Brian Sowers

10/27/2023

Adversarial Behavior

1. Summarize the recent history of adversarial behavior and attacks for your chosen sector.

In recent years, the financial sector has witnessed a significant evolution in cyber threats, marked by a series of targeted attacks with potential systemic impacts. An illustrative incident occurred in July 2016 when cyber attackers sought to siphon off $150 million from banks in South Asia and West Africa. While counterparty banks thwarted these attempts, the episode symbolized a shift in the threat landscape, revealing the ability of adversaries to conduct coordinated attacks on different continents, operating from remote locations worldwide.

As Adrian Nish, head of Threat Intelligence and Response at BAE Systems' Applied Intelligence, notes, "In the years since the July 2016 financial hacks, attackers have not made a habit of disrupting or manipulating the foundations of the financial system, and there has been no direct evidence of escalation" (The Cyber Threat Landscape: Confronting Challenges to the Financial System, 1). However, these incidents raise concerns, especially given the three overarching trends outlined in the article: an increased focus on targeting core banking systems, heightened aggression in disrupting responses, and the emergence of global attacker collaborations.

The financial sector faces a growing challenge stemming from increased connectivity, complexity, and capabilities. Saher Naumaan, a threat intelligence analyst, underscores the

importance of proactive measures, collaboration, and simplifying security to address these challenges. These trends collectively emphasize the necessity for financial institutions to fortify their networks and members against the ever-evolving and multifaceted realm of cyber threats.

2. Evaluate the emerging threat climate for the sector of your choice. Identify two or more areas of vulnerability where the sector will be at future risk.

The financial sector faces a rapidly evolving threat landscape characterized by emerging vulnerabilities that require vigilant attention (Unit42 ASM Threat Report 2023, 32). Two key areas of vulnerability that will be significant for future risks are:

Advanced Capabilities Targeting Core Banking Systems: With attackers developing sophisticated tools to infiltrate core banking systems, financial institutions are at a heightened risk. Core systems are the lifeblood of financial operations, and breaches in these systems can lead to substantial financial losses and a breach of customer trust. The financial sector must strengthen its defenses against such intrusions, focusing on securing transaction processing, payment messaging, and transaction authorization systems. Any vulnerability in these systems could be exploited to manipulate financial transactions or gain unauthorized access (The Cyber Threat Landscape: Confronting Challenges to the Financial System, 1).

Aggressive Disruption and Collaborative Threats: Attackers are becoming more aggressive in disrupting organizations' ability to respond. Destructive malware and other disruptive tactics, when used, can impede the victim's ability to counteract the attack effectively. The collaborative nature of modern cybercriminal activity, spanning multiple geographies and the establishment of criminal enterprises, poses a serious threat. These collaborations increase the risk to the financial

sector as attackers pool their resources, knowledge, and capabilities to target vulnerable financial institutions. Moreover, the impact of such disruptions can extend beyond financial losses to operational inefficiencies, and even systemic implications in some cases (The Cyber Threat Landscape: Confronting Challenges to the Financial System, 1).

To mitigate these vulnerabilities and future risks, the financial sector must prioritize core system security, enhance incident response capabilities, and engage in collaborative efforts to combat these multifaceted threats. These actions are critical to ensuring the resilience and security of the financial system in an increasingly interconnected and complex technological landscape.

Work Cited

"Secure Business Operations Module 1, https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_1.pdf. Accessed: 27 October 2023.

"The Cyber Threat Landscape: Confronting Challenges to the Financial System." Carnegie Endowment. 25 March 2019. https://carnegieendowment.org/2019/03/25/cyber-threat-landscape-confronting-challenges-to-financial-system-pub-78506

"Unit42 ASM Threat Report 2023." *Palo Alto*. Accessed: 27 October 2023.