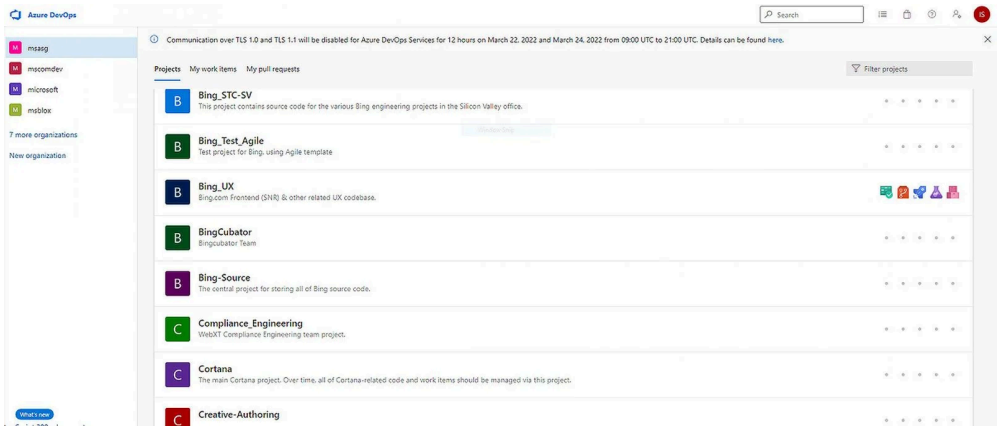
Lapsus$ hackers leak 37GB of Microsoft's alleged source code

By Lawrence Abrams

Published: 2022-03-22 · Archived: 2026-04-05 13:20:42 UTC

The Lapsus$ hacking group claims to have leaked the source code for Bing, Cortana, and other projects stolen from Microsoft's internal Azure DevOps server.

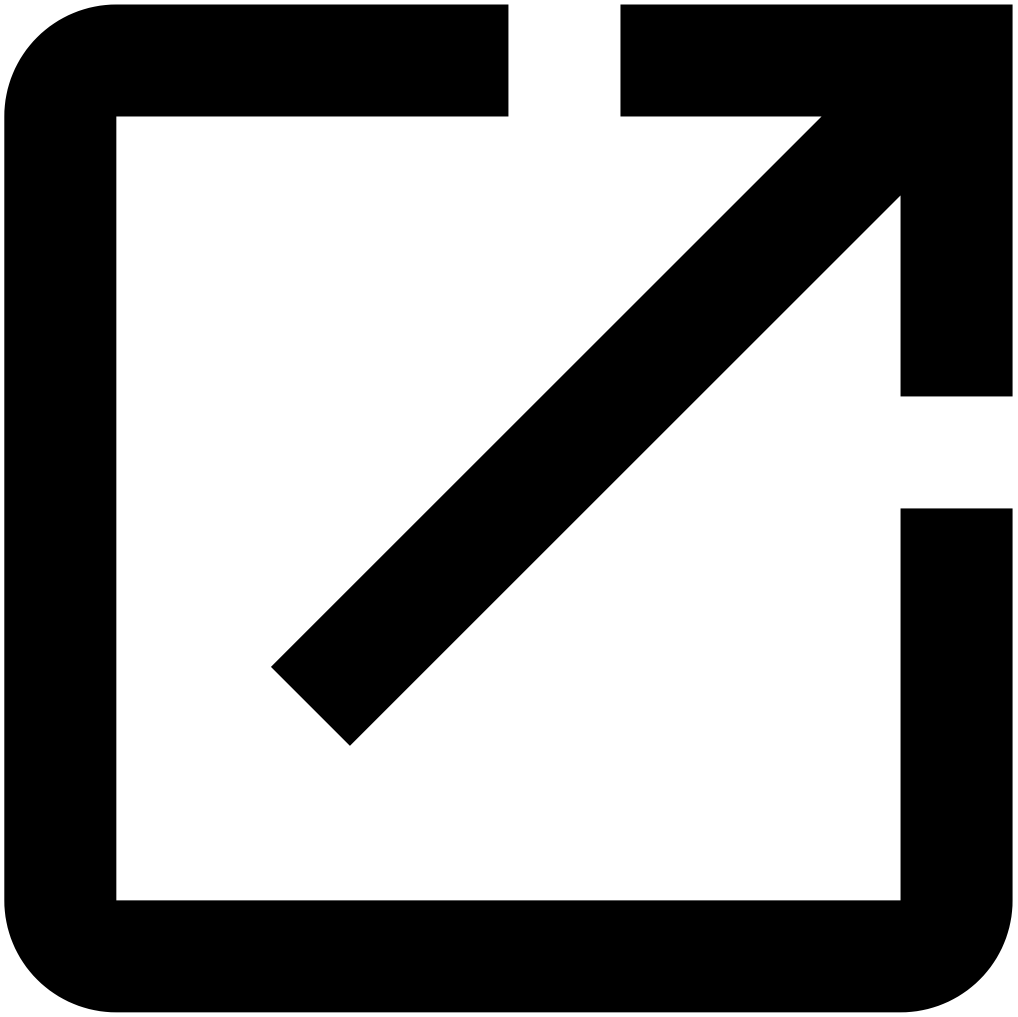
Early Sunday morning, the Lapsus$ gang posted a screenshot to their Telegram channel indicating that they hacked Microsoft's Azure DevOps server containing source code for Bing, Cortana, and various other internal projects.



