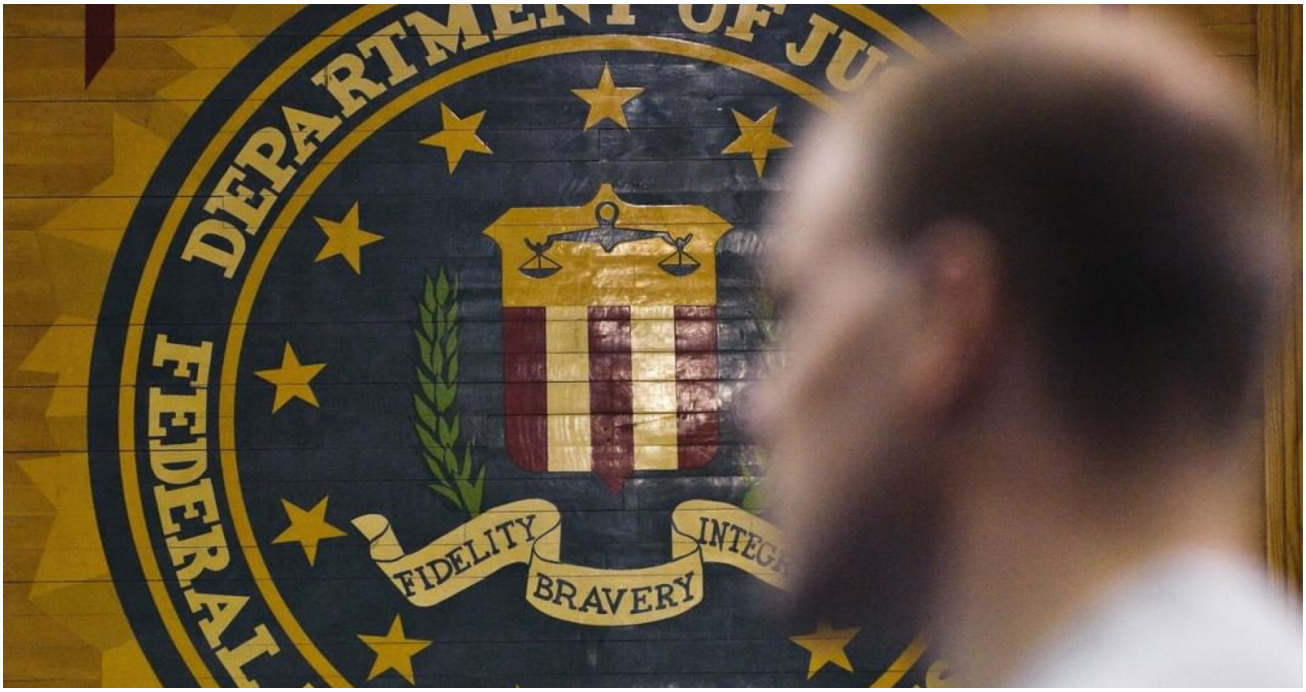
DOJ: SolarWinds hackers breached emails from 27 US Attorneys' offices

bleepingcomputer.com/news/security/doj-solarwinds-hackers-breached-emails-from-27-us-attorneys-offices/

Sergiu Gatlan

By
Sergiu Gatlan

- July 30, 2021
- 08:12 PM
- 0



The US Department of Justice says that the Microsoft Office 365 email accounts of employees at 27 US Attorneys' offices were breached by the Russian Foreign Intelligence Service (SVR) during the SolarWinds global hacking spree.

"The APT is believed to have access to compromised accounts from approximately May 7 to December 27, 2020," the DOJ said in a statement issued earlier today.

"The compromised data included all sent, received, and stored emails and attachments found within those accounts during that time,

"While other districts were impacted to a lesser degree, the APT group ***gained access to the O365 email accounts of at least 80 percent of employees*** working in the U.S. Attorneys' offices located in the Eastern, Northern, Southern, and Western Districts of New York." [emphasis ours]

United States Attorneys' offices breached during the attacks that had at least one employees' Microsoft O365 email account compromised as part of the SolarWinds supply-chain attack directly impacting the U.S. government and the private sector include:

- Central District of California;
- Northern District of California;
- District of Columbia;
- Northern District of Florida;
- Middle District of Florida;
- Southern District of Florida;
- Northern District of Georgia;
- District of Kansas;
- District of Maryland;
- District of Montana;
- District of Nevada;
- District of New Jersey;
- Eastern District of New York;
- Northern District of New York;
- Southern District of New York;
- Western District of New York;
- Eastern District of North Carolina;
- Eastern District of Pennsylvania;
- Middle District of Pennsylvania;
- Western District of Pennsylvania;
- Northern District of Texas;
- Southern District of Texas;
- Western District of Texas;
- District of Vermont;
- Eastern District of Virginia;
- Western District of Virginia; and
- Western District of Washington.

Even though other districts were also affected by the attacks to a lesser degree, the Russian SVR state hackers managed to breach the O365 email accounts of at least 80 percent of employees from US Attorneys' offices located in the Eastern, Northern, Southern, and Western Districts of New York.

"After learning of the malicious activity, the Office of the Chief Information Officer eliminated the identified method by which the actor was accessing the O365 email environment and in accordance with FISMA, the department took steps to notify the appropriate federal agencies, Congress, and the public as warranted," the DOJ added.

The DOJ confirmed that the hacking group behind the SolarWinds supply-chain attack breached the Department's Microsoft O365 email environment in a statement published on January 6, 2021.

In April, the United States government formally accused the Russian government of orchestrating the SolarWinds attack.

The White House named the SVR's hacking division (aka APT29, The Dukes, or Cozy Bear) as the group behind the cyber espionage activity exploiting the SolarWinds Orion platform, which allowed them to access the networks of multiple US federal agencies and private tech sector firms.

The SolarWinds Orion supply-chain attack

The attackers breached SolarWinds' internal systems and trojanized the Orion Software Platform source code and builds released between March 2020 and June 2020.

These malicious builds were later used to deploy a backdoor tracked as Sunburst to "fewer than 18,000" victims, but, luckily, the Russian hackers only picked a substantially lower number of targets for second-stage exploitation.

Before the attack was disclosed, SolarWinds displayed a list of 300,000 customers worldwide [1, 2] on its website: over 425 US Fortune 500 companies, all top ten US telecom companies, as well as a long list of govt agencies (the US Military, the US Pentagon, the State Department, NASA, NSA, Postal Service, NOAA, the US Department of Justice, and the Office of the President of the United States).

Multiple US govt agencies later confirmed that they were breached, including:

- the Department of the Treasury,
- the National Telecommunications and Information Administration (NTIA),
- the Department of State,
- the National Institutes of Health (NIH) (part of the U.S. Department of Health),
- the Department of Homeland Security (DHS),
- the Department of Energy (DOE),
- and the National Nuclear Security Administration (NNSA).

SolarWinds reported expenses of $3.5 million from last year's supply-chain attack in March, including costs related to remediation and incident investigation.

Related Articles:

FTC fines Twitter $150M for using 2FA info for targeted advertising

US links Thanos and Jigsaw ransomware to 55-year-old doctor

US charges hacker for breaching brokerage accounts, securities fraud

REvil ransomware returns: New malware sample confirms gang is back

US and allies warn of Russian hacking threat to critical infrastructure

- Department of Justice
- DOJ
- Russia
- Russian SVR
- SolarWinds
- USA

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

You may also like: