CyTact Threat Assessment

Lapsus$

TLP: **AMBER**

Executive Summary

This report assesses the threat of Lapsus$ to investment company Okto. Lapsus$ were a loosely structured juvenile hacker group that was active from 2021 to 2022. This review analyses their motivations, modus operandi, organisation and structure, infrastructure, and tactics, techniques and procedures (TTPs). It asserts with moderate to high confidence that Lapsus$ and similar groups are unlikely to target a company like Okto, provided that it does not have any high–profile clients that can increase its risk profile. Okto's small employee footprint and limited public presence help its security significantly. Well-organised profit-driven cybercriminals form the highest risk for Okto and should be taken more seriously than the threat from groups like Lapsus$. The report provides recommendations, including to educate employees and clients of the risks of ransomware, to conduct a more detailed risk assessment of Okto's key assets and priorities, and to improve its technical defences accordingly.

Foreword

Beginning in late 2021 and continuing late into 2022, cyber threat actor Lapsus$ attacked dozens of well-known companies and government agencies around the world. The group entered its targets' corporate networks, stole source code, defaced websites, and published its activities in a public Telegram channel. This report contains a detailed CTI assessment of this threat actor. It systematically reviews Lapsus$'s motivations, modus operandi, organisation and structure, infrastructure, and tactics, techniques and procedures (TTPs).

The goal of this review is to provide clarity on whether investment company Okto should be concerned about Lapsus$, similar groups, or other types of threat actors. It provides recommendations to improve the defences of the organisation and helps Okto make decisions about where and how to spend their time and resources.

The scope of the report is strategic: it provides the bigger picture on long term threats and threat actors, and focuses more on trends, motivations and modi operandi than on granular detail and actor-specific indicators of compromise (IOCs). It places Lapsus$ in its broader socio-political context. The recommendations are somewhat more operational in scope, as they aim to mitigate the specific threat to Okto as an organisation. References are made to sources that contain tactical recommendations.

The confidentiality level of this report is **Amber** in line with the Traffic Light Protocol (TLP). This indicates that the report is only to be used and distributed within Okto's organisation (Lee, 2023). Sharing the entire report with trusted clients and consultants may be allowed on a need-to-know basis. Educating clients and consultants on cybercrime threats is encouraged and recommended, and parts of this report can help to do so.

Threat Actor and Activity

The threat intelligence community first observed and tracked Lapsus$ as a named group between September and December 2021, when it started posting on its public Telegram channel and targeted the Brazilian Ministry of Health. Other attacks soon followed: target industries included telecommunications (Embratel, Vodafone, T-Mobile), media (Impresa, Grupo Cogina (Portugal)), technology (Microsoft, Samsung, LG), and gaming-related companies (Ubisoft, Microsoft, NVIDIA) (Tills, 2022). Many target organisations were Portuguese-speaking. The group is also known to take over individual user accounts at cryptocurrency exchanges to drain cryptocurrency holdings (Microsoft, 2022). Lapsus$'s public Telegram channel has grown to more than 40,000 followers as of April 2022 (Krebs, 2022e)

The threat intelligence community has assigned various names to the group. Microsoft named them 'DEV-0537' and later 'Strawberry Tempest' (Microsoft, 2022). Mandiant called Lapsus$ 'UNC3661', and CrowdStrike refers to them as 'SlippySpider' (Intrinsec Sécurité, 2022). The group's email address and public Telegram channel mention the name 'Saudegroup', which appears to be a reference to the attack on the Brazilian Ministry of Health ('Ministério da Saúde' in Portuguese).

Although the exact size of the group cannot be confirmed with 100% certainty, the CyTact team assesses with moderate confidence that the core group consisted of 7 people as of April 2022. This is based on the membership of the group's private Telegram channel as detailed by Krebs (2022e). While channel membership does not automatically imply an individual's culpability, it does indicate a certain level of involvement and privileged access. The Cyber Safety Review Board (CSRB) found the overall group had 8 to 10 known members (CSRB, 2023).

At least one group member speaks Brazilian Portuguese, as both Lapsus$'s defacement messages and the vast majority of messages in the public Telegram channel were written in that language (Intrinsec Sécurité, 2022; DarkOwl Analyst Team, 2022). The other main language was English. The identities of the members remain largely unknown, except for individuals AK, TJ, and 'Mox'. They are three of the seven members of the private Lapsus$ Telegram channel. The 'Organisation and Structure' section will elaborate more on their identities. Any names have been redacted as court proceedings are currently in progress, and because at least some of these individuals are minors. 'AK' and 'TJ' are the actors' initials; 'Mox' is an alias used by the actor.

In March 2022, seven teenagers were arrested in relation to UK law enforcement's investigations into Lapsus$ (BBC News, 2022a). Two of them were released on bail after an appearance at Highbury Corner Youth Court on 1 April 2022 (BBC News, 2022b), and a court case has not been concluded. While this might explain Lapsus$'s inactivity at the time of writing of this

report, the possibility that the former members and associates of the group have adopted new aliases, formed a new group, or continued their activities in a less public form cannot be ruled out.

Motivation

Lapsus$ appeared to be after a combination of clout, notoriety, and challenge, and to a lesser extent, financial gain. Clout and notoriety are evidenced by the fact that they ran an active, public Telegram channel in which they published their hacks and ran polls to ask which stolen data they should release next (Newman, 2022). The group might have been intent on proving itself, possibly because the individual actors came from the script kiddie hacking world which does not enjoy much respect (Allison Nixon of Unit 221b in Temple-Raston, 2022). Their targets included global, well-known organisations, breaches of which would be sure to attract media attention.

Some analysts have categorised Lapsus$ as primarily financially motivated. Microsoft's naming of the group as 'Strawberry Tempest' is a good example, as 'Tempest' indicates financially motivated groups in their taxonomy. However, while Lapsus$ frequently made ransom requests, they did not actually succeed in claiming these ransoms. For example, gaming company EA and Portuguese newspaper Expresso received ransom demands, but no payment method was provided and Lapsus$ never followed up (IPI, 2022; Cox, 2022). Moreover, by publishing their attacks so widely, the group was increasing the likelihood of being caught and risking any profit they could make. Their attack on Microsoft was caught while it happened due to Lapsus$'s Telegram posts, allowing the company to intervene (Microsoft, 2022). In other words, financial gain seemed to be more of an afterthought than a primary motivation.

Comparing Lapsus$ to other threat actors, the group most closely resembles hobby hackers and hacktivists (hackers with an activist purpose). Hobby hackers originated as actors motivated by fun, challenge and curiosity, and later saw a turn to crime and the use of malware. For such actors, breaching the defences of well-known companies like Microsoft and NVIDIA is fun in and of itself, as 'catching the flag' can yield 'street cred' and respect (cf Krebs, 2022e). Lapsus$'s boasting and lack of a structured approach matches this image well.

Hacktivists are motivated by challenge, ideology and current events. They originally focused on trolling and values like freedom of information, and evolved to become more political. Lapsus$ resembled hacktivists in their methods, as they publicly claimed their attacks and engaged in trolling behaviour like website defacement. Examples of this include their attack on the Brazilian Ministry of Health and their redirecting of the Localiza Rent-a-Car website to an adult page. However, Lapsus$ was decidedly less ideological than a group like Anonymous. The group's most political 'message' was probably its targeting of NVIDIA, whom they tried to pressure into open-sourcing its drivers so that its GPUs would be better suited for cryptocurrency mining (Hollister, 2022). Overall, ideology does not seem to be a key motivation for Lapsus$.

