European Repository of Cyber Incidents

# Major Cyber Incidents

## SolarWinds

Other incident names: SUNBURST malware, Solorigate

*By Linda Liang and Mika Kerttunen*

### Description

The Russian state-integrated hacking group APT29/"Cozy Bear"/The Dukes used a supply chain vulnerability within SolarWinds Corp. to compromise multiple targets worldwide. [1] It managed to inject a backdoor malware into a SolarWinds routine update file, which allowed it to escalate privileges and establish permanent access across the internal systems of the company's customers.

**Timeframe**
30 January 2019 – present [2]

**Initiator**
Russian state-integrated APT29/'Cozy Bear'

**Incident Type**
Data theft; Hijacking with Misuse

**Affected Targets**
SolarWinds Corp.; 6 EU institutions, 9 US government agencies, approx. 100 private sector entities from consulting, technology, telecommunications, and critical infrastructure in North America (primarily), Europe, Asia, and the Middle East. [3,4]

### Impact and significance

By exploiting SolarWinds software as a single point of entry, the initiators were able to cost-effectively reach a much larger number of organisations. The attack reportedly compromised mostly US entities. [5] Affected were nine US government agencies, including the Departments of State, Treasury, Commerce, Justice, Homeland Security, and Energy, as well as the National Nuclear Security Administration, NASA, the Federal Aviation Administration, and the National Institutes of Health. [6,7] Six EU institutions were deemed to have suffered "significant impact," alongside a "low single digit number" of UK public sector organisations. [3] Among the approximately one hundred selected entities which were hacked, many from the private sector were technology companies, such as cybersecurity companies FireEye and Microsoft; other targets included software makers, which themselves were vulnerable to becoming the source of a similar attack. Other targets from the consulting, telecommunications, and critical infrastructure sectors were mostly based in North America, but also in Europe, Asia, and the Middle East. [2,8,9]

The attackers' preparatory activities relied on long-term access to target networks through legitimate credentials, accounts, and applications, which enabled them to

gather information and steal data and identities, e.g., through reading email correspondences within the compromised networks. The scope and content of the espionage and data breaches were not disclosed, but news reports indicate leaked data included information on US counter-intelligence investigations, its policy on sanctioning Russian individuals, and the US' COVID-19 response, as well as emails of senior officials. [10] Mandiant, then part of FireEye, reported that the attackers stole red team assessment tools used to test the security of its clients' networks, and also managed to view sensitive information identifying government customers. [11] Furthermore, Microsoft admitted that the cyber actors were able to view its source code. [10]

The incident was unprecedented in premediation, complexity, and scope, and has exploited the trust between legitimate technology providers and customer organisations. It confirms that technology industry leaders are still held to insufficient cybersecurity standards and further highlights the risks resulting from the supply chain to government systems. Governments, especially in the US, have responded with unusually public attributions in the SolarWinds case, with the salience of supply chain security pushed further to the forefront of government agendas.

## Background

SolarWinds Corp. is a US information technology company based in Texas which provides IT service and network management software to high-profile clients such as government agencies and private sector organisations, including Fortune 500 companies, allowing for monitoring and configuring of servers and applications. The software "Orion" is one of its most widely used programmes. Its privileged place in networks allows hackers to hijack connections to jump to other systems without being noticed. [2] Of its 33,000 clients, an estimated 18,000 downloaded the compromised software updates for "Orion," which included the "SUNBURST" malware, and were therefore potential targets. However, the malware led to fewer than 100 network intrusions of customers; this selection included targets deemed of high value by the perpetrator. This reflects the targeted nature of the cyber operation, as it was necessary for the client to have downloaded the update containing the malicious backdoor in the timespan before detection and to have its servers connected to the internet. [3,12]

APT29/"Cozy Bear" is well known for its exceptional technical skill and for being well-resourced, capable of altering a trusted software at its source and remaining undetected in many networks over months. [2] Focussing on essential but inconspicuous software products and maintaining a relatively light malware footprint has been observed to be how the hacker group has protected their persistent and stealthy access to email inboxes, cloud-based resources, and source code repositories since their toolkit was reported in 2018. Their main target has continued to be data relevant to Russian strategic interests, as evidenced by multiple large-scale phishing campaigns against diplomatic entities in 2021 and 2022. [13] Brandon Wale, Director of CISA, has suggested SolarWinds' initial hack was part of a larger operation through which victims were targeted through compromised Microsoft authentication services. [14]

# APT29 attacks on the United States (2007–present)

2007 **Attack on Obama campaign**
Phishing attacks against Barack Obama and government officials before first candidacy.
Data Theft

2014 **State Department hack**
Dutch Intelligence Service AIVD attributed attack through hack into "Cozy Bear'" server.
Data Theft

2015 **DNC hack**
Access to email and chat communications of US Democratic National Committee.
Data Theft | Hijacking with Misuse

