Google notifies 14,000 Gmail users of targeted APT28 attacks

therecord.media/google-notifies-14000-gmail-users-of-targeted-apt28-attacks/

October 7, 2021

Google has sent email notifications to more than 14,000 Gmail users that they've been the target of a spear-phishing attack orchestrated by a state-sponsored hacking group.

"In late September, we detected an APT28 phishing campaign targeting a large volume of Gmail users (approx 14,000) across a wide variety of industries," Shane Huntley, Director of Google's Threat Analysis Group, told *The Record* in an email, following an inquiry about the number of users who took to social media to post the message they received from Google.

> nuclear shitposting so good that a foreign government wants to read my emails pic.twitter.com/logtz5Z0GL
>
> — Katie Mummah (@nuclearkatie) October 6, 2021

> Huh. I've had security warnings before, but this one just came to me hours after a similar Google alert to my @theatlantic colleague @JamesFallows. Both of us already use Advanced Protection. https://t.co/UptU2rrVIr pic.twitter.com/lk2JTrBLh5
>
> — Barton Gellman (@bartongellman) October 7, 2021

"This particular campaign comprised 86% of the batch of warnings we sent for this month," Huntley added.

“Firstly these warnings indicate targeting NOT compromise. If we are warning you there’s a very high chance we blocked,” Huntley said in a separate Twitter thread.

“If you are an activist/journalist/government official or work in NatSec, this warning honestly shouldn’t be a surprise.

“At some point, some government-backed entity probably will try to send you something,” he added while urging users to review account security settings,” he added.

Huntley, who leads the TAG team, a Google security division focused on hunting apex threat actors, said they blocked all the emails sent by the APT28 group in this campaign.

Tracked as **APT28**, but also more commonly known as **Fancy Bear**, the FBI and NSA linked this group earlier this summer to Russia’s military intelligence apparatus—and in particular to the **Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165**.

APT28 has been one of the most active threat actors over the past decade, and the group has often relied on spear-phishing emails to go after targets of interest. Their aim is to breach inboxes, get access to sensitive documents and communications, and then pivot to other individuals or internal networks.

“If you received a warning or are a high-risk user, journalist, politician, celebrity, or CEO, we recommend you enroll in the Advanced Protection Program for work and personal emails,” Huntley said in an email, promoting a Google program meant to add and activate additional security protections to high-risk accounts.

The warnings sent out this week are not a new Gmail feature. Google has been sending alerts about attacks carried out by state-sponsored entities since 2012.

Tags

- APT28
- Fancy Bear
- Gmail
- Google
- Google TAG
- nation-state
- phishing

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against

hackers.