It is important to note that the motivations of individual group members are not necessarily representative of those of the group as a whole. Threat actors are not monolithic entities with singular, unchanging motivations. Indeed, since AK played a central role in the group's decision making and communications (see 'Organisation and Structure' for details), the

above motivations are probably best aligned with him as an individual. Lapsus$ had more members than just him, however, and the motivations of the others are less well-known.

Finally, Lapsus$'s offline context can provide useful information about its motivations. Although the identity of most members remains unclear, some of its key members were teenagers in the UK and US. Lapsus$ was active in 2021, and its predecessor 'Recursion Team' existed from 2020 to 2021 (Krebs, 2022e). This timeline coincides with the global pandemic, during which the group's members were likely to be at home throughout various lockdowns with much time on their hands. Hacking may have given them something 'cool' to do and helped them get away from the dull reality of home schooling and Zoom calls. As we will see in the next sections, Lapsus$'s modus operandi, organisation, infrastructure and TTPs match this reality well.

Modus Operandi

The modus operandi (MO) describes what the threat actor is trying to do and gives us a sense of their capabilities, how they might strike in the future, and what their risk is for a company like Okto. Lapsus$'s MO was centred around social engineering and extortion (Microsoft, 2022), with some destructive elements. The group did not rely on ransomware in its attacks (Newman, 2022).

Lapsus$ carried out a variety of attacks and did not have a consistent kill chain that applied to all of them. Generally speaking, the crime script of their main attacks was as follows:

- Obtain access to an organisation by acquiring credentials from privileged users, e.g. through insider recruitment or SIM swapping;
- Access the target's network through remote desktop tools or VPNs, occasionally aided by the exploitation of known software vulnerabilities;
- Obtain (and sometimes delete) data from the target's network, including source code and knowledge about its business operations;
- Extort the organisation by threatening to release the data, sometimes paired with defacement.

The group did not usually cover its tracks throughout this process and shared its activities on its public Telegram channel. Other attacks included the theft and compromise of crypto wallets and funds, and the use of Emergency Data Requests (EDRs) for initial access, doxxing and harassment purposes (Krebs, 2022f).

Overall, Lapsus$'s MO contained a combination of online and offline vectors, e.g. by employing both offline social engineering methods (such as calling customer support for password resets) and the exploitation of software bugs in tools used by the target organisation. It also cleverly targeted telecommunications companies, access to which could help the group in its SIM swapping activities. This shows that the group understood the interconnected nature of systems and how to exploit its weaknesses.

This general MO is relatively straightforward and does not require a very advanced skillset. It relies on the persistence of the threat actor to find a way into the organisation and suits a group that has ample time and limited resources. It also fits Lapsus$'s motivation to achieve clout and notoriety and to be challenged: the target organisation's data is leaked and/or destroyed, and the compromise of well-known targets results in boasting rights on online platforms. The selection of gaming- and technology-related companies in particular might have struck a chord with hacker communities online.

Similarly, the lack of a consistent MO and the flexibility with which the MO was adjusted are a sign that the group was not very streamlined or organised. A military unit or profit-driven cybercrime group would have been much more focused on their target. Lapsus$, to the contrary, kept adjusting its methods in seemingly random ways without a clear pattern or plan. Indeed, the group could have claimed significant sums of money with the access and valuable data they obtained, but instead did not appear to know what they were looking for (Vaas, 2022). This once again underscores the fact that financial gain was unlikely to be their primary motivation. Being as unstructured as they were, Lapsus$'s MO was both unusual and suboptimal which resulted in them being successful against the odds. As Ken Westin (director of Cybereason) stated, "it was as if they were surprised by their own success and were not sure what to do with it" (ibid).

Organisation and Structure

The introduction of the threat actor and its activity (page 2 of this report) noted that Lapsus$ had 7 to 10 members, three of which were AK, TJ, and 'Mox'. These individuals were all members of a private Lapsus$ Telegram channel. This section provides additional detail on Lapsus$'s members, organisation, and structure.

Overall, Lapsus$ were a loosely connected, small group that consisted at least in part of teenagers. The individual group members seem to have been active on online hacking forums before they formed Lapsus$ (Allison Nixon in Krebs, 2022a). Several Lapsus$ members were involved in 'Recursion Team' (also known as 'Infinity Recursion'), a similar group that existed from 2020 to 2021 and specialised in SIM swapping and swatting (Krebs, 2022b and 2022e; Intrinsec Sécurité, 2022; cf. Internet Archive, 2021). There was almost no hierarchy within Lapsus$ and the CyTact team found no evidence of dedicated roles and responsibilities. There was no apparent centralised coordination (command & control structure) or alignment with a larger goal (e.g. as set by a nation-state actor). The group has claimed it was not state-sponsored (Krebs, 2022a) and no evidence was found that it was, despite the vast impact of its activities. Its inconsistent and flexible MO underscores the group's loose structure, as discussed in the previous section.

The actions of the group showed no concern for authority. This could indicate either that they did not need to worry because they were protected from law enforcement, or that they underestimated the consequences of their actions and were careless when bragging on their public Telegram channel. The latter is most likely true and would be fitting for a brash, juvenile threat actor. The arrests that took place in relation to UK law enforcement's investigation into Lapsus$ (BBC News, 2022a) and the team members' panic in the private chat when they learned

that an AWS server with stolen data had been seized (Krebs, 2022e) seems to refute the possibility that they were protected.

No evidence has been found that the group had highly advanced technical skills, even though their methods were effective. Their creativity, persistence and time was their greatest asset. The group had a strong understanding of the interconnectedness of online and offline systems, even if the frantic MO suggests that it was not highly educated or trained in streamlined operations (Microsoft, 2022). Intrinsec Sécurité (2022) assessed Lapsus$'s level of sophistication according to the STIX format. On a scale from Aspirant, Novice, Practitioner, and Expert to Innovator, they graded Lapsus$ as 'Practitioner'. The group was not entirely self-sufficient, as it tapped into online hacker forums and market places to find insiders in target organisations (Cox, 2022). There is no evidence on how closely the recruited insiders worked together with Lapsus$.

Despite the lack of hierarchy and structure, some members were more prominent than others. The best known members were AK and TJ. AK likely held a leadership position in Lapsus$ as evidenced by the unilateral decisions he took. For example, he made the seemingly whimsical decision to close the group's access to T-Mobile's internal system Atlas, even though team members had worked hard to obtain this (Krebs, 2022e). He also had sole control over the @LapsusJobs Telegram account (Allison Nixon in Krebs, 2022a) and repeatedly bullied other team members, including TJ (Krebs, 2022e).

