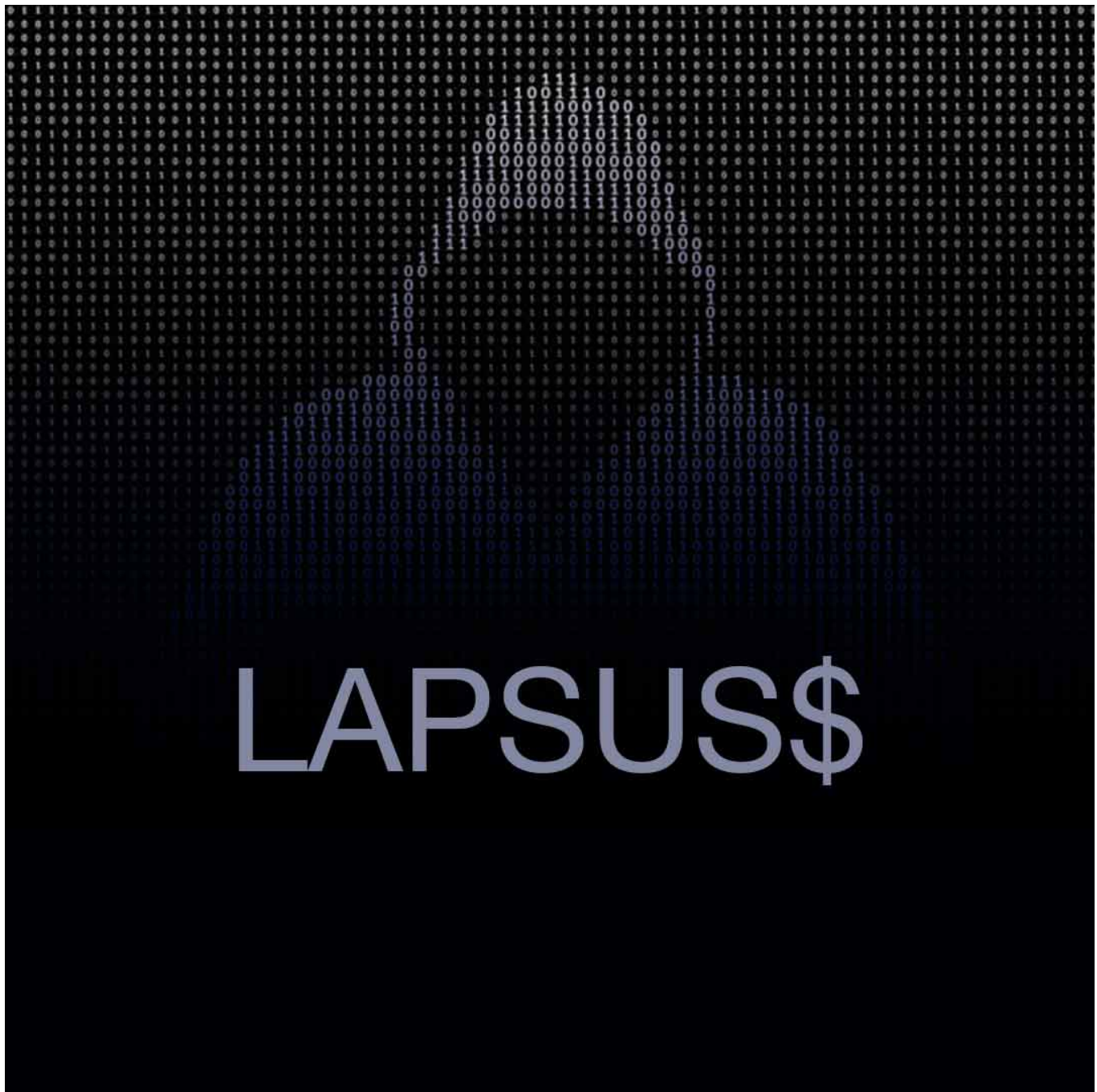


# Detailed Analysis of LAPSUS\$ Cybercriminal Group that has Compromised Nvidia, Microsoft, Okta, and Globant

cloudsek.com/profile-lapsus-cybercriminal-group/

anirudh.batra

April 4, 2022

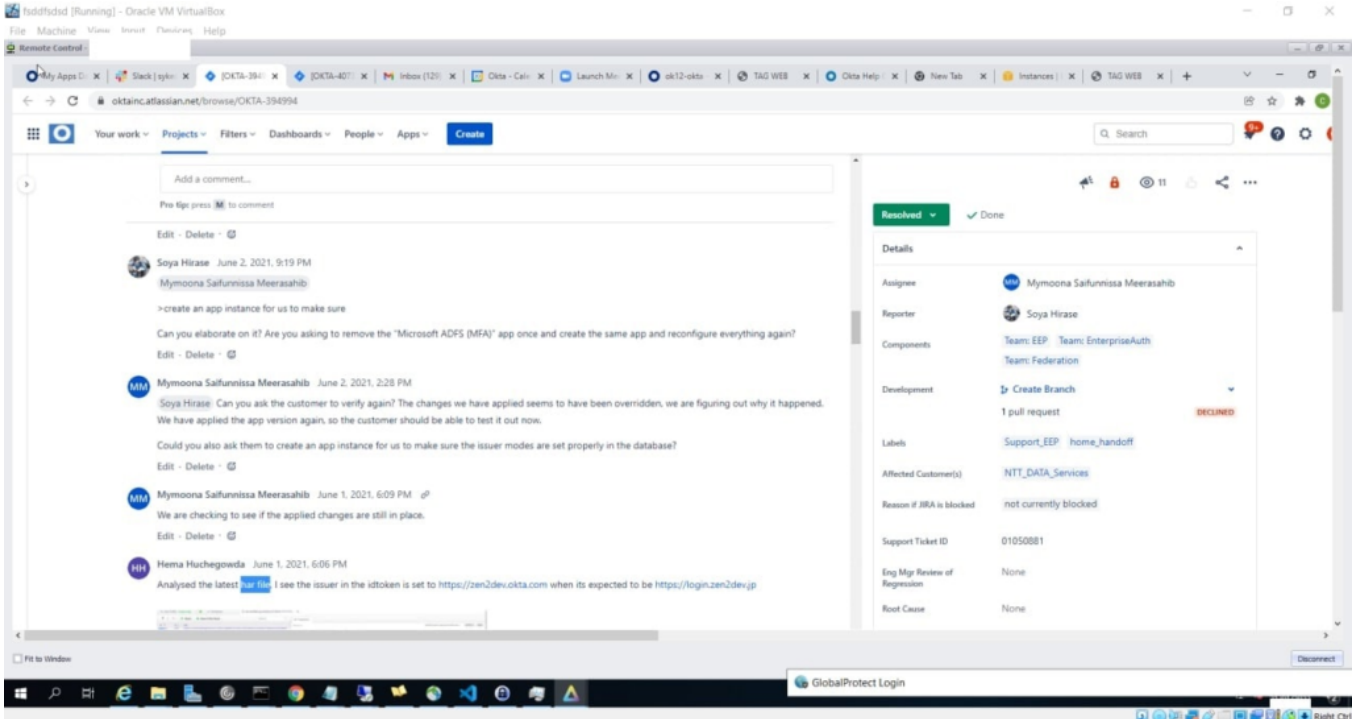


Source: A1 Industry: IT & Technology Region: USA Category: Adversary Intelligence

## Executive Summary

- **Update:** Lapsus\$ ransomware group's recent target is IT and software giant Globant. This article has been updated with the analysis of the attack on Globant, which came to light on 30 March 2022.
- CloudSEK's flagship digital risk monitoring platform *XVigil* discovered a post on Telegram, sharing the Nvidia employee credentials, Samsung's Source code along with that the latest addition to those already high profile targets are Microsoft's Cortana and Bing's Source code and Okta the SSO giant's customer data was exfiltrated.

- Lapsus\$ ransomware gang claimed to have compromised Nvidia and now targets Samsung with the breach. Further claiming to have gained access to source code used in Samsung Galaxy smartphones, Okta's Customer data etc.
- The ransomware gang leaked source code, dehashed credentials, code signing certificates and source code to the driver. The leaked data unlocks the potential for threat actors to gain unauthorized access to personal, proprietary, and Intellectual Property (IP) data of Nvidia and they have also leaked 90% source code of Bing Maps, Bing and Cortana claiming to be at 45%.
- While writing this report, we have discovered that PII (Personally Identifiable Information) or dox Information related to the Lapsus\$ ransomware gang was released at a Russian language cybercrime forum.



This screenshot was posted on the telegram group and while analyzing closely we can see that they have access to Jira, Slack, G-Suite and other internal applications as well. RDP access is being used in the screenshot

## Analysis and Attribution

### Information from the Telegram

On 22nd March, 2022 the group claimed to leak Bing Maps, Bing and Cortana source code. Our threat Intelligence team has confirmed that these claims are true, shortly after there were official blogs from [Microsoft](#) and [Okta](#) confirming the breach.

**LAPSUS\$**

**MS.7z.torrent**  
483.6 KB

Leak of some Bing , Bing Maps and Cortana source code - Bing maps is 90% complete dump. Bing and Cortana around 45%.

