'The Internet Is On Fire': SolarWinds Attack Highlights Demand For Data Center Security

January 24, 2021 | Annie Gaus, Bisnow Data Center Reporter (https://www.bisnow.com/author/annie-gaus-363253) (mailto:annie.gaus@bisnow.com)

A devastating cyberattack that affected multiple government agencies has deeply unsettled the IT industry and could lead to a paradigm shift in how organizations secure data.

SolarWinds, an IT software vendor whose customers include federal agencies and major enterprises, confirmed in December that hackers inserted malware into its Orion platform, a software suite commonly used for network monitoring.

The unusually sophisticated attack compromised the Department of the Treasury, the Department of Commerce and the Department of Homeland Security, and exposed Microsoft (https://www.bisnow.com/tags/microsoft)'s source code, among other things. When the full scope of the attack is revealed, the fallout is expected to be extensive.

"I've told people who don't understand the significance of the breach: The internet is on fire," said Ted Wagner, chief information security officer at SAP National Security Services. "SolarWinds is a prevalent system that's used very widely, and the fact that an adversary accessed the way it distributed updates and software shocked me and many of my peers."

The technique used in the SolarWinds breach is what is known as a supply chain attack, whereby an attacker inserts malware into software created by a third-party vendor, subsequently infecting its customers. In the case of SolarWinds' Orion software, which plugs into network infrastructure, the malware was able to worm its way into critical government systems.

"Network infrastructure doesn't get as much scrutiny as a laptop or endpoint device. ... Many folks expect trust in this area, but there are vulnerabilities," Wagner said.

The SolarWinds incident revealed a blind spot in network security, said Atiq Raza, executive chairman at Virsec Systems, a security software firm.

"SolarWinds was a remote code execution attack that occurred in their supply chain. It executed undetected during runtime, which is a blind spot for most organizations," he said. "Sophisticated attacks that occur at runtime are a notorious blind spot in data centers (https://www.bisnow.com/tags/data-centers) because conventional tools are not enough to detect exploits in memory and do not provide any visibility into runtime."

For the time being, security professionals are rapidly taking stock of how to better vet and monitor key software vendors like SolarWinds, which has about 300,000 total customers, in the future. For its part, the company said in a Dec. 14 regulatory filing (https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/57108215-4458-4dd8-a5bf-55bd5e34d451.pdf) that it issued security updates as soon as the attack was detected and was advising customers on additional mitigation steps.

"The SolarWinds supply chain attack is one of the most damaging attacks we've seen in recent memory, even though we are still understanding the scope of impact. It has also heightened concern for how we can prevent similar types of attacks against the data center (https://www.bisnow.com/tags/data-center)," said Dave Burton, vice president of marketing at Guardicore, which sells data center security software. "IT security professionals should take a 'when, not if' posture to data center breaches."

Physical data centers typically come equipped with various security measures, which could encompass anything from biometric entry points to unusually remote locations in order to safeguard sensitive data. Some data center providers also offer managed services along with physical space, which can add an additional layer of security monitoring above and beyond their customers' own infrastructure.

The SolarWinds incident highlights the role data centers can play, now and in the future, in rooting out bruising cyberattacks. As competition grows in the data center industry, colocation firms are likely to offer increasingly

sophisticated security features (https://www.bisnow.com/san-francisco/news/data-center/how-ai-is-rapidly-reshaping-the-data-center-market-106720) to customers wary of falling prey to a cyberattack.

Data center operators should take the opportunity to examine their security protocols, said Val Milshtein, chief technology officer at Stack Infrastructure, a fast-growing wholesale data center development firm.

"Data center operators must treat IT services such as SolarWinds as public domain, restricting connectivity to critical infrastructure management networks," Milshtein said. "Critical infrastructure management networks underpin the command and control nerve center of data center operations. This latest incident is a good reminder to examine and strengthen control policies preventing outside connections, vendor and client networks, even mobile devices from establishing connections to these networks."

CORRECTION, JAN. 28, 2:45 P.M. ET: *A previous version of this story mischaracterized Stack Infrastructure, which is a wholesale data center developer. The story has been updated.*

Contact Annie Gaus at annie.gaus@bisnow.com (mailto:annie.gaus@bisnow.com)

See Also: Multistory Data Centers On The Rise In Dense Markets (/national/news/data-center/multistory-data-centers-on-the-rise-in-dense-markets-107378)

Related Topics: Data Centers (https://www.bisnow.com/tags/data-centers)