AK is known to have been active in online hacking and harassment forums. He purchased a doxxing website in 2021 but mismanaged it and sold it back to the previous owners at a significant loss (Intrinsec Sécurité, 2022; Krebs, 2022a). In the disagreements that followed, AK was doxxed himself, revealing details about his identity and background (cf. Doxbin, n.d.). Independent experts confirmed much of this information, including that AK was a UK-based teenager who met TJ and others online (Allison Nixon in Krebs, 2022a and Temple-Raston, 2022; Intrinsec Sécurité, 2022). He was involved in the selling and trading of zero-day exploits (software vulnerabilities that can be exploited by hackers) and accumulated a significant amount of Bitcoin. He was a founding member (alias 'Peter') of the 'Recursion Team' (Intrinsec Sécurité, 2022; cf. Internet Archive, n.d.) and used a variety of aliases, including 'White', 'WhiteDoxbin', 'Breachbase', 'Oklaqq', 'Teapothacker', 'SigmA', 'Peter', 'Alexander Pavlov', and variations on these (Krebs, 2022b; SilentPush Labs Team, 2022).

TJ was a UK-based teenager as well and went by aliases 'Amtrak', 'Asyntax', 'DormantCookies', 'Anitsu', 'Miku', and 'Everlynn' (Krebs, 2022b and 2022e). He mentioned living with his parents in the private Lapsus$ Telegram group (ibid). The 'Everlynn' alias is listed as Founder on the 'Recursion Team' website. It has been claimed that TJ was arrested multiple times for issuing fake Emergency Data Requests (EDRs), in which an individual impersonates law enforcement to a target organisation to get emergency access to a victim's account (Krebs, 2022b). AK paid the owner of the doxxing site to publish a doxxing page on TJ after they had a falling out (ibid). This doxxing page appears to be no longer online.

'Mox' is an alias for a third member of the private Lapsus$ chat; their real name is unknown. They said they were based in the United States and mentioned going to school, which suggests a young age. Mox speaks Arabic fluently (Krebs, 2022e). AK, TJ, and Mox appear to have

met each other online. Most activity in the private chat was between AK and TJ, but AK did not seem to treat any of the other members as his confidants or friends (cf. the aforementioned bullying; ibid). AK did not know Mox's real name but tried to find out so that he could dox them. It is unknown whether AK, TJ, and Mox spoke Portuguese and the CyTact team found no known connections between these individuals and Brazil or Portugal.

The March 2022 arrests of seven teenagers in the UK almost certainly included AK and TJ. The Lapsus$ Telegram account started posting again around the time that two of the seven teenagers were released on bail, and several members of the private Telegram channel quizzed AK (using his 'Recursion Team' alias 'Peter') and TJ on whether the authorities had asked them about 'Recursion Team' (ibid). In addition, TJ indicated that the City of London Police had found Lapsus$ Telegram chat conversations on his mobile phone (ibid). No information has been found on the identities of the other five arrested individuals or the other members of the Lapsus$ group.

According to AK's doxxing page, "[h]e works with a team of (not-so) skilled individuals who use him as a front man/mule to spread the word of said breaches. Instead of leaking user data which can be useful and worth the time, he just causes chaos and pointless breaches for clout and notoriety" (Doxbin, n.d.). AK is said to have continued his online activities under new aliases after his release in April. Later in 2022, he allegedly breached Uber and Rockstar Games, the video game publisher that created GTA. The doxxing page furthermore states that he was arrested a second time on 22 September 2022 (as evidenced by a Tweet from the City of London Police (2022)) and has been held in youth custody. These claims have not been verified.

Infrastructure

Having identified Lapsus$ as a small and loosely structured juvenile group, this section assesses the infrastructure used. In general, Lapsus$ did not employ any extensive, costly, or sophisticated tools, and their infrastructure evolved much like their MO did. The following paragraphs address their communications, hardware, software, and budget.

As noted before, the group used Telegram channels to communicate among themselves, publish their work, and post insider recruitment messages (Unit 42, 2022). They had an email address as well, but not much evidence has been found of how this was used. Dark Web forums like Russian Market and Genesis were employed to recruit insiders and purchase access credentials (Krebs, 2022e). The group-account 'InfinityRecursion' and the AK-specific 'Breachbase' account were found on the now-shut RaidForums (Krebs, 2022c and 2022d). There is no evidence of any dedicated Lapsus$ group-accounts on 'regular' social media like Facebook and Twitter. Individual group members did maintain their own accounts, however. For example, AK's doxxing page included screenshots of his personal Facebook and Snapchat accounts, all in his real name. It is unlikely that these accounts were used for any Lapsus$ activity, but it is plausible that individual members may have been 'friends' on platforms like these.

Lapsus$ did not run a leak site, but a Seychelles-based server has been linked to their activities (Intrinsec Sécurité, 2022). This server was rented from a third party that provides 'bulletproof' infrastructure, i.e. the servers are resilient to complaints of illicit activity. Of particular

interest is the related IP address (185.56.83.40), which resolved in the domain name lapsus-group.com. This address was the subject of over 200 abuse reports in the second half of 2021 (AbuseIPDB, n.d.). An SSL certificate was linked to the same address on 10 December 2021 (crt.sh, n.d.), which lines up with Lapsus$'s first claimed attack on the Brazilian Ministry of Health (Intrinsec Sécurité, 2022). Moreover, analyst collective The DFIR Report (Digital Forensices and Incident Response) noted that the same server was a Metasploit C2 (Command & Control) in October 2021 (The DFIR Report, 2021). An attacker can use such servers to maintain more persistent control over a target machine, escalate privileges, and potentially execute lateral movement throughout a targeted network (BeyondTrust, 2022). Intrinsec Sécurité (2022) noted that the Metasploit framework was likely used in at least one Lapsus$ attack (i.e. Vodafone Portugal). As of the time of writing in July 2023, the connection times out when visiting lapsus-group.com. Other domains linked to Lapsus$ include binance-help-desk.com, bitcoin.wiz.biz, doxbin.net (the doxxing site that AK purchased and then sold), amigos.deals, and leaks.direct (Silent Push Labs Team, 2022).

One remarkable aspect of Lapsus$ was that the group decided to not store any stolen data on their personal devices (Krebs, 2022e). They were afraid that an investigator could easily detect it that way and preferred to keep everything in the cloud. This strategy backfired in the end: before the private Lapsus$ Telegram channel was terminated, the group learned it had lost access to their Amazon AWS server, containing months of source code and other stolen information (ibid).

Software-wise, Lapsus$ is known to have used Virtual Private Servers (VPSs) and Virtual Private Networks (VPNs) for data exfiltration. They made sure to link the targeted device to their own system through a VPN in the same geographical area in order to avoid suspicion (Microsoft, 2022). In addition, they repeatedly created virtual machines on their own devices and within the target's cloud environment (ibid). The latter enabled them to perform further attacks across the target organisation. Finally, they employed Redline password-stealing software to steal user credentials.

In general, the group's infrastructure was based on what its individual members already had available or what could be obtained online. The overall budget appears to be low, even though AK had financial resources at his disposal due to his previous experience in trading zero-day vulnerabilities. As noted before, the group predominantly operated during the pandemic and was based in multiple countries. There is no evidence of any offices or dedicated locations to work from, and both AK and TJ are known to have worked from their parents' houses (Krebs, 2022e). AK's parents later stated that they thought he had been playing video games (BBC News, 2022a; Turton & Robertson, 2022).

Similarly, there is no evidence of the use of ransomware or any self-written malicious code that more advanced threat actors might have experience with. Lapsus$'s overall infrastructure might have been more advanced and sophisticated if they had been a more professional or experienced group, but what they were working with was effective nonetheless. This infrastructure matches with what one would expect from a loosely connected juvenile group.