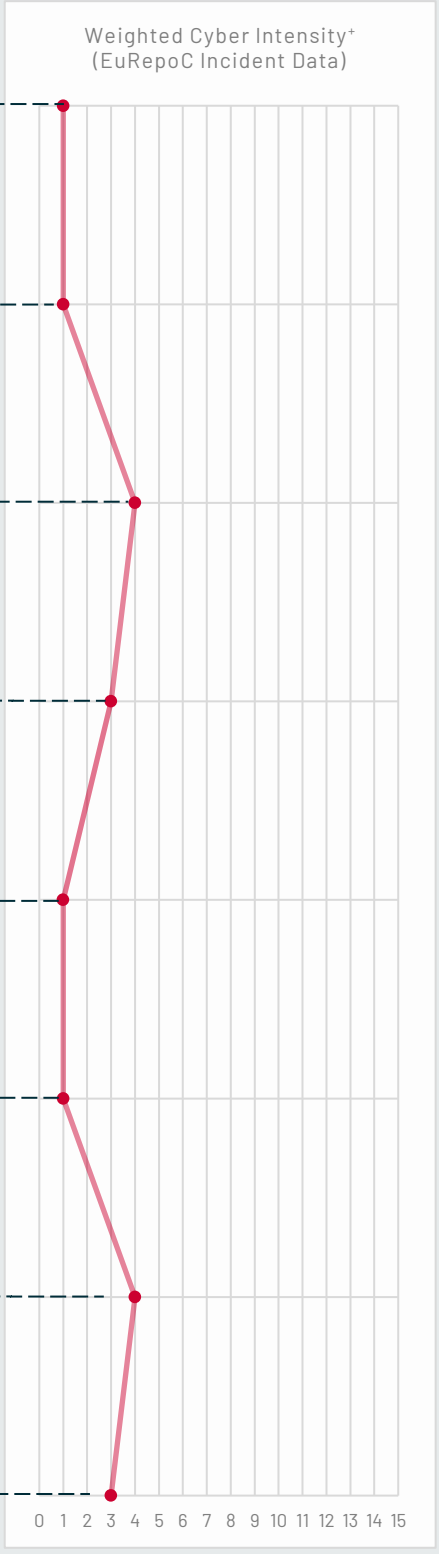
2016 **Hack of US think tanks and NGOs**
After Trump's election victory, "Cozy Bear" launched 5 spear phishing campaigns on US-based targets.
Data Theft | Hijacking with Misuse

2017 **Hacks against US progressive groups**
Groups are faced with ransom demands and loss of sensitive data.
Data Theft

2018 **Hack after year of silence**
Spear phishing campaign targeting multiple US sectors.
Data Theft

2019 **SolarWinds hack**
Supply chain attack, especially targeting multiple agencies and cyber intelligence companies.
Data Theft | Hijacking with Misuse

2020 **Wellmess/WellMail hack**
Malware used to attack research facilities for COVID-19 vaccines.
Data Theft | Hijacking with Misuse




*Continued on next page*

2021 **Republican National Committee hack**

Coincided with ransomware attack. Unclear if Synnex Corp. was the ultimate target.

Hijacking without Misuse

2023 **Hack of Hewlett Packard Enterprise**

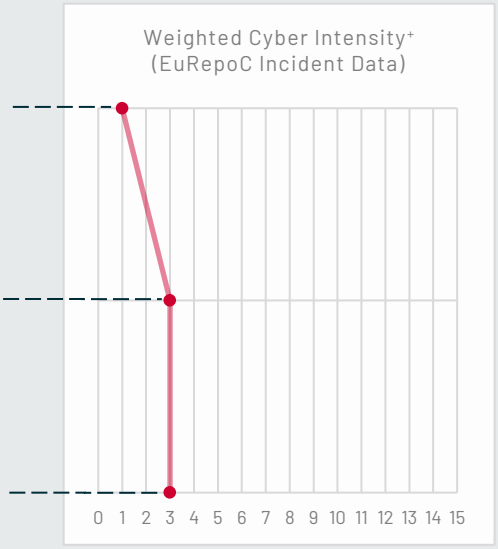
Breach of email environment linked to HPE's cybersecurity department.

Data Theft | Hijacking with Misuse

**Hack of Microsoft**

Breached corporate email accounts, including senior leadership and cybersecurity officials, resulting in breaches impacting federal agencies and other organisations linked to Microsoft.