**NOTE: IF THE TORRENT FAILS MAKE SURE TO ADD TRACKERS!!!**  
[https://ngosang.github.io/trackerslist/trackers\\_best.txt](https://ngosang.github.io/trackerslist/trackers_best.txt)

Enjoy everyone! 46.7K edited 06:47

240 comments

**LAPSUS\$**

**LGE-Hashes.txt**  
8.3 MB

Dump of all hashes for [LGE.com](#) employee's and service accounts - second time we hacked them in ~1 years.

Dump of LG's infrastructure confluence will be released soon.

Might be a good idea to consider a new CSIRT team!

41K 06:47

81 comments

Leaked Information shared on Telegram Channels

### Original Perpetrators of Breach

The LAPSUS\$ cyber-criminal group has been known to exploit the weakest link in the security chain of a corporate network: **Human mistakes and bad practices.**

They achieve initial access using the following tactics:

- Redline Malware stealer logs, which can be understood [here](#)

- Popular market places like amigoss, russian-market to get logs, credentials and session tokens to get access.
- They are known to pay insiders to provide them with VPN, VDI(citrix), Identity providers and even RDP access

#### LAPSUS\$

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

Lapsus Recruitment Post

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

62.8K edited 02:06



851 comments



Publicly available secrets on github/gitlab repositories

#### The next steps involve Privilege escalation and Post Exploitation:

- Exploiting existing vulnerabilities which include unpatched versions of Jira, confluence, Fortiguard, Microsoft exchange servers etc.. We have created a list of curated vulnerabilities that they target
- Accessing version control systems and looking at private repositories to gain access to secrets and gems
- They also access mailboxes/collaboration software like slack to get access to credentials being shared in plain text.

#### LAPSUS\$

<https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/>

I do enjoy the lies given by Okta.

1. We didn't compromise any laptop? It was a thin client.

2. "Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider." -

They have highlighted the post-exploitation steps they took as a part of the

I'm STILL unsure how its a unsuccessful attempt? Logged in to superuser portal with the ability to reset the Password and MFA of ~95% of clients isn't successful?

4. For a company that supports Zero-Trust. \*Support Engineers\* seem to have excessive access to Slack? 8.6k channels? (You may want to search AKIA\* on your Slack, rather a bad security practice to store AWS keys in Slack channels 😊)

response to Okta's latest blog.

#### Microsoft Leak Analysis:

Microsoft in an official blog today has stated the following:

"This week, the actor made public claims that they had gained access to Microsoft and exfiltrated portions of source code. No customer code or data was involved in the observed activities. Our investigation has found a single account had been compromised, granting limited access. Our cybersecurity response teams quickly engaged to remediate the compromised account and prevent further activity. Microsoft does not rely on the secrecy of code as a security measure and viewing source code does not lead to elevation of risk."

The leak contains **56484 directories**, **333743 files** and the source code for Cortana, Bing Maps and Bing. The aggregate size of the data leaked is 37.8 GB.

```
cat ./Aria.Backend/DataApps/Common/Microsoft.Aria.DataApps.Monitoring/Mds/Certificates/password.txt
All passwords for the certs are stored at
https://microsoft.sharepoint.com/teams/SkypeData/_layouts/15/start.aspx#/Lists/Certificates/AllItems.aspx
```

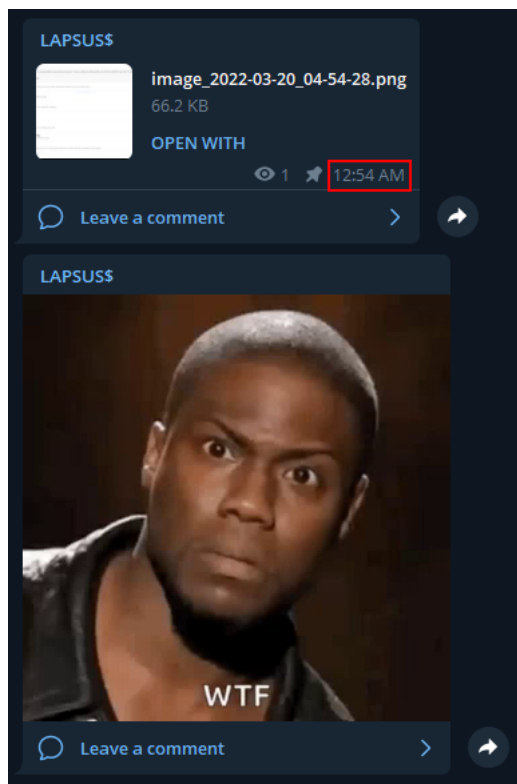
The leak also contains multiple sensitive endpoints like the one mentioned in the above screenshot. Similarly there are 135 .pfx files which are present in the leak. A pfx file contains the SSL certificate(public key) and the corresponding private key. These can in turn be used maliciously.

