Journal of Research in Science and Engineering (JRSE)
ISSN: 1656-1996 Volume-7, Issue-2, February 2025
DOI: 10.53469/jrse.2025.07(02).02

Unlocking the Mystery: Comprehensive Analysis and Insights on Strengthening Organizational Defense

Biswajita Mohanty

Independent Researcher, Seattle, USA

Abstract: ***This paper comprehensively analyzes the attacks and intrusions by the Lapsus$ group. Lapsus$ is notorious for its high-profile attacks on major corporations and governmental entities. This study dives into the modus operandi of Lapsus$ and their tactics, techniques, and procedures (TTPs). This paper analyzes notable cyber compromises to produce actionable insights for organizational cybersecurity enhancements. This research examines case studies of Lapsus$'s significant attacks, including the intrusions into Okta, NVIDIA, and Microsoft, to understand the group's operational patterns, target selection, and the sophisticated nature of its campaigns.***

Keywords: Cybersecurity, Lapsus$, Threat Actor, Threat Intelligence, Blue Team Guide, Breach Analysis

1. Introduction

In 2022, Lapsus$ emerged [1] as a formidable and highly sophisticated threat actor. They gained popularity through high-profile attacks on major corporations and government entities. They swiftly gained notoriety for their tactics and extortion schemes. This group's focus on high-value targets and its ability to inflict significant operational and reputational damage placed it in a unique position within the global cyber threat hierarchy [4]. SaudeGroup is another alias for Lapsus$; they are also known as “Slippy Spider” by Crowdstrike, “DEV-0537” by Microsoft, and “UNC3661” by Mandiant [8].

With cyber threats becoming increasingly sophisticated and targeted, understanding Lapsus$'s operations and methodologies is essential for developing effective defense strategies. This research aims to unravel the group's tactics, techniques, and procedures (TTPs) and offer a granular view of its attack patterns and operational behavior. By analyzing the high-profile compromises attributed to Lapsus$, this study also seeks to provide organizations with detailed insights and strategies to improve cybersecurity posture and resilience against similar threat actors. The paper combines data from cyber threat intelligence reports, incident reports, and the MITRE ATT&CK framework [1][5] to provide a detailed account of Lapsus$'s activities, characteristics and specific strategies to combat it.

2. Methodology

The primary data for this study is sourced from the data available in the public domain. These public documents offer detailed accounts of Lapsus$'s attack campaigns, methodologies, and the aftermath at victim organizations. Information from these public sources is the foundation for analyzing Lapsus$'s Tactics, Techniques, and Procedures (TTPs). These data sources were chosen for their depth of analysis and the reputation of the organization that published them; this ensures a reliable foundation for the study.

A qualitative method like thematic analysis is used to identify patterns and trends in Lapsus$'s operations. Quantitative methods are used at applicable places to assess the impact of an attack. Another quantitative method used in this study is to source data from multiple sources for each attack. Data from various sources is used to ensure the validity and reliability of the data considered for research. The analytical approach for analyzing Lapsus$'s TTPs is based on the MITRE ATT&CK model. Mitre Corporation is a globally recognized organization that publishes knowledge databases for adversary tactics and techniques [1]. Mitre's ATT&CK model offers a taxonomy for categorizing and analyzing Lapsus$'s actions across various stages of their attack lifecycle. By overlapping the group's TTPs with the MITRE ATT&CK framework, this study deciphers the TTPs employed by Lapsus$. Also, it provides a standard language for articulating the threat actor behaviors.

