CYBER SAFETY
REVIEW BOARD

REVIEW OF THE ATTACKS ASSOCIATED WITH LAPSUS$ AND RELATED THREAT GROUPS

July 24, 2023
Cyber Safety Review Board

Table of Contents

MESSAGE FROM THE CHAIR AND DEPUTY CHAIR

In 1983, the movie WarGames captured the imagination of a society navigating its way towards the personal computing revolution. Therein, a seemingly ordinary high school student, with a keen sense of curiosity, uses esoteric magic to hack into the U.S. Department of Defense using just a phone line and an acoustic coupler. Having made a connection, he meets the AI-powered NORAD computer known as the WOPR (or Joshua). The WOPR's primary job is running war simulations for the government, but Joshua also moonlights as a loveable tic-tac-toe opponent thanks to a set of easter eggs implanted by its creator. This moment in movie history came to mind as we took on this review, just as AI and large language models are being incorporated into systems globally. We see one other, more obvious, parallel: teenagers are compromising well-defended organizations using a creative application of many techniques. Not much seems to have changed in the last 40 years. Yet, we saw a clear distinction that stood in stark relief as we dove deeper into the details of the review: namely the vast global for-profit online criminal landscape that curious young people are now encountering. Everything on this front has changed significantly.

In this review, the Board's second, we focused on a loosely organized group of threat actors that styled itself as Lapsus$ for a short period of time in 2021 - 2022. Lapsus$ drew the attention of cybersecurity professionals and the press almost immediately after providing unparalleled transparency into the inner workings of how it targeted organizations and individuals, organized its attacks, and interacted within itself and with other threat groups. Its mindset was on full display for the world to see and Lapsus$ made clear just how easy it was for its members (juveniles, in some instances) to infiltrate well-defended organizations. Lapsus$ seemed to work at various times for notoriety, financial gain, or amusement, and blended a variety of techniques, some more complex than others, with flashes of creativity. But Lapsus$ did not fall into that category of threat actor that grabs most of the headlines: the nation-state threat actor with well-resourced offensive tactics that lurks behind the scenes for years at a time or the transnational ransomware groups that cost the global economy billions of dollars. In fact, Lapsus$ did not use the type of novel zero-day techniques the industry is used to seeing frequently in the news.

Lapsus$ was not unique in the criminal landscape in which it operated; it had membership in common with other similarly motivated groups globally. But Lapsus$ was unique for its effectiveness, speed, creativity, and boldness; it operated in a way that gifted the Board a propitious lens through which we could see systemic issues in the digital ecosystem. Our attention was drawn immediately towards the identity and access management ecosystem; the way threat actors abused telecommunications providers; the relationships between organizations and their outsourcing companies; and how the law enforcement ecosystem plays a vital role in deterrence.

Organizations must act now to protect themselves, and the Board identified tangible ways to do so, with the help of the U.S. government and the companies that are best prepared to provide safe-by-default solutions to uplift the whole ecosystem. Many of the Board's recommendations come within the broader theme of "security by design," reflecting the larger industry conversation, including the Cybersecurity and Infrastructure Security Agency's (CISA's) Secure by Design[1] efforts.

We need better technologies that move us towards a passwordless world, negating the effects of credential theft. We need telecommunications providers to design and implement processes and systems that keep attackers from hijacking mobile phone service. We need to double down on zero trust architectures that assume breach. We need organizations to design their security programs to cover not only their own information technology environments, but also those of their vendors that host critical data or maintain direct network access. We need to give law enforcement the means to disrupt all manner of threat actors. And we need to help curious young people use their growing digital skills for positive purposes. The Board developed actionable recommendations for all these issues and more.

As we reflect on our second review as an institution, we are proud that the Board has further proved this model of deep, after-action reviews of the most significant incidents. The recommendations are strong and specific because we were able to draw from the diverse expertise of the Board's public-private membership, including law enforcement, incident response experts, a critical infrastructure Chief Information Security Officer, and more.

[1] CISA, "*Secure by Design, Secure by Default*," https://www.cisa.gov/securebydesign

We are grateful that, among the impacted companies, several cooperated actively with the Board's work. Their perspectives were critical to the insights and recommendations in this review, and their contributions highlight the public safety need for the Board to gather all information required to do our work effectively. We appreciate as well the voluntary contributions of over 30 other companies, cybersecurity firms, law enforcement organizations, security researchers, and academics that had insights to share. Unfortunately, some organizations that were known to have been impacted by Lapsus$ declined to participate in the review, limiting the Board's opportunity to learn from a range of experiences that would have further enriched our work.

Earlier this year, the Administration recommended that Congress authorize the Board and provide it with the appropriate authorities to ensure that the Board can gather the information needed to advise the cyber community—voluntarily where possible, but with a limited subpoena authority as a backstop when necessary. We are hopeful that Congress will act quickly on this important legislation.

We are grateful to Alejandro N. Mayorkas, Secretary of Homeland Security, for his continued belief in the important mission of this Board, and to Cybersecurity and Infrastructure Security Agency Director Jen Easterly for commissioning our second review and offering CISA's resources and support to ensure the Board could conduct its independent work.

Finally, we give thanks to the many companies and individual experts that offered their support to this comprehensive review. We also express our sincere appreciation to our colleagues on the Board and the talented and dedicated staff that has supported its work.

We look forward to our coming reviews. We will in the meantime continue to fortify the CSRB and its supporting infrastructure, for this Board has become an enduring part of our cybersecurity ecosystem as a true public-private model.

Robert Silvers
Chair
Cyber Safety Review Board

Heather Adkins
Deputy Chair
Cyber Safety Review Board

EXECUTIVE SUMMARY

Beginning in late 2021 and continuing late into 2022, a globally active, extortion-focused cyber threat actor group attacked dozens of well-known companies and government agencies around the world. It penetrated corporate networks, stole source code, demanded payments while rarely following up, lodged political messages in shadowy online forums, and swiftly moved on to its next targets. The cyberattacks were not the work of a nation-state actor, nor did they always involve particularly complex or advanced tooling or methods. Yet the attacks were consistently effective against some of the most well-resourced and well-defended companies in the world. These headline-grabbing incidents were perpetrated by a loosely organized threat actor group known as Lapsus$. Lapsus$ exploited systemic ecosystem weaknesses to infiltrate and extort organizations, sometimes appearing to do so for nothing more than attention and public notoriety.

Lapsus$ operated against a backdrop of other criminal groups employing similar methods that were studied as part of this review. These groups demonstrated the still-prevalent vulnerabilities in our cyber ecosystem. They showed adeptness in identifying weak points in the system—like downstream vendors or telecommunications providers—that allowed onward access to their intended victims. They also showed a special talent for social engineering, luring a target's employees to essentially open the gates to the corporate network.

Lapsus$'s and similar groups' success sounds a warning to organizations across the globe, shining a light on the fragility of our interconnected digital infrastructure. Lapsus$ exploited, to great and wide effect, a playbook of effective techniques, which other threat actors can also use. If richly resourced cybersecurity programs were so easily breached by a loosely organized threat actor group, which included several juveniles, how can organizations expect their programs to perform against well-resourced cybercrime syndicates and nation-state actors? The Cyber Safety Review Board (CSRB, or the Board) therefore focused intently on what additional security controls and improvements can bring needed change to the status quo.

The Board found that the multi-factor authentication (MFA) implementations used broadly in the digital ecosystem today are not sufficient for most organizations or consumers. In particular, the Board saw a collective failure to sufficiently account for and mitigate the risks associated with using Short Message Service (SMS) and voice calls for MFA. In several instances, attackers gained initial access to targeted organizations through Subscriber Identity Module (SIM) swapping attacks, which allowed them to intercept one-time passcodes and push notifications sent via SMS, effectively defeating this widely used MFA control. A lucrative SIM swap criminal market further enabled this pay-for-access to a target's mobile phone services. Despite these factors, adopting more advanced MFA capabilities remains a challenge for many organizations and individual consumers due to workflow and usability issues.

Initial access brokers (IABs) and the "infostealer" malware ecosystem—whereby anyone can buy valid login credentials for a target ("access as a service")—were highly effective means of initial entry. Threat actor groups highly leveraged these underground markets to directly target organizations, but also targeted the organization's third-party servicers and business process outsourcers (BPOs). Organizations did not always consider third parties and BPOs in their risk management programs.

Lapsus$ was not successful in all its attempted attacks. The Board found that organizations with mature, defense-in-depth controls were most resilient to these threat actor groups. Organizations that used application or token-based MFA methods or employed robust network intrusion detection systems, including rapid detection of suspicious account activity, were especially resilient. Organizations that maintained and followed their established incident response procedures significantly mitigated impacts. Highly effective organizations employed mechanisms such as out-of-band communications that allowed incident response professionals to coordinate response efforts without being monitored by the threat actors.

Through extensive efforts, international law enforcement eventually apprehended several of the perpetrators. Yet, those and similar United States (U.S.) government cybersecurity efforts remain unnecessarily hamstrung. In general, law enforcement remains underfunded for resource- and data-intensive investigations and disruptions against the full breadth of cyber threat actors. Similarly, chronic underreporting from the private sector of threats or incidents hampers the federal government's ability to warn other targeted entities, recommend mitigation measures, take down malicious infrastructure, seize ill-gotten cryptocurrency or fiat currency, bring those responsible to justice, or otherwise disrupt malicious activity.

In this review, the Board learned that some of the perpetrators were teenagers. In several jurisdictions, a perpetrator's juvenile status can yield lighter penalties and less severe consequences that may encourage young cybercriminals to re-offend. The Board also noted that while the United Kingdom and the Netherlands have nascent efforts to create pathways for steering talented young hackers away from cybercrime, similar community prevention programs do not exist in the U.S. Resourcing both law enforcement and intervention efforts needs rebalancing.

KEY RECOMMENDATIONS

The Board recommends that organizations urgently implement improved access controls and authentication methods and transition away from voice and SMS-based MFA; those methods are particularly vulnerable. Instead, organizations should adopt easy-to-use, secure-by-default, passwordless solutions such as Fast IDentity Online (FIDO)2-compliant, phishing-resistant MFA methods. Device and software manufacturers will need to innovate and deliver effective solutions that the global digital ecosystem can quickly adopt. To facilitate the transition to passwordless authentication, the Board recommends that the federal government develop and promote a secure authentication roadmap for the nation. The roadmap should include standards, frameworks, guidance, tools, and technology that can enable organizations to assess, progress, and implement leading practices for passwordless authentication.

The Board also calls attention to the risks introduced through use of mobile devices for authentication and urges telecommunications providers to mitigate risk through technological, process, and oversight measures. Carriers should implement more stringent authentication methods for SIM swapping to continue enabling legitimate business processes while introducing more friction to discourage malicious actors. The Board recommends that carriers mitigate retail point-of-sale vulnerabilities by improving asset management. For example, carriers can develop methods to detect and mitigate theft and abuse of point-of-sale devices and tablets by remotely wiping the devices. Carriers can also implement zero trust architecture concepts in retail stores. To this end, technology providers and developers should also harden their applications and application programing interfaces (APIs) by applying industry best practices for sensitive assets.

The Federal Communications Commission (FCC) and Federal Trade Commission (FTC) should engage in oversight and regulatory activities to standardize best practices and combat SIM swapping within the telecommunications industry. The Board recommends that the FCC and FTC strengthen their oversight and enforcement activities focused on SIM-swapping by encouraging regular reporting by telecommunications providers regarding fraudulent SIM swapping prevalence, documenting and enforcing best practices, and incentivizing better security at telecommunications providers.

The Board also recommends that organizations prioritize resiliency and fast recovery to defend against these kinds of attacks. Planning efforts need to extend to third-party suppliers, including BPOs. Organizations should plan for disruptive cyber intrusions by requiring their whole business (including outside sources) to invest in prevention, detection, response, and recovery capabilities. This includes developing and implementing modern enterprise network architectures, developing and testing a cyber incident response plan, communicating with law enforcement and federal response officials, and conducting after-action reviews on incidents.

Organizations should incorporate cybersecurity requirements into contract language and require that third-party service providers and BPOs adhere to similar standards as the company. Furthermore, BPOs should establish information sharing relationships with their industry peers and the federal government should support the maturation of this approach.

Finally, the Board recommends the advancement of "whole-of-society" programs and mechanisms to prevent juvenile cybercrime. Congress should explore funding juvenile cybercrime prevention programs, fostering interruption and redirection programs, and reducing criminal incentives by exploring ways to ensure continuity between federal and state law enforcement authorities.

METHODOLOGY

The Board engaged with nearly 40 organizations and individuals, including representatives from threat intelligence firms, incident response organizations, targeted organizations, international law enforcement, as well as individual researchers and subject matter experts. The engagements comprised a mixture of interviews and written responses to requests for information, in addition to reviewing publicly available information from approximately 130 unique sources. See Appendix A for a list of participating organizations.

Throughout its review, the Board prioritized the use of primary sources, namely those with first-hand observations such as targeted organizations and threat intelligence subject matter experts. Given the unique nature of how the threat actor groups operated in view of the public, the Board found it appropriate to leverage media coverage and industry blogs, as they provided a valuable archive of perceived attacker movements and events.

The Board is grateful for all the contributions, which helped build the timeline of events, corroborate facts, and develop recommendations. The proceeding sections of the report—Facts, Findings, and Recommendations—detail the attacks and their impact, and offer lessons learned that can be applied to any public or private sector organization (domestic or foreign).

SCOPE OF INQUIRY

Lapsus$ was a loosely organized threat actor group that operated against a backdrop of a broader criminal ecosystem, with which it regularly interacted in a fluid and dynamic way. For this reason, threat intelligence experts experienced challenges consistently attributing particular attacks to specific threat actor groups rather than others. Therefore, the Board opened the aperture of its inquiry and looked at reasonably adjacent attack activity that may be attributed to a broader set of threat actors. Similarly, the Board did not attempt to rectify the conflicting views of experts on threat actor naming conventions nor attempt to conclusively attribute any attacks to Lapsus$, preferring instead to focus on the in-common tactics, techniques, and procedures (TTPs) that would allow companies and individuals to better protect themselves against similar attacks. Accordingly, the report uses the term “threat actors” or "this class of threat actors” to refer to the superset of group activity the Board studied.

WORKING WITH TARGETED ORGANIZATIONS

The Board engaged targeted organizations directly to understand how they approached incident response and post-incident mitigation. The Board selected specific organizations to engage based upon public disclosures the organizations had previously made. Several of these organizations generously shared their insights with the Board, which complemented the information provided by experts, including threat intelligence firms and law enforcement. Although some organizations did not agree to participate in the Board’s review, the Board believes it was able to obtain enough information to conduct a meaningful review and deliver strong recommendations that will have a meaningful impact on the cybersecurity ecosystem.

In conducting this review, the Board remained committed to its Core Principles,[2] namely, conducting an *objective, forward-looking review*. As such, this report does not reference targeted organizations by name unless doing so was specifically approved by that organization or where a public reference such as a news article or indictment was available. This approach is consistent with the President’s National Cyber Strategy, which is rooted in collaboration between industry and government to minimize harm from cyber incidents.

[2] “The Board will utilize its fact-finding mission to facilitate lessons learned and advance the cybersecurity goals of the United States. The Board is not a regulatory body and is not focused on finger-pointing. It will foster a just culture and focus on formulating actionable, realistic, and timely recommendations to better secure the community.” *Source: CISA, CSRB, https://www.cisa.gov/csrb*

1. FACTS

Lapsus$ emerged in 2021 within a broad ecosystem of cybercriminal activity, conducting extortion-focused attacks against a wide range of targets. The group gained notoriety because it successfully attacked well-defended organizations using highly effective social engineering; targeted supply chains by compromising business process outsourcing (BPOs) and telecommunications providers; and used its public Telegram channel to discuss its operations, targets, and successes, and even to communicate with and extort its targets.

1.1. THE THREAT ACTORS

Lapsus$ was a transnational group[3] of threat actors based mainly in the United Kingdom (U.K.) and Brazil,[4] with 8 to 10 known members as of April 2022.[5] By some accounts, it formed out of members from two earlier cybercriminal groups known as Cyberteam[6] and Recursion Team.[7] Consistent with the group's own statements,[8] the Cyber Safety Review Board (CSRB, or the Board) received no evidence suggesting Lapsus$ was affiliated with a nation-state or political entity. In general, the threat intelligence community first observed and tracked Lapsus$ as a named group between September and December 2021, which is when the group first posted on its public Telegram channel and attacked South American targets before pivoting to infiltrate many well-known international companies.[9, 10] However, some researchers identified individuals using the Lapsus$ moniker in forums to claim credit for alleged attacks as early as June 2021,[11, 12] indicating that the group or its members may have been active prior to the fall. Additionally, security researchers observed suspected Lapsus$ Telegram activity in March 2022 when a channel belonging to another extortion group reposted content from the official Lapsus$ Telegram channel.[13] However, confirmation of Lapsus$ involvement was not verified, and the Board saw no other apparent connection between the two groups.

Although Lapsus$ as a named group does not appear to be active at the time of this report,[14] the Board cannot rule out the possibility that Lapsus$ members and affiliates have decided to limit their public profile, join other cybercrime groups, or rebrand.[15] As the Board cannot be definitive about the current existence of Lapsus$, for simplicity, this report refers to Lapsus$ in the past tense.

Lapsus$ operated against the backdrop of a dynamic ecosystem of threat actors, each having specific tactics, preferring certain target sectors, malware, or methodology. Within this threat ecosystem, Lapsus$ emerged with different approaches to targeting, credential theft, and direct interaction with the public. For example, Lapsus$ used its private and public Telegram channels as a primary communication platform for operational coordination and

[3] Blackberry, "*LAPSUS$ Group*," 2023, https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/lapsus

[4] Tills, Claire; Tenable, "*Brazen, Unsophisticated and Illogical: Understanding the LAPSUS$ Extortion Group*," July 20, 2022, https://www.tenable.com/blog/brazen-unsophisticated-and-illogical-understanding-the-lapsus-extortion-group

[5] Cybersecurity Company, CSRB Meeting.

[6] Cyberteam is broadly considered by researchers to be a Portuguese-speaking group (possibly pay-for-hire) active roughly 2015-2020 that conducted doxing operations against politicians, distributed denial-of-service (DDoS) attacks and defacement in Brazil. *Source: Intrinsec, "Analysis of Lapsus$ Intrusion Set," March 28, 2022, https://www.intrinsec.com/wp-content/uploads/2022/03/INTRINSEC-LAPSUS-Intrusion-Set-20220324.pdf*

[7] Also known as Infinity Recursion Team in some forums. This group formed in 2021 and specialized in SIM Swaps, swatting, abusing Emergency Disclosure Requests, and attacks that involved knowledge of software development and penetration testing skills. *Source: Krebs, Brian; KrebsonSecurity, "Hackers Gaining Power of Subpoena Via Fake 'Emergency Data Requests,'" March 29, 2022, https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests*

[8] Tills, Claire; Tenable, "*Brazen, Unsophisticated and Illogical: Understanding the LAPSUS$ Extortion Group*," July 20, 2022, https://www.tenable.com/blog/brazen-unsophisticated-and-illogical-understanding-the-lapsus-extortion-group

[9] FBI, CSRB Meeting.

[10] Cybersecurity Company, CSRB Meeting.

[11] Security Researcher 1, CSRB Meeting.

[12] Cybersecurity Company, CSRB Meeting.

[13] Cybersecurity Company, Response to CSRB Request for Information.

[14] At the time of writing, the Board understood the last observed message on the Lapsus$ public Telegram channel was dated March 30, 2022 and directed followers to an alternate platform for future communication. *Source: Cybersecurity Company, Response to CSRB Request for Information.*

[15] FBI, Response to CSRB Request for Information.

engagement with its tens of thousands of followers, sharing efforts to recruit insiders at target companies, announcing its attacks, and taking polls on whom to target next.[16, 17, 18]

Security researchers have faced challenges delineating Lapsus$ activity from that of other threat actor groups. The relative commonality of their attack techniques and the connections between Lapsus$ members and those in other threat actor groups have resulted in fragmented threat intelligence reporting and attribution.[19] Some of these groups have provable ties to one another,[20] but the specifics of any individual relationships are difficult to determine. Due to the fluid and overlapping nature of observed activity, the Board increased the aperture of study, and thusly, this report also includes some activities attributed by experts to other threat groups, including those named below.

- **Yanluowang:** Broadly identified as a ransomware affiliate group that is reported to have some connection with Lapsus$ members.[21] The group was active as of August 2021 and targeted organizations in the financial, manufacturing, information technology (IT), consultancy, and engineering sectors.[22]
- **Oktapus or Roasted Oktapus:** A financially motivated group that is focused on accessing corporate services, obtaining crypto-related account information,[23] and stealing source code.[24]
- **Karakurt:** A data extortion group[25] known for operating a dedicated leak site to auction stolen data.[26]
- **Nwgen Team:** A financially motivated group that split off from Lapsus$ mid-2022 and blended its original tradecraft with additional use of ransomware.[27]
- **#NotLapsus:** Two other unidentified groups, #NotLapsus1 and #NotLapsus2, which have successful alliances with Lapsus$ members and other cybercriminals, such as Yanluowang.[28]

This report uses the term “threat actors” or "this class of threat actors” to refer to this superset of group activity the Board studied, referring specifically by name to any one group only where relevant.

