Lapsus$

March 24, 2022

In news– Microsoft has recently published a detailed cybersecurity blog confirming that its systems were breached by the hacker group Lapsus$.

What is Lapsus$?

- **South America-based Lapsus$ is known for publicly posting details about their hacks and sharing screenshots** of stolen data on platforms such as Telegram and Twitter.
- It is a hacker group that has targeted Microsoft, Samsung, Okta and Nvidia.
- They are also **known for hijacking cryptocurrency accounts**.
- The group has been **given the designation DEV-0537 by Microsoft's cybersecurity researchers,** has been expanding the geographic range of its targets and going after government organizations as well as the tech, telecom and health-care sectors, according to the blog post.
- Lapsus$ has made claims on social media that it's infiltrated several large tech companies besides Microsoft.
- **Microsoft's blog post** said that the **hackers relied on large-scale social engineering and extortion campaigns against multiple organizations.**
- **In social engineering attacks, cybercriminals try to lure individuals into revealing critical personal information** via phishing attacks and this information can then be used to compromise other accounts.
- All of this information might be used to either guess passwords or even answers to security questions for an account.
- According to Microsoft, the group also relied on a "**pure extortion and destruction model without deploying**

ransomware payloads.”

- **Their targets are across a range of sectors:** government, technology telecom, media, retail and healthcare. It is also attacking cryptocurrency exchanges to steal cryptocurrency holdings.
- In some cases, it has even paid employees or suppliers at an organization in order to gain access to privileged networks and systems.
- Another example talks about the group calling up an organization’s helpdesk to reset a target’s credentials.
- **For now, Microsoft has recommended that businesses rely on Multi-Factor Authentication (MFA) t**o protect themselves from such attacks.
- It also recommends against weak MFA factors such as text messages, since these are susceptible to SIM swapping.
- It has also cautioned against simple voice approvals, push notifications, or even “secondary email” based MFA methods.