SolarWinds hack

December 19, 2020

In news

The ‘SolarWinds hack’, a cyberattack recently discovered in the United States, has emerged as one of the biggest ever targeted against the US government, its agencies and several other private companies.

What is ‘SolarWinds hack’?

- SolarWinds hack was first discovered by US cybersecurity company FireEye, and since then more developments continue to come to light each day
- News of the cyberattack technically first broke on December 8, when FireEye put out a blog detecting an attack on its systems.
- CEO of FireEye said that the company was “attacked by a highly sophisticated threat actor”, calling it a state-sponsored attack
- The company also said the attack was carried out by a nation “with top-tier offensive capabilities”, and “the attacker primarily sought information related to certain government customers.” It also said the methods used by the attackers were novel.
- The firm helps with security management of several big private companies and federal government agencies.
- The sheer scale of the cyber-attack remains unknown, although the **US Treasury, Department of Homeland Security, Department of Commerce, parts of the Pentagon are all believed to have been impacted.**

How did so many US government agencies and companies get attacked?

- This is being called a ‘Supply Chain’ attack: Instead of directly attacking the federal government or a private organisation’s network, **the hackers target a third-party vendor, which supplies software to them.**

- In this case, the target was an IT management software called Orion, supplied by the Texas-based company SolarWinds.
- A New York Times report said parts of the Pentagon, Centers for Disease Control and Prevention, the State Department, the Justice Department, and others, were all impacted.
- A Reuters report said that even emails sent by Department of Homeland Security officials were “monitored by the hackers”.

How did the hackers gain access?

- According to FireEye, the hackers gained **“access to victims via trojanized updates to SolarWinds’** Orion IT monitoring and management software”. Basically, a software update was exploited to install the ‘Sunburst’ malware into Orion, which was then installed by more than 17,000 customers.
- It also says that the attackers relied on “multiple techniques” to avoid being detected and “obscure their activity”. The malware was capable of accessing the system files.
- According to FireEye, what worked in the malware’s favour was it was able to “blend in with legitimate SolarWinds activity”.
- **Once installed, the malware gave a backdoor entry to the hackers to the systems and networks of SolarWinds’ customers.** More importantly, the malware was also able to thwart tools such as anti-virus that could detect it.

Where does Russia come in?

- In his New York Times opinion article, Bossert named Russia and its agency SVR, which has the capabilities to execute the attack of such ingenuity and scale.

- Microsoft notes in its blog that “this aspect of the attack created a supply chain vulnerability of nearly global importance, reaching many major national capitals outside Russia”. It goes on to add that sophisticated attacks from Russia have become common.

What is a cyber attack?

A cyber attack is a malicious attempt by a third party to damage, destroy or alter:

- computer networks
- computer information systems
- computer or network infrastructure
- personal computer devices

Criminals launch cyber attacks for many reasons: to steal money, access financial and sensitive data, weaken integrity or disrupt the operations of a company or an individual. Attacks often result in crimes such as financial fraud, information or identity theft.

Examples of cyber attacks

Cyber attackers use many different methods to try to compromise IT systems. Most common practices are:

- remote attacks on IT systems or website
- unauthorised access to information held on a corporate network or systems
- unauthorised access to data held in third-party systems (eg hosted services)
- system infiltration or damage through malware
- disruption or denial of service that limits access to your network or systems

Some of the malware that were in news:

- CovidLock, ransomware, 2020.
- LockerGoga, ransomware, 2019.
- Emotet, trojan, 2018.
- WannaCry, ransomware, 2017.
- Petya, ransomware, 2016.
- CryptoLocker, ransomware, 2013.
- Stuxnet, worm, 2010.

What are the recommendations of the US government and SolarWinds?

- As of now SolarWinds is recommending that all customers immediately update the existing Orion platform, which has a patch for this malware.
- Those unable to update are told to isolate “SolarWinds servers” and it should “include blocking all Internet egress from SolarWinds servers”. The bare minimum suggestion is the “changing passwords for accounts that have access to SolarWinds servers / infrastructure”.
- The US Cybersecurity and Infrastructure Security Agency (CISA) has issued an Emergency Directive 21-01, asking all “federal civilian agencies to review their networks” for indicators of compromise.
  - It has asked them to “disconnect or power down SolarWinds Orion products immediately”.
- The FBI, CISA and office of the Director of National Intelligence issued a joint statement, and announced what is called the **‘Cyber Unified Coordination Group (UCG)”** in order to coordinate government response to the crisis.
  - The statement calls this a “significant and ongoing cybersecurity campaign.”
- President-elect Joe Biden said in a statement: “A good defense isn’t enough; We need to disrupt and deter our adversaries from undertaking significant cyber attacks in the first place.”