1.1.1. Motivation

Many security researchers attribute the primary motive of the broader set of threat actors studied for this report as financial in nature, based on observed activity that involved selling stolen data on underground criminal markets,[29] use

[16] Cybersecurity Company, Response to CSRB Request for Information.
[17] Cybersecurity Company, Response to CSRB Request for Information.
[18] The use of Telegram to directly communicate with its followers in such a public way is a unique hallmark of Lapsus. Source: ReliaQuest, “Meet Lapsus$: An Unusual Group in the Cyber Extortion Business,” March 17, 2022, https://www.reliaquest.com/blog/meet-lapsus-an-unusual-group-in-the-cyber-extortion-business
[19] Cybersecurity Company, CSRB Meeting.
[20] Biasini, Nick; Cisco Talos, “*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*,” August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack
[21] Cybersecurity Company, CSRB Meeting.
[22] Threat Hunter Team; Symantec, “*Yanluowang: Further Insights on New Ransomware Threat*,” November 30, 2021, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-ransomware-attacks-continue
[23] Mirkasymov, Rustam and Martinez, Roberto; Group-IB, “*Roasting Oktapus: The phishing campaign going after Okta identity credentials*,” August 25, 2022, https://www.group-ib.com/blog/Oktapus
[24] Cybersecurity Company, CSRB Meeting.
[25] CISA, “*Cybersecurity Advisory: Karakurt Data Extortion Group*,” June 2, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a
[26] Greig, Jonathan; Recorded Future, “*US Agencies: Karakurt extortion group demanding up to $13 million in attacks*,” May 31, 2022, https://www.therecord.media/us-agencies-karakurt-extortion-group-demanding-up-to-13-million-in-attacks
[27] Technology Company, CSRB Meeting.
[28] Cybersecurity Company, Response to CSRB Request for Information.
[29] Office of Public Affairs; DOJ, “*Criminal Marketplace Disrupted in International Cyber Operation*,” April 5, 2023, https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation

of extortion and ransomware to coerce money out of targeted organizations,[30] theft of cryptocurrency,[31] and even cryptocurrency mining in a few cases.[32]

However, researchers hold a diverse range of opinions on Lapsus$'s motivations. While the group claimed publicly that its only motivation was profit, other plausible motivations appear to include notoriety, amusement, and ideology.[33, 34] Security researchers noted that successfully attacking highly visible targets, including publicly shaming them, generally enabled Lapsus$ to expand its reputation and credibility in the cybercriminal environment.[35] At the same time, Lapsus$'s activity in many of these attacks was consistent with ideological motives. For example, publicly visible chats suggest radical opposition to Brazilian health policies during the Coronavirus Disease 2019 (COVID-19) pandemic, which may explain targeting of the Brazilian Ministry of Health in December 2021.[36] The Board did not receive information determining whether these possible differences in motivation were due to the interests of different group members or individual members conducting independent campaigns attributed to the whole group.

1.2. TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

The threat actors described in this report leveraged a wide diversity of tactics, techniques, and procedures (TTPs), described by researchers as often mixing both non-complex methods and tools with advanced technical knowledge.[37, 38] The threat actors initiated some attacks by employing common phishing methods or leveraging stolen credentials, which they purchased from initial access brokers (IABs).[39] Other attacks demonstrated a deeper familiarity with a target's business and engineering workflows.[40]

Generally, the threat actors did not deploy custom tools, preferring well-known tools built by others[41] or "living off the land" (LOTL).[42] The speed of the attacks and the use of different tools and techniques were notable and, in some cases, appeared automated.[43]

The following sections outline some of the notable TTPs threat actors used as they worked across the aggregated set of targeted entities and are provided here to support the findings and recommendations below. Where possible, descriptions of attack techniques are aligned to the MITRE ATT&CK® Framework taxonomy.[44]

1.2.1. Reconnaissance and Resource Development

The Reconnaissance and Resource Development stages of an attack involve activities such as gathering intelligence and information about a target system or network, then establishing resources to support operations.

[30] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack

[31] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

[32] Cybersecurity Company, CSRB Meeting.

[33] Cybersecurity Company, Response to CSRB Request for Information.

[34] Cybersecurity Company, CSRB Meeting.

[35] ReliaQuest, "*Team A vs Team B: What is Motivating Lapsus$*" April 6, 2022, https://www.reliaquest.com/blog/team-a-vs-team-b-what-is-motivating-lapsus

[36] Intrinsec, "*Analysis of Lapsus$ Intrusion Set*," March 28, 2022, https://www.intrinsec.com/wp-content/uploads/2022/03/INTRINSEC-LAPSUS-Intrusion-Set-20220324.pdf

[37] Cybersecurity Company, CSRB Meeting.

[38] Cybersecurity Company, Response to CSRB Request for Information.

[39] Cybersecurity Company, CSRB Meeting.

[40] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

[41] Cybersecurity Company, CSRB Meeting.

[42] LOTL is a technique where the cybercriminal uses native, legitimate tools within the victim's system to sustain and advance an attack. Threat actor presence in a targeted system may remain undetected for extended periods of time as security tools traditionally identify known malware scripts and files. *Source: CrowdStrike, "What Are Living Off the Land (LOTL) Attacks?" February 22, 2023, https://www.crowdstrike.com/cybersecurity-101/living-off-the-land-attacks-lotl*

[43] Cybersecurity Company, CSRB Meeting.

[44] The MITRE Corporation, "*ATT&CK*," April 25, 2023, https://attack.mitre.org

The threat actors used a variety of well-understood research methods on targets of interest to identify weaknesses that they could exploit. For example, they used social engineering to increase their understanding of a target's business operations, including information about personnel, structure, and crisis response procedures.[45] They also probed networks using standard penetration testing methods, such as port scanning, to find vulnerable external services.[46] Evidence also suggests that the threat actors solicited login credentials on underground criminal forums and, in the case of Lapsus$, this also occurred in its public Telegram channel.[47, 48]

Attacker Infrastructure

The threat actors used a variety of systems to launch and control their attacks, which included infrastructure for command-and-control (C2) servers and destination points for exfiltrated data.[49, 50] Some of the threat groups used dedicated cloud infrastructure from known virtual service providers (VSPs), enabling the group to stage, launch, and execute an operation rapidly.[51] In some cases, threat actors reused infrastructure across multiple targeted organizations, including Internet Protocol (IP) addresses and server-side components like web shells,[52, 53] making attribution tracking across intrusions more straightforward. Threat researchers understand these tactics well; the threat actors did not appear to introduce any novel capabilities in this regard.

To mask its attack traffic, the threat group attempted to use anonymization services like Tor to connect to targeted networks, but then in some instances established new virtual private network (VPN) sessions through residential IP addresses to appear less suspicious.[54] Commercial VPN services such as NordVPN served a similar purpose by allowing the threat actors to select servers in similar geographic locations to their targets to avoid security detections such as "impossible travel" signals (activity from disparate locations between which travel in a given timeframe is humanly impossible).[55, 56, 57]

Emergency Disclosure Request (EDR) Abuse

Several of the threat actors studied for this report, and in particular some members of Lapsus$, used fraudulent Emergency Disclosure Requests (EDRs) to obtain sensitive information about targets that could be used to develop extortion attacks against targeted individuals, for example by taking over their online accounts to access personal photos. The use of fraudulent EDRs for this purpose is a known tactic, although it is still a relatively recent development in the criminal underground.[58] Underlining the scope of this issue, the Board learned that security researchers are tracking at least 112 domains, including those belonging to international law enforcement agencies, that attackers have used to disseminate fraudulent EDRs.[59]

[45] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction
[46] Cybersecurity Company, CSRB Meeting.
[47] Cybersecurity Company, Response to CSRB Request for Information.
[48] Cybersecurity Company, Response to CSRB Request for Information.
[49] Cybersecurity Company, CSRB Meeting.
[50] Cisco provided an exemplary outline of typical attacker infrastructure by this class of threat actor. Source: Biasini, Nick; Cisco Talos, "Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack
[51] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction
[52] Cybersecurity Company, CSRB Meeting.
[53] Cybersecurity Company, CSRB Meeting.
[54] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack
[55] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction
[56] Ackerman, Devon et al.; Kroll, "*MFA Prompt Bombing No More: Countering MFA Bypass Tactics*," May 23, 2022, https://www.kroll.com/en/insights/publications/cyber/mfa-prompt-bombing-no-more
[57] Think Technology Australia, "*Impossible Travel in Microsoft Office 365: Explained*" November 23, 2021, https://www.thinktechnology.com.au/blog/impossible-travel-in-microsoft-office-365-explained
[58] Security Researcher 2, CSRB Meeting.
[59] Security Researcher 2, CSRB Meeting.

Fraudulent EDRs

18 United States Code (U.S.C.) § 2702 enables service providers to immediately respond to governmental entity requests of an emergency nature, i.e., EDRs, to address immediate life-safety issues in the interest of the public. Governmental entities make these requests directly to service providers, which detail their procedures for receiving requests on their website.[60] Providers may also decide to divulge records if they learn about an emergency through another source, such as a concerned parent. Attackers can exploit this method of requesting data to create fake requests by impersonating law enforcement agents and other requestors, for example by embedding official police logos and crests into their requests.[61]

1.2.2. Use of Supply Chain Attacks

Many of the threat actors covered in this study extensively exploited the trust relationships between third-party service providers and their clients or customers to develop attacks against the downstream entity.[62, 63, 64] Since 2019, the Federal Bureau of Investigation (FBI) has observed a wide variety of threat actor groups targeting suppliers in this way.[65] The Board saw discernable patterns in the targeting of three specific sectors for this purpose: BPOs; telecommunications providers; and software as a service (SaaS) providers.

Business Process Outsourcing Companies (BPOs)

BPOs are involved in providing scaled operations to organizations, operating as a third-party supplier, which enables their clients to focus on core competencies while gaining overall cost efficiencies.[66] These services may include extended workforce staffing for customer and technical support, data entry, security services, software development, and many others. Due to their role in their clients' business, and the access required to carry out the necessary operations, BPOs are an attractive consolidation point for threat actors looking to compromise multiple downstream targeted organizations.[67] The threat actors outlined in this report targeted multiple BPOs in this way.

Telecommunications Providers

Telecommunications providers, and in particular mobile phone operators, provide critical infrastructure for the nation, and in recent years have become pivotal in the adoption of multi-factor authentication (MFA) by facilitating the delivery of one-time passcodes (OTPs) via Short Message Service (SMS) and voice calls. The threat actors outlined in this report made use of compromised access to telecommunications provider infrastructure, business processes, and accounts to hijack these OTPs.[68]

Third-Party Service Providers

While the use of third-party service providers, such as SaaS, in enterprise has grown in popularity,[69] the federation of enterprise data and capabilities into these cloud-based platforms comes with security risks that industry may not

[60] For example, see the procedures for Microsoft, Google, Twilio, and Meta: Microsoft; "*Law Enforcement Requests Report*," https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report; Google, "*How Google handles government requests for user information*," https://policies.google.com/terms/information-requests; Twilio, "*Law Enforcement Requests Guidelines*," https://www.twilio.com/en-us/legal/law-enforcement-guidelines; Meta, "*Law Enforcement*," https://about.meta.com/actions/safety/audiences/law

[61] FBI, CSRB Meeting.

[62] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies

[63] Targeted Organization, CSRB Meeting.

[64] Technology Company, CSRB Meeting.

[65] FBI, CSRB Meeting.

[66] CFI Team; Corporate Financial Institute, "*Business Process Outsourcing (BPO)*" June 28, 2023, https://www.corporatefinanceinstitute.com/resources/management/business-process-outsourcing-bpo

[67] Security Researcher 2, CSRB Meeting.

[68] Krebs, Brian; KrebsonSecurity, "*Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code*," April 22, 2022, https://www.krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code

[69] One study suggests that the SaaS market will grow 250% by 2030. Source: Fortune Business Insights, "Market Research Report: Software as a Service (SaaS) Market Size, Share & COVID-19 Impact Analysis, 2023-2030," June 2023, https://www.fortunebusinessinsights.com/software-as-a-service-saas-market-102222

always manage.[70] The threat actors studied for this report are aware of the third-party service provider business trends and the relationship those providers have with their customers, and exploited those partnerships to gain access to their customer data and systems.

Case Study in Supply Chain Attacks
In January 2022, a threat actor studied for this report gained access to privileged internal tools of a third-party service provider by compromising the computer of a customer support contractor from one of its BPOs. The real target of this attack was not the third-party service provider, nor the BPO, but rather the downstream customers of the service provider itself. This is a remarkable example of a creative three-stage supply chain attack used by this class of threat actors.[71]

1.2.3. Initial Access

The initial access stages of an attack provide an attacker with a foothold through which they can facilitate further activity. This may involve a variety of techniques to compromise systems, software, identities, or network access.

Social Engineering

Social engineering was used extensively, and creatively, by most of the threat actors to gain initial access to their targets. The ability to effectively leverage direct contact with employees throughout the lifecycle of the attack, using a wide range of techniques, and in multiple languages, was a hallmark of this class of threat actor.[72] Some characterizations and examples are provided below for illustration.

- Threat actors used publicly available data about targets, including employee profile pictures, department structures, business processes, workflows, and business relationships, to impersonate legitimate personnel.[73]
- Threat actors used spear-phishing that had target employees visit spoofed or hacked websites. These sites tricked employees and contractors into entering their usernames and passwords into the attacker-controlled website.[74] In other cases, these websites were backed by toolkits such as Evilginx2 that passively stole login credentials and session tokens.[75]
- Threat actors used voice phishing (vishing) to impersonate a trusted entity over voice. Information gathered during the reconnaissance phase of the attack, including answers to security questions, helped threat actors to convince support desk employees to reset account credentials over the phone.[76]
- Threat actors used SMS phishing (smishing) to deliver instructions or website links via SMS to a victim's phone. These messages often contained links to seemingly legitimate domains, such as a similar website address, containing user login fields but were instead used by threat actors to harvest user credentials.[77]

[70] Preci, Ejona and Gregory, Peter; ISACA, "*SaaS Security Risk and Challenges*," July 26, 2022, https://www.isaca.org/resources/news-and-trends/industry-news/2022/saas-security-risk-and-challenges

[71] Bradbury, David; Okta, "*Okta Concludes its Investigation into the January 2022 Compromise*," April 19, 2022, https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise

[72] Intrinsec, "*Analysis of Lapsus$ Intrusion Set*," March 28, 2022, https://www.intrinsec.com/wp-content/uploads/2022/03/INTRINSEC-LAPSUS-Intrusion-Set-20220324.pdf

[73] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

[74] Research & Insights Center; SecurityScorecard, "*Lapsus$ Update: How This Technically Unsophisticated Threat Actor Group Breaches Large Organizations*," January 9, 2023, https://www.securityscorecard.com/research/lapsus-update

[75] Cybersecurity Company, CSRB Meeting.

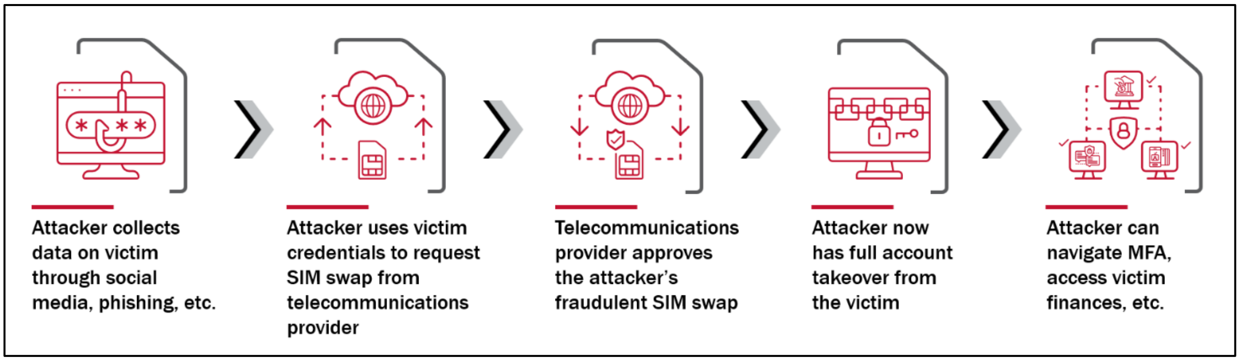
[76] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

[77] Security; Twilio, "*Incident Report: Employee and Customer Account Compromise*," October 27, 2022, https://www.twilio.com/blog/august-2022-social-engineering-attack

- Threat actors used MFA fatigue, spamming employees with MFA prompts with the goal of overwhelming them with access approval requests until they said yes. Sometimes these prompts occurred late at night, or during inconvenient times,[78] possibly to increase the likelihood of the employee accepting the prompt.
- In a few cases, the threat actor impersonated help desk personnel over direct chat messages and encouraged employees to approve the MFA prompts.[79]
- Threat actors convinced employees to navigate to credential-harvesting websites or download remote monitoring and management (RMM) tools, allowing the threat actor to remotely connect and control the target's system.[80]

Hijacking Delivery of Multi-Factor Authentication (MFA) Passcodes

During its research, the Board heard about threat actors' ability to exploit SMS and voice MFA through fraudulent Subscriber Identity Module (SIM) swaps, as depicted in Figure 1. SIM swapping, a generally benign business process that enables mobile phone customers to switch their phone number to new devices was especially pertinent to this review. Threat actors can abuse this business process to fraudulently activate an attacker-controlled SIM with the victim's phone number. This enables the threat actor to intercept SMS and voice calls and receive MFA-related messages that control access to online accounts.[81]



Attacker collects data on victim through social media, phishing, etc.

Attacker uses victim credentials to request SIM swap from telecommunications provider

Telecommunications provider approves the attacker's fraudulent SIM swap

Attacker now has full account takeover from the victim

Attacker can navigate MFA, access victim finances, etc.

Figure 1 - Example of a Fraudulent SIM Swap

To execute fraudulent SIM swaps, Lapsus$ obtained basic information about its victims, such as their name, phone number, and customer proprietary network information (CPNI). Lapsus$ learned the information through a variety of ways, including issuing fraudulent EDRs and using account takeover techniques, to hijack the accounts of telecommunications provider employees and contractors. It then performed fraudulent SIM swaps via the telecommunications provider's customer management tools.[82, 83] After executing the fraudulent SIM swaps, Lapsus$ took over online accounts via sign-in and account recovery workflows that sent one-time links or MFA passcodes via SMS or voice calls.[84, 85]

[78] FBI, CSRB Meeting.

[79] Cybersecurity Company, Response to CSRB Request for Information.

[80] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies

[81] FBI, "Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public," February 8, 2022, https://www.ic3.gov/Media/Y2022/PSA220208

[82] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies

[83] KrebsonSecurity, "*A Closer Look at the LAPSUS$ Data Extortion Group*," March 23, 2022, https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/

[84] Bonifacic, Igor; Engadget, "*Lapsus$ stole T-Mobile's source code before member arrests in March*," April 23, 2022, https://www.engadget.com/lapsus-t-mobile-source-code-185950839.html

[85] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

Impact of Fraudulent SIM Swaps on National Security

Threat actor groups persistently targeted telecommunications providers of United States (U.S.) federal employees to gain access to internal tools that would enable convenient SIM swapping (for hijacking MFA pass codes). In one case Lapsus$ targeted one U.S. telecommunications providers and attempted to use this illegitimate access to compromise mobile phone accounts associated with FBI and Department of Defense (DOD) personnel.[86] This was unsuccessful due to extra protections on these accounts. While the Board did not learn of any nexus between this particular threat actor group and nation-state threat actors, the tactics and techniques shown here would be easily adaptable for any threat actor wishing to target U.S. national security interests.

Insider Recruitment

Some of the threat actors used monetary incentives to recruit employees and contractors of targeted organizations, who then took actions on behalf of the threat actors. This included handing over access credentials to the threat actor, approving upstream MFA requests, and performing actions directly for the attacker using their internal company access. Lapsus$ posted advertisements offering sums of money for access to targeted systems. For access to several telecommunications providers, the group offered as much as United States Dollars (USD) 20,000 per week to conduct SIM swaps.[87, 88]

Vulnerability Exploitation to Gain Initial Access

A limited set of the threat actors exploited known software and configuration vulnerabilities to gain initial access. As threat actors discovered potential vulnerabilities and identified targets using tools such as Shodan,[89, 90] they sometimes circulated the information in online forums, allowing several additional threat actors to take advantage of the exposure. All the observed vulnerabilities during this study were well known, with patched software available; security researchers observed no use of novel or "zero-day" vulnerabilities.[91, 92] Some notable examples of these vulnerabilities are provided below for illustrative purposes.

- Exploitation of a vulnerability in ForgeRock OpenAM (Common Vulnerability and Exposure [CVE]-2021-35464) allowed a threat actor to get initial access and elevate privileges within the victim cloud environment.[93]
- Exploitation of a well-known vulnerability in WSO2 servers (CVE-2022-29464) enabled one of the threat actors to upload its tools and web shells to a targeted server to establish persistence.[94, 95]

Initial Access Brokers (IABs)

IABs are part of a broader criminal ecosystem involved in the theft and sale of access to targeted networks ("access as a service"). They use a variety of techniques to obtain this access, including those outlined in this report: social engineering; recruiting insiders; malware ("malware as a service"); scanning for open remote services with guessable passwords; exploiting vulnerabilities; and selling password database dumps from breaches. IABs obtain access, for

[86] Evidence for this comes from screenshots taken by the threat actors and shared privately between themselves. These private chats were observed by a journalist and reported in publication. The Board chose to include this specific article as part of overall review of the facts, as it provided deeper insight into how Lapsus$ operated. *Source: Krebs, Brian; Krebs on Security, "Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code," April 22, 2022, https://www.krebsonsecurity.com/2022/04/leaked-chats-show-lapsus-stole-t-mobile-source-code*
[87] Cybersecurity Company, Response to CSRB Request for Information.
[88] Krebs, Brian; Krebs on Security, "*A Closer Look at the LAPSUS$ Data Extortion Group*," March 23, 2022, https://www.krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group
[89] Shodan is a search engine that queries and indexes publicly available information about all devices connected to the internet. *Source: Shodan, "What is Shodan?" https://help.shodan.io/the-basics/what-is-shodan*
[90] Cybersecurity Company, CSRB Meeting.
[91] Intrinsec, "*Analysis of Lapsus$ Intrusion Set*," March 28, 2022, https://www.intrinsec.com/wp-content/uploads/2022/03/INTRINSEC-LAPSUS-Intrusion-Set-20220324.pdf
[92] Targeted Organization, CSRB Meeting.
[93] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies
[94] MITRE, "*CVE-2022-29464*," April 18, 2022, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29464
[95] Cybersecurity Company, CSRB Meeting.

example via an affiliate model, and then sell it in online forums.[96] The threat actors studied in this report leveraged IABs in some cases to gain access to targeted networks, including paying with cryptocurrency that had been stolen or extorted from other targets.

1.2.4. Privilege Escalation, Lateral Movement, Persistence

Once an attacker has initial access to a system, the foothold is typically used to elevate privileges, laterally move to desired areas of a victim's systems, and establish long-term access (persistence).

To perform reconnaissance of the network and facilitate privileged access, the threat actors exploited the tendency for enterprises and their employees to document internal procedures, share information on collaboration platforms, and use ticketing systems to perform internal help desk operations. In some cases, they impersonated employees, including help desk and administrator personnel, and conducted social engineering attacks. They scanned systems, searched information repositories, and exploited vulnerabilities to raise privileges.[97, 98] An overview of some notable techniques is outlined in the sections below.

