Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware

Takeo Hariu, Mitsuaki Akiyama, Kazufumi Aoki, Takeshi Yagi, Makoto Iwamura, and Hiroshi Kurakami

Abstract

After outlining trends in cyber attacks mounted mainly through the use of malicious software (malware), we describe technology for detecting malware infections and isolating infection sources and technology for analyzing malware and extracting the features of its functions; describe how information obtained from detection and analysis can be used by countermeasure technology to generate blacklists and defend against attacks on the network; and describe analysis techniques for tracing attacks by using logs kept by network devices.

1. Introduction

Cyber attacks that infect personal computers (PCs) and servers on the Internet to gain unauthorized access to personal information have become a serious problem in society. An example of malicious software (malware) infecting a PC via the web is shown in **Fig. 1**. A PC having a vulnerable web browser or plugin accesses a portal or relay site on which an attacker has prepared content for performing automatic transfers. As a result, the PC's Internet link is automatically transferred to an attack site on which attack code has been placed. The PC then receives this attack code and downloads and executes the related malware. The PC is now infected, enabling information to be sent from the PC to the attacker's command site and commands to be sent from the command site to the PC. Since attackers can exploit a wide variety of vulnerabilities to achieve malware infections, it is difficult to detect which vulnerabilities have been targeted and what caused the infection. Moreover, the continual appearance of new malware is making it more difficult to analyze the functions of each type of malware and gauge its threat.

To develop countermeasures to malware infections, research has been active in technology for detecting infections and determining their causes and technology for analyzing malware. Detecting an infection requires an accurate understanding of the attack mounted at the time of infection, but this requires highly specialized knowledge in the use of detection technologies. Another problem is that new types of attacks and malware are now appearing in extremely short cycles. There is therefore a need to grasp attack trends and research and develop new technologies as early as possible.

2. Malware detection, analysis, and countermeasure technologies

To solve the above problems, NTT is researching and developing malware detection, analysis, and countermeasure technologies [1] in a three-phase manner, as shown in **Fig. 2**. These phases are described below.

In the first phase, detection technology is being developed to receive attacks using a *honeypot*, which is an undercover system for attracting attacks and collecting malware. Communications between the Internet and honeypot can be analyzed and useful information for preventing malware infections can be extracted.

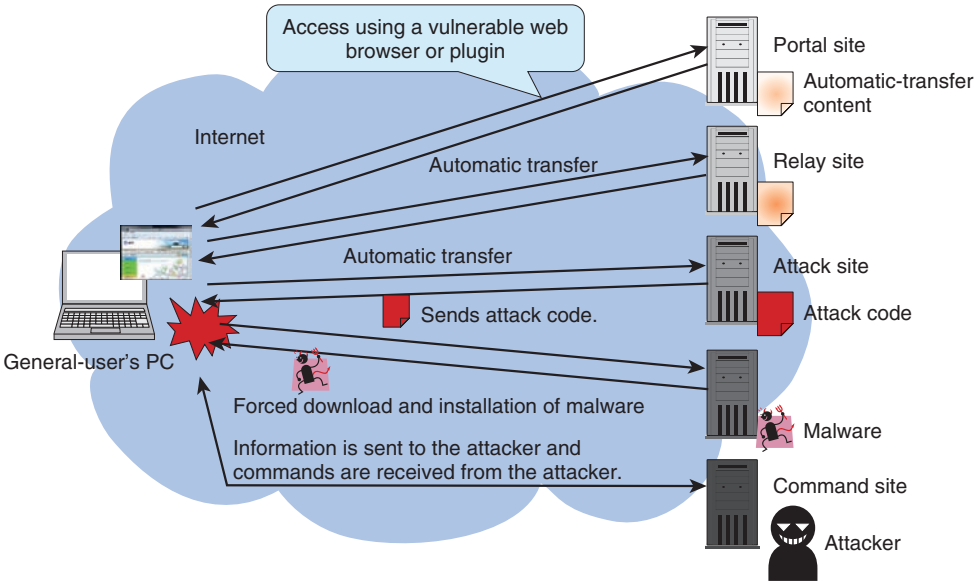

Fig. 1. Malware infection of PC (via web).

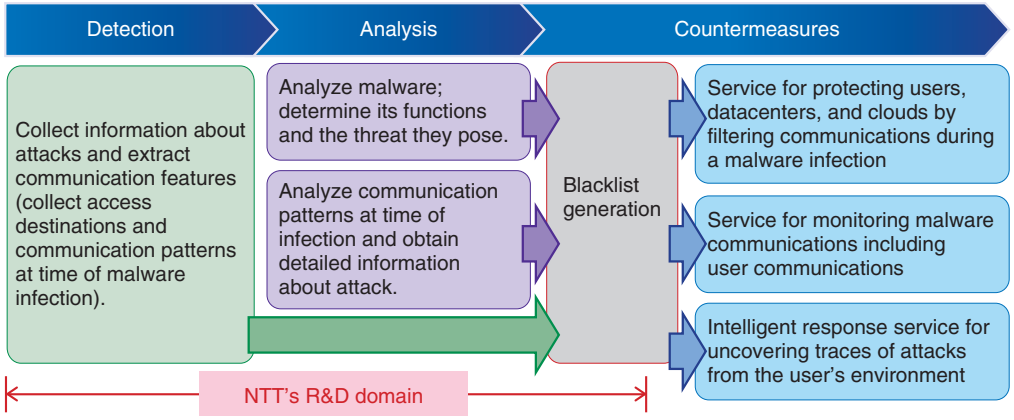

Fig. 2. R&D of malware detection, analysis, and countermeasure technologies at NTT.