3. Overview of Breaches

In 2022, Lapsus$ emerged as a relatively new player in the cyber threat landscape. They initially gained attention for targeted attacks against high-profile public and private entities in South America [2]. Lapsus$ quickly established itself with bold operations; some of the notable ones are against Electronic Arts, The Ministry of Health in Brazil, Microsoft, and Okta. At that time, the group's origins were believed to be in Brazil, with native Portuguese speakers at the group's core [6][8]. However, their activities soon expanded to targets in the United States, South Korea, and France. Lapsus$ group had a distinct approach; they refrained from deploying ransomware in the traditional sense [13]. Instead, they focused on exfiltrating sensitive data, particularly proprietary source code. They threatened the victim organization with public disclosure of stolen data and, in some cases, source code. A unique extortion scheme compared to the run-of-the-mill ransomware groups. Also, these tactics were great examples of Lapsus$'s nuanced understanding of victim's corporate value and their vulnerabilities [2][7][8][9][12]

As Lapsus$ evolved, they demonstrated adeptness in their technical and social engineering tactics. They employed advanced techniques to infiltrate and exploit their targets. They used SIM swap attacks against the telecommunications sector, spear-phishing campaigns, and strategically acquired active passwords and session tokens from dark web markets and forums [2][8][17]. Unlike many contemporary adversaries and ransomware groups, Lapsus$ did not aim for mass disruption or indiscriminate data encryption; instead, they meticulously selected their victims and exfiltrated data that held significant value for competitive advantage or reputation damage. Lapsus$ was also riddled with internal conflicts, evident from the publicly posted incidents within the group [15]. Overall, these characteristics paint a picture of Lapsus$ as a complex, decentralized entity driven by financial gain and notoriety. [2][8][14-33].