Tactics, Techniques, and Procedures (TTPs)

As noted in the 'Modus Operandi' section, Lapsus$ did not follow a single crime script across all of their attacks. As a result, their TTPs are varied as well. This section lists the most common TTPs related to the MO of Lapsus$'s main attacks, in line with the MITRE ATT&CK framework. It does not provide an exhaustive list for all attacks: for such a list, please refer to ATT&CK® Navigator (n.d.) and Intrinsec Sécurité (n.d.).

To clarify, 'tactics' are a high-level description of the goal of the actions being executed by the attacker (i.e. the 'why' of the attack). The MITRE ATT&CK framework indicates these with 'TA' and four digits. 'Techniques' feature a more detailed description of the actions themselves (the 'how') and are indicated with 'T' and four digits. 'Procedures' involve even more detail of the instructions that the attacker is using to implement a given technique. It concerns the specific implementation of the techniques by this group. The main TTPs of Lapsus$ are summarised in Table 1. These TTPs were often followed or accompanied by ineffective ransom demands.

Table 1: Lapsus$'s TTPs

Tactic	Technique	Procedure (Lapsus$ Implementation)
TA0001: **Initial Access** - trying to get into a network		
	T1078: Valid Accounts	
	Obtaining credentials of existing accounts to access the network and remote systems like VPNs and remote desktop tools.	- Purchasing credentials on online criminal forums like Russian Market; - Deploying the Redline password stealer to maliciously obtain passwords and session tokens. This software costs $150-$200 depending on the version (Meskauskas, 2023); - Paying employees at target organisations for their credentials (related: T1597.002 - Purchase Technical Data) (Cox, 2022); - Searching public code repositories for exposed credentials (related: T1593.003 - Search Code Repositories); - Performing a SIM swapping attack (T1451) on a victim's phone number to get past multi-factor authentication restrictions (MITRE ATT&CK, n.d.).
	T1133: External Remote Services	
	Leveraging external-facing remote services to initially access and/or persist within a network.	- Using virtual private networks (VPNs), remote desktop protocols (RDPs), and virtual desktop infrastructure (VDI) to access the target network remotely. Exact tools depended on the target. This was an effective procedure for Lapsus$, as VPNs were commonly used during the pandemic in which they were operating (Krebs, 2022a).

TA0004: **Privilege Escalation** - gaining higher-level permissions			
	T1078: Valid Accounts		
		Obtaining *additional* credentials of existing accounts with higher privileges. Related: Tactic "Discovery", Technique T1087 "Account Discovery"	- Using tools like AD Explorer to enumerate all users and groups in a network to understand which ones have higher privileges (Microsoft, 2022); - Searching internal platforms for credentials and passwords, e.g. Teams and Slack (collaboration tools), Github and GitLab (code repositories), and JIRA (issue-tracking tool) (ibid); - Using social engineering methods to reset a privileged account's credentials (e.g. by calling the organisation's help desk and pretending to be the owner of the account). This was particularly effective in organisations that had outsourced their help desk support (Cox, 2022).
	T1068: Exploitation for Privilege Escalation		
		Taking advantage of software bugs to make changes or execute code for the purpose of adjusting permission levels	- Exploiting software vulnerabilities (e.g. in GitLab and JIRA) to obtain credentials of privileged accounts (Microsoft, 2022); - Using vulnerabilities to simulate the behaviour of a Domain Controller (DC) to retrieve password information (i.e. a DCSync attack) (Joyce, 2021). Lapsus$ used the open-source tool Mimikatz (S0002; MITRE ATT&CK, 2023a) for this (Microsoft, 2022).
TA0043: **Reconnaissance** - gathering information for use in future operations			
	T1589: Gather Victim Identity Information		
		Collecting information about the target's identity that can be used in future attacks. This includes personal information and credentials.	- Using domain administrator access to extract the Active Directory (AD), a database and set of services that connect users with the network resources they need to get their work done. Cf. the attack on NVIDIA, in which Lapsus$ obtained 70k employee email addresses, password hashes, and code signing certificates (Intrinsec Sécurité, 2022)
	T1591: Gather Victim Org Information		
		Gathering information about the organisation of the target, including business relationships, team structures, roles and responsibilities.	- Accessing internal discussion boards for information about the workings of the organisation (ibid); - Joining the organisation's crisis communication calls to understand incident response workflows (Microsoft, 2022)
	T1592: Gather Victim Host Information		
		Collecting information about the target's administrative data and configurations of systems	- Learning what software and client configurations the target uses in order to understand where to attack next
TA0009: **Collection** - gathering data of interest			
	T1213: Data from Information Repositories		
		Mining valuable data from repositories that store information and facilitate collaboration and information sharing between users.	- Obtaining data from systems like Confluence, JIRA, GitHub, GitLab, and SharePoint to understand an organisation's operations (Intrinsec Sécurité, 2022) - Collecting and copying source code or taking screenshots of it (ibid; Microsoft, 2022).

	T1114: Email Collection		
		Targeting user email to collect or forward sensitive information, including trade secrets or personal data from mail servers or clients.	- Creating global admin accounts in the organisation's cloud instances and setting up rules to automatically forward all mail in and out of the organisation to a newly created account (ibid).
TA0010: **Exfiltration** - stealing data			
	T1567: Exfiltration over Web Service		
		Using a legitimate external web service to exfiltrate data. Popular web services may give some cover if the target network is already communicating with these services in another capacity (traffic is permitted).	- Exfiltrating data by using a virtual private server (VPS), combined with a VPN (NordVPN) that was geographically similar to their targets to avoid detection. Stolen data was often used for future extortion or public release (ibid); - Storing stolen data in cloud services like AWS (e.g. in T-Mobile case; Krebs, 2022c) (i.e. T1567.002: Exfiltration to Cloud Storage)
TA0040: **Impact** - manipulating, interrupting, or destroying data or systems			
	T1531: Account Access Removal		
		Deleting, locking, or manipulating accounts to deny legitimate users access to the organisation's resources.	- Having obtained global admin access, Lapsus$ repeatedly removed all other global admin accounts so that they had sole access and effectively locked the organisation out (Microsoft, 2022)
	T1485: Data Destruction		
		Destroying data to interrupt the target's operations and the availability of systems, services, and network resources. Likely irrecoverable.	- Once data had been exfiltrated, Lapsus$ often deleted the target's systems and resources, both on-premise and in the cloud (ibid). Cf the attack on Impresa, which caused a newspaper and TV station to lose access to their archives (IPI, 2022).
	T1491: Defacement (External)		
		Modify visual content to send a message, intimidate, or claim credit for the intrusion.	- Replacing the home page of the victim with a message, claiming the attack (cf. the attack on Impresa (ibid) and the Brazilian Health Ministry (DarkOwl Analyst Team, 2022)) - Redirecting the victim's website to an adult site by means of a DNS spoofing attack (cf the attack on Localiza Rent a Car, Jan 2022) (ibid)

Overall, Lapsus$'s TTPs match those of a loosely structured group with limited resources that is mainly motivated by clout, notoriety, and challenge. They used accessible and existing tools, known vulnerabilities, and social engineering techniques that do not require advanced technical knowledge. As noted in the 'Infrastructure' section, a more advanced or organised attacker might have developed their own specialised tools, but Lapsus$ relied on what was readily available, low budget, and open source. In this, their TTPs much resemble the TTPs of hobby hackers who are mainly focused on getting access and causing disturbance. There is no clear, streamlined business model as one might expect from larger, hierarchical organisations or advanced

profit-driven cybercriminals. Nevertheless, Lapsus$'s impact was severe despite a lack of sophisticated tooling. Simplicity does not automatically imply inconsequential impact.

