What really happened in the SolarWinds cyber-attack?

Date: 16 November 2021

The SolarWinds cyber-attack has been given many adjectives – historic, unprecedented, massive and sophisticated to name a few. What makes this attack unlike any other we've seen in recent times is the fact that it was a supply chain attack of indescribable sophistication.

Criminals managed to compromise the update process of SolarWinds' Orion software. Being a supply-chain attack meant that by infiltrating the network of one service provider (in this case SolarWinds), hackers managed to compromise the systems of all its clients, impacting over 18,000 organisations, including some top tier cybersecurity companies, global giants like Microsoft, Cisco, many US government Agencies, EU institutions and more.

In line with its commitment to educate and empower the cybersecurity community with continuous knowledge and thought leadership, Cyber Management Alliance has launched a massive educational campaign on the SolarWinds cyber-attack.

The idea is to understand what went down and how the criminals managed to succeed in compromising entities that are considered the masterminds of global cybersecurity and information security. The sole objective behind this exercise is to build our collective defences and gain an understanding of what security measures can be undertaken to prevent such complex, devastating attacks from succeeding again and mitigating their impact if they do occur.

As part of this educational campaign, we have created one of the most comprehensive SolarWinds cyber-attack timelines capturing the

chronology of the SolarWinds breach. Complementing the timeline, is a series of webinars, where our CEO and Co-Founder, Amar Singh will discuss the attack methodology, how the attack was discovered, what the gaps were, with other industry experts.

The first of this series of webinars took place recently and can be viewed on our BrightTALK channel here. Entitled, "What Really Happened in the SolarWinds Cyber-Attack?" Amar Singh engaged in conversation with Senior Threat Hunter from IronNet, Joel Bork. Joel and his team were instrumental in detecting the early signs of the attack. In this exciting webinar, Joel discusses how his team actually figured out that something was not right and sheds light on the hackers' advanced techniques.

43:33

Some of the key discussion points that Joel and Amar elucidate in this webinar include:

1. What made the SolarWinds incident so widespread?
2. How did the Nation State actors inject malicious code into the SolarWinds Orion DevOps build cycle?
3. How did they manage to go undetected such that 18,000 organisations downloaded the infected software?
4. Injecting malicious code is common. So, what made this attack so unique and pervasive?
5. What were these exceptional, expert-level evasion techniques that the SolarWinds Russian hackers used to camouflage their modus operandi?

Joel, whose team, was amongst the first to detect the signs of the attack elaborated on the most compelling question that arises out of the

SolarWinds hack – how did the hackers ever manage to succeed at such a massive scale?

Some of the **evasion techniques** that worked for them, as explained by Joel in the webinar, were the following:

1. The Sunburst certificate was properly signed, and the domain was registered a year before - leaving no reason for anyone to doubt it.
2. The cyber criminals disabled logging every time they injected the DLL and then re-enabled logging again. Unless someone was actively looking for an intrusion of this sophistication, there was no obvious evidence of the DLL being injected.
3. The DLL made sure it had not been changed.
4. It was also ensured that it was **not** executed at SolarWinds, in a Sandbox, by security tools. This is critical because if security analysts are looking at this DLL, they are going to do so in a Sandbox. So, the DLL was actually able to evade execution in a sandbox. That's how sophisticated the attack was. It was able to avoid detection at every level.
5. The DLL was also able to execute at random times, up to two weeks after restart.
6. It had a full process list which allowed it to check for endpoint security tools and installed drivers and kill them, successfully evading all EDR capabilities.

Joel also offered a critical insight during the course of the webinar - that IronNet created alerts 6 months before FireEye released the news of being compromised. However, the customer environments weren't able to do much at that time, perhaps because they didn't have the right people with the right training. So now IronNet is rolling out a comprehensive training program and providing services on top of that so that the next time this happens, clients are able to act on it before a year goes by.

Amar Singh reiterated that this is essentially why Cyber Incident Planning & Response is so critical. The human element needs to be better equipped to process and act upon critical alerts such as those issued by IronNet. They need to also be freed up to proactively spot anomalies before it's too late. People also need to be reoriented in how they think. The approach that tells you to only look for alerts and only look for use cases is clearly not enough anymore.

The webinar then moved on to a discussion of what really can be done to prevent similar attacks in the future. The two industry experts agreed that businesses of small to medium sizes are often most worried about the simple question – "Can ransomware affect us?" While this question remains pertinent due to the ever-exploding threat of ransomware infection, it is also wise to look beyond it and invest in some basic hygiene steps such as reviewing the incident response policy, having someone on speed dial to provide incident response, and effectively taking backups amongst others. Because let's be sure, just as we are reviewing what happened and what can we do better next time, so are the attackers. They're looking in the rear-view mirror too to see where they went wrong this time and how not to get undercut the next time.

The only way to beat the advanced adversary for us, as a community, is to work together and collaborate, not just in terms of threat intel but beyond.

In case of the Kaseya ransomware attack earlier this year, for example, because companies worked together, maybe they didn't detect the attack very quickly, but they remediated it much better and therein lies a massive lesson for businesses and the cybersecurity community as a whole.

The SolarWinds Cyber-Attack timeline has also been created with this vision – to empower the community as a whole to work together and do better next time collaboratively. You can download the detailed timeline here.

The webinar was concluded with a succinct list of **recommendations** from IronNet and Cyber Management Alliance. Some of these are:

1. Review your log retention policies very regularly.
2. Create a culture of testing updates from a security perspective.
3. Understand your network and implement Behavioral Network Analytics to assist in finding the TTPs.
4. Work together through collective defence.

Watch the webinar here: What exactly happened in the SolarWinds cyber-attack?

Check out our BrightTALK channel for more interesting conversations about everything cybersecurity.

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

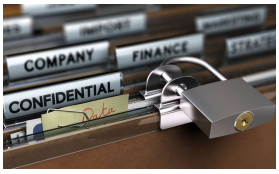
SUBSCRIBE
TO OUR YOU TUBE CHANNEL

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