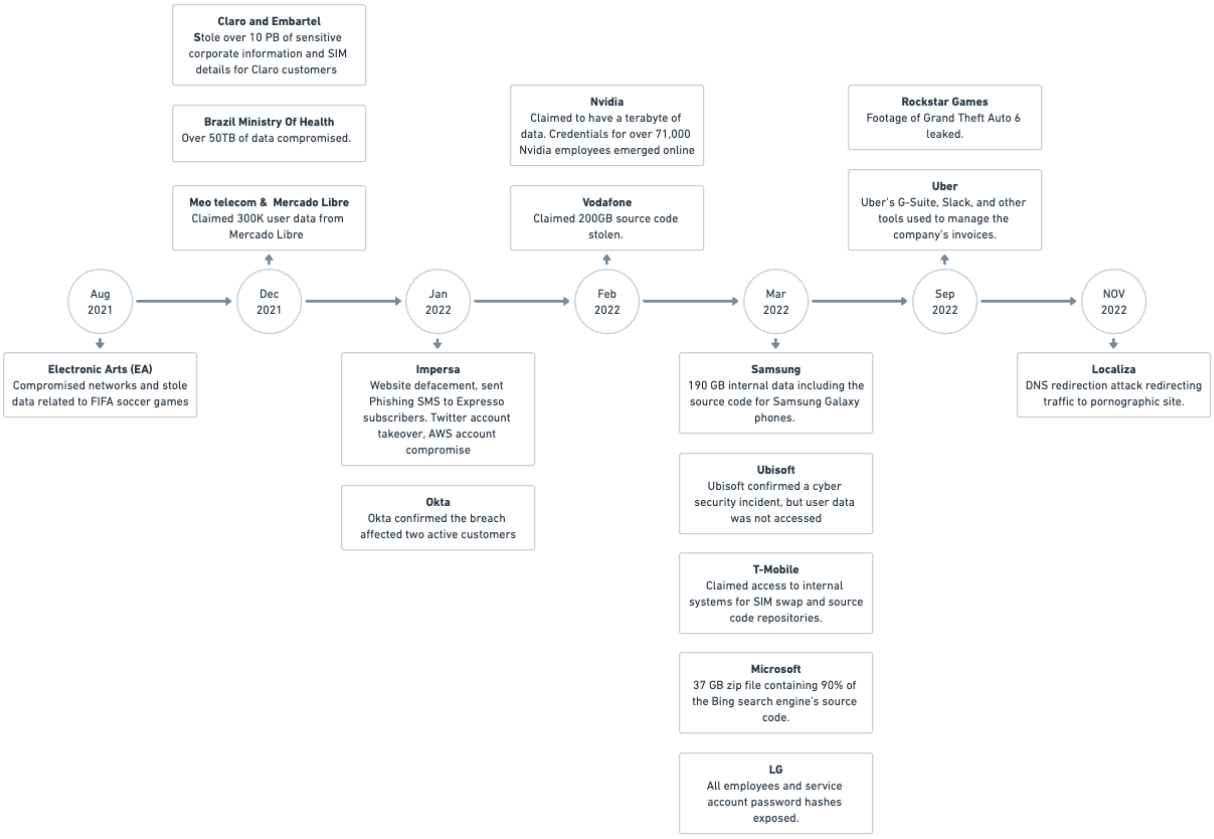

Figure 1: Timeline of intrusions by Lapsus$

4. Tactics, Techniques, and Procedures (TTPs)

4.1 Reconnaissance and Resource Development

In the initial stages, they gathered intelligence and developed resources necessary for subsequent operations. They performed social engineering and standard penetration testing to discover weaknesses. Their infrastructure included command-and-control servers for managing attacks, with some reusing infrastructure, aiding in attribution tracking. To conceal their attack traffic, they utilized anonymization services and commercial VPNs [2][5][8].

Fraudulent EDRs were a tactic of note whereby actors obtained sensitive information under false pretenses, informing their extortion strategies. They misused legal provisions to respond to emergency requests, creating fake EDRs to impersonate legitimate authorities. Supply chain attacks were also a focal strategy; Lapsus$ exploited the trust between third-party service providers and clients. They targeted business process outsourcing companies, telecommunications, and SaaS providers, accessing data and systems through these trusted channels [2].

4.2 Initial Access

Lapsus$ extensively used social engineering for initial access, demonstrating versatility and creativity. They impersonated personnel, utilized various phishing methods, and exploited MFA fatigue. They conducted fraudulent SIM swaps and recruited insiders, offering monetary rewards for system access. Known vulnerabilities were exploited for access, with no use of unreported vulnerabilities observed [2][5][8].

4.3 Privilege Escalation and Lateral Movement

Once initial access was gained, actors escalated privileges and moved laterally. They searched for poorly secured credentials, used common tools for movement, and exploited vulnerabilities. They maintained access by adding accounts and using both legitimate and malicious remote access tools. [5][8].

4.4. Persistence

Lapsus$ is known for sophisticated methods of maintaining persistence in compromised systems. They often obtained legitimate credentials through social engineering, phishing,

and purchasing from other criminals. Usage of legitimate credentials allowed them to access systems without suspicion, additionally, Lapsus$ manipulated authentication tokens to reuse authenticated sessions and exploited Remote Desktop Protocol (RDP) for persistent remote access as well. They also deployed web shells on public-facing servers to retain remote control to execute commands.

Beyond direct access methods, Lapsus$ employed malware and backdoors for persistent access, they modified authentication processes and system registry keys related to startup programs to launch their malicious tools upon system boot. In corporate environments, they manipulated cloud services and configurations to maintain access to resources and data.

4.5 Impact

The impact was extensive, involving data compromise, theft, extortion, and harassment. They targeted valuable data for extortion or resale on criminal forums [15-33].

