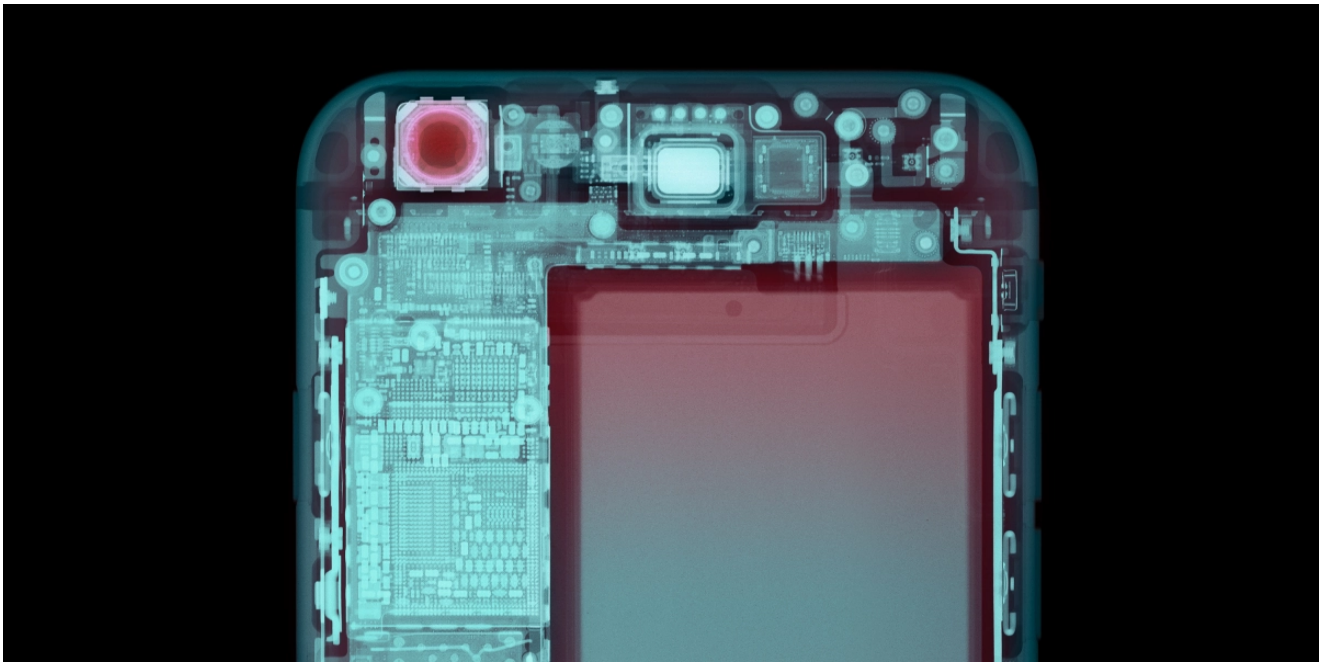
How China turned a prize-winning iPhone hack against the Uyghurs

technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/

Patrick Howell O'Neill



- Beijing secretly used an award-winning iPhone hack to spy on Uyghurs
- The United States tracked the attack and informed Apple
- Tianfu Cup is a “venue for China to get zero-days,” say experts

In March 2017, a group of hackers from China arrived in Vancouver with one goal: Find hidden weak spots inside the world’s most popular technologies.

Google’s Chrome browser, Microsoft’s Windows operating system, and Apple’s iPhones were all in the crosshairs. But no one was breaking the law. These were just some of the people taking part in Pwn2Own, one of the world’s most prestigious hacking competitions.

It was the 10th anniversary for Pwn2Own, a contest that draws elite hackers from around the globe with the lure of big cash prizes if they manage to exploit previously undiscovered software vulnerabilities, known as “zero-days.” Once a flaw is found, the details are handed over to the companies involved, giving them time to fix it. The hacker, meanwhile, walks away with a financial reward and eternal bragging rights.

For years, Chinese hackers were the most dominant forces at events like Pwn2Own, earning millions of dollars in prizes and establishing themselves among the elite. But in 2017, that all stopped.