Data Theft | Hijacking with Misuse




*Incident data from the EuRepoC database: https://eurepoc.eu/table-view/, see also APT29 profile: https://eurepoc.eu/publication/apt29-profile/*

## Attribution

Early reporting by Reuters on 13 December 2020 attributed the attack to Russia, or more specifically, to "Cozy Bear" as part of the Russian Foreign Intelligence Service (SVR). Others, such as the *Washington Post* and the *New York Times*, followed a day later, also already reporting on multiple US agencies being affected. [8,15,16] The first FireEye report on the SUNBURST malware refrained from naming a state actor; only later did it assign the actor it named UNC2452 to "Cozy Bear," in April 2022. [13] In the days following the attack, then-US President Donald Trump played down the link to Russia on the SolarWinds attacks, such as in a Twitter post on 19 December 2020. Meanwhile, the US Secretary of State, Mike Pompeo, explicitly attributed the attackers to Russia in a radio interview. [17]

In a joint statement on 5 January 2021, the US agencies that coordinated the Cyber Unified Coordination Group (UCG), which consisted of the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA), characterised the incident as a "likely" Russian intelligence-gathering operation. [18]

On 15 April 2021, with "high confidence," the US government formally named the Russian SVR, which sponsors "Cozy Bear," as the perpetrator of a broad-scope cyber espionage campaign that exploited the SolarWinds' "Orion" platform and other information technology infrastructures. [19] The accusation was followed by sanctions of six Russian

technology entities, forbidding US businesses to cooperate with the listed companies; this blocked entities' access to property on US territory. [20]
The attribution by the United States was done in concert with its Five Eye allies: Australia [21], Canada [22], New Zealand [23] and the United Kingdom. [24] The NATO alliance supported the attribution [25], as did Poland. [26] Latvia [27] and the European Union [28] both expressed their solidarity with the United States, while France expressed diplomatic support on Twitter. [29]
The Russian government has explicitly denied any involvement, stating that malicious activities in the information space contradict the principles of Russian foreign policy, its national interests, and Russia's understanding of interstate relations, arguing that "Russia does not conduct offensive operations in the cyber domain." [30]

## Operation timeline and attribution

| | |
|---|---|
| January 2019 | System access to SolarWinds Corp. |
| 12 September 2019 | Test run attack on software build environment. |
| 20 February 2020 | System attack<br>SUNBURST malware inserted into 'Orion' software. |
| March–June 2020 | Deployment of trojanised updates to 18,000 SolarWinds' "Orion" customers. |
| | *After a 2-week dormant period: cyberespionage, incl. information-gathering, credential, and data theft of estimated 100 high intelligence-value targets.* |
| 8 December 2020 | FireEye admits being target of successful hack. |
| 13 December 2020 | Reports by Reuters (suggested Russian origin);<br>Statement by SolarWinds on breach of internal systems; FireEye and Microsoft report on supply chain attack. |
| 5 January 2021 | Attribution by US government agencies:<br>Russian intelligence gathering operation "likely." |
| 15 April 2021 | Public attribution by US government to Russian SVR/"Cozy Bear" and sanctions; attribution by other members of Five Eyes: UK, Canada, Australia and New Zealand, as well as Poland and NATO; diplomatic support by Latvia, France, and EU. |

Sources: [2, 8, 9, 31]

## Technical details

It is unclear how the hackers first accessed SolarWinds' software development and internal systems, but investigators have found that an employee's VPN account was compromised by January 2019; this could have which enabled hackers to leapfrog to SolarWinds' Office 365 accounts and stolen source code. [2] The attackers targeted the software build environment and even carried out a test run of their code injection tool SUNSPOT on 12 September 2019. Another few months passed before the attackers added the malicious code SUNBURST into the company's software system "Orion" on 20 February 2020, swapping the legitimate and the compromised files before the final compilation and signing stage of the source code file. As part of routine updates, SolarWinds unwittingly sent out software updates to as many as 18,000 customers that included the hacked code between March and June 2020. [31]

The SUNBURST code created a backdoor to customers' information technology systems, which the attackers used to scour the environment after laying dormant for two weeks. If a target was of interest, they installed additional malware on infected computer systems; this has been estimated to have ultimately affected fewer than 100 entities worldwide. Using a second backdoor, the attackers continued the espionage operation while reducing the risk of exposing the unique backdoor technique of SUNBURST. [31] They were able to escalate privileges through credential theft, bypass multifactor authentication protocols, and, by moving laterally across networks, they conducted espionage in sensitive networks. [32]

## Remedies and consequences

It has been reported that US government agencies, such as the US Department of Justice, had noticed irregular activities by May 2020, but that FireEye, Microsoft, and SolarWinds were not able to detect the SUNBURST malware then. [33] As a cybersecurity company itself, Mandiant, then part of FireEye, first detected suspicious acitivity within its internal networks in November 2020, which led to a public disclosure of it having become a victim of a sophisticated attack on 8 December 2020. [11] It informed SolarWinds of the distributed SUNBURST malware on 12 December 2020, when, according to Reuters, a US National Security Council meeting was convened on this issue the same day. [15]

After detection, SolarWinds worked with customers of its "Orion" products to address the incident. On 13 December 2020, SolarWinds published a statement to its approximately 33,000 "Orion" product customers about its compromised software. The communication contained mitigation steps, including a hotfix update to address the vulnerability in part, as well as additional measures that customers could take to help secure their environments. SolarWinds prepared an update to further address the vulnerability and brought in CrowdStrike and KPMG for internal investigations into the source of the breach. [34]