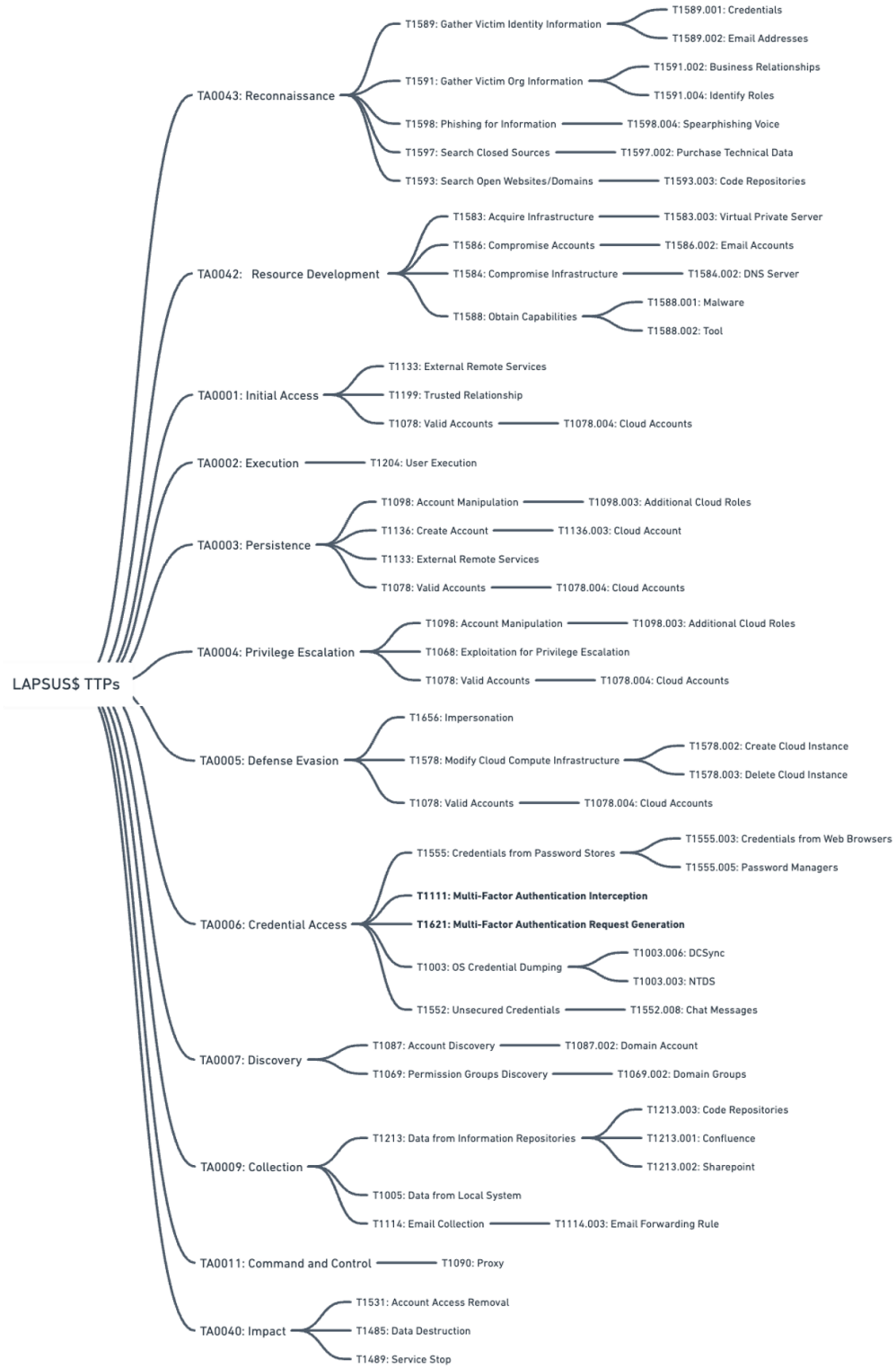

Figure 2: Lapsus$ TTPs – MITRE ATT&CK Matrix. [1][14]

Lapsus$ exemplified a hybrid threat actor adept in traditional cyberattack methods and innovative tactics. Their ability to blend social engineering, exploitation of third-party relationships, and efficient use of available tools made them a distinct and challenging adversary in the cyber threat landscape.

5. Notable Attacks

5.1. Microsoft, March 2022

Initial Breach Detection: Microsoft detected unusual activity indicating a breach. An employee's account was compromised, granting the Lapsus$ group limited access to source code repositories. The breach involved parts of the source code for Bing, Cortana, and other services. Microsoft emphasized that no customer code or data was involved and that viewing the source code did not elevate risk due to their security architecture.[6][12][32]

Public Disclosure by Lapsus$ (March 2022): Lapsus$ publicly disclosed their intrusion, which escalated Microsoft's response. This allowed Microsoft's cybersecurity team to intervene and interrupt the attackers' operations, limiting the broader impact of the breach. Microsoft did not disclose how the account was compromised but provided a general overview of the Lapsus$ group's tactics, techniques, and procedures (TTPs) observed across multiple attacks, including deploying the Redline password stealer, purchasing credentials on underground forums, and insider recruitment for access.

