


# SUNBURST & UNC2452: SolarWinds Breach Resource Center


---

[fireeye.com/current-threats/sunburst-malware.html](https://www.fireeye.com/current-threats/sunburst-malware.html)



 Hero image

Since discovering the global intrusion campaign to distribute malware known as Sunburst and UNC2452, we are committed to supporting our customers and the cyber security community with free resources, tools and services to help you detect and successfully block this threat.

 laptop with charts sitting on a table  
Webinar

**Cyber Espionage Analysis: UNC2452 - WHAT WE KNOW SO FAR**

---

Get the latest on UNC2452, the actor behind the SolarWinds supply chain compromise. Mandiant experts detail the latest intelligence on this threat actor.

[VIEW ON DEMAND](#)

## UNC2452 Resources

---


 red copy  
REPORT AND WEBINAR

### Executive Brief

---

Navigating the UNC2452 Intrusion Campaign

[Get the Executive Brief](#)


 "light in the dark" white copy over black  
WHITE PAPER

### Light in the Dark: Hunting for SUNBURST

---

In December 2020, FireEye revealed the details of a sophisticated threat actor that took advantage of SolarWinds' Orion Platform to orchestrate a wide-scale supply chain attack and deploy a backdoor we call SUNBURST. This attack impacted organizations worldwide, leading executives everywhere to question whether their environment fell victim.

[Watch the Webinar](#)

 close-up of hands on laptop keyboard  
ON DEMAND WEBINAR

### Threat Research Blog

---

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.

[Read the Blog](#)

### Frequently Asked Questions

---

#### What is Sunburst?

This is a threat actor cluster that we are tracking, and the behavior is consistent with nation-state activity. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to victims via trojanized updates to SolarWinds Orion IT monitoring and management software.

#### What are the motivations of this actor?

UNC2452 main motivations are likely espionage by exfiltrating data. So far, no indicators of extortion or financial crime have been discovered by the actor. Also, the actor leveraged Sunburst malware (see below) and does not have any connotation to known ransomware.

### **What is the timeline of activity?**

The campaign we have uncovered appears to have begun as early as Spring 2020 and is currently ongoing. The campaign is the work of a highly skilled actor, and the operation was conducted with significant operational security. Based on our analysis, the attacks that we believe have been conducted as part of this campaign share certain common elements.

### **Who is responsible for this?**

We were tracking the actors behind this campaign as UNC2452, which references to an “uncategorized” group in our intel naming schema. In April 2022, we merged UNC2452 into APT29. UNC2452 activity is now attributed to APT29.

### **Who was affected by this?**

This is a global campaign that introduced a compromise into public and private organizations; networks through the software supply chain. At this point in our investigation, we have detected this activity in multiple entities worldwide. The victims have included government, consulting, technology, healthcare, telecom, and oil and gas entities in North America, Europe, Asia, and the Middle East. There may be additional victims in other countries and verticals.

### **How did this affect FireEye?**

Based on the latest findings from our investigation, we determined the SolarWinds compromise was the original vector for the attack against FireEye. We believe that this is the initial attack vector after which they used other sophisticated techniques to penetrate and remain hidden in our network. Through the combination of our technology, intelligence, and expertise, we uncovered the SUNBURST campaign.

### **Does this affect FireEye products?**

No. We have already updated our products to detect the known altered SolarWinds binaries. We are also scanning for any traces of activity by this actor and reaching out to customers if we see potential indicators.

### **How was the intrusion detected?**

The intrusion was detected by monitoring secondary registrations of our Two-Factor authentication and reporting on suspicious behavior.

## **Free Resources**

---

Open-source Github repositories with Sunburst threat detection signatures.

We've made these resources free to the public to help you detect any indicators of UNC2452 or Sunburst-related activity. For a detailed description of techniques used by UNC2452 see our blog and additional technical details.

## **Mandiant Azure AD Investigator**

---

This repository contains a PowerShell module for detecting artifacts that may be indicators of UNC2452 and other threat actor activity.

[View on GitHub](#)

## **Mandiant Red Team Tool Countermeasures**

---

This repository includes rules categorized as production and supplemental release states in Snort, Yara, ClamAV, and HXIOC.

[View on GitHub](#)

## **Mandiant Sunburst Countermeasures**

---

This repository includes rules categorized as production and supplemental release states in Snort, Yara, ClamAV, and HXIOC.

[View on GitHub](#)

## **Mandiant Advantage**

---

Organizations currently using SolarWinds Orion IT need to see if they are compromised with the Sunburst backdoor and seek further evidence. Mandiant Advantage is an accessible threat intelligence web platform offering vendor-agnostic insight that can make this process easier.

[Get Free Access](#)

## **Mandiant Compromise Assessment**

---

Get a comprehensive analysis of your environment by Mandiant experts to uncover any impact by Sunburst. This assessment focuses on finding evidence of past and ongoing compromises with the help of proprietary technology, a deep library of indicators of compromise, and network forensics.

[Learn More](#)

## **Talk to an Expert**

---

Have questions about a product or solution? Concerned you may have been targeted or breached?

[Schedule a Consult](#)