



Lapsus\$

Threat Report

Dated: 13th April 2022

By Nathan Long

This report contains Threat Hunting research carried out by CSA analysts to outline the subject threat to the reader. It highlights information about current and emerging threats to identify countermeasures which can be put into place to thwart the threat.

Contents

Threat Report.....	2
Executive Summary	2
Summary	3
Tactics, Techniques, Procedures	4
Phase 1: Initial Access.....	5
Phase 2: Reconnaissance and Privilege Escalation.....	8
Phase 3: Exfiltration, destruction, and extortion	9
Latest news	10
Recommendations.....	11
Hunting Queries.....	12
MITRE ATT&CK TTPs used by LAPSUS\$	12
References	14

Private and confidential

The information contained in this report is strictly confidential and intended solely for the use of the recipient. Any other use and any communication, publication or reproduction of the report or any portion of its contents without the written consent of the authors is strictly forbidden. The recipient agrees to indemnify and hold harmless against any damages or claims resulting from such unauthorised use.

Lapsus\$

Threat Report

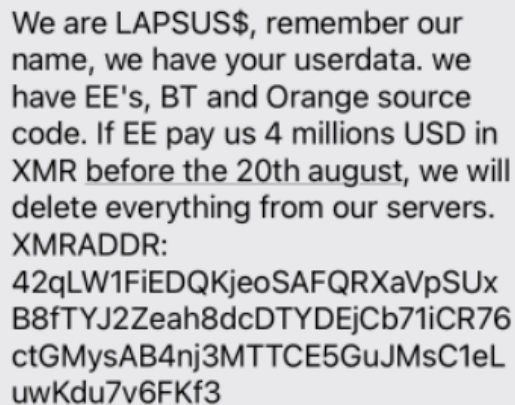
Executive Summary

The purpose of this report is to document the current form and methodologies used by the Lapsus\$ threat actor. The information documented is then used by Cyber Security Associates Ltd (CSA) Cyber Analysts to detect and hunt for the threat within the client environment through the use of our supported SIEMs BorderPoint, Microsoft Sentinel and LogRhythm, and advise on countermeasures to monitor and detect for the subject threat.

This report documents the threat group Lapsus\$ and their TTPs (Tactics, Techniques and Procedures), and contains recommendations to help detect and mitigate the emerging threat. The report also includes references to where the information within this report was identified from.

Summary

Lapsus\$, which is also being tracked as 'DEV-0537,' is a threat group that has been making recent headlines due to a number of confirmed breaches against many large organisations such as Microsoft, Okta, Nvidia, LG, and Globant, to name just a few. Lapsus\$ was first observed in mid-2021, sending threatening texts to UK mobile customers.

A screenshot of a text message with a grey background. The text is in black and reads: "We are LAPSUS\$, remember our name, we have your userdata. we have EE's, BT and Orange source code. If EE pay us 4 millions USD in XMR before the 20th august, we will delete everything from our servers. XMRADDR: 42qLW1FiEDQKjeoSFAFQRXaVpSUx B8fTYJ2Zeah8dcDTYDEjCb71iCR76 ctGMysAB4nj3MTTCE5GuJMsC1eL uwKdu7v6FKf3".

We are LAPSUS\$, remember our name, we have your userdata. we have EE's, BT and Orange source code. If EE pay us 4 millions USD in XMR before the 20th august, we will delete everything from our servers. XMRADDR:
42qLW1FiEDQKjeoSFAFQRXaVpSUx
B8fTYJ2Zeah8dcDTYDEjCb71iCR76
ctGMysAB4nj3MTTCE5GuJMsC1eL
uwKdu7v6FKf3

Figure 1: Mid-2021 Lapsus\$ activity.

What makes Lapsus\$ unique is that their typical attacks do not involve the deployment of malware or ransomware, unlike other well-known threat actors. The group is typically financially motivated, with a heavy focus on data extortion and payment. However, they have proved that this is not always the case. In their Nvidia attack, they demanded the organisation remove the mining hash rate limiters on their RTX 3000-series GPU as ransom. They also gained access to an organisation's cloud environment, wiped their systems, and destroyed thousands of virtual machines, indicating the group is operating on a "pure extortion and destruction model," according to a report by Microsoft.

Another idiosyncratic approach Lapsus\$ take is their online presence. Commonly, threat actors will attempt to operate under the radar, whereas Lapsus\$ do not. They have been seen announcing their attacks on social media, as well as openly advertising interest in buying credentials from potential targets.

