VEDERE LABS

LAPSUS$

The rise, fall and return of a hacking group

30 March 2022

Contents

1. Executive Summary 3
2. Victim History 3
3. Technical Analysis 5
  3.1. Organization and motives 5
  3.2. Tactics, Techniques and Procedures 8
  3.3. Discussion 9
4. IoCs 9
5. Mitigation Recommendations 10
6. References 10

1. Executive Summary

LAPSUS$ is a hacking group that has been active since 2021 and has breached several high-profile organizations, starting with major Brazilian governmental agencies and companies, then moving on to global businesses such as Microsoft, Nvidia and Okta.

Following a series of high-profile data breaches in March 2022, seven teenagers allegedly connected to LAPSUS$ were arrested by the London Police Service on March 24, 2022. The arrests came after one of the teenagers had his personal information exposed on a doxing site by a former partner. Even after the arrests, the group announced a new breach on March 30.

LAPSUS$ has gained notoriety not just because of its targets, but also because the group is very different from the ransomware gangs that have been making headlines recently in at least three ways: relying heavily on obtaining and leveraging valid credentials from employees of their target companies using mostly social engineering techniques; focusing on data exfiltration and public extortion rather than encrypting data on their targets; and resembling a loose collective of hackers rather than a large and very well-organized criminal enterprise like Conti.

In this threat briefing, we report on the victims of LAPSUS$ (Section 2), the group's main tactics, techniques and procedures (Section 3), their indicators of compromise (Section 4) and some mitigation recommendations (Section 5).

2. Victim History

Table 1 shows a list of the victims targeted by LAPSUS$. Most of the content is based on analyzing their public Telegram chats – https://t.me/saudechat and https://t.me/minsaudebr – which amassed more than 50,000 members. Some of the remarks come from other sources, such as information provided by the victims themselves in public statements.

Table 1 – List of LAPSUS$ victims

Victim	Date Announced	HQ Location	Remarks
EA	Jun 2021	United States	Exfiltrated 780GB of source code. This incident was not claimed by LAPSUS$, but after the connections between the group and whitedoxbin (one of the arrested teenagers) became clear, it has been attributed to them. The initial entry was via stolen credentials bought on a dark web marketplace.
Ministério da Saúde (Brazil's Ministry of Health)	Dec 10,2021	Brazil	Accessed AWS and vCenter servers. Obtained 4TB of data and deleted more than 100TB. The first high-profile incident publicly announced by the group.
Correios (Brazil's postal service)	Dec 23, 2021	Brazil	Another Brazilian governmental agency attacked right after the Ministry of Health. The group managed to take the website

			offline, but there was no data leaked and no evidence of data obtained.
Claro	Dec. 24,2021	Brazil	The three breaches were announced together and included access to AWS and vCenter servers, GitLab and SVN repositories, as well as legal documents and e-mails. In total, the group claimed more than 10 PB of exfiltrated data.
Embratel	Dec. 24,2021	Brazil	
NET	Dec. 24,2021	Brazil	
Impresa	Jan 3, 2022	Portugal	The group posted from the victim’s Twitter account and sent phishing SMS to Impresa’s customers.
Localiza	Jan 11, 2022	Brazil	The group redirected website visitors to a pornographic website.
Cofina	Feb 6, 2022	Portugal	This incident was never publicly claimed by LAPSUS$ but has been attributed to them based on the type of victim (Portuguese media company) and the proximity to other incidents.
Vodafone	Feb 24, 2022	Portugal	Another incident that was not claimed by LAPSUS$ but has been attributed to them based on victim type (Portuguese telecom).
NVIDIA	Feb 26, 2022	United States	Maintained access for more than a week and obtained 1TB of data, including source code and digital certificates.
Samsung	Mar 4, 2022	South Korea	Leaked source code of applets in Trusted Execution Environment, biometric operations, bootloaders, online services and others.
Ubisoft	Mar 12, 2022	France	Services were momentarily taken offline but there was no data leaked.
Microsoft	Mar 20, 2022	US	The group used an employee account to access and leak source code of Bing, Bing Maps and Cortana.
LG	Mar 22, 2022	South Korea	The group dumped hashes of employee and service accounts.
Okta	Mar 22, 2022	US	Last breached announced before the arrests. The group claimed to achieve superuser status at some of Okta’s customers and to be able to manage Okta’s employee credentials.

