# VIMPELCOM BOOSTS SECURITY OF MOBILE NETWORK AND SUBSCRIBERS WITH PT TELECOM ATTACK DISCOVERY[1]

*"We have worked for years now with Positive Technologies, whose security specialists have shown themselves as true experts, even in such a niche field as signaling networks, and specifically how to secure them. There are few specialists and ready-to-go solutions for companies with our needs, while Positive Technologies has accumulated unparalleled experience in telecom security. So inviting Positive Technologies to audit SS7 security and test PT Telecom Attack Discovery on our network was the logical next step."*

**Aleksandr Golubev**
IT Security Director
PJSC VimpelCom

VimpelCom

## COMPANY PROFILE

- **Name:** PJSC VimpelCom
- **Industry:** Telecommunications
- **Challenge:** Assess the security level of the mobile network; select methods for handling the most important threats
- **Solution:** Network security monitoring with PT Telecom Attack Discovery

PJSC VimpelCom (marketed under the "Beeline" brand in Russia) is a part of VimpelCom Ltd., an international communications group offering mobile and landline telephony, wired and wireless high-speed Internet access, and IPTV to over 200 million clients worldwide.

## THE CHALLENGE

After years of security through obscurity, telecom security has appeared on the radar screen. Subscribers are using more and more new services, and almost every new gadget has mobile Internet connectivity. But the core for all this communication—the SS7 signaling network—was developed 40 years ago, and integrating new technologies with legacy systems creates some serious security issues.

Vulnerabilities in SS7 make it possible for an attacker anywhere in the world to track the location of a mobile phone, disconnect a subscriber, intercept SMS messages, and even eavesdrop on conversations. Positive Technologies experts assessed many SS7 networks security in 2015–2016 and found troubling results: subscribers could be geotracked on 58% of analyzed networks, have their incoming SMS messages intercepted on 89% of networks, and have their voice calls intercepted on 50% of networks.

Of course, it's impossible to overhaul the existing infrastructure and protocols in a day. That is why it is so important to perform a detailed audit of SS7 networks and related components, as well as quickly identify attacks targeting mobile infrastructure and subscribers and undertake mitigating measures.

PJSC VimpelCom serves over 58 million mobile subscribers, making reliability an absolute priority. The growing number and scale of external threats forced the company to take a fresh look at how to keep its network safe. Several of the key challenges included:

- Get an unbiased picture of the protection level of the mobile network and subscribers in order to analyze the existing risks.
- Devise methods for mitigating the highest-priority threats.
- Decide on methods to monitor network security and detect illegitimate use of the network.

[1] Previously named PT SS7 Attack Discovery.

## HIGHLIGHTS

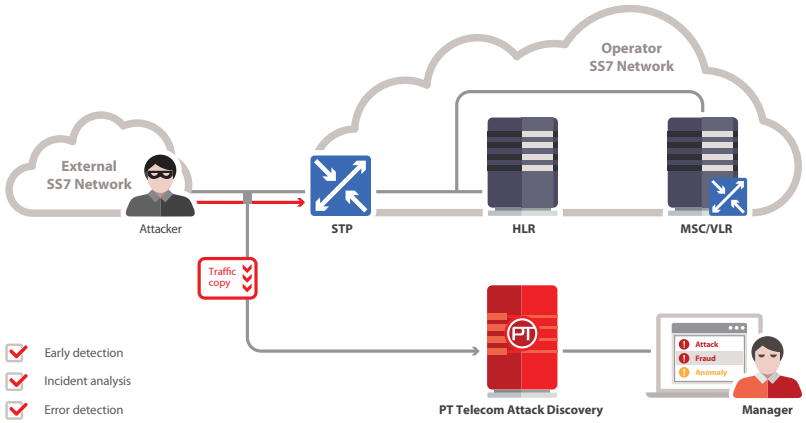
- Identifies all types of SS7 attacks
- Deploys without interfering with network operations
- Correlates system events and distributes loads between multiple STPs
- Powered by constantly updated database of threats and vulnerabilities
- Performs dynamic analysis to detect abnormal SS7 activity
- Visualizes security data

## NETWORK SECURITY ANALYSIS

- Monitoring of network perimeter
- Global threat monitoring and risk assessment
- Regular control of changes
- Rapid and accurate assessment results

## THE SOLUTION

To meet the SS7 security challenge, VimpelCom selected Positive Technologies, which started a common project in 2012 to protect the client's subscribers and network. In the intervening years, VimpelCom and Positive Technologies have continued their partnership in a number of areas, such as optimizing configuration of transport network equipment and investigating 3G/4G modem security. The next level of the partnership arrived with comprehensive auditing of SS7 security and testing of PT Telecom Attack Discovery.




PT Telecom Attack Discovery automates and simplifies detection of illegitimate SS7 network activity. By quickly detecting malicious traffic, this system prevents a number of costly nuisances:

- Denial of service preventing subscriber access or functioning of network infrastructure
- Theft of funds from subscriber accounts
- Bypassing of billing/metering systems
- Interception of calls and SMS messages

Many attacks can be prevented proactively. Assessing network security detects vulnerabilities before they can be exploited, and prevents attacks from gaining a foothold on the network—meaning improved security and subscriber loyalty.

## RESULTS

With the results of the security audit and information on real-world attacks observed on the network, VimpelCom and Positive Technologies were able to prevent denial of service, fraud involving theft of funds from subscriber accounts, and more. The experts at Positive Technologies developed an action list for counteracting the most important and high-priority threats. Cooperation continues with plans to optimize network equipment configuration for improved resilience to attacks, build a vulnerability management process, and set up continuous security monitoring of illegitimate network activity.

## About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.



POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com