To coordinate the US government's response to the SolarWinds attack, a Cyber Unified Coordination Group (UCG) was formed in December 2020 and was composed of the FBI, the CISA, and the ODNI, with support from the NSA. [35] The UCG gathered intelligence and developed tools and guidance to help organisations identify and remove the threat actor. Specifically, the FBI identified the scale and scope of the incident and engaged with affected entities. CISA and the NSA released cybersecurity advisories that detailed adversary techniques and provided mitigation actions for system owners. [35]

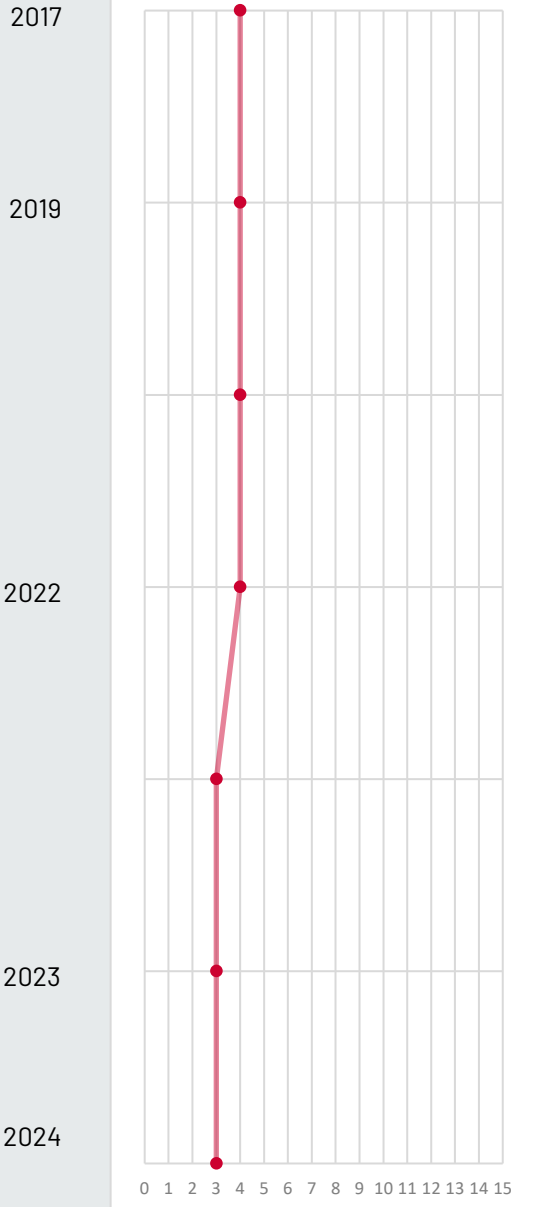
By February 2021, the new US administration under Joe Biden created the new position of Deputy National Security Adviser for Cyber and Emerging Technology, and went on to designate the ongoing situation as a "national cybersecurity crisis" which required additional funds. [36] The US National Security Adviser, Jake Sullivan, outlined that the US response to the SolarWinds attacks would "include a mix of tools seen and unseen, and it will not simply be sanctions." [7] This was followed by an executive order on 15 April 2021 (Executive Order 14028) that strengthened authorities "to demonstrate the Administration's resolve in responding to and deterring the full scope of Russia's harmful foreign activities," coinciding with the announcement of sanctions. Moreover, it directed the US Department of Homeland Security, in consultation with the Attorney General, to establish a Cyber Safety Review Board (CSRB) to review and assess threat activity, vulnerabilities, mitigation activities, and to assess agency responses to significant cyber incidents. The executive order is in line with the US policy of imposing costs in response to strategically and economically impactful acts that destabilize international relations. [9,19]

Further US policy in the past several years has aimed to modernise US cyber defences by adopting a "zero-trust" security model, providing guidance on securing networks against supply chain attacks and implementing comprehensive mandatory regulations for large critical infrastructure companies. [37–41] In July 2023, the US Senate ordered the CISA to investigate the SolarWinds attack. [42] Similarly, the Security and Exchange Commission (SEC) filed a complaint (Oct. 2023) and amended it (Feb. 2024) against SolarWinds and its Chief Information Officer (CISO), Timothy Brown, alleging that they misled investors and customers by overstating the company's cybersecurity practices and preventive measures, then failed to be fully transparent about the impact of the massive breach to its customers. In the subsequent ruling in July 2024, the US District Court of Southern New York dismissed (most) allegations raised by the SEC, including those of disclosure control violations. [52,53]

Policy responses were also seen across other governments. Germany implemented the IT Security Act 2.0 in 2021, while the UK government published a Proposal for Legislation to Improve the UK's Cyber Resilience in 2022, both of which highlight the threat of supply chain attacks. [43,44] The European Commission's Proposal for the Cyber Resilience Act, which seeks to enhance supply chain accountability as well, has reached a consensus within the Council of the EU in July 2023 and is awaiting negotiations with the European Parliament. [45]

# Large-scale global supply chain attacks (2017-present)

A supply chain attack first leverages an attack on a software supplier, which is then used to gain access to the network of the end target. This can be a customer or another software supplier. Their exploitation of trust between clients and software developers and their potentially indiscriminate effect on other actors make supply chain attacks particularly disruptive.