5.2. Okta, Jan 2022

Table 1: Lapsus$ Okta breach timeline. [16][20]

Date	Event
Jan 20, 2022	Okta detects an attempt to compromise a customer support engineer's account at third-party service provider Sitel.
Jan 20, 2022	Okta Security receives an alert about a new factor added to a Sitel employee's Okta account.
Jan 20, 2022	Okta Security investigates the alert and escalates it to a security incident.
Jan 21, 2022	Okta Service Desk assists in containing the user's account, terminating sessions, and suspending the account.
Jan 21 - Mar 10, 2022	Investigation and analysis of the incident by a forensic firm.
Mar 17, 2022	Okta receives a summary report about the incident from Sitel.
Mar 22, 2022	Lapsus$ shares screenshots online indicating compromise. Okta confirms the screenshots are related to the January incident.
Post-Mar 22, 2022	Okta continues the investigation, contacting potentially impacted customers. No impact to Auth0, HIPAA, and FedRAMP customers is reported.

5.3. Samsung, Mar 2022

In early March 2022, the Lapsus$ group carried out a breach against Samsung. The group accessed and stole approximately 190GB of data, including source code for Samsung's trusted applets in the TrustZone environment, algorithms for biometric unlock operations, bootloader source code for recent devices, and confidential source code from Qualcomm. Samsung confirmed the breach and stated that the stolen data did not include any personal information of consumers or employees and did not anticipate any impact on their business or customers [24].

March 4, 2022 - The Lapsus$ group leaked the data obtained from Samsung. The data was distributed in three compressed files, totaling almost 190GB, and made available through a torrent that was popular with more than 400 peers sharing the content. The leaked data included highly sensitive information about Samsung's technology and operations, such as source code for activation servers, technology used for authorizing and authenticating Samsung accounts, including APIs and services.

5.4. Nvidia, Feb 2022

Table 2: Lapsus$ Nvidia breach timeline [2][29][30][31]

Date	Event
Late Feb 2022	Lapsus$ infiltrated NVIDIA's systems, causing outages of developer tools and email systems. NVIDIA acknowledged the incident, stating commercial activities were uninterrupted, and began evaluating the breach's extent.
Feb 25, 2022	News of the breach surfaced, with Lapsus$ claiming responsibility and threatening to release 1 TB of stolen data, including employee credentials and proprietary information.
Feb 26, 2022	Lapsus$ reportedly began leaking data, including NVIDIA employee password hashes, and revealed plans for further data dumps.
Mar 4, 2022	Lapsus$ issued an ultimatum to NVIDIA, demanding the removal of certain firmware limitations and threatening the release of sensitive data, including source codes and chipsets, if demands weren't met.
Early Mar 2022	Lapsus$ accused NVIDIA of hacking back and deploying ransomware to delete the stolen data. NVIDIA did not directly address these claims. Security experts expressed skepticism, suggesting a potential misinterpretation of data loss prevention actions by Lapsus$ as a ransomware attack.
Mar 7, 2022	Active exploitation of the breach reported, with stolen NVIDIA code signing certificates being used to disguise malware.

6. Insights and Recommended Steps

In this section, we delve into pragmatic and strategic measures beyond the conventional defense-in-depth approach and overarching robust security posture. This section is designed to furnish organizations with actionable insights and tailored strategies to bolster their defenses against sophisticated and multifaceted threats like the Lapsus$ group's operations.

