MAVENIR
Trust the Future

Mavenir SpamShield Solution

Subscriber Protection

SOLUTION BRIEF

WITH ADVANCED MONITORING, ANALYTICS, AND MACHINE LEARNING TOOLS FROM MAVENIR'S SPAMSHIELD, CSP'S CAN BLOCK MILLIONS OF FRAUDULENT MESSAGES FROM REACHING SUBSCRIBERS AND PROTECT REVENUES.

WHEN THE CHANNEL IS COMPROMISED THE SUBSCRIBER IS NOT PROTECTED

Messaging is an important source of revenue for Communications Service Providers (CSPs). The number of smartphones accessing carrier networks across the globe is increasing every year. The numbers are staggering. Of the 7.10 billion mobile phones across the globe, 6.37 billion are smartphones, which means 80.6 % of the world population has a smart phone[1].

With the rise in smartphones, various notification capabilities were introduced, however SMS messaging is the most relevant channel.

A recent SMS phishing attack, called "Flubot" has been particularly challenging. Flubot attacks have been identified across many countries, including Spain, Germany, Hungary, Italy, Ireland, Poland, and the U.K, and is now spreading across other regions. Mavenir security teams have seen this attack grow from 50–100 spam messages each day to infected handsets now sending thousands of messages per day.

CSPs are not only experiencing challenges in protecting their subscribers, but they are also experiencing a loss of revenue due to Flubot and other malicious attacks. When subscribers are not protected from the fraudulent spam activity and infected handsets begin sending malicious messages to other networks revenue can be lost through termination fees. Additionally, because of the attacks, support costs with subscribers support calls, and subscriber refunds are going up and affecting the bottom line.

CSPs are facing an increasing, ever-changing flow of spam and fraud traffic that is difficult to detect and control. By improving the effectiveness and timeliness of threat detection and responses with Mavenir's ML-based SpamShield, CSPs can strengthen their security posture against potential of harmful security events and keep revenue streams flowing.

TERMINATION FEE

Unsolicited A2P campaigns generated by SIM boxes and application farms via the P2P channel often terminate outside of the CSP's home network. When this occurs, as there are interconnect agreements related to message termination national and international channels with CSPs, these fraudulent messages represent a direct cost to the originating CSP.

1. Radicati Group 2021
2. Mavenir and GSMA

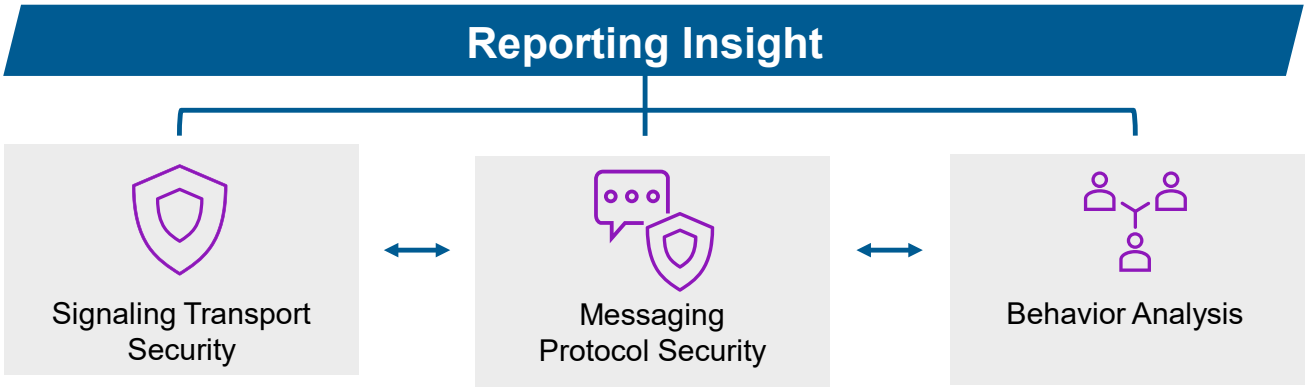
CSP's need to have a solution that offers:

- 360-degree view of the threat landscape
- Real-time detection and blocking of fraudulent traffic
- Sophisticated AI/ML algorithms with automatic detection and response
- Highly qualified fraud analysts and data scientists

MAVENIR'S SPAMSHIELD SOLUTION

Mavenir's SpamShield technology and machine learning can be deployed to carry out automated security analysis and defense. The SpamShield solution provides CSPs with 360-degree control to effectively address specific situations within their networks with speed and flexibility unrivalded by other market solutions.

Starting from detection of signaling vulnerabilities exploits in the core network using Mavenir's Signaling Firewall; SMS protocol level filtering and patented gray-route prevention on the Message Controller and a real-time Machine Learning based detection module that fingerprints the entire network's messaging traffic and engages proprietary ML technology to immediately identify A2P traffic patterns in the form of campaigns. Machine Learning algorithms perform A2P detection without the need to maintain complicated filtering and detection rules, ensuring any fraudster attempting to by-pass detection would be prevented using these ML fraud prediction techniques. Proprietary and specially tuned Machine Learning models also ensure quick adaptation to each mobile network's specific behavioral patterns and become efficient within a very short training period. The latest version of Machine Learning algorithms includes prediction capabilities to qualify detected fraud types which enables even more efficient monetization use cases. Mavenir provides the Security Management and Response Team (SMART) ensure proper daily operation of the platform enabling subscriber protection and revenue assurance in an OPEX efficient way.