Globant	Mar 30, 2022	United States	First breached announced after the arrests. Administrative credentials and 70GB of internal data have been leaked.

On March 23, following news of the Okta breach and one day before seven members were arrested, the group posted the following:

> *A few of our members has a vacation until 30/3/2022.*
>
> *We might be quiet for some times.*
>
> *Thanks for understand us. - we will try to leak stuff ASAP.*

Many thought the group had disbanded after the initial arrests, but as promised, on March 30, it returned by announcing a new breach and a move to a new communications channel:

> *We are officially back from a vacation (spoiler above)*
>
> *For anyone who is interested about the poor security practices in use at Globant.com. i will expose the admin credentials for ALL there devops platforms below.*
>
> [REDACTED TO REMOVE THE CREDENTIALS]
>
> *We created a Element/Matrix chat in the case this Telegram is deleted!*
>
> *https://matrix.to/#/#lapsus:matrix.org*
>
> *We advise everyone to join it!*

At the time of writing, the new chat had more than 1000 members.

3. Technical Analysis

LAPSUS$ often posts on social media (mainly Telegram channels) about its techniques, victims, stolen data, demands and other details, which, when coupled with technical analyses of some of their incidents, allows us to understand the group's motives and compare them to other recent notorious cybercriminal enterprises.

3.1. Organization and motives

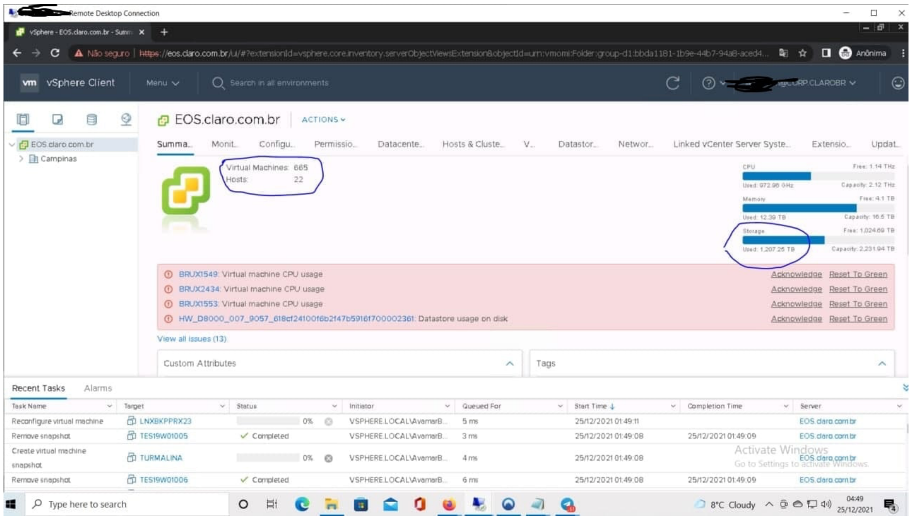
LAPSUS$ appears to be much less structured than recent Ransomware-as-a-service gangs, such as Conti. Conti operates with many "employees" developing specific tools (e.g., encryptors, decryptors, affiliate and victim management portals), acquiring initial access from other groups, hiring and managing talent, negotiating ransom and so on. LAPSUS$, on the other hand, does not have an affiliate program, operates its breaches from beginning to end (i.e., from initial access to data exfiltration and negotiation) and resorts either to low-tech hacking techniques based on social engineering or to reusing existing and well-known malware (more details in Section 3.2).

