FOR IMMEDIATE RELEASE

Development of Technology for Detecting Advanced Persistent Threat Activities

Visualizing correlations among hosts having suspicious activities to detect attacks such as stealth malware

Tokyo, October 13, 2015 --- Hitachi, Ltd. (TSE: 6501, "Hitachi"), announced its development of an innovative technology for detecting Advanced Persistent Threat (APT) *[1]. The purpose of APT is to steal valuable data and cause damage to the network by performing persistent and covey activity in computers and servers after a successful APT. Our new technology to detect APT is first to identify host that is possible under attack and then visualize and correlate the intrusion process among hosts. This technology is aiming at strengthening conventional incident response and allowing an early detection of APT using stealth malware*[2] that is hard to be detected through analyzing individual hosts.

With a purpose of stealing valuable data and causing damage in the network, the number of APT targeting government agencies, private companies, and major infrastructures has increased dramatically in recent years. A survey from the National Police Agency in Japan shows that the number of the APT incidents in 2014 reaches 1723, which is 3.5 times of that in the previous year. In addition, the methods of intrusion attacks have become more sophisticated, for example, a zero-day*[3] vulnerability and stealth malware are leveraged in intrusion attacks. Moreover, there is a trend to abuse the OS built-in commands that are for surveying network status and the free-ware that are not developed for a use of APT. This type of sophisticated attacks does not present obvious malicious activities in each infected host, and which has made them undetectable through the conventional anti-virus software or the existing technologies that perform analysis in each host using the common features from the experienced attacks. One of the potential solutions against the sophisticated attack is to apply whitelisting technique that is capable to detect attack when an unauthorized program is activated. However, this technique is not effective due to the current network reality that new software installation and updates are frequently executed.

Hitachi considers that a new analysis approach to correlate activities among multiple hosts instead of individual host is required to detect this type of sophisticated attacks.

- more -

Thus, a detection technology is developed to show warning signs when multiple hosts present suspicious activities. The developed technology is capable of (1) identifying suspicious hosts that may have undergone APT using machine-learning, and then (2) visualizing the correlation between the suspicious hosts by analyzing the access-timing between them. This technology allows the security administrator to detect attacks that cannot be identified by only analyzing each host individually.

This technology has the following two main characteristics.

(1) Identifying suspicious hosts that may have undergone APT using machine-learning

The purpose of attack is to steal valuable data and cause damage in the network that is different from the original usage of computers and servers such as document generation, web browsing, or network services. Thus, when an intrusion occurs, the host will frequently activate uncommon activities and present suspicious activities. The six types of sensors are developed to identify the suspicious activities such as executing uncommon programs or communicating to hosts that are not accessed commonly by modeling the features of regular activities in host using machine-learning. Based on the number of the suspicious activities reported from those sensors, the analysis server installed in the company's network identifies the suspicious hosts.

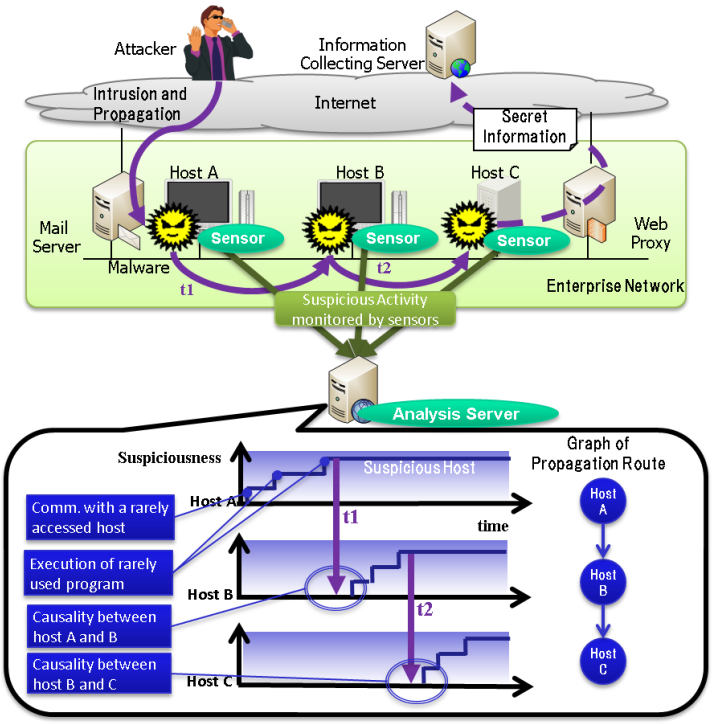
(2) Visualizing the correlation of infected hosts by analyzing their access-timing

The intrusion attack can conduct another attack to other networks by using vulnerability exploits*[4] or illegal remote-login. Hitachi developed a technology that visualizes the correlation between the two hosts into a graph representing the attack routes based on whether the suspicious host identified by machine-learning has been accessed from any suspicious host over a period of time. If the number of hosts with the correlation reaches a certain level, the malicious activities will be determined. Due to the ability of analyzing the attack tactics and routes in each hosts based on the suspicious activities and correlation, this technology is capable of contributing to attack investigation and countermeasure planning.

To measure the performance of this technology, we conduct experiments in one of our local networks with a simulation of typical APTs based on the case studies, reports from security vendors, and academic researches. The experiment results show that

our technology achieves the detection rate of 97%, and reduces the number of false alerts to 10% in a whitelisting technique. This technology achieves both the high detection rate and low false alerts to offer the efficient and effective countermeasures against APTs.

The importance of developing APT incident response technology is not to be restricted in IT systems, but to be expanded to IoT systems and industrial systems. Hitachi will utilize this technology to the major infrastructures in order to contribute to the realization of safe and secure society.
The technical details of the achievement described here will be presented at Computer Security Symposium 2015 (CSS2015), which will be held in Nagasaki Pref. from 21st October 2015.



A process of the developed technology in detecting APT

*1 Attacks that persistently aim at particular government agencies, companies and infrastructures to steal valuable data and cause critical damages. Generally, the attack first infects a host by sending e-mail with malware, and then expanding attack to other hosts step by step.

*2 Malware that is difficult to be detected by antivirus software due to its invisible malicious activities

*3 A new bug or a breach which is not known to security vendors or public.

*4 Attack to gain the control of a host by exploiting the vulnerabilities

About Hitachi, Ltd.

Hitachi, Ltd. (TSE: 6501), headquartered in Tokyo, Japan, delivers innovations that answer society's challenges with our talented team and proven experience in global markets. The company's consolidated revenues for fiscal 2014 (ended March 31, 2015) totaled 9,761 billion yen ($81.3 billion). Hitachi is focusing more than ever on the Social Innovation Business, which includes power & infrastructure systems, information & telecommunication systems, construction machinery, high functional materials & components, automotive systems, healthcare and others. For more information on Hitachi, please visit the company's website at http://www.hitachi.com.

# # #

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