Sources of information

This report is based entirely on open source information that was found through search engines and links in reports and articles. The investigation was initiated with a general search with the aim to get as close to the primary sources as possible. Particularly useful were reports from organisations with direct access to indicators of compromise and sources with access to direct communications from the threat actor.

The report relies exclusively on sources in English, even though Intrinsec Sécurité (2022) showed that the majority of Lapsus$'s public Telegram messages was in Brazilian Portuguese. An attempt was made to find first-hand reporting from Lapsus$'s Brazilian and Portuguese victims, but this effort was unsuccessful. This introduces some bias to the report, as the sources in English might be overemphasised compared to the missing information about Lapsus$'s Brazilian and Portuguese involvement. In addition, the review might contain some cultural bias as the author of this report is a Western-educated adult with matching cultural awareness. This could result in some limitations with regard to understanding hacker- and teenage culture online (cf. Lee, 2023 on whether the CIA is too white; Coleman, 2015).

The key considerations in including sources of information in this report are availability, reliability and credibility, and relevance.

Availability

In terms of availability, this review excludes three types of sources of information: anything that was not open source, deleted information, and information that was published too close to the time of writing. The inclusion of any non-open source data would go against CyTact company policy. Data that would require an account to access, such as the public Lapsus$ Telegram channel and posts on cybercriminal forums, are not considered to be open source. As for deleted information, some original data had been made unavailable at the time of writing of this analysis. This included posts on RaidForums (which was taken down in 2022; Krebs, 2023) and deleted posts on Reddit. Screenshots taken by other researchers (e.g. DarkOwl Analyst Team, 2022; Silent Push Labs Team, 2022) partially filled this gap in intelligence. Finally, the Cyber Safety Review Board (CSRB) published an extensive analysis of Lapsus$ and similar groups on 10 August 2023. This analysis has only been included sparingly due to time constraints, as it came out mere days before the due date of this report.

Reliability and Credibility

Two other key considerations are the reliability of a source and the credibility of the information it provides. These two factors can be graded through the Admiralty Grading System and should be considered independently to make sure that the two do not influence each other (UK Ministry of

Defence, 2011). Even the most reliable sources can produce incorrect information, and unreliable sources can provide high quality intelligence. The two should not be confused. Overall, a source's expertise, motivation and access will affect both reliability and credibility (ibid).

The Admiralty Grading System assigns a letter grade to indicate reliability of the source. Grades range from A (completely reliable) to E (unreliable), and F is used when the reliability cannot be judged. Similarly, a number grade is assigned to indicate the credibility of information. The scores range from 1 (confirmed by other sources) to 5 (improbable), and 6 is used when the truth cannot be judged. This results in an intelligence grading like 'A1', 'C2', etc. The full scoring of the Admiralty Grading System can be found in the Appendix.

The present analysis is based on credible information from reliable sources. Unreliable sources were only used if the information was independently confirmed by reliable sources. Examples of reliable sources (grade A and B) include law enforcement and threat intelligence organisations such as Mandiant. These organisations have significant experience, work methodically, and often have first-hand access to evidence and indicators of compromise. Their published work is usually vetted and reviewed by more than one person. The present analysis relies on these types of sources extensively, e.g. on reports from threat intelligence organisations like Mandiant, Intrinsec Sécurité, the Threat Intelligence team at Microsoft, and others. Law enforcement data was less available as court proceedings are still in progress.

Individual experts and journalists can be a reliable source (grade B) if they have a strong track record. These experts often work for the threat intelligence organisations mentioned above, so they may have access to primary sources and/or conduct their own research. Examples used in this paper include Brian Krebs (Krebs on Security) and Allison Nixon of Unit 221b, who researched Lapsus$'s activities extensively (cf. interviews in Krebs, 2022a and Temple-Raston, 2022). The reliability of individual experts is a notch lower than that of organisations, as their interviews and posts do not go through the same vetting process.

HUMINT such as social media posts on Twitter and other online platforms are not usually considered to be reliable (grade D and E), as their author cannot always be confirmed. This includes Tweets from people who appear to have insider knowledge about Lapsus$ and doxxing pages written about its members (cf. Doxbin, n.d.). Since the author is unknown, their expertise, motivation and access cannot be confirmed. Communications from the threat actor itself (e.g. on their own Telegram chat) are considered to be fairly reliable (grade C), since there is some uncertainty about which member of the group wrote a given message. This uncertainty is reduced for individually owned accounts.

Intelligence from unreliable sources can still be deemed credible, and therefore useful. AK's doxxing page is an excellent example, as it contains much detail about AK's history and online identities and includes screenshots and photos that appear to corroborate the information (cf. Doxbin, n.d). The present report only relied on sources like this if the information was confirmed by another piece of evidence and/or other, reliable sources. The doxxing page was referenced by Krebs and Nixon, for example. Krebs also interviewed 'KT', an insider who knew some of the Lapsus$ members personally and claimed to have written the doxxing page (Krebs, 2022e).

Overall, the credibility of information was considered to be high (grade 1-2) if multiple reports confirmed it independently, or had direct access to primary sources (e.g. the BBC speaking directly with law enforcement; Microsoft analysing indicators of compromise on its own systems). Any information that was deemed possibly true or doubtful (grade 3-4) was identified as being low confidence. Information that was deemed improbable (grade 5) or not possible to judge (grade 6) was not processed in this report, even if it came from a reliable source. An example of this is a Forbes article (Sayegh, 2023) that attributed two 2020 attacks on the US Department of Defense and a 'major healthcare provider' to Lapsus$ without providing any sources. It also states that the group was highly organised, targeted oil and gas companies, and used advanced malware. None of these claims have been confirmed by other sources, so they are not considered to be credible.

Relevance

The goal of this report is to provide clarity on the risk of threat actors like Lapsus$, and to provide Okto with recommendations on how to reduce such risk. Its scope is strategic (i.e. focused on the big picture, instead of on granular details), so any detailed information on what attack occurred when and how is not included. It is not deemed to be relevant to the needs of the audience.

In a similar vein, non-technical information about the threat actor has been redacted, unless relevant to the case. For example, it is relevant that some of Lapsus$'s members were UK-based as that could influence their targeting and operations, but it is unnecessary to include their exact locations as provided on AK's doxxing page. Besides relevance, any doxxing-related information and URLs are omitted for ethical reasons as well. The Doxbin source included details on family, addresses, licence plates, and more. It goes against the ethical principles of the author to include such information, even if it is technically open source. Information on individuals related to Lapsus$ (but not proven to be in the group) was omitted as well, unless relevant to Lapsus$'s operations. Examples include the members of the group ViLE (including 'KT'), who ran Doxbin and were acquaintances of AK.

Overall, the level of confidence in the overall assessment of the threat actor is **high** for the intelligence that was available. The analysis is based on a combination of reliable and credible sources, many of which were verified primary sources. The motivation, MO, organisation and structure, infrastructure and TTPs align well across the board. There are no unexpected elements which might indicate that the overall assessment is lacking in some areas.

