Google’s top security teams unilaterally shut down a counterterrorism operation

technologyreview.com/2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally/

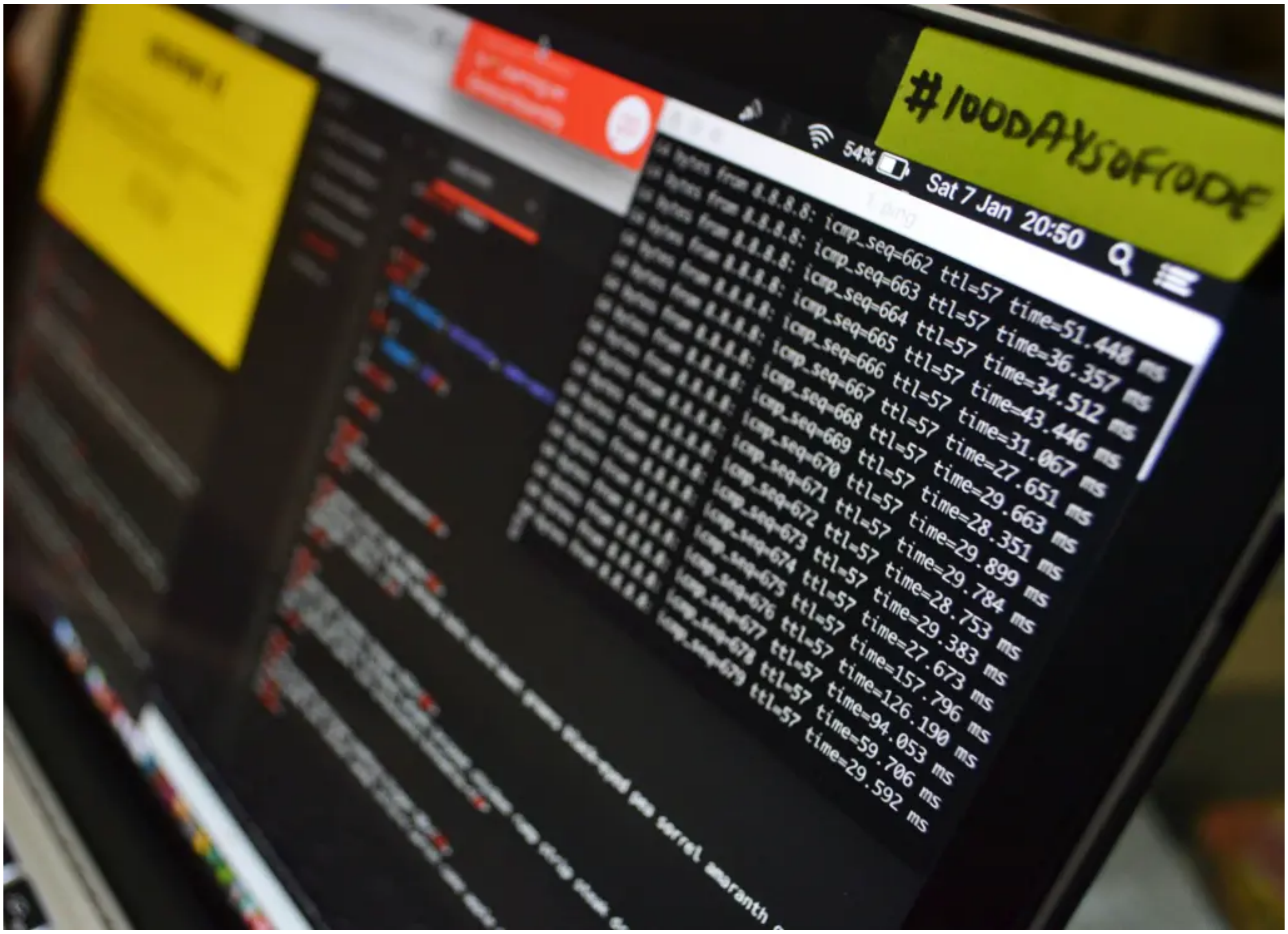
Patrick Howell O'Neill

- Google’s security teams publicly exposed a nine-month hacking operation
- What wasn’t disclosed: The move shut down an active counter-terrorist operation being conducted by a Western government
- The decision has raised alarms inside Google and elsewhere

Google runs some of the most venerated cybersecurity operations on the planet: its Project Zero team, for example, finds powerful undiscovered security vulnerabilities, while its Threat Analysis Group directly counters hacking backed by governments, including North Korea, China, and Russia. And those two teams caught an unexpectedly big fish recently: an “expert” hacking group exploiting 11 powerful vulnerabilities to compromise devices running iOS, Android, and Windows.

