Nobelium Resource Center – updated March 4, 2021

msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/

UPDATE: *Microsoft continues to work with partners and customers to expand our knowledge of the threat actor behind the nation-state cyberattacks that compromised the supply chain of SolarWinds and impacted multiple other organizations. Microsoft previously used 'Solorigate' as the primary designation for the actor, but moving forward, we want to place appropriate focus on the actors behind the sophisticated attacks, rather than one of the examples of malware used by the actors. Microsoft Threat Intelligence Center (MSTIC) has named the actor behind the attack against SolarWinds, the SUNBURST backdoor, TEARDROP malware, and related components as NOBELIUM. As we release new content and analysis, we will use NOBELIUM to refer to the actor and the campaign of attacks and we have updated references appropriate in this document below.*

Alongside our industry partners and the security community, Microsoft continues to investigate the extent of the recent nation-state attack on SolarWinds. Our goal is to provide the latest threat intelligence, Indicators of Compromise (IOC)s, and guidance across our products and solutions to help the community respond, harden infrastructure, and begin to recover from this unprecedented attack. As new information becomes available, we will make updates to this article at https://aka.ms/nobelium.

Executive Summary and Background Information

Microsoft is aware of a sophisticated supply chain attack that has targeted a variety of victims. The attack utilized malicious SolarWinds files that potentially gave nation-state actors access to some victims' networks. Microsoft cybersecurity experts are investigating the attack to help ensure that customers are as secure as possible.

- February 25, 2021: Published Microsoft open sources CodeQL queries used to hunt for Solorigate activity
- February 18, 2021: Published Turning the page on Solorigate and opening the next chapter for the security community
- February 18, 2021: Published Microsoft Internal Solorigate Investigation – Final Update
- February 5, 2021: Published Sophisticated cybersecurity threats demand collaborative, global response
- December 31, 2020: Published a Microsoft Internal Solorigate Investigation Update
- December 17, 2020: Posted an article from Brad Smith on the need for a unified approach to cybersecurity and how we respond to attacks: A moment of reckoning: the need for a strong and global cybersecurity response

- December 13, 2020: Published a blog from John Lambert outlining this dynamic threat landscape and the principles with which we are approaching the investigation and Important steps for customers to protect themselves from recent nation-state cyberattacks – Microsoft On the Issues
- December 13, 2020: Published a summary of what we know about the actors methods. This post will be updated with new information as the investigation continues. **Customers should look to this blog as the one stop for updates on the sophisticated attack**.

Information for Security Operations and Hunters

We encourage customers to implement new detections and protections to identify possible prior campaigns or prevent future campaigns against their systems. We have published the IOC's in this post. This list is not exhaustive and may expand as investigations continue.

We also recommend customers review the IOCs provided by FireEye at Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

- January 28, 2021 A webinar from the Microsoft 365 Defender Research team on protecting, detecting, and responding to Solorigate using M365 Defender.
- January 21, 2021 Published a deep dive into the Solorigate second-stage (SUNBURST to TEARDROP and Raindrop backdoors) including detailed hands-on-keyboard techniques
- December 28, 2020 Published a comprehensive guide for security operations and incident response teams on using Microsoft 365 Defender to identify, investigate and respond to the Nobelium attack at https://aka.ms/detect_solorigate
- December 22, 2020 An article from Alex Weinert on a new Azure AD workbook to help you assess Solorigate risk
- December 21, 2020 An article from Alex Weinert on Understanding "Solorigate"'s Identity IOCs – for Identity Vendors and their customers
- December 21, 2020 An article from Microsoft's Detection and Response Team (DART) with Advice for incident responders on recovery from systemic identity compromises
- December 18, 2020 An article from the Microsoft 365 Defender Research team and Threat Intelligence Center (MSTIC) on Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect
- December 16, 2020 An article from Shain Wray from MSTIC with guidance on SolarWinds Post-Compromise Hunting with Azure Sentinel (this post continues to be updated with new information as it becomes available)
- December 15, 2020 An article from Ariel Saghiv on the Latest Threat Intelligence for Azure Defender for IoT

- December 13, 2020 Microsoft Defender Antivirus and Microsoft Defender for Endpoint released protections for the malicious SolarWinds software and other artifacts from the attack.
- We have updated information about detection and potential impacts to customer environments in the Threat Analytics article within the Microsoft Defender Security Center (sign in is required).

Information for Security Admins

- January 15, 2021 An article from the Microsoft 365 Defender team for security administrators using Microsoft 365 Defender and Azure Defender to increase resilience against Solorigate and other sophisticated attacks patterns using Microsoft Defender
- January 15, 2021 An article by Daniel Niam for Microsoft Defender for Identity on expanding support to AF FS servers
- December 18, 2020 An article by Alex Weinert for Identity professionals and Microsoft 365 admins on how to protect Microsoft 365 from on-premises attacks
- December 15, 2020 An article from the Microsoft 365 Defender Threat Intelligence team on what we are doing to Ensure customers are protected from Solorigate

Further information and guidance for Microsoft security products and solutions

Overviews of the different Microsoft security products:

Where can I get help and assistance?

- Customers with any product support related needs should file a Microsoft Support case at https://support.microsoft.com/contactus
- Get help in the Microsoft 365 security center, Office 365 Security & Compliance center, and Microsoft Defender Security Center by clicking on the “?” Icon in the top navigation bar.
- For deployment assistance please contact https://fasttrack.microsoft.com
- If you believe you have been compromised and require assistance through an incident response, open a Sev A Microsoft support case.

Other Advisories & Additional Resources

- FireEye threat intelligence advisory: Global Intrusion Campaign Leverages Software Supply Chain Compromise.
- SolarWinds security advisory: SolarWinds Advisory.

- The Cybersecurity and Infrastructure Security Agency (CISA) has published information and guidance here: https://us-cert.cisa.gov/ncas/alerts/aa20-352a. For individual country-specific guidance, customers and partners should refer to information go from the appropriate law enforcement or other government entity in that jurisdiction.

Revision History

- 2021-03-04 Added background information on naming the actor and related components as Nobelium.
- 2021-02-18 Added link to the Executive Summary and Background section on the *Microsoft Internal Solorigate Investigation – Final Update* and *Turning the page on Solorigate and opening the next chapter for the security community*
- 2021-02-02 Added link to the Security Ops and Hunters section on the *Microsoft 365 Defender webinar: Protect, Detect, and Respond to Solorigate using M365 Defender*
- 2021-01-21 Added link to the Security Ops and Hunters section on the *deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop*
- 2021-01-15 Added link to the Information for Security Admins section on *Microsoft Defender for Identity expands support to AD FS servers* and *Increasing resilience against Solorigate and other sophisticated attacks with Microsoft Defender*
- 2020-12-31 Added link to *Microsoft Internal Solorigate Investigation Update*
- 2020-12-28 Added link to *Using Microsoft 365 Defender to protect against Solorigate* to *Information for Security Operations and Hunters* and MCAS docs link in *Specific guidance for Microsoft Security products and solutions* section
- 2020-12-22: Added links to an article from Alex Weinert on Azure AD workbook to help you assess Solorigate risk in the Hunting Section
- 2020-12-21: Published