Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise

SUMMARY

This fact sheet provides summaries of three key Joint Cybersecurity Advisories (CSAs) that detail Russian Foreign Intelligence Service (SVR) activities related to the SolarWinds Orion supply chain compromise published jointly by CISA and partners.

KEY JOINT PUBLICATIONS ON SVR ACTIVITIES

Joint NSA-CISA-FBI CSA: *Russian SVR Targets U.S. and Allied Networks*

The Joint NSA-CISA-FBI Cybersecurity Advisory, *Russian SVR Targets U.S. and Allied Networks*, published April 15, 2021, details the vulnerabilities the SVR is leveraging—as well as the techniques it is using—in its attempts to compromise these networks. In response to this activity this Joint CSA provides mitigations—both general and tailored for each technique--to help network defenders protect against this activity. The specific vulnerabilities this CSA addresses are:

- CVE-2018-13379 Fortinet FortiGate VPN
- CVE-2019-9670 Synacor Zimbra Collaboration Suite
- CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 Citrix Application Delivery Controller and Gateway
- CVE-2020-4006 VMware Workspace ONE Access

Joint FBI-DHS-CISA CSA: *SVR Cyber Operations: Trends and Best Practices for Network Defenders*

The Joint FBI-DHS-CISA Cybersecurity Advisory, *SVR Cyber Operations: Trends and Best Practices for Network Defenders*, published April 26, 2021, provides additional information on the SVR's tactics, techniques, and procedures (TTPS). Specifically, this CSA points out the FBI's observation that, starting in 2018, the SVR shifted from "using malware on victim networks to targeting cloud resources, particularly e-mail, to obtain information." Significantly, SVR's compromise of Microsoft cloud environments following their SolarWinds Orion supply chain compromise is an example of this trend. This CSA points out that because SVR actors used compromised accounts or system misconfigurations they were able "to blend in with normal or unmonitored traffic in an environment not well defended, monitored, or understood by victim organizations." This CSA identifies and provides recommendations to defend against the following SVR-leveraged TTPs:

- Password spraying,
- Exploitation of CVE-2019-19781 Citrix Application Delivery Controller and Gateway,
- WELLMESS malware, and
- Additional exploitation activity following initial compromise of trusted SolarWinds Orion software.

This CSA urges organizations and service providers to "strengthen their user validation and verification systems to prohibit misuse of their services."

Joint NCSC-CISA-FBI-NSA CSA: *Further TTPs associated with SVR cyber actors*

The Joint NCSC(UK)-CISA-FBI-NSA CSA, *Further TTPs associated with SVR cyber actors*, published May 7, 2021, details additional SVR TTPs—including some that SVR cyber actors appear to have newly leveraged in response to the CSAs listed above. This CSA points out that because the SVR rapidly moves to exploit newly disclosed vulnerabilities, "network defenders should ensure that systems are patched promptly following CVE announcements for products they manage." This CSA provides details on SVR-leveraged malware, including WELLMESS, WELLMAIL, GoldFinder, GoldMax, and possibly Sibot, as well as open-source Red Team command and control frameworks, Sliver and Cobalt Strike.