LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Lapsus$, Okta and the Health Sector

4/7/2022

TLP: WHITE, ID# ***202204071300***

Agenda

- Introduction
- Profile of Lapsus$
- Operations
- Okta Compromise
- Microsoft Compromise
- Law Enforcement Actions
- Defense/Mitigations
- Conclusions

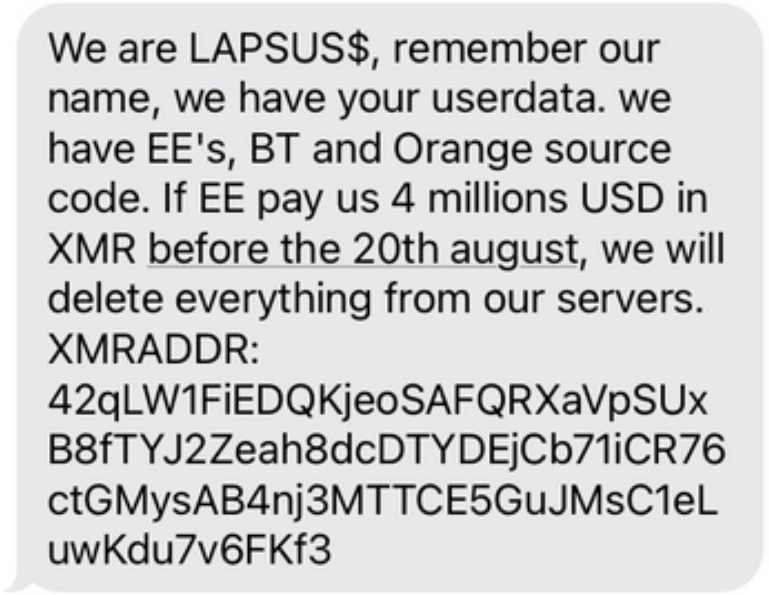
Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction to Lapsis$

- Lapsus$ is a recently discovered cyber threat group with yet-to-be determined motivations.
- They have not brought overly sophisticated tools to an attack but have been successful regardless.
- They have been effective, but also unprofessional and careless:
  - Tactics, techniques and procedures range from simple to moderately complex.
- They have successfully targeted several high-profile organizations to completion.
- Due to the diversity of their techniques, there is no single set of effective defenses or mitigations.
- Possibly a group of teenagers and young adults.
- They utilize “big game hunting” methods – the targeting of large firms.



This brief is accurate as of the date of its delivery (April 7, 2022); however, new information is being released daily on Lapsis$ and their compromised targets.

