INTRINSEC
Innovative by design

High-Profile Data Theft
Intrusion Set LAPSUS

CYBER THREAT INTELLIGENCE

Analysis of LAPSUS$ Intrusion Set

March 28, 2022

Website
www.intrinsec.com

Blog
www.intrinsec.com/blog

Twitter
@Intrinsec

EXECUTIVE SUMMARY

LAPSUS$ is a relatively new **English** and **Portuguese** speaking **intrusion set** that recently made the news by conducting **big game hunting via single extortion schemes** (data theft) on both public and private entities; some of them being **Electronic Arts**, **The Ministry of Health** (MoH) of **Brazil**, **Microsoft** or **Okta**. To this date, Personal Identifiable Information (**PII**) **are less prone to get targeted** and exfiltrated upon attacks, only Mercado Libre & Okta suffered such breaches. Instead, this intrusion set **focuses on proprietary source code** (that could however contain PII) unless not intended end-target are at play (targeting customers' victims or to bypass MFA).

LAPSUS$ intrusion set **does not encrypt victim's data** (with maybe the exception of the MoH), though some members might have employed ransomwares in a pre-LAPSUS$ era (at least one member of the group claimed he did). In order to breach into its victims' networks, this intrusion set **employs not only advanced social engineering techniques** that encompass **SIM swap** attacks **against** the **telecommunication sector and spearphishing**, but also the **acquisition** of **active passwords & session tokens** on specialized **dark web** markets and forums.

The first **targeted countries** were exclusively **Lusophone entities**. LAPSUS$ intrusion set then **broadened its hunting areas to France, the United States, Argentina, South Korea and Nepal**. Several industries operating **in various sectors of activity** have fallen victim to the schemes of the LAPSUS$ intrusion set, including a **video game company, telecom/media conglomerates and high tech firms**. To the best of our knowledge, the **hack of several ministries of the Brazilian government** are the **only public entities that were targeted**.

This intrusion set made **various opsec errors** that **were leveraged**, either by members being part of LAPSUS$, or close enough to the intrusion set **to conduct doxing operations**. At least **one of the LAPSUS$'s member** has seen **its identity doxed** (white aka Alexander). This intrusion set seems **primarily motivated by personal gains more than hacktivism**. **TTPs** observed upon several campaigns could be categorized at the first glance into the scope of ideology (hacktivism) and/or notoriety, which **could emanate from a composite group with misaligned skills and motivations**. We have good reasons to believe that **a more probable scenario is the leveraging of the medias as an echo chamber to increase pressure on victims** to **gather higher ransom amounts**.

In this context, **the City of London Police** announced the 24th of March 2022 that **seven teenagers** between the ages of 16 and 21 **were arrested**. We don't know if the supposedly "mastermind" of the LAPSUS$ intrusion set is amongst the seven, while all have been released under investigation. **LAPSUS$ admins remain active** and Intrinsec CTI team currently cannot confirm what impact those investigations will have on the next operations already planned by this intrusion set.

As one could wonder, we'd like to mention that **this intrusion set is not related whatsoever with the armed conflict in Ukraine**.

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

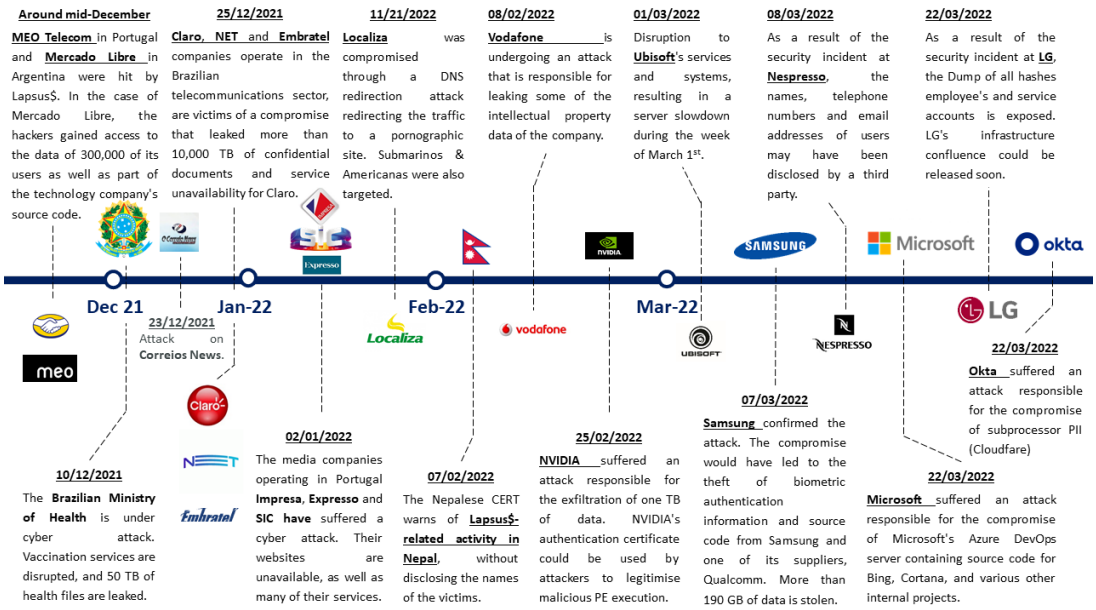
TLP:WHITE

Chronology

LAPSUS$ intrusion set as a group has been active since May 2021 only, strengthening its impact at the beginning of this year. This group could appear rather limited in size and sophistication, though they were able to conduct various Big game hunting attack campaigns. The group’s origin was most likely initially Brazilian (Portuguese native speaker(s); a Brazilian source who has already investigated this threat actor reports that some members could also be from Colombia, while another source mentioned one person living in Russia and a Ukrainian friend of the latter).

At first, LAPSUS$ intrusion set activity targeted mainly Portuguese-speaking entities (Brazil, Portugal). Later, the group also appeared to be compromising victims in Nepal as well as France, South Korea and in the US.

Their victimology does not seem to follow a specific pattern, their sectors of activity being rather different from one another. Refer to the timeline for an overview of the known victims.



Timeline of the confirmed LAPSUS$ attacks. The latter has engaged in extortion attempts against at least 15 different targets.

Alias

- LAPSUS$
- aka SaudeGroup

Aka

- Slippy Spider (Crowdstrike)
- DEV-0537 (Microsoft)
- UNC3661 (Mandiant)