Different from the most prolific cybercriminal groups of recent times, LAPSUS$ does not operate out of Eastern Europe. There have been several U.K. individuals arrested due to links with the group, but it is believed that either there are other members in Brazil or they have a strong connection with Brazilian individuals. That is because most of the initial victims were Brazilian (as shown in Section 2), and many of their messages were posted both in Portuguese and in English, such as the one below:

> *Hi.*
>
> *We write to announce a breach.*
>
> *We inform you Claro, Embratel, and NET has suffered a major data breach, in the past month we have been pivoting to various systems.*
>
> *The systems we access: Many AWS, 2x Gitlab, SVN, x5 vCenter (MCK, CPQCLOUD, EOS, ODIN), Dell EMC storage, all inboxes, Telecom/SS7, Vigia (Police interception), MTAWEB and WPP (customer management), and much more!*
>
> *The total amount of data we had access to exceeds 10pb ~ 10000tb, including customer information, telecom infrastructure,*
>
> *Legal documents, wiretap orders, source code, emails.*
>
> *Although we only took a small portion of the data (the important stuff, legal, wiretap, src codes, svn)*
>
> *We request a Claro representative to contact us at @whitedoxbin or mail us saudegroup@ctemplar.com*
>
> *We will come to some agreement, where such i delete the data in exchange for a small reward/fee.*
>
> *Otherwise we will be forced to share the data with the public eye!*
>
> *I should add that the leakage of the sensitive legal orders and wiretaps would cause law enforcement major issues (the suspect will know they are watched) \\10.1.104.35\JD_Nextel\Wire_Tap\\ and various other areas such as the Vigia*
>
> *Thanks! Nice day!*
>
> *We request a Claro representative to contact us at @whitedoxbin or mail us saudegroup@ctemplar.com*

> *Oi.*
>
> *Escrevemos para anunciar uma violação.*
>
> *Informamos que a Claro, Embratel e NET sofreram uma grande violação de dados, no mês passado estivemos rodando para vários sistemas.*
>
> *Os sistemas que acessamos: Muitos AWS, 2x Gitlab, SVN, x5 vCenter (MCK, CPQCLOUD, EOS, ODIN), armazenamento Dell EMC, todas as caixas de entrada, Telecom / SS7, Vigia (interceptação policial), MTAWEB e WPP (gerenciamento de cliente), e muito mais!*
>
> *A quantidade total de dados aos quais tivemos acesso excede 10pb ~ 10.000 TB, incluindo informações do cliente, infraestrutura de telecomunicações,*
>
> *Documentos jurídicos, pedidos de escuta telefônica, código-fonte, e-mails.*
>
> *Embora tenhamos obtido apenas uma pequena parte dos dados (as coisas importantes, legal, escuta telefônica, códigos src, svn)*
>
> *Solicitamos que um representante da Claro nos contate em @whitedoxbin ou envie-nos um e-mail saudegroup@ctemplar.com*
>
> *Nós chegaremos a um acordo, onde tal eu apago os dados em troca de uma pequena recompensa / taxa.*
>
> *Caso contrário, seremos forçados a compartilhar os dados com os olhos do público!*
>
> *Devo acrescentar que o vazamento de ordens jurídicas confidenciais e escutas telefônicas causaria grandes problemas de aplicação da lei (o suspeito saberá que estão sendo vigiados) \\ 10.1.104.35 \ JD_Nextel \ Wire_Tap \\ e várias outras áreas, como Vigia*
>
> *Obrigado! Bom dia!*
>
> *Solicitamos que um representante da Claro nos contate em @whitedoxbin ou envie-nos um e-mail saudegroup@ctemplar.com*

The part highlighted in red shows LAPSUS$' main extortion technique: exfiltrating sensitive information and demanding victim organizations to pay to avoid having the data exposed. It often coupled such messages with proof of the intrusion in the form of parts of the data leaked or screenshots showing access to internal systems, such as Figure 1.



[redacted]Remote Desktop Connection

vSphere - EOS.claro.com.br - Summ

Não seguro | https://eos.claro.com.br/ui/#?extensionId=vsphere.core.inventory.serverObjectViewsExtension&objectId=urn:vmomi:Folder:group-d1:bbda1181-1b9e-44b7-94a8-aced4...