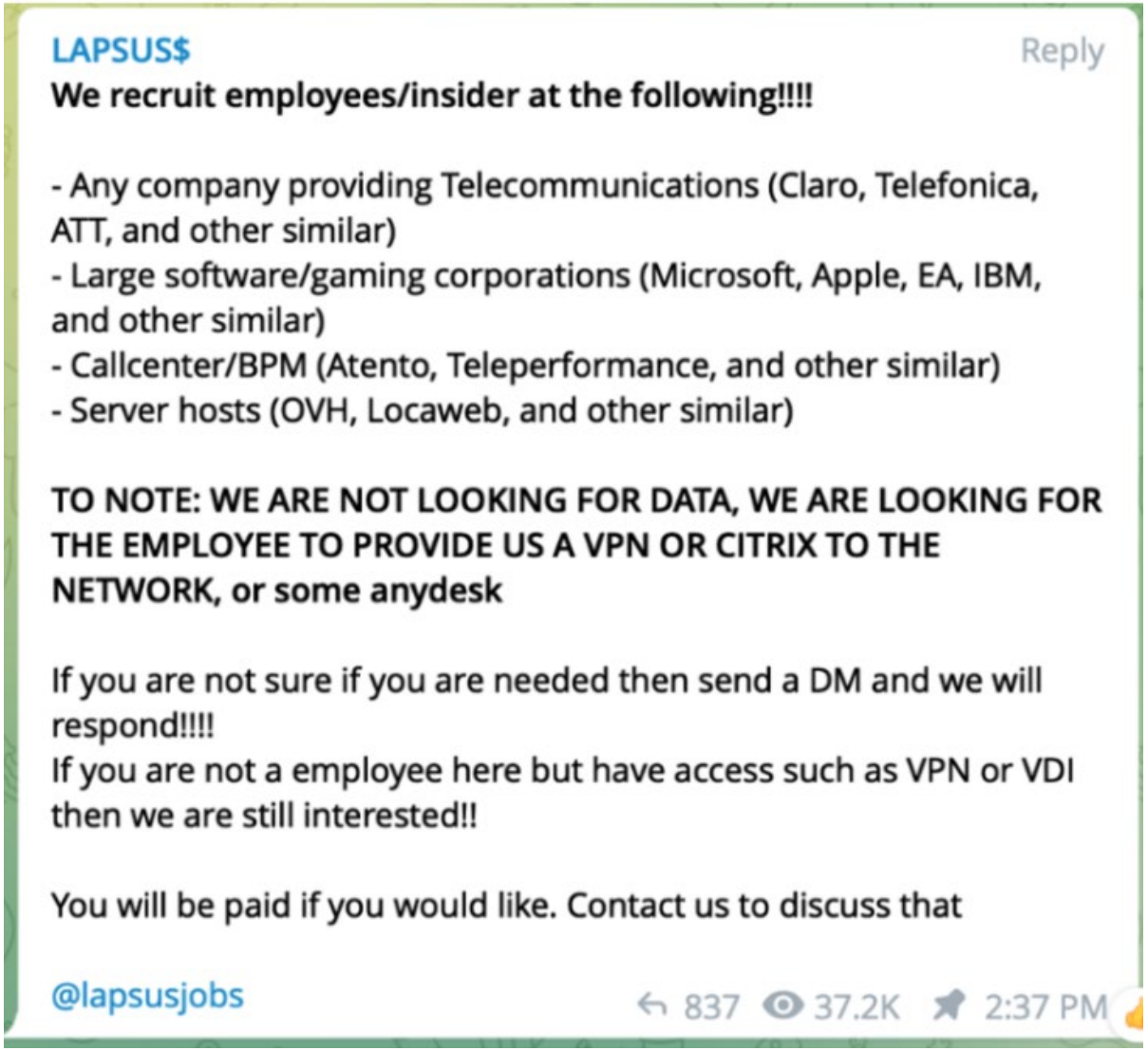
Profile of Lapsus$

- First identified ~April 2020; tracked as DEV-0357 (Microsoft)
- Motivation: Financial gain, destruction, notoriety/fame
  - Extortion without ransomware or any sophisticated malware
- Members are believed to be from Portugal and Latin America
  - Members speak English, Russian, Turkish, German and Portuguese
  - Their recruitment ads are written in Portuguese and English
- Telegram channel: t[.]me/minsaudebr (over 45,000 subscribers); associated email address: saudegroup[at]ctemplar[.]com
- Highly communicative to the public
- Heavy reliance on bribery and non-ransomware extortion
- Common tactics/techniques/procedures (TTPs):
  - Credential theft
  - Multi-factor authentication bypass
  - Social engineering (especially phone-based)
  - Managed service provider compromise
  - SIM-swapping
  - Accessing personal email accounts of employees of target organizations
  - Bribing employees, suppliers, or business partners of target organizations for credentials and multifactor authentication approval
  - Self-injection into ongoing crisis-communication calls of their targets

Profile of Lapsus$, Part 2

- Also targets:
  - Telecommunications providers, software development companies, managed service providers, cryptocurrency exchanges, call centers
  - Initially focused on the UK and South America, but they are expanding globally
  - Targeting clouds
  - Recent public victims have included:
    - Brazilian Ministry of Health
    - Nvidia
    - Samsung
    - Ubisoft
    - Vodafone
    - Microsoft
    - LG
    - Okta
    - Globant
- Often make no effort to cover tracks
  - Advertise intent to purchase credentials