Screenshot of Microsoft's Azure DevOps account leaked by Lapsus$

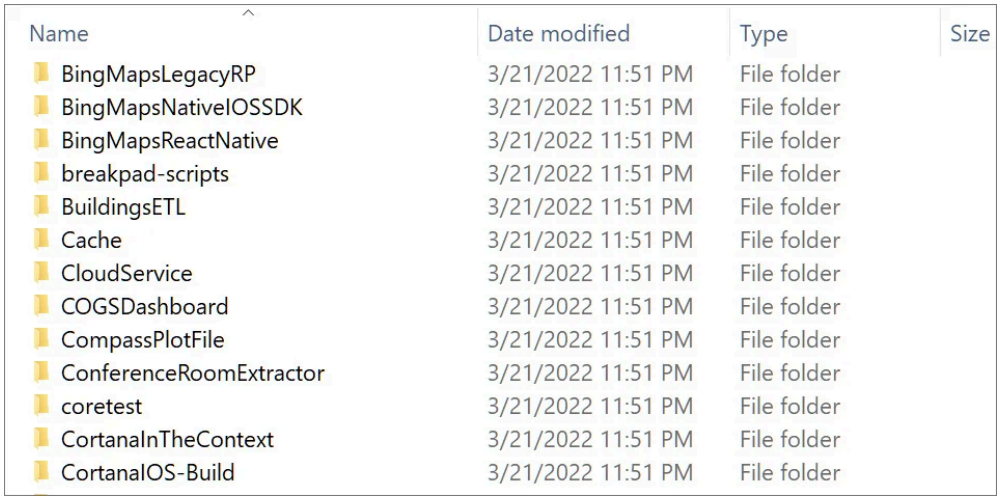
Monday night, the hacking group posted a torrent for a 9 GB 7zip archive containing the source code of over 250 projects that they say belong to Microsoft.


DIE LINKE.
0:00



When posting the torrent, Lapsus$ said it contained 90% of the source code for Bing and approximately 45% of the code for Bing Maps and Cortana.

Even though they say only some of the source code was leaked, BleepingComputer is told that the uncompressed archive contains approximately 37GB of source code allegedly belonging to Microsoft.



Name	Date modified	Type	Size
BingMapsLegacyRP	3/21/2022 11:51 PM	File folder	
BingMapsNativeIOSSDK	3/21/2022 11:51 PM	File folder	
BingMapsReactNative	3/21/2022 11:51 PM	File folder	
breakpad-scripts	3/21/2022 11:51 PM	File folder	
BuildingsETL	3/21/2022 11:51 PM	File folder	
Cache	3/21/2022 11:51 PM	File folder	
CloudService	3/21/2022 11:51 PM	File folder	
COGSDashboard	3/21/2022 11:51 PM	File folder	
CompassPlotFile	3/21/2022 11:51 PM	File folder	
ConferenceRoomExtractor	3/21/2022 11:51 PM	File folder	
coretest	3/21/2022 11:51 PM	File folder	
CortanaInTheContext	3/21/2022 11:51 PM	File folder	
CortanaIOS-Build	3/21/2022 11:51 PM	File folder	

Leaked source code projects

Security researchers who have pored over the leaked files told BleepingComputer that they appear to be legitimate internal source code from Microsoft.

Furthermore, we are told that some of the leaked projects contain emails and documentation that were clearly used internally by Microsoft engineers to publish mobile apps.

The projects appear to be for web-based infrastructure, websites, or mobile apps, with no source code for Microsoft desktop software released, including Windows, Windows Server, and Microsoft Office.

When we contacted Microsoft about tonight's source code leak, they continued to tell BleepingComputer that they are aware of the claims and are investigating.

Lapsus$ leaks data left and right

Lapsus$ is a data extortion hacking group that compromises corporate systems to steal source code, customer lists, databases, and other valuable data. They then attempt to extort the victim with ransom demands not publicly to leak the data.

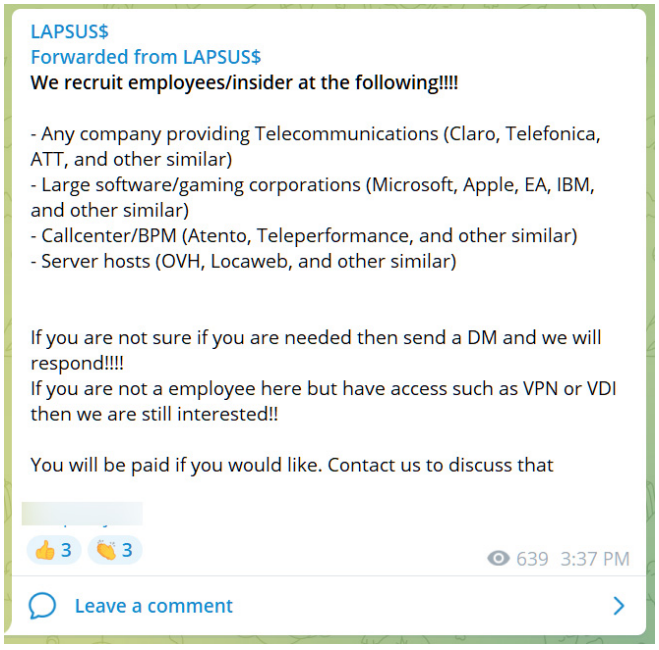
Over the past few months, Lapsus$ has disclosed numerous cyberattacks against large companies, with confirmed attacks against NVIDIA, Samsung, Vodafone, Ubisoft, and Mercado Libre.

So far, most of the attacks have targeted source code repositories, allowing the threat actors to steal sensitive, proprietary data, such as NVIDIA's lite hash rate (LHR) technology that enables graphics cards to reduce a GPU's mining capacity.

It is unknown how the threat actors are breaching these repositories, but some security researchers believe that they are paying corporate insiders for access.

"From my perspective, they keep on getting their access using corporate insiders," threat intelligence analyst Tom Malka told BleepingComputer.

This theory is not far-fetched, as Lapsus$ has previously announced that they are willing to buy access to networks from employees.



Lapsus$ recruiting corporate insiders

However, it may be more than that, as Lapsus$ posted screenshots of their access to what they claim are Okta's internal websites. As Okta is an authentication and identity management platform, if Lapsus$ successfully breached the company, they could potentially use that as a springboard to the company's customers.

As for Lapsus$, they have grown a large following on Telegram, with over 33,000 subscribers on their main channel, and over 8,000 on their chat channel.

The extortion group uses their very active Telegram channels to announce new leaks, attacks, and to chat with their fans, and they seem to be enjoying the notoriety.

With the RaidForums data breach forum shut down, we are likely seeing many of the regulars from that site now interacting together in Lapsus$'s Telegram channels.

For the time being, we will likely see more breaches coming while Lapsus$ and their fans celebrate the data leaks.
