CUSTOMER STORY

Leading Japanese Artist Management Agency Strengthens Security Strategy with FireEye Solutions

FACTS AT A GLANCE

INDUSTRY

Entertainment, Media and Hospitality

CUSTOMER PROFILE

Artist management company Amuse, Inc. works with famous Japanese bands and individual musicians, such as Southern All Stars, Fukuyama Masaharu, Pornograffitti, BEGIN, and Perfume. The company also has been successful in a wide variety of other media genres; including representing actors, actresses, idols, cultural icons, and other talented individuals. Its media team conducts filming, planning, production and sales. The nature of Amuse's activities also dictates the need for a content team to maintain intellectual property rights. Developing these diverse aspects of the arts has enabled Amuse to become a highly-respected entertainment corporation.

Only kandou—Japanese for "deeply moving people"—can change their hearts: This is the governing philosophy of Amuse, Inc., a diversified Japanese business that focuses on artist management and many other related facets of entertainment. The agency runs multiple web-based applications, including a fan web site and an online store, all of which must be continually accessible to the public. However, zero-day and targeted attacks occur on a daily basis and have to be constantly managed. Identifying the need to strengthen its internal network security, Amuse chose the FireEye® Network Threat Prevention Platform as its leading countermeasure in confronting these threats and attacks.

In recent years Amuse has opened an online shop selling artist-related goods and created a fan club membership system to manage the club's subscribers. Additionally, the agency has leveraged the full power of the Internet in developing and using innovative online tools. These tools are critical in facilitating business relationships with other multimedia organizations, which the company fosters to widen the portfolio of superstars it can offer to its paying clients. However, these systems and tools also expose the company's network to potential security attacks.

> "The best product to effectively defend against zero-day malware and targeted attacks is FireEye."
>
> — **Kunio Shimizu,** Amuse, Inc.

Kunio Shimizu, spokesperson for Amuse and a Certified Information Systems Auditor (CISA), described his security strategy; "We place a high priority on our public network system and are continually reviewing and analyzing currently available solutions. As a result of our research we deployed a new tool to fight cyber attacks: We purchased the FireEye Network Threat Prevention Platform, which regularly checks for weakness and maintains a high-quality level of security. Zero-day and targeted attacks use advanced technology and proliferate the security risk, therefore the security of our in-house network became a pressing issue to confront."

Malware infection calls for strengthening of network security

Amuse's legacy in-house security network architecture originally utilized a firewall as the primary barrier against attacks. At the time, anti-virus software on PCs and email servers were determined to be sufficient supplemental protection. However in November 2013, a rise in the volume of email messages caused the performance of the mail server to decrease. "Our department is not just about providing public-facing Internet service but we also are responsible for setting up all the internal servers for business use," said Shimizu. "We implemented an authentication function on the email servers, which stopped third-party 'middlemen,' and protected us against spam.

We managed, and had control over, every minute detail, yet our accounts were still getting hijacked. We determined that there was a chance that spam could still be sent out, so we immediately halted all accounts and investigated the failure. We were unable to identify any direct cause. Although there was no discernible source or actual harm done, we reviewed the whole network system and fundamentally reexamined the possible origins of the breaches."

At first, Shimizu suspected the problem was caused by targeted attacks focused on a specific mail server vulnerability. He recalled, "We entrusted a partner, Global Security Expert (GSX), to overcome these weaknesses. We asked GSX to perform a vulnerability inspection of the suspected server. However, this also failed to uncover the intrusion, so we had to examine all of our corporate intranet and web-based systems, and yet we still could not find the vulnerability. Once we finished scanning our servers without finding anything wrong, we strongly suspected it had to be a malware infection that was undetectable by traditional anti-virus software."

To detect unknown threats and defend against targeted attacks, Amuse enlisted the help of consultants from FireEye to do a proof of concept: A number of malware infections were immediately revealed. "The FireEye Platform was able to detect multiple malware infections: Even though the AV pattern file had been updated a few days after the malware infection was first suspected, the PC anti-virus software still couldn't find anything. Only at a much later time, after repeated scans, was the anti-virus application finally able to detect the infection. The strength of FireEye of detection capability was very obvious," said Shimizu."

Why FireEye: the best in unknown threat detection capability

When selecting an anti-malware solution Shimizu considered several alternative options as candidates alongside FireEye. Firewall functions differed between the applications and while base security functions against malware could be added to the products, FireEye was the only one that could be installed without changing or replacing existing firewalls or network configurations. This is partly what led Shimizu to his conclusion, "The best product to effectively defend against zero-day malware and targeted attacks is FireEye. The decisive factor in FireEye being introduced was the overwhelmingly high detection rate against unknown threats."

He continued, "In Amuse's business, there are the obvious phishing emails but there also are cases in which malware hides in emails that recipients have no choice but to open, which inevitably infect systems without anyone being aware. So we must always account for the risk of malware. With some of the other products considered, we studied which one had the highest probability of detecting unknown malware, and determined that it was FireEye.

Other companies had anti-malware products, often with acquisition-based integrated security solutions but this wasn't the case with FireEye. The FireEye Network Threat Prevention Platform is a unique solution, from its proprietary malware protection technology origins, it has grown significantly in terms of technology, reliability and performance."

The adoption of FireEye has been especially effective within the media industry. GSX suggested the FireEye® Forensics Analysis Platform be deployed as an addition to

> "The best way to guard against increasingly complex and sophisticated security threats, such as targeted attacks, is an ongoing investment with FireEye."
>
> — **Kunio Shimizu,** Amuse, Inc.

the anti-malware solutions that were deployed. Shimizu noted, "Our IT planning activities are very intensive, so we cannot spend time just focusing on security management issues. Only FireEye has the dual capabilities of malware infection detection and callback communication blocking. In addition, GSX is able to report on how to deal with the threat identification, so we now operate with confidence."

Responding to complex, sophisticated attacks with a comprehensive solution

The FireEye Network Threat Prevention Platform protects against malware that infects through the web. When it detects an attack, the platform sends a signal to the Command and Control server and automatically shuts off external communication. At the same time, an alert is sent to the administrator and GSX analysis team. The GSX security engineers then analyze the information remotely and immediately provide Amuse personnel with mitigation measures."If you look at the reports, it is easy to find which terminal or which network was infected. By disconnecting the device from the network, the user can deal with issues quickly," said Shimizu.

With FireEye, malware that typically slipped through the anti-virus software on the mail server and PCs is consistently detected. Shimizu was not previously familiar with the risk of zero-day attacks and without detection he could not respond to them. He reflected, "When you witness the alerts that FireEye emits you can tell that we are being well protected. We now have peace of mind.

"In the entertainment business, email is an important tool and needs to be kept secure. We obviously stay suspicious of any content we open in email, as it is very risky to open a link in a message because of the threat of malware. However, even if an email is infected with malware, we can detect it in real-time. Attackers are now unable to enter the network from the inside. Because of this, our sense of security is immeasurable."

He concluded, "The best way to guard against increasingly complex and sophisticated security threats, such as targeted attacks, is continued investment in security measures."

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