INTRUSION SET ANALYSIS

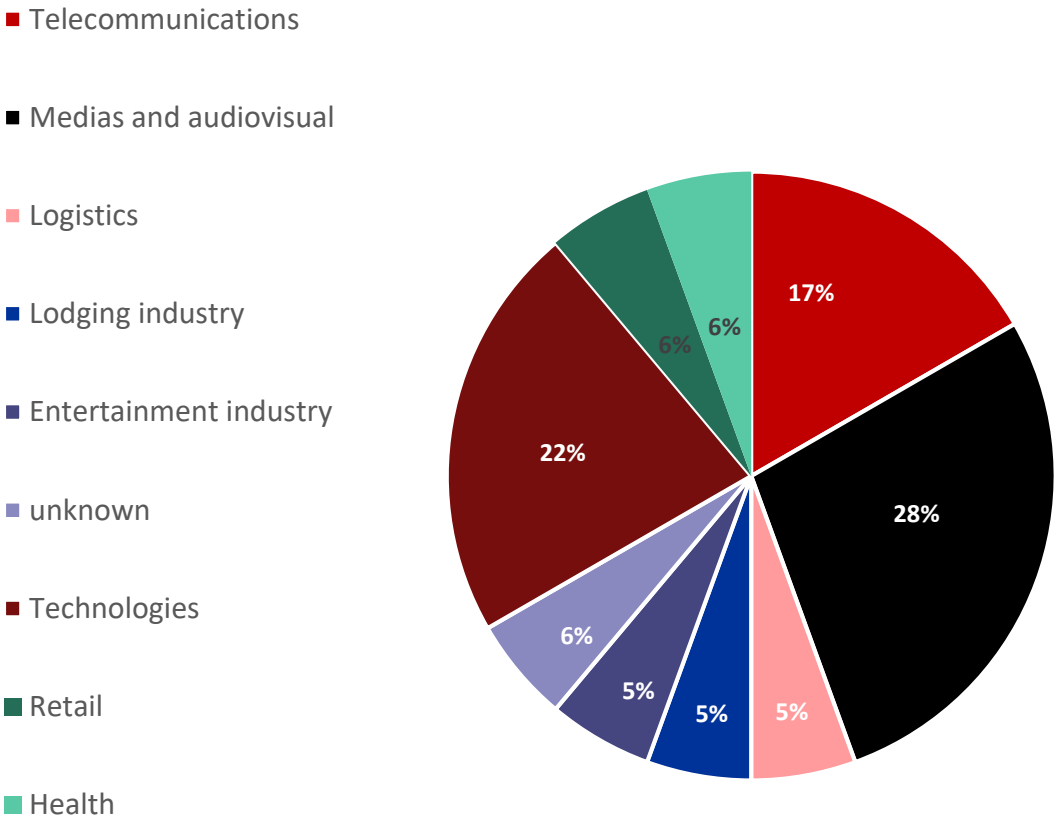
Analysis of “LAPSUS$” intrusion set

TLP:WHITE

Targeted sectors

- Telecommunications
- Medias and audiovisual
- Entertainment industry
- Technologies
- Health
- Unknown (victims in Nepal)
- RetailManufacturing

LAPSUS$ intrusion set preferred sectors include government entities as well as private companies, mainly in the media and telecommunications sectors. It is probable that Telecommunication conglomerates were at first most targeted because of pre-LAPSUS$ member activities being specialized in SIM swap attacks and largely employed against this sector.



INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

TLP:WHITE

Targeted geographical area

- Brazil (6)
- Portugal (5)
- United States of America (4)
- Nepal (unknown; set to 1 but most likely more victims were hit)
- Argentine (1)
- France (1)
- Republic of Korea (1)

In its infancy, LAPSUS$ intrusion set activity targeted mainly Portuguese-speaking entities (Brazil, Portugal). The latter also compromised victims in Nepal and then also in Argentina, United States of America, France and South republic of Korea.

The analysis reporting attacks in Nepal did not provide any information on the sectors, number of victims or a timeframe; the LAPSUS$ intrusion set did not mention Nepalese victims to the best of our knowledge. Only one member of the LAPSUS$’ Chat has made a request for an attack in Nepal to this group. It might be worth mentioning however that the Nepalese community in Portugal is relatively important. It is the result of legal immigration as well as smuggling (as documented by UNODC).

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

TLP:WHITE

Primary motivation

- Financial gain

Objective

- Monetization
- Destabilization

Intrusion sets suspected

- Lapsus$
- Recursion Team (some members of LAPSUS$ could have been part of this Team)
- Cyber Team (some members of LAPSUS$ could have been part of this Team)

Technical details

Motivations

We must first emphasize that the LAPSUS$ intrusion set is likely composite and formed by diverse threat actors with various skills and potentially motivations, from which can stem internal tensions that we already witnessed on their Telegram chat.

- The primary motivation would be **financial** as indicated by their modus operandi, which **favours simple extortion without data encryption**, **targeting** the most **confidential** and **valuable data.** This intrusion set might have already harvested a relatively high amount of money (750,000 $ in one year). One member of LAPSUS$ called “White”, could have personally gained of about 14m$ via sim swap attacks that he seems having spent almost entirely in gambling (cross checked with two sources whom have been close enough to the threat actor assessed to a moderate reliability).

We assess the **level of reliability** according to the STIX format at **Good** (Low, Moderate, **Good** and Strong).

Technical details

Motivations

- Another motivation of one or more members of the group falls at the first glance into the scope of **hacktivism** based on:
  - A **semantic analysis of the public conversation of the *LAPSUS$* Chat group focused on members alleged to be part or close enough to the group**. It allows us to draw up their ideological profile, which is radically opposed to the current power in Brazil and in particular the health policies applied upon the covid-19 crisis. The topics and content of messages resonate with the **presidential campaign of October 2022, which will take place in Brazil in October**
  - The search for notoriety/peer **recognition** with the aim of **demonstrating control of the site and making it known**. This statement relies on their presence on Zone-h (an archive of **defaced websites used by hacktivists**), and the use of more radiating communication channels **such as Telegram, Reddit or to a less extent Twitter** (use only to monitor their public audience and hijack accounts of victims) than encrypted onion ones only accessible via TOR
  - After the NVIDIA hack was discussed the possibility to **open the code of firmware to turn it open source**, a common driver for hacktivists. The fact that **only big private corporations were targeted** and **several public ministries** of Brazil (see victimology)
  - Lots of PII affecting Brazilian family members can be found within the leaked database of Doxbin, which were temporarily administrated by White (key member of LAPSUS$)
  - See sophistication level section in which we assess it to a practitioner level

Overall, some or all members of LAPSUS$ intrusion set could have or still embrace hacktivism at some point. However, we conjecture that this posture could either serve their need of notoriety and/or turn the screws on the victims by leveraging social networks, and in fine, mainstream media as an echo chamber more than being driven by a genuine political ideology. This is based on the fact that so far, LAPSUS$ only shared only a tiny fraction of the claimed stolen volume of data with its community.

We assess the **level of reliability** according to the STIX format at **Moderate** (Low, **Moderate**, Good and Strong)

N.B. Looking at the levels of reliability of the motivations, it is possible that they will be reversed in the light of new knowledge about this MOA.

Technical details

Sophistication

- Though very impacting, **the level of sophistication of the LAPSUS$ intrusion set** in terms of entry vector and modus operandi falls in the range of **intermediate capabilities** (or practitioner).

We assess the **level of sophistication** according to the STIX format at **practitioner** (Aspirant, Novice, **practitioner**, expert, and innovator)

Aims/Objectives

Demonstrate a takeover of the site and make it known with different objectives. We observe two main objectives which are **destabilisation** and **monetisation** of attacks:

- **Destabilisation** is achieved either by **damaging the image and/or stopping services** temporarily by **DNS spoofing** or by **deleting essential data** for the continuity of the service or reselling it to third parties. The main communication channels of the victim such as Twitter accounts could be hijacked upon an attack
- **According to one of the LAPSUS$’ member, the intrusion set focuses on simple extortion without encryption of data**, **targeting** the most **confidential** and **valuable data**. They describe this method as **more effective** than **using traditional ransomware**, with **less disruption to paying customers**. If the victim does **not pay** then they either **delete the data** or **arrange for it to be leaked to buyers' networks**

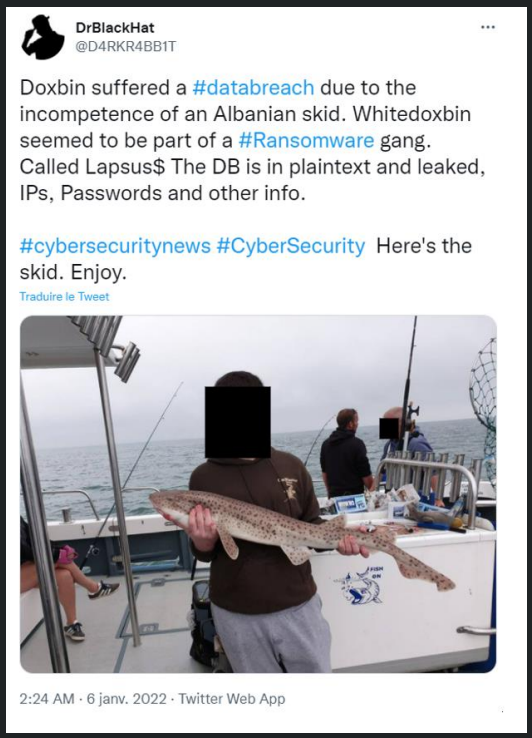
Regarding the link sometimes established in the cybersec community between LAPSUS$ and a ransomware brand (LAPSUS$ Ransomware) **we assess with good reliability that this link is misled**. Indeed, two pieces of information cross-referenced from both a private message between @smelly (vx-underground) and a message from an administrator of the Telegram group "LAPSUS$ chat" indicate that **this intrusion set has used ransomware in the past only**.

However, to our knowledge this does **not** seem to have been the case so far **since they caught the malicious activity as LAPSUS$** (the only doubt remaining though is upon the Brazilian MoH hack). Moreover, neither information is given on the level of sophistication of the ransomware that some of the group members may have employed in the past nor whether the source code is open or closed. We might have indications that a variant of the open-source Babuk ransomware could have been employed but this information requires more investigations (see attribution/genealogy).

Technical details

Identities tied to LAPSUS$

- After a search on Twitter around the term “LAPSUS$” more than two month ago, we detected that the user "@D4RKR4BB1T" published personal data about a young individual whom he explicitly identified as a member of the LAPSUS$ group, associated with the username "Whitedoxbin". The user @D4RKR4BB1T introduce himself as a former blackhat who is now serving the ‘good’ as a whitehat.
- A google dork search on the username "whitedoxbin" brought us to the Telegram channel of the user @whitedoxbin whose two shared photos are similar to those posted by "@D4RKR4BB1T" on Twitter. A link to a doxing operation (disclosure of data of a physical person with the aim of harming him or her) was published on 19 January 2022 on this Telegram channel, which links to the site *doxbin[.]com.* This individual is the latest person who have been publicly ashamed on the degrading *'Wall of Autism'* accessible on this website, amongst others.



- Flashpoint and Cyble have already analysed in great detail a recent massive data leak from the *doxbin[.]com* site exposing authentication and personal data of over 40,000 users. This dataleak may have fed and triggered this doxing operation. Indeed, the passwords of the administrator of the Doxbin site were spotted in this database. This would have allowed the former owner of the site to take control of the Twitter account @doxbin_org and various accounts and email addresses associated with "white" and "doxbinwhite".

```
('doxbinwhite', 'Crack[redacted]'),
('white', 'Crack[redacted]'),
```

- The motivations behind this doxing operations are unclear. Alexander was accused by users to destroy the reputation of Doxbin and break handful features.
  - It should be noted that these operations are common in the threat landscape between individuals following internal disputes about their malware, but also to extort the administrators of cybercriminal forums, particularly the most influential ones.

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

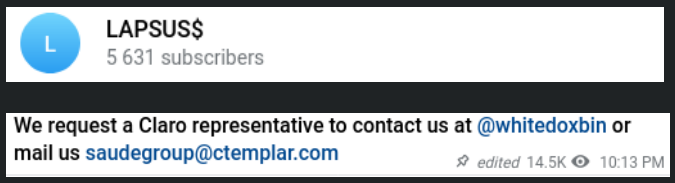
TLP:WHITE

Technical details

Identities tied to LAPSUS$

- The user White purchased the doxbin forum in 2020. He allegedly changed the administration email address `doxbinwhite@protonmail.com`. Then, the user allegedly made some bad decisions according to the site's users and tried to launch a doxing operation on the site's former owner, after the latter had bought it, via a publication on Twitter. As a revenge, the latter allegedly took control of the Twitter account doxbin_org (which has since been suspended) and doxed the "white" user, who is said to be A**** K***** aka Breachbase, and who is said to be *"leading a budding ransomware group"* called LAPSUS$.

- This dox, published on 8 January 2022, tells that A**** K****, aka *White*, aka breachbase, has allegedly accumulated around 300 BTC for various hacks (nearly 14 million USD), and is part of the LAPSUS$ group, either as an operator or an affiliate. The publication exposes several pieces of evidence identifying A**** K**** and his relatives. Of particular interest are his likely links to LAPSUS$. A message on the LAPSUS$ Telegram channel published on 30 December 2021 mentions the channel whitedoxbin for contact.



INTRUSION SET ANALYSIS

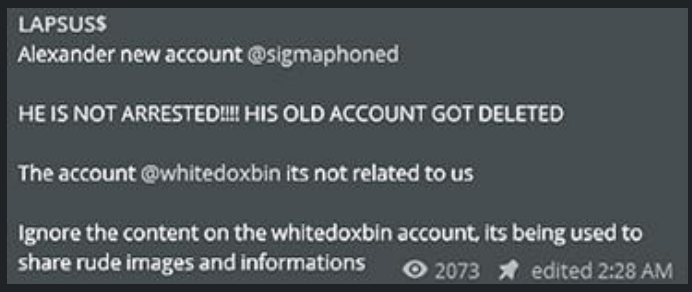
Analysis of “LAPSUS$” intrusion set

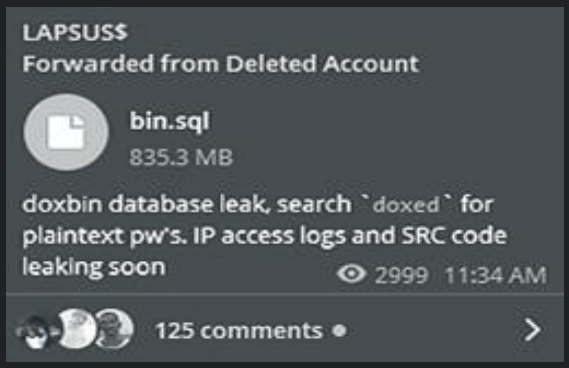
TLP:WHITE

Technical details

Identities tied to LAPSUS$

- On 6 January, a Telegram group admin of the LAPSUS$ group posted a message stating that Alexander; he no longer has his account and that he has a new account named **@sigmaphoned**. The message also states that @whitedoxbin is not connected to the LAPSUS$ group and is being used for a doxing operation.





- The LAPSUS$ group also announced that the doxbin database would soon be made available.
- This database indicates that the user "white" was the owner of the admin address `doxbinwhite@protonmail.com`, with a link in the bio to the Telegram *whitedoxbin* (as a reminder, the name whitedoxbin was put forward by LAPSUS on 30 December 2021).

- Finally, a comment on a Flashpoint twitter post indicating a leak of a doxbin database, mentions a link between white and A**** K****, on 7 January, 12 days before the *doxing operation* was published.

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

TLP:WHITE

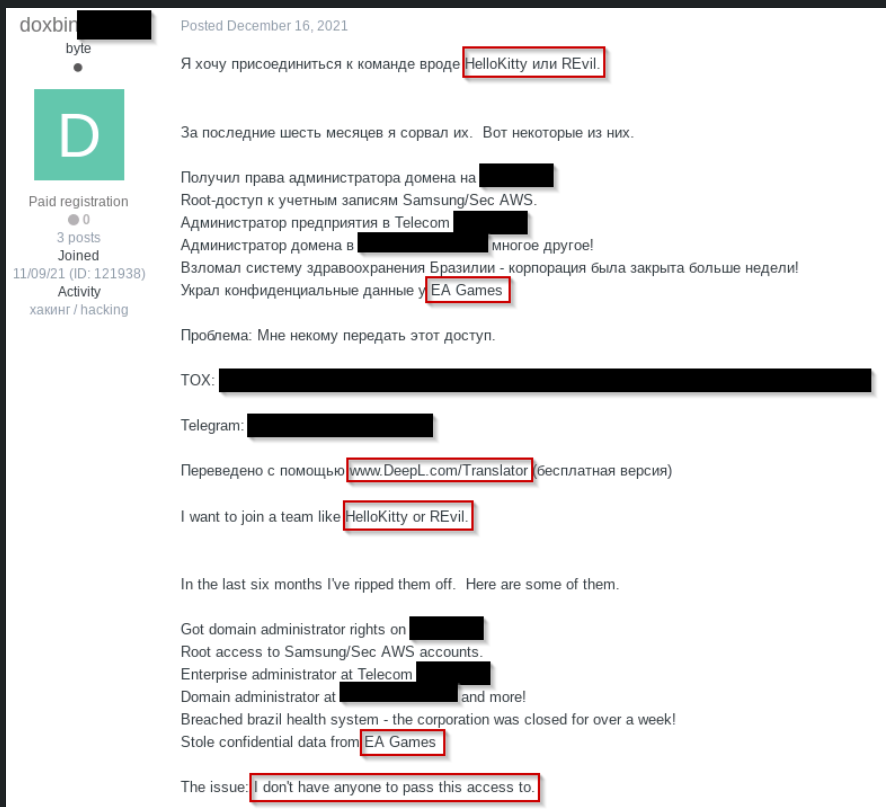
Technical details

Attribution/Genealogy (LAPSUS$)