Lapsus$: Open Recruiting for Assistance



LAPSUS$ Reply

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 837 37.2K 2:37 PM

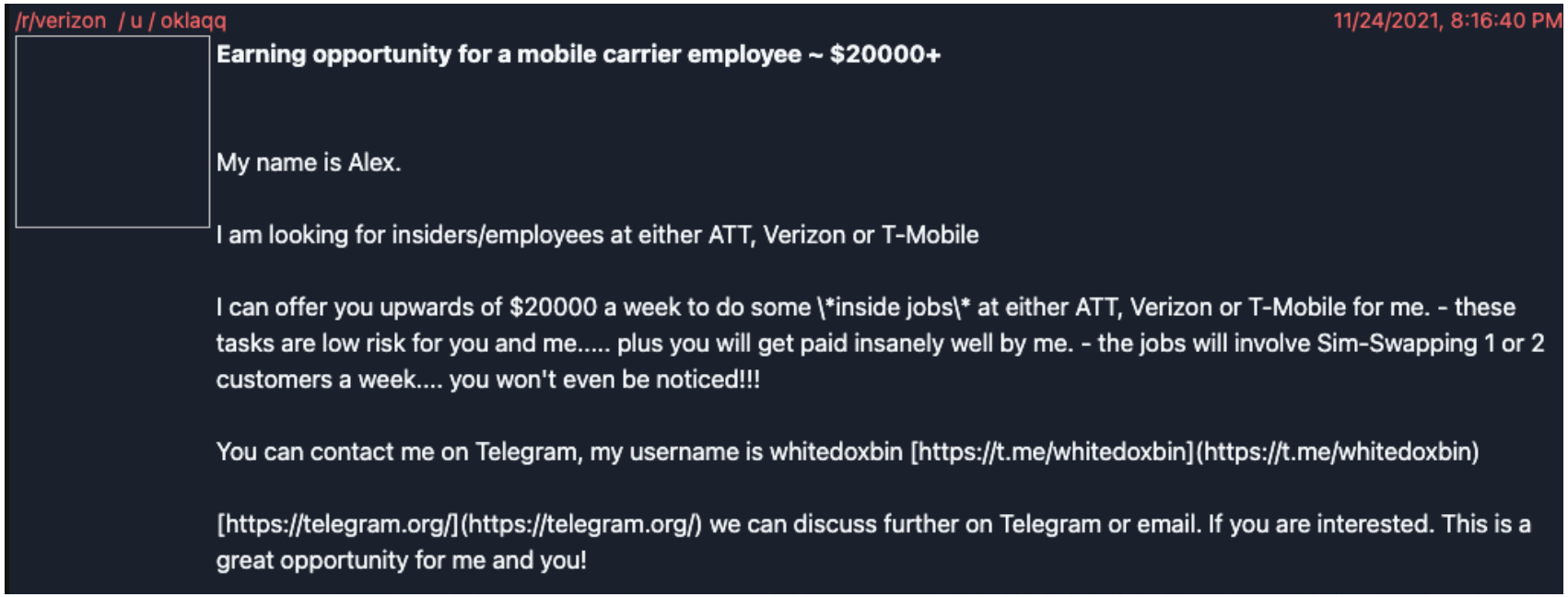
Cyberattack on Brazilian Ministry of Health, December 2021

Defacement of the Brazilian Ministry of Health website:

Lapsus$: Initial Access

Lapsus$ uses several methods to compromise user identities to gain initial access, including:

- Deploying the malicious Redline password stealer to obtain passwords and session tokens
- Purchasing credentials and session tokens from criminal underground forums
- Paying organizational/suppliers/business partners for access to credentials and MFA approval
- Multifactor authentication prompt bombing – that is, annoying the target into clicking away notifications that allow attackers to access their account, or to execute malicious code
- Searching public code repositories for exposed credentials



Lapsus$: Reconnaissance, Lateral Movement and Privilege Escalation

After Lapsus$ gains access to a target, they often move on to lateral movement, privilege escalation and reconnaissance. They do this by:

- Targeting vulnerabilities in platforms such as JIRA, Gitlab and Confluence
- Searching public code repositories for exposed credentials
- Leveraging Active Director (AD) Explorer
- Mimikatz
- DCSync
- Targeting the victim's help desk via social engineering

Lapsus$: Data Exfiltration and Destruction

Once they have identified the data they need, Lapsus$ uses the following for exfiltration and destruction:

