SolarWinds Orion Software Supply Chain Attack

Russian state-sponsored cyber actors accessed the software development infrastructure of U.S. company SolarWinds—possibly as early as January 2019, according to its CEO—and secretly modified the source code of its Orion network management software to enable malicious follow-on activity.

Among the 18,000 government and private users that downloaded the compromised software via an automatic security update, nine federal agencies and about 100 private-sector companies publicly disclosed follow-on compromises enabled by this software supply chain attack. As of June 2021, ongoing incident remediation efforts continue to uncover additional follow-on intrusions as a result of the Orion compromise.

On 15 April 2021, the U.S. Government formally named the Russian Foreign Intelligence Service (SVR), also known in cyber security circles as APT 29, Cozy Bear, and The Dukes, as the perpetrator of the cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures. The accompanying White House release stated the U.S. Intelligence Community has high confidence in its assessment of attribution to the SVR.

The unprecedented scale of the attack and its potential for enabling destructive follow-on actions motivated government and commercial entities to re-examine their supply chain vulnerabilities and the threats posed to them.

- **Type:** Software supply chain attack.
- **Vector:** Build environment.
- **Impact:** Enabled cyber espionage conducted against hundreds of government and commercial organization across the United States and Europe.
- **Mitigations:** NSC activated Presidential Policy Directive 41 and convened its Cyber Response Group. The House Committee on Homeland Security and House Committee on Oversight and Reform announced an investigation.
  - 5 JAN 2021: CISA, FBI, NSA, and ODNI announced formation of Cyber Unified Coordination Group to investigate and respond.
  - 15 APR: Joint CISA-FBI-NSA advisory highlighting additional SVR TTPs used to exploit U.S. and allied networks.
  - 26 APR: Joint CISA-FBI-NSA advisory on SVR cyber operations.
  - 07 MAY: Joint UK-CISA-FBI-NSA advisory on additional SVR TTPs.