The rise of LAPSUS$ took officially place with the hack of the Brazilian Ministry of Health (MoH) the 10th of December, 2021. The attack was focused on the healthcare declaration for travellers seeking to enter into Brazil via airports. The context around the attack is important here as it occurred near after the Anvisa (Agência Nacional de Vigilância Sanitária) decided to cancel the World Cup qualifier match between Brazil and Argentina as several Argentinian players were accused of breaking COVID-19 travel protocols.

Actually, we found that the intrusion set also hacked Electronic Arts about 6 month before the rise of LAPSUS$ (see the figure below). Indeed, one of the main actors of Lapsus$ known as White who could be a 16 year old boy living in UK, claimed it on the cybercriminal forum Exploit the 16th of December 2021 (under the alias of doxbinwh1ite). The latter has joined the forum the 9th of November 2021 and participated rapidly after to an auction to acquire initial access both to a Citrix VPN solution of a Brazilian company in the electric power sector and to a client Remote Desktop web Admin Local of an Italian company. *Doxbinwh1ite* shown also interest into getting an exploitation code to leverage the Palo Alto CVE-2021-3064 as an entry vector.

*One of the main threat actor of LAPSUS$ intrusion set sought partners in crime such as **REvil** or **HelloKitty***



doxbin[redacted]
byte

D

Paid registration
0
3 posts
Joined
11/09/21 (ID: 121938)
Activity
хакинг / hacking

Posted December 16, 2021

Я хочу присоединиться к команде вроде HelloKitty или REvil.

За последние шесть месяцев я сорвал их. Вот некоторые из них.

Получил права администратора домена на [redacted]
Root-доступ к учетным записям Samsung/Sec AWS.
Администратор предприятия в Telecom [redacted]
Администратор домена в [redacted] многое другое!
Взломал систему здравоохранения Бразилии - корпорация была закрыта больше недели!
Украл конфиденциальные данные у EA Games

Проблема: Мне некому передать этот доступ.

TOX: [redacted]

Telegram: [redacted]

Переведено с помощью www.DeepL.com/Translator (бесплатная версия)

I want to join a team like HelloKitty or REvil.

In the last six months I've ripped them off. Here are some of them.

Got domain administrator rights on [redacted]
Root access to Samsung/Sec AWS accounts.
Enterprise administrator at Telecom [redacted]
Domain administrator at [redacted] and more!
Breached brazil health system - the corporation was closed for over a week!
Stole confidential data from EA Games

The issue: I don't have anyone to pass this access to.

Technical details

Attribution/Genealogy (LAPSUS$)

The user White claimed that he hacked targets such as Electronic Arts (this one was not claimed publicly), the MoH of Brazil and Samsung. Two other potential targets in the Telecom sector are listed and are geolocated in Argentina and Portugal (we alerted both of them).

We then investigated around the EA hack by pivoting via the Monero wallet ID left in the ransom note. We have indications that the ransom note and the Monero wallet supported a surge of scam text attacks that encompasses EA that was investigated by EE enterprise in the UK. This wave of attack occurred between the 1st of August (at least see here) and September with a common ransom note and all pointing the same XMR wallet being claimed by LAPSUS$ (see IOCs section).

An interesting aspect was the will of *Doxbinwh1ite* to join ransomware-as-a-service groups such as HelloKitty or REvil, which gives a hint on his primary motivation being hence **financially driven**. The alias Kajit replied to his demand and asked @Quake3 ‘whether or not the kid was ready or not to be introduced’.

‘Kajit’ was the former admin of the RAMP forum and allegedly a former REvil / DarkSide operator. ‘Kajit’ replaced ‘Orange’ while the actual admin is known as ‘Stallman’. Though it is not clear whether or not Kajit, Orange and Stallman are the same person, American blogger Brian Krebs recently unravelled the identity of Orange as being the operator of Babuk. Kajit was accused to be a snitch and was banned from the main cybercrime forums. As a reminder, RAMP first hosted a name-and-shame blog operated by the Babuk ransomware gang and the Payload.bin marketplace of leaked corporate data. Hello Kitty/FiveHands actors, when ransoms were not paid were used to post victim data to the Babuk site (payload.site) or sell it. This could be a link between Kajit and HelloKitty.

N.B: We must emphasize that Doxbinwh1ite seem not to speak Russian as he used deepl to translate his message in English (though it could be a trick to blur the lines but we think is not likely).

Technical details

Attribution/Genealogy (Cyberteam)

Knowing that White sought to team up with privateers, we discuss the possibility of having known Portuguese-speaking low sophistication groups being part of LAPSUS$. Based on the analysis of TecMundo (one of the most visited tech websites in Brazil), one of such group located in Portugal is dubbed CyberTeam.

Cyberteam was active in between 2015-2020 conducting doxing operations against politicians, DDoS and defacements attacks again public / private entities. Main victims encompass VODAFONE PT, EDP, KPMG (May 2017) and Steam from Valve a month after. They also post-exploited governmental targets around November 2020 (claiming other groups conducted the attacks) leaking the database of the ministry of Justice (TSE) and defaced the Ministry of Health (MoH) that was exposed on the Doxbin website. They also leaked a series of internal information of the court to demonstrate vulnerability into the Superior Electoral Court (TSE), and this, the day of municipal elections throughout Brazil.

On the carder UK, this group appeared on 22 June, 2021 as ‘- Hire Hacker – CyberTeam’ on a website accessible via Tor (now offline). The website offers “hardcore hacking services” such as data mining, hacking e-commerce websites, servers; Identity theft, digital framing of individuals, DDoS, hacking of entire systems, etc.. Prices are listed on the site and to complete orders is required a manual email communication.

Investigations that were conducted by the Federal Police of Portugal (that also conducted searches in Brazil) indicate that Zambrius is one of the leaders of Cyberteam. Zambrius, claimed to have acted alone, without political encouragement or funding. However, as he declares himself against governments, his motivation is likely politically driven.

We and others have shown that White was the ex-administrator of Doxbin and a key member of LAPSUS$ that is a platform also employed by Cyberteam. Moreover, we found mentions of such group in the official TG channel of Lapsus$. Of course this holds only a weak signal, but a link between White and CyberTeam for instance throughout doxbin remains a possibility, which could rationalize the hybrid behaviour of the LAPSUS$ intrusion set in its last form as we see today.

Technical details

Attribution/Genealogy (Recursion Team)

We conjectured previously how Alexander (aka White) could have teamed up with the lusophone group *CyberTeam*. Let’s now now to go back in time a bit more to analyse the past history of Alexander. Recently Unit 221B together with Unit42 Palo Alto identified already the latter in 2021 and have been assisted law enforcement seeking to prosecute this group. They revealed that the TTPs we witnessed upon recent attacks conducted by the LAPSUS$ intrusion set were already at play *“to target employees and contractors working for the major mobile phone companies … involving social engineering techniques* & SIM-Swapping attacks*”.*

Krebs also mentions a key information concerning Alexander as back in May 2021, “*WhiteDoxbin’s Telegram ID was used to create an account on a Telegram-based service for launching distributed denial-of-service (DDoS) attacks*” while the latter acquired the Doxbin Website at about the same time. This information is important as we witnessed recent conversations posted on the Doxbin telegram channel, in which Alexander unveiled his genuine motivation behind such acquisition. Indeed, the latter intended to offer a new generation of DOS stresser for its own profits by leveraging the Doxbin’s traffic website, a market which lacks of competitors and thus promises higher gains.

