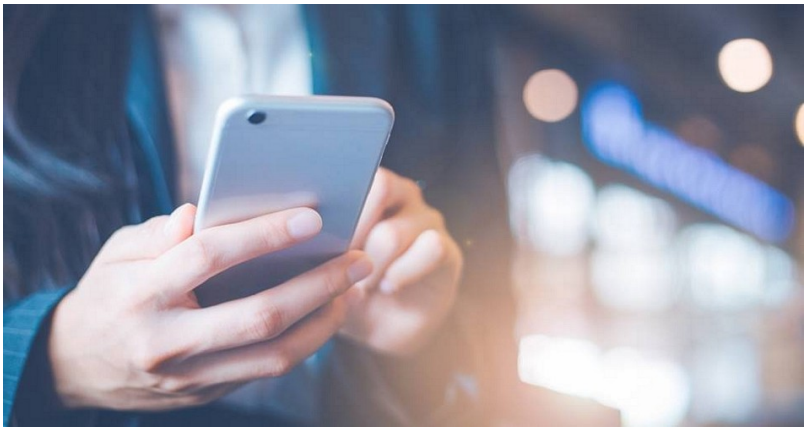
Written by **C. Mitchell Shaw** on August 30, 2019

Google's Project Zero Reveals Stunning iPhone Hack



A recently disclosed hacking operation that ran for two and a half years and had "attacked thousands of [iPhone] users a week" was used to steal nearly all data stored on and used by those devices. That data included up-to-the-minute location information, all passwords, contacts, chat logs, e-mails, and more.

The complexity of the hack was simply astounding. Using a few hacked websites, the hackers were able to deliver malware to devices running iOS simply by the device being used to visit the sites. No user interaction beyond visiting those sites was needed for the devices to be taken over by the hackers; simply visiting the hacked websites was sufficient to launch the attack and install the malware that was then used to grant the hackers remote access to the devices. This particular type of remote access is known as a "monitoring implant."

While it is unknown who the hackers were, the complexity and efficiency of the attack indicates that they possessed both a skill-set and organizational structure usually seen in state-sponsored hacking organizations. This hack involved five separate exploit chains made up of 14 distinct bugs. Due to the difficulty of hacking the iPhone, developing or purchasing the information needed for a single exploit chain for an up-to-date iPhone can cost up to $3 million, according to a report by Motherboard. That means that this hack had a price possible tag in the $15 million range.

The nature of the monitoring implant was such that access to the devices was lost whenever they were restarted and would remain lost until those devices accessed those hacked sites again. However, the data harvested each time one of the sites was accessed allowed the hackers to continue accessing users' data through the accounts to which they then had access via passwords and other login credentials.

"Given the breadth of information stolen, the attackers may nevertheless be able to maintain persistent access to various accounts and services by using the stolen authentication tokens from the keychain, even after they lose access to the device," Google security researcher Ian Beer wrote.

One thing that set this attack apart is that is was not "targeted." Any iPhone user who visited one of the compromised websites would have been sent the malware. Once the malware attack was successful, the hackers would gain access to any data the monitoring implant was designed to access.

The hack was discovered and disclosed by Project Zero, an elite group of "white-hat" hackers at Google, whose name comes from their focus on finding — and disclosing — so called "zero day exploits." A zero

day exploit is a bug that has not yet been discovered by the vendor responsible for the software containing the bug (in this case, Apple), meaning that there are "zero days" to fix the bug before it could be exploited. Project Zero works to find such vulnerabilities and make the vendor aware so that the vulnerability can be patched before it is exploited. Project Zero has a controversial policy of making such vulnerabilities public 90 days after reporting them to the victim company — even if they have not been patched.

In this case, Apple was made aware of the vulnerabilities on February 1, and Apple patched iOS with an update less than a week later, on February 7.

In a blog post, Project Zero's Ian Beer wrote, "This was a failure case for the attacker," since the exploit was eventually patched, however, "For this one campaign that we've seen, there are almost certainly others that are yet to be seen." One could reasonably disagree with Beer's assessment that this was a "failure," since the hackers undoubtedly harvested millions of pieces of useful data about iPhone users during their "successful" two-and-a-half-year run. But he is certainly correct that there are likely many more vulnerabilities that have been discovered by nefarious hackers than are known to the vendors.

Since the iPhone hack was an end-point device attack and involved accessing the stored keychain — which keeps track of passwords and other credentials as well as the databases for secured communication apps, such as WhatsApp, iMessage, and others — the end-to-end encryption of those apps would have done nothing to protect those communications.

Since the iPhone attack would provide hackers with account login credentials for any accounts stored on the device, *The New American* recommends that all iPhone users change all of their passwords to all accounts accessed using their iPhones in the past.

Beer also wrote, "All that users can do is be conscious of the fact that mass exploitation still exists and behave accordingly; 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." Of course, that means not using your mobile device for anything you would consider sensitive. But what is sensitive and what you think is sensitive are not always the same thing.

Considering the power of aggregated data, one must realize that one piece of seemingly innocuous data added to many other pieces of innocuous data adds up to a very powerful — and accurate — profile of your habits and activities. In fact, that profile is likely a picture of you that is more accurate than the picture you have of yourself, since the algorithms used to analyze those pieces of data are not fooled by your own self image.

The take-away, then,is that smartphone users need to think of their devices as necessary evils that cannot be trusted unless those devices are designed — from the ground up — with privacy in mind. That would mean a device that runs only open-source software which can be audited by anyone. One example of that would be the soon-to-be-released Librem 5 smartphone by Purism, running neither iOS nor Android, but a pure mobile version of Linux.

For those committed to staying with either iPhone or Android, Beer's warning serves as a stark reminder that the device you carry may be watching you and reporting to someone you don't know and cannot trust.

Image: apichon_tee via iStock / Getty Images Plus