> One of China's elite hacked an iPhone…. Virtually overnight, Chinese intelligence used it as a weapon against a besieged minority ethnic group, striking before Apple could fix the problem. It was a brazen act performed in broad daylight.

In an unexpected statement, the billionaire founder and CEO of the Chinese cybersecurity giant Qihoo 360—one of the most important technology firms in China—publicly criticized Chinese citizens who went overseas to take part in hacking competitions. In an interview with the Chinese news site Sina, Zhou Hongyi said that performing well in such events represented merely an "imaginary" success. Zhou warned that once Chinese hackers show off vulnerabilities at overseas competitions, they can "no longer be used." Instead, he argued, the hackers and their knowledge should "stay in China" so that they could recognize the true importance and "strategic value" of the software vulnerabilities.

Beijing agreed. Soon, the Chinese government banned cybersecurity researchers from attending overseas hacking competitions. Just months later, a new competition popped up inside China to take the place of the international contests. The Tianfu Cup, as it was called, offered prizes that added up to over a million dollars.

The inaugural event was held in November 2018. The $200,000 top prize went to Qihoo 360 researcher Qixun Zhao, who showed off a remarkable chain of exploits that allowed him to easily and reliably take control of even the newest and most up-to-date iPhones. From a starting point within the Safari web browser, he found a weakness in the core of the iPhones operating system, its kernel. The result? A remote attacker could take over any iPhone that visited a web page containing Qixun's malicious code. It's the kind of hack that can potentially be sold for millions of dollars on the open market to give criminals or governments the ability to spy on large numbers of people. Qixun named it "Chaos."

Two months later, in January 2019, Apple issued an update that fixed the flaw. There was little fanfare—just a quick note of thanks to those who discovered it.

But in August of that year, Google published an extraordinary analysis into a hacking campaign it said was "exploiting iPhones en masse." Researchers dissected five distinct exploit chains they'd spotted "in the wild." These included the exploit that won Qixun the top prize at Tianfu, which they said had also been discovered by an unnamed "attacker."

The Google researchers pointed out similarities between the attacks they caught being used in the real world and Chaos. What their deep dive omitted, however, were the identities of the victims and the attackers: Uyghur Muslims and the Chinese government.

A campaign of oppression

For the past seven years, China has committed human rights abuses against the Uyghur people and other minority groups in the Western province of Xinjiang. Well-documented aspects of the campaign include detention camps, systematic compulsory sterilization, organized torture and rape, forced labor, and an unparalleled surveillance effort. Officials in

Beijing argue that China is acting to fight “terrorism and extremism,” but the United States, among other countries, has called the actions genocide. The abuses add up to an unprecedented high-tech campaign of oppression that dominates Uyghur lives, relying in part on targeted hacking campaigns.

China’s hacking of Uyghurs is so aggressive that it is effectively global, extending far beyond the country’s own borders. It targets journalists, dissidents, and anyone who raises Beijing’s suspicions of insufficient loyalty.

Shortly after Google’s researchers noted the attacks, media reports connected the dots: the targets of the campaign that used the Chaos exploit were the Uyghur people, and the hackers were linked to the Chinese government. Apple published a rare blog post that confirmed the attack had taken place over two months: that is, the period beginning immediately after Qixun won the Tianfu Cup and stretching until Apple issued the fix.

Related Story

Apple says China’s Uighur Muslims were targeted in the recent iPhone hacking campaign

The tech giant gave a rare statement that bristled at Google’s analysis of the novel hacking operation.

MIT Technology Review has learned that United States government surveillance independently spotted the Chaos exploit being used against Uyghurs, and informed Apple. (Both Apple and Google declined to comment on this story.)

The Americans concluded that the Chinese essentially followed the “strategic value” plan laid out by Qihoo’s Zhou Hongyi; that the Tianfu Cup had generated an important hack; and that the exploit had been quickly handed over to Chinese intelligence, which then used it to spy on Uyghurs.

The US collected the full details of the exploit used to hack the Uyghurs, and it matched Tianfu’s Chaos hack, MIT Technology Review has learned. (Google’s in-depth examination later noted how structurally similar the exploits are.) The US quietly informed Apple, which had already been tracking the attack on its own and reached the same conclusion: the Tianfu hack and the Uyghur hack were one and the same. The company prioritized a difficult fix.

