Solar Wind Cyber Attack

sanskritiias.com/current-affairs/solar-wind-cyber-attack

Context: The massive cyber attack hits government agencies and Microsoft.

In Detail: The scale of a sophisticated cyber attack on the U.S. government that was unearthed recently is much bigger than first anticipated. The Cybersecurity and Infrastructure Security Agency said in a summary that the threat poses a grave risk to the federal government.

It added that state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations are also at risk. CISA believes the attack began at least as early as March. Since then, multiple government agencies have reportedly been targeted by the hackers, with confirmation from the Energy and Commerce departments so far.

Microsoft has not confirmed what source code was accessed by the hackers. However, the fact that the hackers got in so deep is quite worrying, given source code is crucial to how any piece of software works.

As part of its ongoing investigations in the SolarWinds cyberattack, Microsoft has revealed that its internal source code was likely accessed by the attackers. The company had earlier confirmed that it too was compromised is what is being seen as one of the world's largest cyberattack, that primarily targeted the United States (US) government and several other private organisations. The SolarWinds cyberattack was first revealed in December by cyber-security firm FireEye.

We take a look at what Microsoft's latest investigation has revealed, and what it means.

Investigation & Impact

The Internal team for Security and Research of the has found evidence that the attackers accessed some internal source code in the company's systems. The Solorigate incident as Microsoft has termed it in the writing, showed there were attempted activities beyond just the presence of malicious SolarWinds code in our environment.

They detected unusual activity with a small number of internal accounts and upon review, they discovered one account had been used to view source code in a number of source code repositories. According to the post, the account did not have required permissions to access the code, to modify it, nor was it authorized to access the engineering systems.

The company says so far the investigation confirmed no changes were made to this source code. These accounts were investigated and remediated.

Threat to Data

It is still not confirmed what source code was accessed by the hackers. However, the fact that the hackers got in so deep is quite worrying, given source code is crucial to how any piece of software works. Source code is the key to how a software product is built and if compromised could leave it open to new, unknown risks. Hackers could use this information to exploit any potential weakness in the programmes.

Microsoft says this activity has not put at risk the security of our services or any customer data, but adds they believe this attack was carried out by a very sophisticated nation-state actor. The company says that there's no evidence that its systems were used to attack others.

Other Related Investigations

Based upon the further investigation, Microsoft presumed that attackers might have knowledge of source code they rely on "open-source software development best practices" and "an open source-like culture" for development of software. Typically, source code is viewable by teams within Microsoft, according to the blog. Microsoft is downplaying the risk saying just viewing the source code should not cause any new elevated risks.

Microsoft says it has plenty of defense protections in place to stop attackers if and when they do gain access. It says there is evidence the activities of the hackers were “thwarted” by the company’s existing protections.

Graveness

The problem with this cyberattacks is that it has been going on for so long that the full scale remains unknown. In fact, the attack may have started earlier than last spring as previously believed. It is stated that at the moment the US government does not have hard evidence that classified government secrets were compromised by the hackers.

The sheer scale of the attack also remains unknown, according to most reports. Meanwhile, FireEye, which discovered the attack, has revealed new details about the Sunburst malware. The malware exploited the SolarWinds Orion software, which is used by thousands of companies, including several US government agencies.

Conclusion

According to FireEye, Sunburst a malicious version of a digitally signed SolarWinds Orion plugin contains a backdoor that communicates via HTTP to third-party servers. It appears that the plugin remains dormant period of up to two weeks, after which it starts executing commands and carrying out tasks such as transfer of files, execute files, profile the system, reboot the system, and disable system services.

It also appears that the malware “performs numerous checks to ensure no analysis tools are present,” according to FireEye. This cautious approach is what helped the malware “evade detection by anti-virus software and forensic investigators for seven months after its introduction to the SolarWinds Orion supply chain,” according to the cyber-security firm.

Connecting the Article

Question for Prelims : Consider the following statements:

1.Source code is the key to how a software product is built.

2.Hackers could use information to exploit weakness in the programmes.

Which of the statements given above is/ are correct?

(a) 1 only

(b) 2 only

(c) Both 1 and 2

(d) Neither 1 nor 2

Question for Mains : Malware performs numerous checks to ensure no analysis tools are present. Explain.

« »

- SUN
- MON

- TUE
- WED
- THU
- FRI
- SAT

-
-
-
-
-
- 01
- 02
- 03
- 04
- 05
- 06
- 07
- 08
- 09
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
-

-
-
-
-
-