# IN THE SHADOW OF SUNBURST:

## Hunting for Firmware Persistence in the Context of Supply Chain Attack IR

In the wake of the Sunburst attack, IR and threat hunting are more important than ever, and firmware should be a key part of these efforts. As organizations continue to uncover the magnitude of these events, it is time to consider persistence and stealth techniques that dive below the OS. Similar threat actors have repeatedly demonstrated the capability and willingness to use these techniques in previous attacks. And now that at least some of the attack is in the open, we have highly capable attackers who will be digging deeper in order to maintain persistence, reinfect machines, and eventually steal data or cause damage. Taken together, this is a recipe for risk that includes both likelihood and impact.

To compensate, organizations and their IR and hunt teams need the tools and processes to verify the integrity of their devices and find any threats buried within their firmware. This means active monitoring and forensics at the firmware level. But before they can do that, teams need to know where to look, what to look for, and why. With that in mind, let's take a closer look at Sunburst in the context of firmware in the IR and hunt process.

### FIRMWARE, PERSISTENCE, AND SUNBURST

The industry is still unpacking the many implications of Sunburst with new analysis, TTPs, and associated malware being identified on an almost daily basis. However, it is abundantly clear that it is a highly sophisticated, long-term operation and most likely the work of Russian state-backed actors.

Such attackers have a long history of targeting firmware as part of their operations. The Lojax malware campaign run by APT28 used firmware to maintain persistence on infected devices even if the devices were re-imaged. Russian hackers also targeted firmware for destructive purposes in crippling attacks against the Ukrainian power grid and more recently implicated in widespread attacks targeting the firmware in network devices.

Firmware attacks are not limited to a specific set of threat actors. The massively popular Trickbot malware introduced new firmware-focused capabilities known as TrickBoot, which scans UEFI firmware for vulnerabilities and opens the door for firmware implants. These techniques are becoming far more popular because they provide persistence and stealth.

Persistence and stealth are also hallmarks of Sunburst. Attackers remained undetected within SolarWinds' most sensitive systems for at least 15 months before the attack was discovered. By that time, more than 18,000 organizations had been potentially compromised by a backdoor embedded in the SolarWinds Orion Platform.

## THE LONG TAIL OF SOLARWINDS

The SolarWinds Orion Platform is a particularly powerful asset for an attacker due to the strategic role it plays within an organization. As a monitoring and management tool, Orion interacts with a wide range of critical enterprise devices, including network devices, servers, hypervisors, and other infrastructure. The platform provides an inventory of devices and delivers new updates to software and firmware. This requires the platform to hold the credentials needed to connect to and manage those devices (using SMB, SSH, HTTP, etc.). As a result, if attackers can compromise the management infrastructure, then they can steal the keys to the systems it manages including an organization's network infrastructure. This is a serious concern in the case of Sunburst as Mimecast recently confirmed that the actors were able to steal credentials to a variety of service accounts.

Orion also holds cached software and firmware images for the endpoint and network devices it manages. With control over Orion, attackers could manipulate those images and push malicious versions to the managed devices. This could give attackers low-level control over an organization's network infrastructure in order to persist, infect additional devices, or ultimately cause damage. In short, the management system's access and privileges become the attacker's access and privileges. Red teams and pen testers routinely target such systems for just this purpose.

This is an immediate risk for SolarWinds customers as there are readily available tools to help attackers dump credentials from Orion systems. As noted in the linked blog, Orion systems will often hold far more credentials than are shown in the SolarWinds UI.

