UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00258

LAPSUS$ STRIKES AGAIN: OKTA & MICROSOFT

DATE ISSUED: 30th March 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Microsoft and Okta have joined the growing list of companies who have suffered a breach at the hands of the Lapsus$ gang, who seek to recruit employees to provide insider access and compromise their victims.

BREAKDOWN

Microsoft has confirmed that Lapsus$ managed to gain limited access to project source code repositories by compromising an employee's account. With reassurances that no customer data was involved, their investigation led to the quick resolution and remediation of the compromised account to prevent further activity. Lapsus$ reportedly successfully exfiltrated source code relating to Bing Search Engine, Bing Maps and Cortana voice assistant. Okta have also made it onto the Lapsus$ hit list with approximately 2.5% of its customer affected in a January attack with further data exfiltration occurring in March. Sitel has been named as the third-party vendor responsible for the breach of Okta, however Okta have admitted their due diligence assessments were not up to scratch. They took the company's word that they had the necessary security provisions in place and had fully disclosed the nature and extent of the breach, which it turns out, was not the case. In more recent news, police in the UK have arrested seven individuals who are suspected to be linked to Lapsus$.

REMEDIATION STEPS

- Use Multifactor Authentication (MFA) wherever possible to shore up account entry defences
- Only use modern authentication option for VPNs when connecting remotely to corporate resources
- Apply security-in-depth principles across your endpoints, external facing services and cloud environment
- Educate users on the dangers of social engineering and phishing attacks as well as general cybersecurity best practices.

REFERENCES & RESOURCES

Threatpost
https://threatpost.com/microsoft-lapsus-compromised-one-employees-account/179048/
https://threatpost.com/okta-goofed-lapsus-attack/179129/
https://threatpost.com/lapsus-data-kidnappers-claim-snatches-from-microsoft-okta/179041/
https://threatpost.com/uk-cops-collar-7-suspected-lapsus-gang-members/179098/

ZDNet
https://www.zdnet.com/article/okta-revises-lapsus-impact-upwards-to-potentially-2-5-of-customers/
https://www.zdnet.com/article/okta-names-sitel-in-security-incident-potentially-impacting-hundreds-of-customers/