Spandan College1
spandanktm@gmail.com
9841017798

Google and Apple ||almuni Connect|| 2019-08-31 00:13:00

Contributors

Khalti	**Spandan Subba**	**Ranjan Pokharel**	**Mega Bank**
Sponsor	Author	Author	Knowledge Partner
Online pay	student	student	Bank

Anuj Ghimire	**Kantipur**
Author	Knowledge Partner
Almuni	Media Company

Google and Apple

Security researchers at Google have found evidence of a “sustained effort” to hack iPhones over a period of at least two years.

Spandan College1
spandanktm@gmail.com
9841017798

Photographer: Michael Short/Bloomberg

© 2017 BLOOMBERG FINANCE LP

The attack was said to be carried out using websites which would discreetly implant malicious software to gather contacts, images and other data.

Google's analysis suggested the booby-trapped websites were said to have been visited thousands of times per week.

Apple told the BBC it did not wish to comment.

The attack was shared in great detail in a series of technical posts written by British cybersecurity expert Ian Beer, a member of Project Zero, Google's taskforce for finding new security vulnerabilities, known as zero days.

"There was no target discrimination," Mr Beer wrote.

"Simply visiting the hacked site was enough for the exploit server to attack your device, and if it was successful, install a monitoring implant."

Mr Beer and his team said they discovered attackers were using 12 separate security flaws in order to compromise devices. Most were bugs within Safari, the default web browser on Apple products.

'Sustained effort'

Once on a person's iPhone, the implant could access an enormous amount of data, including (though not limited to) contacts, images and GPS location data. It would relay this information back to an external server every 60 seconds, Mr Beer noted.

The implant also was able to scoop up data from apps a person was using, such as Instagram, WhatsApp and Telegram. Mr Beer's list of examples also included Google products such as Gmail and Hangouts, the firm's group video chat app.

The attackers were able to exploit "almost every version from iOS 10 through to the latest version of iOS 12", Mr Beer added.

"This indicated a group making a sustained effort to hack the users of iPhones in certain communities over a period of at least two years."

Spandan College1
spandanktm@gmail.com
9841017798

Are you protected?

Apple issued a software fix to address the flaw back in February.

If you are an iPhone user, you should make sure your device is running the latest version of iOS, to make sure you are protected.

To do this, go to Settings and tap General. Under 'Software Update' you should be running iOS 12.4.1.

If you are not running iOS 12.4.1 you will be given the opportunity to update your device.

Apple's fix

Google's team notified Apple of the vulnerabilities on 1 February this year. A patch was subsequently released six days later to close the vulnerability. Apple's patch notes refer to fixing an issue whereby "an application may be able to gain elevated privileges" and "an application may be able to execute arbitrary code with kernel privileges".

Spandan College1
spandanktm@gmail.com
9841017798

Media captionApple boss Tim Cook unveils new privacy protections

iPhone users should update their device to the latest software to make sure they are adequately protected.

Unlike some security disclosures, which offer merely theoretical uses of vulnerabilities, Google discovered this attack “in the wild" - in other words, it was in use by cybercriminals.

Mr Beer’s analysis did not speculate on who may be behind the attack, nor how lucrative the tool may have been on the black market. Some “zero day” attacks can be sold for several millions dollars - until they’re discovered and fixed.

_____

Follow Dave Lee on Twitter @DaveLeeBBC

Do you have more information about this or any other technology story? You can reach Dave directly and securely through encrypted messaging app Signal on: +1 (628) 400-7370