**NotPetya attack**

Russian government-backed APT Sandworm initially targeted Ukrainian infrastructure.

Infrastructure | Ukraine

**REvil attack on Texas**

Russian ransomware group "REvil" targeted 23 local governments, disrupting including a water treatment facility and a law enforcement dispatch system.

Government | Infrastructure | United States

**SolarWinds attacks**

Russian government-backed "Cozy Bear" attacks multiple US government agencies and tech companies through a software developer.

Government | Corporation | United States

**Viasat hack**

Russian GRU attributed in attack on satellite services of US communications company Viasat in Ukraine, supporting the Russian invasion.

Infrastructure | Ukraine | EU member states

**Ukraine government network hack**

Data theft by likely Russian actor from Ukrainian government networks via trojanised Windows 10 installers.

Government | Ukraine

**RedCurl attack**

Russian-language cybercriminal hackers gained access to unspecified major Russian bank through a contractor's shared network drive.

Finance | Russia

**Russian attacks on Ukraine infrastructure**

Report by CERT-UA on cyberattacks on around twenty critical infrastructure facilities by APT44/Sandworm, in part through supply chain attacks.

Infrastructure | Ukraine

*Incident data from the EuRepoC database: https://eurepoc.eu/table-view/*

## Enablers

In the same month that the SolarWinds compromise was discovered, the US Government Accountability Office (GAO) reported that none of the 23 US civilian agencies it had investigated had fully implemented supply chain risk management practices; in other words, selected foundational practices for managing information and communication technology (ICT) supply chain risks. GAO stressed that, as a result of not fully implementing these practices, the agencies were at a greater risk of malicious actors exploiting vulnerabilities in the ICT supply chain. [35] Subsequent reporting also revealed that, while the DOJ had already informed CISA in May 2020 that it had investigated suspicious activities with Mandiant's support, it had not contacted other agencies such as the NSA, and both the DOJ and CISA withheld their prior knowledge about the compromise when news broke in December 2020. [33]

This "culture of obfuscation" coincides with a growing complexity of software development and distribution and the increasing reliance of organisations on third-party software providers. It was also reported that many SolarWinds clients had failed to adopt standard practices to configure servers to only communicate with SolarWinds and put them behind firewalls. Further, many affected US and EU public organisations were missing network logs, making it impossible for response teams to reconstruct what data was hacked. [2,3]

## Private Sector Engagement

FireEye detection and mitigation, testimony [11]
Microsoft mitigation, testimony [46,47]
CrowdStrike forensics
KPMG forensics

## Legal Assessment

Economic sanctions by the US Department of the Treasury and other US countermeasures against what has been characterised as Russian espionage [54] are seen as legitimate by the US government, given the scope and the undue burden placed on the private sector by the SolarWinds attacks, as well as the risk of disruption that made the attack "destabilising." [48,49] Despite considerable debate about a more forceful response, including calls for "retaliation" and "punishment" beyond economic sanctions, the incoming Biden administration stopped short of a visible and robust (cyber) response, while determining in Executive Order 14024 (15 April 2021) that Russia's malicious cyber-enabled activities were "violating well established principles of international law," including the respect for the integrity of states. [50,55,56] In a related development, during a testimony to the US House of Representatives, representatives from Microsoft emphasised the need for clearer international regulations which prohibit indiscriminate and disproportionate supply chain attacks by state actors that put users at risk and undermine trust. [47]

## Further Reading

Joe Panettieri (2021). *SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details*. ChannelE2E. Available at: https://web.archive.org/web/20240820020235/https://www.channele2e.com/news/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details [51]

Kim Zetter (2023). *The Untold Story of the Boldest Supply-Chain Hack Ever.* Wired. Available at: https://web.archive.org/web/20230502100408/https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ [2]

Michael N. Schmitt (2020). *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*. JustSecurity. Available at: https://web.archive.org/web/20240423135918/https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/ [56]

## Sources

References


[1] Kevin Poulsen, Robert Mcmillan, and Dustin Volz (2020). *SolarWinds Hack Victims: From Tech Companies to a Hospital and University.* The Wall Street Journal. Available at: https://web.archive.org/web/20230926171632/https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402 [Archived on: 26 September 2023].

[2] Kim Zetter (2023). *The Untold Story of the Boldest Supply-Chain Hack Ever*. Wired. Available at: https://web.archive.org/web/20230502100408/https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ [Archived on: 2 May 2023].