But MIT Technology Review has learned that the hackers in question were actually Western government operatives actively conducting a counterterrorism operation. The company’s decision to stop and publicize the attack caused internal division at Google and raised questions inside the intelligence communities of the United States and its allies.

Related Story



```
icmp_seq=662 ttl=57 time=51.448 ms
icmp_seq=663 ttl=57 time=36.357 ms
icmp_seq=664 ttl=57 time=34.512 ms
icmp_seq=665 ttl=57 time=43.446 ms
icmp_seq=666 ttl=57 time=31.067 ms
icmp_seq=667 ttl=57 time=27.651 ms
icmp_seq=668 ttl=57 time=29.663 ms
icmp_seq=669 ttl=57 time=28.351 ms
icmp_seq=670 ttl=57 time=29.899 ms
icmp_seq=671 ttl=57 time=29.784 ms
icmp_seq=672 ttl=57 time=28.753 ms
icmp_seq=673 ttl=57 time=29.383 ms
icmp_seq=674 ttl=57 time=27.673 ms
icmp_seq=675 ttl=57 time=157.796 ms
icmp_seq=676 ttl=57 time=126.190 ms
icmp_seq=677 ttl=57 time=94.053 ms
icmp_seq=678 ttl=57 time=59.706 ms
icmp_seq=679 ttl=57 time=29.592 ms
```

Google says it's too easy for hackers to find new security flaws

Attackers are exploiting the same types of software vulnerabilities over and over again, because companies often miss the forest for the trees.

A pair of recent Google blog posts detail the collection of zero-day vulnerabilities that it discovered hackers using over the course of nine months. The exploits, which went back to early 2020 and used never-before-seen techniques, were "watering hole" attacks that used infected websites to deliver malware to visitors. They caught the attention of cybersecurity experts thanks to their scale, sophistication, and speed.

Google's announcement glaringly omitted key details, however, including who was responsible for the hacking and who was being targeted, as well as important technical information on the malware or the domains used in the operation. At least some of that information would typically be made public in some way, leading one security expert to criticize the report as a "dark hole."

"Different ethical questions"

Security companies regularly shut down exploits that are being used by friendly governments, but such actions are rarely made public. In response to this incident, some Google employees have argued that counterterrorism missions ought to be out of bounds of public disclosure; others believe the company was entirely within its rights, and that the announcement serves to protect users and make the internet more secure.

“Project Zero is dedicated to finding and patching 0-day vulnerabilities, and posting technical research designed to advance the understanding of novel security vulnerabilities and exploitation techniques across the research community,” a Google spokesperson said in a statement. “We believe sharing this research leads to better defensive strategies and increases security for everyone. We don’t perform attribution as part of this research.”

It’s true that Project Zero does not formally attribute hacking to specific groups. But the Threat Analysis Group, which also worked on the project, does perform attribution. 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.

But Western operations are recognizable, according to one former senior US intelligence official.

“There are certain hallmarks in Western operations that are not present in other entities … you can see it translate down into the code,” said the former official, who is not authorized to comment on operations and spoke on condition of anonymity. “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.”

> “There are certain hallmarks in Western operations that are not present in other entities … you can see it translate down into the code.”

“The oversight is baked into Western operations at the technical, tradecraft, and procedure level,” they added.

Google found the hacking group exploiting 11 zero-day vulnerabilities in just nine months, a high number of exploits over a short period. Software that was attacked included the Safari browser on iPhones but also many Google products, including the Chrome browser on Android phones and Windows computers.

But the conclusion within Google was that who was hacking and why is never as important as the security flaws themselves. Earlier this year, Project Zero’s Maddie Stone argued that it is too easy for hackers to find and use powerful zero-day vulnerabilities and that her team faces an uphill battle detecting their use.

Instead of focusing on who was behind and targeted by a specific operation, Google decided to take broader action for everyone. The justification was that even if a Western government was the one exploiting those vulnerabilities today, it will eventually be used by others, and so the right choice is always to fix the flaw today.

