The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russian SolarWinds Hackers Target 150 Organizations in New Attack

By Rob Lever for AFP

May 28, 2021



The SolarWinds attack has been connected to Russian state-backed hackers. **Christopher Schirner / Flickr (CC BY-SA 2.0)**

The state-backed Russian group behind a massive hacking campaign revealed last year has re-emerged with a series of attacks on government agencies, think tanks, consultants and other organizations, according to officials and researchers.

A security update from Microsoft late Thursday said the group known as Nobelium has stepped up attacks, notably targeting government agencies involved in foreign policy as part of intelligence gathering efforts.

The U.S. government's Cybersecurity and Infrastructure Security Agency posted a link to the Microsoft update and urged computer network administrators to "apply the necessary mitigations."

Microsoft said it detected a "sophisticated" and large-scale campaign that delivered phishing emails delivering malicious software and enabling the hackers to get protected data from victims.

Related article: Russia 'Likely' Behind SolarWinds Hack – U.S. Intelligence Agencies

"This wave of attacks targeted approximately 3,000 email accounts at more than 150 different organizations," Microsoft vice president Tom Burt said in a blog post.

The news comes a month after Washington imposed sanctions and expelled Russian diplomats in response to Moscow's involvement in the massive attacks last year on SolarWinds, a security software firm, as well as for election interference and other hostile activity.

"When coupled with the attack on SolarWinds, it's clear that part of Nobelium's playbook is to gain access to trusted technology providers and infect their customers," wrote Burt.

"By piggybacking on software updates and now mass email providers, Nobelium increases the chances of collateral damage in espionage operations and undermines trust in the technology ecosystem."

The new attacks enabled the hackers were able to gain access to email servers operated by the firm Constant Contact to be able spoof to the U.S. Agency for International Development and send out mass emails with disinformation, according to the update.

In one example, emails appearing to be from USAID showed a "special alert" stating that "Donald Trump has published new documents on election fraud."

Users who clicked on the link were directed to a site delivering malicious software and enabling the hackers to exfiltrate data, according to Microsoft.

Attack is ongoing

"This attack is still active, so these indicators should not be considered exhaustive for this observed activity," Microsoft said in its update.

The security firm Volexity, which also published research on the hacking, said it appears "the attacker is likely having some success in breaching targets."

The security firm said in a blog post: "While Volexity cannot say with certainty who is behind these attacks, it does believe it has the earmarks of a known threat actor it has dealt with on several previous occasions," citing a Russian-based hacker group.

John Dickson of the security firm Denim Group said the latest attacks suggest the sanctions imposed by Washington are insufficient.

"I think the sanctions were a starting point and we need to ratchet them up," Dickson told AFP.

Related article: French Cyber Agency Reveals Suspected Russian Hacks

Dickson said the various hacking operations from Russia "are all different iterations of the same information operations" with Kremlin approval and that "they're doing it without fear of retribution."

SolarWinds last year disclosed that as many as 18,000 customers and more than 100 U.S. companies were affected by the hack. Its roster of clients includes government agencies and companies among the top 500 in the United States.

Hackers used Orion to gain entry into networks, allowing them to swipe data and install malicious codes that served as "backdoors" that could be used to sneak into systems as desired.

Washington has accused Russia of orchestrating the online assault, explicitly citing its Foreign Intelligence Service (SVR).

The hacking revelation comes as U.S. President Joe Biden and Russian leader Vladimir Putin prepare for their first summit next month in Geneva.

The June 16 meeting will include discussions on "the full range of pressing issues, as we seek to restore predictability and stability to the U.S.-Russia relationship," White House Press Secretary Jen Psaki said earlier this week.

Original url:
https://www.themoscowtimes.com/2021/05/28/russian-solarwinds-hackers-target-150-organizations-in-new-attack-a74047