ADDRESSING REVENUE PROTECTION SCENARIOS

Mavenir's SpamShield solution has a modular structure and delivers each component to target a specific problem and match the CSP existing architecture. SpaamShield addresses the main revenue protection scenarios by:

National Termination Fee:

Costs: There are costs to terminate SMS national and international messages from one CSP network to other national CSP networks. SIM boxes and application farms generate A2P traffic, which also has an associated cost to terminate to national connect. SIM boxes and application farms use a flat fee from SMS packages.

Solution: Mavenir's SpamShield detects all fraudulent campaigns from SIM boxes and application farms, unconditionally stops all outgoing campaigns to national connect. Revenue savings come from the reduced national connect costs.

Approximately 500k revenue savings on termination fees per month after deploying SpamShield

ADDRESSING REVENUE PROTECTION SCENARIOS

The unique and innovative SpamShield solution uses real-time artificial intelligence (AI)/machine learning technology with unique message fingerprinting algorithms that enable automatic detection of messaging fraud scenarios and even sophisticated by-pass methods used by the gray aggregators and fraudsters. While other vendor solutions must define rules and policies to perform detection and must know the attack vector, SpamShield will detect an attack vector automatically using finely tuned algorithms that adapt to the current network conditions and subscriber behavior to stop spammers and fraudsters in real-time. This technology has proven its efficiency in multiple head-to-head comparisons with other vendor solutions demonstrating much vastly improved precision.

Spam detection technology used by Mavenir is based on Artificial Intelligence (AI) principles and Machine Learning (ML) developed with a detailed understanding of the subject area, specially tuned for real-time detection. Traditional detection and prevention techniques are based on deterministic rules that are easily detected and bypassed by spammers and fraudsters. SpamShield AI/ML detection algorithms adapt to current network conditions and subscriber behavior to continually detect spammer and fraudster attempts.

SpamShield's advanced correlation techniques with external learning feeds include a spam reporting service, centralized spam database, hyperlink reputation statistics and call-back number reputation, all of which enable real-time prevention of malicious campaigns. AI/ML techniques implemented in SpamShield address traditional text-based messaging and multimedia content used in Rich Communications Services (RCS).

The solution addresses all major security use cases for messaging channel control for SMS, MMS, and RCS messaging protocols and provides CSPs with 360-degree control to effectively address harmful events within their networks.

MAVENIR'S SPAMSHIELD SOLUTION IN ACTION

There has been a significant impact to Application-to-Person (A2P) SMS, which is now forecasted to grow at 6.7% CAGR through 2024, increasing the global revenues to over $21B[3]. As the industry continues to grow, so does the proliferation of spam and phishing attacks.

Action Fraud, the UK's national reporting centre for fraud and cybercrime, says that between June 2020 and January 2021 it received 2,867 crime reports mentioning DPD (package delivery service), and that victims reported losing £3.4m over the same period. In December alone, 533 fake DPD emails a day were sent on to the suspicious email reporting service, which was launched last year.

A leading CSP in Europe began seeing an uptake in attacks coming through mobile devices in the form of SMS phishing.

According to U. K's National Cyber Security Centre, mobile phone users across the U.K. and Europe are being targeted by these SMS smishing text messages containing a piece of spyware called "Flubot." This malicious software targets unsuspecting customers with SMS texts, prompting the user to download a "missed packaged delivery" application. Once installed, the spyware gains permission to websites and banking information, lifting passwords that are stored on the device. This spyware also gains control of the user's phone, sending out additional text messages to all the contacts on the device. Just like the flu, it goes viral, hence the name, Flubot.

To combat this threat, the CSP worked with Mavenir to implement Mavenir's SpamShield solution.

With advanced monitoring, analytics, and machine learning tools from Mavenir's SpamShield, the CSP is reducing the potential for harmful events by quickly identifying and acting on threats. Mavenir's SpamShield uses proprietary machine learning technology specifically designed to predict messaging fraud. This predictive technology automates and simplifies the work for the CSPs operating team, allowing them to easily see potential threats to their network.

The CSP has seen a 90% reduction in reports to the 7726 (SPAM) service. With Mavenir's SpamShield technology, the CSP blocks millions of malicious messages per day and is at the forefront of protecting its customers from these harmful events.

The Value of SpamShield

SpamShield, Mavenir's world-leading messaging fraud control solution employs advanced machine learning techniques to rapidly identify and automatically control fraudulent traffic. CSPs can maximize additional A2P revenues and protect their subscribers with the latest in fraud technology.

3. Global A2P Messaging Market Report 2021: Analysis and Forecast 2020-2026 - ResearchAndMarkets.com|Business Wire
4. Research and Markets Report 2021

MAVENIR™
Trust the Future

About Mavenir

Mavenir is leveraging our DNA as a pioneer in advanced technology to focus on the vision of a single, software-based mobile network that can run on any cloud. We are reshaping the industry with our multi-generational, cloud-native, end-to-end software that is reducing complexity, de-risking digital transformation and rapidly modernizing networks. We are the trusted partner to customers around the globe, who are transforming the way the world connects — realizing the amazing new services and the promise of 5G and beyond.

For more on Mavenir solutions please visit our website at www.mavenir.com