[3] Catalin Cimpanu (2021). *SolarWinds hack affected six EU agencies.* The Record. Available at: https://web.archive.org/web/20240819082939/https://therecord.media/solarwinds-hack-affected-six-eu-agencies [Archived on: 19 August 2024].

[4] Mandiant (2020). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.* FireEye Blog. Available at: https://web.archive.org/web/20240912201433/https://cloud.google.com/blog/topics/threat-intelligence/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor/ [Archived on: 12 September 2024].

[5] Brad Smith (2020). *A moment of reckoning: the need for a strong and global cybersecurity response*. Microsoft. Available at: https://web.archive.org/web/20240912201431/https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/ [Archived on: 12 September 2024].

[6] Natasha Bertrand and Eric Wolff (2020). *Nuclear weapons agency breached amid massive cyber onslaught*. Politico. Available at: https://web.archive.org/web/20240912072509/https://www.politico.com/news/2020/12/17/nuclear-agency-hacked-officials-inform-congress-447855 [Archived on: 12 September 2024].

[7] Ellen Nakashima (2021). *Biden administration preparing to sanction Russia for SolarWinds hacks and the poisoning of an opposition leader*. The Washington Post. Available at: https://web.archive.org/web/20240518104132/https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html [Archived on: 18 May 2024].
[8] Ellen Nakashima and Craig Timberg (2020). *Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce.* The Washington Post. Available at: https://web.archive.org/web/20240912034310/https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html [Archived on: 12 September 2024].
[9] U.S. Government Accountability Office (GAO) (2022). *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents*. Available at: https://web.archive.org/web/20240824230555/https://www.gao.gov/assets/gao-22-104746.pdf [Archived on: 24 August 2024].
[10] Joseph Menn and Christopher Bing (2021). *Hackers of SolarWinds stole data on U.S. sanctions policy, intelligence probes*. Reuters. Available at: https://web.archive.org/web/20240903202511/https://www.reuters.com/world/us/hackers-solarwinds-breach-stole-data-us-sanctions-policy-intelligence-probes-2021-10-07/ [Archived on: 3 September 2024].
[11] Kevin Mandia (2021). *Prepared Statement, Hearing before the U.S. Senate Select Committee on Intelligence*. Available at: https://web.archive.org/web/20240911205132/https://www.intelligence.senate.gov/sites/default/files/documents/os-kmandia-022321.pdf [Archived on: 11 September 2024].
[12] U.S. Securities and Exchange Commission (2021). *Current Report: SolarWinds Corporation, Investigative Update*. Available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000173994221000076/swi-20210507.htm
[13] Mandiant (2022). *Assembling the Russian Nesting Doll: UNC2452 Merged into APT29.* Mandiant. Available at: https://web.archive.org/web/20240906021433/https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29 [Archived on: 6 September 2024].
[14] Robert Mcmillan and Dustin Volz (2021). *Suspected Russian Hack Extends Far Beyond SolarWinds Software, Investigators Say*. The Wall Street Journal. Available at: https://web.archive.org/web/20240913225733/https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601 [Archived on: 13 September 2024].
[15] Christopher Bing (2020). *Suspected Russian hackers spied on U.S. Treasury emails - sources.* Reuters. Available at: https://web.archive.org/web/20201213225356/https://uk.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PG [Archived on: December 13, 2023].

[16] David E. Sanger, Nicole Perlroth, and Eric Schmitt (2020). *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit*. The New York Times. Available at: https://web.archive.org/web/20240912112801/https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html [Archived on: 12 September 2024].
[17] Warren P. Strobel (2020). *Pompeo Blames Russia for Hack as Trump Casts Doubt on Widespread Conclusion*. The Wall Street Journal. Available at: https://web.archive.org/web/20240327182143/https://www.wsj.com/articles/pompeo-blames-russia-for-solarwinds-hack-11608391515 [Archived on: 27 March 2024].
[18] Cybersecurity and Infrastructure Security Agency (CISA) (2023). *Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)*. CISA. Available at: https://web.archive.org/web/20240910080727/https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure [Archived on: 10 Septmber 2024].
[19] The White House (2021). *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government.* The White House. Available at: https://web.archive.org/web/20240912204343/https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ [Archived on: 12 September 2024].
[20] James Reddick (2023). *Treasury Department hits Russian disinformation operators with sanctions.* The Record. Available at: https://web.archive.org/web/20240520112424/https://therecord.media/treasury-department-hits-russian-disinformation-operators-with-sanctions [Archived on: 20 May 2024].
[21] Australian Department of Foreign Affairs and Trade (2021). *Attribution of cyber incident to Russia*. Available at: https://web.archive.org/web/20240716043503/https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-cyber-incident-russia [Archived on: 16 July 2024].
[22] Global Affairs Canada (2021). *Statement on SolarWinds Cyber Compromise*. Government of Canada. Available at: https://web.archive.org/web/20240912153841/https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html [Archived on: 12 September 2024].
[23] New Zealand Government (2021). *SolarWinds compromise attributed to Russian state actor.* Release. Available at: https://web.archive.org/web/20240415132628/https://www.beehive.govt.nz/release/solarwinds-compromise-attributed-russian-state-actor [Archived on: 15 April 2024].
[24] UK Foreign, Commonwealth and Development Office (2021). *Russia: UK exposes Russian involvement in SolarWinds cyber compromise*. Press Release. Available at: https://web.archive.org/web/20240906020055/https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise [Archived on: 6 September 2024].