6.1. Multi-Factor Authentication (MFA)

Not all MFAs are equal. OTP delivery and push notifications using SMS, voice calls, and email are susceptible to social engineering and SIM swap attacks facilitated by a criminal

market that profits from hijacking mobile phone services. SMS, in particular, is not intended for sensitive transactions like OTPs, and it invites such exploits. MFA with number matching and hardware-backed FIDO2 solutions have stronger resilience than others. Specifically resilient against MFA Fatigue attacks. Okta Lapsus$ breach was an excellent example; in this case, Lapsus$ exploited the concept of MFA fatigue, where they repeatedly attempted to authenticate using the victim's credentials, prompting the victim to receive multiple MFA requests. Overwhelmed and exhausted by the repeated notifications, the victim approved an authentication request, granting the attacker access [11][32][33][35]

6.2. Conditional Access

Conditional access policies ensure that not just anyone with credentials can access a system. Access decisions are based on a range of conditions like user role, device compliance status, location, and risk levels associated with the user or the sign-in attempt. Even if Lapsus$ acquires user credentials, conditional access can prevent unauthorized entry by analyzing the context of each login attempt. For example, an access attempt from a new location or device can be flagged or denied. By setting conditions on the frequency and circumstances under which MFA requests are made, conditional access can reduce the risk of MFA fatigue, where users are bombarded with authentication requests until they inadvertently approve a malicious one.

Conditional access can ensure that only devices that are fully updated, managed, and compliant with the organization's security standards can access sensitive resources, reducing the risk of breaches via compromised devices. It can also be integrated with advanced security solutions that assess the risk level of a sign-in based on user behavior and other signals. Access can be automatically limited in high-risk scenarios, or additional authentication can be required.

6.3. Zero Trust Network Access

A Zero Trust Network Access (ZTNA) solution could significantly mitigate the TTPs of groups like Lapsus$ by enforcing strict access controls and continuous verification [2]. ZTNA does not assume trust based on network location and would thus limit the effectiveness of stolen credentials and unauthorized access. It requires verification of every individual and device attempting to access resources, which could hinder or expose social engineering attempts. Continuous monitoring and adaptive access policies under ZTNA also help detect and respond to abnormal behavior, potentially intercepting attacks before they fulfill their objectives. MFA with number matching or FIDO2 with ZTNA solution provides a more resilient defense.

6.4. Employee Awareness and Insider Risk Management

Enhancing employee awareness and insider risk management would be pivotal in defending against threats like those from the Lapsus$ group [36]. By educating employees about social engineering tactics, organizations can foster a culture of skepticism and vigilance, making it harder for attackers to use human centric TTPs. Insider risk management programs that monitor and control user behavior could detect and prevent the misuse of credentials and unauthorized access attempts, thereby reducing the attack surface that groups like Lapsus$ exploit. This proactive human-centric defense is a critical layer in a comprehensive cybersecurity strategy.

6.5. Cloud Identity and Access Management and IP based constraints

Lapsus$ often used social engineering tactics to manipulate individuals into granting access to sensitive areas of cloud infrastructure. They also openly recruited insiders in target organizations to gain privileged access. The group took advantage of weak or stolen credentials and instances where Multi-Factor Authentication (MFA) was either not enforced or could be bypassed to gain unauthorized access to cloud environments. Inherently with the cloud, one could create local identities and they are mostly used for programmatic access. These identities do not have MFA enabled. They are generally termed as service accounts; these service accounts should be limited to use within a predefined IP range to prevent attackers from using them from remote locations post credential theft or leak. Secondly all administrator roles should also have IP based constraints for the same reason.

6.6. Avoid Bring Your Own Device (BYOD)

Avoiding "Bring Your Own Device" (BYOD) policies could have provided significant defense advantages against groups like Lapsus$ [35]. BYOD environments often introduce security risks, such as the potential for unpatched devices accessing the network, the risk of unauthorized access to employee devices, and the increased likelihood of data loss through device theft or misplacement. Personal devices are inherently more susceptible to compromises and malware. They are frequently targeted by phishing campaigns seeking to exploit less stringent security controls that might be in place outside the corporate environment. Moreover, personal devices, if compromised, could be used as a conduit to access corporate systems, exploiting the increased attack surface that BYOD policies inadvertently create. Organizations should consider formulating strong BYOD policies to counter such risks if they cannot avoid BYOD altogether. These policies should include using Mobile Device Management (MDM) solutions, providing end-user awareness training, and implementing a robust employee transition plan to remove sensitive data from personal devices when an employee leaves the company.

