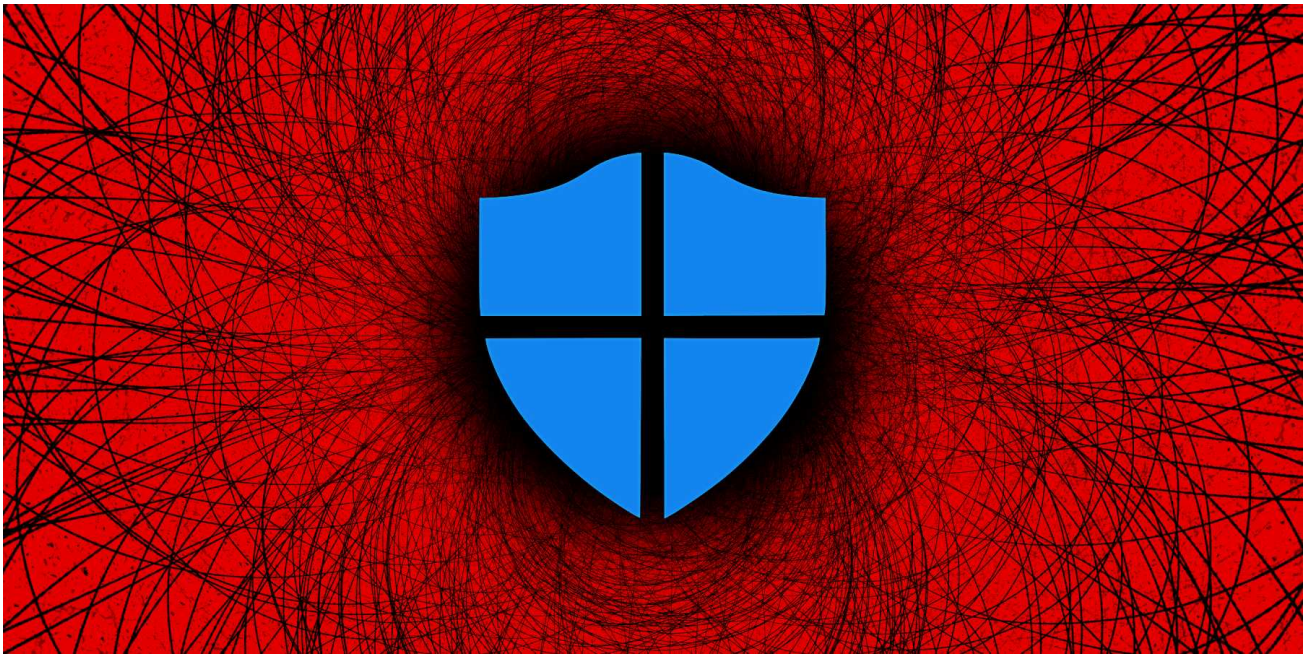
Microsoft confirms they were hacked by Lapsus$ extortion group

bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/

Lawrence Abrams

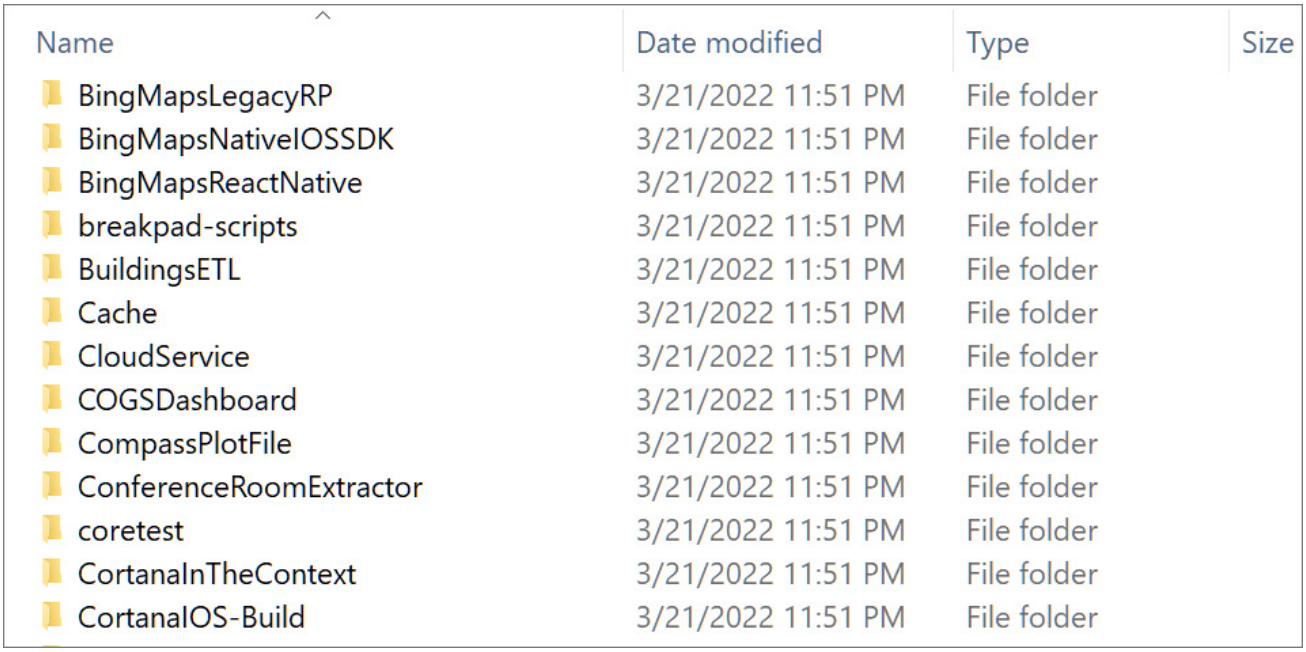
By
Lawrence Abrams

- March 22, 2022
- 08:13 PM
- 0



Microsoft has confirmed that one of their employees was compromised by the Lapsus$ hacking group, allowing the threat actors to access and steal portions of their source code.

Last night, the Lapsus$ gang released 37GB of source code stolen from Microsoft's Azure DevOps server. The source code is for various internal Microsoft projects, including for Bing, Cortana, and Bing Maps.



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

In a new blog post published tonight, Microsoft has confirmed that one of their employee's accounts was compromised by Lapsus$, providing limited access to source code repositories.

"No customer code or data was involved in the observed activities. Our investigation has found a single account had been compromised, granting limited access. Our cybersecurity response teams quickly engaged to remediate the compromised account and prevent further activity," explained Microsoft in an advisory about the Lapsus$ threat actors.

"Microsoft does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk. The tactics DEV-0537 used in this intrusion reflect the tactics and techniques discussed in this blog."

"Our team was already investigating the compromised account based on threat intelligence when the actor publicly disclosed their intrusion. This public disclosure escalated our action allowing our team to intervene and interrupt the actor mid-operation, limiting broader impact."

While Microsoft has not shared how the account was compromised, they provided a general overview of the Lapsus gang's tactics, techniques, and procedures (TTPs) observed across multiple attacks.

Focusing on compromised credentials

Microsoft is tracking the Lapsus$ data extortion group as 'DEV-0537' and says they primarily focus on obtaining compromised credentials for initial access to corporate networks.

These credentials are obtained using the following methods:

- Deploying the malicious Redline password stealer to obtain passwords and session tokens
- Purchasing credentials and session tokens on criminal underground forums
- Paying employees at targeted organizations (or suppliers/business partners) for access to credentials and multi-factor authentication (MFA) approval
- Searching public code repositories for exposed credentials

Redline password stealer has become the malware of choice for stealing credentials and is commonly distributed through phishing emails, watering holes, warez sites, and YouTube videos.

Once Laspsus$ gains access to compromised credentials, they use it to log in to a company's public-facing devices and systems, including VPNs, Virtual Desktop infrastructure, or identity management services, such as Okta, which they breached in January.

Microsoft says they use session replay attacks for accounts that utilize MFA, or continuously trigger MFA notifications until the user becomes tired of them and confirms that the user should be allowed to log in.

Microsoft says that in at least one attack, Lapsus$ performed a SIM swap attack to gain control of the user's phone numbers and SMS texts to gain access to MFA codes needed to log in to an account.

Once they gain access to a network, the threat actors use AD Explorer to find accounts with higher privileges and then target development and collaboration platforms, such as SharePoint, Confluence, JIRA, Slack, and Microsoft Teams, where other credentials are stolen.

The hacking group also uses these credentials to gain access to source code repositories on GitLab, GitHub, and Azure DevOps, as we saw with the attack on Microsoft.

"DEV-0537 is also known to exploit vulnerabilities in Confluence, JIRA, and GitLab for privilege escalation," Microsoft explains in their report.

"The group compromised the servers running these applications to get the credentials of a privileged account or run in the context of the said account and dump credentials from there."

The threat actors will then harvest valuable data and exfiltrate it over NordVPN connections to hide their locations while performing destructive attacks on the victims' infrastructure to trigger incident response procedures.

The threat actors then monitor these procedures through the victim's Slack or Microsoft Teams channels.

Protecting against Lapsus$

Microsoft recommends that corporate entities perform the following steps to protect against threat actors like Lapsus$:

- Strengthen MFA implementation
- Require Healthy and Trusted Endpoints
- Leverage modern authentication options for VPNs
- Strengthen and monitor your cloud security posture
- Improve awareness of social engineering attacks
- Establish operational security processes in response to DEV-0537 intrusions

Lapsus$ has recently conducted numerous attacks against the enterprise, including those against NVIDIA, Samsung, Vodafone, Ubisoft, Mercado Libre, and now Microsoft.

Therefore, it is strongly advised that security and network admins become familiar with the tactics used by this group by reading Microsoft's report.

Related Articles:

Attackers hijack UK NHS email accounts to steal Microsoft logins

Heroku forces user password resets but fails to explain why

Microsoft says Russia hit Ukraine with hundreds of cyberattacks

The top 10 password attacks and how to stop them

Hackers use Conti's leaked ransomware to attack Russian companies

- Credential Theft
- Credentials
- Cyberattack
- Lapsus$
- Microsoft
- Source Code

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: