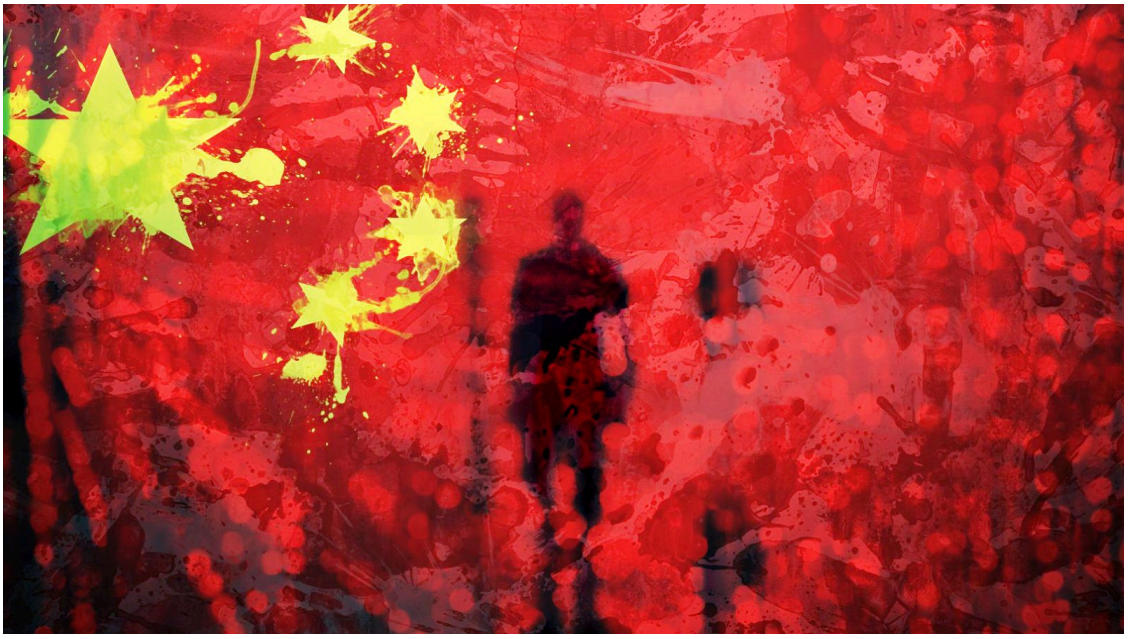
Google: Chinese hackers target Gmail users affiliated with US govt

By Sergiu Gatlan

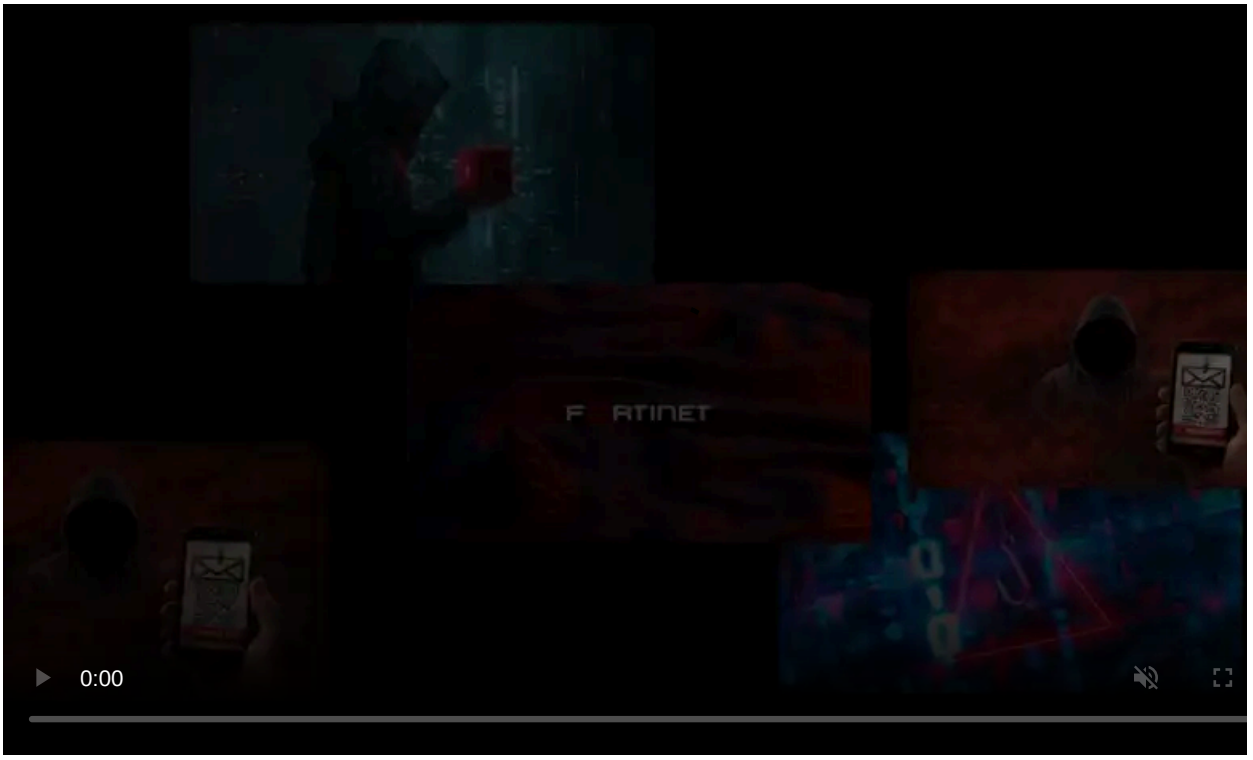
Published: 2022-03-08 · Archived: 2026-04-05 21:21:53 UTC