6.7. Out of Band Validation for Critical Administrator Account Activities

Out-of-band validation for privileged administrator account password resets can provide a robust defense against the tactics of groups like Lapsus$. Out-of-band validation involves using a separate communication channel for verification, making it significantly more difficult for attackers to intercept or manipulate the process. For example, even if a Lapsus$ member obtained an admin's credentials via social engineering, an Out-of-band validation step such as a phone call or a push notification to a pre-registered device could thwart unauthorized password resets or access. This method ensures that even if the primary communication

channel is compromised, the authentication request cannot be completed without verification through the secondary, out-of-band channel. If it is not possible to include out-of-band validation in the authentication flow, set up a post-authentication validation by security operations. Thus, Out-of-band validation can serve as a critical checkpoint to confirm the legitimacy of requests, particularly for actions as sensitive as password resets for highly privileged accounts.

6.8. User Behavior Analysis (UBA)

User Behavior Analysis (UBA) capabilities are particularly effective against threats posed by groups like Lapsus$, especially in scenarios involving bribed or coerced insiders. UBA tools are designed to establish a baseline of normal user behavior and can detect deviations from that pattern. If an insider starts to act under the influence of a threat actor, their behavior, such as accessing systems at unusual hours or downloading large volumes of data and searching for sensitive key words like 'password' and 'keys' in collaboration tools would likely change and should trigger alerts. UBA systems are adept at identifying subtle signs of insider threats that other tools might miss; they can pick up on huge shifts and incremental behavioral changes too. Traditional security measures focus on defending the perimeter, but they are less effective against insiders who already have access to the network. UBA focuses on what happens inside the perimeter, thus providing defense against threats that have already bypassed external security measures. Focusing on behavior complements other security layers, creating a more comprehensive defense against sophisticated threat actors like Lapsus$.

7. Future Work

The rise and explosive success of Lapsus$ demonstrated a pattern where threat actors employ sophisticated and daring tactics to exploit technical vulnerabilities and human factors. In addition to traditional security measures, organizations should adopt comprehensive, defense-in-depth security strategies to combat these new-age adversaries. More emphasis should be given to security awareness training, resilient defense strategies, swift incident response procedures, and cultivating a security-conscious culture within the organization. These will be critical in addressing emerging threats and preparing us for tomorrow's challenges.

Secondly, research into groups like Lapsus$ offers valuable insights. However, there are various limitations, primarily from rapidly evolving adversary tactics and a constant challenge of attributing threat actors' activities and understanding their operations. Future studies could focus on researching multiple threat actors and their TTPs to produce insights for organizations to develop new strategies. Future work can also be done to foster stronger public-private partnerships for threat intelligence sharing, which would help organizations quickly learn from others.

8. Conclusion

In conclusion, this paper reflects on the intricate details of cyber threats that the Lapsus$ group embodies. This research has not just been about understanding a threat actor; it's been about adapting our defense mechanisms to the evolving landscape of cyber threats. Lapsus$, with its audacious strategies and expertise in exploiting both technical and human vulnerabilities, gives us an opportunity to rethink our cybersecurity paradigms. From exploiting cloud misconfigurations to employing social engineering with a finesse that blurs the lines between coercion and cooperation, Lapsus$ has exemplified the modern cyber adversary who is sophisticated, unpredictable, and relentlessly innovative.

However, this journey doesn't end with understanding the threat. It's about harnessing this understanding to fortify our defenses. Our discussions, ranging from tightening Cloud Identity and Access Management to embracing Zero Trust architectures, are more than recommendations. They are a call to action. Organizations should strive to adapt, innovate, and stay ahead in this relentless cybersecurity race. The journey of understanding Lapsus$ is just a chapter in this ongoing saga. The real story is how we use this understanding to redefine an organization's security posture.