Lapsus\$ execute many of their attacks using credentials either purchased or obtained from dumps or spear phishing. They're also known to bypass common security mechanisms such as MFA (Multi-factor Authentication), use social engineering, SIM swap, and compromise MFA/Telecom providers.

Tactics, Techniques, Procedures

Tactics, Techniques, and Procedures (TTP) describes an approach of analysing an advanced persistent threat's (APT's) operation, or can be used as means of profiling a certain threat actor.

Tactics is meant to outline the way an adversary chooses to conduct their attack from the beginning till the end. Technological approach of achieving intermediate results during the campaign is described by the **Techniques** the attacker uses. Lastly, the organisational approach of the attack is defined by the **Procedures** used by the threat actor.

In order to understand and fight the enemy, one must understand the Tactics, Techniques and Procedures (TTP) the attacker uses. Understanding the Tactics of an adversary can help in predicting the upcoming attacks and detect those in early stages. Identifying the Techniques used during an attack allows you to identify an organisation's blind spots and implement countermeasures in advance. Finally, the analysis of the Procedures used by the adversary can help you understand what the adversary's looking for within their target's infrastructure.

TTPs that are described within this research are based of the information that CSA analysts have been able to identify prior to the release of this document. The threat may change and adapt as it matures, to increase its likelihood of evading defence.

Hackers

A 'hacker' is a person who finds it interesting to interfere with computer systems. Often seen as a challenge, a hacker will attempt to breach a system because it tests their skills and knowledge.

Hactivists

A 'hactivist' is a person who gains unauthorised access to computer files or networks in order to further social or political ends.

Insider Threats

An employee or 'insider' is a person within a group or organisation, especially someone with knowledge of information unavailable to others.

State Sponsored

A 'state actor' is a person who is acting on behalf of a governmental body, and is therefore subject to regulation under their human rights.

Organised Crime

A 'criminal gang' is a group of people that take part in organised unlawful activity. They may target a business to gather information on customers, or to gather financial data which could be sold.

Phase 1: Initial Access

Lapsus\$ are known to use a variety of methods to gain initial access to an organisation, including:

- Using the malicious RedLine password stealer, capable of obtaining passwords and session tokens
- The use of criminal forums to purchase credentials and session tokens
- Paying employees at a target organisation (or suppliers/business partners) for access to credentials and MFA approval
- Scraping public code repositories for exposed credentials

Once the group have acquired compromised credentials or session tokens, they are known to exploit External Remote Services (MITRE ID: T1133), including virtual private networks (VPN), remote desktop protocols (RDP), virtual desktop infrastructures (VDI) and more. Lapsus\$ have been observed using two techniques to bypass MFA, including session token replay and utilising compromised passwords to trigger an MFA approval, in the hope that the legitimate user will consent to the prompt and grant access.

A number of cases were also reported whereby the group would target an individual's personal or private accounts in attempt to gain access and look for additional credentials that could be utilised to gain access to corporate systems. Lapsus\$ also abused the access to reset passwords and attempt account recovery actions.

Another method Lapsus\$ actively used was recruiting employees/insiders at target organisations. On the group's Telegram page, they posted their interest and stated that individuals would be paid if they wished to help provide access.

MITRE ATT&CK

MITRE developed the Adversarial Tactics, Techniques and Common Knowledge framework (ATT&CK), which is used to track various techniques attackers use throughout the different stages of cyber attack to infiltrate a network and exfiltrate data.

The framework defines the following tactics that are used in a cyber attack:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