[25] North Atlantic Treaty Organization (2021). N*orth Atlantic Council Statement following the announcement by the United States of actions with regard to Russia.* Press Release (2021) 015. Available at: https://web.archive.org/web/20240903232453/https://www.nato.int/cps/en/natohq/official_texts_183168.htm [Archived on: 3 September 2024].
[26] Polish Ministry of Foreign Affairs (2021). S*tatement on Solar Winds Orion cyberattacks*. Available at: https://web.archive.org/web/20210416100807/https://www.gov.pl/web/diplomacy/statement-on-solar-winds-orion-cyberattacks [Archived on: 16 April 2021].
[27] Latvian Ministry of Foreign Affairs (2021). *Latvia's statement following the announcement by the United States of actions to respond to the Russian Federation's destabilizing activities*. Available at: https://web.archive.org/web/20210415150055/https://www.mfa.gov.lv/en/news/latest-news/67813-latvia-s-statement-following-the-announcement-by-the-united-states-of-actions-to-respond-to-the-russian-federation-s-destabilizing-activities [Archived on: 15 April 2021].
[28] Council of the EU (2021). *Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation*. Press Release. Available at: https://web.archive.org/web/20240529020114/https://www.consilium.europa.eu/web/20240529020114/https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/ [Archived on: 29 May 2024].
[29] French Ministry for Europe and Foreign Affairs (2021). *Cyberattack against #SolarWinds*. @Francediplo_EN Twitter Account. Available at: https://twitter.com/francediplo_EN/status/1382720234247847942?s=20
[30] Embassy of Russia in the USA (2023). *Embassy comment December 14, 2020*. Facebook. Available at: https://web.archive.org/web/20240902191054/https://www.facebook.com/RusEmbUSA/posts/1488755328001519 [Archived on: 2 September 2024].
[31] Isabella Jibilian and Katie Canales (2021). *What is the SolarWinds hack and why is it a big deal?* Business Insider. Available at: https://web.archive.org/web/20240909060230/https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12 [Archived on: 9 September 2024].
[32] Microsoft Threat Intelligence (2020). *Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers.* Microsoft Security Blog. Available at: https://web.archive.org/web/20240913175515/https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/ [Archived on: 13 September 2024].
[33] Kim Zetter (2023). D*OJ Detected SolarWinds Breach Months Before Public Disclosure*. Wired. Available at: https://web.archive.org/web/20230429133155/https:/www.wired.com/story/solarwinds-hack-public-disclosure/ [Archived on: 30 August 2024].

[34] U.S. Securities and Exchange Commission (2020). *Current Report: SolarWinds Corporation*. Available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm
[35] Vijay A. D'Souza (2021). *Cybersecurity. Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks*. U.S. Government Accountability Office (GAO). Available at: https://web.archive.org/web/20220826021254/https://science.house.gov/imo/media/doc/D'Souza%20Testimony.pdf [Archived on: 26 August 2022].
[36] Maggie Miller (2021). *Biden: US taking 'urgent' steps to improve cybersecurity*. The Hill. Available at: https://web.archive.org/web/20240313225129/https://thehill.com/policy/cybersecurity/537436-biden-says-administration-launching-urgent-initiative-to-improve-nations/ [Archived on: 13 March 2024].
[37] Jon Boyens, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon (2022). *Cybersecurity supply chain risk management for systems and organizations.* U.S. National Institute of Standards and Technology. Available at: https://web.archive.org/web/20240912132437/https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf [Archived on: 12 September 2024].
[38] Sergiu Gatlan (2022). N*SA shares supply chain security tips for software suppliers.* BleepingComputer. Available at: https://web.archive.org/web/20230825185156/https://www.bleepingcomputer.com/news/security/nsa-shares-supply-chain-security-tips-for-software-suppliers/ [Archived on: 25 August 2023].
[39] Elias Groll (2023). *White House cybersecurity strategy to force large companies to make systems secure by design*. CyberScoop. Available at: https://web.archive.org/web/20240405104450/https://cyberscoop.com/white-house-cybersecurity-strategy/ [Archived on: 5 April 2024].
[40] The White House (2021). *Executive Order on Improving the Nation's Cybersecurity*. The White House. Available at: https://web.archive.org/web/20240914181058/https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ [Archived on: 14 September 2024].
[41] Brian Krebs (2023). *Highlights from the New U.S. Cybersecurity Strategy*. Krebs on Security. Available at: https://web.archive.org/web/20240416002915/https://krebsonsecurity.com/2023/03/highlights-from-the-new-u-s-cybersecurity-strategy/ [Archived on: 16 April 2024].
[42] Michael Mestrovich (2023). *The Senate's defense-policy bill looks for threats in the rear-view mirror*. Defense One. Available at: https://web.archive.org/web/20231116140443/https://www.defenseone.com/ideas/2023/08/4-ways-defense-spending-bill-could-have-addressed-ai-other-issues-boost-cybersecurity/389586/ [Archived on: 16 November 2023].
[43] German Federal Office for Information Security (2021). *Die Lage der IT-Sicherheit in Deutschland 2021/The current state of IT security in Germany in 2021.* Available at: https://web.archive.org/web/20240308215401/https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3 [Archived on: 8 March 2024].