There are documentation files as well as internal pdf files:

```
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/Directions.imageset/directions.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/ZoomIn.imageset/zoom-in.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/ZoomOut.imageset/zoom-out.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/ZoomInDisabled.imageset/zoom-in-disabled.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/StylePicker.imageset/style-picker.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/TiltDisabled.imageset/tilt-disabled.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/ZoomOutDisabled.imageset/zoom-out-disabled.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/Default.imageset/default.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/UserLocation.imageset/user-location.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/Compass.imageset/compass.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/Tilt.imageset/tilt.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftMaps/assets.xcassets/Dark.imageset/dark.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftNavigation/navigation.xcassets/Anger.imageset/Anger.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftNavigation/navigation.xcassets/Thinking.imageset/Thinking.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftNavigation/navigation.xcassets/Love.imageset/Love.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftNavigation/navigation.xcassets/Sad.imageset/Sad.pdf
./NativeMaps-Client/src/SDK/Projects/iOS/MicrosoftMaps/MicrosoftNavigation/navigation.xcassets/Like.imageset/Like.pdf
./Spatial/WebServices/External/PowerThreading/Power Threading License.pdf
./Spatial/WebServices/External/PowerThreading/Power Threading Overview.pdf
./IndoorUnity/src/IndoorUnity/Assets/TextMesh Pro/Documentation/TextMesh Pro User Guide 2016.pdf
```

By looking at the files we can conclude the following:

- No customer data was affected
- No PII was leaked
- Source code along with certificates and pfx files were leaked
- The Lapsus\$ group is not very strong with Operational Security as they posted a Proof of Concept in the Telegram channel while the exfiltration was still underway

A screenshot of a file explorer window showing a directory listing for 'Microsoft > MS > Aria.Backend'. The table below shows the files and their modification dates, with a red box highlighting the date '3/20/2022 12:24 AM' for all entries.

Name	Date modified
azure-pipelines.yml	3/20/2022 12:24 AM
dirs.proj	3/20/2022 12:24 AM
dirs.sln	3/20/2022 12:24 AM
fix_csproj.py	3/20/2022 12:24 AM

### Okta Breach Analysis:

Okta has also released a statement earlier in the form of a blog stating:

“Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider. As part of our regular procedures, we alerted the provider to the situation, while simultaneously terminating the user’s active Okta sessions and suspending the individual’s account. Following those actions, we shared pertinent information (including suspicious IP addresses) to supplement their investigation, which was supported by a third-party forensics firm.”

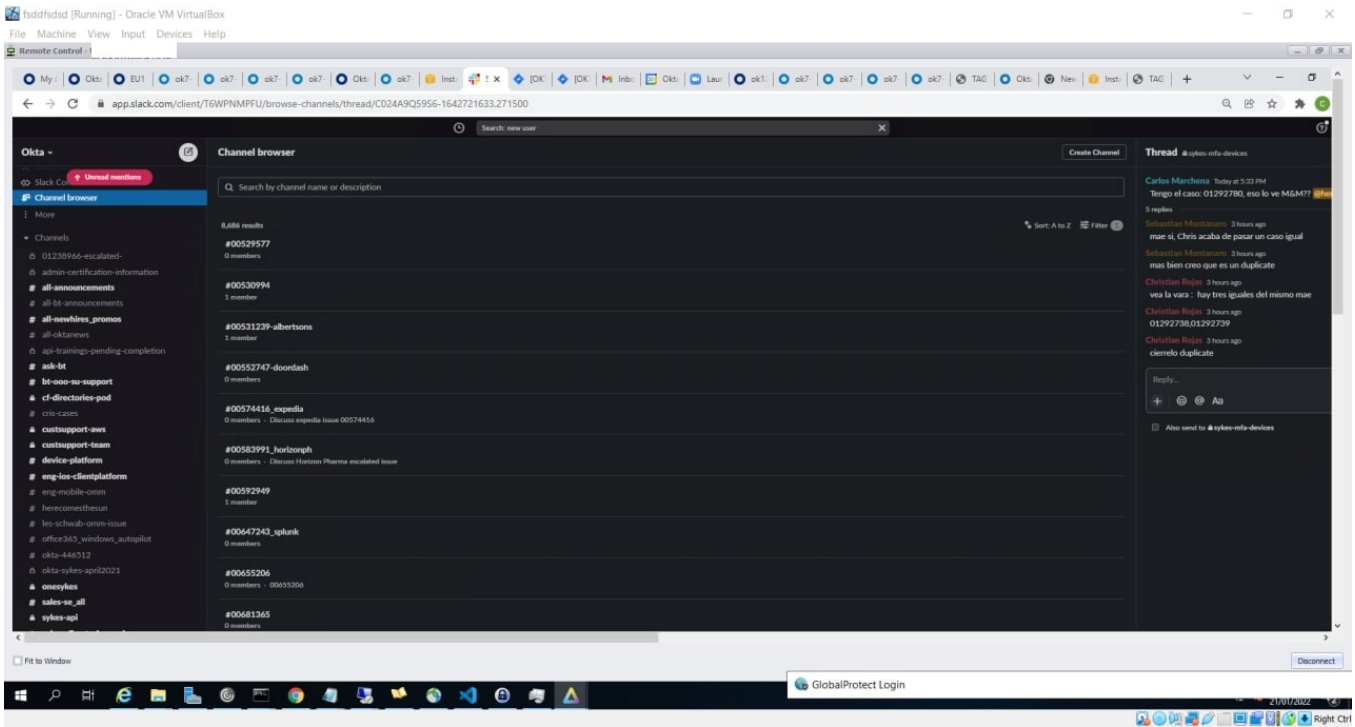
“After a thorough analysis of these claims, we have concluded that a small percentage of customers - approximately 2.5% - have potentially been impacted and whose data may have been viewed or acted upon. We have identified those customers and are contacting them directly. If you are an Okta customer and were impacted, we have already reached out directly by email. We are sharing this interim update, consistent with our values of customer success, integrity, and transparency”

