Detailed writeup on LAPSUS$ Cybercriminal Group who have compromised Microsoft and Okta

by anirudh.batra Threat Actor - Lapsus$ GroupThreat Actor - Lapsus$ Group

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

Executive Summary

- 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 screenshotThis 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
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.

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 amigos, 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 Recruitment PostLapsus Recruitment Post
Lapsus Recruitment Post

- 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.

  They have highlighted the post exploitation steps they took as a part of response to Okta's latest blog.They have highlighted the post exploitation steps they took as a part of response to Okta's latest blog.
  They have highlighted the post-exploitation steps they took as a part of the 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.

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:

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
-

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

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.
- The doxed information shows a lot of personal information:
    - Name: Arion Kurtaj
    - Interests: Minecraft, Fishing, selling 0days
    - Age: 16 years
    - Potential Address: Spain
    - Nationality: British
    - DOB: February 19th, 2005
    - Personal Emails:

, , , , , , , ,

- Aliases:

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 vulneraility exists in Gitea before 1.7.0 using the OpenID URL	CVE-2021-44957: Global buffer overflow vulnerability exist in ffjpeg through 01.01.2021
CVE-2021-44956: Two Heap based buffer overflow vulnerabilities exist in ffjpeg 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 ffjpeg 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	9d123f8ca1a24ba215deb9968483d40b5d7a69feee7342562407c42ed4e09cf7
065077fa74c211adf9563f00e57b5daf9594e72cea15b1c470d41b756c3b87e1	bcb1d8872831e54a3989d283bcd27560cc12f54f831874162a80dc9dcddf0b3
07ffa010ee48af8671fe74245bdfb54d9267aef748d9dc1fc8ca8df4966b871a	26683864b9c90e43de444ca09d5b2806c26dd9402c2010d0799f1963fd584c1
a7c3ce181e5c3956bb6b9b92e862b6fea6d6d3be1a38321ebb84428dde127677	36fec39a0f826fccca47e1997239c510ba93861faadbe8292053287ba5ab991a
0210a766da3e6d0cecbf166437a254c8ad6b380b077355a027fd0b7e3c2ccc9f	939294c6593f8339609c4db3b4861289c0612851f1ff43573c03af2e108221d
2f578cb0d97498b3482876c2f356035e3365e2c492e10513ff4e4159eebc44b8	
IPv4	
185.56.83.40	139.162.22.146
172.105.209.6	54.203.159.179
Domain	
lapsus-group.com	

Impact & Mitigation

Impact	Mitigation
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.	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 actorLeaked Nvidia Drivers information shared by threat actor
Leaked Nvidia Drivers information shared by threat actor

Leaked Microsoft internal source codeLeaked Microsoft internal source code
Leaked Microsoft internal source code

- Author Details

anirudh.batraanirudh.batra anirudh.batra Threat Analyst I am an information security enthusiast and currently preparing for OSCP. I am tenacious, hardworking and passionate about security. I have completed my Btech in CSE from VIT, Vellore

-

× anirudh.batraanirudh.batra anirudh.batra Threat Analyst I am an information security enthusiast and currently preparing for OSCP. I am tenacious, hardworking and passionate about security. I have completed my Btech in CSE from VIT, Vellore

-

Latest Posts

- Threat Actor - Lapsus$ GroupThreat Actor - Lapsus$ Group