Qihoo 360 and Tianfu Cup did not respond to multiple requests for comment. When we contacted Qixun Zhao via Twitter, he strongly denied involvement, although he also said he couldn’t remember who came into possession of the exploit code. At first, he suggested the exploit wielded against Uyghurs was probably used “after the patch release.” On the contrary, both Google and Apple have extensively documented how this exploit was used before January 2019. He also pointed out that his ‘Chaos’ exploit shared code from other hackers. In fact, within Apple and US intelligence, the conclusion has long been that these exploits are not merely similar—they are the same. Although Qixun wrote the exploit, there is nothing to suggest he was personally involved in what happened to it after the Tianfu event (Chinese law requires citizens and organizations to provide support and assistance to the country’s intelligence agencies whenever asked.)

By the time the vulnerabilities were closed, Tianfu had achieved its goal.

“The original decision to not to allow the hackers to go abroad to competitions seems to be motivated by a desire to keep discovered vulnerabilities inside of China,” says Adam Segal, an expert on Chinese cybersecurity policy at the Council for Foreign Relations. It also cut top Chinese hackers from other income sources “so they are forced into a closer connection with the state and established companies,” he says.

The incident is stark. One of China’s elite hacked an iPhone, and won public acclaim and a large amount of money for doing so. Virtually overnight, Chinese intelligence used it as a weapon against a besieged minority ethnic group, striking before Apple could fix the problem. It was a brazen act performed in broad daylight and with the knowledge that there would be no consequences to speak of.

Concerning links

Today, the Tianfu Cup is heading into its third year, and it's sponsored by some of China's biggest tech companies: Alibaba, Baidu, and Qihoo 360 are among the organizers. But American officials and security experts are increasingly concerned about the links between those involved in the competition and the Chinese military.

Qihoo, which is valued at over $9 billion, was one of dozens of Chinese companies added to a trade blacklist by the United States in 2020 after a US Department of Commerce assessment that the company might support Chinese military activity.

Others involved in the event have also raised alarms in Washington. The Beijing company Topsec, which helps organize Tianfu, allegedly provides hacking training, services, and recruitment for the government and has employed nationalist hackers, according to US officials.

The company is linked to cyber-espionage campaigns including the 2015 hack of the US insurance giant Anthem, a connection that was accidentally exposed when hackers used the same server to try to break into a US military contractor and to host a Chinese university hacking competition.

Related Story

Hackers are finding ways to hide inside Apple's walled garden

The iPhone's locked-down approach to security is spreading, but advanced hackers have found that higher barriers are great for avoiding capture.

Other organizers and sponsors include NSFocus, which grew directly out of the earliest Chinese nationalist hacker movement called the Green Army, and Venus Tech, a prolific Chinese military contractor that has been linked to offensive hacking.

One other Tianfu organizer, the state-owned Chinese Electronics Technology Group, has a surveillance subsidiary called Hikvision, which provides "Uyghur analytics" and facial recognition tools to the Chinese government. It was added to a US trade blacklist in 2019.

US experts say the links between the event and Chinese intelligence are clear, however.

"I think it is not only a venue for China to get zero-days but it's also a big recruiting venue," says Scott Henderson, an analyst on the cyber espionage team at FireEye, a major security company based in California.

Tianfu's links to Uyghur surveillance and genocide show that getting early access to bugs can be a powerful weapon. In fact, the "reckless" hacking spree that Chinese groups launched against Microsoft Exchange in early 2021 bears some striking similarities.

In that case, a Taiwanese researcher uncovered the security flaws and passed them to Microsoft, which then privately shared them with security partners. But before a fix could be released, Chinese hacking groups started exploiting the flaw all around the world. Microsoft, which was forced to rush out a fix two weeks earlier than planned, is investigating the potential that the bug was leaked.

These bugs are incredibly valuable, not just in financial terms, but in their capacity to create an open window for espionage and oppression.

Google researcher Ian Beer said as much in the original report detailing the exploit chain. "I shan't get into a discussion of whether these exploits cost $1 million, $2 million, or $20 million," he wrote. "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."