Privilege Escalation via Improperly Stored Passwords and Keys

A prevalent method of escalating privilege seen across the organizations involved the threat actors searching for, and exploiting, situations where the organization had improperly secured credentials. This enabled them to use legitimate credentials to further their attack goals, which had the added benefit of appearing to be legitimate user behavior in the forensic record. Examples included:

- administrative passwords documented in a spreadsheet;[99]
- Amazon Web Services (AWS) access keys stored in Slack;[100]
- sensitive data stored in collaborative platforms, code repositories, and communication channels;[101]
- processes for accessing source code stored in enterprise knowledge shares;[102]
- privileged credentials embedded in a PowerShell script, stored on a misconfigured network share;[103] and
- credentials from password databases, browser password caches, and keychains.[104, 105]

Privilege Escalation and Lateral Movement using Common Tools

The threat actors leveraged initial and privileged access to further elevate access and laterally move to other systems. A mix of system utilities, diagnostic extensions, administrative databases, and malicious tools was used.[106, 107] The

[96] An overview on Initial Access Brokers can be found at: Center for Internet Security, "*Initial Access Brokers How They're Changing Cybercrime*," January 18, 2023, https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime

[97] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack

[98] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies

[99] Whittaker, Zack; TechCrunch, "*Lapsus$ found a spreadsheet of accounts as they breached Okta, documents show*," March 28, 2022, https://www.techcrunch.com/2022/03/28/lapsus-passwords-okta-breach

[100] Porter, John and Byford, Sam; The Verge, "*Okta hack puts thousands of businesses on high alert*," March 22, 2022, https://www.theverge.com/2022/3/22/22990637/okta-breach-single-sign-on-lapsus-hacker-group

[101] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

[102] Targeted Organization, CSRB Meeting.

[103] CyberArk Blog Team; CyberArk, "*Unpacking the Uber Breach*," September 20, 2022, https://www.cyberark.com/resources/pam-self-hosted/unpacking-the-uber-breach

[104] Targeted Organization, CSRB Meeting.

[105] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack

[106] Mandiant Intelligence; Mandiant, "*SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack*," May 16, 2023, https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial

[107] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack

following is not an exhaustive list of all techniques used across the threat actor groups but is a representative sample to show the extensive understanding of post-compromise exploitation techniques known to this threat actor community. Examples included:

- deploying credential dumping using tools such as MiniDump and Impacket, as well as other offensive security tools like Cobalt Strike, PowerSploit,[108] Metasploit,[109] and LinPEAS;[110, 111]
- abusing Windows "ntdsutil.exe" utility to dump NT Directory Services (NTDS),[112] a Windows credential database, to extract credentials used in the targeted environment, and administrative tools like RustScan[113] and AdFind;[114]
- leveraging internal communication channels, such as internal Slack, to impersonate employees and conduct internal social engineering attacks;[115]
- using built-in cloud diagnostic extensions to back up virtual machines (VMs) and collect logs from systems;[116] and
- using compromised AWS tokens to request and assume permissions of an instance role and creating temporary credentials for non-existent users with open source cloud management tools like AWS_consoler.[117]

Privilege Escalation by Exploiting Vulnerabilities

In some cases, the threat actors leveraged well-known vulnerabilities to elevate privileges in critical systems. Examples include:

- exploiting unpatched vulnerabilities in Microsoft's Active Directory (AD);[118] specific to Lapsus$, an estimated 40-60% of compromises involved exploitation of AD;[119]
- exploiting Microsoft Exchange Servers using ProxyShell attacks, which leverage three known CVEs: CVE-2021-34473; CVE-2021-34523; and CVE-2021-31207;[120, 121]

[108] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack

[109] Intrinsec, "*Analysis of Lapsus$ Intrusion Set*," March 28, 2022, https://www.intrinsec.com/wp-content/uploads/2022/03/INTRINSEC-LAPSUS-Intrusion-Set-20220324.pdf

[110] LinPEAS is a script that searches for privilege escalation paths on Linux, Unix, and MacOS hosts. Source: Polos, Carlos; GitHub, "LinPEAS – Linux Privilege Escalation Awesome Script," August 7, 2020, https://www.github.com/carlospolop/PEASS-ng/tree/master/linPEAS

[111] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies

[112] Windows NTDS, specifically the "NTDS.dit" file, is a database that stores all AD data, including password hashes for all users of a domain. *Source: Warren, Jeff; Netwrix, "Extracting Password Hashes from the Ntds.dit File," November 30, 2021 (updated March 17, 2023), https://blog.netwrix.com/2021/11/30/extracting-password-hashes-from-the-ntds-dit-file*

[113] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies

[114] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack

[115] Targeted Organization, CSRB Meeting.

[116] Mandiant Intelligence; Mandiant, "*SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack*," May 16, 2023, https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial

[117] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies

[118] AD is a directory service that stores information about user accounts, shared infrastructure resources, and computer accounts in a Windows domain network, allowing administrators to manage authentication and authorization controls. *Source: Microsoft, "Active Directory Domain Services Overview," August 16, 2022, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview*

[119] Cybersecurity Company, CSRB Meeting.

[120] Cybersecurity Company, CSRB Meeting.

[121] Sanchez, Adrian et al.; Mandiant, "*PST, Want a Shell? ProxyShell Exploiting Microsoft Exchange Servers*," September 2, 2021, https://www.mandiant.com/resources/blog/pst-want-shell-proxyshell-exploiting-microsoft-exchange-servers

- exploiting vulnerabilities against Windows User Profile Service to escalate local privileges, including CVE-2021-34484[122] and CVE-2022-21919;[123]
- leveraging lateral movement techniques to abuse weaknesses in Windows environments with hashed credentials, such as pass-the-hash attacks;[124, 125] and
- exploiting vulnerabilities in Confluence, JIRA, and GitLab to obtain privileged access to information.[126]

Persistence via Threat Actor-Added Resources

The threat actors created and maintained access and administrative privileges by adding their own accounts and devices to the targeted organization's environment. Examples include:

- adding an administrator account using the built-in Windows "net.exe," then adding it to the local Administrators group;[127]
- registering attacker-controlled devices for MFA and modifying settings to possibly disable or register their own MFA during an intrusion;[128] and
- creating new accounts within the target's cloud infrastructure.[129]

Persistence via Legitimate and Malicious Remote Access Tools

Some of the threat actors established persistence in the targeted environment for ongoing access, but this was not a consistent practice across all groups. Methods included the use of legitimate utilities, remote access administration tools, and malware. Some threat actors had access to more advanced toolkits than others. The following is not an exhaustive list, but the examples cited below show the breadth of capability generally available to this threat actor community. Examples include:

- using stolen employee credentials to log into virtual desktop infrastructure (VDI) environments such as Citrix;[130]
- deploying reverse Secure Shell Protocol (SSH) tunnels to establish communication with an attacker controlled C2 server;[131]
- leveraging reverse proxy tools, including rsocx[132] and ngrok;[133]

[122] Cybersecurity Company, Response to CSRB Request for Information.
[123] Cybersecurity Company, Response to CSRB Request for Information.
[124] CrowdStrike, "*PASS-THE-HASH ATTACK*," May 18, 2022, https://www.crowdstrike.com/cybersecurity-101/pass-the-hash
[125] Cybersecurity Company, CSRB Meeting.
[126] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction
[127] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack
[128] Cybersecurity Company, CSRB Meeting.
[129] Cybersecurity Company, CSRB Meeting.
[130] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction
[131] Mandiant Intelligence; Mandiant, "*SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack*," May 16, 2023, https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial
[132] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies
[133] Cybersecurity Company, CSRB Meeting.

- installing or using stolen employee credentials to log into a target's RMM tools like RealVNC,[134] Remote Desktop Protocol (RDP), ManageEngine, AnyDesk, LogMeIn, TeamViewer, and ThinScale;[135, 136]
- implanting simple backdoors via commands sent in JavaScript Object Notation (JSON) that communicated via Hypertext Transfer Protocol (HTTP);[137] and
- deploying malicious Remote Access Trojans (RATs) such as Quasar RAT.[138]

Disabling Security Monitoring Tools

Several threat actors studied for this report intentionally bypassed or disabled usage of enterprise security solutions to either hide their presence or facilitate further access. Some notable examples are that threat actors:

- used "Bring Your Own Vulnerable Driver" (BYOVD) attacks to deploy malicious kernel drivers signed by stolen code-signing certificates (obtained from another targeted entity) to bypass security detection and disable security controls;[139]
- modified the host firewall, for example to allow RDP connections;[140] and
- used a Unified Extensible Firmware Interface (UEFI) bootkit called "BlackLotus."[141]

1.3. IMPACT

The threat actors stole proprietary data, extorted organizations, disrupted services, and harassed individuals. Due to the dynamic and ongoing nature of the attacks described in this report, and the threat actors' ongoing extended influence and impact within the broader criminal ecosystem, quantifying the impact of their attacks with a high level of specificity is difficult. The sections below provide examples of some of the identifiable impacts that these attacks had on organizations and their employees and customers.

1.3.1. Data Compromise and Theft

In many instances, attackers compromised and stole data that would be most useful to them for extortion, ransom, or harassment purposes, or to sell later on criminal forums. This included intellectual property for marquis high-profile software products, user data, and other data types that were leveraged in further attacks. However, in some cases, attacks appeared to reflect a "smash-and-grab" approach that seemed to prioritize speed over strategy and sometimes

[134] Cybersecurity Company, Response to CSRB Request for Information.
[135] Parisi, Tim; CrowdStrike, "*Not a SIMulation: CrowdStrike Investigations Reveal Intrusion Campaign Targeting Telco and BPO Companies*," December 2, 2022, https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies
[136] BeyondTrust, "*Lapsus$ Breaches Remind us Service Desks & Insiders often Weakest Link*," March 29, 2022, https://www.beyondtrust.com/blog/entry/lapsus-breaches-remind-us-service-desks-insiders-often-weakest-link
[137] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack
[138] Research & Insights Center; SecurityScorecard, "*Lapsus$ Update: How This Technically Unsophisticated Threat Actor Group Breaches Large Organizations*," January 9, 2023, https://www.securityscorecard.com/research/lapsus-update
[139] Code-signing certificates are used to establish the legitimate creator and distributor of software. By signing malware with a stolen code-signing certificate, the code can appear as legitimate to the system and any security related software. In this instance the, signed malware was used in combination with CVE-2015-2291 to "use the privileged driver space provided by the vulnerable Intel driver to overwrite specific routines in the CrowdStrike Falcon sensor driver with adversary-created trampoline code." CrowdStrike also observed threat actors using this technique to bypass other endpoint tools. *Source: Intelligence Team; CrowdStrike, "SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security," January 10, 2023, https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic*
[140] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack
[141] Cybersecurity Company, CSRB Meeting.

missed opportunities to extract higher-value data, with at least one instance of attackers losing their access by publicly claiming access, allowing the victim company to respond and disrupt exfiltration of the data.[142, 143]

The following examples enumerate public reporting, attacker claims, and authorized disclosures to the Board for inclusion in this report. Attackers:

- accessed one organization's enterprise tools, including SaaS applications that contained source code and customer data, such as Atlassian, Cloudflare, and Slack;[144, 145]
- stole source code from one telecommunications provider;[146]
- stole 200 gigabytes (GB) of corporate data from a Kansas-based surgical and rehabilitation center;[147]
- stole 750 GB of source code from a company, including application programming interface (API) keys and debug tools, proprietary game frameworks, and other intellectual property;[148]
- stole approximately 37 GB of source code for over 250 projects from a technology company, after which the threat actors (Lapsus$) made it available to download in an online torrent posted on its Telegram channel;[149]
- downloaded internal Slack messages, accessed or downloaded information from an internal invoice management tool and bug bounty reports of one organization, and captured screenshots of tools they accessed;[150]
- stole and published source code for two flagship games from a gaming company, including related assets from the company's Confluence and Slack servers;[151]
- stole 190 GB of a technology company's source code and made it available to download via torrent;[152]
- claimed to steal the hashes of a technology company's employee and service accounts and posted the dump to Telegram;[153]
- stole 70 GB of a technology company's source code and project-related documentation along with administrator passwords, which the threat actors made available to download via torrent;[154]
- stole and deleted 50 terabytes (TB) of data, including a COVID-19 database,[155] from a non-U.S. government agency;[156]

[142] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

[143] Krebs, Brian; KrebsonSecurity, "*The Original APT: Advanced Persistent Teenagers*," April 6, 2022, https://krebsonsecurity.com/2022/04/the-original-apt-advanced-persistent-teenagers

[144] Cybersecurity Company, Response to CSRB Request for Information.

[145] Okta; "*Okta Security Action Plan*," September 30, 2022, https://support.okta.com/help/s/okta-security-action-plan

[146] FBI, CSRB Meeting.

[147] Rodriguez, Sarai; TechTarget - Heath IT Security, "*HC3 Report Uncovers Key Data Exfiltration Trends in Healthcare*," March 15, 2023, https://www.healthitsecurity.com/news/hc3-report-uncovers-key-data-exfiltration-trends-in-healthcare

[148] Gatlan, Sergiu; Bleeping Computer, "*Hackers breach gaming giant Electronic Arts, steal game source code*," June 10, 2021, https://www.bleepingcomputer.com/news/security/hackers-breach-gaming-giant-electronic-arts-steal-game-source-code

[149] Abrams, Lawrence; Bleeping Computer, "*Lapsus$ hackers leak 37GB of Microsoft's alleged source code*," March 22, 2022, https://www.bleepingcomputer.com/news/microsoft/lapsus-hackers-leak-37gb-of-microsofts-alleged-source-code

[150] Targeted Organization, Response to CSRB Request for Information.

[151] Teapotuberhacker; GTAForums, "*GTA 6 (Americas) leak – 90+ .mp4 footage/videos*," September 17, 2022, https://gtaforums.com/topic/985481-gta-6-americas-leak-90-mp4-footagevideos/#comments

[152] Ilascu, Ionut; Bleeping Computer, "*Hackers leak 190GB of alleged Samsung data, source code*," March 4, 2022, https://www.bleepingcomputer.com/news/security/hackers-leak-190gb-of-alleged-samsung-data-source-code

[153] Eun-jin, Kim; Business Korea, "*Hacker Group Lapsus$ Claims to Have Attacked LG Electronics*," March 23, 2022, http://www.businesskorea.co.kr/news/articleView.html?idxno=89525

[154] Lakshmanan, Ravie; The Hacker News, "*IT Firm Globant Confirms Breach after LAPSUS$ Leaks 70GB of Data*," March 30, 2022, https://thehackernews.com/2022/03/lapsus-claims-to-have-breached-it-firm.html

[155] DarkOwl, "*Darknet Threat Actor Report: LAPSUS$*" February 18, 2022, https://www.darkowl.com/blog-content/darknet-threat-actor-report-lapsus

[156] Temple Raston, Dina; Recorded Future, "*Lapsus$: The script kiddies are alright*," April 25, 2022, https://therecord.media/lapsus-the-script-kiddies-are-alright

- compromised and deleted data on debts of employees of a non-US law enforcement agency;[157]
- stole over 10 petabytes (PB) of a telecommunications provider's corporate and customer information;[158]
- claimed to steal 200 GB of source code from a telecommunications provider;[159]
- claimed to steal 1 TB of data, releasing approximately 150 GB, from a technology company, including proprietary information[160] and two code-signing certificates that were later used to sign files containing malware;[161]
- downloaded non-sensitive data from a Box instance associated with a compromised account belonging to a technology company employee, as well as employee authentication data from AD;[162] and
- accessed individual user accounts at cryptocurrency exchanges and stole cryptocurrency holdings.[163]

1.3.2. Extortion and Ransoms

Threat actor groups frequently attempted to extort organizations and ransom stolen data. However, the effectiveness of these coercion techniques is difficult to quantify. Threat actor groups demanded payment directly by communicating with the targeted organizations, but these attempts were uneven in their approach, with some being posted publicly to embarrass or harass the target, or poorly coordinated in their demands for payments and deadlines.

The effectiveness of extortion as a technique and whether the threat actors monetarily gained from their attempts is unclear. The Board spoke with targeted companies, threat intelligence firms, and law enforcement, and while ransomware attacks are widely acknowledged to have been lucrative in the past,[164] interviewees expressed no clear consensus on how much, if any, money was ever paid to any of the threat actors to alleviate extortion. In fact, FBI reported that it was not aware of Lapsus$ selling stolen data, nor had it found evidence that anyone ever paid ransoms. However, FBI has not ruled out the possibility that some paid ransoms without informing law enforcement.[165] This contrasts with other experts that observed Lapsus$ extorting organizations with some paying ransoms.[166]

The following examples enumerate public reporting, attacker claims, and authorized disclosures to the Board for inclusion in this report. This is not an exhaustive list but demonstrates the breadth of experiences shared across targeted organizations.

- Threat actors attempted to extort one technology company by threatening to release its confidential and proprietary data if the company did not push an update to its product that would remove a cryptocurrency mining limitation.[167, 168] When the extortion attempt failed, the threat actor offered to sell a bypass for the

[157] Istoe Dinheiro, "*Federal Police systems have been down for 10 days*," (translated), January 20, 2021, https://www.istoedinheiro.com.br/sistemas-da-policia-federal-estao-fora-do-ar-ha-10-dias/

[158] DarkOwl, "*Darknet Threat Actor Report: LAPSUS$*" March 16, 2022, https://www.darkowl.com/blog-content/darknet-threat-actor-report-lapsus

[159] Kovacs, Eduard; SecurityWeek, "*Vodafone Investigating Source Code Theft Claims*," March 10, 2022, https://www.securityweek.com/vodafone-investigating-source-code-theft-claims

[160] Flashpoint Intel Team; Flashpoint, "*All About LAPSUS$: What We Know About the Extortionist Group*," March 23, 2022, https://flashpoint.io/blog/lapsus

[161] Pieter Arntz; Malwarebytes, "*Stolen Nvidia certificates used to sign malware—here's what to do*," March 15, 2022, https://www.malwarebytes.com/blog/news/2022/03/stolen-nvidia-certificates-used-to-sign-malware-heres-what-to-do

[162] Biasini, Nick; Cisco Talos, "*Cisco Talos Shares Insights Related to Recent Cyber Attack on Cisco*," August 10, 2022, https://blog.talosintelligence.com/recent-cyber-attack

[163] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction

[164] Unit 42 Palo Alto Networks, "*Ransomware and Extortion Report*," March 2023, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2023-unit42-ransomware-extortion-report.pdf

[165] FBI, CSRB Meeting.

[166] Cybersecurity Company, CSRB Meeting.

[167] Ilascu, Ionut; Bleeping Computer, "*Hackers to NVIDIA: Remove mining cap or we leak hardware data*," February 28, 2022, https://www.bleepingcomputer.com/news/security/hackers-to-nvidia-remove-mining-cap-or-we-leak-hardware-data

[168] Heiligenstein Michael; Firewall Times, "*Lapsus$ Group Cyberattacks: Methods, Motives, and Timeline*," September 19, 2022, https://firewalltimes.com/lapsus-group-cyberattacks

mining limitation for USD 1 million,[169] plus an unspecified percentage of the proceeds. However, whether any money was made from this transaction remains unknown.[170]

- Threat actors attempted to coerce executives from a technology company via email, but their attempts were ignored with no further consequence.[171]
- Threat actors attempted to extort a company with different demands, which had different amounts and deadlines. The attempts coincided with the threat actors posting stolen source code for an online auction.[172]
- Threat actors attempted to extort a gaming company (over email) to negotiate a potential ransom for an unspecified amount.[173] The threat actors also offered to the sell the company's source code for a well-known game for a minimum of USD 10,000 (but stated other stolen games were not for sale).[174]
- Threat actors attempted to extort a telecommunications provider for USD 4 million via text message.[175]
- Threat actors attempted to extort a telecommunications provider for a "small reward/fee" in exchange for deleting its stolen data.[176]
- Threat actors defaced a media company's website with a ransom note, though it did not demand a specific amount.[177]

1.3.3. Network and Service Disruptions

Some of the threat actors, and Lapsus$ in particular, made use of disruptive and destructive techniques to bring negative attention to organizations and force public admissions of attacks, potentially as an angle on extortion attempts.[178, 179] In most instances, damage to resources occurred before organizations knew about the attack, giving threat actors the means to create a crisis.[180]

The following examples enumerate public reporting, attacker claims, and authorized disclosures to the Board for inclusion in this report. This is not an exhaustive list but demonstrates the breadth of experiences shared across targeted organizations.

- Threat actors conducted website defacement with tactics that included Domain Name System (DNS) hijacking.[181] They also disabled several websites belonging to non-U.S. organizations, including one instance where they compromised a company's website and redirected visitors to a pornographic site for a "couple of" hours.[182, 183]

[169] InfotechLead, "*Nvidia cyber security issue: LAPSUS$ exposes data of 71,000 employees*," May 3, 2022, https://www.infotechlead.com/security/nvidia-cyber-security-issue-lapsus-exposes-data-of-71000-employees-71487
[170] Cybersecurity Company, Response to CSRB Request for Information.
[171] Technology Company, CSRB Meeting.
[172] Targeted Organization, CSRB Meeting.
[173] Cybersecurity Company, Response to CSRB Request for Information.
[174] Brisk Infosec, "*Threatsploit Adversary Report*," October 10, 2020, https://www.briskinfosec.com/assets/threatsploit/Threatsploit-Adversary-Report-October-2022-Edition-50.pdf
[175] DarkOwl, "*Darknet Threat Actor Report: LAPSUS$*" March 16, 2022, https://www.darkowl.com/blog-content/darknet-threat-actor-report-lapsus/
[176] Vedere Labs; Forescout, "*The Rise, Fall and Return of a Hacking Group*," March 30, 2022, https://www.forescout.com/resources/lapsu-the-rise-fall-and-return-of-a-hacking-group/
[177] Cimpanu, Catalin; The Record, "*Lapsus$ ransomware gang hits SIC, Portugal's largest TV channel*," January 2, 2022, https://therecord.media/lapsus-ransomware-gang-hits-sic-portugals-largest-tv-channel/
[178] Tills, Claire; Tenable, "*Brazen, Unsophisticated and Illogical: Understanding the LAPSUS$ Extortion Group*," July 20, 2022, https://www.tenable.com/blog/brazen-unsophisticated-and-illogical-understanding-the-lapsus-extortion-group
[179] Cybersecurity Company, CSRB Meeting.
[180] Technology Company, CSRB Meeting.
[181] Cybersecurity Company, CSRB Meeting.
[182] DarkOwl, "*Darknet Threat Actor Report: LAPSUS$*" February 18, 2022, https://www.darkowl.com/blog-content/darknet-threat-actor-report-lapsus
[183] Hay Newman, Lily; Wired, "*The Lapsus$ Hacking Group Is Off to a Chaotic Start*," March 15, 2022, https://www.wired.com/story/lapsus-hacking-group-extortion-nvidia-samsung

- Threat actors destroyed cloud environments, including mass deletion of VMs, storage, and configurations.[184]
- Threat actors disrupted a gaming company's online games, systems, and services.[185]
- Threat actors disabled the website and several internal systems of a non-U.S. agency, including resources related to the nation's immunization program and issuance of digital vaccination certificates.[186] The attack rendered the website dysfunctional and resulted in significant data loss, including the deletion of the country's entire COVID-19 vaccination records database.[187]

1.3.4. Harassment

Multiple organizations and individuals involved in responding to the attacks experienced varying levels of personal harassment from some of the threat actors, with an intent to retaliate, halt investigations, or silence researchers.