Nevertheless, some gaps in the intelligence persist, e.g. in relation to the remaining members of the group, the Brazilian and Portuguese connection, and details on the law enforcement proceedings. This information is unlikely to change the conclusions on the motivations, MO, organisation and structure, infrastructure and TTPs of this threat actor, however. It might add more definition, but it is deemed improbable that the cited evidence regarding Lapsus$'s will be disproven.

Probability that Okto will be targeted

This section assesses how probable it is that Okto will be targeted by Lapsus$, similar threat actors, and other, different types of threat actors. It starts by outlining Okto's most valuable assets or 'crown jewels', and then considers whether Lapsus$ and the other threat actors might be interested in those assets. It is important to emphasise that it is impossible to protect perfectly against everything, even if one has unlimited resources at their disposal. Okto is a small organisation, so prioritisation and a solid understanding of what is worth protecting will be necessary.

Okto's Crown Jewels

Okto is a London-based investment company that manages the assets of a small number of wealthy families through property and other investments. Its only full-time employees are the CEO, CFO and IT manager. Okto does not have a website and does not openly solicit clients.

An organisation like this has various resources that might be of interest to a threat actor. The most important ones are included in Table 2 below. These are the resources that Okto should aim to protect the most. The table gives an indication of the impact of compromise (i.e. 'what if it were to go wrong?') and the likelihood of compromise (i.e. 'how probable is it that this asset would be targeted?'). This assessment could benefit from more detailed information about Okto's assets and organisation..

Table 2: Okto's Crown Jewels

Asset	Explanation	Impact	Likelihood
Access to clients' assets	Since Okto's clients are wealthy and hold a variety of investments, threat actors may be interested in obtaining access for their own financial gain.	High (severe threat to reputation, trust, and business continuity)	Unknown; dependent on specific assets and current defences
List of clients	The client list itself can contain valuable information for a threat actor. Since Okto limits its business to wealthy clients, being included on the list of clients could imply that a family has significant financial resources. A threat actor could use this knowledge as a starting point to select a target, whether to target them through Okto's systems or through external means.	Medium - High	Unknown; dependent on where such information might be stored. Higher risk if clients have a strong public presence and/or share Okto's name.
Employee data and credentials	Access to information about employees can be used for reconnaissance (e.g. to understand the organisation and its weak spots) and extortion purposes. Employee credentials can enable a threat actor to access the organisation's internal tools.	Medium - High	Likely low due to the small employee footprint; more data needed on any consultants Okto might work with

Reputation and trust	A threat actor with a grudge against Okto could try to hurt its reputation and its clients' trust. Both are of critical importance in the financial services industry; any damage can have severe consequences for business continuity.	High (severe threat to business continuity)	Likely low due to the low profile of the organisation

Please note that Table 2 does not contain an exhaustive list of Okto's assets: it focuses on the most important ones only. These assets would severely risk the business if they were compromised. Other assets include Okto's own financial resources and office space.

The fact that Okto is a small company without a website or pro-active client recruitment helps with keeping a low profile. The organisation is not widely known and does not have a large employee footprint, reducing the risk that the company will make headlines if it were compromised. Threat actors motivated by clout and notoriety might therefore be less interested in targeting Okto.

Being targeted by Lapsus$

The CyTact team assesses with moderate confidence that Lapsus$ is not active at the time of writing (July/August 2023). Its core members appear to have been arrested (BBC News, 2022) and no attacks have been claimed by the group since then (Vaas, 2022). Nevertheless, it may be too early to tell whether these arrests meant the permanent end of Lapsus$. The arrests concerned UK-based members, but court proceedings are still in progress and the arrested individuals are known to not have been acting alone. Other individuals could still take over leadership of the group.

In the scenario that Lapsus$ is still active, the probability that the group would select Okto as a target is low. As detailed in the sections above, Lapsus$ was predominantly motivated by clout, notoriety, and challenge. Their main targets were global and prominent companies with many customers and a multitude of possible attack vectors. Okto's low profile and small footprint are not inviting to such a threat actor, even though its clients might be valuable targets. If the goal were financial gain, easier targets could be found (e.g. through phishing attempts and stealing of crypto wallets). As for clout and notoriety, attacking an organisation that does not have a website does not result in many boasting rights. Any attack would be unlikely to make the headlines or be shown off in the Telegram group.

This risk assessment might change if Okto has any high-profile clients. Indeed, it would be advisable to do an internal risk assessment of all clients to consider whether any of them run a higher risk of being targeted. High-profile clients in particular might draw more attention and headlines, and could therefore form a more appealing target. Besides requiring additional defences for their own assets, these clients could also increase the risk for Okto as a whole (see also: "Recommendations").

Being targeted by similar threat actors

As detailed in the Threat Assessment section, Lapsus$ as a group is most similar to hobby hackers and hacktivists. This section considers how likely it is that Okto will be targeted by these types of threat actors. As a starting point, Table 3 summarises their motivations, MO, organisation and structure, and infrastructure. The TTPs depend on specific actors and are therefore not included in this general overview.

Table 3: Hobby Hackers and Hacktivists

	Hobby hackers	Hacktivists
Motivations	Challenge and fun; later turn to profit and cybercrime	Challenge, ideology, current events (flashpoints)
Modus Operandi	Trying different methods until something yields results (e.g. access, profit, etc)	Publicly trolling a specific entity (e.g. by defacing a website or leaking embarrassing data) and claiming and publicising it
Organisation and structure	Loosely structured and ad hoc without clear hierarchy. Similar to friend groups	Loosely structured, smaller groups. Much like a collective that unifies around an idea
Infrastructure	Limited to what is available to them, e.g. open source software, public forums, and lower budgets	Generally limited to what is available to them; could become more sophisticated when aligned with a larger group

Overall, the risk from hacktivist threat actors is low, unless Okto happens to have high-profile clients or clients that might be involved in controversial or politicised practices. In that case, an actor could try to target that specific client or Okto's reputation and trust as retribution for working with them. Such attacks could hurt Okto's business as a whole.

The risk from hobby hackers is moderate. Lapsus$ has shown that simple methods can have a large impact without requiring many resources, but Okto's low profile and small footprint help the organisation's security. It makes the company more difficult to discover and less likely to become the target of an attack. If there are more accessible targets out there, a typical threat actor is likely to focus on those first.

Being targeted by threat actors in general

According to Europol's Internet Organised Crime Threat Assessment (IOCTA: Europol, 2021), today's biggest cybersecurity threat comes from profit-driven cybercriminals who continue to evolve, mature, and specialise. Europol states that, while the use of ransomware is not new, these threat actors are increasingly moving towards more calculated target selection. They are focusing their efforts on high-value attacks on large organisations and spear phishing attempts of upper-level management, for example.

While Okto cannot be characterised as a 'large organisation', a well-prepared attack could certainly be of high value. As such, **profit-driven cybercriminals form the highest risk for an organisation like Okto and should be taken more seriously than the threat from groups like Lapsus$**. The motivations, MO, organisation and structure, and infrastructure of profit-driven cybercriminals have been summarised in Table 3.

