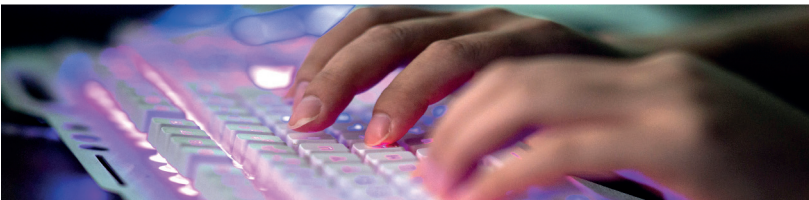


Massive cyber attack hits U.S. agencies

Following a global cyber-espionage attack that penetrated multiple U.S. government agencies and private organisations, governments worldwide are scrambling to see if they, too, are victims



■ **Supply chain attack:** Pathway into victim's network relies on access to supplier, in this case **SolarWinds**. Texas-based company provides **Orion** network monitoring services to government agencies and companies

■ **Dec:** Cybersecurity company **FireEye** discovers its Orion software has been hacked. Attackers steal FireEye's tools used to probe its customers' defences

solarwinds



■ **Mar-Jun 2020:** Malicious code creates "**Sunburst**" backdoor in updates to SolarWinds' Orion Platform software.



Hackers gain remote access into networks of some 18,000 agencies that have installed updates

■ **Sunburst backdoor:** Masquerades as Orion software, appearing as legitimate traffic. Backdoor gives unrestricted access to internal email systems of agencies



■ **Hacked networks:** Communicate with hackers' server domain name – **avsvmcloud[.]com** – one of several domains that attackers have set up to control victims' networks



FireEye probes 50,000 lines of SolarWinds source code and discovers backdoor. Alerts SolarWinds and law enforcement

■ **Dec 17:** FireEye teams up with **Microsoft** and domain registrar **GoDaddy** to create "**killswitch**" for backdoor

■ **Killswitch:** GoDaddy redirects domain **avsvmcloud[.]com** to IP address **20.140.0.1** that belongs to Microsoft. Malicious traffic coming to this domain is analysed to identify perpetrators

■ **U.S. government agencies affected:** Energy, Commerce, Homeland Security, Pentagon, Treasury, U.S. Postal Service, National Institutes of Health