- They operate in known virtual private server (VPS) providers
- They create virtual machines in the target's cloud environment to utilize in further attacks against the victim's infrastructure
- They leverage NordVPN for its egress points to be geographically near their targets
- They seize cloud resources by:
  - Creating global admin accounts in the organization's cloud instances
  - Creating an Office 365 tenant level e-mail transport rule to send all incoming/outgoing e-mail in and out of the organization to the newly created account
  - Removing all other global admin accounts
- After exfiltration, they delete the target's systems and resources:
  - Both on-premises and in the cloud, to trigger the organization's incident and crisis response process
  - They join the organization's crisis communication/internal discussion communications to understand the incident response and workflow response process
  - Understanding the organization's mindset provides extortion negotiation advantages

Okta Compromise

Who is Okta?

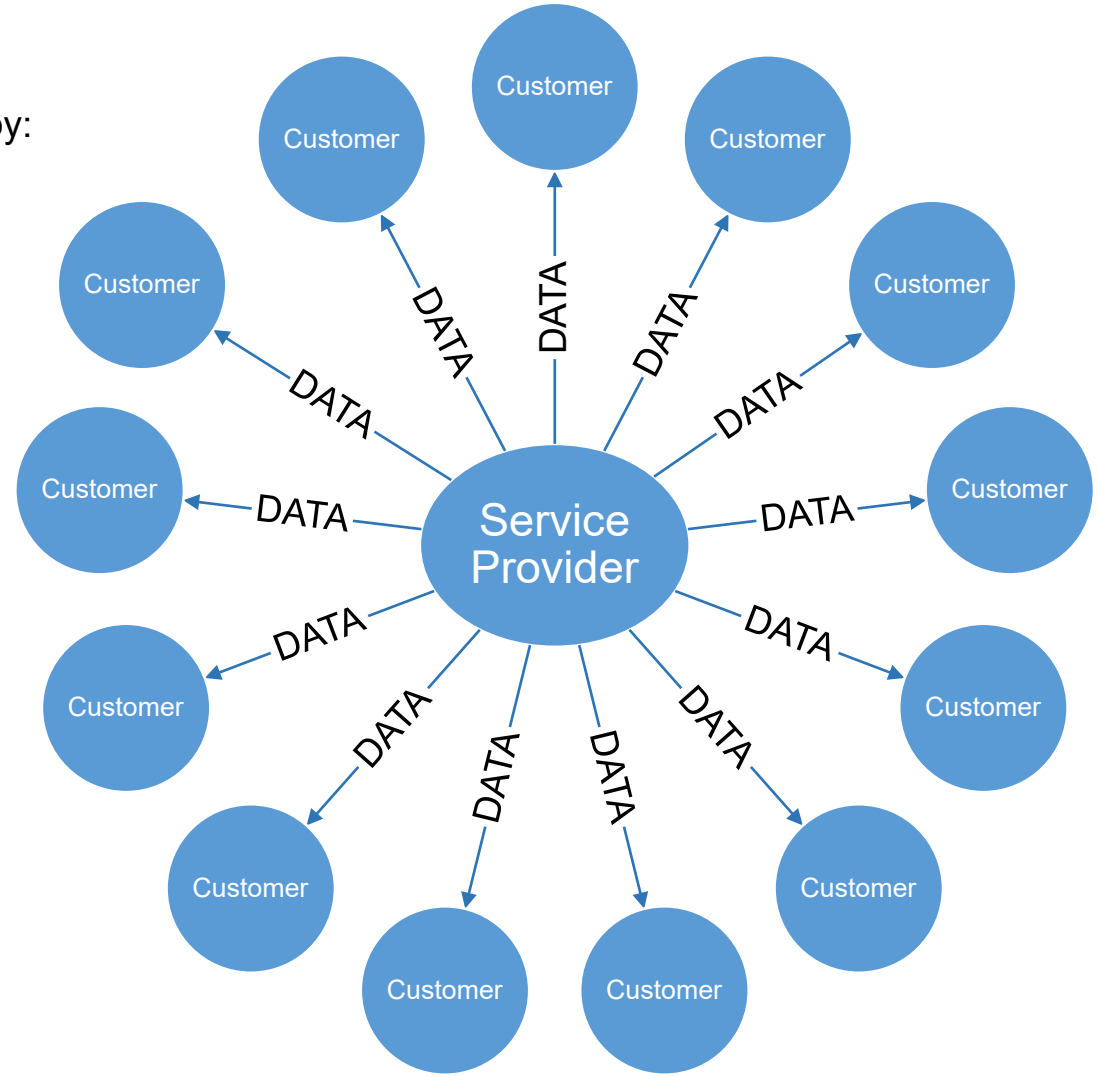
- Identity management service provider
  - Allows client employees to authenticate to internal resources (e-mail, applications, databases, etc.)
- Claims over 15,000 customers
- On January 21, 2022, Lapsus$ posted screenshots of Okta's internal resources to their Telegram channel
- Okta admitted that ~3.5% (366 customers) had their data exposed to Lapsus$ members
- One of their customers, Sykes, confirmed that they were also compromised in late January
- Lapsus$'s motives were unclear; there has yet to be any publicly known impacts to this attack
  - They are believed to have acquired a list of domain passwords from Sykes