EOS.claro.com.br

Virtual Machines: 665
Hosts: 22

CPU — Free: 1.14 THz — Used: 972.96 GHz — Capacity: 2.12 THz
Memory — Free: 4.1 TB — Used: 12.39 TB — Capacity: 16.5 TB
Storage — Free: 1,024.69 TB — Used: 1,207.25 TB — Capacity: 2,231.94 TB

BRUX1549: Virtual machine CPU usage — Acknowledge — Reset To Green
BRUX2434: Virtual machine CPU usage — Acknowledge — Reset To Green
BRUX1553: Virtual machine CPU usage — Acknowledge — Reset To Green
HW_D8000_007_9057_618cf24100f6b2f47b5916f700002361: Datastore usage on disk — Acknowledge — Reset To Green

View all issues (13)

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
Reconfigure virtual machine	LNXBKPPRX23	0%	VSPHERE.LOCAL\AvamarB...	5 ms	25/12/2021 01:49:11		EOS.claro.com.br
Remove snapshot	TES19W01005	✓ Completed	VSPHERE.LOCAL\AvamarB...	3 ms	25/12/2021 01:49:08	25/12/2021 01:49:09	EOS.claro.com.br
Create virtual machine snapshot	TURMALINA	0%	VSPHERE.LOCAL\AvamarB...	4 ms	25/12/2021 01:49:08		EOS.claro.com.br
Remove snapshot	TES19W01006	✓ Completed	VSPHERE.LOCAL\AvamarB...	6 ms	25/12/2021 01:49:08	25/12/2021 01:49:09	EOS.claro.com.br

Figure 1 - Screenshot showing access to Claro's internal system

In other instances, mainly when targeting large technology organizations, the group went after intellectual property instead of other types of sensitive data but presented similar demands, as shown in the conversation below:

> *We hacked NVIDIA,*
>
> *The hack is kinda public atm, and here's our announcement,*
>
> *We were into nvidia systems for about a week, we fastly escalated to admin of a lot of systems.*
>
> *We grabbed 1TB of data,*
>
> *We grabbed the most important stuff, schematics, driver, firmware, etc…*
>
> *We are still waiting for nvidia to contact us.*
>
> *We are also selling a full LHR V2 (GA102-GA104) -> we hope it will soon be removed by nvidia*
>
> *If NVIDIA doesn't contact us, we will take actions.*
>
> *Please note: We are not state sponsored and we are not in politics AT ALL.*
>
> *Btw NVIDIA tried but failed, we have all the data.*
>
> *We also have documentation, private tools and SDKs, and everything about falcon, we know what is valuable, nvidia, please contact us.*
>
> *Can mail us @ nvidia_chats@protonmail.com*
>
> *Nvidia data leak part 1*
>
> *Today we will leak part one of Nvidia data, this leak contains source code and highly confidential/secret data from various parts of NVIDIA gpu driver. Falcon, LHR, and such.*
>
> *Soon will come another part!*

Besides the targeted data, the other parts highlighted in the messages above contain some discussion about the group's motivation. It claimed to be motivated financially and not politically, as well as not to be state-sponsored. At the same time, it stored a data leak on an S3 bucket named "jairbolsonaro" – likely a joke referring to the Brazilian president.

A last interesting point that can be extracted from the group's conversations is about its own operational security. The messages above show that they rely on Telegram and e-mail for communication, which is again different from the .onion infrastructure typically adopted by modern ransomware gangs. The group's choices and apparent lack of concern with operational security led to several adverse events for the group. For example, Microsoft managed to stop its breach before a full source code leak because the group mentioned the attack on Telegram as it was happening. In another instance, NVIDIA infiltrated its systems and encrypted part of the data obtained by the group, as discussed in their chat below:

> *To address all the rumours about how nvidia hacked us.*
>
> *Its simple.*
>
> *Access to nvidia employee VPN requires the PC to be enrolled in MDM (Mobile Device Management).*
>
> *With this they were able to connect to a VM we use.*
>
> *Yes they successfully encrypted the data. However we have a backup and it's safe from scum!!!*
>
> *We are not hacked by a competitors groups or any sorts.*

3.2. Tactics, Techniques and Procedures

If we again compare LAPSUS$ with major RaaS gangs, we can notice both similarities and differences in their TTPs. In summary, their initial access and Impact methods are very different, while their lateral movement is somewhat similar.

For initial access, LAPSUS$ relies mainly on obtaining valid credentials to the targeted organizations. These are obtained via several means, such as recruiting employees at the breached companies, compromising personal accounts, convincing help desk personnel to reset credentials, searching public repositories for exposed credentials, SIM swapping and buying credentials in dark web markets such as Genesis. In some instances, LAPSUS$ has relied on the Redline Stealer password-stealing malware. With the compromised credentials, it typically leverages access to VPN, RDP or VDI systems and from there move laterally to systems containing sensitive data.

Below is an example of the group openly recruiting employees at targeted organizations to provide them with initial access to the environment in the form of VPN and VDI credentials:

> *We recruit employees/insider at the following!!!!*
>
> *- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)*
>
> *- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)*
>
> *- Callcenter/BPM (Atento, Teleperformance, and other similar)*
>
> *- Server hosts (OVH, Locaweb, and other similar)*
>
> *TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk*
>
> *If you are not sure if you are needed then send a DM and we will respond!!!!*
>
> *If you are not a employee here but have access such as VPN or VDI then we are still interested!!*
>
> *You will be paid if you would like. Contact us to discuss that*
>
> *@lapsusjobs*

For lateral movement, LAPSUS$ exploits known vulnerabilities in internal applications (often JIRA, Confluence and GitLab), searches for credentials in internal repositories and uses typical Windows admin/exploitation tools such as AD explorer coupled with DCsync attacks and Mimikatz.

For impact, it usually limits actions to data collection and exfiltration without encrypting data on the target networks. As discussed in Section 3.1, this data is then either leaked directly or threatens organizations with leaking it unless the group gets paid.

Other forms of impact, such as denial of service on public websites or defacement, were common in the initial incidents that happened at the end of 2021, but they have not been seen in some time, and the group seems to have specialized in data exfiltration.

3.3. Discussion

LAPSUS$ shows that even loose groups of hackers motivated by financial gain and without developing sophisticated tools or hacking techniques can cause serious damage to organizations. It also shows the importance of monitoring valid employee or system accounts and anomalous behavior coming from those. We discuss recommendation mitigations in Section 5.

Two of the group's incidents highlight the issues with supply chain security:

- As part of the NVIDIA breach, LAPSUS$ leaked valid certificates that can be used to sign malware and make it appear as a trusted application. There is already evidence of malware signed with these certificates surfacing, and they are listed in Section 4.
- As part of the Okta breach, there were conflicting versions about what it could have done as a superuser managing the accounts of employees at thousands of organizations. So far, there has been no evidence of further compromises via Okta, but this raises the concern that this kind of application could be an initial access point to breach or drop malware into several organizations, as seen in previous incidents such as Kaseya/REvil in July 2021.

4. IoCs

.

Table 2 lists IoCs related to LAPSUS$ shared on https://otx.alienvault.com/pulse/62324535fc8686a6577c135a/.

Table 2 – IoCs

IoC	Type	Description
http://8.3.1.0	URL	
51.89.208.22	IPv4	
198.244.205.12	IPv4	
108.61.173.214	IPv4	
104.238.222.243	IPv4	
185.56.83.40	IPv4	
104.238.222.158	IPv4	

103.195.100.11	IPv4	
2f578cb0d97498b3482876c2f356035e3365e2c492e10513ff4e4159eebc44b8	FileHash	DLL signed with stolen NVIDIA certificate.
065077fa74c211adf9563f00e57b5daf9594e72cea15b1c470d41b756c3b87e1	FileHash	Quasar RAT malware signed with stolen NVIDIA certificate.
43bb437d609866286dd839e1d00309f5		Certificate serial number for NVIDIA stolen certificate.
14781bc862e8dc503a559346f5dcc518		Certificate serial number for NVIDIA stolen certificate.

5. Mitigation Recommendations

Since the group used varied techniques ranging from social engineering to password-stealing malware, the mitigation recommendations are diverse.

- Train employees on social engineering and phishing to avoid valid credentials being used for initial access.
- Use strong and unique passwords.
- Monitor data leaks and underground markets for exposed credentials.
- Employ multi-factor authentication whenever possible to ensure that stolen credentials cannot easily be used.
- Identify vulnerable devices, patch them and segment the network to avoid lateral movement.
- Monitor insider threats and large data transfers to prevent data leakage.

6. References

- https://www.flashpoint-intel.com/blog/lapsus/
- https://www.darkowl.com/blog-content/darknet-threat-actor-report-lapsus/
- https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/
- https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/