Gallagher Re

CYBER IQ

What SolarWinds means in a Cyber Insurance Context

What Happened?

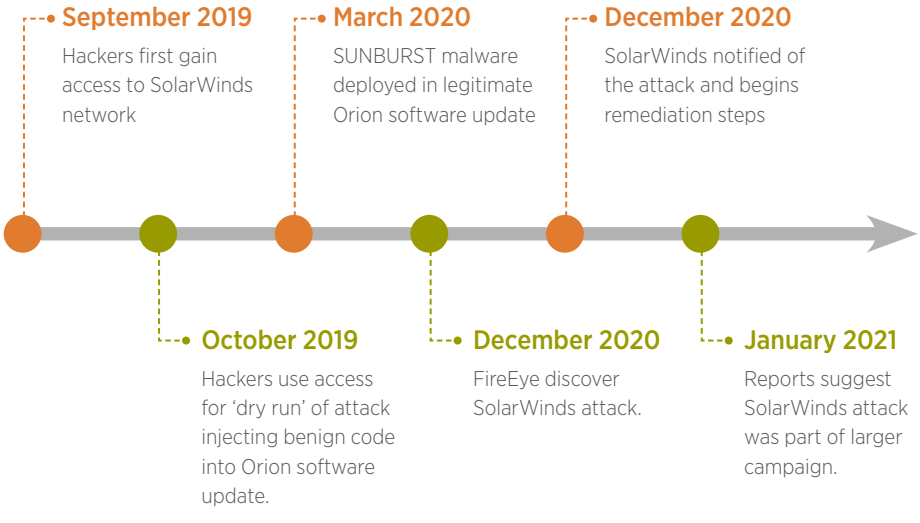
In early December 2020, FireEye – a prominent cyber security company – reported a breach to their systems, announcing some of their cyber tools had been compromised by a sophisticated threat actor.

Over the coming days and weeks, it was discovered that FireEye had been the first announced victim of a supply chain attack stemming from SolarWinds, a company which produces network and application monitoring software and enjoys widespread adoption.

The advanced threat actor had infiltrated SolarWinds and gained access to its clients' networks by pushing malicious code as part of a wider legitimate software update.

It's estimated that 18,000 entities – including many of the largest companies in the world across key industries – installed the software update and were theoretically compromised. However, the true number of entities affected is currently estimated around 250* due to the motives and methods of the attacker. It's also unlikely that all of those impacted will have lost sensitive data.

Figure 1: High Level Attack Timeline



* https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

Part of a wider campaign?

Early attempts at attribution focused on CozyBear, a suspected Russian APT (Advanced Persistent Threat) group associated with many sophisticated cyber campaigns in recent years. However, analysis of the malware used in the SolarWinds attack started to present a more complex picture.

Other leading software and technology managed service providers began to reveal they had also been targeted – with varying degrees of success. The commonality between these companies was their privileged access to client networks, making them attractive targets from which to launch supply chain attacks akin to SolarWinds.

We're still learning about the scope of these attacks, but it's becoming more likely that SolarWinds was part of a larger coordinated attack by multiple (likely Russian state-sponsored) APT groups working together in a coordinated manner with a clear division of labour.

Attacker Profile

- **Suspected Russia state-sponsored APT group(s).**
- **Attacker(s) exfiltrate small amounts of data over a long timeframe.**
- **Attackers target Intellectual Property and Confidential Data.**

Is SolarWinds Unique?

Whilst the SolarWinds event is a headline attracting large scale attack – both in size and sophistication – many of its key building blocks can be observed in other recent campaigns widely attributed to advanced nation state actors. The Cloudhopper and NotPetya campaigns (figure 2) are two pertinent examples.

It's less common for multiple suspected APT groups to be observed working together towards a common goal. The campaign also showed sophistication in its technical and strategic orchestration e.g. hosting attack infrastructure in the US to compound efforts at remediation by US agencies.

Figure 2: Suspected Nation State Driven Campaigns

Similarity to SolarWinds

NotPetya	Cloudhopper
Suspected nation state affiliated attack compromises software company and distributes malicious code to company's clients in legitimate software update.	Suspected nation state compromises multiple tier 1 and 2 managed service providers as staging point for supply chain attack impacting 100s of large companies in key industries.

