PT VIP PROTECT: EMPOWERING OPERATORS TO SAFEGUARD THEIR HIGH-PROFILE CLIENTS

Globally, mobile operators are waking up to the risks created by vulnerabilities in the SS7 protocol, ranging from fraud and interruption of services to intercepting calls and texts and theft of other confidential data, such as a user's current location. And while the general public may not have heard of SS7, the growing number of celebrity phone hacking scandals has meant that mobile users are also becoming aware of dangers to their privacy.

All this creates a security challenge, which mobile operators are scrambling to address using solutions such as PT SS7 Attack Discovery™ from Positive Technologies. But SS7 security doesn't have to be just an expensive headache. Successfully identifying and eliminating SS7 vulnerabilities, it should allow a telco to differentiate themselves in the market, and even to upsell premium protection to select clients:

PT VIP PROTECT: HOW IT WORKS

The operator supplies PT SS7 Attack Discovery™ with the details of selected mobile accounts, which require a premium level of security scrutiny on a temporary or permanent basis. The solution monitors these accounts 24/7 and immediately highlights any suspicious activity to the mobile operator with recommendations for remedial action. The mobile operator is able to generate on-demand reports within PT SS7 Attack Discovery™ that detail:

- all attempts (successful or not) to use SS7 flaws to interfere with a VIP user's service,
- the type of attacks attempted (SMS intercept, eavesdropping, location tracking, etc.),
- the source of each attempted attack to the Global Title (GT) level,
- the recommended course of remedial action to address or block the threat.

The mobile operator can then provide the VIP user with the reassurance that the recommended remedial action has been taken to address or block the threat. Depending on the type and severity of attacks detected, they may also suggest the user takes further action themselves, such as updating social media and banking passwords or reporting repeated attempts to law enforcement.

For more on this topic, see the work that Positive Technologies has done with international news outlets such as the BBC's technology program "Click" and Forbes magazine to highlight the risks of SS7 to calls, texts, and messages through services like Facebook and WhatsApp.

BUSINESS BENEFITS

- **Drive ARPU.** Offering personalized privacy protection as a paid upgrade to selected clients opens up new revenue streams for mobile operators.
- **Build brand loyalty.** Choose to offer this additional level of security assurance as a value-add to develop loyalty among celebrity clients who may have a strong social media following.
- **Attract new corporate clients.** Differentiate yourself from other mobile operators in corporate procurement negotiations by offering added protection to an organization's most valued staff and communications.
- **Grow a reputation for security.** Operators can enhance the level of trust in their brand by offering a solution with a reputation for securing high-profile individuals.

Watch As Hackers Hijack WhatsApp Accounts Via Critical Telecoms Flaws

Find out more about PT SS7 Attack Discovery™

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