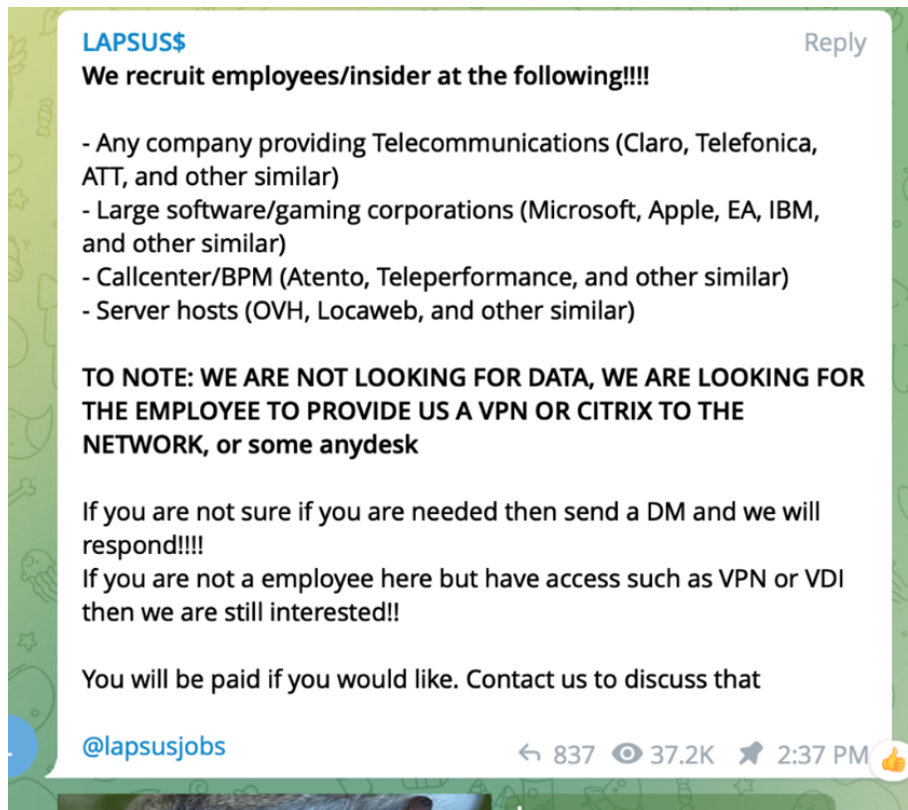


Figure 2: Lapsus\$' Telegram ad, recruiting employees/insiders to provide access to their employees' networks.

Lapsus\$' initial access can be mapped to the following Mitre ATT&CK techniques:

Technique	ID	Description
<u>External Remote Services</u>	T1133	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations.
<u>Valid Accounts</u>	T1078	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defence Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network, and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, and remote desktop.
<u>Exploit Public-Facing Application</u>	T1190	Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spear phishing. In spear phishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.
<u>Trusted Relationship</u>	T1199	Adversaries may breach or otherwise leverage organisations who have access to intended victims. Access through trusted third-party relationships exploit existing connections that may not be protected, or receive less scrutiny than the standard mechanisms of gaining access to a network.

Phase 2: Reconnaissance and Privilege Escalation

Lapsus\$ were also observed, on multiple occasions, using tactics to discover additional credentials or potential intrusion points to further increase their access, including:

- Exploiting known unpatched vulnerabilities on services such as JIRA, GitLab, and Confluence
- Searching discovered code repositories or collaboration platforms for exposed credentials

The group utilise the tool AD Explorer, which can enumerate all users and groups in a network. This allows them to further target accounts that may have higher privileges.

When exploiting the known vulnerabilities in common services, they often use DCSync attacks and Mimikatz to perform privilege escalation. DCSync is an attack that allows an adversary to simulate the behaviour of a domain controller (DC), and retrieve password data via domain replication. Mimikatz is an open-source application that allows users to view and save authentication credentials such as Kerberos tickets.

When the group achieves administrator access, they use the built-in ntdsutil utility, which can extract the AD database.

Cyber Kill-Chain

The cyber kill-chain is a process that traces the stages of a cyber attack. This starts at the early reconnaissance stages that eventually leads to data exfiltration.

The kill-chain can help one to understand and combat ransomware, advanced persistent threats (APTs), and security breaches.

The cyber kill-chain defines the following tactics that are used in a cyber attack:

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Obfuscation/Anti-forensics
- Denial of Service
- Exfiltration

Phase 3: Exfiltration, destruction, and extortion

Microsoft claims to have observed the threat group using their own dedicated infrastructure on virtual private server (VPS) providers. However, they have not explicitly stated the providers that are being utilised. The group actively tries to avoid common detection mechanism such as 'Impossible travel' alerts, by leveraging service such as NordVPN to ensure their connections originate from the same geographic region as their targets. Lapsus\$ will typically proceed to download copious amounts of sensitive data from the compromised target for extortion or public release to the system joined to the organisation's VPN and/or Azure AD-joined system.

The group commonly targets organisations using cloud services (such as AWS or Azure), creating new virtual machines within the cloud environments, and then leveraging the virtual machines to perform further attacks on the target.