A technology company reported that it was now tracking several groups as part of a new class of cybercriminal threat that has added targeted harassment to its toolbox and observed them targeting incident response professionals and their family members.[188] Some experts view this as an escalation in violence that is the result of cybercrime gangs competing for dominance.[189]

The seriousness of this activity ranged from mischief to dangerous behavior. Lapsus$ was known to join and monitor an organization's incident response channels, and in one instance took over a screen share and deleted resources live in front of the victim. Similarly, Lapsus$ publicly posted screenshots of victim environments[190] to demonstrate their access.[191] On the more serious end of this behavior, loosely affiliated threat actors threatened and harassed security professionals by publishing their personal information online, i.e., doxing,[192] and pestered targeted organizations' employees on Keybase, Twitter, and other online forums.[193] The Board also heard of a subset of threat actors that recruited forum members to hijack cybersecurity professionals' online accounts,[194] and conducted swatting attacks[195] against them and their families.[196] This demonstrates the potentially serious physical threat these groups posed.

1.4. PRIVATE SECTOR RESPONSE AND MITIGATION

Private sector organizations experienced varying levels of success in incident response and mitigation. However, organizations that prepared incident response and mitigation plans reported better recovery outcomes against incidents involving Lapsus$.[197, 198] At times, organizations simultaneously had to manage an active attack on their internal systems and harassment from the threat actor in public settings. In general, most organizations found they

[184] Research and Intelligence Fusion Team; NCC Group, "*Lapsus$: Recent techniques, tactics and procedures*," April 28, 2022, https://research.nccgroup.com/2022/04/28/lapsus-recent-techniques-tactics-and-procedures

[185] Ubisoft, "*Ubisoft Cyber Security Incident Update*," March 10, 2022, https://news.ubisoft.com/en-gb/article/3tSsBh25mhHhlbGSy1xbRw/ubisoft-cyber-security-incident-update

[186] Fonseca, Pedro and Paraguassu, Lisandra; Reuters, "*Brazil health ministry website hit by hackers, vaccination data targeted*," December 10, 2021, https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10

[187] DarkOwl, "*Darknet Threat Actor Report: LAPSUS$*" February 18, 2022, https://www.darkowl.com/blog-content/darknet-threat-actor-report-lapsus

[188] Technology Company, CSRB Meeting.

[189] Security Researcher 1, CSRB Meeting.

[190] Technology Company, CSRB Meeting.

[191] Brewster, Thomas; Forbes, "*Fury As Okta—The Company That Manages 100 Million Log-ins—Fails To Tell Customers About Breach For Months*," March 22, 2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/fury-as-okta-the-company-that-manages-100-million-logins-fails-to-tell-customers-about-breach-for-months

[192] Security Researcher 1, CSRB Meeting.

[193] Cybersecurity Company, CSRB Meeting.

[194] Technology Company, CSRB Meeting.

[195] Swatting is a form of harassment whereby a malicious party exploits law enforcement's emergency response procedures by falsely reporting a critical public safety concern. This results in a SWAT team being sent to the target's location. *Source: FBI Las Vegas, "FBI Las Vegas Federal Fact Friday: The Dangers of Swatting," September 23, 2022, https://www.fbi.gov/contact-us/field-offices/lasvegas/news/press-releases/fbi-las-vegas-federal-fact-friday-the-dangers-of-swatting*

[196] Cybersecurity Company, CSRB Meeting.

[197] Targeted Organization, Response to CSRB Request for Information.

[198] Cybersecurity Company, CSRB Meeting.

needed to adapt their existing incident response procedures and implement new security controls rapidly, adjusting to the dynamism of the threat actors. The following sections outline some of these measures.

1.4.1. Operational Security

Organizations initiated stricter security controls and communication strategies to limit future and ongoing accessibility by threat actors. One victim company enhanced its operational security by prohibiting bring-your-own-device (BYOD) usage in high-risk areas of the enterprise and selectively granting employees access to necessary resources.[199] Some organizations also made use of "out-of-band communications" (any alternative system or technology that allows communication separate from the primary channel),[200] an incident response procedure best established ahead of attacks,[201] to improve response operations by prohibiting threat actors from observing incident response communications and activities or taunting response teams.[202, 203, 204]

1.4.2. Disruption and Security Posture

Organizations adjusted their security posture to eradicate the threat actor from their environment and prevent re-entry. Authentication, employee verification, and access weaknesses combined to create a central theme in how the threat actors targeted organizations. The following section outlines some of the measures that organizations employed to mitigate the attack impact mid- and post-attack.

Mitigations were often disruptive to the organization's business operations as changes were rolled out rapidly or took critical business resources offline. In some situations, organizations needed to shut down resources to mitigate the attack. However, they sometimes did not know which resources they could safely take offline. Organizations needed to update their system inventories and document their architectures before completely understanding which systems they could safely shut down.[205] As events unfolded, one organization with existing security monitoring processes identified the issue and moved to respond, for example by disabling affected and potentially affected tools and locking down its codebase to prevent potential code changes.[206]

After threat actors gained access to corporate credentials and bypassed MFA to access victim systems, one organization took steps, such as conducting enterprise-wide password resets[207] while another required all employees to re-authenticate after restoring internal tool access.[208] An organization also disabled global SMS one-time passwords (OTP), enabled an ability for employees to flag suspected false authentication requests, and only allowed MFA that required employees to use a passcode on their screen to validate or leverage hardware-based authentication.[209]

Post-attack, organizations took additional steps to improve their security posture. For example, some organizations shortened their authentication and session lengths to force more frequent re-authentication for access to company platforms.[210, 211] Other organizations also rotated keys to many internal services to effectively reset access,[212] required

[199] Targeted Organization, CSRB Meeting.
[200] Hudak, Tyler; TrustedSec, "*To OOB, or Not to OOB?: Why Out-of-Band Communications are Essential for Incident Response*," December 29, 2022, https://www.trustedsec.com/blog/to-oob-or-not-to-oob-why-out-of-band-communications-are-essential-for-incident-response/
[201] CISA, "Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems," November 16, 2021, https://www.cisa.gov/sites/default/files/2023-02/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
[202] Cybersecurity Company, CSRB Meeting.
[203] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction
[204] Targeted Organization, CSRB Meeting.
[205] Cybersecurity Company, CSRB Meeting.
[206] Uber Security Team; Uber, "*Uber Newsroom Security Update*," September 19, 2022, https://www.uber.com/newsroom/security-update
[207] Technology Company, CSRB Meeting.
[208] Uber Security Team; Uber, "*Uber Newsroom Security Update*," September 19, 2022, https://www.uber.com/newsroom/security-update
[209] Technology Company, CSRB Meeting.
[210] Targeted Organization, Response to CSRB Request for Information.
[211] Targeted Organization, CSRB Meeting.
[212] Targeted Organization, Response to CSRB Request for Information.

all access to company internal systems to originate from corporate-managed machines, and blocked third-party remote desktop support software.[213]

Companies took targeted steps to improve MFA practices, including

- implementing phishing-resistant hardware tokens for MFA;[214]
- eliminating MFA push alerts;[215]
- verifying employee identities through video verification to reduce social engineering when fulfilling MFA reset requests;[216] and
- transitioning to using Fast IDentity Online (FIDO)-supported applications and passwordless authentication.[217, 218]

Organizations also adjusted their audit procedures and established additional security requirements for their service providers to ensure they meet an acceptable level of security. These measures varied but included the adoption of zero trust architecture (ZTA),[219] use of MFA for authentication, and safer access methods such as VDIs.[220]

1.4.3. Detection

Organizations found that early detection of attacks was important to enabling effective response. Companies took both mid- and post-attack actions to better detect and block suspicious events and attacks.

After detecting an attack, an organization increased monitoring of its internal environment to identify any further suspicious activity.[221] Discovering how a threat actor used compromised credentials to access its Slack environment, another organization implemented session fingerprinting to identify potentially re-used Slack sessions to detect attackers that were session hijacking.[222]

Post attack, an organization increased the resiliency of its detection by creating endpoint detection and response agent redundancy after discovering that threat actors deleted its original detection and response platform from its cloud environment.[223] One company improved its logs by making them more transparent to customers and enabling alerts every time support personnel accessed their information.[224]

Regarding fraudulent SIM swaps, an organization also shared a historically practiced and successful method to detect suspicious anomalies where certain legitimate information relating to a customer is vastly different from that provided in connection with the requested SIM swap.[225]

1.4.4. Personnel Security Awareness

As part of preventative strategies to mitigate attacks, some organizations create awareness and education programs to enable employees to better recognize attacker TTPs and intrusion attempts. One organization developed an internal risk mitigation awareness campaign to engage and educate almost 100,000 employees and contractors in its workforce, creating increased incident reporting and a dramatic improvement of workers identifying simulated phishing

[213] Targeted Organization, Response to CSRB Request for Information.
[214] Targeted Organization, Response to CSRB Request for Information.
[215] Targeted Organization, Response to CSRB Request for Information.
[216] Targeted Organization, CSRB Meeting.
[217] The FIDO Alliance is an open industry association promoting authentication standards that aims to reduce the reliance on passwords. *Source: FIDO Alliance, "Changing the Nature of Authentication?" December 2, 2014 (updated December 1, 2022), https://fidoalliance.org/overview*
[218] Targeted Organization, CSRB Meeting.
[219] Bradbury, David; Okta, "*Okta Concludes its Investigation into the January 2022 Compromise*," April 19, 2022, https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise
[220] Technology Company, CSRB Meeting.
[221] Targeted Organization, Response to CSRB Request for Information.
[222] Targeted Organization, CSRB Meeting.
[223] Targeted Organization, CSRB Meeting.
[224] Targeted Organization, CSRB Meeting.
[225] Technology Company, CSRB Meeting.

attempts after training.[226] To simulate as authentic an attack as possible, one company trains its agents using actual vishing attempts (voice phishing) to familiarize employees.[227] A company impacted by Lapsus$ also emphasized the importance of training employees of attack methods, which it credited with suspicious login reporting across its enterprise.[228]

1.4.5. Threat Intelligence and Information Sharing

Multiple organizations reported that sharing threat intelligence, including TTPs and indicators of compromise (IOCs), with peer companies and law enforcement contributed to a more effective response by helping to attribute threat activity and develop meaningful mitigations.[229, 230, 231] Information was distributed through public avenues such as websites, blogs, and threat intelligence notices.[232] In the aftermath of attacks, generally speaking, organizations are improving their threat intelligence sharing network to better prepare themselves and their customers against similar cyber threats. The following outlines some examples of where organizations successfully leveraged information sharing. It is not an exhaustive list but illustrates some positive outcomes.

Industry Initiatives:

- A victim organization initiated threat intelligence sharing arrangements with technology industry leaders, threat intelligence companies, and other corporate entities.[233]
- An impacted company created an in-house threat intelligence team to share weekly intelligence with clients and peer organizations.[234]

Customer-Facing Initiatives:

- One organization shared customized threat briefings to educate customers on how to identify threat actor behavior in their environments.[235]
- After an attack, an organization began reviewing its communication policies to adopt new systems that would help quickly and clearly notify customers when security or availability issues exist.[236]

Law Enforcement Initiatives:

- Leveraging an existing relationship with the cyber branch of the local FBI field office, one affected organization was able to contact an international law enforcement agency and share information that led to the arrest of one of the attackers.[237]

1.5. DISRUPTION EFFORTS

Successful coordination and collaboration with U.S., international law enforcement, and other government partners, was necessary to disrupt Lapsus$ and related threat actors. The sections below highlight how incident reporting plays into disrupting threat actors and summarize international law enforcement actions against Lapsus$.

[226] Cisco, "*Keeping Cisco Safe*," March 11, 2020, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-keeping-cisco-safe-casestudy.pdf
[227] Targeted Organization, CSRB Meeting.
[228] Targeted Organization, CSRB Meeting.
[229] Technology Company, CSRB Meeting.
[230] Targeted Organization, CSRB Meeting.
[231] Targeted Organization, Response to CSRB Request for Information.
[232] Roth, Emma; The Verge, "*Lapsus$ cyberattacks: the latest news on the hacking group*," September 26, 2022, https://www.theverge.com/22998479/lapsus-hacking-group-cyberattacks-news-updates
[233] Targeted Organization, Response to CSRB Request for Information.
[234] Targeted Organization, CSRB Meeting.
[235] Technology Company, CSRB Meeting.
[236] Bradbury, David; Okta, "*Okta Concludes its Investigation into the January 2022 Compromise*," April 19, 2022, https://www.okta.com/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise
[237] Targeted Organization, Response to CSRB Request for Information.

1.5.1. Incident Reporting

The Board heard that multiple targeted organizations reported attacks to FBI,[238] and is aware of at least one prior victim company that confirmed FBI was able to share information with it about the threat actor, which was obtained from information shared with law enforcement.[239] Another company reported to the Board that it shared information with the U.S. government beyond FBI and Cybersecurity and Infrastructure Security Agency (CISA) by reaching out to the General Services Administration (GSA), Federal Risk and Authorization Management Program (FedRAMP), the Defense Industrial Base Network (DIBNet), and briefing select members of Congress and the White House regarding its Lapsus$ attack.[240] A victim company found the interaction with law enforcement to be collaborative and mutually beneficial.[241]

Reporting Cyber Incidents to the U.S. Government

In the U.S., law enforcement agencies and private sector organizations often cooperate to effectively counter threat actors. Federal law enforcement agencies have the authority to carry out sweeping countermeasures and otherwise act to disrupt a threat actor's malicious activities. The agencies also have authority to enable widespread data sharing to improve resiliency and mitigation practices. Private industry has a dual mandate to defend its own organizations and ensure adequate information sharing with law enforcement and its peers within industry to enable the most comprehensive response to threat actors.

FBI and CISA reported to the Board that their effectiveness and responsiveness in supporting organizations impacted by cyber intrusions can benefit from those organizations having prior relationships with FBI or CISA, the timely reporting of incidents to either FBI or CISA, and the organization's willingness to voluntarily report and share further threat and incident information to help protect others from being targeted by similar malicious activities using the same infrastructure or TTPs.[242]

FBI and CISA informed the Board that victim organizations sometimes choose to rely on third-party incident response firms without reporting the incident to FBI or CISA.[243] An organization's decision not to report limits the U.S. government's ability to take disruptive action, such as the recovery of ransom payments or the decryption of data, either alone or in partnership with foreign and private sector partners.[244] FBI and CISA stressed to the Board that victim organizations working with incident response firms and sharing information with the U.S. government will serve to maximize available remediation and disruption resources, improving outcomes for victim organizations and the cyber resilience of the U.S.[245]

1.5.2. Investigations and Arrests

Through the course of its review, the Board heard how U.S. agencies and global partners collaborated to disrupt Lapsus$. Notable examples include:

- International law enforcement's efforts to disrupt ongoing attacks by Lapsus$ and related members was evident when media sources publicly reported the arrests of several individuals in 2022. On March 24, 2022, the City of London Police released information about the arrest of seven individuals in connection with Lapsus$.[246]

[238] Cybersecurity Company, CSRB Meeting.
[239] Targeted Organization, Response to CSRB Request for Information.
[240] Targeted Organization, CSRB Meeting.
[241] Targeted Organization, Response to CSRB Request for Information.
[242] FBI and CISA Panel Interview, CSRB Meeting.
[243] FBI and CISA Panel Interview, CSRB Meeting.
[244] Vorndran, Bryan A.; FBI Cyber Division, "*Oversight of the Federal Bureau of Investigation*," March 29, 2022, https://www.congress.gov/117/meeting/house/114533/witnesses/HHRG-117-JU00-Wstate-VorndranB-20220329.pdf
[245] FBI and CISA Panel Interview, CSRB Meeting.
[246] Peters, Jay; The Verge, "*Seven teenagers arrested in connection with the Lapsus$ hacking group*," March 24, 2022, https://www.theverge.com/2022/3/24/22994563/lapsus-hacking-group-london-police-arrest-microsoft-nvidia

- On April 1, 2022, the City of London Police announced that it had charged two juveniles with various cyber offenses related to an international police investigation into the Lapsus$ threat group.[247, 248]
- On September 22, 2022, as part of an investigation by the U.K.'s National Crime Agency (NCA), the City of London Police arrested a seventeen-year-old from Oxfordshire on suspicion of hacking.[249] While the related announcement did not disclose details about the nature of the investigation, media sources and one cyber threat intelligence firm believed the arrests were related to Lapsus$'s attacks against technology and gaming companies.[250, 251]
- On October 19, 2022, as an offshoot of an operation codenamed "Operation Dark Cloud," Brazilian police announced that they had arrested a Brazilian national suspected of belonging to Lapsus$.[252]

Security researchers reported the group's highly public communication style decreased after media sources reported that the City of London Police had arrested some of the group's members in March 2022.[253] However, researchers observed Lapsus$ attacking an organization in September 2022,[254] and compromising and leaking content from a video game company in the same month.[255, 256] Lapsus$ appears to have become inactive after September 2022.[257] Although this cannot be conclusively linked to law enforcement actions, the timing is noteworthy. Further, although the Board cannot rule out the possibility that the remaining Lapsus$ members have decided to limit their public profile, join other cybercrime groups, or rebrand, doing so often comes with an operational pause or other costs that are nonetheless positive developments from a cybersecurity perspective, even if only in the short term.

1.5.3. Limiting Factors

Law enforcement agencies face inhibiting factors when disrupting transnational networks of threat actors, as shown in the case of Lapsus$. The section below elaborates on three categories of issues that the Board heard.

Information Sharing and International Collaboration

International law enforcement and other government entities have made progress collaborating to advance cybercrime investigations. In recent years, the U.S. Department of Justice (DOJ) conducted several successful multinational operations against cyber threat actors with partner countries.[258] For example, law enforcement recently launched a coordinated international operation against the Genesis Market cybercrime marketplace that resulted in the arrest of many Genesis Market users around the world.[259] In January 2023, the FBI announced it had covertly infiltrated the Hive ransomware network, preventing victims from having to pay, by conservative estimates, more than USD 130 million in ransom and providing over 1,000 decryption keys to victims. The FBI highlighted its coordination with international

[247] City of London Police, "*Two Teenagers Charged in Connection with Investigation into Hacking Group*," April 1, 2022, https://www.cityoflondon.police.uk/news/city-of-london/news/2022/march/two-teenagers-charged-in-connection-with-investigation-into-hacking-group
[248] BBC, "*Lapsus$: Two UK teenagers charged with hacking for gang*," April 1, 2022, https://www.bbc.com/news/technology-60953527
[249] BBC, "*Oxfordshire teen arrested in police hacking investigation*," September 23, 2022, https://www.bbc.com/news/uk-england-oxfordshire-63010523
[250] Lakshmanan, Ravie; The Hacker News, "*London Police Arrested 17-Year-Old Hacker Suspected of Uber and GTA 6 Breaches*," September 24, 2022, https://www.thehackernews.com/2022/09/london-police-arrested-17-year-old.html
[251] Cybersecurity Company, Response to CSRB Request for Information.
[252] Ministério da Justiça e Segurança Pública, "*PF arrests Brazilian suspected of being part of international criminal organization*" (translated), October 19, 2022, https://www.gov.br/pf/pt-br/assuntos/noticias/2022/10/pf-prende-brasileiro-suspeito-de-integrar-organizacao-criminosa-internacional
[253] Research & Insights Center; SecurityScorecard, "*Lapsus$ Update: How This Technically Unsophisticated Threat Actor Group Breaches Large Organizations*," January 9, 2023, https://www.securityscorecard.com/research/lapsus-update
[254] Uber Security Team; Uber, "*Uber Newsroom Security Update*," September 19, 2022, https://www.uber.com/newsroom/security-update
[255] Abrams, Lawrence; Bleeping Computer, "*GTA 6 source code and videos leaked after Rockstar Games hack*," September 18, 2022, https://www.bleepingcomputer.com/news/security/gta-6-source-code-and-videos-leaked-after-rockstar-games-hack
[256] Cybersecurity Company, Response to CSRB Request for Information.
[257] FBI, CSRB Meeting.
[258] Monaco, Lisa; DOJ, "*Comprehensive Cyber Review*," July 18, 2022, https://www.justice.gov/dag/page/file/1520341/download
[259] Office of Public Affairs; DOJ, "*Criminal Marketplace Disrupted in International Cyber Operation*," April 5, 2023, https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation

partners including law enforcement and a tech-specific crime unit that led to the seizure of Hive servers and websites, dismantling its network.[260]

Despite these successes, the Board heard that law enforcement-to-law enforcement information sharing can still be a challenge. Due to budgetary constraints, limited personnel are devoted to such cooperation in the cyber context, for example FBI has approximately 22 cyber-specific assistant legal attachés and DOJ has only one prosecutor focusing on coordinating international disruption operations, thereby limiting the number of planned coordinated operations that can be conducted at any given time.[261] Legal frameworks and practices can also differ across countries, limiting the available consequences for cybercriminals or law enforcement's ability to act against threat actors in certain countries (e.g., countries that traditionally serve as safe havens for cybercriminals, such as the Russian Federation [Russia], People's Republic of China [PRC], Islamic Republic of Iran [Iran], and Democratic People's Republic of Korea [DPRK, also known as North Korea]).[262, 263] Additionally, countries may have different requirements for both informal and formal law enforcement information sharing, which in some cases must be conducted pursuant to the requirements of negotiated mutual legal assistance treaties that are often executed by a limited number of law enforcement personnel in each country.[264] Finally, threat actor groups operated across many personas or group names and were also tracked under multiple identifiers[265] across the cybersecurity industry, making it difficult to achieve consensus on the makeup of the groups and even their exploits in some cases.[266]

Victim Engagement

FBI faced challenges when engaging victim organizations following an incident due to the lack of pre-existing, trusted relationships with victims and their outside counsel; victims' lack of familiarity with information-sharing mechanisms and protections; the lack of a continuous flow of information between victims and the FBI; multiple government entities requesting information from victims; and initial questions about attribution that may delay the assignment of agents with experience on the underlying threat groups.[267, 268]

The Board heard from FBI that, following a high-profile incident, victims are often contacted by multiple government agencies with varying information needs, such as information regarding impact on victim company operations and threat actor TTPs and IOCs that are necessary to disrupt the threat actors' ongoing or future efforts. Such inquiries can take a victim's incident response team away from critical recovery efforts and restoring business operations, delaying the reconstitution of services, and potentially causing further financial or reputational damage, or other consequences. FBI recognizes the need to balance the drive to pursue the threat actors and other governmental information requirements with the need to allow the victim's incident response efforts to continue unimpeded.[269]