The 13th of March, 2022, we remarked the creation of a new telegram canal named ‘BOTNET - Lapsus$ crew” (became the 26th of March 2022 only). The latter substantiate our previous hypothesis as it advertise weekly/monthly DOS stressing services (both in English and Chinese). Moreover, the contact person (@Lapsus33) replies in a polished English (as White would do). We think the Chinese language was generated (*e.g.,* via Deepl) to reach Asian clients and/or resellers (hitting gambling websites for ransoms for instance). We’ve seen @lapsus33 prior advertising its services on the DDoS萌新交流群·二次元黑客集中营 Telegram channel.

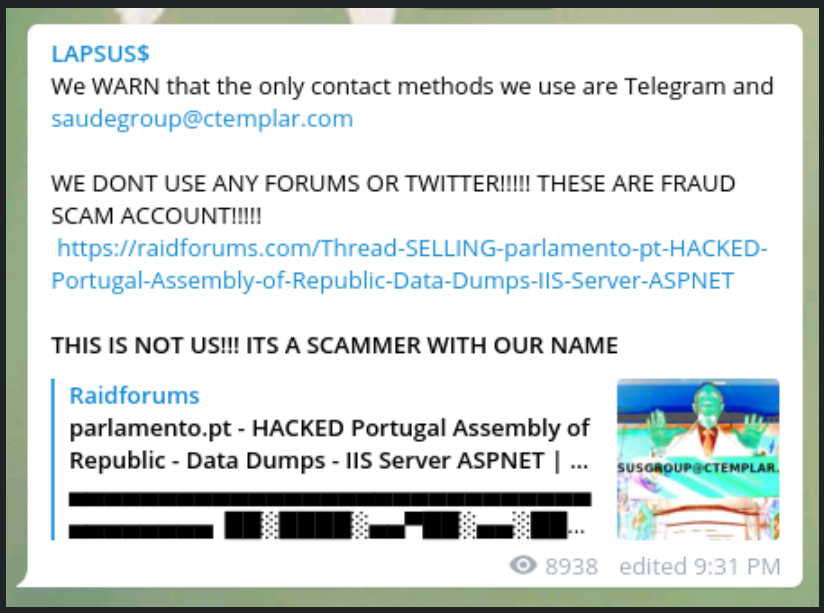
Chief research officer at Unit 221B, Allison Nixon, also confided to B.Krebs that Alexander was a founding member of a cybercriminal group dubbed “Recursion Team.” specialized in targeted SIM swapping [T1451] & swatting attacks. We found that Alexander indeed used the telegram username *pornpeternew* at that time, which was also part of the doxing operation published on the clearweb that unveiled he’s an underage boy living in UK. Recursion team was advertising a variety of services in particular on the cybercriminal forum *cracked.to* under the alias of *InfinityRecursion,* redirecting to DM on the @everlynn_uwu (aka Miku) telegram account who founded the group in 2021. Alexander could be a cofounder of this team.

Technical details

Public communication of the intrusion set LAPSUS$

It should be noted that LAPSUS$ intrusion set’s franchise has been spoofed not only on Twitter but also on the Russian cybercriminal forum RAMP.

The figure below shows a post that was published by one of the admins, which indicates that they only communicate through this channel. The accounts on the Raidforums forum as well as the posts on Twitter and RAMP in their name were thus usurped.



*One of the main threat actor of LAPSUS$ intrusion set sought partners in crime such as **REvil** or **HelloKitty***

As far as Raidforums is concerned, it remains true apart from the extortion attempt against the company Electronic Arts (see victims section). Another channel employed in the early moments of LAPSUS$ since mid-last year is REDDIT, in which the usernames Oklaqq and whitedoxbin posted recruitment messages seeking threat insiders.

Besides, it should ne noted that Oklaqq (aka White) is also active on Russian cybercriminal forums (XSS, Exploit) but is considered to communicate for himself and not on behalf of LAPSUS$.

INTRUSION SET ANALYSIS

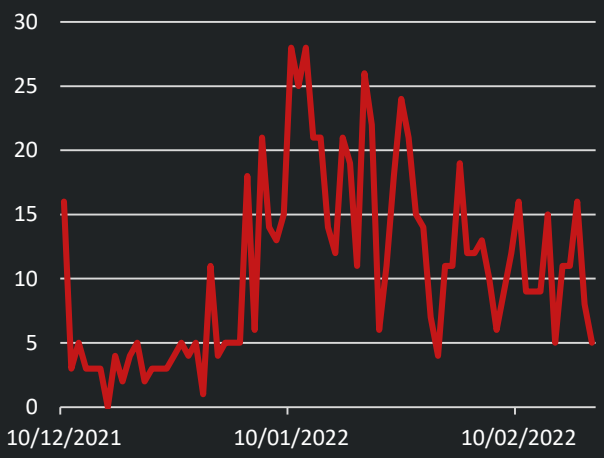
Analysis of “LAPSUS$” intrusion set

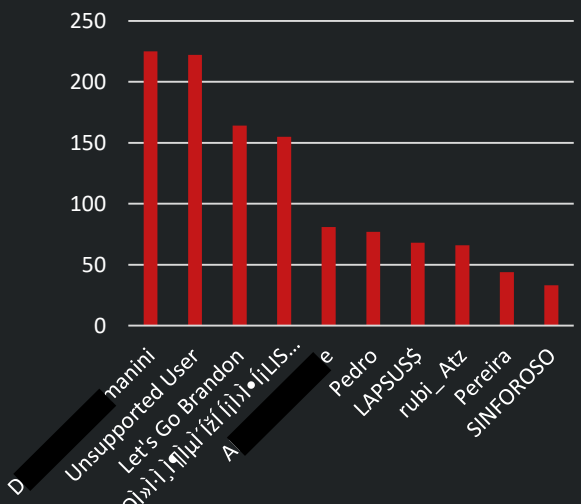
TLP:WHITE

Technical details

Analysis of the “LAPSUS$ Chat” Telegram channel

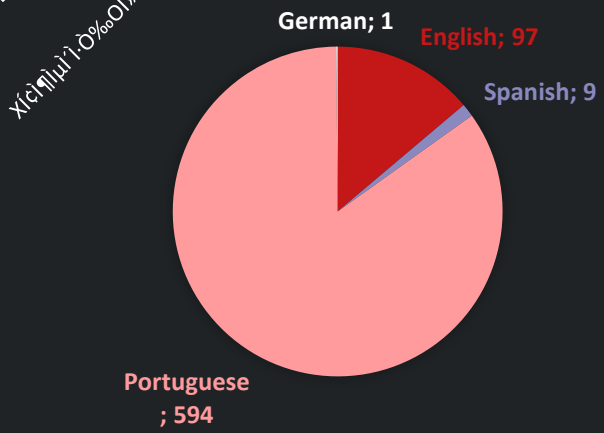
Earlier this year, we engaged an analysis of the telegram channel @saudechat, which was created and advertised by LAPSUS$. First, we share an analysis of the number of active users per day (using the number of users that posted a message in the group each day). The first histogram reveals that a reached an all-time high between the beginning of January and mid-February. Since then, the number of active users has slowly decreased. This shows that this chat was more active when the group LAPSUS made the headline, starting in January with the doxing operation affecting a member of the group, followed by the Vodafone attack.





Left: Number of active users per day. Please note that we stopped the analysis around mid-February 2022. Right: Top 10 of posts per user

The figure on the right inside unveils the most active users on the chat. LAPSUS$ admin(s) is(are) the 7th in number of posts. The most active users have mainly posted messages discussing world event, unrelated to the various hack advertised by LAPSUS$. However, weak signals let us think that some of them were or are still part of LAPSUS$.