Table 3: Profit-Driven Cybercriminals

	Profit-driven cybercriminals
Motivations	Financial gain
Modus Operandi	Attacking an entity with ransomware, data breach attacks, or similar, and extorting them for money
Organisation and structure	Semi-hierarchical, structured groups in which different actors play different roles
Infrastructure	More advanced: could host C&C servers and have their own ransomware, website, and even offices. Engages in online marketplaces

These threat actors form a higher risk because they are clearly motivated by financial gain, which can be found with Okto's clients. Cybercriminals tend to be more specialised and advanced as well: some groups create their own ransomware, design highly customised spear phishing attacks, and outsource parts of their operations to specialised third parties (ibid). Their organisation has clearer roles and responsibilities than that of loosely connected groups like Lapsus$, increasing their efficiency. Moreover, they are likely to be more effective in claiming ransoms than Lapsus$ was, as profit is their main reason for existence. As the Cyber Safety Review Board stated, "[i]f richly resourced cybersecurity programs were so easily breached by a loosely organized threat actor group which included several juveniles [i.e. Lapsus$], how can organizations expect their programs to perform against well-resourced cybercrime syndicates (...)?" (2023, p.iv). Combining Lapsus$'s most effective methods with an increased level of structure and focus yields a high risk threat actor.

Recommendations

These recommendations are intended to mitigate the threat from organised, profit-driven cybercriminals. There are three groups of recommendations, namely those related to education, a more detailed assessment of Okto's present state, and technical defences. The scope is strategic.

Education

The success rate of attacks from profit-driven cybercriminals is improved significantly when personal information and credentials are obtained, as these are instrumental for all kinds of social engineering attacks (Europol, 2021). Threat actors also put more pressure behind ransomware demands, including by cold-calling victims and attacking a target from multiple sides at once.

Considering this reality, it is of critical importance that Okto educates its employees, consultants (if applicable), and clients on the risks of ransomware, social engineering, and phishing. Anyone with access to critical systems and information should be educated first. Prevention is the best line of defence against any threat actor, and frequent training and reminders of threats will help.

On a related note, Okto should embrace a culture of openness in the organisation. If someone has even the slightest suspicion of suspicious activity on the network (whether internal or external), they should feel comfortable to reach out to the IT manager instantaneously. Similarly, if someone accidentally clicks on a malicious link, they should feel comfortable to share this right away without feeling ashamed or fearing retribution. Anyone can fall victim to social engineering attacks, and catching them early will help to prevent further escalation.

Detailed risk assessment

As noted in the section on Okto's crown jewels, more information is needed to assess which assets are most likely to be subjected and vulnerable to an attack. Recall that the crown jewels were access to clients' assets, the list of clients, employee data and credentials, and reputation and trust. Knowing which of these four is least defended will allow Okto to prioritise its time and resources in strengthening its defences. For example, while clients' assets might be most valuable, they might already be protected appropriately by banks' extensive security measures (cf. Know Your Customer (KYC) practices as mandated by the European Union). Banks outside of the EU might not have these same standards in place.

A risk assessment should also include Okto's list of clients to see if any of them are high profile individuals, public figures, or engaging in controversial or politicised practices. Public figures in particular could increase the public's awareness of Okto as an investment company. Okto's low profile helps its security significantly, and should therefore be maintained as desired.

Okto should also consider the extent to which it works with external consultants. While there are only three full-time employees, anyone with passing access to the network could expand the organisation's footprint and therefore its vulnerability to compromise.

Technical defences

The best defence against ransomware and phishing attacks is to maintain strong Multi-Factor Authentication (MFA) practices for key systems. It is advisable to use physical security keys (FIDO tokens) or authenticator apps as a second factor solution, rather than phone numbers. Lapsus$ has demonstrated that SIM swapping is not difficult to do, so phone number-based MFA does not provide sufficient security. MFA should be used for any system that carries important information for the organisation or its clients. This includes but is not limited to log-ins to email, clients' investment accounts, VPNs, and database access accounts, and should be used whether the user logs in on-premises or remotely.

Employees should be strongly discouraged from ever storing any credentials in open text, even if they are stored on an internal system. Such information can be found by any threat actor

with initial access to the network and could significantly worsen the damage they can do. The use of password managers and randomised passwords is strongly recommended. Passwordless systems are even more preferable, if it is within scope to adopt such a system.

The number of endpoints from which users can log in should be limited as much as possible (within workability limits). Any log-ins from personal devices should be discouraged. Company-provided devices should consistently be monitored to ensure that they remain trusted and compliant with the latest security recommendations. It is strongly advisable that Okto adopts secure remote-working tools (e.g. VPNs and remote desktop tools with MFA). Threat actors are known to increasingly take advantage of vulnerabilities in this kind of software (Europol, 2021) and this recommendation can help to reduce the attack vector of malicious actors.

More detailed technical defences, including how to set up alerts on suspicious activity, can be found in reports by Microsoft (2022), Intrinsec Sécurité (2022), CSRB (2023), Europol (2021), Platsis (2023), and the Research & Intelligence Fusion Team (2022).

Conclusion

This report assessed threat actor Lapsus$ and the risk of this and similar actors to Okto. It established that Lapsus$ was a loosely structured juvenile group with 7 to 10 members, motivated by a combination of clout, notoriety, and challenge. Their MO was to obtain initial access to an organisation by acquiring credentials from existing users, obtain and sometimes delete data from the target network, and then extort the organisation by threatening to release the data. The group's infrastructure was limited, as could be expected from a threat actor like this.

The review is based on open source information that was available, reliable, credible, and relevant to the audience. Overall, the CyTact team has a high level of confidence in the overall threat assessment of the actor. While some gaps in the intelligence persist, this information is unlikely to change the overall conclusions of the report.

The probability that Okto will be targeted centres around its 'crown jewels', i.e. its most important assets. For Okto, these are access to client's assets, the list of clients, employee data and credentials, and its reputation and trust.

It is unlikely that Okto will be targeted by Lapsus$ itself: it appears that the group is no longer active and Okto does not fit the description of a typical target for the group. Threat actors similar to Lapsus$ (i.e. hobby hackers and hacktivists) might consider attacking, but predominantly if Okto happens to have high-profile clients or clients that are involved in controversy or politicised practices.

Overall, profit-driven cybercriminals form the highest risk for an organisation like Okto and should be taken more seriously than the threat from groups like Lapsus$. The risk can be mitigated by educating Okto's employees and clients, conducting a more detailed risk assessment to understand the key priorities of the organisation, and improving Okto's technical defences accordingly.

