The SolarWinds supply chain attack is already one of the most serious and significant cybersecurity incidents ever. Over 18,000 SolarWinds customers were affected, including US Treasury and departments of Commerce, Defense, Energy, and Homeland Security, Microsoft, Intel, Cisco, and Deloitte, etc. While it's not easy to quantify the financial impact associated with the attack, some estimated that the cost of containing and repairing the damage at upwards of $100 billion[1].

The malware was deployed in March 2020 as part of an update from SolarWinds' own servers and was digitally signed by a valid certificate bearing its name. It was not discovered until December 2020. After an initial dormant period of up to two weeks, the malware would retrieve and execute commands to transfer files, execute files, profile the system, reboot the system, and disable system services.

While the attackers used creative methods to deliver the malware and leveraged multiple techniques to evade detection and obscure their activity, they chose the ubiquitous DNS to exfiltrate data, just like a huge percentage of malwares because DNS traffic sails through firewalls. Stolen data was transmitted by appending it to recursive DNS queries. DNS also played a major role in communications between the malware and C2 (Command and Control) servers.

DNS is essential to business functions, but it is often overlooked when it comes to securing the enterprise network. This attack demonstrated the importance to secure the DNS layer of the network. ***CleverDetect® for DNS*** can help monitor the health of your DNS service for availability and performance. It also provides real-time ***DNSDiff™*** to ensure the data integrity of your critical DNS records.

Learn More About CleverDetect for DNS and AES CLEVER Family of Products

Free Trial **Webinar** **Website** **Email**

Applied Expert Systems LLC | PO BOX 50927, Palo Alto, CA 94303