Cyber Safety Review Board Issues Compelling Report about Lapsus$, MFA Vulnerabilities, and Helpful Recommendations

Article By:

Joseph J. Lazzarotti

The Cyber Safety Review Board (Board) issued a report entitled, Review of the Attacks Associates with Lapsus$ and Related Threat Groups (Report), released by the Department of Homeland Security on August 10, 2023. The Report begins with a message from the Board's Chair and Vice Chair discussing *WarGames*, a movie with interesting parallels to the present day – the leveraging of AI and large language models into systems (see Joshua/WOPR) and teenagers compromising sophisticated systems (Matthew Broderick as a high school student hacking into the Dept. of Defense). The Report looks at "Lapsus$," described as a loosely organized group of threat actors, that included juveniles in some cases, which gained lots of attention after providing a window into its inner workings.

"Lapsus$ made clear just how easy it was for its members (juveniles, in some instances) to infiltrate well-defended organizations."

Established under President Biden's Executive Order (EO) 14028 on 'Improving the Nation's Cybersecurity', the role of the Board is to review major cyber events and make concrete recommendations that would drive improvements. The Report does not disappoint in terms of its description of the targeting and nature of attack by Lapsus$ and similar groups, as well as the Board's recommendations, one being to move toward a "passwordless" world.

While we cannot cover all of the critical and helpful information in the 59-page Report, here are a few highlights.

Multi-factor Authentication Implementations Used Broadly Today are Insufficient

A reliable joke at any data security conference is how "password" or "123456" continue to be the most popular passwords. Another weakness is the use of the same account credentials across multiple accounts. Multi-factor authentication (MFA) was designed to address these practices by going beyond the password to require one or more additional authenticators before access is permitted. MFA often comes highly recommended to help protect against one of the most financially damaging online crimes, business email compromise (BEC).

Perhaps a bit unsettling for many that have implemented MFA thinking it is the answer to system access vulnerabilities, the Report explains:

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-foraccess 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.

As expected, however, some methods of MFA are better than others. The Report observed that application or token-based MFA methods, for example, were more resilient.

If you are not familiar with SIM swaps, the process goes something like this, as detailed in the Report:

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

2. Attacker uses victim's credentials to request SIM swap from telecommunications provider.

3. Telecommunications provider approves the attacker's fraudulent SIM swap.

4. With full account takeover, attacker can navigate MFA, access victim's personal account, including their employer's systems.

"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"

Insider Recruitment

Many organizations might not realize or want to believe it, but employees are vulnerable to monetary incentives to assist with providing system access to the attackers. The Report notes that in some cases these incentives could be as high as $20,000 per week. Compromised employees might hand over access credentials, approving upstream MFA requests, conduct SIM swaps, and perform other actions to assist the attackers with getting access to the organization's systems.

Supply chain attacks

Lapsus$ and similar groups do not just directly attack organizations, they also go after targets that provide access to many organizations – third-party service providers and business process outsourcers (BPOs). Evidence of this strategy by threat actor groups are the recent attacks on secure file transfer services, such as Accellion and the GoAnywhere service offered by Fortra. By gaining access to these services, the attackers have entrée to files uploaded to these services by their many customers.

Per the report:

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.

Recommendations

The Board outlines several recommendations, some are more likely to be within an organization's power to mitigate risk than others. The recommendations fall into four main categories

- 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.

As noted above, one of the strongest suggestions for enhancing IAM is moving away from passwords. The Board encourages increased use of Fast IDentity Online (FIDO)2-compliant, hardware backed solutions. In short, FIDO authentication would permit users to sign in with passkeys, usually a biometric or security key. Of course, biometrics raise other compliance risks, but the Board observes this technology avoids the vulnerability and suboptimal practices that have developed around passwords.

Another recommendation is to develop and test cyber incident response plans. As we have discussed on this blog several times (e.g., here and here), no system of safeguards is perfect. So, as an organization works to prevent an attack, it also must plan to respond should one be successful. Among other things, these plans should:

- identify critical data, systems, and assets that should be prioritized during an attack,
- outline a tested process for recovering from back-ups,
- have an internal communications plan,
- involve BPOs and third-party service providers in the developing and practicing of the plan,
- identify and maintain contact information for internal and external individuals and groups that are critical to the response process – key employees, DFIR firms, law enforcement, outside counsel, insurance carriers, etc.

The Report is a great read for anyone involved in some way in addressing data risk to an organization. A critical take-away for anyone reading this report is threats are evolving and come in many forms. A control implemented in year 1 may become a significant vulnerability in year 2. Forty years later, the movie *WarGames* continues to be relevant, even if only to show that some of the most secure systems can be compromised by a handful of curious teenagers.

National Law Review, Volume XIII, Number 226

Source URL:https://natlawreview.com/article/cyber-safety-review-board-issues-compelling-report-about-lapsus-mfa-vulnerabilities