Why is the Okta compromise important to healthcare?

- HC3 is aware of healthcare organizations that were compromised in this attack
- It is a managed service provider attack, which are often used as part of cyberattacks on the health sector

Additional details of the Okta compromise can be found here: https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise

- With distributed attack vectors, adversaries attempt to maximally compromise victims in a single attack by:
  - Managing service provider compromise,
  - Managing supply chain compromise,
  - And managing software components

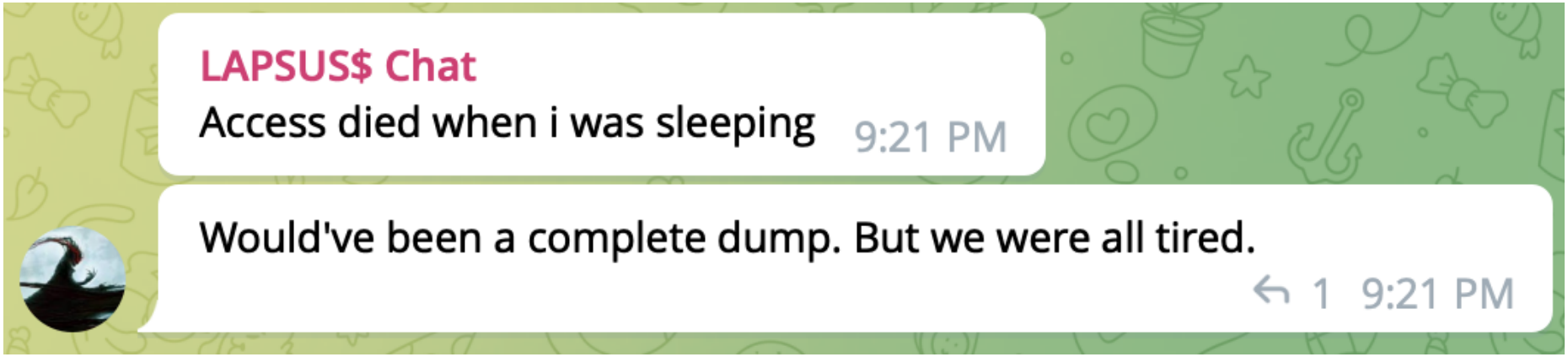


Okta was yet another example of a distributed attack vector.

Other recent examples: Solar Winds, Kaseya, and Log4J/Log4Shell

Microsoft Compromise

- On March 22, 2022, Microsoft announced in a blog post that they interrupted source code exfiltration by Lapsus$.
  - The Lapsus$ members apparently fell asleep during the download.
- Lapsus$ dumped what it described as source code from Microsoft's Bing search engine, Maps, and Cortana virtual assistant software.
- Lapsus$ also claimed that multifactor authentication prompt bombing was successful in this attack.
- Microsoft claimed Lapsus$ gained “limited access” to their infrastructure and did not exfiltrate any code.
  - Microsoft also noted that they do not rely on code secrecy for security, and so even if the code was leaked, it would not lead to an increase in risk.



