

The Solar ‘Winds’ continue to shift

 by Danika Blessman  25 February 2021



Investigations into the SolarWinds cyberattack are ongoing

Following the announcement of the SolarWinds supply-chain compromise last December, and since our last blog update in mid-January, details continue to stream in; both the scale and ramifications of the breach are yet to be determined.

Topics in this article

Cybersecurity

Privacy, which appears to have affected over 18,000 entities worldwide, is being investigated. And, despite the massive number of entities potentially

having been affected, it appears that only a handful of organizations – primarily government and private sector – were actual targets. This is a highly used tactic, likely designed to obfuscate the intended targets of an attack.



Mimecast confirmed the breach compromised a software certificate used to secure connections to Microsoft cloud services

To give a better understanding of how massive this attack campaign is, recent evidence from Microsoft suggests that the operation may have included over 1,000 Russian state-backed operatives, and that about 4,000 lines of Orion update code were rewritten to help the attackers achieve their end goal.

Security firm Mimecast confirmed that the attackers were able to compromise a software certificate that the firm used to secure connections to Microsoft cloud services. This underscores just how deeply embedded the suspected Russian Advanced Persistent Threat (APT) group was in major technology companies.

As the analysis continues, it also appears that the group – or groups – behind the attack used multiple attack vectors to gain entry to its victims, including having access to emails at SolarWinds for at least nine months before the discovery. A statement from the acting director of the US Cybersecurity and Infrastructure Security Agency (CISA) suggests that ‘significant numbers of both the private-sector and government victims linked to this campaign had no direct connection to SolarWinds’, further broadening the investigation

Further attacks at U.S. organizations

It has come to light that the same suspected Russian APT group, tracked as Dark Halo by one security firm, breached a U.S. think tank earlier in 2020. Although it is unknown whether the two breaches were for related operations, one of the attack waves exploited the compromised SolarWinds supply chain.



Chinese attackers took advantage of yet another SolarWinds software vulnerability to compromise computers at the National Finance Center, New

Orleans, USA.

In addition, three new vulnerabilities have been patched by SolarWinds. Tracked as CVE-2021-25274, CVE-2021-25275, and CVE-2021-25276, two of these vulnerabilities affect SolarWinds Orion User Device Tracker, while the third affects SolarWinds Serv-U FTP for Windows. Successful exploitation of these vulnerabilities could allow an attacker functionality including adding new accounts, access to sensitive data, systems, or servers, and complete control of the underlying operating system.