In response to the above statement, Lapsus\$ group has also released a message which can be summarized in the following points:

- They were successful in breaching a Superuser/Admin account that had access to Slack, Jira, Confluence boards etc ..



- It is suspicious that the customer support engineer had access to ~8.6k slack channels and internal applications.
- They had access to internal AWS secret and key pairs/ other API keys as they were being shared in plain text over Slack and emails
- The breached account had the ability to reset the Password and MFA of ~95% of their clientele



The screenshot was shared by Lapsus as a POC claiming they had access to Slack and other applications.

## Globant Leak Analysis:

Globant in an official confirmation has not contested the claim of Lapsus\$. Globant released the following statement:

“We have recently detected that a limited section of our company’s code repository has been subject to unauthorized access. We have activated our security protocols and are conducting an exhaustive investigation. According to our current analysis, the information that was accessed was limited to certain source code and project-related documentation for a very limited number of clients. To date, we have not found any evidence that other areas of our infrastructure systems or those of our clients were affected”

The 70 GB data leak contains public and private keys (SSH and SSL) present in the leak asa part of their source code. It consists of the following information for a number of their clients:

```

./CloudNativePatrol/vms-cli/cli_vms/certs/client.crt
./Arcos-Dorados/app-db-migration-api-services/src/main/resources/ssl_certificate/root.crt
./Arcos-Dorados/app-db-migration-api-services/src/main/resources/ssl_certificate/postgresql.crt
./Citibanamex/marketplace/sslcert/server.crt
./Globant/microsites-xappia/wp-includes/certificates/ca-bundle.crt
./Globant/microsites-giant-monkey-robot/wp-includes/certificates/ca-bundle.crt
./Globant/base-image-wp/wp-includes/certificates/ca-bundle.crt
./Globant/GBN980-tech/wp-includes/certificates/ca-bundle.crt
./Globant/microsites-sentinel-report/wp-includes/certificates/ca-bundle.crt
./Globant/microsites-inspire/wp-includes/certificates/ca-bundle.crt
./Globant/microsites-bluecap/etc/ssl/certs/ca-certificates.crt
./Globant/microsites-bluecap/cert/bluecap.com.crt
./Globant/microsites-bluecap/web/app/lib/eM/SocialMedia/includes/fb_ca_chain_bundle.crt
./Globant/drupal-local-environment/configurations/nginx/ssl/certificate.crt
./apple-health-app/smu-fork/node_modules/node-gyp/test/fixtures/server.crt
./apple-health-app/smu-fork/node_modules/node-gyp/test/fixtures/ca-bundle.crt
./apple-health-app/smu-fork/node_modules/node-gyp/test/fixtures/ca.crt

```

```

/racetrac/racetrac-azure-templates/PreProd/AzurePreProdEnvironment/UbuntuVM/Keys/ubuntu-preprod-private.key
/racetrac/racetrac-azure-templates/PreProd/AzurePreProdEnvironment/UbuntuVM/Keys/ubuntu-preprod-public.key
/racetrac/racetrac-azure-templates/Resource upload files/Ubuntu VMs/ubuntu-dev-public.key
/racetrac/racetrac-azure-templates/Resource upload files/Ubuntu VMs/ubuntu-preprod-private.key
/racetrac/racetrac-azure-templates/Resource upload files/Ubuntu VMs/ubuntu-prod-private.key
/racetrac/racetrac-azure-templates/Resource upload files/Ubuntu VMs/ubuntu-dev-private.key
/racetrac/racetrac-azure-templates/Resource upload files/Ubuntu VMs/ubuntu-prod-public.key
/racetrac/racetrac-azure-templates/Resource upload files/Ubuntu VMs/ubuntu-preprod-public.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel73-prod-private.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel73-preprod-private.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel-prod-private.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel73-prod-public.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel-dev-public.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel-preprod-public.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel-prod-public.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel73-preprod-public.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel-dev-private.key
/racetrac/racetrac-azure-templates/Resource upload files/RHEL VMs/rhel-preprod-private.key
/cloudNativePatrol/vms-cli/cli_vms/certs/client.key
/Arcos-Dorados/app-db-migration-api-services/src/main/resources/ssl_certificate/postgresql.key
/Citibanamex/marketplace/sslcert/server.key
/Galicia-Agro/gres-greco-system-bff/app/config/public.key
/Galicia-Agro/gres-greco-system-bff/app/config/private.key
/Galicia-Agro/gres-greco-system-bff/server.key