If the group manages to successfully compromise a cloud environment with increased privileges, they are known to create global admin accounts and set O365 tenant level mail transport rules to send all mail in and out of the organisation to a new account created by themselves. They typically proceed to remove all other global admin accounts, locking out the organisation.

Lapsus\$ will occasionally delete an organisation's valuable resources in order to trigger the incident response process. They do this to learn and understand the how the organisation will respond once they've infiltrated it, and they can follow the process from start to finish. They use this knowledge to further enhance their capabilities, and refine their attack methods.

Latest news

The City of London Police recently arrested seven people between the ages of 16 and 21 due to alleged connections to the Lapsus\$ threat group. Detective Inspector Michael O'Sullivan said in a statement shared with The Hacker News:

"Seven people between the ages of 16 and 21 have been arrested in connection with this investigation and have all been released under investigation. Our enquiries remain ongoing."

An update from the City of London Police later revealed:

"Both teenagers have been charged with: three counts of unauthorised access to a computer with intent to impair the reliability of data; one count of fraud by false representation and one count of unauthorised access to a computer with intent to hinder access to data. The 16-year-old has also been charged with one count of causing a computer to perform a function to secure unauthorised access to a program. They will both appear at Highbury Corner Magistrates Court this morning (1 April 2022)."

The City of London Police would not confirm the identities of the teenagers, whose names were not released as they are subject to the UK's reporting restrictions on identifying non-adults.

However, the day after the announcement of the arrests, the group claimed some of its members were taking "a vacation." The group later denied that any of its members had been arrested.

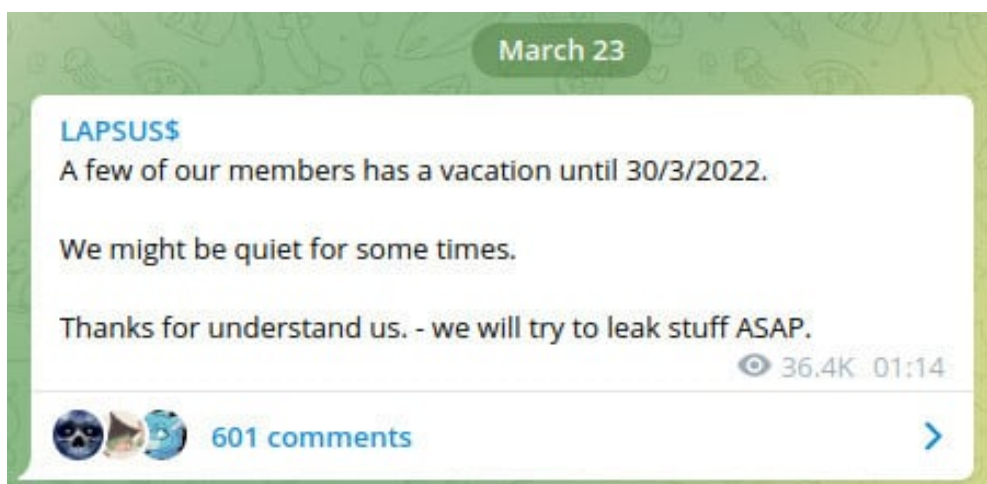


Figure 3: Lapsus\$' Telegram, stating some members were on vacation.

The group later announced their return from vacation stating: "We are officially back from a vacation" and proceeded to leak 70GB worth of data stolen from software development giant Globant. Despite the series of arrests, the Lapsus\$ group continues to operate as normal.

Recommendations

Multifactor authentication (MFA)

- Ensure MFA is enabled and enforced for all users
- Require MFA for internal environments as well as external
- Avoid using telephony-based MFA methods to avoid the possibility of SIM-jacking. More secure methods such as FIDO tokens, or Microsoft Authenticator with number matching, are recommended
- Implement user and sign-in risk-based policies that block high impact user actions like device enrolment and MFA registration
- Ensure there are no MFA exception policies, such as specific locations being excluded, that could be abused

Updated and Compliant Endpoints

- Ensure all Endpoints are updated and compliant with your organisation's security policies (consider a Zero Trust approach for best coverage)
- Implement a patch management software
- Ensure the principle of least privilege is being used for all accounts and users (consider a Privileged Access Management solution)

Modern and secure VPN solutions

- Use a modern VPN solution, with either OAuth or SAML authentication
- Ensure your VPN solution has stringent conditional access requirements before a user can connect. These can include ensuring AV is running, systems are joined to the domain, devices meet a required patch level, and so on

