The stakes are too high for Apple to spin the iPhone exploits

Today, Apple responded to Google's discovery of a major iPhone security flaw with a bristling statement that accused its rival of creating "false impressions." But Apple did very little to clear up those false impressions, and seems to have created some of its own, as we'll see by taking a close read.

First, let's talk about what Apple *did* confirm. When Google originally published detailed information about the iOS exploits, it conspicuously did not say specifically why they were created or who they were targeted at. Following Google's disclosure, *TechCrunch* reported that the exploits were part of a state-sponsored attack that was meant to target China's minority Uighur population. (The attackers also reportedly targeted Android and Windows devices.) It has been widely reported that China is persecuting the Uighur minority in the country with torture, internment, and surveillance; just yesterday, Reuters and CNN reported that China is trying to hack telecoms to track Uighurs across Asia. So there's plenty of looming context regarding the potential source and aim of iOS exploits like the one disclosed by Google.

Apple confirmed today that the iOS exploits indeed were targeted at Uighurs; Apple says that they "affected fewer than a dozen websites that focus on content related to the Uighur community." But Apple's framing minimizes the context and potential consequences of the exploit against that community in favor of irritation at Google's blog post and the subsequent media coverage.

To its credit, Apple did disclose and confirm the exploit targeted the Uighur community, which Google did not do. But Apple's statement is almost entirely focused on Google's perceived failings, instead of the ongoing persecution of a religious minority in China, which is one of Apple's largest markets and also the focus of an ongoing trade war that directly implicates the company's products.

Several times in today's statement, Apple takes something Google itself said and spins it as an act of omission.

Apple:

> *First, the sophisticated attack was narrowly focused, not a broad-based exploit of iPhones "en masse" as described. The attack affected fewer than a dozen websites that focus on content related to the Uighur community.*

Google:

> *Earlier this year Google's Threat Analysis Group (TAG) discovered a small collection of hacked websites. The hacked sites were being used in indiscriminate watering hole attacks against their visitors, using iPhone 0-day.*

Here Apple *repeats* Google's own original claim, but spins it by connecting it to a line later in Google's piece about the attack being "en masse." Reasonable people may disagree about the scope of "en masse," which means both "a group" and "all together," but Google certainly did not omit information about the vector of the attack.

Apple:

> *Google's post, issued six months after iOS patches were released, creates the false impression of "mass exploitation" to "monitor the private activities of entire populations in real time," stoking fear among all iPhone users that their*

> *devices had been compromised.*

Google:

> *Real users make risk decisions based on the public perception of the security of these devices. The reality remains that security protections will never eliminate the risk of attack if you're being targeted. To be targeted might mean simply being born in a certain geographic region or being part of a certain ethnic group. 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.*
>
> *[…]*
>
> *I shan't get into a discussion of whether these exploits cost $1 million, $2 million, or $20 million. I will instead suggest that all of those price tags seem low for the capability to target and monitor the private activities of entire populations in real time.*

Apple takes Google's quotes here completely out of context. Google is talking about the perception of risk and the inherent vulnerability of computing, which is not really up for debate. It's also talking about the mass targeting of a specific community; as we learned today, that community happens to be a religious minority being actively persecuted in China. It's bizarre that Apple marginalizes them here by ignoring the nuance of the attack and extrapolating Google's concerns to "all iPhone users."

Apple:

> *Second, all evidence indicates that these website attacks were only operational for a brief period, roughly two months,*

> *not “two years” as Google implies.*

Google:

> *TAG was able to collect five separate, complete and unique iPhone exploit chains, covering almost every version from iOS 10 through to the latest version of iOS 12. 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.*
>
> *[…]*
>
> *Initial analysis indicated that at least one of the privilege escalation chains was still 0-day and unpatched at the time of discovery (CVE-2019-7287 & CVE-2019-7286). We reported these issues to Apple with a 7-day deadline on 1 Feb 2019, which resulted in the out-of-band release of iOS 12.1.4 on 7 Feb 2019. We also shared the complete details with Apple, which were disclosed publicly on 7 Feb 2019.*

Where does Google imply the website attacks were operational for two years? Google explicitly says their evidence indicated “a group making a sustained effort” over those two years, not that iPhone users were compromised that whole time, and points to its disclosure of those vulnerabilities to Apple. Apple’s reading here is disingenuous at best.

Google:

> *There was no target discrimination; simply visiting the hacked site was enough for the exploit server to attack your device, and if it was successful, install a monitoring implant. We estimate that these sites receive thousands of visitors per week.*

Apple:

> *Regardless of the scale of the attack, we take the safety and*

> *security of all users extremely seriously.*

Apple has not earned a “regardless” here. It has given us no idea of the actual scale of the attack. It does not even respond to Google’s estimate that thousands of visitors may have been affected *per week*. Even if we take Apple’s word that the exploit was only operational for two months, that’s potentially tens of thousands (or more) of unwitting victims who are members of a vulnerable population that is currently being targeted by a repressive government. “Taking the safety and security of all users extremely seriously” would keep the focus on the users under attack, not the Google researchers who discovered the exploits.

https://www.theverge.com/2019/9/6/20853393/apple-iphone-ios-exploits-statement-security-google-false-impressions