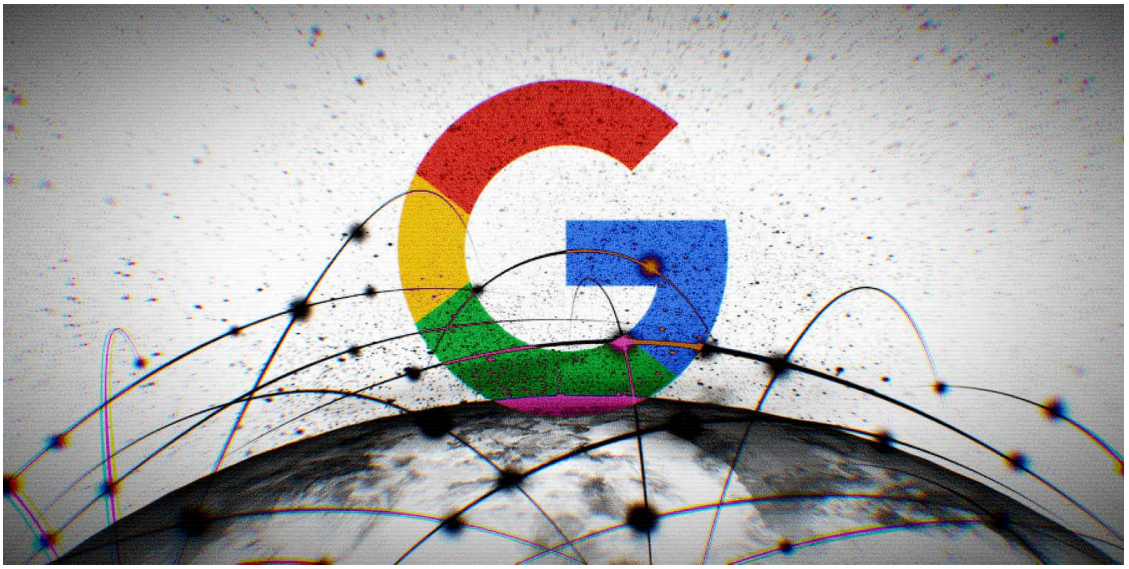
Google warned users of 33,000 state-sponsored attacks in 2020

By Sergiu Gatlan

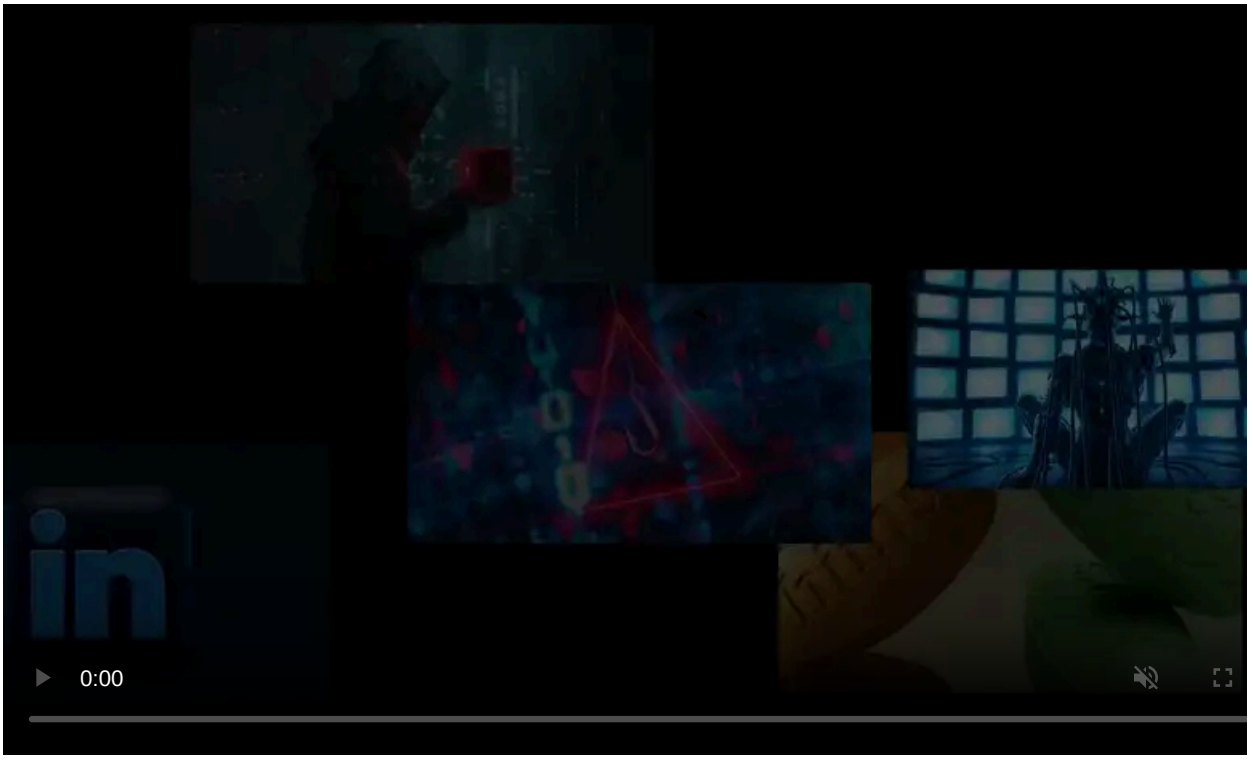
Published: 2020-10-16 · Archived: 2026-04-05 17:28:44 UTC