Figure 3: Example Nightmare Scenario

1

INITIAL COMPROMISE

Advanced organised crime group with APT links successfully compromise multiple leading IT services/ software companies

2

PRIVILEGE ESCALATION

Attackers elevate privileges, using access to embed malicious code in legitimate software update

3

ACTION ON OBJECTIVE

Once most targets have applied update, attackers use backdoor to deploy wormable ransomware AND/ OR wiperware

Key Takeaways for Insurance

1 The 'nightmare scenario' is unlikely

The nightmare scenario – figure 3 – outlines an attack by advanced organise crime, coupling the SolarWinds approach with criminal motives, resulting in a Cyber CAT event.

Current organised crime sophistication and security changes made by companies to guard against supply chain attacks after SolarWinds makes an attack on this scale unlikely, but not impossible

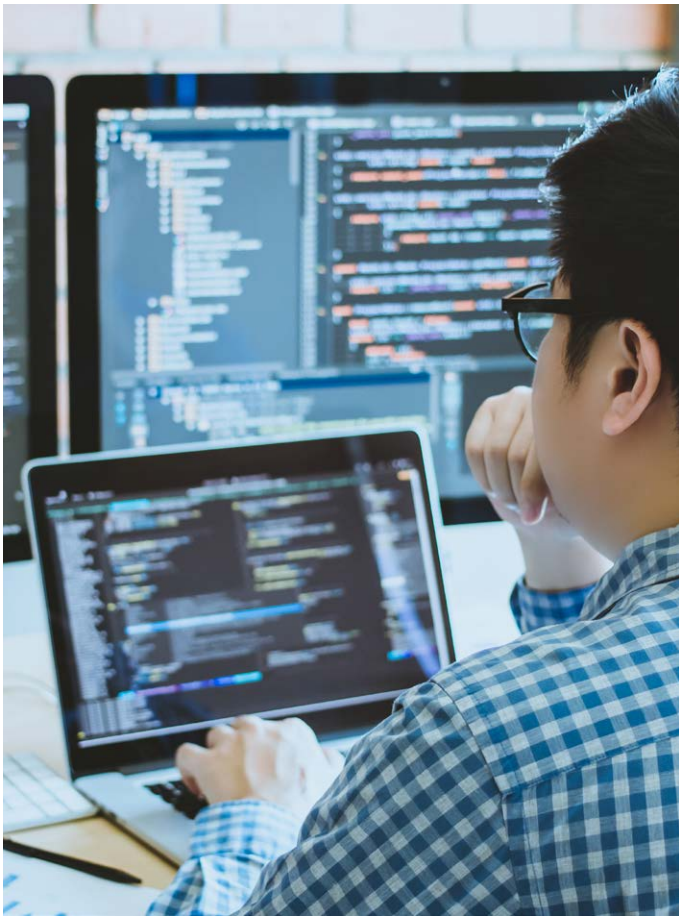
2 There's likely a 'cap' to SolarWinds campaign insurance loss

The true scope of this campaign will take months to uncover and may never be fully known.

However, attackers were highly targeted in the data they accessed and stole to avoid tripping any alarms, this results in a likely hard cap on the number of entities and amount of data impacted.

3 Risk selection won't insulate insurance from the next SolarWinds

Due to nation state sophistication, companies and insurers can't fully plan to secure themselves for the next SolarWinds. Instead, the insurance market could use SolarWinds to facilitate conversations around how insureds manage supply chain risk and encouraging adoption of stronger security controls.



Would you like to talk?

Ian Newman
Global Head of Cyber
E: Ian_Newman@GallagherRe.com

Justyna Pikinska
Head of Specialty Analytics
E: Justyna_Pikinska@GallagherRe.com

Ed Pocock
Senior Cyber Security Consultant
E: Ed_Pocock@GallagherRe.com

CONDITIONS AND LIMITATIONS

This information is not intended to constitute any form of opinion or specific guidance and recipients should not infer any opinion or specific guidance from its content. Recipients should not rely exclusively on the information contained in the bulletin and should make decisions based on a full consideration of all available information. We make no warranties, express or implied, as to the accuracy, reliability or correctness of the information provided. We and our officers, employees or agents shall not be responsible for any loss whatsoever arising from the recipient's reliance upon any information we provide and exclude liability for the statistical content to fullest extent permitted by law.

www.gallagherre.com

Gallagher Re is a trading name of Arthur J. Gallagher (UK) Limited which is authorised and regulated by the Financial Conduct Authority. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company Number: 1193013. FP174-2021 Exp. 10.02.2022.

© 2021 Arthur J. Gallagher & Co. | ARTUK-2072

Gallagher Re