Appendix

Admiralty Grading System (JDP2-00, 2011, p3-21)

Reliability of the collection capability		Credibility of the information	
A	Completely reliable	1	Completely credible
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

References

AbuseIPDB. (n.d.). *185.56.83.40 | DataShield Inc.* Retrieved August 13, 2023, from https://www.abuseipdb.com/check/185.56.83.40?page=1#report

ATT&CK® Navigator. (n.d.). *Lapsus$—G1004*. Retrieved August 14, 2023, from https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG1004%2FG1004-enterprise-layer.json

BBC News. (2022a, March 24). Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal. *BBC News*. https://www.bbc.co.uk/news/technology-60864283

BBC News. (2022b, April 1). Lapsus$: Two UK teenagers charged with hacking for gang. *BBC News*. https://www.bbc.com/news/technology-60953527

BeyondTrust. (2022, November 30). *How to Use Metasploit for Command & Control*. https://www.beyondtrust.com/blog/entry/how-to-use-metasploit-for-command-control

City of London Police. (2022, September 23). *@CityPolice on Twitter*. Twitter. https://twitter.com/CityPolice/status/1573281533665972225

Coleman, G. (2015). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. https://www.amazon.co.uk/Hacker-Hoaxer-Whistleblower-Spy-Faces/dp/1781689830

Cox, J. (2022, March 24). LAPSUS$: How a Sloppy Extortion Gang Became One of the Most Prolific Hacking Groups. *Vice*. https://www.vice.com/en/article/3abedn/who-is-lapsus-hacking-gang

crt.sh. (n.d.). *Lapsus-group.com*. Retrieved August 13, 2023, from https://crt.sh/?q=lapsus-group.com

Cyber Safety Review Board. (2023, August 10). *Review Of The Attacks Associated with Lapsus$ And Related Threat Groups Report | CISA*. https://www.cisa.gov/resources-tools/resources/review-attacks-associated-lapsus-and-related-threat-groups-report

DarkOwl Analyst Team. (2022, February 18). *Darknet Threat Actor Report: LAPSUS$*. DarkOwl, LLC. https://www.darkowl.com/blog-content/darknet-threat-actor-report-lapsus/

Doxbin. (n.d.). *Doxbin page for AK*. Retrieved July 15th, 2023.

Europol. (2021, December 1). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Europol. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Hardcastle, J. L. (2023, April 25). *Mandiant: Teenagers among "most prevalent threat actors."* https://www.theregister.com/2023/04/25/mandiant_rsa_teenage_hackers/

Hollister, S. (2022, March 4). *As Nvidia hacker deadline looms, 71,000 employee accounts have reportedly been exposed*. The Verge. https://www.theverge.com/2022/3/4/22962217/nvidia-hack-lapsus-have-i-been-pwned-email-breach-password

Internet Archive. (2021, April 10). *Infinity Recursion—Capture of http://recursion.team*. https://web.archive.org/web/20210410013319/http://recursion.team/

Intrinsec Sécurité. (n.d.). *Intrusion Set Lapsus$—ATT&CK® Navigator*. Retrieved August 14, 2023, from https://mitre-attack.github.io/attack-navigator/#layerURL=https://raw.githubusercontent.com/Intrinsec/IOCs/main/Extorsion-group_LAPSUS%24/LAPSUS%24_intrusion_set_ATT%26CK_Navigator.4.5.5_layer_4.3.json

Intrinsec Sécurité. (2022, March 28). *Analysis of LAPSUS$ Intrusion Set*. https://www.intrinsec.com/analysis-of-lapsus-intrusion-set/

IPI. (2022, February 10). Portugal's Expresso newspaper still recovering from debilitating ransomware attack. *International Press Institute*. https://ipi.media/portugals-expresso-newspaper-still-recovering-from-debilitating-ransomware-attack/

Joyce, K. (2021, November 30). What Is DCSync Attack? *Https://Blog.Netwrix.Com/*. https://blog.netwrix.com/2021/11/30/what-is-dcsync-an-introduction/

Krebs, B. (2022a, March 23). *A Closer Look at the LAPSUS$ Data Extortion Group*. https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/

Krebs, B. (2022b, March 29). *Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests."* https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/

Krebs, B. (2022c, April 6). *The Original APT: Advanced Persistent Teenagers*. https://krebsonsecurity.com/2022/04/the-original-apt-advanced-persistent-teenagers/

Krebs, B. (2022d, April 12). *RaidForums Gets Raided, Alleged Admin Arrested*. https://krebsonsecurity.com/2022/04/raidforums-get-raided-alleged-admin-arrested/

Krebs, B. (2022e, April 22). *Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code*. https://krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code/

Krebs, B. (2022f, May 12). *DEA Investigating Breach of Law Enforcement Data Portal*. https://krebsonsecurity.com/2022/05/dea-investigating-breach-of-law-enforcement-data-portal/

Krebs, B. (2023, March 14). *Two U.S. Men Charged in 2022 Hacking of DEA Portal*. https://krebsonsecurity.com/2023/03/two-us-men-charged-in-2022-hacking-of-dea-portal/

Lee, M. (2023). *Cyber Threat Intelligence*.

Meskauskas, T. (2023, March 17). *RedLine Stealer Malware*. https://www.pcrisk.com/removal-guides/17280-redlinestealer-malware

Microsoft (Incident Response & Threat Intelligence teams). (2022, March 22). *DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

MITRE ATT&CK. (n.d.). *SIM Card Swap, Technique T1451*. Retrieved August 13, 2023, from https://attack.mitre.org/techniques/T1451/

MITRE ATT&CK. (2023a, March 7). *Mimikatz, Software S0002*. https://attack.mitre.org/software/S0002/

Newman, L. H. (2022, March 15). The Lapsus$ Hacking Group Is Off to a Chaotic Start. *Wired*. https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/

Platsis, G. (2023, April 6). How to Defend Against Extortion Groups Like Lapsus$. *Security Intelligence*. https://securityintelligence.com/articles/how-to-defend-against-extortion-groups-lapsus/

Research & Intelligence Fusion Team. (2022, April 28). *LAPSUS$: Recent techniques, tactics and procedures*. NCC Group Research Blog. https://research.nccgroup.com/2022/04/28/lapsus-recent-techniques-tactics-and-procedures/

Sayegh, E. (2023, March 15). *Teenagers Leveraging Insider Threats: Lapsus$ Hacker Group*. Forbes. https://www.forbes.com/sites/emilsayegh/2023/03/15/teenagers-leveraging-insider-threats-lapsus-hacker-group/

Silent Push Labs Team. (2022). *Lapsus$ Group—An emerging dark net threat actor leveraging insider threats-or was it?* Silent Push Threat Intelligence. https://www.silentpush.com/blog/lapsus-group-an-emerging-dark-net-threat-actor

Temple-Raston, D. (2022, April 26). *Lapsus$: The script kiddies are alright*. https://therecord.media/lapsus-the-script-kiddies-are-alright

The DFIR Report. (2021, October 22). *@TheDFIRReport on Twitter*. Twitter. https://twitter.com/TheDFIRReport/status/1451567772471865350

Tills, C. (2022, July 20). *Brazen, Unsophisticated and Illogical: Understanding the LAPSUS$ Extortion Group*. Tenable®. https://www.tenable.com/blog/brazen-unsophisticated-and-illogical-understanding-the-lapsus-extortion-group

Turton, W., & Robertson, J. (2022, March 23). Teen Suspected by Cyber Researchers of Being Lapsus$ Mastermind. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2022-03-23/teen-suspected-by-cyber-researchers-of-being-lapsus-mastermind

UK Ministry of Defence. (2011). *Joint Doctrine Publication 2-00: Understanding and Intelligence Support to Joint Operations*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf

Unit 42. (2022, March 24). Threat Brief: Lapsus$ Group. *Unit 42*. https://unit42.paloaltonetworks.com/lapsus-group/

Vaas, L. (2022, March 24). *UK Cops Collar 7 Suspected Lapsus$ Gang Members*. https://threatpost.com/uk-cops-collar-7-suspected-lapsus-gang-members/179098/