You survived the SolarWinds hack. Now what?

Aidan Lynch, VIAVI

Aidan Lynch is director, enterprise and cloud, Viavi Solutions

Maybe your organization only suffered a minor intrusion - but you need to protect against future events

August 12, 2021 Comment

So, your company survived the SolarWinds attack of 2020, also known as the Sunburst hack, relatively unscathed, with only a minor intrusion into your network. Perhaps the hackers didn't get any sensitive data... this time. Next time you may not be so lucky. As the frequency and sophistication of cyber-attacks continues to escalate, so do the costs — in terms of time, legal fees and the incalculable damage to your reputation.

Threat detection and remediation can be a time-consuming process, involving significant hours spent manually reviewing logs, quarantining servers, and shutting down user credentials. How can enterprises reduce their exposure to future breaches, and what are the most important considerations for conducting remediation after this type of inevitable attack?

Zero Trust evolution

The hack is deemed by some to be the biggest cyber-attack of 2020, and possibly the past decade. It began with a breach in the Orion IT network management software used by SolarWinds, a software company with extensive US government contracts, and affected at least 18,000 organizations, ranging from enterprises such as Microsoft and Intel, to multiple branches of the US government. Considering the overwhelming success achieved by the hackers (believed to be working for the Russian government), it's a safe bet that a similar tactic will be used again. But how do you protect against a breach where a trusted vendor unwittingly serves as a back door?

In today's cloud-first, work from anywhere (WFX) environment, many enterprises are moving to Zero Trust security frameworks to protect against risks inside the traditional network boundaries, such as malicious internal actors or stolen credentials. A departure from the 'trust but verify' approach to network security, Zero Trust is more than just authentication. These frameworks lock down every pair of credentials, all devices, every vendor, and the organization's complete database of data sets.

Because Zero Trust eliminates implicit trust in any network element or service, continuous real-time verification is required to maintain access to the network. Successfully implementing this security model requires a comprehensive strategy and a complete picture of the state of the network. This intricate operation is further complicated by today's complex network architectures, as well as continuing migration to the cloud.

As organizations adopt Zero Trust, an inconvenient truth is that some employees will try to find simpler ways to work around strict network access protocols. In fact, as workers were sent home to work remotely at the start of the Covid-19 pandemic, the use of unauthorized remote access tools increased by 75 percent between January and March 2020. The ongoing WFX trend is only going to exacerbate this rise in shadow IT.

Even with the adoption of more stringent security protocols, the next supply chain cyber-attack is inevitable. The question remains: How do you know if the hacker has accomplished their goals? If a bad actor can enter the network via trojanized software updates, there will be clues in the network history. Evidence-based risk management strategies apply information gleaned from the network itself to determine the scope and impact of the breach, in order to facilitate remediation.

According to the Cybersecurity and Infrastructure Security Agency (CISA), the first step in threat remediation is to forensically image system memory and/or host operating systems. Network operations (NetOps) teams should then look for new user or service accounts, privileged or otherwise, and analyze stored network traffic for indications of compromise. However, the ability to take those steps is dependent on the network monitoring and forensics tools in place in the network. And, of course, the time to implement those tools is *before* a breach in order to have historical data that chronicles the malicious activity.

In addition, it's important to consider the type of network monitoring being used. Even if an organization implements Zero Trust security, real-time monitoring is key to being able to detect, investigate and remediate intrusions. If monitoring tools are merely 'sampling' traffic, rather than capturing real-time packet and flow data, it's very easy to miss the telltale signs of abnormal network activity until it's too late.

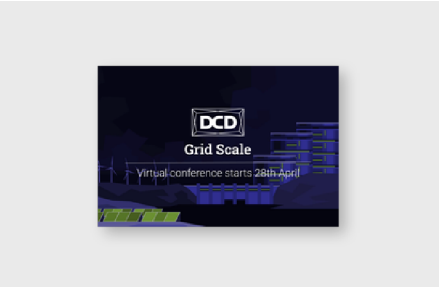
The growing number and variety of devices and applications in today's hybrid IT environment are becoming increasingly difficult to monitor — from IoT devices, cloud migrations and SD-WAN, to remote users at the network edge. Network observability with full forensic detail is needed to accurately determine dependencies across the organization. Enriched flow data allows NetOps to have increased visibility from one end of the network to the other in real-time, providing insight into the devices that are connected, who is talking, and what they are saying. This level of detail, for example, can help an IT professional identify the actual server involved in the conversation, instead of just the virtual address of the load balancer assigning a conversation to a server.

Beyond best efforts

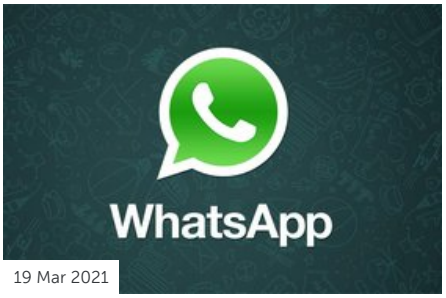
It may sound cliché, but the fact remains that it's not a matter of *if* there will be another cyber-attack, but *when* the next breach will occur. When it comes to threat detection and remediation, as Yoda would say, "Do... or do not. There is no try." In other words, your 'best effort' is not good enough anymore. You need to achieve 110 percent preparation or you *will* experience serious consequences.

It may not be possible to prevent future breaches. But enterprises can still take precautions to safeguard their networks by adopting a holistic security solution that incorporates a Zero Trust model in combination with network monitoring, threat detection and forensic remediation capabilities.

More in Outages

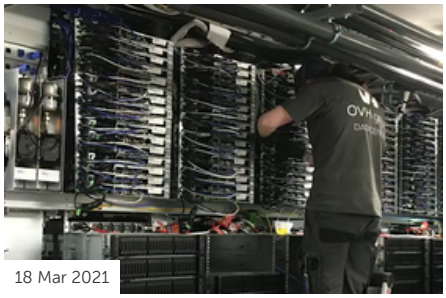


DCD>Grid Scale Event Preview



19 Mar 2021

Facebook, Instagram, and WhatsApp briefly down



18 Mar 2021

OVH fire: racks are switched on in SBG1