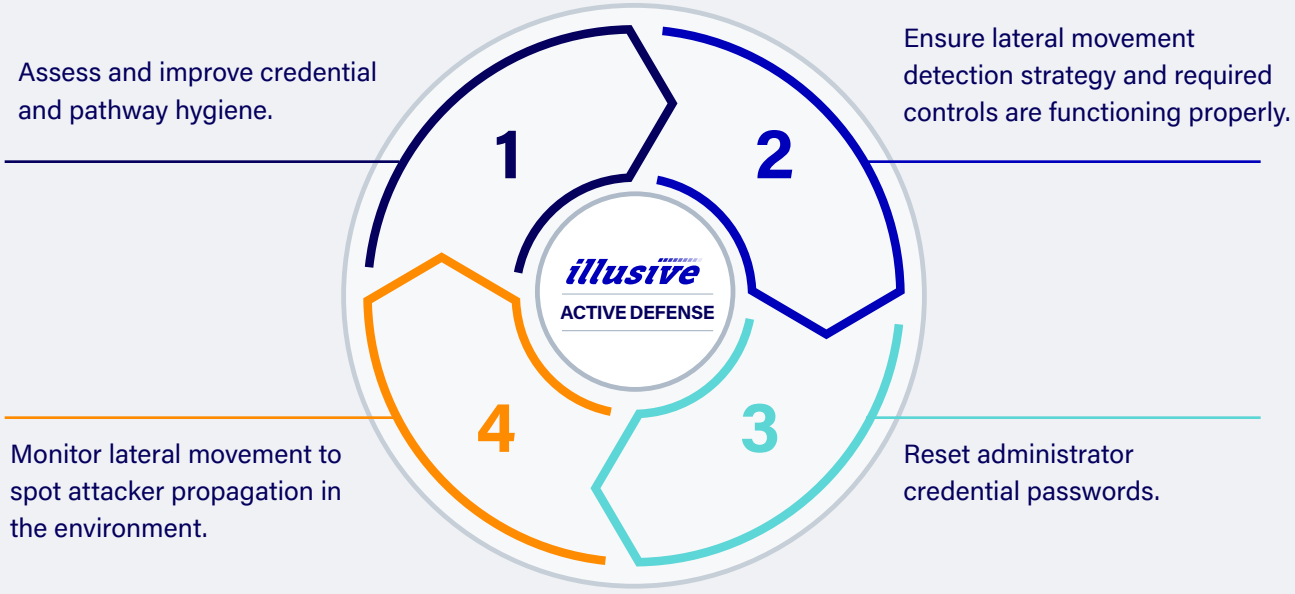
4 Step Plan to Prepare for Nation-State Attacks

Since last week and continuing into this week, details of the attack first perpetrated on FireEye and subsequently on the US Government Departments of Treasury and Commerce continue to evolve. We now know that the attack's origin was the SolarWinds Orion IT management software versions 2019.4 HF 5 and 2020.2 HF 1, containing a backdoor (Sunburst). According to the FireEye analysis, this campaign may have started as early as spring 2020. We recommend you follow the remediation guidelines from SolarWinds, and any other organizations directly involved in the attack.

It's still early, and industry knowledge about the attack remains incomplete, nevertheless we have learned enough to start developing plans to assess and reduce risk for organizations running the affected versions of SolarWinds Orion software. In this attack, as with most other advanced attacks like APTs and the new forms of targeted (human-operated) ransomware, attackers establish an initial beachhead, surveil their surroundings and move laterally to harvest privileged credentials that give them access to valuable information – "crown jewels".

Currently available evidence suggests that the attacker has stealthily operated for months on the internal networks of organizations with sophisticated security tools, teams, and processes. This highlights apparent lateral movement detection gaps in existing security visibility and controls. Our assumption is attackers have more footholds in many organizations and are waiting to complete their mission. We expect currently dormant attackers to become active in the coming weeks and recommend that all organizations: 1) Clean up potential access to the environment by locating all SolarWinds Orion instances and remediate per vendor guidance; and 2) Assume compromise because even if you don't have SolarWinds Orion, your suppliers and/or partners might, so you should assume attackers are in.
As preparatory and analysis measures in response to exposure of this attack, we believe at-risk organizations would benefit from preparing for and executing a "shake the tree" lateral movement hygiene and detection exercise. There are four parts to the exercise, which I will describe below.

Shake the Tree" Exercise Process



1. Hygiene

Nearly all high-impact attacks have a phase in which the attacker must conduct lateral movement from the beachhead to the ultimate target. To do this, the attacker needs a combination of credentials and available connections between systems. The attacker prefers to move through the network using native system tools and connectivity - "living off the land".

During a normal workday, cached credentials and connections proliferate within a network. The access footprint changes constantly as users log on and off, restart systems, change roles, and access resources. Sometimes people knowingly gain access they shouldn't have, but most connectivity and high value cached credentials result from ordinary, authorized activity. For example:

- Usernames and passwords are often stored in the web browser
- Domain admin credentials can be retained in system memory after a remote support session
- Hostnames and credentials are stored in applications, such as SSH and FTP clients, to conveniently access the servers.
- User privileges are accidentally escalated (shadow admins) due to the complexity inherent in Active Directory.

Once inside, attackers use tools to automate and accelerate credential harvesting, network discovery, and privilege escalation. The richer the access footprint, the more pathways an attacker has to reach the crown jewels – and the faster damage can be done.

A regular assessment and removal of unnecessary privileged credentials and connections will reduce the attack surface for this attack and others, improving the success security tools and teams have in detecting lateral movement and other suspicious activities

2. Lateral Movement Detection

Enact a strategy and solution to continuously detect any suspicious lateral movement. Relying on security controls not specializing in lateral movement detection can yield inaccurate results. Consequently, we recommend using a solution specializing in lateral movement detection to ensure detection accuracy.

3. Reset Administrator Passwords

Upon completion of the hygiene and lateral movement detection steps, reset all administrator passwords. By doing so, the attacker loses access and is forced to move laterally and harvest new privileged credentials to continue to leverage their presence on the network.

You might be tempted to shortcut the defined process and simply perform a password reset to prevent privilege escalation and crown jewel access, however it's difficult to reset all passwords (e.g., cached). Running this process in the defined sequence ensures that all passwords are cleaned from stored locations and the process achieves the desired objective.

4.Monitor Lateral Movement

The attacker may take several days, weeks, or even months to perform reconnaissance and attempt lateral movement, so detection activities should persist for an extended period, preferably within a permanent detection capability. Any lateral movement detection should include detailed telemetry for the attacker so that an analysis of their activities and tactics can be performed, and targeted detection and prevention measures can be implemented.

We'll provide additional guidance on potential actions to identify and mitigate the risks of the SolarWinds Supply Chain Attack as more information becomes available.