Juvenile Offenders

Many of Lapsus$ members' high-profile arrests involved juvenile members (other threat groups likely have similar demographics). Some evidence from cybersecurity researchers suggests that existing perceptions, such as a lack of sufficient consequences for minors who engage in cybercrime, do not effectively deter some young people from repeatedly engaging in malicious behavior even when identified by law enforcement.[270, 271] For example, on March 24, 2022, media outlets reported that the City of London Police arrested seven juveniles in relation to the Lapsus$

[260] Office of Public Affairs; FBI, "*U.S. Department of Justice Disrupts Hive Ransomware Variant*," January 26, 2023, https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[261] DOJ, Response to CSRB Request for Information.
[262] The White House, "*National Cybersecurity Strategy*," March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[263] Office of Public Affairs; DOJ, "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," September 16, 2020, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
[264] FBI and CISA Panel Interview, CSRB Meeting.
[265] Technology Company, CSRB Meeting.
[266] Cybersecurity Company, CSRB Meeting.
[267] FBI and CISA Panel Interview, CSRB Meeting.
[268] Cybersecurity Company, CSRB Meeting.
[269] FBI and CISA Panel Interview, CSRB Meeting.
[270] Zhadan, Anna; Cybernews, "*Teen cyber cartels: when world's most prolific cybercriminals are minors*," October 13, 2022, https://www.cybernews.com/editorial/teen-cyber-cartels
[271] Cybersecurity Company, CSRB Meeting.

group.[272] However, shortly after the arrests, Lapsus$ announced it was “back from vacation” on March 29, posting a teaser screenshot of exfiltrated data and administrator credentials on its Telegram channel.[273] Although juveniles are often swiftly released from custody, thus calling into question the level of disruption and impact from the juvenile justice system,[274] FBI reported that it last observed Lapsus$ activity in September 2022 and assessed that the decrease in activity was likely due to the arrests of Lapsus$ members.[275]

Threat groups’ recruitment of juveniles is a systemic issue.[276] Forums and online games operate as pipelines for recruiting and developing juveniles. In one example, a security researcher observed a Lapsus$ member presenting early warning signs when the member posted on forums about network exploitation when as young as 11 or 12. The Board heard from a security researcher who believed that juvenile recruitment in cybercrime is a systemic issue with insufficient attention in the cyber ecosystem, as threats posed by juveniles are commonly underprioritized.[277] Juvenile enforcement is further governed by certain procedures and laws that are not applicable to adult prosecutions.[278]

Juvenile Pathways into Cybercrime

Some studies have found that adolescents can start hacking between the ages of 10 and 15,[279] primarily learning their skills through online forums and websites. This has a particular nexus with the development of cheats for popular video games.[280] Forums, including those where game tips are shared and discussed, effectively serve as “talent development” pipelines for criminal elements that openly recruit juvenile and novice participants.[281, 282] Sandbox games, where players have a high degree of freedom to explore and interact, are acting as a gateway for minors to develop technical skills that can be leveraged for malicious intent.[283] Sandbox games also offer an avenue for turning in-game currency into real money, and researchers have noted the intersection of a monetary incentive and a lack of adult supervision is a factor in adolescent participation in online criminal communities.[284] Criminal gangs, in turn, exploit adolescents’ legal status in the criminal justice system, redirecting repercussions that could be imposed on adult threat actors operating in the background. Some members of Lapsus$ and its related groups seem to have followed this path.[285]

[272] Peters, Jay; The Verge, “*Seven teenagers arrested in connection with the Lapsus$ hacking group*,” March 24, 2022, https://www.theverge.com/2022/3/24/22994563/lapsus-hacking-group-london-police-arrest-microsoft-nvidia

[273] Lisa Vaas; Threatpost, “*Lapsus$ ‘Back from Vacation*,’” March 30, 2022, https://www.threatpost.com/lapsus-back-from-vacation/179156

[274] NCJFCJ, “*Juvenile Delinquency Guidelines: Improving Court Practice in Juvenile Delinquency Cases*,” July 1, 2005, https://www.ncjfcj.org/wp-content/uploads/2019/10/Juvenile-Delinquency-Guidelines.pdf

[275] FBI, CSRB Meeting.

[276] Beaming, “*Why do young people commit cyber crime?*” July 24, 2018, https://www.beaming.co.uk/insights/young-people-get-cybercrime

[277] Security Researcher 1, CSRB Meeting.

[278] Jarrett, H. Marshall et al.; Office of Legal Education, “*Prosecuting Computer Crimes*,” October 2010, https://www.justice.gov/criminal/file/442156/download

[279] UNDOC, “*Comprehensive Study on Cybercrime*,” February 21, 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[280] Robson, Kurt; Verdict, “*Many of today's hackers are teenagers and access to 'mass resources online' are helping to train them*,” September 28, 2022, https://www.verdict.co.uk/most-of-todays-hackers-are-teenagers

[281] Zhadan, Anna; Cybernews, “*Teen cyber cartels: when world’s most prolific cybercriminals are minors*,” October 13, 2022, https://www.cybernews.com/editorial/teen-cyber-cartels

[282] Huang, Keman et al.; Massachusetts Institute of Technology, “*Systematically Understanding the Cyber Attack Business: A Survey,*” March 22, 2018, http://delivery.acm.org/10.1145/3200000/3199674/a70-huang.pdf

[283] National Cyber Crime Unit / Prevent Team; NCA, “*Pathways Into Cyber Crime*,” January 13, 2017, https://nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file

[284] Security Researcher 2, CSRB Meeting.

[285] Security Researcher 1, CSRB Meeting.

Juvenile Pathways into Cybercrime

The U.K.'s NCA maintains programs such as Cyber Choices alongside the U.K.'s National Cyber Security Centre's (NCSC) CyberFirst (Cyber Security Career Program), and the Dutch National High Tech Crime Unit (NHTCU) maintains Hack_Right; these programs aim to deter and divert juveniles away from cybercrime.[286, 287] The NCA's Cyber Choices program uses online and in-person educational campaigns and modules to promote the positive use of cyber skills and provide awareness of the consequences associated with cybercrime.[288] The U.K.'s NCSC CyberFirst program works with higher education institutions to provide activities, courses, scholarships, and other support that introduce and encourage interested juveniles into a cybersecurity career.[289] Hack_Right focuses on deterring at-risk juveniles or those early on in their cybercriminal career from committing more cybercrimes and redirecting their skills to cybersecurity-enhancing pursuits.[290]

[286] NCA, "*Cyber Choices*," https://www.nationalcrimeagency.gov.uk/cyber-choices; NCSC, "*CyberFirst overview*," December 8, 2017, https://www.ncsc.gov.uk/cyberfirst/overview
[287] Ilascu, Ionut; Bleeping Computer, "*20 Companies Pledge Support for the Hack_Right Program*," November 1, 2019, https://www.bleepingcomputer.com/news/security/20-companies-pledge-support-for-the-hack-right-program/
[288] NCA, "*Cyber Choices*," https://www.nationalcrimeagency.gov.uk/cyber-choices
[289] NCSC, "*CyberFirst overview*," December 8, 2017, https://www.ncsc.gov.uk/cyberfirst/overview
[290] Public Prosecution Service, "*Hack_Right*," October 1, 2018, https://www.om.nl/onderwerpen/cybercrime/hack_right

2. FINDINGS

The Board's findings and conclusions are the result of its independent review. They are based on information gleaned from literature searches, interviews, requests for information, and analysis of public, private, and government source information. The Board relied upon the voluntary participation of numerous organizations affected by this intrusion set.

The findings and conclusions in this section are not intended to assign blame or fault to any individual or collective parties, but rather to highlight opportunities where the community can understand lessons and apply safety improvements for the future.

2.1. SUMMARY OF FINDINGS

Most organizations were not prepared to prevent the attacks described in this report, but most were able to rapidly change their security programs to account for vulnerabilities and make improvements to thwart future attacks. Companies that had prepared for the possibility of these kinds of attacks, against their own infrastructure as well as their suppliers, proved most resilient.

The complex intersecting relationships between telecommunications providers and BPOs with their customers and clients were favored targets of the threat actors. The exploitation of insiders and insider processes in the supply chain of many organizations, especially, added an extra level of complexity for mitigating the attacks across the broader ecosystem. Unsurprisingly, successful social engineering techniques were also effective for atypical business processes, such as EDRs.

The role of information sharing with law enforcement and the broader ecosystem played a vital role in the mitigation of attacks and disruption of threat actors. This is, however, an area with ongoing challenges. Organizations still experience friction in their ability or willingness to share information about attacks due to confusion about the government's role, or perceived negative consequences of making attack details known, or a lack of familiarity with legal authorities designed to encourage such sharing. International and juvenile criminals also frustrate the under-resourced U.S. law enforcement apparatus.

Finally, threat actors' unauthorized access and theft of sensitive and proprietary data, in tandem with extortion, subjected targeted companies to repercussions, including reputational damage, service disruption, and regulatory implications.

2.2. IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and access management (IAM) weaknesses were a consistent theme in attacks across all targeted entities and present opportunities to make ongoing improvements.

In the past decade, the emphasis on MFA has driven the adoption of more secure solutions to improve resiliency against attacks and phishing in particular.[291] Enterprise and consumer adoption of MFA has been a beneficial step forward away from use of just passwords for authentication. However, the Board's review found that the types of MFA used broadly in the online ecosystem today are not sufficient for most organizations or consumers defending against the type of attacks described in this report.[292] In particular, OTP delivery and push notifications using SMS and voice calls (and even email) are vulnerable to social engineering and SIM swap attacks, and the attacker ecosystem is readily capable of exploiting these weaknesses. A lucrative SIM swap criminal market is enabling pay-for-access to victim

[291] The cybersecurity community has advocated for increased MFA adoption for over a decade, with modest success outcomes. For example, adoption of MFA for customers in the banking industry has increased substantially. *Source: Sinigaglia, Federico et al.; Computers & Security (Volume 95), "A survey on multi-factor authentication for online banking in the wild," August 1, 2020, https://doi.org/10.1016/j.cose.2020.101745*

[292] This is a well-recognized finding by the broader cybersecurity community. For example, see: Kapko, Matt; Cybersecurity Dive, "*Multifactor authentication is not all it's cracked up to be*," October 5, 2022, https://www.cybersecuritydive.com/news/multifactor-authentication-weaknesses/633399; Meyer, Lucas Augusto et al.; arXiv (Cornell University), "*How effective is multifactor authentication at deterring cyberattacks?*" May 1, 2023, https://doi.org/10.48550/arXiv.2305.00945

mobile phone services with a focus on hijacking SMS messages and voice calls.[293, 294, 295] SMS was not designed to transact sensitive information such as OTPs, and its wide use as such incentivizes criminals to perform SIM swap attacks, porting fraud, and similar techniques.

The use of MFA with number matching[296] was an improvement for some organizations, and hardware-backed FIDO2 MFA solutions proved most resilient. However, adopting advanced MFA capabilities remains a challenge for many organizations and individual consumers due to workflow and usability issues.[297] The Board concurs that usable solutions will be necessary to evolve toward a more secure and passwordless user experience.[298, 299]

Most of the attackers leveraged some form of social engineering at all stages of the attack chain, using a dynamic mix of phishing, vishing, and smishing to obtain passwords for initial entry, obtain sensitive information about the targeted organization, effect SIM swapping and call forwarding, negate ZTA (with device additions), and achieve other far-reaching consequences. This tracks closely with industry observations on the human element being a factor in most breaches,[300] and organizations will need to take additional measures to counter the effects of social engineering. Expensive endpoint security solutions were not an effective control to protect enterprise identities against social engineering.

Attackers leveraging the “infostealer” malware ecosystem to buy target entity login credentials (“access as a service”) was a highly effective means of initial entry in many of the attacks perpetuated by these threat actors.[301] The active development and deployment of malware toolkits (“malware as a service”) to steal web session cookies and other credentials from victim systems for later use has evolved into a lucrative and pernicious global pay-for-credentials underground market, whereby low-skill attacks can be initiated for a few thousand dollars and then deployed effectively against even well-defended organizations. Defense strategies against these types of attacks rely on endpoint security controls, and additional layers of defense are necessary to curb the increasing trend.

[293] Fraudulent SIM Swapping has been a problem for many years; an early example occurred in South Africa in 2007. Source: Jordaan, Louis and von Solms, Basie; International Workshop on Open Problems in Network Security (Volume 6555), “A Biometrics-Based Solution to Combat SIM Swap Fraud,” February 7, 2011, https://doi.org/10.1007/978-3-642-19228-9_7

[294] In 2019 the FBI issued a private industry notification about cybercriminals leveraging SIM swap attacks. Source: FBI, “Private Industry Notification: Cyber Criminals Use Social Engineering and Technical Attacks to Circumvent Multi-Factor Authentication,” September 17, 2019, https://info.publicintelligence.net/FBI-CircumventingMultiFactorAuthentication.pdf

[295] Over the past decade, several law enforcement operations disrupted SIM swap fraud rings in Europe and the United States. Source: Venkat, Apurva; BankInfoSecurity, “Numerous Arrests in 2 SIM-Swapping Schemes,” March 16, 2020, https://www.bankinfosecurity.com/numerous-arrests-in-2-sim-swapping-schemes-a-13949

[296] MFA with number matching is an extra layer of security during a transaction that requires users to enter a code shown to them in an app. *Source: CISA, “Implementing Number Matching in MFA Applications,” October 31, 2022, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf; Microsoft Learn; Microsoft, “How number matching works in multifactor authentication (MFA) push notifications for Authenticator - Authentication methods policy,” May 10, 2023, https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match#multifactor-authentication*

[297] The human accessibility issues of many MFA solutions are well-noted in the academic literature. Source: Das, Sanchari; arXiv (Cornell University), “Evaluating User Perception of Multi-Factor Authentication: A Systematic Review,” August 16, 2019, https://doi.org/10.48550/arXiv.1908.05901

[298] Passwordless authentication mechanisms de-emphasize the importance of passwords as a factor in login flows, which many platform providers support. *Source: FIDO Alliance, “Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins,” May 5, 2022, https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins*

[299] The U.S. government now encourages its agencies to pursue greater use of passwordless authentication. For example, see: OMB, “*M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*,” January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[300] Between November 2021 and October 2022, Verizon assessed that 73% of data breaches involved a human element, such as social engineering. *Source: Verizon, “Data Breach Investigations Report: Summary of Findings,” June 6, 2023, https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings*

[301] Between Q1 and Q4 2022, Recorded Future observed a 600% year-over-year increase in the number of credentials being sold in the access as a service underground markets because of Infostealer malware, indicating a pervasive and systematic problem in the ecosystem. *Source: Insikt Group; Recorded Future, “2022 Annual Report,” March 2, 2023, https://go.recordedfuture.com/hubfs/reports/ta-2023-0302.pdf*

2.3. TELECOMMUNICATIONS VULNERABILITIES

The Board heard from many experts that telecommunications providers are providing the government, enterprises, online commerce, and consumers with critical infrastructure. Threat actors clearly understand the role telecommunications providers play in the ecosystem and are targeting those providers to gain access to their customers. The defense of telecommunications infrastructure, service offerings, and operational processes that govern their business transactions is of vital importance for the nation's security.[302, 303]

The Board determined that customers are at risk when attackers can impersonate them and initiate changes to their mobile phone service, including for SIM swaps (when getting a new phone), number porting (when changing telecommunications providers), setting up call forwarding, and so on. The Board heard that improving these processes is challenging, as telecommunications providers need to maintain low-friction customer experiences for a wide range of user needs and account for unique and emergent situations, including domestic abuse, loss of identification cards, and global travel.[304] Furthermore, the carriers currently have limited options for identity verification and other solutions may not be scalable.

The Board learned through attackers' public comments and interviews with targeted entities that attackers can socially engineer, coerce, or bribe telecommunications staff, including those in customer support centers, retail stores, and elsewhere. In comparable industries, such as banking, where employees need to access sensitive personal data to service customers, additional advanced insider threat controls and strong identity verification can be helpful in preventing threat actors from tricking, coercing, or bribing staff to act on their behalf.[305]

The security of telecommunications infrastructure that provides service to customers is vital to the security of these transactions. In several instances, the threat actors leveraged known vulnerabilities to hijack telecommunications tools, placing backdoors for initial entry or otherwise modifying their behavior. This underscores the importance of using robust software development lifecycle and secure-by-default coding and system management practices to design, implement, and maintain internal systems over their lifetime.

Telecommunications provider retail stores were also an effective avenue of attack, with attackers planting malware on point-of-sale systems and stealing retailer devices with privileged access to make fraudulent changes to customer mobile phone service. Attackers also co-opted employees as insiders in retail stores,[306] a trend that is challenging to counter as these jobs are typically lower pay with low-vetted personnel, including juveniles, who can move untracked between companies.

2.4. RESILIENCY WITH A FOCUS ON BUSINESS PROCESS OUTSOURCING (BPO)

The Board found that the threat actors had a remarkable understanding of their targets' core business, associated business processes, and their weaknesses. In some instances, they successfully leveraged low-complexity attack methods that circumvented security preventative and detective controls. Even well-defended companies fell prey, but those with layered, mature defense-in-depth controls were most resilient, including use of ZTA, strong authentication, robust detection, adaptable MFA capabilities, vulnerability management programs, response plans, and awareness

[302] The importance of telecommunications industry defense is globally recognized. In the past decade, coordinated attacks and criminal rings aimed at telecommunications providers gave rise to new efforts to bolster and mandate security improvements. For example, see: Industrial Cyber, "*Cybersecurity issues in telecoms sector call for protection of network infrastructure and availability*," January 29, 2023, https://industrialcyber.co/features/cybersecurity-issues-in-telecoms-sector-call-for-protection-of-network-infrastructure-and-availability

[303] The U.S. government is asserting more stringent guidance and requirements for the security of telecommunications infrastructure and services. For example, see: CISA, "*NSTAC Report to the President: Strategy for Increasing Trust in the Information and Communications Technology and Services Ecosystem*," February 21, 2023, https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf; Executive Office of the President, "*Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector*," April 8, 2020, https://www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states

[304] Technology Company, CSRB Meeting.

[305] Eggenschwiler, Jacqueline et al.; Computer Fraud & Security, "*Insider Threat Response and Recovery Strategies of Financial Service Firms*," November 15, 2016, https://www.cs.ox.ac.uk/files/9225/2016_cfs_ean-author-final.pdf

[306] The Board heard examples of co-opted retail employees ("innies") being paid as little as USD 500-1000 to perform SIM swaps. *Source: Security Researcher 2, CSRB Meeting.*

training. These organizations either fully repelled or quickly recovered from attacks, with little long-term impact on their business.

Other organizations that had not matured their security controls had more challenges recovering, and, in some cases, were hindered by misaligned cybersecurity budgets.[307] For example, BYOD policies are cost efficient as they enable employees to use their own computers. However, BYOD enabled the threat actors studied for this report to pivot into corporate environments after compromising employees' personal devices and accounts. The trend of using more cost-effective workforce options, such as BPOs, for sensitive business workflows was another example of how cost-saving mechanisms may not be in line with an organization's threat model.

Employee awareness and insider risk management factored heavily into whether organizations defended well against this class of threat actors. The threat actors impersonated a wide range of legitimate company personnel via phishing, smishing, and vishing to trick employees into acting on their behalf, for example by accessing customer records. These social engineering tactics may require prevention, detection, and response capabilities that mirror insider threat programs so that privileged access cannot be abused by a threat actor leveraging an employee's account.[308] Designing employee awareness programs that cover this specific class of threat actors was also helpful in some organizations for early detection and resiliency against attacks.

Enterprise-wide security hygiene was a major factor in whether organizations successfully repelled attacks. The Board heard of several intrusions that involved exploiting, for example, weak MFA implementations or misconfigured or unpatched AD infrastructure, which gave the threat actors their opportunity. Standard network and system-level visibility (telemetry) and programmable detection were also critical for organizations looking for past and ongoing attack activity. The Board concurs with the views of several briefers in determining that adopting perceived advanced, novel, or sophisticated (and often expensive) security solutions cannot replace the need for basic security hygiene and capabilities.[309]

Having established and practiced response plans was the final important element of resiliency. For example, in instances where the threat actors took over internal communications used by the response teams, organizations that had previously setup out-of-band communications were able to avoid having their activities monitored or interrupted. Previously established industry and law enforcement relationships also enabled organizations to quickly attribute the attacks and share best practices for mitigating the threat actors. However, the Board also heard that some organizations may be hesitant to share information regarding security attacks due to concerns over loss of attorney-client privilege, regulatory and legal implications, and reputational damage. These challenges are ongoing hinderances to frictionless collaboration.

2.4.1. Business Process Outsourcing (BPO) Risks

These attacks demonstrated how threat actors can exploit BPOs so the threat actors can then attack their clients, and how other serious threat actor groups, including nation-states, are using this class of attacks as a model. The U.S. government, the cybersecurity community, and BPO client organizations need to understand the specific risk exposures in the outsourcing sector, given the role BPOs are playing for organizations, including those supporting critical infrastructure.

The BPO operating structure related to their clients' trusted access and sensitive data enables threat actors to access targeted entities by bypassing the target's defenses and going through the sometimes lesser defenses of the BPO. Some organizations the Board spoke with had not previously considered their BPOs in their attack surface and risk management programs, even though they hold sensitive levels of access to clients' systems and data. Many BPO employees and workflows were onboarded and risk-managed differently from the client organization, leading to potential risk exposures and governance challenges for both the BPO and its clients. Industry-gathered data mirror these findings closely and suggest that many organizations lack confidence that a breach at their third-party supplier

[307] Gordon, Lawrence A. et al.; Journal of Cybersecurity (Volume 6), "*Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model*," March 30, 2020, https://www.doi.org/10.1093/cybsec/tyaa005
[308] Microsoft Defender Threat Intelligence and MSTIC; Microsoft, "*DEV-0537 criminal actor targeting organizations for data exfiltration and destruction*," March 22, 2022, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction
[309] Cybersecurity Company, CSRB Meeting.

would be reported to them and that breaches may be under-reported.[310] The Board noted the broader industry conversation on these issues, including the increasing use of the legal system for recourse.[311]

In the aftermath of the attacks, many targeted organizations pivoted slowly to improve the security posture at the BPO to be commensurate with their own if they could not insource workflows.[312, 313] Other organizations terminated their partnerships with BPOs (bringing workflows in-house). Client organizations that remained with their BPOs found it challenging to verify the BPO was upholding sufficient security standards and found few mechanisms for accountability. Most legal contractual agreements did not clearly outline the roles and responsibilities between BPOs and their clients to support either preventative controls improvement or incident response activities.