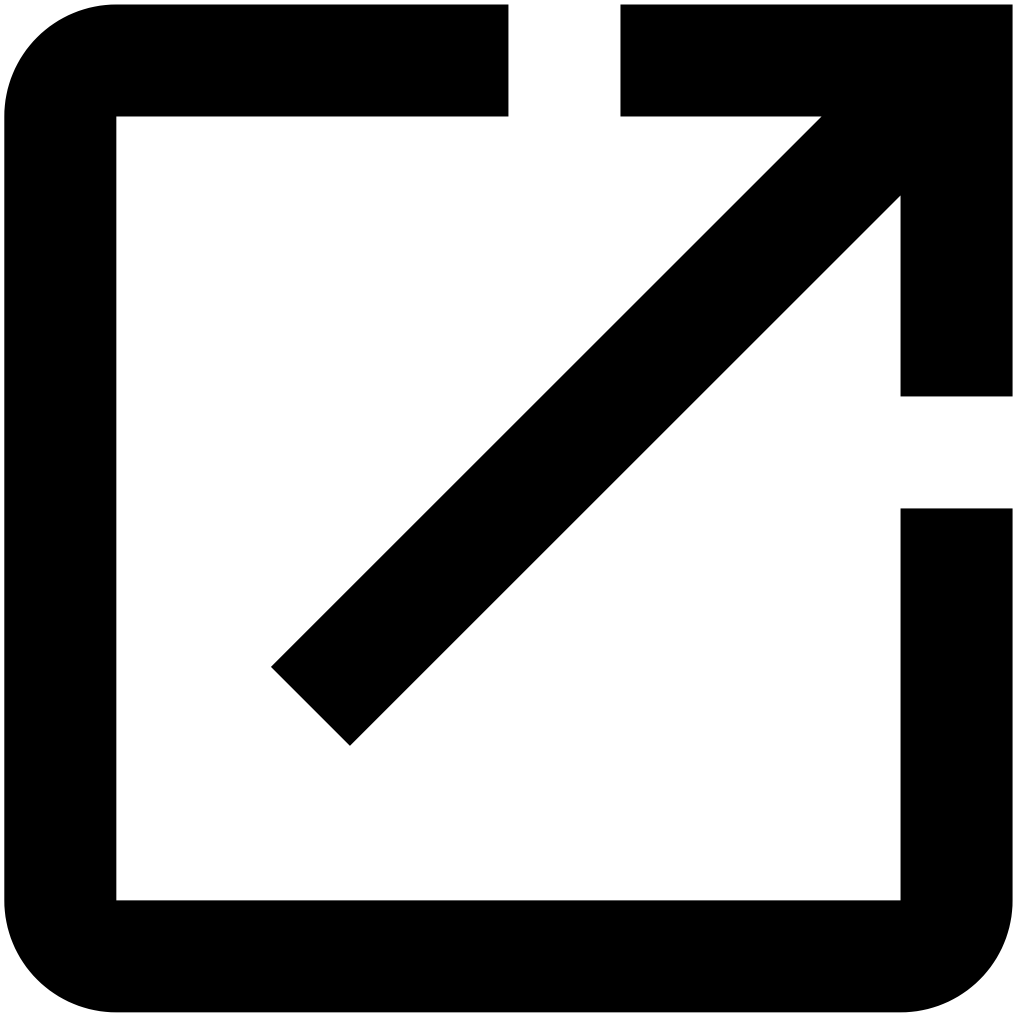


Google's Threat Analysis Group has warned multiple Gmail users that they were targeted in phishing attacks conducted by a Chinese-backed hacking group tracked as APT31.

