MITSUBISHI ELECTRIC
Changes for the Better

for a greener tomorrow

MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

FOR IMMEDIATE RELEASE **No. 3002**

Customer Inquiries

Information Technology R&D Center
Mitsubishi Electric Corporation
www.MitsubishiElectric.com/ssl/contact/company/rd/form.html
www.MitsubishiElectric.com/company/rd

Media Inquiries

Public Relations Division
Mitsubishi Electric Corporation
prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news

Mitsubishi Electric Develops Cyber Attack Detection Technology

Preventing information leakage by monitoring behavior patterns typical of viruses

TOKYO, February 17, 2016 – Mitsubishi Electric Corporation (TOKYO: 6503) announced today it has developed a cyber-attack detection technology that can classify computer virus behavior into about 50 different patterns. Symantec's latest report on Internet security suggests a million new viruses are spawned every day, but Mitsubishi Electric's new technology offers the capability of detecting even previously unknown viruses through their behavior, preventing information leakage and its associated damages.

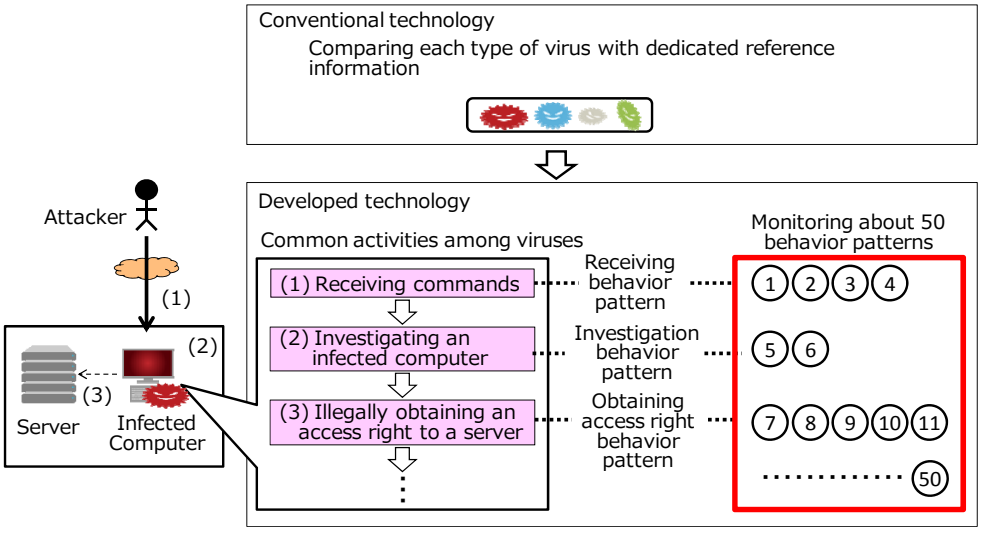

Fig 1. Monitoring behavior patterns

During a cyber attack, the virus has to take several steps, such as infecting a targeted computer, receiving commands from the attacker, investigating the infected computer, and then illegally obtaining access rights to further expand its activities. Each of those steps also has a set of associated behavior patterns. For example, when investigating an infected computer, the attacker determines which information should be obtained and how by searching documents, finding communication routes, and checking the configuration of

security measures. Mitsubishi Electric has identified about 50 behavior patterns, and has defined dedicated log analysis rules for each that allow the system to monitor suspicious activity and accurately detect a virus for preventing information leakage. While the number of new viruses each year grows astronomical, a dozen common behavior patterns are expected to evolve each year. These patterns can quickly be added to the detection system, stopping all new viruses that might seek to exploit the pattern.

Previously, it was hard to distinguish legitimate activities from a malicious cyber attack. Mitsubishi Electric's new technology defines a sequence of behaviors as a cyber-attack scenario. By using correlation analysis to determine whether a particular sequence of activities follows the scenario or not, the technology is able to distinguish between legitimate activities that follow similar patterns and actual cyber attacks.

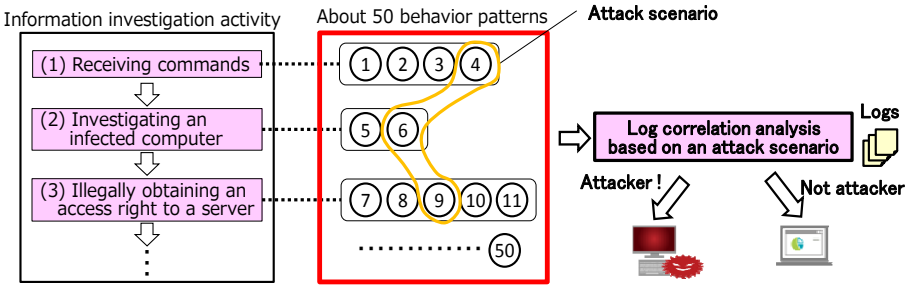

Fig 2. Cyber attack detection based on a scenario

Patents

Pending patents for the technology announced in this news release number six in Japan and six abroad.

###

About Mitsubishi Electric Corporation

With over 90 years of experience in providing reliable, high-quality products, Mitsubishi Electric Corporation (TOKYO: 6503) is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. Embracing the spirit of its corporate statement, Changes for the Better, and its environmental statement, Eco Changes, Mitsubishi Electric endeavors to be a global, leading green company, enriching society with technology. The company recorded consolidated group sales of 4,323.0 billion yen (US$ 36.0 billion*) in the fiscal year ended March 31, 2015. For more information visit:
http://www.MitsubishiElectric.com
*At an exchange rate of 120 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2015