2.5. LAW ENFORCEMENT AND JUVENILE DISRUPTION

The Board found that while arrests have chilling effects on the cybercriminal community, law enforcement is challenged by a lack of sufficient resources devoted to disrupting cybercrime; a hesitancy from victims and their legal advisors to report cybercrimes and share actionable information; vulnerabilities in the processes some providers have for requests to obtain consumer data from organizations during emergency situations; and countries that act as safe havens for cybercriminal activity. Additionally, the deterrence value of available criminal justice consequences remains limited for juvenile cybercrime offenders, and few (and no U.S.-based) cyber-specific intervention programs exist that can help divert potential offenders to legitimate cybersecurity-related activities.

The Board found that the EDR process creates a significant exposure point for communications services providers because the process is not standardized across the industry and often lacks a method for authentication and validation. As a result, threat actors could exploit providers' employees by spoofing EDR materials using compromised government email addresses and official logos. Further, the Board found that EDR process exploitation was not limited to Lapsus$, but points to a broader, systematic risk exposure issue, which threat actors can exploit to gain valuable intelligence about their targets.

2.5.1. Victim Assistance Operations

The Board heard that law enforcement is hampered in its efforts to effectively combat cyber threats if victim organizations do not report attacks with actionable information. However, targeted organizations and their legal counsel are often unfamiliar with the information-sharing mechanisms and protections for reporting incidents to government contacts, which hinders the much-needed flow of information between victims and FBI or other law enforcement and diminishes the support the government can provide to a victim, similarly situated victims, and would-be victims. These findings indicate that prompt notifications to law enforcement about cyberattacks and above-board information sharing from organizations increase the likelihood of preserving critical evidence and recovering ransom payments or decrypting data, streamline government assistance, prevent uncoordinated government inquiries, and allow for more frequent and impactful cybercrime disruptions, all of which are a net cybersecurity benefit for society.

That said, some organizations the Board spoke to were confused about the federal roles and responsibilities for cyberattacks and which agency they should call to receive assistance and aid in future disruptions. The Board recognizes that the federal government has improved its governance and incident response coordination with national policies such as the Presidential Policy Directive 41[314] and its evolving implementation. However, clear messaging to the public and private sector about roles and responsibilities is lacking—in particular, where entities and individuals can go to receive specific services or meet statutory and regulatory reporting requirements. Therefore, the Board endorses

[310] In a recent study, only 34% of surveyed respondents believed their third-party suppliers would report a breach to them. Over 50% experienced a breach that originated from one of their third-party suppliers within the last 12 months, with the rates increasing over time. *Source: Ponemon Institute, "Data Risk in the Third-Party Ecosystem," September 12, 2022, https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study*

[311] For example, several BPO providers faced class action lawsuits resulting from data breaches. Source: Cantu, Cesar; Nearshore Americas, "Lawsuits Against BPOs Pile Up As Cybercriminals Grow Bolder," February 14, 2023, https://nearshoreamericas.com/lawsuits-against-bpos-pile-up-as-cybercriminals-grow-bolder

[312] Collier, Zachary A. and Sarkis, Joseph; International Journal of Production Research, "*The zero trust supply chain: Managing supply chain risk in the absence of trust*," February 17, 2021, https://www.doi.org/10.1080/00207543.2021.1884311

[313] Security Researcher 1, CSRB Meeting.

[314] The White House, "*Presidential Policy Directive -- United States Cyber Incident Coordination*," July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

the federal government's plans, as stated in Strategic Objective 1.4 of the National Cybersecurity Strategy (Update Federal Incident Response Plans and Processes), to "strengthen processes, procedures, and systems to more fully realize the policy that 'a call to one is a call to all.'"[315]

2.5.2. Cybercrime Investigations

The Board learned that disrupting transnational networks of threat actors presents myriad challenges. Law enforcement remains underfunded for resource- and data-intensive investigations against the full breadth of threat actors; has complex coordination processes with international partners, including obtaining evidence from multiple international jurisdictions; faces some victims' reluctance to report incidents and share actionable information; and is restricted by sovereignties that disregard peacetime norms of responsible state behavior in cyberspace or otherwise act as safe havens for cybercriminals. But a properly resourced and dedicated investigative team can still find methods to impose consequences on these difficult-to-reach actors, as recently demonstrated by FBI's Hive decryptor operation, Snake malware takedown, and the arrest of several enablers of the ransomware ecosystem.

In addition, the cybersecurity industry tracks threat actors, which operate under many personas and group names, with multiple identifiers, such as TTPs, target geography, target sector, and motivation. This can delay attributing behaviors and attacks to the correct threat actors and may prolong assigning agents with experience to the appropriate case concerning specific threat groups.[316] The National Cybersecurity Strategy[317] recognizes many of these challenges, indicating that the successful coordination and collaboration of U.S. and international law enforcement and government partners, as well as a more agile and well-resourced law enforcement, can counter the threat posed by cybercriminals and mitigate existing response challenges.

2.5.3. Early Intervention

Law enforcement entities face an increasing cadre of technically savvy cybercriminals, some of whom begin their malicious activities as juveniles. However, the juvenile status of certain threat actors can limit federal law enforcement's role and yield lighter penalties under their home countries' legal frameworks. Depending on the applicable laws, the post-conviction punishment for a juvenile is typically not as severe as it would be for an adult.[318] Nevertheless, juvenile justice issues are not limited to the cyber context and reflect the relevant society's broader conclusions about the criminal culpability and just punishment of minors. As a result, the Board found that less severe consequences may not adequately deter young cybercriminals from re-offending.

To curb juvenile participation in cybercrime, the Board found that several law enforcement entities are implementing preventative tactics and program initiatives[319] that demonstrate cost-effective means to identify and redirect at-risk juveniles that can also improve the pool of employable personnel to fill cybersecurity jobs.[320] This finding indicates that encouraging positive and legal alternatives, for example events at gaming conferences, to channel the energy and technical savviness of youth may potentially support hobbies and careers that benefit juveniles' technical skills advancement.

Other last-resort interventions, including non-prosecutorial and deferred prosecutorial disruption,[321] have proven useful for alerting unaware parents to juvenile cybercrime activity and dissuading future activity.

[315] The White House, "*National Cybersecurity Strategy*," March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[316] Cybersecurity Company, CSRB Meeting.
[317] The White House, "*National Cybersecurity Strategy*," March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[318] FBI and CISA Panel Interview, CSRB Meeting.
[319] FBI, CSRB Meeting.
[320] Stupp, Catherine; The Wall Street Journal, "*Dutch Program Aims to Deter Young Hackers Before They Commit Crimes*," December 21, 2020, https://www.wsj.com/articles/dutch-program-aims-to-deter-young-hackers-before-they-commit-crimes-11608546602
[321] For an example, see: Holcomb, Jayme W.; DOJ Office of Justice Programs, "*Knock and Talks*," August 1, 2006, https://www.ojp.gov/ncjrs/virtual-library/abstracts/knock-and-talks

2.6. IMPACT ON BUSINESS OPERATIONS

In aggregate, many organizations experienced costly and destructive impacts from these attacks. However, the Board learned that while some incidents directly affected targeted organizations' revenue streams, the impact of cyberattacks on business extends far beyond immediate financial loss.

Organizations lost control of "crown jewel" intellectual property and consumer data, subjecting them to remediation expenses, consumer notification and monitoring expenses, reputational harm, and litigation risk. As a result, the Board learned that differing costs exist between destructive attacks and data theft. For example, in a ransomware negotiation scenario, threat actors can financially impact an organization by destroying its IT infrastructure. However, regulatory implications can culminate in even greater costs to impacted organizations, ultimately giving threat actors more control over their targets.[322]

Organizations also expended time, productivity, and money on incident response, remediation efforts, reputation management, and system reconfigurations, as well as other follow-on effects such as termination of contracts (among BPOs and client companies) and insurance adjustments. The Board determined the rise in cyberattacks necessitate investments in security measures and business processes; however, the ongoing cost of maintaining and updating these controls can pose a significant burden to organizations, possibly impacting customer friction, innovation, and profitability.

The Board found that innocuous personal information such as job titles, employer information, and work locations, which employees often post on social media, can provide threat actors with enough information to cross-reference public information sources and discover important personal data about critical employees. While reinforcing operational security measures may diminish threat actors' resources for leveraging dangerous harassment techniques, like doxing and swatting, the Board concluded that many of these measures are time-consuming and severely interrupt an employee's private life.

[322] Cybersecurity Company, CSRB Meeting.

3. RECOMMENDATIONS

The Cyber Safety Review Board's (CSRB, or the Board) recommendations are organized under four themes: strengthening identity and access management (IAM); mitigating telecommunications and reseller vulnerabilities; building resiliency across multi-party systems with a focus on business process outsourcers (BPOs); and addressing law enforcement challenges and juvenile cybercrime.

The recommendations outlined in this section reflect the Board's tasking to identify improvements for cybersecurity and make independent, strategic, and actionable recommendations to the President. The Board calls on organizations to implement improvements to build resiliency against the threats posed by groups like Lapsus$, particularly through stronger access controls and authentication methods, and mature risk management for their entire enterprises, including third party vendors. The Board calls on telecommunications providers to employ stronger security protocols to prevent SIM swapping, and on federal regulators such as the Federal Communications Commission (FCC) and Federal Trade Commission (FTC) to ensure those improvements are made through appropriate regulatory oversight and supervision. The Board also calls on lawmakers to create and support community programs that disincentivize juveniles from engaging in, while helping law enforcement deter, cybercrime and ensuring government agencies receive adequate funding and resources.

3.1. IDENTITY AND ACCESS MANAGEMENT (IAM)

IAM weaknesses described in this report are some of the most serious vulnerabilities in the digital ecosystem. Dramatic improvements are necessary and will require a "whole of industry" approach to innovate and implement meaningful solutions.

National Cybersecurity Strategy

As laid out in the National Cybersecurity Strategy, the burden of change should fall on the organizations most capable and best positioned to make the digital ecosystem secure and resilient.[323] In line with federal agencies' adoption of modern multi-factor authentication (MFA),[324] enterprises should implement appropriate controls and alternative authentication factors to better protect their environments, partners, suppliers, and employees. To support these efforts, the federal government should provide funding, incentives, and guidance for organizations to mature their authentication methods and work toward a passwordless world.

3.1.1. Everyone Must Progress Toward a Passwordless World

The attacks described in this report illustrate how easy attackers find obtaining authentication strings, including plaintext passwords, application programming interface (API) keys, session tokens, one-time passcodes, and other credentials via phishing and malware, as well as gaining access to password databases and credentials stored in source code. The digital ecosystem needs to prioritize moving beyond use of text-based strings for authentication.

Technology Providers Should Design and Deliver Secure IAM Solutions by Default

The Board recommends that technology providers innovate and deliver easy-to-use, secure-by-default IAM solutions that eliminate the need for text-based strings for authentication.

- Web and mobile application developers should **leverage Fast IDentity Online (FIDO)2-compliant, hardware-backed solutions built into consumer devices by default.**[325, 326] Use of these built-in tokens should have easy

[323] The White House, "*National Cybersecurity Strategy*," March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[324] OMB, "*M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*," January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[325] FIDO Alliance, "*Android Now FIDO2 Certified, Accelerating Global Migration Beyond Passwords*," February 25, 2019, https://www.fidoalliance.org/android-now-fido2-certified-accelerating-global-migration-beyond-passwords
[326] FIDO Alliance, "*Expanded Support for FIDO Authentication in iOS and MacOS*," July 1, 2020, https://www.fidoalliance.org/expanded-support-for-fido-authentication-in-ios-and-macos

integration with applications and web-based services, leveraging standards such as WebAuthn[327] and technologies such as Passkeys.[328]

- Technology providers should **immediately begin to transition away from Short Message Service (SMS) and voice MFA**. Transitioning from SMS and voice MFA to stronger MFA methods is consistent with National Institute of Standards and Technology (NIST) 800-63B (Rev. 3) and other globally accepted guidance.[329, 330, 331] See Appendix B for further details on the strengths and weaknesses of different authentication methods.
- Operating system developers, web browser designers, and hardware manufacturers should **address the widespread theft and monetization of authentication cookies, such as via infostealer malware, by implementing secure-by-default safety mechanisms** that protect these credentials. For example, online service providers could automatically and silently reissue cookies, possibly every hour, to reduce the window of opportunity for attackers to reuse them.
  - Hardware-backed schemes could help raise the bar for defending against cookie theft. For example, proposals like Device Bound Session Credentials (DBSC) and Browser Proof-of-Possession (BPoP) aim to mitigate cookie and token theft techniques by providing application-level binding and browser-initiated refreshes.[333, 334]

Secure by Design

In 2023, CISA introduced an initiative to drive technology providers to prioritize consumer safety in every stage of the product development lifecycle. Building in robust IAM solutions would be an important step to achieving more security and reduced risk for consumers.[332]

The U.S. Government Should Provide Standards, Guidance, and Tools to Support Organizations' Authentication Journeys

The United States (U.S.) government is responsible for shaping the digital ecosystem in a direction that puts the user first and harmonizes security and accessibility. The National Cybersecurity Strategy commits the U.S. government to take urgent steps in defending today's digital ecosystem while simultaneously building a more sustainable and resilient future.[335] Modernizing and securing authentication is at the forefront of this approach. The Office of Management and Budget's (OMB) Zero Trust Strategy and the Cybersecurity and Infrastructure Security Agency's (CISA) More Than a Password campaign emphasize the importance of MFA.[336, 337] The Board recommends that the U.S. government support organizations' authentication maturity roadmaps by providing guidance that addresses their respective realities and dependencies.

The U.S. government, specifically OMB, NIST, and CISA, in consultation with the Office of the National Cyber Director and other Departments and Agencies, as appropriate, should collaborate with industry stakeholders to **develop and promote a secure authentication roadmap that can help organizations make the transition to a world without passwords**. This roadmap should include standards and frameworks, guidance, tools, and technology specific to organizations' needs and circumstances that account for size, industry, threat profile, as well as privacy and civil liberties considerations. This guidance should also enable organizations to assess their authentication maturity and

[327] Balfanz, Dirk et al.; W3C, "*Web Authentication: An API for accessing Public Key Credentials Level 1*," March 4, 2019, https://www.w3.org/TR/webauthn-1
[328] Bertocci, Vittorio; Auth0, "*Our Take on Passkeys*," August 24, 2022, https://auth0.com/blog/our-take-on-passkeys
[329] NIST, "*SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management*," June 2017 (updated March 2, 2020), https://www.doi.org/10.6028/NIST.SP.800-63b
[330] CISA, "*Implementing Phishing-Resistant MFA*," October 31, 2022, https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
[331] ENISA and CERT-EU, "*Joint Publication 22-01: Boosting your Organisation's Cyber Resilience*," February 14, 2022, https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience/@@download/fullReport
[332] CISA, "*Secure by Design, Secure by Default*," https://www.cisa.gov/securebydesign
[333] The proposal for DBSC aims to reduce account takeover via cookie theft. For additional information, see: Web Incubator Community Group; W3C, "*DBSC (Device Bound Session Credentials)*" July 5, 2023, https://github.com/WICG/proposals/issues/106
[334] The proposal for BPoP aims to prevent unauthorized or illegitimate parties from using leaked or stolen access tokens. For additional information, see: Microsoft Edge, "*Demonstrating Proof-of-Possession in the Browser Application (BPoP)*," June 9, 2023, https://github.com/MicrosoftEdge/MSEdgeExplainers/blob/main/BindingContext/explainer.md
[335] The White House, "*National Cybersecurity Strategy*," March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[336] OMB, "*M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*," January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
[337] CISA, "*More than a Password*," June 6, 2022, https://www.cisa.gov/MFA

progress toward leading practices, including password policies and strategies, zero trust architecture (ZTA) implementation, and authentication lifecycle management.

3.1.2. Organizations Should Prioritize Efforts to Reduce the Efficacy of Social Engineering

As organizations integrate more robust authentication capabilities within their environments, they have an opportunity to reduce the efficacy of social engineering attacks. This will require prioritizing culture alongside more effective technology capabilities.

- Organizations should begin to **require an explicit authentication event using a form of phishing-resistant MFA, such as FIDO2-backed tokens, for each sensitive transaction executed on their systems**. The definition of a sensitive transaction will be dependent on the nature of the organization's business but may include accessing a sensitive customer record; using privileged access in the infrastructure, for example to raise privileges to Administrator; or performing a Subscriber Identity Module (SIM) swap.
- Organizations should educate employees on a frequent and regular basis, possibly monthly, and in a relatable and easily digestible manner, on the latest threat landscape trends and how to prevent them. Organizations **should foster a security culture where employees are incentivized to report potential intrusions** while training employees on how to identify and respond to creative social engineering attacks.[338]

The U.S. government should spearhead the development and promotion of resources that help organizations develop a robust security culture, including monthly training material and example protocols that help deter common social engineering techniques. In doing this**, the government should continue fostering cross-sector collaboration and information sharing between organizations, government agencies, and cybersecurity experts**.

3.2. TELECOMMUNICATIONS AND RESELLER VULNERABILITES

As observed in this review, threat actors targeted telecommunications providers and the critical infrastructure in which they operate. Customers and retailers are at risk for social engineering and other manipulation schemes, which allow threat actors to access sensitive information and backdoors to additional targets. The telecommunications industry, as well as federal regulators, should take steps to build resiliency against fraudulent activities and help defend individual customers, retail employees, and the industry as a whole from threat actors.

3.2.1. Build Resiliency Against Fraudulent Subscriber Identity Module (SIM) Swapping

Telecommunications providers and resellers should implement countermeasures for SIM swap attacks. While some of these measures will add friction into the customer experience, the Board believes countermeasures are necessary to further prevent fraudulent SIM swaps, and follow-on crimes, from occurring. To comprehensively address the most common mechanisms behind fraudulent SIM swaps, telecommunications providers should take the following actions.

Build Resiliency Against Social Engineering in SIM swapping Procedures to Protect the Consumer

- **Provide the ability for customers to lock their accounts to prevent SIM swaps.** This should lock SIM swap capabilities at all levels of the telecommunications provider's systems, including backend and customer support access, operated either by the telecommunications provider directly or their BPOs, vendors, and partners. Customers should also be provided with a strong multi-layered identity validation process to unlock their account for a valid SIM swap.
- Make **strong identity verification for SIM swaps the default on all customer accounts** such that customers would have to "opt out" of having enhanced authentication security protections.
- **Treat SIM swaps as a highly privileged action** with tight controls on who can perform them. Best practice controls should be put in place, such as those used in the banking industry.[339] This may include:

[338] The Board acknowledges the background context provided by SocialProof Security; CSRB Subcommittee Meeting.
[339] FDIC, "*Banker Resource Center: Information Technology (IT) And Cybersecurity*," https://www.fdic.gov/resources/bankers/information-technology

- **enforcing a waiting period of up to 24 hours**, based on risk modeling, if a customer does not have sufficient identity credentials available. This would allow the provider to notify an account holder of an attempt to activate a new SIM card on their account, as well as provide the customer a window of opportunity to confirm or reject the request;
- **applying additional measures, such as taking a photo of the SIM swap requester**, if strong authentication credentials are unavailable. This measure would create a deterrence for malicious actors while balancing the needs of vulnerable populations such as victims of domestic violence, homeless people, single parents, etc., who might not have strong credentials;
- **requiring strong identity validation before performing a SIM swap** while also maintaining robust exceptions procedures if a customer cannot provide this identification. Strong identity validation could include providing two forms of government-issued credentials in person, or through a third-party identity provider like login.gov;
- **requiring a requestor to use video chat or a comparable tool to visually provide strong credentials** when completing a transaction online or over the phone. If video chat is unavailable, a waiting period of at least 24 hours would ensue with the same purpose;
- **providing account holders with a detailed record when a SIM swap occurs**, including who initiated the request, when it was initiated, how the action was performed, and other relevant information;
- **providing increased, mandatory, frequent, and recurring cybersecurity training** focusing on fraudulent SIM swaps and insider threats to retail employees and others involved in adding, modifying, and deleting phone service;
- **limiting the number of persons** allowed to perform SIM swaps to those trained, reviewed, and trusted, and regularly reviewing access permissions;
- **improving personnel security checks** and employee tracking across telecommunications providers and retail stores to the extent possible in compliance with applicable employment laws;[340]
- **limiting collection and sharing of personally identifiable information (PII)** with employees to what is necessary for the specific transaction and regularly removing unnecessary data from their systems;
- **requiring** an employee (also partner, vendor, BPO, etc.) issuing the SIM swap request **to successfully complete an authentication challenge when the request is submitted to the system**, using a strong MFA solution such as a hardware-backed FIDO key or a biometric authentication;
- **tracking the number of fraudulent SIM swaps** monthly by dealer/reseller and **imposing business costs,** such as ceasing to continue business, with those that do not take action to mitigate or stop fraudulent swaps; and
- **handling fraudulent SIM swaps as a crime**, including referral of cases to law enforcement.

[340] CSRB recognizes that employees suspected of wittingly engaging in fraudulent SIM swaps or repeatedly completing them may not always be subject to criminal or legal action apart from having their employment terminated. While recognizing that employment laws in some states may prohibit a former employer from sharing disciplinary information or reasons for termination, CSRB encourages the telecommunications industry to consider reviewing and where possible, adopting insider threat models and other practices employed by industries such as the financial sector and airports.

Additional Methods to Exploit SMS/voice MFA

While not attributed to the threat actors in this review, the Board heard of additional methods threat actors use to exploit SMS/voice MFA that informed its recommendations to telecommunications providers and resellers. Methods to initiate a fraudulent SIM swap with internal resources include generating telecommunications provider codes;[341] stealing customer account management devices in "smash-and-grabs" at wireless retail stores; deploying malware on point-of-sale workstations at telecommunications provider stores; and using an automated Telegram bot to abuse wireless carriers' APIs to PII, Customer Proprietary Network Information (CPNI), and corporate data.[342]

Similar to SIM swapping is a technique called port-out fraud, where a threat actor impersonates the target to that individual's phone provider to transfer the target's phone number to an account set up by the threat actor. This tactic directs phone calls and texts that were intended for the target to the threat actor's phone, allowing the intercept of SMS and voice MFA.[343, 344]

Prevent Exploitation of Vulnerabilities on Point-of-Sale Systems through Improved Asset Management

- **Detect and mitigate theft and abuse of point-of-sale devices and tablets** at retail stores that are used to process customer transactions. If the devices are stolen or abused in-store, they should be rendered unable to perform any privileged actions, including SIM swaps, by wiping them remotely within a standardized timeframe or revoking trusted access until they can be properly assessed.