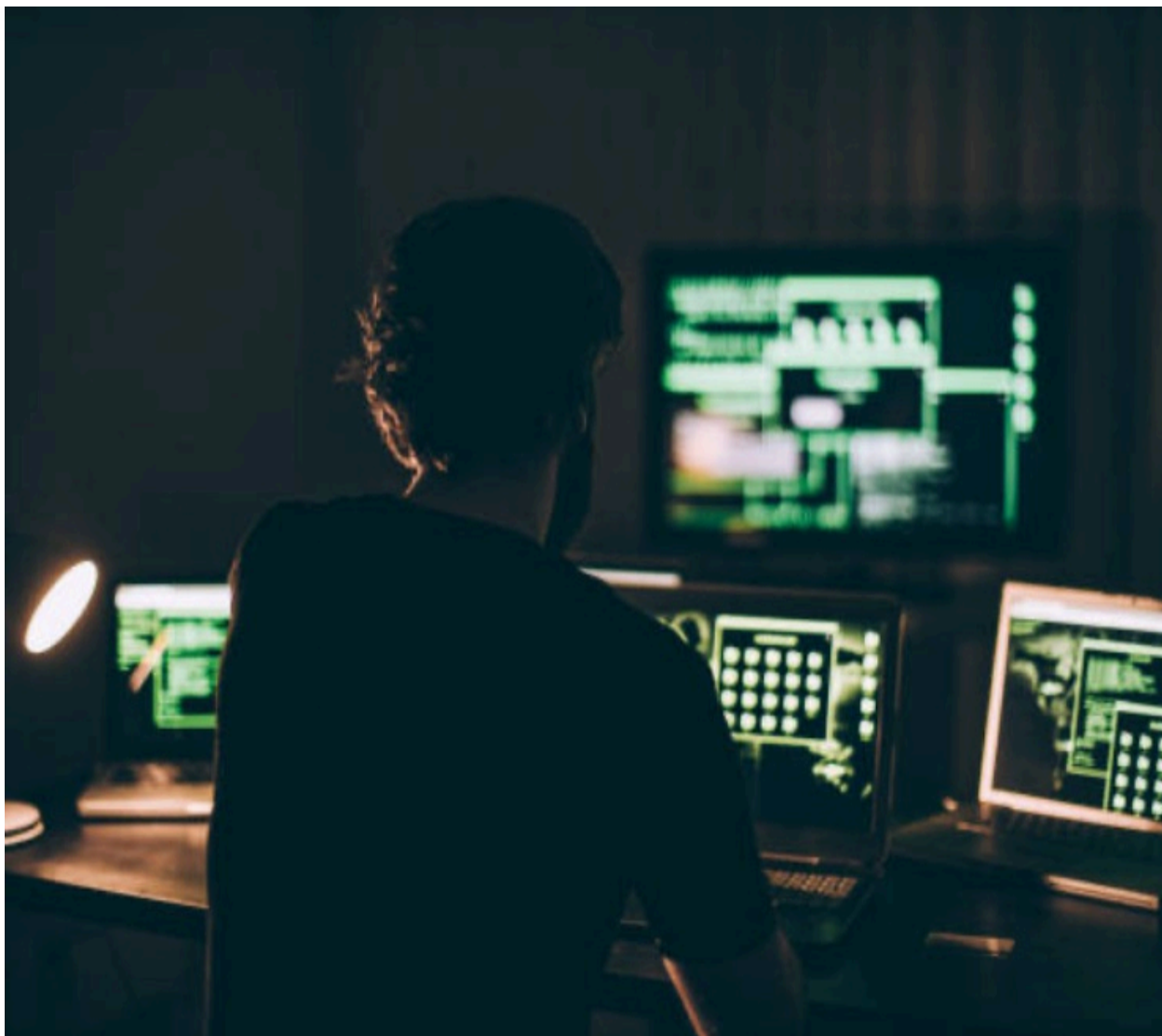
In the latest twist to this investigation, however, it appears that suspected Chinese attackers took advantage of yet another SolarWinds software vulnerability to compromise computers at the National Finance Center, and potentially other U.S. government agencies, although earliest evidence does not show ties between the two campaigns.

Frighteningly, despite each new detail that emerges from this investigation, it's been evident that many SolarWinds clients and victims have neglected to secure their networks following disclosure of this attack. According to RiskRecon, a risk assessment firm, many companies exposed to this espionage campaign have not yet followed protocol or taken steps toward mitigation of threats to their vulnerable environment.

The aftermath of the SolarWinds compromise

As mentioned in our previous SolarWinds blog, we should still expect to see copycat campaigns or follow-on attacks reusing the malware, particularly as these vulnerabilities are not being defended or patched in vulnerable environments.





According to RiskRecon many organizations have still not taken steps toward mitigation of threats to their vulnerable environment.

It is difficult to defend against legitimate files from trusted sources. As such, a layered approach is best. It's no longer enough to say 'vet all of your vendors and third-party resources.'

To that end, and as we continue to learn of new victims, techniques, and implications, perhaps building in a zero-trust model (i.e.: time-limited access and just-enough access), along with implementing the principle of least privilege, would add to the efficacy of a layered defense against these types of attacks, both in the design and implementation of your networks. Keep in mind that this breach is well beyond incident response, as its intent seems to point to espionage and theft of information rather than attempting to destroy data or property. That places this breach into the counterintelligence space. Affected organizations, and their clients, would be served well in keeping this aspect in mind: keep abreast of

the geopolitical climate, as well as understand why your organization may be a target.

References

CISA Says Many Victims of SolarWinds Hackers Had No Direct Link to SolarWinds

FSB warns of US cyberattacks after Biden administration comments

EXCLUSIVE-Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency –sources

7 Things We Know So Far About the SolarWinds Attacks

*Danika
Blessman*

Danika Blessman

Senior Threat Intelligence Analyst, Threat Intelligence Communications Team, NTT Ltd.



INDUSTRIES

SERVICES

INSIGHTS

SOLUTIONS

ABOUT NTT DATA

CAREERS

LEGAL

 Facebook Social

 twitter social

 YouTube Social

[Contact us](#)

[Terms of use](#)

[Do not sell my personal information](#)

[Sitemap](#)

[Report ethical concerns](#)

[Privacy](#)

[Cookie preferences](#)

[Unsubscribe](#)

[Careers](#)

Copyright © 2024 NTT DATA, Inc.

