SolarWinds Cyber-Attack Timeline

Date: 9 November 2021

The SolarWinds hack, also now widely known as Solorigate, is the most unprecedented cybersecurity breach till date & the reason it's considered a cyber intrusion like no other is because of the impact it had. Hackers managed to breach the world's most robust cyber power - the United States and its many government agencies, dozens of top businesses including one of the most respected cybersecurity companies - FireEye, other Fortune 500 companies, think-tanks etc. The ripple effect of the attack, of course, is still being felt in the USA and beyond, making it a global attack of unmatched proportions.

Clearly, this hack contains more lessons than any other - be it about good cybersecurity practices, cyber incident response or crisis management.

Quick reading guide:

Disclaimer: *This document has been created with the sole purpose of encouraging discourse on the subject of cybersecurity and good security practices. Our intention is not to defame any company, person or legal entity. Every piece of information mentioned herein is based on reports and data freely available online. Cyber Management Alliance neither takes credit nor any responsibility for the accuracy of any source or information shared herein.*

About SolarWinds

The SolarWinds cyber-attack, being touted as the most sophisticated in history, has managed to create ripples across the globe. As it was a software supply chain attack, it managed to compromise a vast set of SolarWinds' clients including government agencies and top businesses like Microsoft and FireEye.

Hackers managed to break into the SolarWinds systems and inject malicious code into its Orion software updates. These updates were then installed by Orion software customers, including federal agencies and leading multinationals alike.

Hackers managed to get remote access to sensitive information, confidential data, emails and documents. Yet, the attack remained undetected for months by SolarWinds and its clientele.

This hack underlines, like no other, that preparation and breach-readiness need to be spoken of more extensively than ever if another SolarWinds has to be prevented or its impact mitigated. Detection and Response…..

SolarWinds Cyber Attack Timeline

We have compiled a detailed timeline of the SolarWinds cyber-attack, also known as Solorigate, based on information that's available freely on the internet and in media reports. Our objective is to simply present this information in an easy-to-consume visual guide that can help cybersecurity practitioners and enthusiasts to get further clarity on what went wrong and how. You can read this comprehensive timeline here.

What Can We Learn

The idea of us creating this timeline is **not to** vilify/defame any business or victims of a cyber-attack. However, from every cyber incident there is something all of us can learn about covering our bases when it comes to being truly cyber-resilient.

The SolarWinds hack contains overwhelming lessons on responding to cyber-attacks and the responsibility of every private organisation towards its cybersecurity. It also highlights one of the biggest truths of the cybersecurity industry - Nobody or no organisation, regardless of its size and resources, is safe from being attacked. Some of the world's most

powerful organisations with the strongest cybersecurity brains in the world and seemingly limitless resources got compromised.

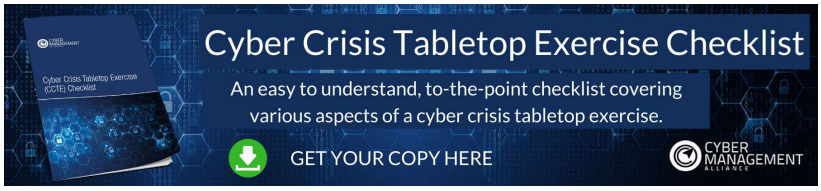
The biggest lesson of the Solorigate hack is that no matter who you are and what you have done to bolster your defences, you are NOT safe and you need to continuously prepare for *when*, and not *if*, you get attacked. And you need to spend as much energy into testing your crisis management plans.

Is there a Better Way?

We believe that the only way a business stands a remote chance of surviving a sophisticated and determined cyber-attacker today is to first start by acknowledging that it's defences will be breached. This should be followed by adopting a strategic policy and executive mandate on cyber resilience.

If you are truly interested in ramping up your security infrastructure and making sure that your business doesn't suffer the kind of damage other victims of cyber-attacks have, you may be interested in pursuing our NCSC-Certified Cyber Incident Planning and Response course. We offer this course as an online public training or as a private training for individual organisations on-site or virtually.

> ***Disclaimer:*** *This document has been created with the sole purpose of encouraging discourse on the subject of cybersecurity and good security practices. Our intention is not to defame any company, person or legal entity. Every piece of information mentioned herein is based on reports and data freely available online. Cyber Management Alliance neither takes credit nor any responsibility for the accuracy of any source or information shared herein.*



Get Email Updates on our Latest News

Simply enter you details in the form below to subscribe:

Email Address*

SUBSCRIBE

Drop us a line on:
info@cm-alliance.com

Or call us on:
+44 (0) 203 189 1422

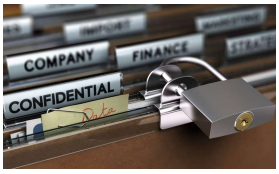
SUBSCRIBE
TO OUR YOU TUBE CHANNEL

Show comments

Like this article? Share it with others!

Tweet Share Like 0 Share

Related posts



27 September 2022

Simple Steps to Secure Your Organisational Data in 2022

23 September 2022

How to Protect Your Data & Privacy Online

18 September 2022

Uber Cyber-Attack: A Live Timeline

14 September 2022

Top Swiss Cybersecurity groups ISSS & SIGS invite CM-Alliance to host a roundtable on Incident Response

CYBER ESSENTIALS CERTIFIED

Crown Commercial Service Supplier

Certified Training in association with National Cyber Security Centre

IASME Consortium Self-certified Company

Simply fill in your details to request a free callback:

Your Name* Your Phone Number* Country*

Please Select

GET A CALLBACK

Sign up to our Newsletter:

Email

Email us at:

info@cm-alliance.com

Or call us on:
+44 (0) 203 189 1422

CYBER MANAGEMENT ALLIANCE

Follow us on

Privacy Policy