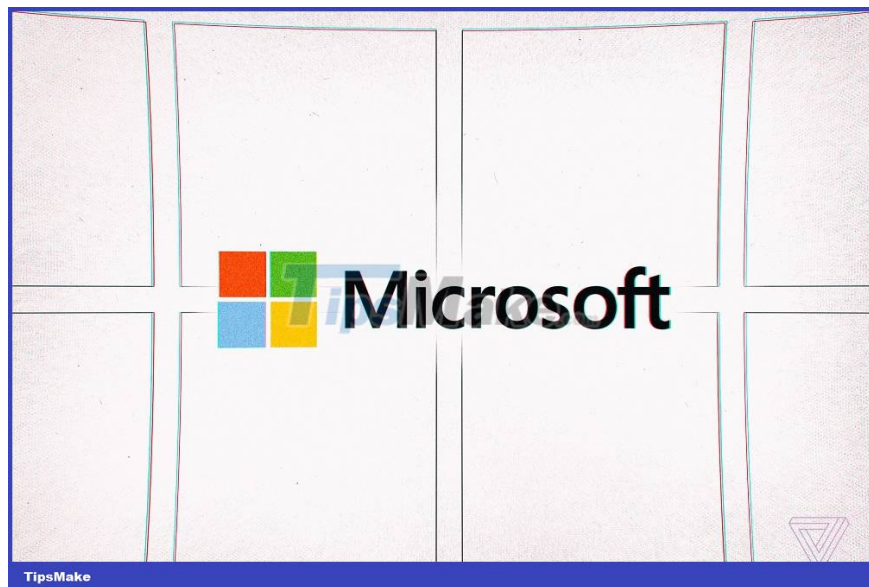


Microsoft admits that hacker Lapsus\$ stole the source code

A series of major technology companies in the world are becoming victims of the Lapsus\$ hacker group. After attacking Nvidia, Samsung and many other companies, recently this group of hackers also claimed to have successfully hacked Microsoft and obtained part of the source code of Bing and Cortana in a block of data of nearly 37GB.

After investigation, Microsoft itself now has to admit that a group of hackers known by the company as DEV-0537 compromised "a single account" and stole part of the source code of some of its products.

The company's security blog post said that Microsoft investigators have been tracking Lapsus\$ for weeks now, as well as details of the method they used to penetrate the victim's system.



According to the Microsoft Threat Intelligence Center (MSTIC), "the goal of the DEV-0537 group is to gain high-level access through the theft of credentials to steal data and perform attacks." sabotage against the targeted organization, often leading to extortion. Tactics and targets indicate that this is a cybercrime fueled by theft and vandalism."

Microsoft also asserted that the leaked source code was not severe enough to pose a high risk and that the company's response team blocked the hacker's attack.

Lately, Lapsus\$ has become a terror to major tech companies when the group claims to have collected data from companies including Okta, Samsung, Ubisoft, Nvidia and now Microsoft. While companies like Samsung and

Nvidia acknowledged the data was stolen, Okta denied the group's claims, saying: "Okta's services were not compromised and remain fully functional."

This is not the first time Microsoft has suggested that attackers have gained access to their source code - something similar happened in the recent Solarwinds attack. Lapsus\$ also admitted that it only had access to 45% of the Bing and Cortana source code and about 90% of the Bing Maps source code. Even so, the Bing Maps source code doesn't appear to be as valuable as the other two products even as Microsoft worries about the source code exposing their vulnerabilities.

In its blog post, Microsoft outlines several steps other organizations can take to improve their security, including multi-factor authentication, which doesn't use weak authentication methods. like SMS messages or secondary email addresses, train team members on the dangers of cyberattacks, and create a process to respond to attacks like Lapsus\$'s.

You finished reading the article "**Microsoft admits that hacker Lapsus\$ stole the source code**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.