Solving two challenges with one Endpoint; "Advanced Malware" and “Legacy Operating System"

Fujikura Head Office building

Profile

Fujikura

Customer	Fujikura Ltd.
Industry	Manufacturing
Country	Japan
Employees	56,961 (Consolidated)
Websites	www.fuj kura.co.jp/eng

Responsible for producing and distributing social infrastructure products that contribute greatly to society on a global scale. Information security measures include annual company-wide training courses and the implementation of security measures on standard PCs

Fujikura Ltd. (hereafter, "Fujikura") is a BtoB-orientated enterprise involved in the worldwide production and distribution of industrial equipment, electronic and electrical equipment and other products that contribute greatly to the society, such as electrical wires, optical fiber and other social infrastructure products, along with electronic components in smartphones and electrical components in automobiles. The company established the "realization of Fujikura Group as a household name on the global stage, as well as among investors" as a core goal in its "2020 Medium-term Management Plan" in FY2015, setting FY2020 as the final year to achieve its targets. The environmental, social and governance (including cyber security measures) initiatives set to achieve these goals are detailed in the "2020 Medium-term CSR Priority Measures".

Fujikura has formed an Electronic Information Security Committee, which is responsible for establishing electronic security systems that set basic policies, guidelines and regulations on electronic information security, along with detailed security-related rules. The Committee is made up of members across the entire company, including the Information Business System Engineering Division. The Committee Secretariat implements company-wide training on electronic information security (held every year, targeting all employees), implements various measures and confirms the state of implementation of measures at each division (auditing), and maintains an inventory count of company PCs.

It is also involved in detailing standard PC specifications for domestic use and the administration and management of company PCs, including a centralized system implementation and installation. In addition, it is involved in various other PC security measures undertaken company-wide at all sites in Japan, including the installation and use of anti-virus software, the encryption of PC HDDs, and the implementation of a PC login system using IC cards.

Implementation Background

Simultaneously resolving two major issues - "the implementation of countermeasures to Advanced Persistent Threat(APT) attack" and "extending the life of outdated OSs in use"

With the recent increase of APT attacks, Fujikura has looked into additional measures to reduce the risk of malware infections, information leaks, and other various risks.

"With the widespread media coverage into the APT attack on the Japan Pension Service in 2015, and the continuation of information security training for regular users implemented every year, there were relatively few reports and inquiries from users who accidentally opened a targeted attack e-mail. Having said that, the manner in which targeted e-mail attacks presented themselves were becoming shrewder by the day, and insufficiencies with countermeasures to risks such as unknown virus infections and so-called zero-day attacks found at the point of quarantine using conventional anti-virus software and next generation firewalls were becoming increasingly apparent". (Mr. Sakuma)

Additionally, on some client PCs installed at manufacturing sites for equipment control and data collection, we had been using Windows XP - a now unsupported OS - for some time until said manufacturing equipment and data collection equipment was either updated or replaced. We were able to extend the use of Windows XP through the use of isolated networks and gateway devices. However, the bolstering of these information security measures also remained a pressing concern.

"While 'dealing with APT attacks' and 'extending the life of outdated OSs' were initially seen as two separate issues, with each being tackled in different ways, upon additional consideration we found 'FFRI yarai' to provide the potential for resolving both of these issues in tandem, which was a key factor leading to its implementation". (Mr. Sakuma)

Implementation History

"Behavioral detection", "multi-layer protection using the five engines", together with its "proven track record" held in high regard

Two key features focused on when selecting FFRI yarai was its "behavioral detection" system, and its implementation of "multi-layer protection using the five engines".

"FFRI yarai's 'behavioral detection' and 'multi-layer protection using the five engines' features offered superior detection and protection capabilities against threats as a countermeasure against the risk of unknown virus infection and zero-day attacks. These features also presented a solution to resolving the two previously mentioned issues facing the company, namely the 'implementation of a countermeasure to APT attacks' and 'extending the life of outdated OSs'. FFRI yarai's widespread use in government offices and elsewhere, and its ability to work with already implemented security products were other areas where FFRI yarai was held in high regard". (Mr. Sakuma)

Implementation Results

Detecting suspicious files previously undetectable with anti-virus software and next generation firewalls

FFRI yarai is built over a series of steps consisting of (1) deployment in the client operating environment, (2) assessment (checking logs in detection mode and preparing a white list), and (3) the start of operation in normal (block) mode. Fujikura is currently applying FFRI yarai in detection mode as a step towards rolling FFRI yarai out on company PCs at all offices nationwide.

"The admin console is extremely easy to use, allowing us to install or uninstall all units, update licenses and perform a range of other functions. The admin console screen display is also extremely easy to view". (Mr. Tachikawa)

Looking ahead we will scan from programs and scripts found in detection mode at each site, whitelisting essential items, before transitioning on to normal (block) mode use. Even now, however, the strength of FFRI yarai's "behavioral detection" tools became readily apparent immediately after applying detection mode.

"Upon receiving notification from outside the company that an unauthorized access attempt had been made from the company's IP address, FFRI yarai made short work of identifying the company PC responsible. While we initially saw FFRI yarai's 'behavioral detection' feature as a means for detecting unknown threats, I don't think we would have been able to detect and verify the cause of this issue using conventional anti-virus and next generation firewall measures alone". (Mr. Sakuma, Mr. Tachikawa)

Future Outlook

Further reducing security risk using products working in tandem with FFRI yarai

"While the nature of cyber security continues to change on a day by day basis, requiring that countermeasures constantly remain a step ahead, the introduction of FFRI yarai resolves all pressing issues for the foreseeable future, and helps us establish a set level of security measures to serve as an endpoint in the fight against cyber threats". (Mr. Sakuma)

Looking ahead, we plan to further alleviate security risk by reviewing the potential for solutions capable of working in conjunction with FFRI yarai, such as malware analysis tools and products tracing malware infection paths.

View all Yarai case studies at www.ffri.jp/en/resources/case-studies

FFRI North Amer ca, Inc. 65 Enterprise,Aliso Viejo, CA,92656
Email: Sales@ffri-inc.com

The information provided in this case study was current at the time of initial publication (June 2017) and may no longer be applicable. This case study is provided simply for the purpose of sharing information. FFRI provides this information with no guarantee, either implicit or explicit. FFRI and yarai are registered trademarks of FFRI, Inc. Other trademarks are property of their respective owners.