CUSTOMER STORY

FireEye

Energy Ministry Detects Shamoon Malware with FireEye Network Security

FACTS AT A GLANCE

INDUSTRY

Government

CUSTOMER PROFILE

The Kingdom of Saudi Arabia's Ministry of Petroleum and Mineral Resources is the government entity that is chartered with policy implementation and oversight responsibilities for the exploration, development, refining and distribution of oil, gas and minerals. The Ministry monitors and oversees oil and gas companies that are wholly or partially owned by the government of Saudi Arabia, such as Saudi Aramco, Saudi Chevron and Aramco Gulf Operation Ltd. and others. The Minister is Chairman of the Board of Saudi Aramco.

Business challenge

The oil and gas industry is a prime target for all types of adversaries. Nation-state actors, rogue terrorists, criminals and hacktivists have varying motives, including sabotage, espionage, financial gain, or political causes. The number and severity of cyber incidents in the energy sector are on the rise. Saudi Arabia's Ministry of Petroleum and Mineral Resources faces a constant barrage of compromise attempts from every angle and takes a strong, proactive stance when it comes to IT security. In 2011, the organization knew it could no longer rely on firewall and antivirus technologies to defend against advanced attackers and began seeking solutions.

"When it comes to detecting and preventing advanced attacks, the power of FireEye's MVX technology has no competition."

Solution

In 2011, after a proof-of-concept (POC), the Ministry purchased FireEye® Network Threat Prevention Platform (NX Series). The Ministry also recommended the FireEye solution to Saudi Aramco and arranged for a proof-of-concept (POC) in 2012. FireEye NX series was running in POC monitoring mode when Saudi Aramco was attacked with the Shamoon malware in August 2012. The FireEye NX Series had detected the virus, but since it was deployed in monitor-only mode, it could not block the virus. The Ministry is confident that, had FireEye NX Series been fully deployed in inline blocking mode, Saudi Aramco would have avoided Shamoon's costly destruction and disruption.

"When I discovered FireEye in 2011, I knew it was the right solution for us," said IT General Manager and Chief Information Officer Wahid Hammami. "When it comes to detecting and preventing advanced attacks, the power of FireEye's Multi-Vector Virtual Execution™ (MVX) engine technology has no competition. It is the only defense available in the market to protect against zero-day attacks."

The Ministry confronts attacks on multiple fronts, prompting them to expand their initial FireEye NX Series deployment to include FireEye® Email Threat Prevention Platform (EX Series) and then FireEye® Central Management (CM Series) to consolidate administration, reporting and data sharing across the FireEye solution. To take advantage of the latest global threat intelligence, the Ministry subscribes to FireEye® Dynamic Threat Intelligence (DTI). They also use FireEye® Malware Analysis Platform (AX Series) to inspect malicious files.

The Ministry's multi-faceted security posture is exemplary. With a suite of FireEye products, they are able to:

- **Detect and Stop Advanced Attacks on Multiple Fronts:** FireEye NX Series detects and dynamically analyzes traffic emanating from or to suspicious URLs, while FireEye EX Series analyzes the contents and file attachments of emails. When threats are confirmed, communication is blocked and malicious files are quarantined.
- **Prevent Data Theft and Multi-Stage Attacks:** FireEye NX Series blocks communication with nefarious web hosts across HTTP, FTP, IRC and other protocols to prevent attackers from stealing data or downloading additional tools.
- **Consolidate Intelligence and Reporting:** The Dynamic Threat Intelligence subscription ensures that the Ministry receives the latest intelligence on attacker tactics gathered around the globe by the FireEye community. Reports generated through FireEye Central Management are shared with top officials at the Ministry for continual awareness.
- **Investigate Malware Across Multiple Windows Environments:** FireEye AX Series enables the Ministry to test and analyze malware behavior across a spectrum of browsers, plug-ins, applications and operating systems.

Organizational benefits

By deploying multiple FireEye products, the Saudia Arabia Ministry of Petroleum and Mineral Resources has comprehensive threat detection, prevention and intelligence within an integrated solution. Intelligence sharing is automated and cross-product reporting is easy.

"Integration across the product suite through Central Management, along with shared intelligence through the Dynamic Threat Intelligence subscription sets FireEye apart from other vendors," said Wahid Hammami, CIO. "In June of 2013, the entire government energy sector was targeted and we were able to prevent it."

With FireEye's acquisition of Mandiant in 2013, the Ministry also has access to the world's most talented security experts.

"In Saudi Arabia, you cannot find security skills comparable to Mandiant," said Hammami. "Mandiant recently completed a security review of our security environment and processes and provided a comprehensive advisory report." Through its investment in FireEye products and Mandiant services, the Ministry has:

- **Detected and Prevented Numerous Attacks:** The Ministry and its affiliate companies in the energy sector are routinely targeted. FireEye has repeatedly detected and prevented compromise attempts through web and email.
- **Reduced Operational Disruption and Remediation Costs:** Attacks targeting the energy sector are notoriously destructive, but early detection, blocking of communication with malicious hosts and malware quarantine have enabled the Ministry to remain operational and avoid remediation efforts.
- **Implemented Advice from the World's Leading Security Experts:** The Ministry has overcome a lack of security expertise in Saudi Arabia by contracting with Mandiant's renowned professional services team for ongoing guidance.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye®