JANUARY 27, 2021

Alert: Nation-State Cyber Attacks

IMMEDIATE INTELLIGENCE & ACTIONABLE GUIDANCE

Nation-state actors often leverage the effects of cyber operations to achieve their strategic objectives on the world's stage.

The latest example of this type of advanced persistent threat (APT) cyber attack involves U.S. federal agencies and high-profile companies that were breached via a compromised and weaponized version of a SolarWinds software update from a connected third party. Publicly reported information indicates that a vendor was infiltrated by a sophisticated nation-state cyber attack, which allowed for malware to be embedded and hidden in software updates that were legitimate, creating an entry point to any machine that installed the updates. These types of breaches often proliferate for weeks or months before being discovered because the targeted company does not realize that their vendor has been compromised. We also understand that there are other vectors of compromise implicated in this campaign that do not leverage the referenced weaponized software via a supply chain attack, such that all entities must be on high alert. This includes malware being placed directly on systems that host SolarWinds Orion and disguised to appear as legitimate.

The Cybersecurity and Infrastructure Security Agency (CISA) has released a freely available tool called Sparrow.ps1. It was created to help identify compromised accounts and applications through automated data gathering. FTI Cybersecurity recommends that incident responders use this tool to assist with their investigations. Access the Sparrow.ps1 script here.

Why This Matters To You

You may need to assume a breach at your organization. Issues caused by vendor software can create significant problems, from monitoring email traffic and collecting sensitive and valuable information, to severely interrupting business operations. Further, nation-state actors can steal proprietary tools and use them to benefit their own cause, whether that's launching additional cyber attacks, or leveraging intellectual property to create products of their own.

IMMEDIATE RECOMMENDATIONS

- Block all domains and IP addresses associated with the incident on your network perimeter.
- Ensure the antivirus and intrusion detection solution deployed has detections in place for the indicators of compromise included in the appendix.
- Conduct hunt team searches against your network infrastructure to determine if any endpoints have established communications associated with this incident.
- Ensure servers, workstations, and applications are all operating with the latest patches applied.
- Run up-to-date antivirus or endpoint detection and response products that detect compromised SolarWinds' libraries.
- Review authentication logs for compromised accounts, unauthorized logins, and misuse of tokens
- Ensure user accounts with administrative rights follow best practices. Administrators should reduce the number of users that are members of highly privileged Directory Roles.
- Ensure service accounts and service principals with administrative rights are monitored for changes or unauthorized access.
- Reduce surface area by removing/disabling unused or unnecessary applications, servers, or redundant infrastructure.
- Update software that is being trojanized and isolate the infected software from the environment.
- Consider engaging an independent, external firm with experience in identifying and addressing sophisticated cyber threats.
- Change credentials used to manage network devices.
- Validate network device firmware/software stored or managed by SolarWinds and download known good versions.

How FTI Can Help

A global team of cybersecurity experts with extensive experience hunting, identifying, and responding to advanced persistent threat (APT) actors at government and private organization. Our team, capable of deploying worldwide, consists of dedicated cybersecurity experts, incident response consultants, developers, and data scientists with extensive investigative backgrounds. With our global team's deep experience in intelligence, law enforcement, and senior levels of government, **we maintain relationships with the top global intelligence agencies, regulatory authorities, and private agencies** to better support our clients in their prevention, response, and investigation of cyber threats and incidents. We can help by:

- **Understanding and assessing potential impact to your organization**: Analysis of systems and networks to determine if a breach occurred, and if so, what was affected and how to properly proceed.
- **Independent expert investigative task force**: Rapid response and surge capabilities anywhere in the world, capable of unearthing key facts and data sets.
- **Incident response**: Assist with containment, eradication, and recovery, including prohibiting data from leaving networks and preventing further damage.
- **Reviewing and assessing network architecture**: Audit of various network aspects in order to identify potential weaknesses in existing network configurations or changes to those configurations that may pose a risk to the organization.
- **APT threat-hunting services**: Ensure that the indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with this threat do not exist within your network. This service offering will focus on the following areas:
  - User authentication events analysis to ensure only expected events exists.
  - Host-based threat hunting for IOCs associated with this event.
  - Network threat hunting for the network IOCs associated with this event.
- **Holistic cybersecurity program assessment**: Ensure that existing policies and procedures are in place to handle an incident of this nature.

Issued Advisories (Updated January 27, 2021)

- CISA Malware Analysis on Supernova
- CISA Updates Emergency Directive 21-01 Supplemental Guidance and Activity Alert on SolarWinds Orion Compromise
- Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- Active Exploitation of SolarWinds Software
- Emergency Directive 21-01: Mitigate SolarWinds Orion Code Compromise
- SolarWinds Security Advisory
- Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor
- SUNBURST Countermeasures

ANTHONY J. FERRANTE
Senior Managing Director
Global Head of Cybersecurity
ajf@fticonsulting.com

JORDAN RAE KELLY
Senior Managing Director
Head of Cybersecurity, Americas
jordan.kelly@fticonsulting.com

KYUNG KIM
Senior Managing Director
Head of Cybersecurity, APAC
kyung.kim@fticonsulting.com

JOSHUA BURCH
Senior Managing Director
Head of Cybersecurity, EMEIA
joshua.burch@fticonsulting.com