```

Credential files leaked:

```

/Ensure-IAC/modules/rds_service/cert-db-creds.yml
/Ensure-IAC/modules/rds_service/db-dev-creds.yml.encrypted
/Ensure-IAC/db-qa-creds.yml.encrypted
/Ensure-IAC/db-dev-creds.yml.encrypted

```

Sensitive information and PII leaked:

```

{
  "number": " ",
  "separateCardNumber": " ",
  "stablishment": " ",
  "name": " ",
  "firstLastName": " ",
  "secondLastName": " ",
  "company": " ",
  "typePerson": " ",
  "typePersonDisplayed": " ",
  "alias": "OAC CARD 1",
  "accountNumber": " ",
  "branch": " ",
  "cashCardProduct": " ",
  "cellphone": " ",
  "separateCellPhone": " ",
  "clabe": " ",
  "cardAbv": "**087"
}

```

SQL files leaked:

```

/Abbott/CC-Esb/docker-db/docker-entrypoint-initdb.d/init.sql
/Avengers/recognition-api-aws/src/main/resources/database/recognition.sql
/Avengers/recognition-api-open-source/src/main/resources/database/recognition.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V2_setup_database_create_user_analytics_event_table.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V7_create_data_retention_policies.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V3_create_continuous_aggregate_for_conversation_flow.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V8_create_continuous_aggregate_fallback_events.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V9_create_conversation_event_metrics_aggregates.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V5_create_continuous_aggregate_user_metrics.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V1_base_line.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V6_create_indexes.sql
/Fluentlab/chatbot-platform/fluentlab-analytics/src/main/resources/analytcs/db/migration/V4_create_continuous_aggregate_for_user_information.sql
/Fluentlab/fluentlab-example-staging/fluentlab-analytics-load-test/dump.sql
/Fluentlab/fluentlab-example-staging/fluentlab-analytics/dump.sql

```

## Information from the Cyber Crime forum

Lapsus Ransomware group emerged in early January 2022.

- The group is actively operating over their Telegram channel and engages with subscribers. They keep their subscribers updated on their upcoming data breaches and host polls.
- Recently, we came across a post on a Russian speaking cybercrime forum that mentioned PII as the operator of the Lapsus\$ group.

Lapsus\$ Ransomware's owner doxed.

UnknownDeath · Yesterday at 4:59 AM

Jump to new · Wat

Yesterday at 4:59 AM

**TO THE MODS: THIS INFORMATION IS FROM 3RD PARTY SOURCES, IT IS EDUCATIONAL AS IT SHOWCASES BAD OPSEC IN HOPES OTHERS LEARN FROM THE MISTAKES OF OTHERS. IF YOU HAVE A PROBLEM PLEASE RESTRICT OR REMOVE THE THREAD. I'M JUST RELAYING INFO.**

NVIDIA + Samsung recently suffered a data breach, however 2 months prior: Lapsus\$ ransomware's owner "Lapsus\$" Was doxed by doxbin's staff. However NVIDIA nor Samsung wants to do anything regarding the matter. LAPSUS\$ is 16 almost 17 year old autistic skid whom previously lived in the United Kingdom and bought a website called "Doxbin" for \$75,000 USD after running the site for a while he completely derailed it via lack of care.

UnknownDeath  
RAID array  
User  
Joined: Jul 31, 2021  
Messages: 72  
Reaction score: 14

The doxed information shows a lot of personal information:

- o Name: Arion Kurtaj
- o Interests: Minecraft, Fishing, selling Odays
- o Age: 16 years
- o Potential Address: Spain
- o Nationality: British
- o DOB: February 19th, 2005
- o Personal Emails:

[email protected], [email protected], [email protected], [email protected], [email protected], [email protected], [email protected], [email protected], [email protected]

Aliases:

```
Alias(s):
  Sigma (Most recent)
  Lapsus$
  white
  White
  breachbase
  shadowarion4384
  Toyota
  ToyotaCorrola
  Hack0001
  DDoSshop
  OfficialPole
  nutnether
  ArionK4
  arion4384
```

### Common Vulnerabilities and Exposures(CVE)

Lapsus\$ gang previously targeted an organization in Nepal and an investigation blog was published for the same mentioning the targeted CVEs.