Strengthen and monitor your security posture

- Monitor your logs for any suspicious or abnormal activity 24/7, with a focus on any suspicious activity related to identities and access. Modifications of Azure AD roles, Exchange Online transport rules, and tenant-wide configurations, should be monitored carefully (consider SIEM solutions, managed SIEM services, or user entity and behavioural analytics solutions)
- Encourage staff to report any suspicious activity from the IT helpdesk that's out of the ordinary
- Consider a forced password reset for high/medium user risk for all users
- Block high/medium sign-in risk logins for privileged users

E-learning

- Provide staff with E-learning to help raise awareness of social engineering attacks

- IT and Security teams should be vigilant for suspicious activity, and ensure an incident response process is in place

Hunting Queries

Microsoft have produced a number of hunting and detection queries and responses, which can be found here:

<https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/#:~:text=Detecting%2C%20hunting%2C%20and,data%20exfiltration%20attempts>

MITRE ATT&CK TTPs used by LAPSUS\$

TA0001: Initial Access

- T1078: Valid Accounts
- T1133: External Remote Services
- T1190: Exploit Public-Facing Applications
- T1199: Trusted Relationships

TA0002: Execution

- T1059: Command and Scripting Interpreter
- T1059.001: Command and Scripting Interpreter: PowerShell
- T1059.003: Command and Scripting Interpreter: Windows Command Shell
- T1059.004: Command and Scripting Interpreter: Unix Shell

TA0003: Persistence

- T1078: Valid Accounts
- T1078.002: Domain Accounts
- T1078.003: Local Accounts
- T1078.004: Cloud Accounts
- T1021: Services
- T1021.001: Services: Remote Desktop Services
- T1114: Email Collection
- T1114.003: Email Collection: Email Forwarding Rules

TA0004: Privilege Escalation

- T1068: Exploitation for Privilege Escalation

- T1078: Valid Accounts
- T1078.002: Domain Accounts

TA0005: Defence Evasion

- T1562: Impair Defences
- T1562: Impair Defences: Disable or Modify Tools
- T1027: Obfuscated Files or Information
- T1027.002: Obfuscated Files or Information: Software Packing
- T1553: Subverted Trust Controls
- T1553.003: Subverted Trust Controls: Code Signing
- T1078: Valid Accounts
- T1078.002: Domain Accounts
- T1078.003: Local Accounts
- T1078.004: Cloud Accounts

TA0006: Credential Access

- T1552: Unsecured Credentials
- T1552.002: Unsecured Credentials: Credential in Files
- T1552.004: Unsecured Credentials: Private Keys
- T1003: Credential Dumping
- T1003: Credential Dumping: LSASS Memory
- T1111: Two Factor Authentication Interception

TA0007: Discovery

- T1082: System Information Discovery

TA0008: Lateral Movement

- T1021: Services
- T1021: Services: T1021.001: Services: Remote Desktop Services
- T1078: Valid Accounts
- T1078.002: Domain Accounts

TA0009: Collection

- T1114: Email Collection
- T1114.003: Email Collection: Email Forwarding Rules

TA0010: Exfiltration

- T1537: Transfer Data to Cloud Account

- T1114.003: Email Collection: Email Forwarding Rules

References

- <https://www.cityoflondon.police.uk/news/city-of-london/news/2022/march/two-teenagers-charged-in-connection-with-investigation-into-hacking-group/>
- <https://threatpost.com/lapsus-back-from-vacation/179156/>
- <https://unit42.paloaltonetworks.com/lapsus-group/>
- <https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/>
- <https://thehackernews.com/2022/03/7-suspected-members-of-lapsus-hacker.html>
- https://techcrunch.com/2022/04/01/uk-police-teenagers-lapsus/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGkj5nuH0tVX2nLwxJHfuNr6P3WWYb3L3sQ5v3FIRSBc-Fz2rVT_YdYA0h_Y_aaoYXVqdTGswzU2fWYTSszStHyp7L5c7iO8tdnZdQH0dSZpPUjOvd7obypnnYXs8G-e1YrSQVcPs6vd2Z9-ZKgrsKtWrtdYxIXNDcczfULI4uI6
- <https://michaelkoczvara.medium.com/lapsus-ttps-431d1ca21e80>
- <https://blog.checkpoint.com/2022/03/07/lapsus-ransomware-gang-uses-stolen-source-code-to-disguise-malware-files-as-trustworthy-check-point-customers-remain-protected/>