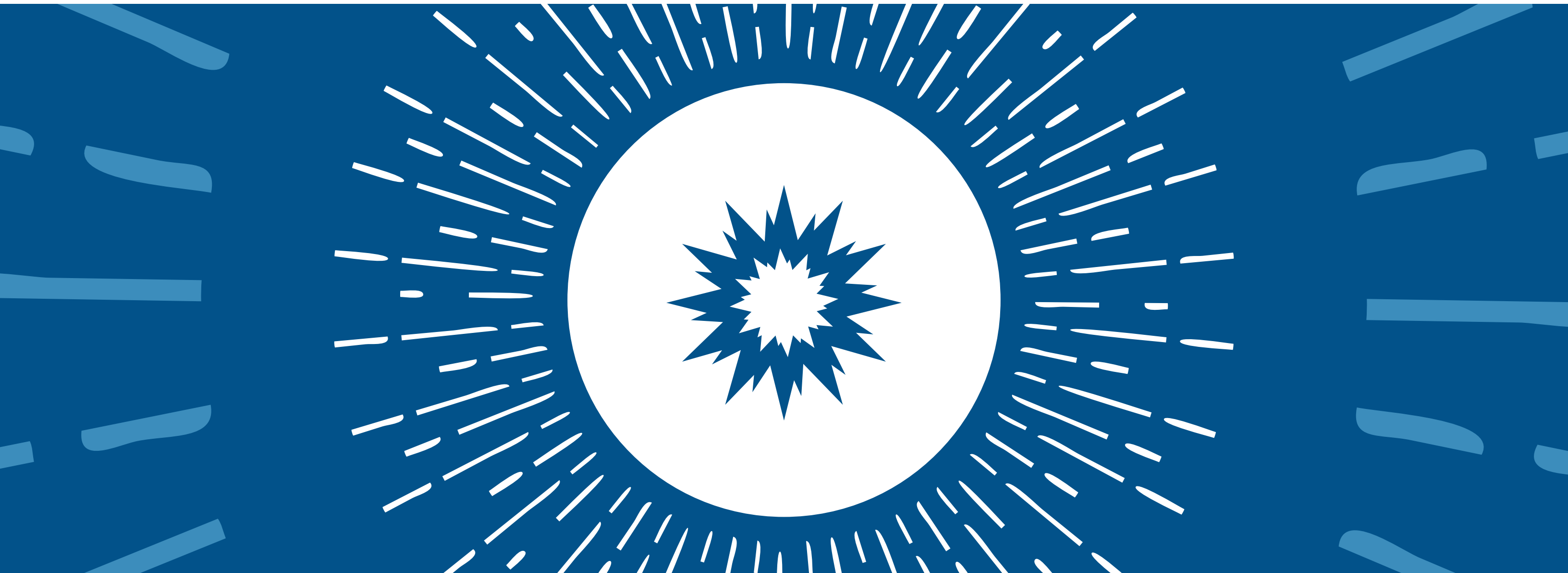
In the context of Sunburst this means that in addition to the Orion servers themselves, all the devices managed by Orion must likewise be treated as suspect and verified to be clean. This is directly born out in the recent DHS/CISA Emergency Directive 21-01:

> *4. After (and only after) all threat actor-controlled accounts and identified persistence mechanisms have been removed:*
>
> *a. Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed.*

## RECOMMENDATIONS AND NEXT STEPS

Organizations must be prepared for threat actor motives and TTPs to evolve now that the initial Sunburst campaign has been exposed and heavily researched by IR teams and a growing list of now-confirmed 'stage 2' victims. The adversary in question has already demonstrated a focus on stealth, evasiveness, and persistence, and security teams must anticipate that the threat actor may turn to alternative tactics in order to survive IR efforts. In this context, firmware persistence is a highly coveted method for achieving this persistence and evasion.

Past Russian nation-state actors have leveraged UEFI persistence (LoJax) as well as kernel level bootkits (Drovorub) to evade detection. It is important to note that the UEFI persistence observed in LoJax campaigns is able to survive a hard drive replacement and complete OS rebuild. Organizations will need to account for this type of persistence as they approach eradication, restoration, and re-provisioning of assets. Likewise,



the potential for actors to compromise and backdoor an organization's network infrastructure could allow attackers to maintain stealthy surveillance of an organization and even infect or reinfect devices.