- **Use ZTA concepts in retail stores** to prevent untrusted or new devices from joining the network, including virtual systems. This should include regular vulnerability scanning and subsequently de-trusting devices that do not have up-to-date patching or configurations.

Apply Measures to Harden the Technology Stack

- **Assess and harden all applications and APIs used to manage customer accounts, including those enabling SIM swaps.** These applications and APIs should be considered sensitive and use industry best practices, including secure coding principles;[345] server and application hardening, for example transmission confidentiality and integrity and information flow enforcement;[346] and routine third-party audits and penetration tests.

3.2.2. Strengthen Federal Communications Commission (FCC) and Federal Trade Commission (FTC) Oversight and Enforcement Activities

Organizations' and consumers' reliance on mobile phones and cellular service make them essential components of the nation's telecommunications practices. Fraudulent SIM swaps undermine the security and reliability of the telecommunications ecosystem. While fraudulent SIM swaps happen relatively infrequently, the consequences can be extraordinarily damaging and disruptive. Victims are often impacted both financially and physically, as the threat actors are often involved in "traditional" crimes such as theft, kidnapping, extortion, murder, and sexual abuse.[347]

Telecommunications industry regulators need to standardize and facilitate the adoption of best practices to reduce or eliminate fraudulent SIM swaps. FCC and FTC **should strengthen oversight and enforcement activities** focused on fraudulent SIM swapping transactions with the following actions.

[341] Security Researcher 1, CSRB Meeting.

[342] Security Researcher 2, CSRB Meeting.

[343] FCC, "*Port-Out Fraud Targets Your Private Accounts*," September 16, 2019, https://www.fcc.gov/port-out-fraud-targets-your-private-accounts

[344] Lee, Kevin et al.; USENIX Association, Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020), "*An Empirical Study of Wireless Carrier Authentication for SIM Swaps*," August 10, 2020, https://www.usenix.org/system/files/soups2020-lee.pdf

[345] Turpin, Keith et al.; OWASP, "*Secure Coding Principles: Quick Reference Guide*," December 2022, https://www.owasp.org/www-project-secure-coding-practices-quick-reference-guide/

[346] NIST, "SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations," September 2020, https://www.doi.org/10.6028/NIST.SP.800-53r5

[347] The Board acknowledges publicly available reports of SIM swaps occurring as recently as 2023, including instances where SIM swappers allegedly stole tens of millions of dollars of cryptocurrency; took over social media accounts to extort their victims financially and sexually; and participated in homicides, swatting, and other crimes. *Source: Vice, "SIM Swapping," https://www.vice.com/en/topic/sim-swapping*

- **Require regular reporting**, for example monthly or annually, on the number of fraudulent SIM swaps impacting a service provider's customers. Reporting should include attacks for all customers using the cellular network of the provider, including attacks involving customers of downstream Mobile Virtual Network Operators.
- **Document and enforce best practices** (see Recommendation 3.2.1) for telecommunications industry business processes, including for their BPOs, retailers, dealers, resellers, and others, for verifying the identity of a customer and performing a SIM swap on their behalf. The banking industry has similar controls and regulatory oversight.[349]
- **Incentivize better security** at telecommunications providers by enacting penalties for fraudulent SIM swaps or lax controls.

FCC Proposed Rules to
Protect Consumers' Cell Phone Accounts

In July 2023, the FCC announced for consideration new rules to protect consumers from SIM swap and port-out fraud. The proposed Report and Order attempt to protect customers by revising the FCC's CPNI Local Number Portability (LNP) rules to require wireless providers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider.[348] While the rules are still pending final vote at the time of publication, continued focus on and specific measures to prevent fraudulent SIM swaps will help build resiliency across the cyber ecosystem.

3.3. RESILIENCY WITH A FOCUS ON BUSINESS PROCESS OUTSOURCERS (BPOs)

Organizations, including associated BPOs and service providers, with robust cybersecurity programs that follows industry-standard practices are better positioned to defend against attacks by external threat actors. Designing, building, and maintaining a strong security framework does not create perfect defense, but it forms the essential foundation for ongoing risk management of complex and dynamic business needs, technology, and attacker tradecraft.

3.3.1. Plan for Disruptive Cyber Intrusions and Invest in Prevention, Response, and Recovery Capabilities

Organizations should create roadmaps to **rapidly adopt emerging modern architectures** that can best defend against disruptive cyber-intrusions caused by groups such as Lapsus$ and related threat actors.

- Organizations should carefully **tune their cybersecurity program to adopt best practices** in the NIST Cybersecurity Framework (CSF),[350] with a particular emphasis on:
  - robust information technology (IT) asset management practices to **identify an organization's critical infrastructure** (CI), provide adequate visibility of networks, and map attack surfaces to the greatest extent possible;
  - **effective implementation of least privilege access methodology and auditing,** especially for assets, accounts, and actions that are highly sensitive; and
  - insightful and actionable **monitoring capabilities** enabled through sound, centralized log management policies. The ability to detect heuristic anomalies in these log files can alert security of an impending incident and capture log file data during an incident already underway and can aid investigation, disruption, and prevention of future attacks.

[348] FCC, "FCC Privacy Task Force Announces Proposed Rules to Protect Consumers' Cell Phone Accounts," July 11, 2023, https://docs.fcc.gov/public/attachments/DOC-395019A1.pdf
[349] FDIC, "*Banker Resource Center: Information Technology (IT) And Cybersecurity*," https://www.fdic.gov/resources/bankers/information-technology
[350] NIST, "*Cybersecurity Framework*," June 8, 2023, https://www.nist.gov/cyberframework

- **Design and implement ZTA** following guidelines or roadmaps such as CISA's Zero Trust Maturity Model[351] that are adapted to each organization's needs and resource constraints.[352]
- **Adopt strong authentication** (see Recommendation 3.1.2).
- Provide employees with **simple processes for reporting suspicious activity**, such as phishing attempts, communications received, or computer irregularities.[353]

Develop and Test a Cyber Incident Response Plan Specific to Extortion, Ransomware, and Harassment-Related Events

Organizations with previously developed cyber incident response plans generally recovered faster from attacks by the class of threat actor discussed in this report. The Board recommends all organizations take similar measures, in particular referencing the NIST Special Publication (SP) 800-61: Computer Security Incident Handling Guide, but also specifically consider the following actions to address the unique nature of the attacks outlined in this report.

During an incident, organizations should follow their established response plan, notify law enforcement as soon as possible, and monitor communications closely for unauthorized participants to reduce impact and prevent future intrusions.[354, 355]

- Outline the organization's desired **response plan procedures to handle and mitigate unique elements of ransomware, extortion, and harassment-related events.**[356, 357, 358]
  - **Determine which mission-critical data, networks, assets, or services**, i.e., the organization's critical infrastructure, should receive prioritized attention and restoration during and after a cyber incident.
  - Lessen the impact of extortion demands and ransoms by documenting **when and how to restore backup data or replace systems** to ensure the integrity of backups. These procedures should be regularly tested and validated to ensure that they can be successfully performed within the organization's required timeframe, for example within six hours.
  - Establish **relationships and information sharing agreements with government and industry partners**, building upon existing communities like Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and trade associations, to create a "community of trust" that supports actionable cooperation before, during, and after an incident.
  - Be prepared to **work closely with law enforcement** (see Recommendation 3.4.2) and to make any **mandatory reporting to regulators.**

[351] Cybersecurity Division; CISA, "*Zero Trust Maturity Model*," April 2023, https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

[352] Computer Crime & Intellectual Property Section, Criminal Division; DOJ, "*Best Practices for Victim Response and Reporting of Cyber Incidents*," September 26, 2018, https://www.justice.gov/criminal-ccips/file/1096971/download

[353] Cisco uses "Keep Cisco Safe" to communicate and educate employees in a genuine way and provide the knowledge necessary for employees to consistently report suspected cybersecurity incidents. *Source: Cisco, "Keeping Cisco Safe," March 11, 2020, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-keeping-cisco-safe-casestudy.pdf*

[354] One company engaged law enforcement, which assisted with attribution. *Source: Targeted Organization, CSRB Meeting.*

[355] FBI investigates malicious cyber activity and gathers intelligence leading to the attribution of cyberattacks to threat actors and deterrence of future intrusions. FBI collects information from victims to assist in the investigation and identify threats to national security to prevent future victimization. If FBI has information in its holdings about the intrusion or threat actors, it can share that information to help a victim's incident response team with mitigation and future resilience. On a limited basis and pending the timeliness and extent of an entity's engagement, FBI may be able to take further action such as freezing stolen funds or providing decryption keys. When victims engage with their local FBI field office as part of the cyber incident response plan, they will contribute to the FBI's mission and overall security of the global cyber ecosystem. *Source: FBI and CISA Panel Interview, CSRB Meeting.*

[356] Microsoft, "*Quickly deploy ransomware preventions*," April 24, 2023, https://learn.microsoft.com/en-us/security/ransomware/protect-against-ransomware

[357] EEOC, "*Promising Practices for Preventing Harassment*," November 11, 2017, https://www.eeoc.gov/laws/guidance/promising-practices-preventing-harassment

[358] Barker, William et al.; NIST, "*NISTIR 8374, Ransomware Risk Management: A Cybersecurity Framework Profile*," February 23, 2022, https://csrc.nist.gov/publications/detail/nistir/8374/final

  - ○ **Develop an internal communication plan** that includes how to contact personnel, how to proceed if they are unreachable, and backup, **out-of-band communication** mechanisms personnel can use if routine lines of communication are disrupted or if their integrity is compromised by the attackers.[359]
  - ○ **Devise procedures to handle swatting and doxing protection for employees.**[360]
  - ○ **Implement a training program** for its workforce on roles, responsibilities, and processes for incident handling notifications and what to expect from threat actors of this kind.

- **Regularly test, update, and exercise** its incident response plan (ideally, quarterly).
- **Encourage BPOs and their clients to agree upon contractual terms** and co-develop response plans, regularly test them, and cooperate fully during incidents as an extension of the client organization (see Recommendation 3.3.2).
- **Build pre-incident trust relationships and establish information sharing agreements** with other private sector organizations; law enforcement, such as Federal Bureau of Investigation (FBI); federal responders, such as CISA; and relevant sector risk management agencies (SRMAs), as needed, to expedite coordination during an incident.
- **Establish clearly defined roles, responsibilities, and contact information** for personnel leading critical response functions during a cyber incident, including, but not limited to, decision makers for notification to response organizations like FBI and CISA; oversight of the cyber incident response effort, including technical mitigation and operational decisions; courses of action to mitigate attacker activity; compliance regarding cyber incident law, policy, and regulations; and public communications (see Recommendation 3.3.2).
- Source and validate **contact information for external industry and government partners**, including, but not limited to, incident response firms and/or security operations centers (SOCs); knowledgeable legal counsel; local FBI[361] and CISA offices; and affected third-party clients or vendors, for example BPOs, cloud service providers, and commercial data centers.

Conduct After-Action Reviews Following an Incident

Affected organizations also reported on the benefits of conducting a robust after-action review to learn from an incident and identify areas for improvement. Such after-actions should, at minimum:[362]

- consider the need to improve the **organization's incident response plan**, including its assigned roles and responsibilities; communication and training plans; and technical mitigation processes and priorities;
- **address legal, policy, and regulatory considerations** before a future incident occurs; such hurdles might include, but are not limited to, liability and privilege concerns the general counsel may have experienced when sharing incident information with government entities;[363] and

[359] In some intrusions, a Cybersecurity Company knew that Lapsus$ was reading emails and recommended that a victim company use out-of-band communications. *Source: Cybersecurity Company, CSRB Meeting.*

[360] NIJ, "*Ranking Needs for Fighting Digital Abuse: Sextortion, Swatting, Doxing, Cyberstalking and Nonconsensual Pornography*," November 20, 2020, https://nij.ojp.gov/topics/articles/ranking-needs-fighting-digital-abuse-sextortion-swatting-doxing-cyberstalking#identification-of-top-tier-needs-to-address-technology-facilitat

[361] FBI told the Board its goal is to build trust with the organizations it serves across both the private and public sectors. It can most effectively accomplish this by developing relationships with organizations before a cyber intrusion occurs. When FBI has an established relationship with an organization, it can share unique intelligence and be transparent about what FBI can and cannot do. *Source: FBI and CISA Panel Interview, CSRB Meeting.*

[362] Since the Lapsus$ attack, one company implemented monthly conversations for BPOs to discuss threat intelligence, which they had not been doing previously. Another company enhanced its telemetry to enable visibility of device content and trust levels across the organization, an ability it did not have prior to January 2022. *Source: Targeted Organization, CSRB Meeting.;* Targeted Organization*, CSRB Meeting.*

[363] Some respondents shared that the U.S. government should consider expanding liability and privilege protection for the victimized organization, which can otherwise serve as a barrier to post-intrusion reporting. We should seek to expand liability and privilege protections so victims can engage efficiently and without risk, with non-regulatory federal government agencies. In recent years, Congress and the U.S. government have taken important steps to reduce barriers to cybersecurity-related information sharing by the private sector, including the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

- **determine whether to report additional details** about the incident to the government or a trust community to spread awareness about the threat, reduce the likelihood of a similar event happening to others, and further the relationships by which advance warning of future threats may be shared.

3.3.2. Business Process Outsourcers (BPOs) and Client Companies Should Mature and Strengthen their Risk Management Practices Reflecting their Shared Risk, and the United States (U.S.) Government Should Support These Efforts

Client Organizations and BPOs Should Agree Upon a Shared Responsibility Model for Cybersecurity Risk, Enshrined in Contracts

Organizations should **incorporate cybersecurity requirements in contract language** to ensure that BPO operations meet the same level of security as internal company practices. This should include clear definitions of the service level agreements (SLAs) that enable monitoring and risk management.

In some circumstances, such as BPOs handling highly sensitive transactions, consider **securing BPO staff operations similar to the standards for client company staff**, including BPO staff use of client-owned hardware and client-driven cybersecurity processes. Generally, these contractual requirements should consider:

- the use of strong authentication for access management, especially for sensitive transactions (see Recommendation 3.1.1);
- training for BPO employees with respect to their client organization;
- data handling, processing, and storage;
- secure software development lifecycle (SDLC) management;
- device management and compliance for BPO employees; and
- co-ownership of incident response, with clear roles and responsibilities (see Recommendation 3.3.1).

BPOs Should Establish Mature Information Sharing Relationships with their Industry Peers

Recognizing that attackers look for sector-specific vulnerabilities, BPOs should **grow and mature grassroots information sharing efforts**, potentially establish an ISAC or ISAO (or similar trust community) that facilitates information sharing, develop best practices, and coordinate industry development and delivery of training based on recurring threats.

- When developing pre-incident relationships, BPOs should consider ahead of time how best to engage during an incident. This pre-incident coordination and planning will likely improve the effectiveness of government and victim response and empower the U.S. government to prevent future attacks against other would-be victims.

The U.S. Government Should Drive Mechanisms to Gain Visibility into Aggregate Risk Associated with BPOs

The Board recommends that **CISA support the establishment and operation of trust communities among BPOs** and their clients. Additionally, CISA should encourage private sector data set creators, such as those that author threat intelligence summaries, to **tag their underlying incident history data** to get increased visibility on BPO incidents and support community collaboration.

3.4. LAW ENFORCEMENT AND JUVENILE CYBERCRIMES DISINCENTIVES

Disruption of threat actors and their ongoing attacks are necessary components of a resilient and robust ecosystem that can keep the nation safe from the type of criminal activities described in this report. This requires a collaboration between law enforcement, the private sector, and international partners. The ability to disrupt the attacks by Lapsus$

However, the Board's interactions with certain victims, or lack of interactions with other victims who have declined to speak with the Board, reveal that more work needs to be done to ensure that concerns about legal liability relating to an intrusion, and actions that victims and their counsel take to minimize exposure to such liability, are still inhibiting the sharing of cybersecurity information, leading to a net negative for collective cybersecurity and public safety.

and related groups was complicated by several factors: the juvenile status of some of the threat actors; geographically dispersed threat actors; and the cross-border nature of the crimes. The following recommendations emphasize the need for an international and "whole-of-society" effort to mitigate these challenges.

3.4.1. Advance "Whole-of-Society" Programs and Mechanisms for Juvenile Cybercrime Prevention and Intervention

The Board recommends developing stronger U.S. juvenile cybercrime prevention and intervention programs. For example, the Cyber Offender Prevention Squad (COPS), part of the Dutch National High-Tech Crime Unit (NHTCU), started an information campaign, with workshops and an intervention program to deter young people from online criminal activity, offering positive and legal alternatives. Their initiatives focused on preventing potential offenders as well as engaging prior offenders to decrease recidivism.[364] These programs arose out of a realization that young cybercrime offenders, unlike counterparts operating primarily in the physical world, are often able to evade parental, educator, community, and law enforcement scrutiny and intervention on their journey to significant cybercriminal activity. Despite the federal government and the private sector's expenditure of tens of billions of dollars annually on cybersecurity, the Board's inquiry did not identify any notable juvenile cybercrime prevention and intervention programs in the U.S. at the federal government, local government, community, or private sector level.

- **Congress should explore funding juvenile cybercrime prevention programs** through national law enforcement and national grant-making programs like those managed by Department of Justice's (DOJ) Office of Justice Programs (OJP), and other appropriate mechanisms.[365]
- Although federal law enforcement often leads investigations of significant cybercrime groups targeting U.S.-based victims, the Federal Juvenile Delinquency Act requires that most juvenile hacking prosecutions must be brought in state courts.[366] **Congress should explore funding or other mechanisms to ensure continuity and an eventual prosecution upon the transfer of juvenile cybercrime investigations from federal to state authorities,** which could have the effect of more successfully deterring U.S.-based juvenile hacking and hacking-enabled cybercrimes and preventing recidivism.

3.4.2. Increase Timely Reporting of Cyberattacks to Federal Responders

Organizations experiencing cyberattacks are not currently required to report such crimes to federal law enforcement or any other single federal agency. Some may not clearly understand the importance of their reporting of cybercrime incidents to law enforcement and other federal agencies that can disrupt ongoing and future incidents and mitigate risks to other potential victims, thereby creating blind spots and hampering collective cybersecurity. Without information gathered from targeted organizations, the federal government may not be able to understand the larger threat landscape and may be hampered in its timely ability to warn other targeted entities; recommend mitigation measures; take down malicious infrastructure; seize ill-gotten cryptocurrency or fiat currency; bring those responsible to justice; or otherwise disrupt malicious activity. While implementation of required reporting of covered cyber incidents and ransom payments by covered entities under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, will improve federal agencies' visibility significantly, voluntary reporting of confirmed or suspected cyberattacks and suspicious activity will continue to be critical to collective cybersecurity efforts. For such reasons, the Board recommends private sector organizations impacted by malicious cyber activity to fortify

[364] Ramaker, S. and Zonderland, L.; inCyber, "*Prevention is better than cure*," August 23, 2021, https://www.incyber.org/en/prevention-is-better-than-cure-2

[365] The Department of Justice's Office of Justice Programs "provides federal leadership in developing the nation's capacity to prevent and control crime, administer justice, and assist crime victims." *Source: DOJ, "Organization, Mission and Functions Manual: Office of Justice Programs," August 27, 2014 (updated September 22, 2022), https://www.justice.gov/doj/office-justice-programs*

[366] The Board examined a possible recommendation to increase deterrence for adults who may consider using a minor to commit a cyber or cyber-enabled crime. However, the Board noted that the United States Sentencing Guidelines already contain an enhancement for instances where an adult defendant "used or attempted to use a person less than eighteen years of age to commit the offense or assist in avoiding detection of, or apprehension for, the offense." United States Sentencing Guidelines, § 3B1.4 (2021), and the application note provides further that, in an instance where a defendant uses or attempts to use more than one person less than eighteen years of age, an upward departure from the applicable Guidelines range may be warranted. *Source: United States Sentencing Commission Guidelines Manual, "§3B1.4, Using a Minor To Commit a Crime," 2021, https://guidelines.ussc.gov/gl/%C2%A73B1.4*

relationships with federal security and mitigation partners pre-incident and improve frequency and prompt reporting to such partners upon an incident occurring.

- **Private sector organizations should increase reporting of cyber incidents and indicators of compromise (IOCs) to the federal government** when the organizations suspect or suffer from a cyber intrusion or attack.
- **Private sector organizations should report incidents in a timely fashion** to enable appropriate federal responders to support victims and render immediate assistance. Federal responders may have specific knowledge about threat actors, allowing them to freeze stolen funds; provide decryption keys; take down malicious infrastructure like exfiltration servers, leaks sites, command-and-control (C2) infrastructure, or botnets; or aid a victim's incident response team with mitigation or future resilience planning. Timely reporting may also support warnings and the development of mitigation recommendations to protect other potential victims.

The National Cybersecurity Strategy outlines the federal government's plan to strengthen the National Cyber Incident Response Plan, specifically, to further **implement a policy that "a call to one is a call to all."**[367] As part of that effort, the Board therefore recommends the U.S. government provide clear, consistent guidance, or clarify and further publicize existing guidance, about federal departments' and agencies' cyber incident-related roles and responsibilities in a highly visible and unified manner to improve coordination during and post cyber incidents.

- **Provide private and public sector partners with information concerning federal and state responder contact information, available services for victims, and individual agencies' unique missions and authorities** to best assist a targeted entity during a cyberattack.
- **Explain the liability and privilege protections afforded to victims and personnel that share cybersecurity-related information with federal responders** and with each other. The Cybersecurity Information Sharing Act of 2015 (CISA 2015) provides statutory protections to non-federal entities that share cyber threat indicators and defensive measures in accordance with CISA 2015 with the federal government and with each other.[368] However, the lack of awareness or confusion around these provisions inhibits respondents and their legal counsel from reporting critical information. As CISA 2015 approaches its sunset and potential renewal in 2025, **Congress should seek out stakeholder feedback to understand why private sector entities continue to report cybercrimes and share cyber threat information at low levels that inhibit collective cybersecurity efforts.**
- **Legislate to provide more protection for providers of online services whose platform security personnel identify evidence of a crime** in online communications while conducting their standard platform protection duties. At least one cybersecurity researcher respondent advised the Board that their employer's legal counsel was confused by the term "inadvertently" in 18 U.S. Code (U.S.C.) § 2702(b)(7)(A) and whether personnel conducting platform protection duties could be deemed to have "inadvertently" found information that appears to pertain to the commission of a crime (and thus be able to provide the contents of relevant customer communications to law enforcement) if those personnel were actively looking to identify and prevent such abuse. The researcher noted that such confusion had prevented their ability to share such information with law enforcement on countless occasions.
- **Clarify the relationship, or lack thereof, between law enforcement and federal regulators**, to address private sector misconceptions that law enforcement is a regular conduit of information to regulators.