The warnings came after Gmail's defenses automatically blocked all these phishing emails after tagging them as spam.

"In February, we detected an APT31 phishing campaign targeting high profile Gmail users affiliated with the U.S. government," Google Threat Analysis Group's Director Shane Huntley revealed today.


F RTINET
0:00



"Today, we sent those people who were targeted government backed attacker warnings. We don't have any evidence to suggest that this campaign was related to the current war in Ukraine."

In October, Google TAG security engineer Ajax Bash said the company sent roughly 50,000 alerts of state-sponsored hacking or phishing attempts to customers throughout 2021, 15,000 of them linked to the APT28 threat group part of Russia's General Staff Main Intelligence Directorate (GRU).

Google sends government-backed attack alerts when detecting attacks launched using infrastructure linked to known government-sponsored threat groups.

The company has warned its users of such attacks starting with 2012 and redesigned the alert system in 2017, revamping it with added info on the potential attack vector.

On Monday, Google TAG also said Russian, Belarusian, and Chinese threat actors targeted Ukrainian and European government and military orgs in widespread phishing campaigns and DDoS attacks.

"Over the past two weeks, TAG has observed activity from a range of threat actors that we regularly monitor and are well-known to law enforcement, including FancyBear and Ghostwriter," Huntley said in the report.

China-sponsored hacking group Mustang Panda (aka Temp.Hex and TA416) switched to phishing attacks against European entities using lures related to the Ukrainian invasion.

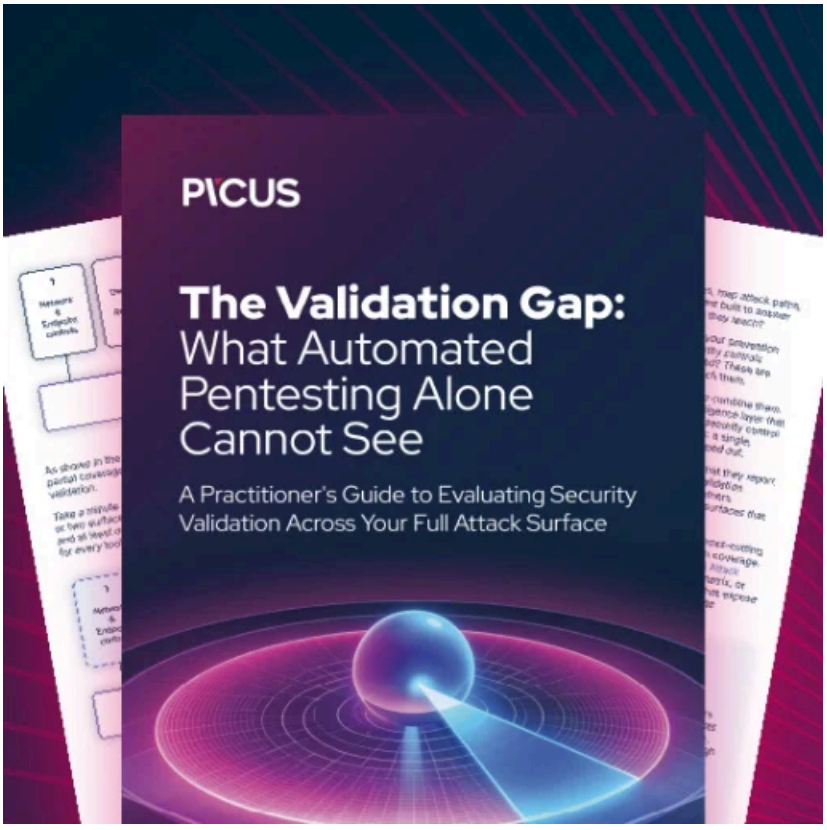
Proofpoint also revealed this week that Mustang Panda is phishing "European diplomatic entities, including an individual involved in refugee and migrant services."

APT31 (also tracked as Judgment Panda and Zirconium) is a hacking group working for the Chinese Government and known for its numerous espionage and information theft operations targeting organizations worldwide.

It has been linked in the past with the theft and repurposing of the EpMe NSA exploit, years before Shadow Brokers leaked it in April 2017.

Microsoft previously observed APT31 attacks targeting high-profile individuals associated with the Joe Biden presidential campaign.

This hacking group was also detected by Google while targeting "campaign staffers' personal emails with credential phishing emails and emails containing tracking links."



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/google-chinese-hackers-target-gmail-users-affiliated-with-us-govt/