Marine Safety Information Bulletin

Commandant
U.S. Coast Guard
Inspections and Compliance Directorate
2703 Martin Luther King Jr Ave, SE, STOP 7501
Washington, DC 20593-7501

MSIB Number: 03-21
Date: February 10, 2021
Phone: (202) 372-2904
E-Mail: CyberWatch@uscg.mil

CONTINUED AWARENESS: ACTIVE EXPLOITATION OF SOLARWINDS SOFTWARE

The Coast Guard continues to monitor the maritime impact from the ongoing Advanced Persistent Threat (APT) cyber incident in the United States, as previously reported in Marine Safety Information Bulletin (MSIB): 25-20. For more details, please see the Joint Statement by the recently established Cyber Unified Coordination Group (UCG) composed of the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Office of the Director of National Intelligence, and National Security Agency.

This incident will require a sustained and dedicated effort to remediate. The UCG believes that the APT actor's compromise of the SolarWinds Orion supply chain affected approximately 18,000 public and private sector customers and that the actor targeted a much smaller subset of that group with follow-on activity. CISA continues efforts to identify and confirm initial access vectors and identify any changes to the APT's tactics, techniques, and procedures (TTPs). Please continue to refer to CISA Alert AA20-352A: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. A comprehensive repository of CISA resources related to this incident is available at https://www.cisa.gov/supply-chain-compromise. CISA will update these resources as new information is discovered.

Even if you do not own SolarWinds Orion, you may be impacted as your third-party networks, services, and vendors may use SolarWinds Orion. It is critical that the Coast Guard understands the potential risks of this APT actor on marine transportation system networks and supply chain connections.

Reporting malicious cyber activity enhances maritime domain awareness and allows us all to be better postured to prevent and respond to cyber incidents that could disrupt commerce or jeopardize national security. Any owner or operator of a Maritime Transportation Security Act (MTSA)-regulated facility or vessel that relies on SolarWinds software for a system that serves or supports a critical security function per its security plan shall, in accordance with 33 CFR 101.305(b) and CG-5P Policy Letter No. 08-16, Section 3.A.i, report a **breach of security** if:

- They have downloaded the trojanized SolarWinds Orion plug-in (see FBI Private Industry Notification 20201222-001 https://www.ic3.gov/Media/News/2020/201229.pdf); or
- They note any system with a critical security function displaying any signs of compromise, including those that may have not originated from the SolarWinds Orion compromise but utilize similar TTPs (see CISA Alert AA20-352A).

CISA recommends utilizing three open-source tools—including a CISA-developed tool, Sparrow—to help in detecting and remediating malicious activity connected to this incident. Specifically, Sparrow was created to detect possible compromised accounts and applications in the Azure/Microsoft 365 environment. For guidance on all three tools, see CISA AA21-008A: Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.

Any potential threat to the physical security or cybersecurity of your vessel or facility should be taken seriously. Any Breach of Security or Suspicious Activity resulting from Cyber Security Incidents for MTSA-regulated vessels or facilities shall be reported to the National Response Center at 1-800-424-8802. If you have any version of SolarWinds Orion but are unsure if you are at risk, or for any other questions regarding cyber threats or potential compromises, consider also contacting the Coast Guard Cyber Command 24x7 watch at 202-372-2904 or CyberWatch@uscg.mil.

Richard V. Timme, RDML, U. S. Coast Guard, Assistant Commandant for Prevention Policy sends