Some victim organizations may well choose to provision brand new IT equipment instead of re-provisioning affected devices. It is important in this scenario that the newly provisioned devices are baselined at the OS *and device firmware levels* prior to connecting them to networks that have been affected by the overall campaign. This ensures that these advanced actors are truly eradicated from a contested environment.

Since firmware-specific security measures are new to many organizations, we have included the following set of recommendations. Organizations that are potentially compromised should be sure to verify the firmware integrity of the Orion server(s) as well as all the devices that are managed by Orion. Network devices such as firewalls and switches will have unique firmware considerations as compared to Windows-based devices and other more traditional servers. While the overall goals are the same, we have separated recommendations into two sections to better address the unique needs of network devices. We also encourage organizations to review the previously referenced DHS directive as well as the DHS advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, which highlights the importance of firmware and addresses common mistakes in incident response.

### Recommendations for Network Devices

a. **Verify firmware integrity of suspect devices** - The firmware and logs of network devices should be independently checked outside of the Orion platform to verify that they match those provided by the vendor and to detect any indicators of compromise.

b. **Verify vendor-provided security features are enabled** - Network devices may contain proprietary security features or modes that are unique to the vendor. Check to make sure that any such available security options are enabled.

c. **Change credentials for access and remote management** - Any credentials used by Orion to manage the device should be considered potentially compromised and replaced. This can include the HTTPS, SSH, SNMP, or other credentials used for access. Credentials should not be shared across multiple devices in order to reduce the impact if a given device is compromised.

d. **Verify device configuration** - Ensure that devices are properly configured according to established baselines for the device. This includes verifying only needed services or ports are enabled, logging features are properly configured, and security features are provisioned and actively enforced.

e. **Establish independent baselines for devices** - Any prior baselines may be unreliable if the management tools have been compromised. Organizations should independently establish and check security baselines for critical network devices outside of the Orion platform.

### Recommendations for Windows or PC Devices

a. **Verify firmware of suspect devices** - Scan firmware to identify devices that have been compromised. This includes verifying firmware components against known good versions of vendor firmware, scanning firmware for techniques used by implants, and detecting indicators of known firmware threats. For example, the MosaicRegressor rootkit made heavy use of the well-known Hacking Team UEFI implant. Where possible, teams should also check the firmware of key system components such as storage drives and network interfaces.

b. **Monitor for anomalous firmware behavior** - The nature of the Sunburst supply chain attack highlights that organizations cannot always blindly trust vendor code even when it is valid and properly signed. The ShadowHammer attacks on update infrastructure in 2019 posed a very similar type of problem. Firmware risk detection tools can monitor the behavior of firmware in order to identify any suspicious or malicious actions.

c. **Assess devices for firmware vulnerabilities and device misconfigurations** - Firmware vulnerabilities make it far easier for attackers to compromise the device. Firmware risk assessment includes identifying known firmware CVEs, verifying that updates require firmware to be properly signed, properly using boot protection mechanisms such as SecureBoot, and properly maintaining the firmware revocation lists (such as UEFI DBX).

d. **Establish baselines for replacement devices** - This will include many of the previous steps but will provide new devices with a critical reference point that changes can be measured against while ensuring that they are free from critical vulnerabilities.

These best practices will provide IR and hunt teams with a solid foundation for dealing with threats compromising firmware in their network and endpoint devices. These steps can be performed using the Eclypsium platform, which automates these actions and includes other advanced capabilities such as behavioral detection of unknown firmware threats and a host of operational capabilities such as logging, alerting, and dashboards for IT and security teams.

Organizations will have many considerations as they respond and adapt to the Sunburst attack. Given the nature of the attack and the threat actors behind it, firmware inside network devices managed by the Orion platform and inside endpoints affected by the breach should undergo a thorough assessment as part of post-breach incident response and threat hunting activities. The Eclypsium team is available to assist in any way we can and encourage interested parties to contact us at info@eclypsium.com to learn more.