The pie chart demonstrates Portuguese as the main used language (including LAPSUS$ at first), with several hundred posts (594), while English is still used (97) notably by LAPSUS$. Few messages were published in Spanish and one message was published in German.

Technical details

Infrastructure

The intrusion set infrastructure analysis started with the IoCs present on the Vairav blog. Of particular interest is the IP address *185.56.83[.]40* which resolves a domain name related to the intrusion set Lapsus$, accessible via the domain name *lapsus-group[.]com*. The server would be **geolocated in Switzerland** since March 1, 2021, however the coordinates of the **Whois database refer to the Seychelles (AS211720)**.

An SSL certificate have been linked to this IP address through the free and automated certification authority *Let's encrypt* since December 10, 2022. However, no other domains could be gathered via an SSL pivot.

From the **contact email to report any abuse or complaint** (abuse@xor.sc), we find the terms of service on the website xor[.]sc which can **provide "bulletproof" infrastructure** either dedicated [1583.004] or virtualized [1583.003] with various specifications depending on the price per month and which are **located in Switzerland**. **VPN services are allowed, disk encryption and anti-DDoS protection is offered**. According to Microsoft, NordVPN is used.

As far as we know this website didn't help to expose victim’s data and only exposed their motivations in the wake of the Ministry of Health hack and since then a default page proving the presence of a Windows server (Microsoft-IIS) around January 7, 2022 that his is corroborated by the Shodan network logs:

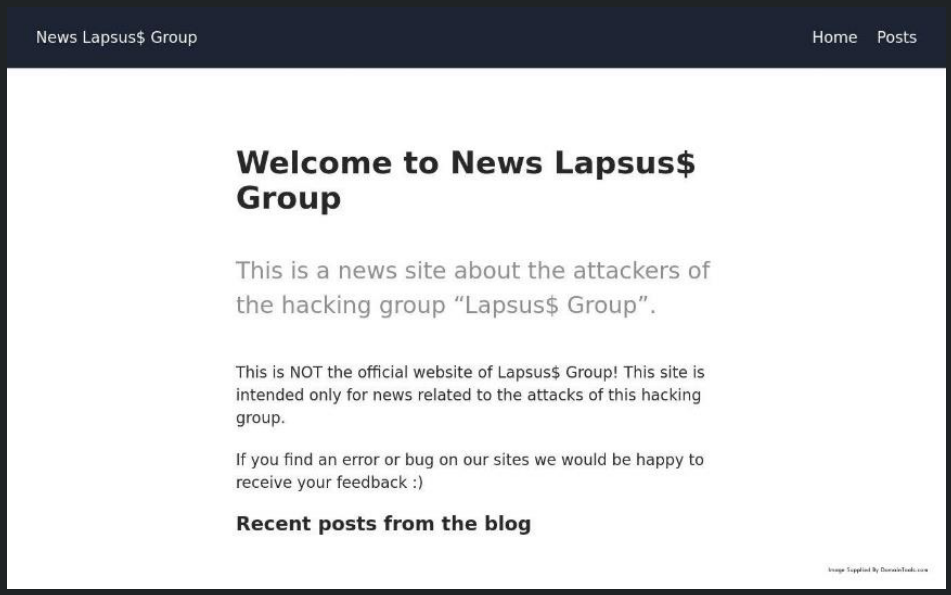
- OS: Windows 10/Windows Server 2019
- Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.4.24
- Server: Microsoft-HTTPAPI/2.0
- Server: **Microsoft-IIS/10**.0)
- First activity date: 2021-08-22T23:24:23.934975
- Last activity date: 2022-02-13T09:45:37.255408

Note that **the IP address range is the subject of a large number of abuse reports** including reported as **C2 METASPLOIT** from October 2021, **attempts to exploit the Proxyshell flaw** in June 2021, **Log4J, RDP Brute force**. Note that we confirm the **likely use of the METASPLOIT framework** at more recent dates spanning beyond the Vodafone’s attack. Indeed, we identified the use of the **default TCP 3790 SSL port** chosen **upon an installation of the Metasploit framework** in the **Shodan logs** that is time-stamped on **2022-02-12**T06:51:52.567592.

Technical details

Infrastructure

Another domain tight to LAPSUS$ was found from a screenshot we gathered via domaintools (see the figure below). The website, which was active till the 9th of January 2022, intended to exhibit news related to the LAPSUS$ group (most likely a mirror of their Telegram channel).



Screenshot of the News LAPSUS$ group website. Was active till 09-01-2022. The Cloudfare hosting was removed the 11th of March 2022.

This project seem to have been abandoned by the intrusion set LAPSUS$. As this website was not claimed by the latter on their official telegram group, though not probable, we can’t elude the fact that their brand was intended to be usurped by another threat actor.

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

TLP:WHITE

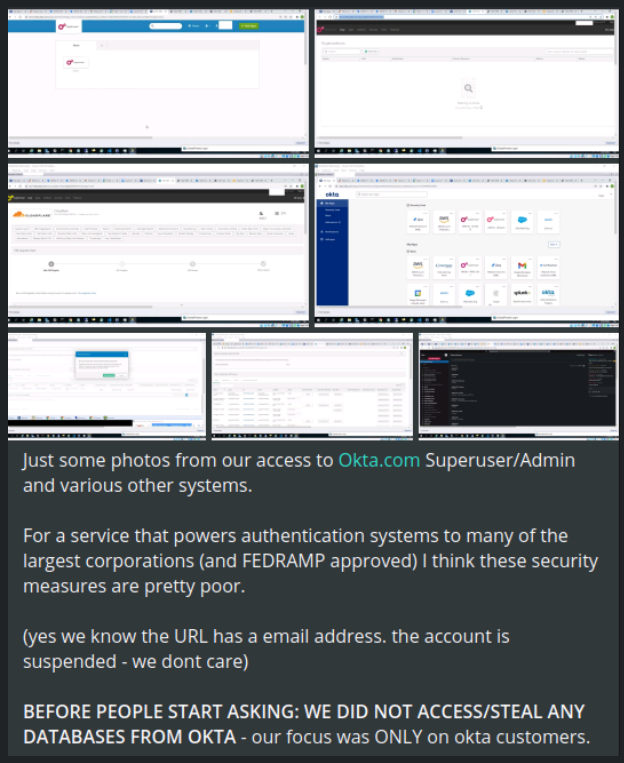
Technical details

Highlighted Campaign: OKTA

LAPSUS$’ last victim claimed on their official Telegram channel turns out to be Okta. Several proofs are attached to the post (see the figure on the right). From a first analysis we assess with high reliability that the intrusion set indeed had privileged rights on the network of Okta. Between January 16 and 21, LAPSUS$ obtained Remote Desktop access to an actual OKTA sub processor employee’s laptop.

Okta was aware of the incident and announced that they *detected on January 20, 2022, a new factor added to a Sitel customer support engineer’s Okta account*; Sitel is an Okta sub-processor outsourced to expand workforces.

In their last update Okta added *We have determined that the maximum potential impact is 366 (approximately 2.5% of) customers whose Okta tenant was accessed by Sitel.*



Screenshot of the official Telegram channel (Chat group) of the LAPSUS$ intrusion set taken the 22nd of March, 2022.

We believe these information are diminishing the risk level substantially from critical to **moderate**.

We think that the timing chosen by the intrusion set to claim the hack might have been driven either by attempting a publicity stunt to further crank up its notoriety, or to pressurize OKTA to pay a higher ransom.

Another goal of the intrusion set could also be to obtain victims’ customer data for further attacks conducted via social engineering techniques.

