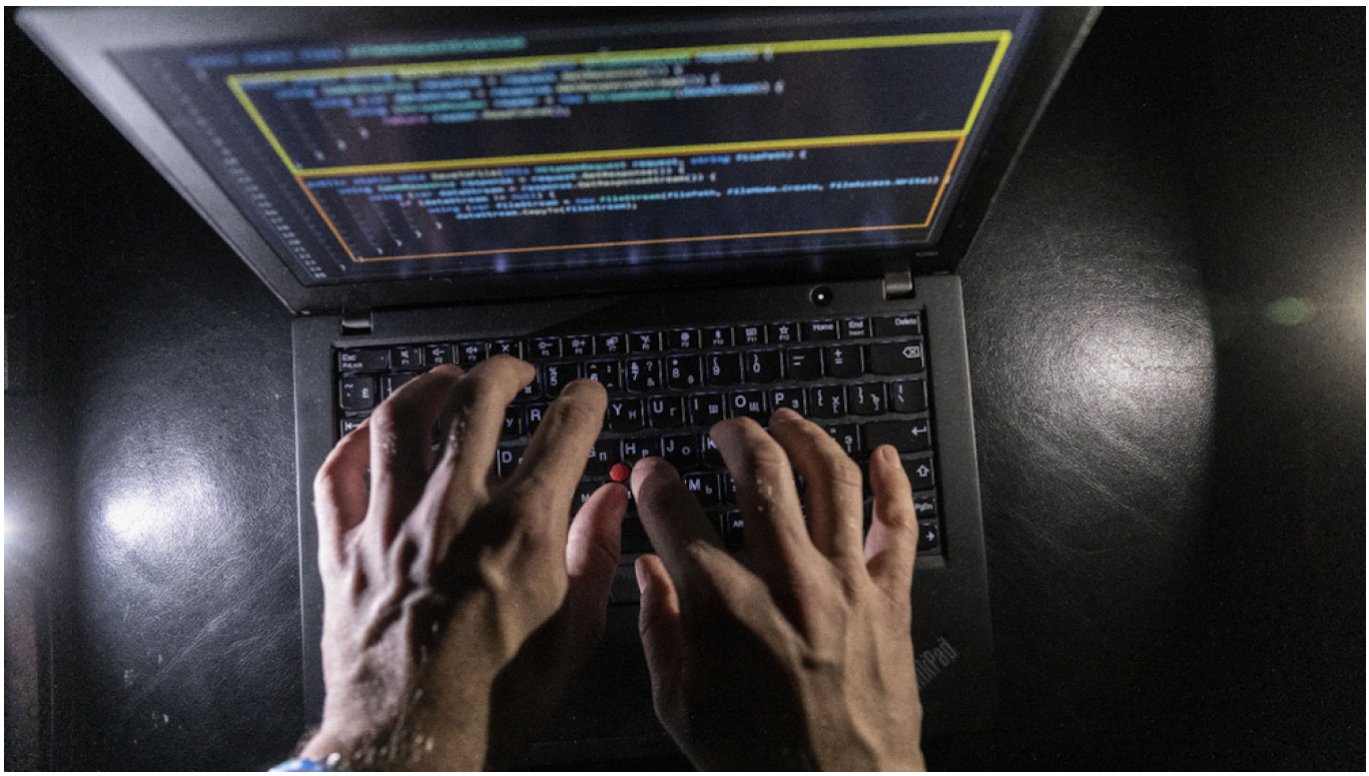
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. RNC Breach Traced to Russia-Linked Hacking Group – Bloomberg

July 07, 2021



The RNC hack comes as U.S. President Joe Biden seeks to take a stern stance against alleged Russian harboring of cybercriminals. **Evgeny Razumny / TASS**

Russian government-linked hackers were behind last week's cyberattack targeting the U.S. Republican National Committee, Bloomberg reported Tuesday, citing two unnamed sources familiar with the matter.

The hack appears to have originated with APT29, also known as Cozy Bear, a hacker group that is widely believed to be linked to Russia's intelligence agencies and was previously accused of the 2016 hacking of the Democratic National Committee, Bloomberg reported.

It marks the latest in a wave of Russia-linked attacks in recent months, with other high-profile targets including government agencies such as USAID and private companies Colonial Pipeline and JBS Foods.

It's unclear what information, if any, the hackers were able to view or steal, Bloomberg reported. RNC officials denied that any information had been stolen, saying the breach was

limited to third-party provider Synnex.

“Over the weekend, we were informed that Synnex had been breached. We immediately blocked all access from Synnex accounts to our cloud environment. [...] No RNC data was accessed,” Bloomberg cited RNC chief of staff Richard Walters as saying in a statement.

Related article: U.S. Software Firm Moves to Restart After Huge Ransomware Attack Linked to Russia-Based Group

The Russian Embassy in Washington “strongly rejected” the reports of Moscow’s involvement in the RNC hack, saying in a statement on Facebook: “We emphasize that the party itself denied the fact of a cyber attack. There is no evidence that the attack took place.”

The Kremlin also denied Moscow’s involvement in the cyberattack, saying it had no information on the incident.

Cozy Bear has been accused of several other high-profile attacks dating back to at least 2014. It is suspected to be behind the SolarWinds hack that was disclosed in December 2020, one of the largest data breaches in history.

The RNC hack comes as U.S. President Joe Biden seeks to take a stern stance against alleged Russian harboring of cybercriminals. In Biden’s June 16 summit with Russian President Vladimir Putin, the U.S. President presented his Russian counterpart with a list of clearly defined areas of U.S. critical infrastructure that he declared “off limits” to Russian cyberattacks.

On July 1, the U.S. National Security Agency released a report detailing “ongoing” efforts by groups linked to the Russian government to execute cyberattacks on “hundreds of U.S. and foreign organizations.”

“Targets include government and military, defense contractors, energy companies, higher education, logistics companies, law firms, media companies, political consultants or political parties and think tanks.”

Related article: Russia Points Finger Back at U.S. Over Latest Cyberattack Accusations

Many of these attacks take the form of ransomware. Victims are ordered to pay ransoms, often in bitcoin or other cryptocurrencies, or risk losing access to their computer systems forever.

While the RNC hack does not seem to have involved ransomware, another massive ransomware hack on U.S. software firm Kaseya over the weekend reportedly left the Biden administration “scrambling” to respond.

Commenting on the Kaseya hack, White House press secretary Jen Psaki on Tuesday reiterated the warning Biden gave to his counterpart Vladimir Putin about Russia harboring cybercriminals, stating that "if the Russian government cannot or will not take action against criminal actors residing in Russia we will take action, or reserve the right to take action on our

own."

Includes reporting from AFP.

Original url:
https://www.themoscowtimes.com/2021/07/07/us-rnc-breach-traced-to-russia-linked-hacking-group-bloomberg-a74453