CASE STUDY Kiwi.com

Kiwi.com (formerly Skypicker) is a fast-growing online travel agency. Founded in 2012, it has grown to over 1100 employees, and continues to grow rapidly. It serves millions of consumers every year by combining flights from carriers who do not offer route coordination. Kiwi.com administers a diversified network serving approximately 1,900 devices. The aim of the GREYCORTEX MENDEL implementation was to enable Kiwi.com to focus fully on their core business while keep their dynamically growing IT infrastructure secure and reliable.

> *"Since its deployment in November, 2016, GREYCORTEX helped us immensely. We were able to find security policy breaches and performance problems, and link these to problems experienced by users that previous tools had not seen. We could see attacks as they were developing and take action. We have really strengthened our security posture and are very happy with the results."* (Josef Staša, IT Operations Manager)

Challenges

While the business and team are growing quickly, Kiwi.com's IT infrastructure and network are growing even faster.

Kiwi.com's main reason for deploying MENDEL was to ensure that the goodwill and reputation which Kiwi.com had built through a reliable and secure IT infrastructure was preserved. It was critical to the day-to-day operations of the whole company that this be done effectively. Kiwi.com needed the ability to oversee their network's technical infrastructure and network administration from an operational, performance, and security monitoring perspective.

Other challenges included:

- Protection of customer data
- Detection of modern threats and protection against attacks targeted at network users
- Provision of a security-focused overview of network infrastructure behavior, including an automated analysis of normal behavior for individual network segments, devices, and individual users
- Improved security policy enforcement
- Monitoring Kiwi.com's current security infrastructure configuration and effectiveness
- Easy scalability

Challenges

- Protection of customer data
- Detection of future APTs, RATs, zero-day attacks, etc.
- Growing IT infrastructure
- Network visibility
- Security policies

Advantages

GREYCORTEX MENDEL includes several important features that benefited Kiwi.com's IT team. The most important is a behavioral detection engine based on advanced machine learning and artificial intelligence. Outputs are integrated with an hourly updated list of blacklisted IPs and signatures. Because these tools are integrated, MENDEL can detect threats based not only on known signatures, but based on atomic-level symptoms of attack; for example, where an advanced persistent threat lies dormant, but communicates with its Command and Control. MENDEL also includes application performance monitoring capabilities, offering teams detailed data for business critical transactions, combined with security events for easy root cause analysis; all in real time, without slowing the network. Finally, MENDEL helped to enforce Kiwi.com's existing security policies and maintain its compliance with government regulations.

Advantages

- Behavior-based detection of advanced, unknown threats
- Signature-based detection of known threats
- Application performance monitoring
- Network visibility

Results

GREYCORTEX MENDEL was installed quickly, and it immediately and automatically began to learn the network. Kiwi.com's original security posture, while strong, was greatly improved with GREYCORTEX MENDEL and is now prepared for more advanced threats. Among other results, MENDEL helped Kiwi.com achieve the following:

- Better enforcement of security policies and quicker resolution of incidents
- Complete network visibility
- Discovery and analysis of network and application performance problems
- Forensic analysis

Results

- Effective detection
- Security policies implemented
- Greater visibility
- Forensic analysis