Check Point and ElevenPaths

Mobile Threat Prevention and Investigation – A Solution Brief

BACKGROUND

Modern living brings greater connectivity to both personal and business environments. An increasing number of companies and services integrate mobile solutions as a prominent part of their business engagements; internally and externally alike.

Along the convenience of using emails, Sales-Force and other business apps, grows the trend of mobile cybercrime. This new industry involves sophisticated attackers working in a business-based structure, who are able to bypass traditional malware detection techniques. As mobile attackers are growingly detouring antivirus companies, organizations are looking for a comprehensive solution to face harmful threats through detection, mitigation and analysis.

THREAT DETECTION, MITIGATION AND INVESTIGATION – ALL-AROUND SOLUTION

Check Point SandBlast Mobile and ElevenPaths' Tacyt have partnered to provide a one-stop, all-inclusive solution to face mobile cyberthreats and allow security professionals to intuitively move from threat detection to investigation and analysis.

Check Point SandBlast Mobile provides the highest level of security for iOS and Android smartphones and tablets. It is designed to find known and unknown 0day threats by applying threat emulation, advanced static code analysis, app reputation and machine learning. In addition to threat detection, Check Point SandBlast Mobile scores mobile threat risks and mitigates them in real-time by removing threats and denying access to sensitive systems via mobile device management (MDM), as well as blocking network and SMS attacks.

Following detection and mitigation, companies will need to investigate and analyze exposed threats. Check Point SandBlast Mobile's seamless integration with ElevenPaths' Tacyt allows customers to conduct in-depth research into any detected incidents. This solution provides full context and a better understanding of the exposure to cyberthreats on mobile devices supported by the enterprise.

ElevenPaths, Telefónica's Cyber Security Unit, which chose SandBlast Mobile as its mobile security offering for its enterprise customers, offers this joint solution today.

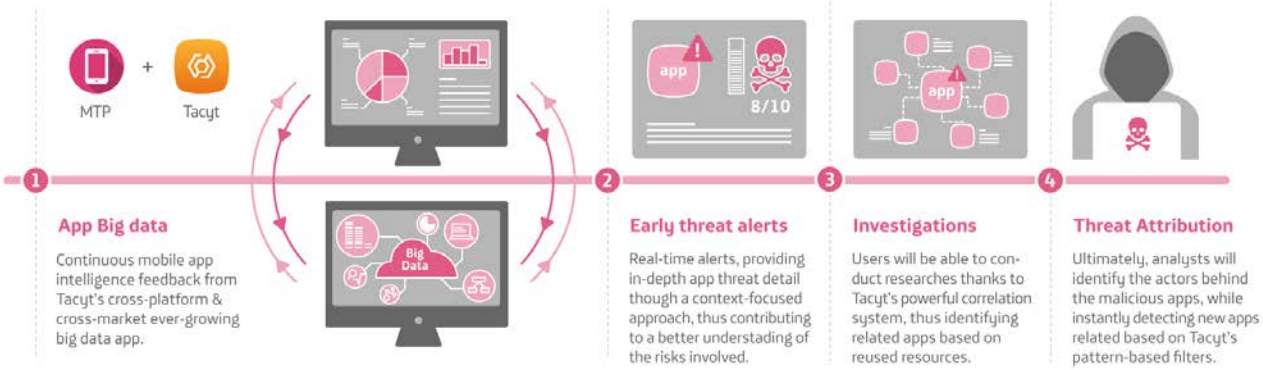
BENEFITS

- Holistic view of the threat mobile landscape, enabling analysts to conduct in-depth research into any android or iOS mobile app
- Context-based intelligence, providing proactive detection of campaigns, actors and TTPs based on Tacyt's pattern-focused approach
- Cross-Platform and Cross-Market mobile app big data
- Check Point SandBlast Mobile Threat Cloud IoC enrichment via Tacyt's continuous app intelligence feeding
- Check Point SandBlast Mobile behavioral analysis and machine learning output improvement through Tacyt's behavioral-based filters

TACYT'S THREAT INVESTIGATION – HOW DOES IT WORK?

While Check Point SandBlast Mobile detects and mitigates real-time malware, ElevenPaths' Tacyt offers an additional layer of in-house classification and attribution to found threats. Tacyt provides professionals and security experts with big data technology for easy mobile app environment investigation.

This innovative tool allows analysts to search, match, and investigate different parameters (metadata) of iOS and Android apps that Tacyt obtains thanks to its powerful cross-market and cross-platform search engine. The solution enables the analyst to identify potential "singularities," a concept which refers to whatever data – technical or circumstantial – that makes the app or its developer – as a person – singular or unique from others within a reasonable margin of error. Additionally, it comprises indicators of compromise (IoCs), properties, and identifiers from the app, building up a unique app big data set with a historical record of over 6 million current and past versions.



Classifying, attributing and performing in-depth analysis is critical in mobile malware because:

- The mobile ecosystem is extremely dynamic, so cybercriminals are constantly evolving the tools they use to keep up.
- Attribution and malware family categorization reveals trends in the broader cybercriminal community. This helps enterprises deploy appropriate defenses before a trend turns into an epidemic.
- Proper malware risk categorization is of particular importance for mobile threat defense in Bring Your Own Device (BYOD) deployments.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (https://www.checkpoint.com) is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT ELEVENPATHS

At ElevenPaths, Telefónica Cyber Security Unit (https://www.elevenpaths.com), we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We're always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life. ElevenPaths is a Mobility Technology Partner of Check Point SandBlast Mobile.

