Google shuts down a hacking operation being conducted by ally of the US government

Kevin Reed
30 March 2021

Two of Google's anti-hacking teams uncovered and unilaterally took down a malware distribution operation that was being run by an undisclosed US ally, according to a report last Friday in *MIT Technology Review*.

The report, written by the publication's cybersecurity senior editor Patrick Howell O'Neill, says that the Google teams—Project Zero and Threat Analysis Group—"caught an unexpectedly big fish recently: an 'expert' hacking group exploiting 11 powerful vulnerabilities to compromise devices running iOS, Android, and Windows."

O'Neill also wrote that *MIT Tech Review* "has learned that the hackers in question were actually Western government operatives actively conducting a counterterrorism operation" and that Google's decision to shut down and publicly expose the hack caused internal divisions and "raised questions inside the intelligence communities of the United States and its allies."

Google's Project Zero specializes in finding what are known among cybersecurity experts as zero-day vulnerabilities, i.e., flaws in software that developers are aware of but have not yet been able to fix. These unintended weaknesses are called zero-day because they can be exploited by cybercriminals and hackers while developers have "zero days" to patch the software.

According to Google's website, the Threat Analysis Group is responsible for countering targeted and government-backed hacking against the company's products and users. Much of TAG's previous actions have been taken against "influence operations" reported to have government backing from North Korea, Russia or China, for example.

The hacks in question were discovered by Google's teams as far back as February 2020 and were reported on in a blog post published by Project Zero on March 18. The post entitled, "In-the-Wild Series: October 2020 0-day discovery," detailed seven instances of zero-day exploits within Apple, Google and Samsung browsers running on iOS, Windows and Android operating systems.

The malware was delivered using mechanisms referred to as "watering hole" attacks, which pointed a handful of websites to two exploit servers that hosted the malware for each of the operating systems. The attack name is derived from predators in the natural world who wait around watering holes to attack their prey.

In his *MIT Tech Review* story, O'Neill explains that Google omitted details, such as specifically what country was responsible and who was targeted, as well as "important technical information on the malware or the domains used in the operation." He also said that these kinds of details would typically be made available to the public, but in this case, they were withheld.

While it is not unusual for cybersecurity firms to shut down exploits being used by "friendly governments," it is rare that the action is made public. As O'Neill points out, this was the source of the internal conflict over the disclosure by Google, with some employees arguing "that counterterrorism missions ought to be out of bounds of public disclosure" and others believing "the company was entirely within its rights, and that the announcement serves to protect users and make the internet more secure."

While Project Zero does not research the source or national origin of the exploits it finds, this is a regular part of the TAG's reporting. O'Neill says, "Google omitted many more details than just the name of the government behind the hacks, and through that

information, the teams knew internally who the hacker and targets were. It is not clear whether Google gave advance notice to government officials that they would be publicizing and shutting down the method of attack."

O'Neill interviewed an unnamed former US intelligence official, who sought to justify the hacking operation, saying, "There are certain hallmarks in Western operations that are not present in other entities … you can see it translate down into the code. And this is where I think one of the key ethical dimensions comes in. How one treats intelligence activity or law enforcement activity driven under democratic oversight within a lawfully elected representative government is very different from that of an authoritarian regime."

In other words, when the Russians or the Chinese are blamed for hacking, it is illegal, but when the US and its allies engage in cyberwarfare, it is permitted because "oversight is baked into Western operations at the technical, tradecraft, and procedure level."

However, anyone familiar with the mass surveillance operations of the National Security Agency (NSA) exposed by Edward Snowden in 2013—which were built upon sophisticated hacking and malware implementations—knows that the US government and its "Five Eyes" allies have no problem "baking in" hacking and spying operations that dispense entirely with fundamental democratic rights. The "Five Eyes" intelligence alliance is made up of the US, the United Kingdom, Canada, Australia and New Zealand.

This is not the first time a tech firm inserted itself into a US-related cyberintelligence operation. In 2018 the Moscow-based global cybersecurity company Kaspersky Lab exposed an active US-counterterrorism operation it called "Slingshot" that had penetrated thousands of devices in Africa and the Middle East. Although Kaspersky did not attribute Slingshot to a country or government, US intelligence officers later admitted that the program had been run by the US military for six years, and the highly intrusive malware could "siphon large amounts of data from infected devices."

The Kaspersky exposure caused the US military to abandon the program—reportedly used to locate and monitor the activity of ISIS and al-Qaeda targets—and "burn" some of the digital infrastructure that the Pentagon Special Operations Command was using to manage the surveillance operation. This and several other developments led to Kaspersky Lab being placed on a list of organizations that pose a national security risk to the US.

While *MIT Tech Review* defended Google's exposure on the grounds that the company has an obligation to customers to protect them from hacking, it also studiously avoided pointing a finger at the specific "Western government" engaged in the malware operation. O'Neill declared that "some argue that counterterrorism operations are different, with potentially life-and-death consequences that go beyond day-to-day internet security."

In any case, the exposure by Google of a nine-month-long hacking operation by a global state partner of US imperialism—regardless of the limitations of the information that has been disclosed—indicates that there are employees within the giant tech company who want these activities stopped and publicly exposed.

This development takes place in the context of growing political activism within the tech corporations, including staff opposition at Google in 2018 which ended the Pentagon artificial intelligence-related technologies contract used for warfare purposes called Project Maven.