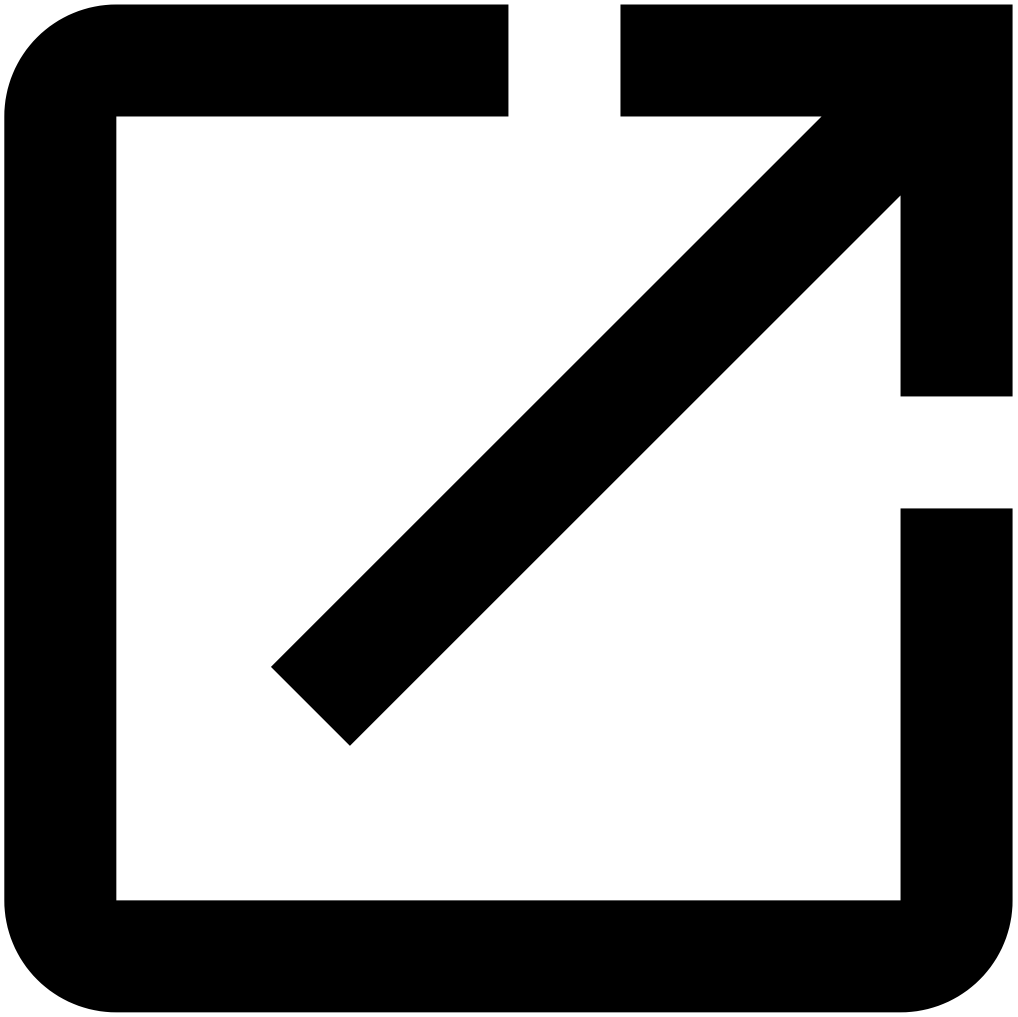


Google delivered over 33,000 alerts to its users during the first three quarters of 2020 to warn them of state-sponsored phishing attacks targeting their accounts.

"In these cases, we also shared our findings with the campaigns and the Federal Bureau of Investigation," Shane Huntley, Director at Google's Threat Analysis Group (TAG), said.

The prominent reminders sent to Google users targeted in government-backed attacks were displayed even when the hacking attempts were blocked to inform them of the danger.


0:00



Google also notifies the users' G Suite administrators to raise awareness of the risk their corporate network is facing to provide them with an early warning of a potential attack.

