Quad Miners

At a glance

Industry

- Bank

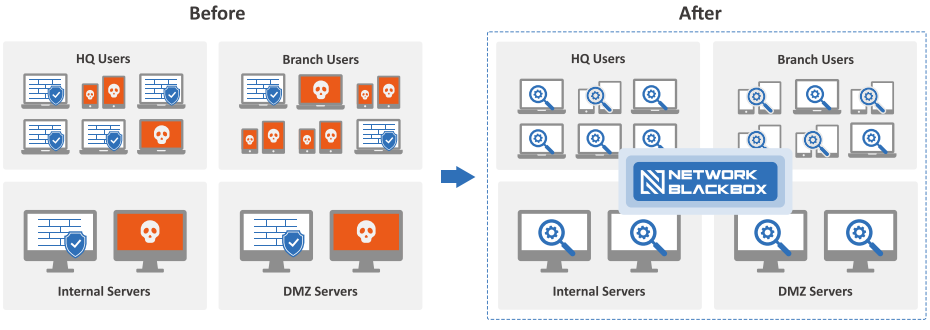
Challenge

- Need to deploy EPP/EDR security system to respond the malicious code and ransomware
- Malicious code infection blind spots occurred in many devices, IOT, and servers without an Agent installed
- Focusing on perimeter security on the Internet network

Outcome

- Establishment of Malicious Code Response System without Blind Spot
- Files across all traffic with dynamic analysis of file hash and origin files all inspected
- Malicious code analysis and response systematization through multi-APT solution integration

Establishing a Network Traffic Investigation System to Prevent Malicious Code



In today's digital age, the threat of ransomware attacks on businesses is all too real. For financial institutions like banks, the stakes are especially high, as a successful attack could not only result in significant financial losses but also damage to their reputation and customer trust. Quad Miners, a cybersecurity software vendor, recently worked with a large bank to implement an innovative solution to combat ransomware attacks. By integrating a quarantine station and eliminating blind spots in their response to headquarters and branch ransomware, Quad Miners was able to provide the bank with a comprehensive defense against this growing threat. In this case study, we'll explore how Quad Miners and the bank worked together to implement this solution and the results they achieved.

Background

The national bank is a major financial institution with a large network infrastructure, which spans across multiple locations and data centers. The bank has a complex network environment due to the numerous transactions that occur between its headquarters, branches, offices, data centers, and customer service networks. The bank's network infrastructure is critical to its operations, as it enables it to provide reliable and efficient banking services to its customers.

To ensure the security and integrity of its network infrastructure, the national No. 1 bank has partnered with Quad Miners to deploy an NDR solution. The NDR solution provides advanced threat detection and response capabilities, allowing the bank to proactively identify and respond to potential security threats before they can cause any damage. The bank faced the constant threat of cyber attacks, including malware infections and ransomware attacks, which could result in significant financial losses and reputational damage. The bank had previously relied on perimeter security solutions to protect its internet network, but these were not enough to safeguard against the ever-evolving threat landscape.

Given the complexity of the bank's network infrastructure, the NDR solution must be able to monitor and analyze network traffic across all its locations and data centers. This requires the deployment of sensors and probes at various points throughout the network to capture and analyze traffic in real-time.

Challenge

One of the primary challenges the bank faced was the need to deploy an EPP/EDR security system to respond to malicious code and ransomware attacks. These attacks can occur in many different forms, including phishing emails, drive-by downloads, and watering hole attacks, making them difficult to detect and prevent. Without an effective EPP/EDR system in place, the bank was vulnerable to these types of attacks.

Another challenge the bank faced was the presence of blind spots in its security defenses. Many devices, including IoT devices and servers, were without an agent installed, leaving them vulnerable to malicious code infections. These blind spots created a gap in the bank's security defenses, which could be exploited by cybercriminals.

Finally, the bank was overly focused on perimeter security solutions, which could leave internal systems and data vulnerable to attack. While perimeter security is important, it cannot provide complete protection against sophisticated cyber-attacks. They had lots of other security solutions, but they provided security events information with syslog or flow analytic data. With this information only, they couldn’t analyze and respond quickly due to lack of concrete evidence against faced threat. To address this challenge, the bank needed a comprehensive security solution that could detect and respond to threats across all systems and devices, including those within the bank's internal network.

Solution

Quad Miners' NDR solution Network Black Box for the bank involved several key features that helped to enhance their network security posture. The solution was designed to mirror South-North and East-West traffic on the core and backbone switches. This allowed for comprehensive visibility into all network traffic, which is crucial for detecting and responding to potential security threats.

To manage the traffic mirroring, the solution leveraged Network Packet Brokers (NPBs) to deduplicate packets and perform session-based mirroring traffic load balancing. This ensured that network security tools received a manageable and balanced load of mirrored traffic, which helped to avoid any bottlenecks that could impact network performance.

The solution also included a Network Blackbox, which was used to extract all files between network communications through a total inspection of traffic with full packet captured data. This feature enabled the bank to check for threats to files in real-time, allowing them to quickly identify and respond to any malicious activity.

Finally, the solution incorporated an Integrated Quarantine Station, which was also implemented through the Network Blackbox. The Quarantine Station was integrated with multiple Advanced Persistent Threat (APT) solutions, providing the bank with a comprehensive defense against advanced threats. It could find the verdict of the infection by known/unknown malware with multiple checking.

Outcome

The implementation of NetworkBlack Box enabled the bank to establish a Malicious Code Response System that left no blind spots not only in South-North traffic but also in East-West Traffic. The solution was designed to thoroughly inspect all files across all traffic, utilizing dynamic analysis of file hash and origin files.

Outcome

By integrating a multi-APT solution, Network BlackBox enabled the bank to systematize their malicious code analysis and response processes. This helped the bank to identify and respond to potential threats quickly, minimizing the risk of cyberattacks and data breaches.

Overall, the Malicious Code Response System implemented through Network BlackBox proved to be highly effective. The bank was able to maintain compliance with industry regulations while safeguarding customer data, thanks to the system's robust security coverage.