Senda-Nexus Integrated Observation Report

- Purpose: Collect and analyze SYN observations, high-speed scanner-type observations, Mirai-related observations, and BlackIP observations in the Senda-Nexus environment, then create an integrated report for exhibition use.
- Data Source: Senda-Nexus MCP
- Note: This final report integrates stage-level reports and adds cross-stage synthesis.

1. Executive Summary

The analysis of SYN, high-speed scanner-type, Mirai-related, and BlackIP observations from the Senda-Nexus environment indicates significant variability and potential security risks. Key findings include sudden spikes in SYN traffic, notable activity from China and the United States in high-speed scanners and Mirai botnets, and a marked increase in malicious IP addresses detected on April 12th. These results suggest that ongoing or newly initiated threat campaigns could be targeting Senda-Nexus's infrastructure. Immediate actions should focus on enhancing network security measures and closely monitoring for unusual activity.

2. Stage Highlights

2.1 SYN

SYN traffic volumes have shown significant variability over the past month, peaking at approximately 141 million packets on March 25th. The United States has been one of the primary sources of SYN traffic during this period, with more than 12.57 million packets reported on April 11th.

2.2 High-Speed Scanner-Type Observations (SEQ)

The high-speed scanner-type observations in the Senda-Nexus environment show significant activity, particularly from China and the United States. The data indicates fluctuating patterns with peak values on March 25th and March 27th.

2.3 Mirai-Related Observations

The Mirai botnet continues to exhibit significant activity, particularly from China and the United States. Notable attacks have been observed targeting IP addresses associated with major internet service providers such as Microsoft, GTT Communications Inc., and Comcast. The latest data shows a high volume of Mirai-related activities, peaking at over 13,000 observations from China and nearly 9,000 from the United States on April 11th.

2.4 BlackIP Observations

The BlackIP observations indicate a significant increase in the number of IP addresses identified as malicious, with a notable spike observed on April 12th. The value increased from 190 to 424 between April 11th and 12th, representing a 123.7% increase in detected malicious IP addresses.

3. Cross-Stage Correlation

Overlaps and Reinforcing Signals

There is a clear overlap in the geographical regions of high activity noted across all stages: China and the United States stand out as primary sources for both SYN traffic, high-speed scanner-type activities, and Mirai-related attacks. This reinforces that these regions are key areas to monitor closely.

Contrasts and Monitoring Priorities

Despite overlaps, there are notable contrasts:

- The high volume of SYN traffic does not correlate with high-speed scanner activities or specific Mirai-related activity.
- While the United States is a significant source of SYN traffic, its role in other stages is less pronounced. China's presence in both high-speed scanners and Mirai-related attacks is more consistent.

Monitoring Priorities

- **Monitor SYN traffic from specific countries, such as the United States.**
- **Closely watch for unusual patterns in network activity related to Mirai attacks.**
- **Enhanced monitoring for IP addresses associated with major internet service providers.**

4. Integrated Recommended Actions

1. **Implement rate limiting and anomaly detection mechanisms** to mitigate potential DDoS risks.
2. **Conduct a deeper analysis on the ASN associated with high traffic volumes**, such as GOOGLE-CLOUD-PLATFORM and M247 Europe SRL.
3. **Increase network monitoring and alerting thresholds specifically targeting IP addresses flagged as malicious**.

5. Final Conclusion

The integrated report from the SYN, high-speed scanner-type, Mirai-related, and BlackIP observations of the Senda-Nexus environment highlights significant security risks. Ongoing or newly initiated threat campaigns are actively targeting Senda-Nexus's infrastructure, particularly through increased activity in China and the United States. Immediate actions should focus on enhancing network security measures to mitigate these risks and closely monitoring for unusual activities.