#### CVEs targeted by Lapsus\$

CVE-2022-21702: XSS vulnerability in Grafana	CVE-2022-0510: XSS reflected in Packagist pimcore/pimcore prior to 10.3.1.
CVE-2022-0139: Use After Free in GitHub repository radareorg/radare2 prior to 5.6.0	CVE-2021-45328: URL Redirection to Untrusted Site ('Open Redirect') via internal URLs
CVE-2021-45327: Trusting HTTP Permission Methods on the Server Side when referencing the vulnerable admin or user API	CVE-2021-45326: CSRF vulnerability exists in Gitea before 1.5.2 via API routes
CVE-2021-45325: SSRF vulnerability exists in Gitea before 1.7.0 using the OpenID URL	CVE-2021-44957: Global buffer overflow vulnerability exist in ffmpeg through 01.01.2021
CVE-2021-44956: Two Heap based buffer overflow vulnerabilities exist in ffmpeg through 01.01.2021	CVE-2021-44864: TP-Link WR886N 3.0 1.0.1 Build 150127 Rel.34123n is vulnerable to Buffer Overflow
CVE-2021-34473: Microsoft Exchange Server Remote Code Execution Vulnerability	CVE-2021-31207: Microsoft Exchange Server Security Feature Bypass Vulnerability
CVE-2021-26858: Microsoft Exchange Server Remote Code Execution Vulnerability	CVE-2021-26857: Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2021-26855: Microsoft Exchange Server Remote Code Execution Vulnerability	CVE-2020-23852: A heap based buffer overflow vulnerability exists in ffmpeg through 2020-07-02
CVE-2020-23705: A global buffer overflow vulnerability through 2020-06-22	CVE-2020-12812: An improper authentication vulnerability in SSL VPN in FortiOS
CVE-2019-5591: A Default Configuration vulnerability in FortiOS	CVE-2018-13379: An Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet

### Indicators of Compromise (IoCs)

Nvidia was targeted by Lapsus\$ group last month. Subsequently, earlier this month, malware samples began to appear in the wild, signed with Nvidia certificates. Some of these samples have got very low detection on VirusTotal because of the legitimate certificates attached, and hence could pose a threat. Following are the malware samples signed with stolen certificates:

SHA256

0e1638b37df11845253ee8b2188fdb199abe06bb768220c25c30e6a8ef4f9dee	9d123f8ca1a24ba215deb9968483d40b5d7a69fee734256240
065077fa74c211adf9563f00e57b5daf9594e72cea15b1c470d41b756c3b87e1	bc1d8872831e54a3989d283bcd27560cc12f54f831874162a8c
07ffa010ee48af8671fe74245bdfb54d9267aef748d9dc1fc8ca8df4966b871a	26683864b9c90e43de444ca09d5b2806c26dd9402c2010d079c
a7c3ce181e5c3956bb6b9b92e862b6fea6d6d3be1a38321ebb84428dde127677	36fec39a0f826fcca47e1997239c510ba93861faadbe82920532
0210a766da3e6d0cecbf166437a254c8ad6b380b077355a027fd0b7e3c2ccc9f	939294c6593f8339609c4db3b4861289c0612851ff43573c03e
2f578cb0d97498b3482876c2f356035e3365e2c492e10513ff4e4159eebc44b8	

**IPv4**

185.56.83.40	139.162.22.146
172.105.209.6	54.203.159.179

**Domain**

lapsus-group.com [email protected]

