IP flow based detection of cyber threats

Purpose of this document

Number of cyber threats is growing constantly. They have become more sophisticated, precisely targeted and they are able to overcome traditional security solutions for data network perimeter. If these attacks break the security mechanisms, they can easily infiltrate the internal network of organizations, leaving limited options for defense. They usually target sensitive data, systems or specific individuals, steal intellectual property, corporate and government secret information in order to gain unfair competitive advantage in both commercial and public sectors.

This document describes:

- Main challenges in protecting networks against advanced cyber threats
- Solutions for advanced cyber attacks based on IP flow monitoring
- How to leverage your current enterprise infrastructure to ease the deployment and lower the cost of the solution

Picture 1: Selected vendors capable to export IP flow records compatible with Flowmon solution[i]

Challenges

Already known cyber threats are efficiently detected and eliminated by firewall, antivirus, IDS/IPS or similar solutions. However, advanced cyber threats are designed as non-detectable by commonly available tools and if they overcome the security perimeter, they can easily spread uncontrolled in the network and behave in a way that they are regarded as legitimate. Thanks to their covert activity, they can access sensitive information or systems being unnoticed for a long period of time. The challenge here is to detect these attacks as soon as possible rather than investigate how to avoid them.

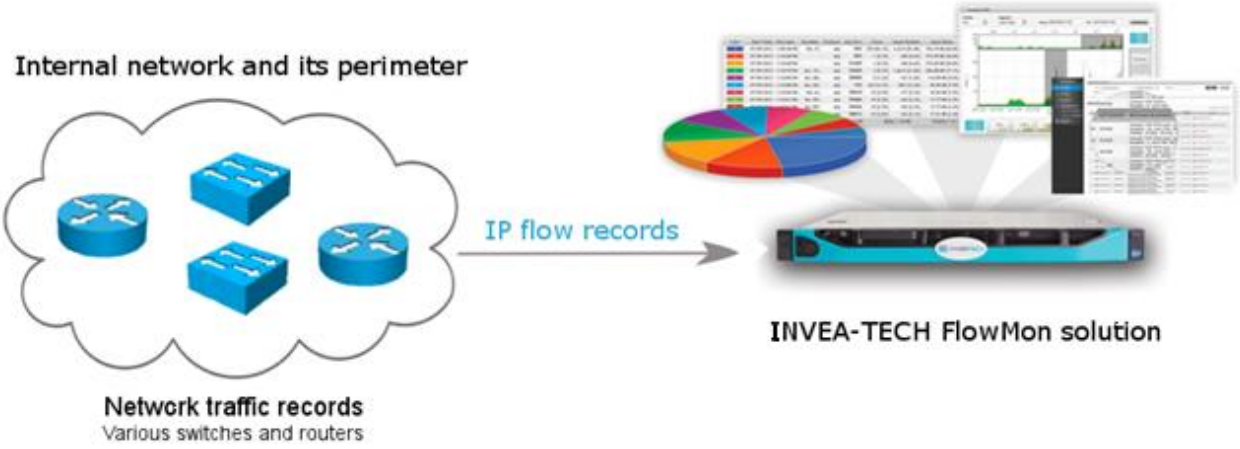
One of the examples is malware called Flame, which had gone undetected for five years until it was discovered by accident. Flame has infiltrated more than 5.000 networks, stealing data and providing access to the infected stations.

The analysis of activities within the data network is the only way to detect these cyber threats. Although they seem to be invisible in legitimate network traffic, they can be detected using detailed analysis of network traffic and detection of real network anomalies. The analysis and detection have to be fully automated since today's network traffic volume, increasing network complexity and dynamics disable manual analysis.

Solution

Advanced cyber threat solution for data networks combines the following elements to ensure complete insight into network and automated detection of cyber threats:

- Network traffic visibility is ensured by active components (routers, switches) that are able to generate IP flow based records (NetFlow, JFlow, sFlow, IPFIX, etc.) of communication in the network.
- Automated network traffic analysis is performed by Flowmon solution, which has been repeatedly recognized by Gartner's vendor analysis report as one of the world's TOP 10 solutions for network traffic monitoring and advanced threats detection.



Picture 2: Components of IP flow based detection of cyber threats

Using this complete solution, security analysts gain an overview of the incidents, anomalies or occurrence of specific activities, which are typically followed by successful attacks. Typical risks include:

- Exploration of network vulnerabilities – actions to identify suitable targets of attacks or spread of malicious software,
- Malware mitigation – attacking stations across the internal network in order to collect data or create backdoors for unauthorized access to the network,
- Botnets – ongoing communication between infected stations and control systems of the attackers,
- Data theft – leakage of sensitive information from the internal network by malware or internal attackers.

Benefits

Flowmon solution focuses on detection of complex and dangerous threats which breaks into internal network despite the perimeter protection and can operate unnoticed for several months or even years. Major benefits include:

- Protection of internal network, which is most vulnerable to advanced cyber threats.
- Detection of threats closer to the origin and in time, minimizing the damage and reducing the risk of further spread.
- Scalable, non-invasive and cost-effective security monitoring of the entire network.
- Simplification and automation of expensive manual process of inspecting incidents.
- Ability to leverage existing network infrastructure.

Solution components

Traffic visibility across the network

The new functionality of various switches and routers provides integrated traffic monitoring of the internal network – from user workstations, servers, to mobile devices. Most of the current switches and routers provide native IP flow data export without impacting the performance of the device. Thanks to this data it is possible to detect threats that break the perimeter and try to hide inside standard traffic.

IP flow data aggregation, recording and analysis to detect threats and suspicious behavior

Flowmon solution, a top class in Network Behavior Analysis (NBA), provides automated detection of threats, incidents and anomalies. Flowmon processes data in real-time and ensures the possibility of immediate protection against threats. It also provides long-term history of network traffic, evidence records and documents for forensic analysis several years back.

Primary components of Flowmon solution are:

- Flowmon Collector – for aggregating and storing of flow data (NetFlow v5/v9, IPFIX, sFlow, JFlow, etc.) from an unlimited flow data sources. It provides advanced reporting and analytical tools for flow data analysis and management.
- Flowmon ADS (Anomaly Detection System) – a system for flow data automated processing implementing the Network Behavior Analysis technology.

Optional Flowmon solution component includes:

- Flowmon Probes – specialized devices for exporting of NetFlow or IPFIX data in an environment, where it is not possible to generate IP flow data using existing network infrastructure.

How to protect your network against advanced cyber threats?

The combination of IP flow data export from network elements and Flowmon solution for the automated detection of threats provides an effective way how to protect your organization from advanced cyber threats where common tools in use do not help. With complete visibility of the internal network, the solution simplifies network management and reduces operational and development costs.

More information

For more information, please contact Flowmon Networks or your Flowmon Networks partner.

[i] Used logos belong to their respective owners