FireEye
SECURITY REIMAGINED

JAIST Detects Malicious Callbacks with FireEye

CUSTOMER STORY

SECURITY REIMAGINED

CUSTOMER PROFILE

The Japan Advanced Institute of Science and Technology (JAIST) is a center of academic research excellence. JAIST is a postgraduate university that promotes faculty and student exchanges with leading institutes around the world, emphasizing a global approach to education and research.

BUSINESS CHALLENGE

The Japan Advanced Institute of Science and Technology (JAIST) is on the cutting edge of science, with research centers focused on the development of nano materials and recyclable polymers, robotics, green device research, advanced computing, simulation science, and more. The renowned postgraduate university routinely open its doors to an international body of scholars and students for collaboration, joint workshops, and knowledge exchange conferences. The Institute's innovative projects will shape tomorrow's world, making them a target for criminals and spies looking to steal lucrative research data.

The Information Society Research Center is the department within JAIST responsible for maintaining the institute's information technology infrastructure, including security.

Through the FRONTIER project, the Information Society Research Center provides massively parallel computation support, wide area network access, and large-scale storage of advanced research databases. Assistant Professor Uda Hitoshi is proud of FRONTIER's stability and reliability and works to safeguard the infrastructure with security measures that protect the network without hindering research.

The Center deployed anti-virus software and terminal firewalls, but was concerned about signature-less and latent malware that lies dormant for some period before becoming active. Students and faculty often conduct online research and email exchange, putting them at risk of visiting a compromised site containing malicious unknown malware (web driveby download) or receiving an email with a malicious file attachment. They also travel and invite guests, meaning that personal devices previously connected to networks with unknown security measures could jeopardize the University's infrastructure with undetected infections.

The security team could not block access to email or the web because that would impact research efforts. Instead, the Institute looked for a solution that would detect, analyze and block suspicious files, such as PDFs, Flash, and ZIP/RAR/TNEF archives, on the network. And, in cases where students, faculty or guests connected personal devices already infected to the network, they wanted the solution to be able to detect callback communication by undetected malware.

SOLUTION

The Institute chose to pilot the FireEye® Network Threat Prevention Platform (NX Series) to monitor threats that traditional and next generation firewalls,

FireEye NX Platform has also detected initial callback communication from undetected malware, enabling the Institute to stop attackers from downloading additional support tools, moving laterally, or stealing data.

IPS, anti-virus, and web gateways miss. They deployed the NX Series in inline blocking mode in December 2013 and have been impressed by FireEye's ability to detect and block malicious files that bypass the anti-virus software provided to students free of charge.

The power behind this is FireEye® Multi-Vector Virtual Execution™ (MVX) engine, which executes suspicious binaries and web objects against a range of browsers, plug-ins, applications, and operating environments, looking for vulnerability exploitation, memory corruption, and other malicious actions. As the attack plays out in the virtualized environment, FireEye MVX captures callback channels, dynamically creates blocking rules, and transmits this information back to the FireEye NX platform.

FireEye NX has also identified initial callback communication from undetected malware, enabling the Institute to stop attackers from downloading additional support tools, moving laterally, or stealing data.

FireEye NX enables JAIST's security team to:

- **Detect and stop advanced targeted attacks from the web.** FireEye NX detects and dynamically analyzes traffic emanating from or to suspicious URLs. When threats are confirmed, communication is blocked and malicious files, such as images, PDFs, Flash, or ZIP/ RAR/TNEF archives, are quarantined.

- **Prevent data theft and multi-stage attacks.** FireEye NX blocks communication with nefarious web hosts across HTTP, FTP, IRC, and other protocols to prevent attackers from stealing data or downloading additional tools.

VISION

The Information Society Research Center is considering adding FireEye® Email Threat Prevention Platform to detect and block spear-phishing emails containing malicious URLs.

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

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**