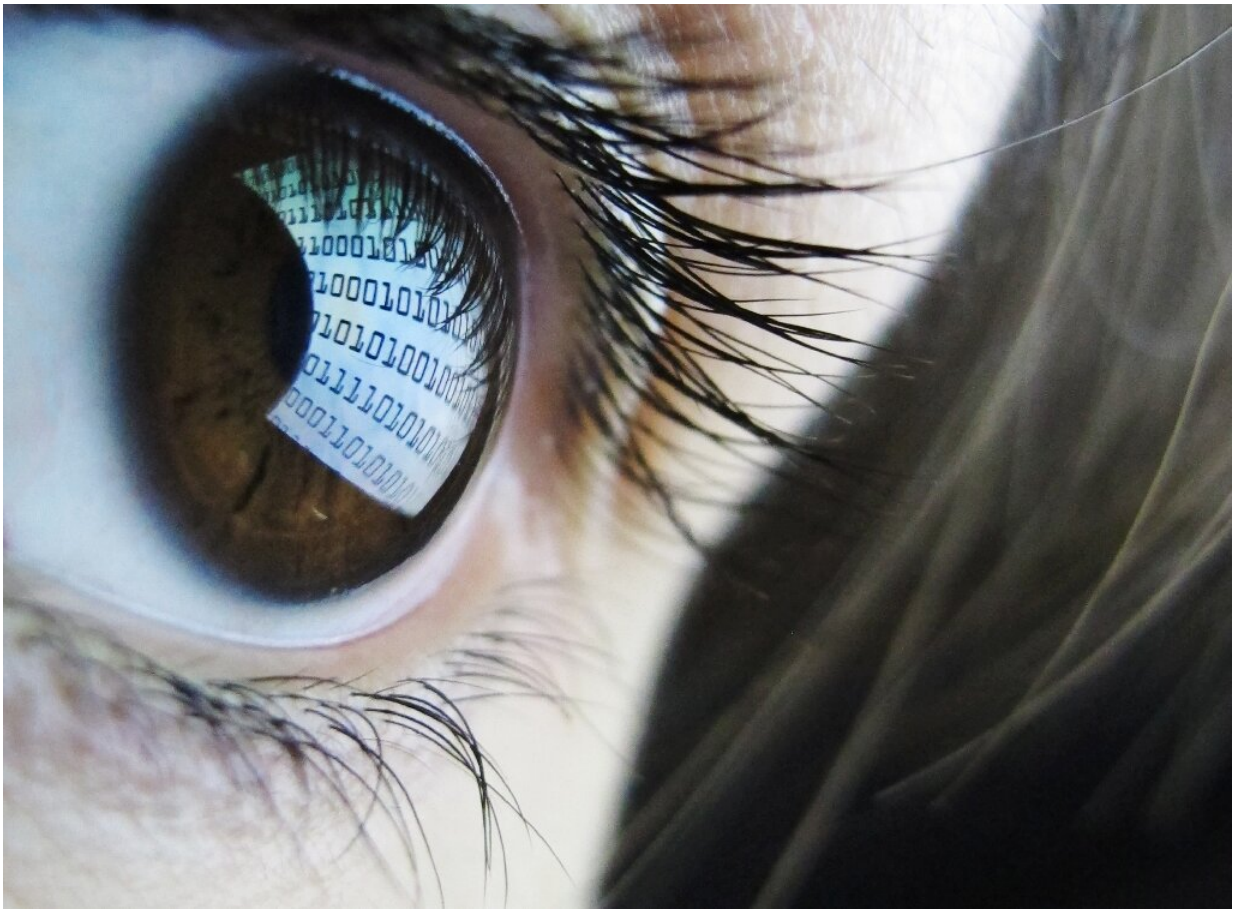
Data crunching consequences of SolarWinds cyberattack

December 17 2020



The cyberattack via SolarWinds software compromised the systems of several US government agencies, but the extent of the damage is still unknown

Thousands of companies and institutions across the globe have to check

if they have been hacked via security software from Texan firm SolarWinds at the heart of a cyberattack on several US government agencies.

Here is what we know to date about the sophisticated attack:

How did the hackers get in?

Hackers managed to compromise and instal malware on a piece of security software -– the Orion security tool developed by SolarWinds which is used for management and supervision of IT networks at many large companies and several US government agencies.

Rather than attack directly clients who include top accounting firms—but also the full gamut of military branches—the hackers aimed to compromise the software's automatic update function.

Beyond the content of the data hacked, the break-in further allowed the crypto burglars to gain an idea of their victim's systemic structural vulnerabilities.

The attack was discovered by cybersecurity company FireEye, which, along with SolarWinds, has pointed the finger at people linked to the Russian government.

Taking care only to upload stolen data in relatively small quantities, the hackers reportedly breached software used by the US Treasury Department, the Commerce Department and the Department of Homeland Security, allowing them to view internal email traffic, prompting an FBI investigation.

The software had enjoyed much commercial success based not least on its state of the art ergonomic interface.

The malware was laced into the software updates that breached network security and allowed access to data including mail, with FireEye saying the breaches began around last March.

Who are the victims?

According to SolarWinds, 18,000 users of Orion have potentially suffered a security breach, including government agencies and Fortune 500 companies.

For now, experts say the hackers seem primarily to have used a security flaw, dubbed Sunburst, to break into US governmental agencies, insert malicious code and gain access to data to aid state espionage.

FireEye discovered the flaw through its own usage of SolarWinds and was itself affected by certain tools it was deploying to test its clients' security.

According to FireEye, what it termed a state sponsored attack targeted governments as well as leading global enterprises notably in the technology and energy sectors in North America, Europe, Asia and the Middle East.

According to Jacques de la Riviere, who runs French cybersecurity firm Gatewatcher, it is still too early to know which other firms or institutions have been infiltrated.

The actual content of what the hackers were targeting and to what extent they were successful also remains unknown.

Cybersecurity systems across the globe are on alert to track any suspicious activity that could suggest the compromising of data held by SolarWinds.

Firms or institutions that have used infected updates are urged to disconnect their servers and check for telltale signs their data might have been compromised.

Who is to blame?

FireEye and Microsoft believe the attack was by a nation state and expert analysis has pointed the finger at Russia, as have anonymous US security sources. As yet, Washington has yet to give the accusation its official seal.

These US sources have focused on an organisation known as advanced persistent threat (APT) 29, or Cozy Bear, which is believed to be linked to one or more Russian intelligence agencies and previously pirated the White House under President Barack Obama.

Lessons to learn

Jacques de la Riviere says he has responded by ramping up protection on his own servers.

Beyond that he hopes the high-profile attack will encourage firms and institutions to be more demanding when it comes to stewardship of their data and software security.

"This could be a turning point, where many clients are going to start saying 'I no longer want to purchase software that has not been certified by a third party'," he said.

Citation: Data crunching consequences of SolarWinds cyberattack (2020, December 17)