Hive Pro

THREAT ADVISORY

LAPSUS$ - New extortion group involved in the breach against Nvidia, Microsoft, Okta and Samsung	TA2022075
Threat Level RED	**Publish Date –** Mar 25, 2022

Lapsus$ (DEV-0537) is an extortion threat group that first appeared on December 10, 2021, and has since breached the Brazilian Ministry of Health, NVIDIA, Samsung, Vodafone, Ubisoft, Octa, and Microsoft. Unlike other extortionist groups, which utilize a combination of ransomware and data leaks to monetize their operations, LAPSUS$ is only focused on funding their operations through data leaks publicized on Telegram.

To gain initial access to an organization, Lapsus$ employs a range of tactics, the majority of which are centered on compromising user identities, such as using the malware Redline password stealer to gain access to credentials and session tokens or purchasing session tokens and credentials from criminal underground forums. The threat actor also contacts employees at targeted organizations (or suppliers/business partners) who are then compensated for accessing credentials and MFA clearance. To gain privileges on the target network, the threat actor tries to exploit unpatched vulnerabilities on internally accessible servers, including JIRA, Gitlab, and Confluence. After gaining privileged access to cloud instances of the organization, the threat actor creates a global admin account and sets an Office 365 tenant-level mail transport rule to send all mail in and out of the organization to the newly created account, and then removes all other global admin accounts, effectively locking the organization out of all cloud resources. Lapsus$ often deletes the target's resources and systems after exfiltration.

Organizations can mitigate some of the risks by using the following recommendations:

- A Multifactor Authenticator should be required for all users arriving from all places, including those that are believed to be trustworthy. To reduce the risks of SIM-jacking, avoid using telephony-based MFA approaches.
- Improve and keep an eye on your cloud security posture.
- Improve awareness of social engineering attacks.

The MITRE TTPs commonly used by Lapsus$ are:

TA0001 - Initial Access
TA0003 - Persistence
TA0004 - Privilege Escalation
TA0005 - Defense Evasion
TA0006 - Credential Access
TA0007 - Discovery
TA0009 - Collection
TA0011 - Command and Control
TA0010 - Exfiltration
TA0034 - Impact
T1078 Valid Accounts
T1133 External Remote Services
T1190 Exploit Public-Facing Application
T1199 Trusted Relationship

T1547.006 Boot or Logon Autostart Execution: Kernel Modules and Extensions
T1133 External Remote Services
T1027.002 Obfuscated Files or Information: Software Packing
T1056.004 Input Capture: Credential API Hooking
T1552 Unsecured Credentials
T1111 Two-Factor Authentication Interception
T1497 Virtualization/Sandbox Evasion
T1120 Peripheral Device Discovery
T1082 System Information Discovery
T1012 Query Registry
T1571 Non-Standard Port
T1537 Transfer Data to Cloud Account
T1485 Data Destruction
T1491 Defacement
T1490 Inhibit System Recovery

Actor Details

Name	Target Locations	Target sectors	Motive
Lapsus$ (DEV-0537)	Brazil, United Kingdom, United States	Telecommunication, Technology, Higher education, gaming and government organizations	Data theft and Destruction

Recent Breaches

https://www.microsoft.com
https://www.okta.com/
https://www.nvidia.com/en-us/
https://www.samsung.com/

References

https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/