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

TLP:WHITE

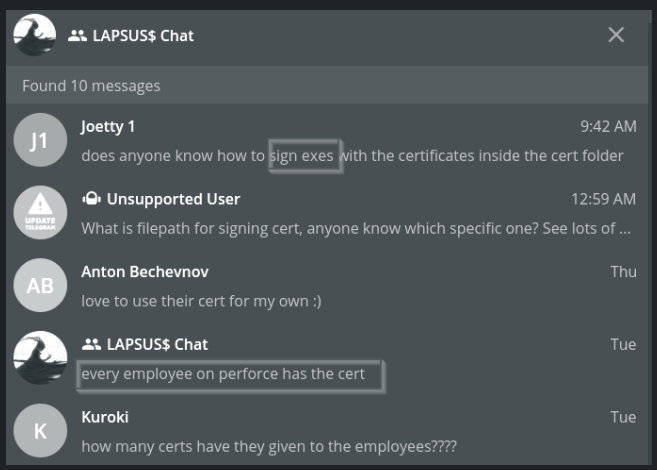
Technical details

Highlighted Campaign: NVIDIA

NVIDIA was targeted by the LAPSUS$ intrusion set around the February 23, 2022. The attack was claimed a couple of days after on their official Telegram channel.
The disclosed information included more than 70,000 employee email addresses, NTLM password hashes (single sign on offered by Microsoft to authenticate users’ identity), and screenshots of source code, many of which were later hacked and distributed within the hacking community.

There’s been a controversy after the hack of NVIDIA about whether or not they launched a retaliatory strike via a ransomware. We assess that **NVIDIA did not hack back LAPSUS$’ intrusion set via a ransomware** but that an automatic data loss prevention might have been at play. Moreover, a few days later, LAPSUS$ deleted the post from their Telegram chat room.

Even worse is the LAPSUS$’ grasp of the NVIDIA code signing certificates that allows to sign malwares and thus evade defenses.
We would like to mention though, that the stolen code signing certificates from NVIDIA were not necessarily weaponized by the LAPSUS$ intrusion set; it could also be independently leveraged by its community (see the figure on the right) and/or other threat actors.
Another important point to underline is that although the certificates are expired now, Microsoft makes by design an exception for signed drivers. As a result this opens a path to malicious drivers to appear trustworthy and to be loaded into Windows. Windows Defender Application Control (WDAC) policies are recommended to be set as stated by Microsoft. One can “create a policy with the Wizard and then add a deny rule or allow specific versions of Nvidia”



Screenshot of the official Telegram channel (Chat group) of the LAPSUS$ intrusion set taken the 04/03/22.

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

TLP:WHITE

Technical details

Highlighted Campaign: Vodafone

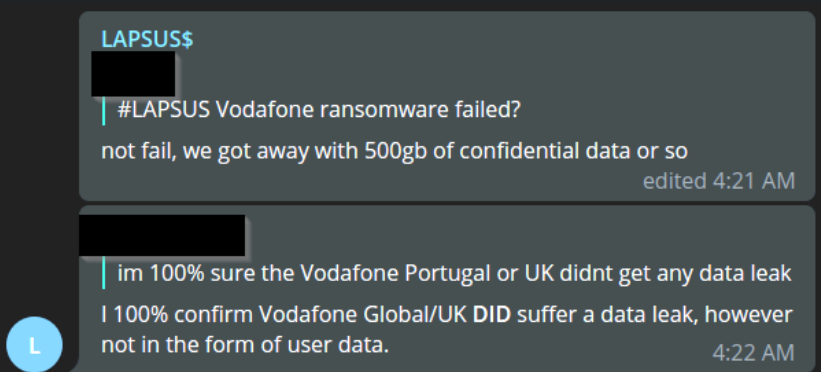
Chronology

- **February 7-8, 2022**: The Portuguese subsidiary of the British mobile operator Vodafone suffered an attack interrupting part of its services (4G/5G networks, users' fixed lines, TV and SMS services), announced in a statement. The attack impacted millions of users and cut off essential services
- **February 11, 2022**: Service disruptions following the cyber-attack are resolved

Attribution

Semantic analysis of the Lapsus$ group's Telegram chat, presented as their only communication tool, reveals **the mention of Vodafone's name as early as in February 9, 2022**. The administrators of this Telegram channel then clarified that they **were neither confirming nor denying the hypothesis** that they were behind the attack.

One of the administrators, **however, claimed later responsibility for the attack on February 11 in their second Telegram channel** dedicated for open discussions with peers (thousands of users have already joined the channel). One admin claims that **Lapsus$ would have conducted successfully the exfiltration of over 500GB of data that would not be PII (stolen data could be internal source code)**.



Screenshot of the official Telegram channel (Chat group) of the LAPSUS$ intrusion set taken the 11th of February 2022.

We attribute the attack against the Portuguese subsidiary of Vodafone to the Lapsus$ intrusion set (with high confidence). The latter indeed claimed the attack in a conversation we discovered on their official chat on Telegram.

TTP Highlight

Initial Access TA0001

- **Threat insider TTPs**
  - Note that LAPSUS$ group could use the tactic of "recruiting moles" to infiltrate the digital infrastructure of the victim organisation. Before Claro was attacked, Lapsus$ offered bounties to threat insiders for privileged access (BRL 50000$ +/week for access to Claro or Vivo). This were publicly disclosed more recently on the official post on telegram of Lapsus$.
  - Amongst all techniques that could or would take place once a threat insider is involved in the attack chain, the one more likely used is called ‘sim swapping attack’. Besides the official announcement of Lapsus$ that could as well be a lure, this technique was reported at least in the Vodafone’s attack, where the intrusion set would have obtained the employee's credentials with a cloned mobile phone card, thus bypassing the two-step verification. However, it is not yet clear whether the bypass of MFA was facilitated by a threat insider or via a malicious spear phishing email sent to an employee. In the case where the MFA is linked to the SIM card and not the device itself, it could be bypassed without the interaction of the phone’s owner.

- **Vulnerabilities**
  - This group makes extensive use of the [T1190] technique as a tactic to gain initial access to the target network (TA00001), *i.e.* exploiting vulnerabilities in front-end servers or network services on the Internet. Among the vulnerabilities already exploited we can note:
    - Microsoft Exchange Server
    - FortiGate Firewall
    - Public AWS infrastructure
  - Potential usage of CVE-2021-34484, a Windows User Profile Service Elevation of Privilege Vulnerability downloaded from Github as a pre-built version
  - Once a foothold is gained on the victim’s network the latter exploited unpatched CVEs on internally accessible servers such as:
    - Confluence
    - JIRA
    - Gitlab for privilege escalation

- Malicious spam email (sent by another intrusion set, *i.e.*, not necessarily LAPSUS$)
  - InfoStealer malware (*c.g.*, Redline Stealer, Raccoon Stealer, AZORult, or Vidar Stealer)
  - Exfiltrate web browser credentials are resold on infamous cybercriminal underground marketplaces (Genesis, BHF, Russian Market, etc)
  - LAPSUS$ Intrusion Set bought such cookies and abused IT helpdesk with social engineering techniques (N.B: this technique was used at least for the EA hack and reported by Microsoft)

TTP Highlight

Threat insider TTPs

Malware(s)

No malware have been firmly associated to the LAPSUS$ intrusion set, to our knowledge.

- We found that METASPLOIT framework is present on the intrusion set infrastructure. Although it is not clear, at this stage of the analysis, which modules of METASPLOIT were used in the attack campaigns, the **TTPs associated with the numerous modules** have been recently published on the praetorian's Github.
- Microsoft reported on the usage of DCSync attacks [T1003.006] via Mimikatz [S0002] to perform privilege escalation routines (Mimikatz embarks DCSync functionality included in its ‘lsadump’ module). Could be downloaded by LAPSUS$ directly from Github.
- Please note that numerous signed malwares with the leaked NVIDIA certificates have been observed in the wild in the wake of the hack. Although these are not (yet) linked, to the best of our knowledge and at the time of writing to this intrusion set, please find here IOCs and a YARA detection rule for real time monitoring and/or threat hunting purposes.