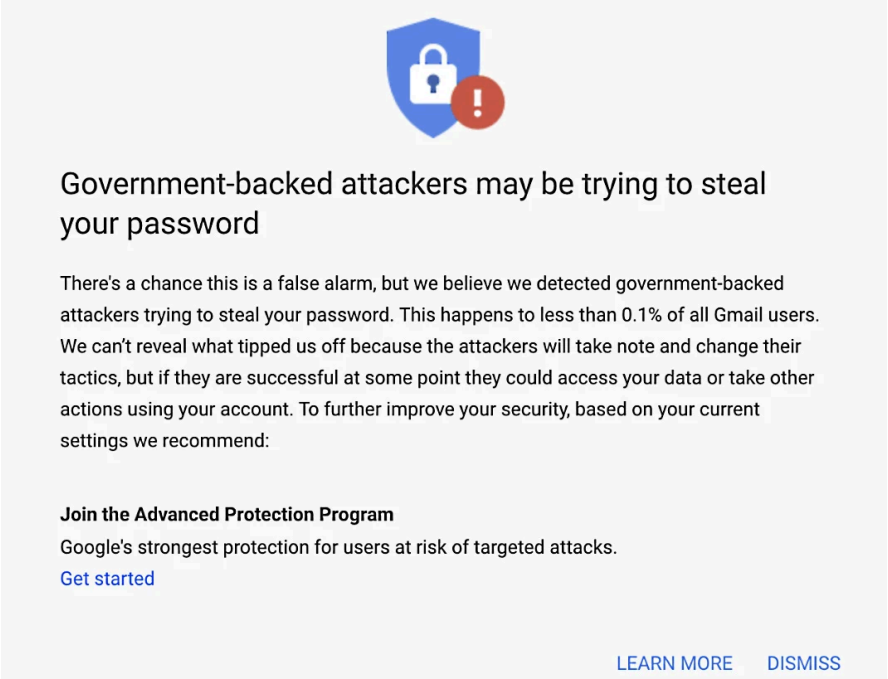


Image: Google

These notifications are shown to up to 0.1% of all Gmail users according to Google, who advises them to take several measures to secure their accounts.

These include enrolling in the Advanced Protection Program, keeping software up to date, enabling Gmail 2-step verification, as well as using Google Authenticator and/or a physical security key for 2-step verification.

In all, Google sent 33,015 government-backed phishing warnings in 2020 until now, with 11,856 alerts sent during Q1 2020, 11,023 in Q2 2020, and 10,136 in Q3 2020.

In March, Google said that it delivered around 40,000 alerts of state-sponsored phishing or malware hacking attempts during 2019, with a 25% drop compared to 2018.

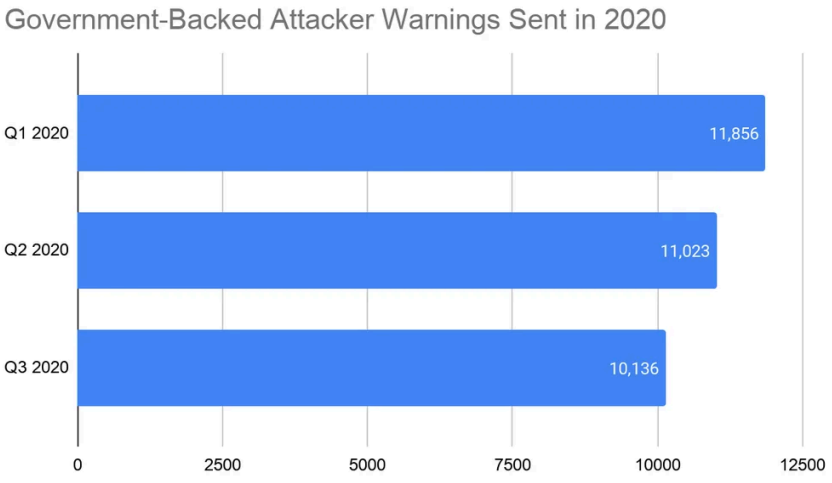


Image: Google

Last month, Microsoft also reported that it observed nation state-sponsored hacking groups operating from Russia, China, and Iran actively targeting individuals and organizations involved in the 2020 US presidential elections.

"We have directly notified those who were targeted or compromised so they can take action to protect themselves," Microsoft said at the time.

One of the groups behind the attack tracked by Microsoft, the Chinese-backed APT31, was also detected by Google while targeting "campaign staffers' personal emails with credential phishing emails and emails containing tracking links."

APT31 also hosted malware payloads that used Dropbox for command and control comms, as well as delivering fake McAfee Total Protection installers onto victims' computers to deploy malware in the background.

North Korean APTs were also observed by Google while switching targets to focus on "COVID-19 researchers and pharmaceutical companies."

The Google and Microsoft reports confirm intelligence shared by the US government on Russian, Iranian, and Chinese hacking groups attempting to "compromise the private communications of U.S. political campaigns, candidates and other political targets."

Today, Google also disclosed that in 2017 a nation-state actor targeted thousands of Google IP addresses in the largest DDoS attack ever, amounting to more than 2.54 terabits per second.

Source: https://www.bleepingcomputer.com/news/security/google-warned-users-of-33-000-state-sponsored-attacks-in-2020/