References

[1] The Mitre Corporation, "LAPSUS$, DEV-0537, Group G1004," June 09, 2022
[2] CSRB, "Review of The Attacks Associated with Lapsus$ and Related Threat Groups," July 24, 2023
[3] MSTIC, DART, M365 Defender, "DEV-0537 Criminal Actor Targeting Organizations for Data Exfiltration and Destruction," May 17, 2022.
[4] UNIT 42, "Threat Brief: Lapsus$ Group," May 17, 2022.
[5] The MITRE Corporation, "ATT&CK", April 25, 2023
[6] Microsoft Defender Threat Intelligence and MSTIC, "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction," March 22, 2022
[7] ReliaQuest, "Team A vs Team B: What is Motivating Lapsus$," April 6, 2022
[8] Intrinsec, "Analysis of Lapsus$ Intrusion Set," March 28, 2022
[9] Themis, "Ransomware Gangs: Lapsus$," October 11, 2022
[10] Emil Sayegh, "Teenagers Leveraging Insider Threats: Lapsus$ Hacker Group," March 15, 2022
[11] Biasini, Nick, Cisco Talos, "Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco,"
[12] Monique Becenti, "Unveiling the Tactics of Lapsus$: A Review of Internal Attacks Vectors, Mobile Device Exploitation, and Social Engineering Techniques," August 29, 2023
[13] ReliaQuest, "Team A vs Team B: What is Motivating Lapsus$," April 6, 2022
[14] Brown, D., et al. "LAPSUS$: Recent techniques, tactics and procedures," December 22, 2022.
[15] Krebs, Brian; KrebsonSecurity, "Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code," April 22, 2022,
[16] Bradbury, David; Okta, "Okta Concludes its Investigation into the January 2022 Compromise", April 19, 2022,

[17] Mandiant Intelligence; Mandiant, “SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack,” May 16, 2023,
[18] Research & Insights Center; SecurityScorecard, “Lapsus$ Update: How This Technically Unsophisticated Threat Actor Group Breaches Large Organizations,” January 9, 2023
[19] Krebs, Brian; KrebsonSecurity, “The Original APT: Advanced Persistent Teenagers,” April 6, 2022,
[20] Okta, “Okta Security Action Plan,” September 30, 2022
[21] Rodriguez, Sarai, TechTarget - Heath IT Security, “HC3 Report Uncovers Key Data Exfiltration Trends in Healthcare,” March 15, 2023,
[22] Gatlan, Sergiu, Bleeping Computer, “Hackers breach gaming giant Electronic Arts, steal game source code,” June 10, 2021,
[23] Abrams, Lawrence, Bleeping Computer, “Lapsus$ hackers leak 37GB of Microsoft’s alleged source code,” March 22, 2022,
[24] Teapotuberhacker, GTAForums, “GTA 6 (Americas) leak – 90+ .mp4 footage/videos,” September 17, 2022,
[25] Ilascu, Ionut, Bleeping Computer, “Hackers leak 190GB of alleged Samsung data, source code,” March 4, 2022,
[26] Eun-jin, Kim, Business Korea, “Hacker Group Lapsus$ Claims to Have Attacked LG Electronics,” March 23, 2022,
[27] Lakshmanan, Ravie, The Hacker News, “IT Firm Globant Confirms Breach after LAPSUS$ Leaks 70GB of Data,” March 30, 2022
[28] DarkOwl, “Darknet Threat Actor Report: LAPSUS$” February 18, 2022
[29] Adam Bannister, “Cyber-attack on Nvidia linked to Lapsus$ ransomware gang,” February 28, 2022
[30] Pieter Arntz, “Nvidia, the ransomware breach with some plot twists,” March 3, 2022
[31] Alicia Hope, Nvidia Data Leak Exposed Proprietary Information but Wasn’t a Russian Ransomware Attack, Company Says, March 11, 2022
[32] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, “DEV-0537 criminal actor targeting organizations for data exfiltration and destruction,” March 22, 2022
[33] George Platsis, “How to defend against extortion groups like Lapsus$,” April 6, 2023
[34] Gal Nakash, “A Closer Look at the Hacking Techniques Used by the Lapsus$ Data Extortion Group,” October 10, 2023
[35] Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security,” January 10, 2023,
[36] BeyondTrust, “Lapsus$ Breaches Remind us Service Desks & Insiders often Weakest Link,” March 29, 2022