CYBER SAFETY
REVIEW BOARD

CSRB REVIEW: ATTACKS ASSOCIATED WITH LAPSUS$ AND RELATED THREAT GROUPS—KEY FINDINGS AND RECOMMENDATIONS

The U.S. Department of Homeland Security established the Cyber Safety Review Board (CSRB) in February 2022, pursuant to President Biden's Executive Order 14028 on improving the Nation's Cybersecurity. The CSRB reviews significant cyber security events in order to make concrete recommendations that would drive improvements within the private and public sectors. The CSRB is comprised of senior U.S. government officials and senior industry executives. The CSRB is led by Robert Silvers, Under Secretary for Policy at DHS (Chair) and Heather Adkins, Vice President, Security Engineering at Google (Deputy Chair).

The CSRB's first review covered the vulnerabilities in the Log4j software library, and was published in July 2022. The CSRB's second review focused on the activities associated with a loosely organized criminal group known as Lapsus$, which successfully compromised the systems of some of the world's most well-resourced and well-defended companies.

Summary and Key Findings

Between 2021 and 2022, Lapsus$ conducted extortion-focused attacks against dozens of companies and government agencies around the world. Lapsus$ exploited vulnerabilities in the identity and access management ecosystem, penetrated corporate networks, stole source code, and demanded ransom payments.

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 the cyber ecosystem. They showed adeptness in identifying weak points in the system—like downstream vendors or telecommunication 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.

The CSRB engaged with nearly 40 organizations and individuals to gather insights into Lapsus$'s actions and develop recommendations on behalf of public and private sector organizations. Highlights of the CSRB's findings include the following.

- Lapsus$ employed low-cost techniques, well-known and available to other threat actors, revealing weak points in our cyber infrastructure that could be vulnerable to future attacks.
- 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.
- Threat actors can easily gain initial access to targeted organizations through Subscriber Identity Module (SIM) swapping attacks, which are exacerbated by a lucrative SIM swap criminal market. Current security protocols in the U.S. are not sufficient to prevent fraudulent SIM swapping.
- Many companies do not sufficiently consider third-party service providers and business process outsourcers (BPOs) in their risk management programs, enabling threat actors to exploit client relationships and conduct downstream attacks.
- The juvenile status of certain threat actors can limit federal law enforcement's role and yield lighter penalties under their home countries' legal frameworks. Less severe consequences may not adequately deter juveniles and few cyber-specific intervention programs exist that can help divert potential offenders to legitimate cybersecurity activities.

RECOMMENDATIONS

Based on the CSRB's review of attacks associated with Lapsus$ and related threat groups, the CSRB recommends organizations strengthen identity and access management, mitigate telecommunication and reseller vulnerabilities, and build resiliency across multi-party systems. Furthermore, the CSRB recommends lawmakers address law enforcement challenges and juvenile cybercrime. See next page for a full list of recommendations.

Identity and Access Management (IAM)

IAM weaknesses are some of the most serious vulnerabilities in the digital ecosystem and will require dramatic improvements focused on innovative controls and alternative authentication factors.

- **Everyone must progress towards a passwordless world.** Technology providers should design and deliver secure identity and access management solutions by default, including immediately beginning to transition away from voice- and SMS-based two-step MFA. Web and mobile application developers should leverage Fast IDentity Online (FIDO)2-compliant, hardware-backed solutions built into consumer devices by default.
- **Organizations should prioritize efforts to reduce the efficacy of social engineering.** As organizations integrate more robust authentication capabilities, they can reduce the efficacy of social engineering attacks, such as by requiring an explicit authentication event using a form of phishing-resistant MFA for each sensitive system transaction and fostering a positive security culture by incentivizing employees to report potential intrusions.

Telecommunication and Reseller Vulnerabilities

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 illicit activities and help defend against threat actors.

- **Build resiliency against illicit SIM swapping.** Telecommunication providers should build resiliency against social engineering in SIM swapping to protect the consumer, including treating SIM swaps as highly privileged actions, letting consumers lock their accounts, and requiring strong identity verification by default. Telecommunication providers should also improve asset management to prevent exploitation of point-of-sale systems, and harden applications and APIs used to manage customer accounts, including those enabling illicit SIM swaps.
- **Strengthen Federal Communications Commission (FCC) and Federal Trade Commission (FTC) oversight and enforcement activities** by requiring regular reporting of illicit SIM swaps, documenting and enforcing best practices, and incentivizing better security by penalizing illicit SIM swaps or lax controls.

Resiliency with a Focus on Business Process Outsourcers (BPOs)

Organizations should design their security programs to cover both their own information technology environments as well as their vendors that host critical data or maintain direct network access, to create a strong foundation for ongoing risk management.

- **Plan for disruptive cyber intrusions and invest in prevention, response, and recovery capabilities** by creating roadmaps to rapidly adopt emerging modern architectures, design and implement zero trust architecture (ZTA) following guidelines such as CISA's Zero Trust Maturity Model, and strengthening their authentication practices.
- **BPOs and client companies should mature and strengthen their risk management practices reflecting their shared risk, and the U.S. Government (USG) should support these efforts.** Client companies and BPOs should enshrine their shared responsibility for cybersecurity in their contracts; BPOs should enhance information sharing relationships with industry peers; and the USG should drive mechanisms to gain visibility into aggregate risk associated with BPOs.

Law Enforcement/Juvenile Cybercrimes Disincentives

Disruption of threat actors and their attacks requires coordination among law enforcement, industry, and international partners.

- **Advance "whole-of-society" programs and mechanisms for juvenile cybercrime prevention and intervention**. Congress should explore funding juvenile cybercrime prevention programs and reducing criminal incentives by exploring ways to ensure continuity between federal and state law enforcement authorities.
- **Increase timely reporting of cyberattacks to federal responders**. Organizations should fortify relationships with federal and mitigation partners pre-incident and improve prompt reporting to such partners, while the USG should provide clear, consistent guidance about its cyber incident-related roles and responsibilities.
- **Increase international law enforcement cooperation**. The USG should enhance resources devoted to international law enforcement cooperation and strengthen international collaboration mechanisms to ensure effective information sharing and deconfliction to better prevent cybercriminals from evading the rule of law.
- **Build resilience for Emergency Disclosure Requests (EDRs) against social engineering attacks.** Communications providers may share user data with government entities in an emergency, usually upon receipt and evaluation of an EDR. Given that threat actors abused this process to obtain sensitive information, providers should examine whether to design and implement new mechanisms for verifying EDRs using solutions such as standardized digital signatures.