[44] UK Department for Digital, Culture, Media and Sport (2022). *Proposal for legislation to improve the UK's cyber resilience*. Consultation Outcome. Available at: hhttps://web.archive.org/web/20240816064626/https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/proposal-for-legislation-to-improve-the-uks-cyber-resilience#ministerial-foreword [Archived on: 16 August 2024].
[45] European Parliament (2023). *Horizontal cybersecurity requirements for products with digital elements.* Legislative Train Schedule. Available at: https://web.archive.org/web/20240606095809/https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act [Archived on: 6 June 2024].
[46] Brad Smith (2021). *Strengthening the Role of Digital Technology in Defending the Nation*. Testimony to the Senate Armed Services Committee in Hearing on Emerging Technologies and Their Impact on National Security. Available at: https://web.archive.org/web/20240910012356/https://www.armed-services.senate.gov/imo/media/doc/Smith_02-23-21.pdf [Archived on: 10 September 2024].
[47] U.S. Congress (2021). *Joint Hearing "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and the Ongoing Campaign."* Committee on Oversight and Reform, Committee on Homeland Security. Available at: https://web.archive.org/web/20240605024953/https://www.govinfo.gov/content/pkg/CHRG-117hhrg43755/pdf/CHRG-117hhrg43755.pdf [Archived on: 5 June 2024].
[48] Kristen Eichensehr (2021). *SolarWinds: Accountability, Attribution, and Advancing the Ball*. Just Security. Available at: https://web.archive.org/web/20240417015952/https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball/ [Archived on: 17 April 2024].
[49] The White House (2021). *Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021.* The White House. Available at: https://web.archive.org/web/20240902060003/https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/ [Archived on: 2 September 2024].
[50] Jon Bateman (2022). T*he Purposes of U.S. Government Public Cyber Attribution.In: Managing U.S.-China Tensions Over Public Cyber Attribution*. Carnegie Endowment for International Peace. Available at: https://web.archive.org/web/20240912230435/https://carnegieendowment.org/2022/03/28/purposes-of-u.s.-government-public-cyber-attribution-pub-86696 [Archived on: 12 September 2024].
[51] Joe Panettieri (2021). *SolarWinds Orion Security Breach: Cyberattack Timeline and Hacking Incident Details*. ChannelE2E. Available at: h https://web.archive.org/web/20240820020235/https://www.channele2e.com/news/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details [Archived on: 20 August 2024].

[52] Jennifer Lee, et al. (2024). *Takeaways from SEC v. SolarWinds Motion to Dismiss Hearing*. Harvard Law School Forum on Corporate Governance. Available at: https://web.archive.org/web/20240715200625/https://corpgov.law.harvard.edu/2024/06/09/takeaways-from-sec-v-solarwinds-motion-to-dismiss-hearing/ [Archived on: 15 July 2024].
[53] Shardul Desai, et al. (2024). *Court in SolarWinds Case Blows Down SEC's Cyber Enforcement Authority*. Holland &Knight Blog. Available at: https://web.archive.org/web/20240729215028/https://www.hklaw.com/en/insights/publications/2024/07/court-in-solarwinds-case-blows-down-secs-cyber-enforcement-authority [Archived on: 29 July 2024].
[54] Asaf Lubin (2020). *SolarWinds as a Constitutive Moment: A New Agenda for the Inter-national Law of Intelligence*. Just Security. Available at: https://web.archive.org/web/20240915172809/https://www.justsecurity.org/73989/solarwinds-as-a-constitutive-moment-a-new-agenda-for-the-international-law-of-intelligence/ [Archived on: 15 September 2024].
[55] The White House (2021). *Executive Order 14024, Blocking Property With Respect to Harmful Activities of the Government of Russian Federation*. Available at: https://www.federalregister.gov/documents/2021/04/19/2021-08098/blocking-property-with-respect-to-specified-harmful-foreign-activities-of-the-government-of-the
[56] Michael N. Schmitt (2020). *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law*, December 21, 2020, Available at: https://web.archive.org/web/20240423135918/https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/ [Archived on: 23 April 2024].

*Last updated: 01.10.2024*