**Impact & Mitigation**

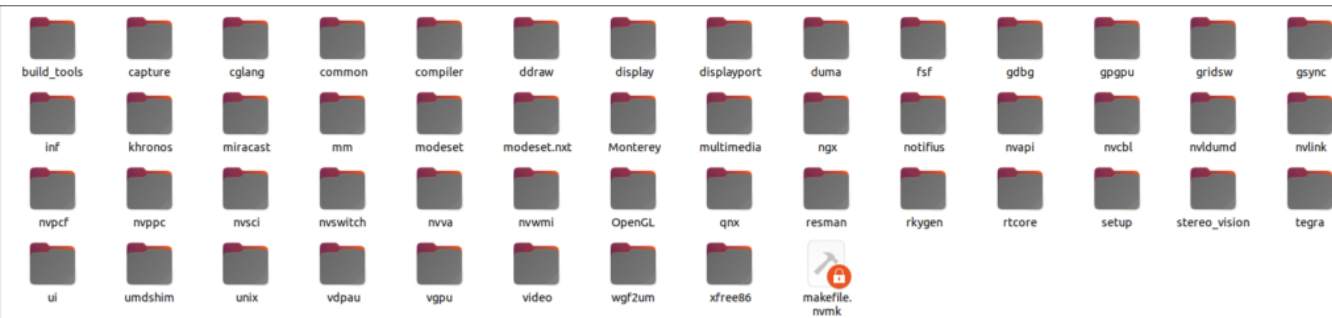
**Impact**

The published credentials could enable other threat actors to gain access to the organization's networks. The exposed Personally Identifiable Information (PII) could enable threat actors to orchestrate social engineering schemes, phishing attacks, and even identity theft. Since password reuse is a common practice, threat actors could leverage the exposed credentials to gain access to the users' other accounts. Exposed IP addresses and login credentials can lead to potential account takeovers. The exposed confidential details could reveal business practices and intellectual property.

**Mitigation**

Reset the compromised user login credentials and Implement a strong password policy for all user accounts. Check for possible workarounds and patches while keeping the ports open. Use MFA (multi-factor authentication) across logins. Patch all vulnerable and exploitable endpoints. Monitor for anomalies, in user accounts and systems, that could be indicators of possible takeovers.

**Appendix**



Leaked Nvidia Drivers information shared by threat actor



```
12288 Mar 23 12:35 .
4096 Mar 23 12:35 ..
4096 Mar 20 06:52 3SDataExplorer
4096 Mar 20 06:52 3sDataScience
4096 Mar 20 06:52 3SScorecardCOLStorage
4096 Mar 20 06:52 Answers
4096 Mar 20 06:52 AppStreamingApiManagement
4096 Mar 20 06:52 AppStreamingControllerServiceDT0
4096 Mar 20 06:52 AppStreamingLogon
4096 Mar 20 06:52 AppStreamingWebSockify
4096 Mar 20 06:52 AppVImageBuilder
4096 Mar 20 06:53 Aria.Backend
4096 Mar 20 06:53 Aria.CommandService
4096 Mar 20 06:53 Aria.E2E
4096 Mar 20 06:53 Aria.E2EClone
4096 Mar 20 06:53 Aria.Fluent
4096 Mar 20 06:53 Aria.GenevaActions
4096 Mar 20 06:53 Aria.HealthMonitoring
4096 Mar 20 06:53 Aria.K8sPlayground
4096 Mar 20 06:53 Aria.Kubernetes
4096 Mar 20 06:53 Aria.Models
4096 Mar 20 06:53 Aria.Samples
4096 Mar 20 06:53 Aria.Sdks
4096 Mar 20 06:53 Aria.Sessionization
4096 Mar 20 06:53 Aria.Stat
4096 Mar 20 06:53 'Aria.Stat (1)
4096 Mar 20 06:53 Aria.SupportCenter
4096 Mar 20 06:53 Aria.SupportCenter.Deployment
4096 Mar 20 06:54 Aria.Tools
4096 Mar 20 06:54 Aria.Web
4096 Mar 20 06:54 AssistantScorecard
4096 Mar 20 06:54 Auriga
4096 Mar 20 06:54 AurigaHealthDashboard
4096 Mar 20 06:54 AurigaPipelineValidation
4096 Mar 20 06:54 AurigaSentry
4096 Mar 20 06:54 Auriga.Spec.Generator
4096 Mar 20 06:54 AzureQueuesMonitor
4096 Mar 20 06:54 AzureRelay
4096 Mar 20 06:54 Azure-TDSP-ProjectTemplate
4096 Mar 20 06:54 Azure-TDSP-Utilities
4096 Mar 20 06:54 B2BPlatformADF
4096 Mar 20 06:54 BasisTranscoder
4096 Mar 20 06:54 BeaconBond
4096 Mar 20 06:54 BeaconClient
4096 Mar 20 06:54 BeaconDemoApp-iOS
4096 Mar 20 06:54 BeaconForegroundPrototype-iOS
4096 Mar 20 06:54 BeaconGroundTruthLogger
4096 Mar 20 06:54 BeaconGroundTruthTestData
4096 Mar 20 06:54 BeaconMotionActivityPrototype
4096 Mar 20 06:54 BeaconReferenceApps
4096 Mar 20 06:54 BeaconSharedClient
4096 Mar 20 06:54 BeaconTestFramework
4096 Mar 20 06:54 BingActionIOS
4096 Mar 20 06:54 BingMapsAzurePortal
4096 Mar 20 06:54 BingMapsIOSSDK
4096 Mar 20 06:54 BingMapsLegacyRP
4096 Mar 20 06:54 BingMapsNativeIOSSDK
4096 Mar 20 06:54 BingMapsReactNative
```

*Leaked Microsoft internal source code*