The Board endorses Strategic Objective 2.1 of the National Cybersecurity Strategy (Integrate Federal Disruption Activities), which seeks to make federal disruption campaigns "so sustained and targeted that criminal activity is rendered unprofitable" while "increas[ing] the volume and speed of these integrated disruption campaigns."[369]

[367] Strategic Objective 1.4: Update Federal Incident Response Plans and Processes. The White House, "*National Cybersecurity Strategy*," March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[368] Pursuant to CISA 2015, DHS and CISA have issued joint guidance explaining how non-federal entities can share this information with the federal government and avail themselves of these protections. *Source: DHS and DOJ, "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity and Information Sharing Act of 2015," October 2020, https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf*

[369] Strategic Objective 2.1: Integrate Federal Disruption Activities. The White House, "*National Cybersecurity Strategy*," March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

However, the Board notes that compared to its irreplaceable role in advancing these goals and the country's cybersecurity, federal law enforcement is under-resourced within the federal government. Unless Congress addresses this issue, no amount of increased victim reporting will accomplish the Administration's strategic goals to dramatically reduce the incidence and impact of cybercrime.

3.4.3. Increase International Law Enforcement Cooperation

Respondents consistently noted that timely international cooperation is essential to the long-term disruption of cybercrime threats generally. Some respondents specifically noted that such collaboration between U.S. and international law enforcement partners led to the late 2022 arrest of Lapsus$ members, thereby apparently causing the group's malicious activities to cease. Central to their opinions regarding the necessity for such international cooperation was the dispersed networks of cybercriminals and the transnational nature of online infrastructure, service, and digital asset technologies (and their underlying records), which require global collaboration to locate digital evidence, infrastructure, and persons involved in cybercrime activities.

To improve the timeliness and effectiveness of law enforcement efforts of the type that disrupted the Lapsus$ group in 2022, the Board endorses the law enforcement-related efforts described in Pillar 5 of the National Cybersecurity Strategy (Forge International Partnerships to Pursue Shared Goals) and related recommendations.

- **Enhance law enforcement resources devoted to international law enforcement cooperation, including operational collaboration** against transnational cyber threats, such as FBI's Cyber Legal Attaché program and dedicated federal prosecutors.
- **Strengthen international collaboration mechanisms to ensure effective information sharing and deconfliction** to better prevent cybercriminals from evading the rule of law.

3.4.4. Build Resilience for Emergency Disclosure Requests (EDRs) Against Social Engineering Attacks

Title 18 U.S.C. § 2702 generally prohibits providers from disclosing their users' records and communications, but exceptions in that statute permit providers to divulge a subscriber's information, including the content of communications, to a government entity based upon the provider's good faith belief that "an emergency involving danger of death or serious physical injury to any person requires disclosure without delay." Providers often decide to divulge records after law enforcement informs them of such an emergency through a form called an "Emergency Disclosure Request" (EDR). Providers may also decide to divulge records if they learn about an emergency through another source, such as a concerned parent. Providers are responsible for deciding whether an emergency exists and must assess the credibility and authenticity of anyone submitting an EDR.

Recognizing that providers are faced with difficult choices between protecting customer privacy and preventing death or serious bodily injury, providers should devote appropriate resources to the task of verifying the authenticity and credibility of EDRs so that providers reduce mistakes in either direction. For example, providers should examine whether they should design and implement new mechanisms for verifying the authenticity of EDRs using solutions such as standardized digital signatures. These measures should:

- address **how threat actors have or could abuse existing EDR processes** to fraudulently obtain sensitive information; and
- assign roles and responsibilities for service providers to **verify the legitimacy of EDRs**.

APPENDIX A: SUMMARY OF CSRB INTERVIEWS AND REQUESTS FOR INFORMATION

The Board's review involved organizations and individuals representing a variety of viewpoints, including targeted organizations, law enforcement, cyber threat intelligence, incident response, regulators, cybersecurity and industry experts, cyber incident focused law firms, insurers, and others. The Board requested information in the form of briefings and written materials.

The Board is grateful for the voluntary participation of those parties that provided timely responses. Their efforts helped the Board collect the observable timeline of events, corroborate facts, and understand the complex and nuanced dimensions of the incidents associated with Lapsus$ and similar groups.

TARGETED ORGANIZATIONS

During its review, the Board contacted 12 targeted organizations, which remain anonymized given the sensitivity of their participation.

- Submitted materials or briefed the Board (6)
- Did not respond (2)
- Declined to participate (4)

RELATED BRIEFINGS

The Board also engaged with 28 other organizations with expertise in Lapsus$ and associated threat actor groups, as well as other organizations for their expert input on related topics. Those organizations are identified below.

- Arceo Labs, Inc d/b/a Resilience
- CrowdStrike Holdings, Inc.
- CTIA – The Wireless Association
- Cybercrime Support Network
- Cybersecurity and Infrastructure Security Agency (CISA)
- Dutch National Police
- EJ2 Communications d/b/a Flashpoint
- Fast IDentity Online (FIDO) Alliance, Inc.
- Federal Bureau of Investigation (FBI)[370]
- Federal Communications Commission (FCC)
- Federal Trade Commission (FTC)
- First Mile Group Inc, d/b/a Alloy
- Homeland Security Investigations (HSI)
- Intrinsec Securite
- Kroll Inc.
- Mandiant, Inc.
- Microsoft Corporation
- National Crime Agency (NCA)
- Paladin Capital Management, LLC
- Palo Alto Networks, Inc.

[370] FBI caveated that their analysis is limited to the time of their reporting to the Board and may be superseded by additional intelligence or investigative information, if discovered following the publication of the report.

- Princeton University, Center for Information Technology Policy (CITP)[371]
- Recorded Future, Inc.
- Security Scorecard, Inc.
- ShadowDragon, LLC
- SocialProof Security, LLC
- Stroz Friedberg, Inc. (acquired by Aon Risk Solutions)
- Unit 221B, LLC
- Verizon Communications Inc.

MEDIA AND INDUSTRY BLOGS

Throughout its review, the Board prioritized the use of primary sources, assigning greater weight to statements and reports by targeted organizations and subject matter experts. However, in some instances, organizations provided the Board access to non-public information, or they provided material information only to secondary sources such as journalist. In these instances, the Board thought necessary to attributed information to a secondary source. These include articles and industry blogs written by the following persons; their materials are cited in this report where the information was referenced.

[371] The Board recognizes the individual contributions of Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan.

APPENDIX B: MULTI-FACTOR AUTHENTICATION (MFA) TYPES AND RISK ASSESSMENT

BACKGROUND

The National Institute of Standards and Technology (NIST) defines multi-factor authentication (MFA) as an authentication system that requires more than one distinct authentication factor for successful authentication. The three authentication factors are something you know, such as a password or personal identification number (PIN); something you have, like a cryptographic identification device or token; or something you are, like a biometric.[372]

Organizations may differ slightly in how they categorize the various forms of MFA, but industry, European Union (EU), and Office of Management and Budget (OMB) guidance is consistent with CISA's and NIST's rankings for the following methods of MFA from most secure to least secure: phishing-resistant MFA; app-based MFA (differentiated further by number matching and push notification approaches to MFA); and Short Message Service (SMS)/voice MFA.[373, 374, 375] Figure 2 and the following sections detail the various vulnerabilities of each form of MFA and common exploitation methodologies.

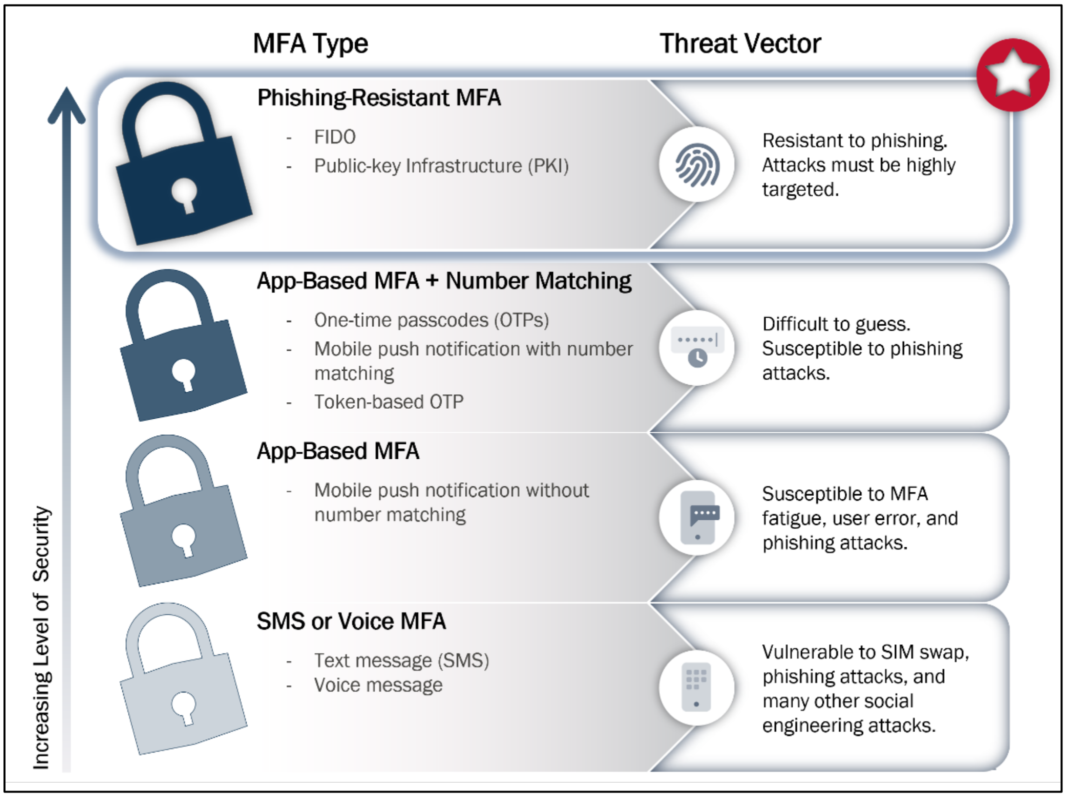

MFA Type
Threat Vector
Increasing Level of Security
Phishing-Resistant MFA
- FIDO
- Public-key Infrastructure (PKI)
Resistant to phishing. Attacks must be highly targeted.
App-Based MFA + Number Matching
- One-time passcodes (OTPs)
- Mobile push notification with number matching
- Token-based OTP
Difficult to guess. Susceptible to phishing attacks.
App-Based MFA
- Mobile push notification without number matching
Susceptible to MFA fatigue, user error, and phishing attacks.
SMS or Voice MFA
- Text message (SMS)
- Voice message
Vulnerable to SIM swap, phishing attacks, and many other social engineering attacks.

Figure 2 - MFA Methods and Common Exploitation

[372] Information Technology Laboratory; NIST, "*MFA*," https://csrc.nist.gov/glossary/term/mfa

[373] NIST, "*NIST Update: Multi-Factor Authentication and SP 800 63 Digital Identity Guidelines*," February 15, 2022, https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf

[374] ENISA and CERT-EU, "*Joint Publication 22-01: Boosting your Organisation's Cyber Resilience*," February 14, 2022, https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience/@@download/fullReport

[375] Shyamsundar, Teju; Okta, "*Why You Should Ditch SMS as an Auth Factor*," May 20, 2020, https://www.okta.com/blog/2020/05/why-you-should-ditch-sms-as-an-auth-factor

PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION (MFA)

Phishing-resistant MFA, including FIDO and public key infrastructure (PKI),[376] which enables digital signatures and encryption, is currently the strongest approach to MFA with the United States (U.S.) government's OMB requiring agencies to adopt the method and the European Union Agency for Cybersecurity and the Computer Emergency Response Team (CERT)-EU releasing a joint publication identifying it as a best practice.[377, 378] FIDO, the only widely available phishing-resistant authentication, runs on top of the WebAuthn authentication protocol and is supported by major browsers, operating systems, and smartphones. PKI is less widely available but effectively ties MFA to an enterprise PKI infrastructure. An example of PKI-based MFA is the use of smart cards, including Common Access Card (CAC) or Personal Identity Verification (PIV), by many government agencies to establish the second identification factor.[379]

APP-BASED MULTI-FACTOR AUTHENTICATION (MFA)

As depicted in Figure 3, app-based MFA is an authentication method that uses a mobile application to provide the second authentication method to log in to a user's account. App-based MFA solutions verify a user's identity by generating a one-time passcode (OTP)[380] or by sending a "push" notification, possibly with number matching implemented, to a mobile application for a user to accept. In the OTP or number matching implementation, the user has an additional step that requires them to type in the OTP or numbers. While they are resilient to some of the vectors available to SMS/voice-based MFA, OTP or number matching is still vulnerable to phishing while push notifications without number matching remain vulnerable to MFA fatigue attacks and user error. CISA recommends OTP or number matching MFA over push notification MFA because of the additional step that can mitigate against MFA fatigue and identifies this method as optimal for organizations that cannot immediately implement phishing-resistant MFA.[381, 382]

[376] PKI is the set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public keys. PKIs are the foundation that enables the use of technologies, such as digital signatures and encryption, across large user populations. *Source: Thales, "What is PKI and What is it used for?" https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki*

[377] OMB, "*M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*," January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

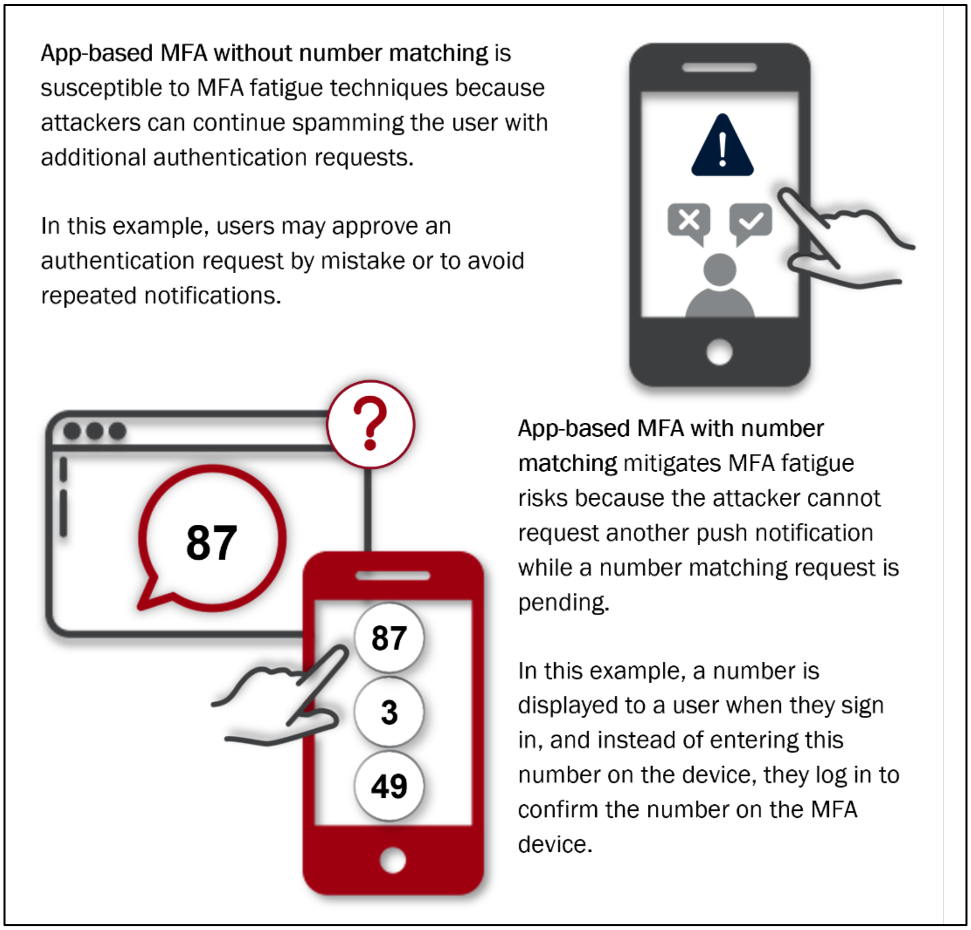
[378] ENISA and CERT-EU, "*Joint Publication 22-01: Boosting your Organisation's Cyber Resilience*," February 14, 2022, https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience/@@download/fullReport

[379] CISA, "*Implementing Phishing-Resistant MFA*," October 31, 2022, https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[380] Tokens can also generate OTPs, which CISA considers a subcategory of app-based MFA. Source: CISA, "Implementing Phishing-Resistant MFA," October 31, 2022, https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[381] CISA, "*Implementing Phishing-Resistant MFA*," October 31, 2022, https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[382] CISA, "*Implementing Number Matching in MFA Applications*," October 31, 2022, https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c.pdf



App-based MFA without number matching is susceptible to MFA fatigue techniques because attackers can continue spamming the user with additional authentication requests.

In this example, users may approve an authentication request by mistake or to avoid repeated notifications.

App-based MFA with number matching mitigates MFA fatigue risks because the attacker cannot request another push notification while a number matching request is pending.

In this example, a number is displayed to a user when they sign in, and instead of entering this number on the device, they log in to confirm the number on the MFA device.

Figure 3 - App-based MFA

SMS/VOICE MULTI-FACTOR AUTHENTICATION (MFA)

NIST, CISA, and Okta are among those organizations that consider SMS/voice MFA the weakest form of MFA. SMS/voice MFA involves sending a code to the user's phone or email, which the user then uses to complete their login. This approach to MFA is subject to relatively simple attack vectors that are easy to exploit without advanced technical skill, like Signaling System #7 (SS7) protocol vulnerabilities[383] and, as demonstrated in many Lapsus$ attacks, social engineering such as Subscriber Identity Module (SIM) swapping and phishing. Although NIST, CISA, and Okta advise that this form of MFA should be avoided to the extent possible, they acknowledge that any MFA method is better than no MFA.[384, 385, 386]

[383] SS7 attacks are mobile cyberattacks that exploit security vulnerabilities in the SS7 protocol to compromise and intercept voice and SMS communications on a cellular network, effectively enabling the threat actor to steal the authentication message sent to a mobile device. *Source: Adam Weinberg, "A Step by Step Guide to SS7 Attacks," April 30, 2023, https://www.firstpoint-mg.com/blog/ss7-attack-guide*

[384] NIST, "*NIST Update: Multi-Factor Authentication and SP 800 63 Digital Identity Guidelines*," February 15, 2022, https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf

[385] CISA, "*Implementing Phishing-Resistant MFA*," October 31, 2022, https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[386] Shyamsundar, Teju; Okta, "*Why You Should Ditch SMS as an Auth Factor*," May 20, 2020, https://www.okta.com/blog/2020/05/why-you-should-ditch-sms-as-an-auth-factor

APPENDIX C: CYBER SAFETY REVIEW BOARD MEMBERS

The following members participated in this review of the Cyber Safety Review Board.

Robert Silvers, Under Secretary for Policy, Department of Homeland Security (Chair)

Heather Adkins, Vice President, Security Engineering, Google (Deputy Chair)

Dmitri Alperovitch, Co-Founder and Chairman, Silverado Policy Accelerator and Co-Founder and former Chief Technology Officer (CTO) of CrowdStrike, Inc.

Jerry Davis, Founder, Gryphon X

Chris DeRusha, Federal Chief Information Security Officer, Office of Management and Budget

Chris Inglis, National Cyber Director, Office of the National Cyber Director

Rob Joyce, Director of Cybersecurity, National Security Agency

Marshall Miller, Principal Associate Deputy Attorney General, Department of Justice

Katie Moussouris, Founder and CEO, Luta Security

David Mussington, Executive Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency

Chris Novak, Co-Founder and Managing Director, Verizon Threat Research Advisory Center

Tony Sager, Senior Vice President and Chief Evangelist, Center for Internet Security

John Sherman, Chief Information Officer, Department of Defense

Bryan Vorndran, Assistant Director, Cyber Division, Federal Bureau of Investigation

Kemba Walden, Acting National Cyber Director, Office of the National Cyber Director

Wendi Whitmore, Senior Vice President, Unit 42, Palo Alto Networks

APPENDIX D: ACRONYM LIST

AD	Active Directory
API	Application Programming Interface
AWS	Amazon Web Service
BPO	Business Process Outsourcing
BPoP	Browser Proof-of-Possession
BYOD	Bring-Your-Own-Device
BYOVD	Bring Your Own Vulnerable Driver
C2	Command-and-Control
CAC	Common Access Card
CERT	Computer Emergency Response Team
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CISA	Cybersecurity and Infrastructure Security Agency
CISA 2015	Cybersecurity Information Sharing Act of 2015
CITP	Center for Information Technology Policy
COPS	Cyber Offender Prevention Squad
COVID-19	Coronavirus Disease of 2019
CPNI	Customer Proprietary Network Information
CSF	Cybersecurity Framework
CSRB; the Board	Cyber Safety Review Board
CVE	Common Vulnerability and Exposure
DBSC	Device Bound Secure Credentials
DDoS	Distributed Denial-of-Service
DIBNet	Defense Industrial Base Network
DNS	Domain Name System
DOD	Department of Defense
DOJ	Department of Justice
DPRK	Democratic People’s Republic of Korea
EDR	Emergency Disclosure Request
EU	European Union
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FedRAMP	Federal Risk and Authorization Management Program
FIDO	Fast IDentity Online
FTC	Federal Trade Commission
GB	Gigabyte
GSA	General Services Administration
HSI	Homeland Security Investigations
HTTP	Hypertext Transfer Protocol
IAB	Initial Access Broker
IAM	Identity and Access Management
IOC	Indicator of Compromise

IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
JSON	JavaScript Object Notation
LNP	Local Number Portability
LOTL	Living off the Land
MFA	Multi-Factor Authentication
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NHTCU	Dutch National High Tech Crime Unit
NIST	National Institute of Standards and Technology
NTDS	Windows NT Directory Services
OJP	Office of Justice Programs
OMB	Office of Management and Budget
OTP	One-Time Passcode
OWASP	Open Web Application Security Project
PB	Petabyte
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RMM	Remote Monitoring and Management
SaaS	Software as a Service
SDLC	Software Development Lifecycle
SIM	Subscriber Identity Module
SLA	Service-Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SRMA	Sector Risk Management Agency
SS7	Signaling System #7
SSH	Secure Shell Protocol
TB	Terabyte
TTP	Tactics, Techniques, and Procedures
U.K.	United Kingdom
U.S.	United States
U.S.C.	United States Code
UEFI	Unified Extensible Firmware Interface
USD	United States Dollar
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine

VPN	Virtual Private Network
VSP	Virtual Service Provider
ZTA	Zero Trust Architecture