The FBI Is Looking for Assistance in Identifying Lapsus$ Members

SEEKING INFORMATION

LAPSUS$

Cyber Intrusions of United States-Based Technology Companies
March 21, 2022

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of computer networks belonging to United States-based technology companies.

On March 21, 2022, individuals from a group identifying themselves as Lapsus$ posted on a social media platform and alleged to have stolen source code from a number of United States-based technology companies. These unidentified individuals took credit for both the theft and dissemination of proprietary data that they claim to have illegally obtained. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Francisco

Arrests of Seven Alleged Members of Lapsus$

- London police announced on March 25, 2022, that they arrested seven alleged members of Lapsus$
  - Ages ranging from 16 to 21
  - 16-year-old from Oxford is alleged to be the leader, having amassed $14 million
    - AKA “White” or “Breachbase” (also WhiteDoxbin?)
    - Such a skilled hacker that investigators initially believed the activity was automated
  - What led to this?
    - WhiteDoxbin purchased a site called Doxbin in 2021, which is a public forum used to post personal information on targets.
    - Doxbin was not administered very well, and the community of users expressed their discontent.
    - WhiteDoxbin sold Doxbin back to its original owner for a significant loss but leaked a lot of private data associated with the site’s members.
    - These members responded by doxxing WhiteDoxbin, up to and including publishing a video of where he allegedly lived as revenge.
- Ironically, members of a doxxing site who were frustrated because their information was leaked in turn leaking information about the site’s owner/administrator, is what ultimately led to the arrests.

Technology	Details
Multifactor authentication	Require MFA for all users
	Leverage passwordless authentication
	Implement user and sign-in risk-based policies that block high impact user actions, like device enrollment and MFA registration
	Disallow text, SMS push, secondary email and voice approvals as MFA options
	Do not implement location-based exclusions
Virtual private networks (VPNs)	Leverage modern authentication options such as OAuth or SAML
Zero trust	Implement zero trust as applicable across the enterprise, with the idea that Lapsus$ frequently attempts to compromise insiders, and so this can potentially limit the impact
Network segmentation	Ensure that enterprise infrastructure is architected in such a way to limit access to especially sensitive networks and data to only those who require its use, and keeping sensitive data protected from exposure to the Internet and all the threats that exist there
Social engineering	Ensure training is adequate for employees; implement testing programs as necessary
Data backup	Ensure most critical data is properly backed up; implement the 3-2-1 rule

What does all this mean for the HPH?

- When comparing Lapsus$ motivations and tactics to health sector operations, the health sector is within their scope of targeting:
  - They steal data for extortion purposes
  - They target managed service providers
  - Their operations are global, and they look for targets of opportunity
- While law enforcement has began pressuring the group and even arresting some alleged members, operations are expected to continue.
  - Other members will very likely continue to operate under the Lapsus$ banner or as part of another group
  - The geographic diversity of this group will make them especially difficult to permanently quash
- The diversity of their tactics, and their lack of reliance of specific malware variants, make them very difficult to detect or stop.
- They have already compromised healthcare organizations and have no reason to stop.

Reference Materials

References

What are the possible consequences of Okta hack?
https://www.kaspersky.com/blog/okta-hack-consequences/43971/

Cyber company Okta is latest potential victim cited by Lapsus$ hackers
https://www.cyberscoop.com/cyber-company-okta-is-latest-potential-victim-of-lapsus-hackers/

LAPSUS$ & OKTA: The Cyber Attacks Continue
https://blog.checkpoint.com/2022/03/22/lapsuss-okta-the-cyber-attacks-continue/

OKTA breached by Lapsus$ Ransomware Gang
https://blog.checkpoint.com/2022/03/22/okta-breached-by-lapsus-ransomware-gang/

Okta confirms support engineer's laptop was hacked in January
https://www.bleepingcomputer.com/news/security/okta-confirms-support-engineers-laptop-was-hacked-in-january/

Okta revises LAPSUS$ impact upwards to potentially 2.5% of customers
https://www.zdnet.com/article/okta-revises-lapsus-impact-upwards-to-potentially-2-5-of-customers/

Authentication Giant Okta Breached Through Customer Support
https://www.vice.com/en/article/jgmnwk/authentication-giant-okta-breached-through-customer-support