Tool(s)

- [T1087.001] Active Directory explorer tool (a publicly available tool to collect information on users & groups)
- Ntdutil (a LOLBAS to extract the AD database)
- Process Hacker (downloaded from github)

Further discovery

- Once on the victim’s network the intrusion set seeks collaborative platforms to discover further high-privilege account credentials and gain other sensitive information:
  - SharePoint
  - Confluence
  - Issue-tracking solutions (*e.g*, JIRA)
  - Code repositories (*e.g*, Github or Gitlab)
  - Organization collaboration channels (*e.g*, Teams or Slack)

INTRUSION SET ANALYSIS

Analysis of “LAPSUS$” intrusion set

TLP:WHITE

Tactics, Techniques & Procedures (MITRE ATT&CK)

- Tactics, Techniques and Procedures (TTPs) observed to date for the LAPSUS$ intrusion set were made available on our public GitHub repository
- The TTPs conform to the MITRE ATT&CK framework
- The JSON file format compatible with the MITRE ATT&CK Navigator highlights shared Tactics, Techniques and Procedures (TTPs) according to the MITRE ATT&CK framework
- Please note that we only shared vetted TTPs with TLP:WHITE; but we collected more TTPs with TLP:AMBER or RED, which were shared with our clients and trusted circles

Indicators of compromise

- Indicators of compromise were made available on our public GitHub repository
- Please note that we only shared vetted IOCs with TLP:WHITE; but we collected more IOCs with TLP:AMBER or RED, which were shared with our clients and trusted circles
- Please note that if you are an Intrinsec SOC (Security Operation Center) customer, the IOCs related to this campaign are being integrated into our MISP

INTRINSEC ADVICE

OKTA's client security posture

- Collect and retain all Okta System logs
- Rotate Okta privileged passwords
- Check the creation of privileged accounts as of December 2021
- If you are a client of Okta and they have not reached out to you, you are probably not concerned by the exposure of PII
- Please follow the next recommendations based on what we know of this intrusion set

To avoid DNS attacks (follow ANSSI recommendations)

- Deploy a managed DNS solution such as Infoblox and get logs monitored by a SOC
- Renewing authentication elements
- Use the Registry Lock
  - Can be activated at any time and freezes WHOIS information
- Choose a registrar with strong authentication
- Use a registrar-level lock
- Choose a registrar that supports DNSSEC
- Search the relevant domains in the public transparency journals
- Check the current integrity of the zones
- Check mail relay logs to identify any traffic diversion

To prevent Threat Insiders

See most commonly encountered TTPs associated with threat insiders drifting away from the "did" category of TTPs into "would". Corresponding proposed mitigations by the MITRE ATT&CK framework should be assessed by defenders.

In case of big companies present in several countries, consider focusing efforts on your entities based in countries where you qualify a higher risk of corruption.

INTRINSEC ADVICE

To prevent the takeover of an asset

- Raise awareness among your staff (IT and engineering teams on site as a priority) and educate them regularly about the risks of phishing and especially to detect lured pushed notifications for MFA [M1017].
- Follow the ANSSI IT security guide https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
- Regularly review and list your system assets
- Implement a patch management strategy
- Create or implement a recovery plan to maintain business continuity in the event of a cyber attack
- Implement an AppLocker policy in whitelist mode for critical items
- Implement a process for managing information system vulnerabilities
- Cookie-stealing malware incidents should be tackled seriously. Accounts should be reset and browser caches should also be cleared
- Consider a proactive employee credential assessment (logs, session cookies, login/pass etc.) on prioritized Dark web forums by CTI teams to mitigate the risk of account takeover

Resilience

- Implementing a backup management strategy
- Plan regular audits and penetration tests at different sites, as well as an annual Red Team exercise
- Create or update a disaster recovery plan to maintain business operations in the event of a cyber attack.
- Implement a 3-tier Active Directory administration model that allows for the segmentation of domain account roles and activities. This architecture isolates and secures important resources from high-risk components (e.g. workstations) against cyber-attacks

INTRINSEC ADVICE

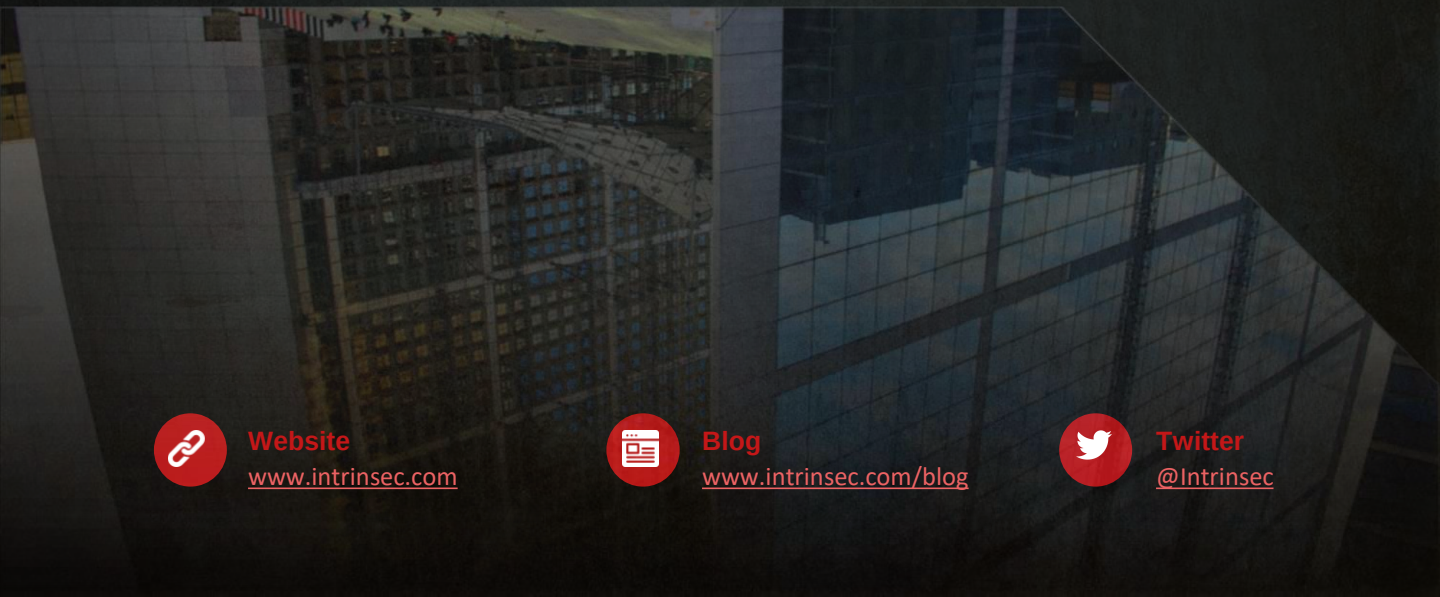
Detection and Protection

- Defend the perimeter:
  - Analysis of email attachments with sandbox detonation
  - URL analysis with dynamic filtering and sandbox detonation
  - Setting up filtering for equipment with and without VPN (*SaaS proxy* solution recommended)
  - Strengthen the filtering of outgoing flows (especially browsing), in order to detect access to C&C and illegitimate traffic peaks (information leaks)
- Maintain an up-to-date inventory of assets, and perform network/system scans on a regular basis
- Migrate obsolete systems to Microsoft-supported versions of Windows that take advantage of the latest security advances, such as CredentialGuard
- Deploy an endpoint detection and response (EDR) solution on the network
  - Disabling of your EDR without recovery should be investigated immediately
- Carry out regular penetration tests on infrastructure and services exposed to the Internet
  - Take into account the results in the SOC's ISS supervision
- Study and implement a security policy based on the "zero trust" principle, particularly for cloud environments
- Conduct regular ISS crisis management exercises
- By using the latest security advances, such as CredentialGuard

Threat hunting (post-mortem analysis)

- Search into your audit logs for suspicious activity
  - Focus on your superuser/admin Okta accounts as they pose the largest risk
  - For this you can use various existing Sigma Rules to search for specific Okta behaviors

If you have any questions regarding this note, please contact veille-cti@intrinsec.com or your lead analyst directly.



Website
www.intrinsec.com

Blog
www.intrinsec.com/blog

Twitter
@Intrinsec