"It's not their job to figure out"

This is far from the first time a Western cybersecurity team has caught hackers from allied countries. Some companies, however, have a quiet policy of not publicly exposing such hacking operations if both the security team and the hackers are considered friendly—for example, if they are members of the "Five Eyes" intelligence alliance, which is made up of the United States, the United Kingdom, Canada, Australia, and New Zealand. Several members of Google's security teams are veterans of Western intelligence agencies, and some have conducted hacking campaigns for these governments.

In some cases, security companies will clean up so-called "friendly" malware but avoid going public with it.

"They typically don't attribute US-based operations," says Sasha Romanosky, a former Pentagon official who published recent research into private-sector cybersecurity investigations. "They told us they specifically step away. It's not their job to figure out; they politely move aside. That's not unexpected."

While the Google situation is in some ways unusual, there have been somewhat similar cases in the past. The Russian cybersecurity firm Kaspersky came under fire in 2018 when it exposed an American-led counterterrorism cyber operation against ISIS and Al Qaeda members in the Middle East. Kaspersky, like Google, did not explicitly attribute the threat but nevertheless exposed it and rendered it useless, American officials said, which caused the operatives to lose access to a valuable surveillance program and even put the lives of soldiers on the ground at risk.

Kaspersky was already under heavy criticism for its relationship with the Russian government at the time, and the company was ultimately banned from US government systems. It has always denied having any special relationship with the Kremlin.

Google has found itself in similar water before, too. In 2019, the company released research on what may have been an American hacking group, although specific attribution was never made. But that research was about a historical operation. Google's recent announcements, however, put the spotlight on what had been a live cyber-espionage operation.

Who's being protected?

The alarms raised both inside government and at Google show the company is in a difficult position.

Google security teams have a responsibility to the company's customers, and it is widely expected that they will do their utmost to protect the products—and therefore users—who are under attack. In this incident, it's notable that the techniques used affected not just

Google products like Chrome and Android, but also iPhones.

While different teams draw their own lines, Project Zero has made its name by tackling critical vulnerabilities all over the internet, not just those found in Google's products.

Related Story

The NSA found a dangerous flaw in Windows and told Microsoft to fix it

The secretive security agency identified the vulnerability and is taking public credit as part of an effort to "build trust."

"Each step we take towards making 0-day hard, makes all of us safer," tweeted Maddie Stone, one of the most highly respected members of the security team, when the latest research was published.

But while protecting customers from attack is important, some argue that counterterrorism operations are different, with potentially life-and-death consequences that go beyond day-to-day internet security.

When state-backed hackers in Western nations find cybersecurity flaws, there are established methods for working out the potential costs and benefits of disclosing the security gap to the company that is affected. In the United States it's called the "vulnerabilities equities process." Critics worry that US intelligence hoards large numbers of exploits, but the American system is more formal, transparent, and expansive than what’s done in almost every other country on earth, including Western allies. The process is meant to allow government officials to balance the advantages of keeping flaws secret in order to use them for intelligence purposes with the wider benefits of telling a tech company about a weakness in order to have it fixed.

> “The level of oversight even in Western democracies about what their national security agencies are actually doing is, in many cases, a lot less than we have in the United States.”

Last year the NSA made the unusual move to take credit for revealing an old flaw in Microsoft Windows. That kind of report from government to industry is normally kept anonymous and often secret.

But even though the American intelligence system’s disclosure process can be opaque, similar processes in other Western nations are often smaller, more secretive, or simply informal and therefore easy to bypass.

“The level of oversight even in Western democracies about what their national security agencies are actually doing is, in many cases, a lot less than we have in the United States,” says Michael Daniel, who was White House cybersecurity coordinator for the Obama administration.

“The degree of parliamentary oversight is much less. These countries do not have the robust inter-agency processes the US has. I’m not normally one to brag about the US—we’ve got a lot of problems—but this is one area where we have robust processes that other Western democracies just don’t.”

The fact that the hacking group hit by the Google investigation possessed and used so many zero-day vulnerabilities so rapidly could indicate a problematic imbalance. But some observers worry about live counterterrorism cyberoperations being shut down at potentially decisive moments without the ability to quickly start up again.

“US allies don’t all have the ability to regenerate entire operations as quickly as some other players,” the former senior US intelligence official said. Worries about suddenly losing access to an exploit capability or being spotted by a target are particularly high for counterterrorism missions, especially during “periods of incredible exposure” when a lot of exploitation is taking place, the official explained. Google’s ability to shut down such an operation is likely to be the source of more conflict.

“This is still something that hasn’t been well addressed,” the official said. “The idea that someone like Google can destroy that much capability that quickly is slowly dawning on folks.”