Microsoft and Okta confirm, detail impact of Lapsus$ gang's attacks
https://www.helpnetsecurity.com/2022/03/23/microsoft-okta-lapsus/

Microsoft investigating hacking group's claims of successful breach
https://www.cyberscoop.com/microsoft-hack-lapsus-breach/

Leaked stolen Nvidia key can sign Windows malware
https://www.theregister.com/2022/03/05/nvidia_stolen_certificate/

References

DEV-0537 criminal actor targeting organizations for data exfiltration and destruction
https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

Okta 'identifying and contacting' customers potentially affected by Lapsus$ breach
https://therecord.media/okta-identifying-and-contacting-customers-potentially-affected-by-lapsus-breach/

Okta investigating claims of customer data breach from Lapsus$ group
https://www.bleepingcomputer.com/news/security/okta-investigating-claims-of-customer-data-breach-from-lapsus-group/

Microsoft investigating claims of hacked source code repositories
https://www.bleepingcomputer.com/news/security/microsoft-investigating-claims-of-hacked-source-code-repositories/

Microsoft confirms they were hacked by Lapsus$ extortion group
https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/

Okta says breach evidence posted by Lapsus$ hackers linked to January 'security incident'
https://www.zdnet.com/article/okta-says-breach-evidence-shared-by-lapsus-ransomware-group-linked-to-january-hack-attempt/

Cybercriminals who breached Nvidia issue one of the most unusual demands ever
https://arstechnica.com/information-technology/2022/03/cybercriminals-who-breached-nvidia-issue-one-of-the-most-unusual-demands-ever/

The Lapsus$ Hacking Group Is Off to a Chaotic Start
https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung/

References

Threat Brief: Lapsus$ Group
https://unit42.paloaltonetworks.com/lapsus-group/

Okta confirms support engineer's laptop was hacked in January
https://www.bleepingcomputer.com/news/security/okta-confirms-support-engineers-laptop-was-hacked-in-january/

Microsoft confirms they were hacked by Lapsus$ extortion group
https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/

Okta revises LAPSUS$ impact upwards to potentially 2.5% of customers
https://www.zdnet.com/article/okta-revises-lapsus-impact-upwards-to-potentially-2-5-of-customers/

LAPSUS$ Claims to Have Breached IT Firm Globant; Leaks 70GB of Data
https://thehackernews.com/2022/03/lapsus-claims-to-have-breached-it-firm.html

Globant confirms hack after Lapsus$ leaks 70GB of stolen data
https://www.bleepingcomputer.com/news/security/globant-confirms-hack-after-lapsus-leaks-70gb-of-stolen-data/

Lapsus$ suspects arrested for Microsoft, Nvidia, Okta hacks
https://www.bleepingcomputer.com/news/security/lapsus-suspects-arrested-for-microsoft-nvidia-okta-hacks/

Leaked Details of the Lapsus$ Hack Make Okta's Slow Response Look More Bizarre
https://www.wired.com/story/lapsus-okta-hack-sitel-leak/

Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal
https://www.bbc.com/news/technology-60864283

References

Lapsus$ and SolarWinds hackers both use the same old trick to bypass MFA
https://arstechnica.com/information-technology/2022/03/lapsus-and-solar-winds-hackers-both-use-the-same-old-trick-to-bypass-mfa/

Okta confirms January breach after hackers publish screenshots of its internal network
https://techcrunch.com/2022/03/22/okta-january-hack-breach/

The Third-Party Okta Hack Leaves Customers Scrambling
https://www.wired.com/story/okta-hack-customers-lapsus-breach/

Frequently Asked Questions Regarding the January 2022 Compromise
https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise

Lapsus$ found a spreadsheet of accounts as they breached Okta, documents show
https://techcrunch.com/2022/03/28/lapsus-passwords-okta-breach/

'This Is Really, Really Bad': Lapsus$ Gang Claims Okta Hack
https://www.wired.com/story/okta-hack-microsoft-bing-code-leak-lapsus/

The Third-Party Okta Hack Leaves Customers Scrambling
https://www.wired.com/story/okta-hack-customers-lapsus-breach/

Questions

Upcoming Briefs

- 4/27 – Insider Threats and the Healthcare Industry

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV