Ovum
TMT intelligence | informa

On the Radar: Positive Technologies protects against SS7 network vulnerabilities

PT SS7 Attack Discovery detects SS7 network intrusions

Publication Date: 14 Feb 2017 | Product code: IT0022-000885

Andrew Kellett

Summary

Catalyst

In the telecommunications market, a very high proportion (around 85%) of mobile traffic operates across legacy signal system 7 (SS7) networks. SS7 is the international telecom standard that defines how public switched telephone networks (PSTN) exchange digital signaling information. It has been in use since 1975, and because of security vulnerabilities that would not have been considered at that time, mobile providers and their users are now vulnerable to a variety of difficult-to-detect attacks and fraudulent activities. Positive Technologies' SS7 Attack Discovery solution identifies vulnerabilities in SS7 networks and advises on remediation and response requirements.

Key messages

- Core SS7 threat detection capabilities include the ability to examine and collect signaling data in order to identify threats and abnormal-looking activity.
- Capabilities include the detection of location tracking, message interception, identification of short message service (SMS) and unstructured supplementary service data (USSD) spoofing, cellular DoS security, and subscriber and billing protection.
- PT SS7 Attack Discovery is a no-impact network infrastructure protection solution that sits at the edge of the SS7 network, passively analyzing traffic and therefore avoiding negative impacts on network throughput.
- PT SS7 Attack Discovery technology is supported and underpinned by the expertise of the specialist Positive Technologies Telecoms Research Lab.

Ovum view

SS7 networks originates from the mid-1970s, but remains responsible for determining how mobile and fixed calls are routed and managed. Because the service delivery technology was designed well before today's security and network management challenges were known, it comes with inherent vulnerabilities that need to be addressed. In this context, the PT SS7 Attack Discovery solution has an important threat-identification role to play.

Recommendations for enterprises

Why put PT SS7 Attack Discovery on your radar?

The PT SS7 Attack Discovery solution provides network perimeter protection services for core SS7 networks. It acts as a dynamic intrusion detection system (IDS), and its analytics and threat correlation capabilities are used to reconstruct messages and identify attack patterns and malicious traffic as they enter or leave the network. These are the key threat detection requirements that telecoms providers need to have in place to provide the information resources needed to respond to threats as they occur. This is particularly the case when dealing with the ever-growing requirements of the mobile sector, including the use of smart communications devices and Internet of Things (IoT).

Highlights

Depending on each client's operational requirements, the PT SS7 Attack Discovery product can be delivered either as on-premise hardware or as a virtual solution. It is an analytics-based IDS solution that provides the security intelligence needed by telecom providers to block malicious activities that could compromise their services. The technology operates as a perimeter protection system for SS7 networks. Its combination of IDS, analytics, and correlation engine facilities are used to identify suspicious traffic flows and malicious behavior before they cause problems. Functional capabilities include the ability to analyze incoming and outbound traffic. PT SS7 Attack Discovery reviews all SS7 traffic flows by using an external signal transfer point (STP) interface to detect threats against telecom service providers.

Core detection and reporting capabilities that the PT SS7 Attack Discovery product provides include security intelligence on threats against SS7 networks and their subscriber services. It covers the ability to flag up DoS-based threats, as well as fraudulent network activities such as call and SMS interception, line tapping, and the unauthorized redirection of calls to premium rate services.

Detected threats are reported to the client organization's information security department for early incident response and remediation. In addition, the PT SS7 Attack Discovery technology can also be used to carry out retrospective analysis of signaling traffic and can assist client security teams with their forensic analysis tasks.

Core PT SS7 Attack Discovery capabilities include:

- Detection and reporting on known SS7 network vulnerabilities. This includes the ability to examine and report on network threats and the safety of the data held, identify threats that involve user location tracking, intercept calls and SMS messages and spoofed SMS and USSD messages, and deal with cellular DoS attacks, billing bypass activity, and the alteration of subscriber profiles/categories.
- The provision of passive, but at the same time efficient, threat identification services that due to their operation at the perimeter of the SS7 network and the lightweight nature of the threat identification tools, have zero impact on everyday signaling services and traffic flows.
- Message correlation facilities for complex operational systems that involve the need for load-balancing services. This approach ensures that the whole operator network can be covered and helps address false-positive issues.
- A regularly updated knowledge base. The PT SS7 Attack Discovery product set benefits from Positive Technologies' Telecoms Research Lab expertise, where specialist researchers are available to ensure that the latest SS7 vulnerability lists are kept up to date and new threats are addressed.
- Dynamic analysis and monitoring facilities that are used to identify irregular SS7 network activity that puts an organization at risk.

Data visualization and analysis facilities are combined with user-friendly dashboards to display information about threat interactions. From this knowledge base, a single stream of threat discovery information is delivered to the client's threat discovery database, and in addition to in-depth analysis of the fraudulent and malicious activities identified, the PT SS7 Attack Discovery technology can be used to detect and highlight equipment errors and find bottlenecks in the client's infrastructure.

Background

Positive Technologies is a privately held organization and was founded in 2002 by its CEO Yury Maksimov. Its international headquarters are in London, and the company has evolved to become a leading provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. The organization has more than 14 years of experience in large-scale penetration testing and source code analysis, and has vulnerability analysis expertise and experience in areas as diverse as telecom systems, e-banking, ERP, and SCADA systems. This security and vulnerability analysis and protection expertise is now being brought to bear in support of the company's newest product release, the PT SS7 Attack Discovery solution, which provides telecoms clients with the information needed to identify and respond to attacks on SS7 networks.

Current position

Global SS7 facilities continue to underpin the deployment of core telecommunications services. The relevance and the importance of the technology remains and continues to grow because of the need to the deliver an ever-growing range of smart mobile communication services. For telecom providers, their services need to be delivered seamlessly and with minimum risk to the user community. Positive Technologies' PT SS7 Attack Discovery product deals with the security vulnerabilities that exist in SS7 operations and helps service providers and their users function in a safe and trustworthy way.

Data sheet

Key facts

Table 1: Data sheet: Positive Technologies

Product name	PT SS7 Attack Discovery	**Product classification**	Threat analytics, IDS, monitoring, and management
Version number	V1	**Release date**	July 2016
Industries covered	Mobile networks operators (MNOs) and mobile virtual network operators (MVNOs)	**Geographies covered**	Global supported from company locations in EMEA and the Far East
Relevant company sizes	Small, medium, and large	**Licensing options**	Perpetual, term, and SaaS
URL	https://www.ptsecurity.com/ww-en/	**Routes to market**	Direct and through channel partners
Company headquarters	London, UK	**Number of employees**	700

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

2017 Trends to Watch: Security, IT0022-000808 (October 2016)

"Arbor Networks adds big data analytics to its SP portfolio," IT0022-000868 (January 2017)

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions

Andrew.kellett@ovum.com

Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Source:

CONTACT US

www.ovum.com

askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo

Source:

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Ovum

TMT intelligence | informa

CONTACT US

www.ovum.com

analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing

Dubai

Hong Kong

Hyderabad

Johannesburg

London

Melbourne

New York

San Francisco

Sao Paulo

Tokyo