Next, in the second phase, analysis technology is being developed to analyze the malware collected by the honeypot and the associated communication patterns. The aim is to understand the malware's functions and determine the threat that it poses, and in general, to acquire detailed information about the attack.

Finally, in the third phase, countermeasure technology is being developed to use the information obtained by the above detection and analysis technologies to generate blacklists in a format that can be used by services. Addresses of access destinations appearing at the time of a malware infection extracted by detection technology can be used to generate blacklists consisting of URL (uniform resource locator) lists, IP (Internet protocol) address lists, etc. In the example in Fig. 1, the URLs of malicious sites—from the portal to the command site—can be added to a blacklist. Such a blacklist can be used as a communications filter to protect the user from malware infections during access to the Internet. Likewise, the addresses of access destinations appearing after a malware infection, as determined by analysis technology, can be used to generate a blacklist. Such

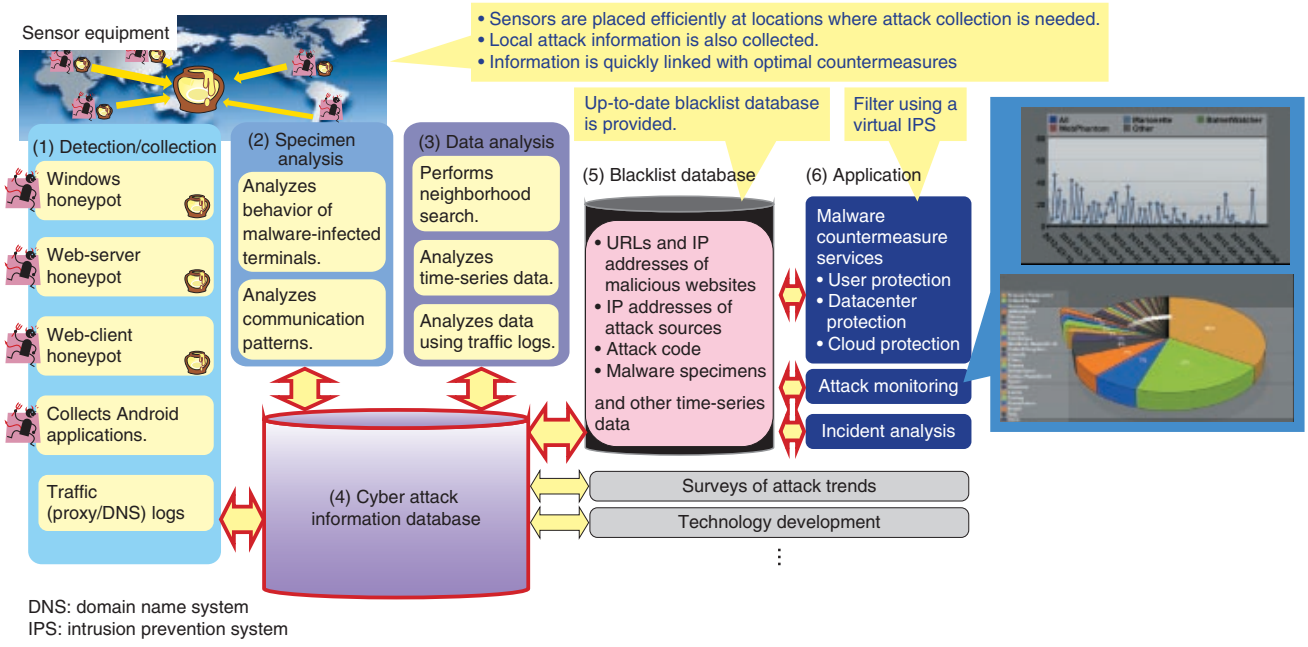

Fig. 3. Blacklist generation technology.

blacklists can be used by incident response services to check for the presence of malware infections or the occurrence of damage in a user's environment. Section 3 describes blacklist generation technology in more detail.

3. Blacklist generation technology

Blacklist generation technology takes information about malicious URLs, IP addresses, etc. extracted or identified by detection and analysis technologies and converts it into blacklists in a form conducive to actual use (**Fig. 3**). These blacklists make it possible to conduct filtering based on malicious-site information without requiring the user to have extensive, specialized knowledge.

First, detection technology is used to collect malware-related information through the use of various types of honeypots that enable information about malware infections to be collected in a safe manner ((1) in Fig. 3). Honeypots are developed specifically for different types of malware infection methods that pose threats to society. For example, there are Windows honeypots targeting attacks that exploit vulnerabilities in the Windows operating system, web-server honeypots targeting attacks that exploit vulnerabilities in web applications [2], and web-client honeypots targeting attacks that exploit vulnerabilities in web browsers [3].

NTT has developed analysis technology for analyzing malware specimens (2) consisting of open-environment-type malware dynamic analysis technology [4] and a debugger for analyzing the behavior of malware on a computer [5]. The former runs malware within an analysis environment that, while not allowing communications that would create more harm such as the spread of a malware infection, does allow communications with actual attackers on the Internet. This makes it possible to analyze behavior such as malware communication patterns on the network. The latter enables the behavior of malware to be analyzed without the malware itself being aware of the debugger's existence. As advanced technologies unprecedented in Japan or abroad that can accurately grasp malware functions, these developments reflect NTT's R&D strength.

Data analysis technology (3) consists of neighborhood search technology for automatically and efficiently discovering malicious URLs similar in structure to malicious URLs that have already been discovered [6], time-series data analysis technology for retrospectively analyzing the data collected by honeypots when a new attack or malware program is discovered, and data analysis technology for inspecting user access destinations by using traffic logs when a web-client honeypot was used. In particular,

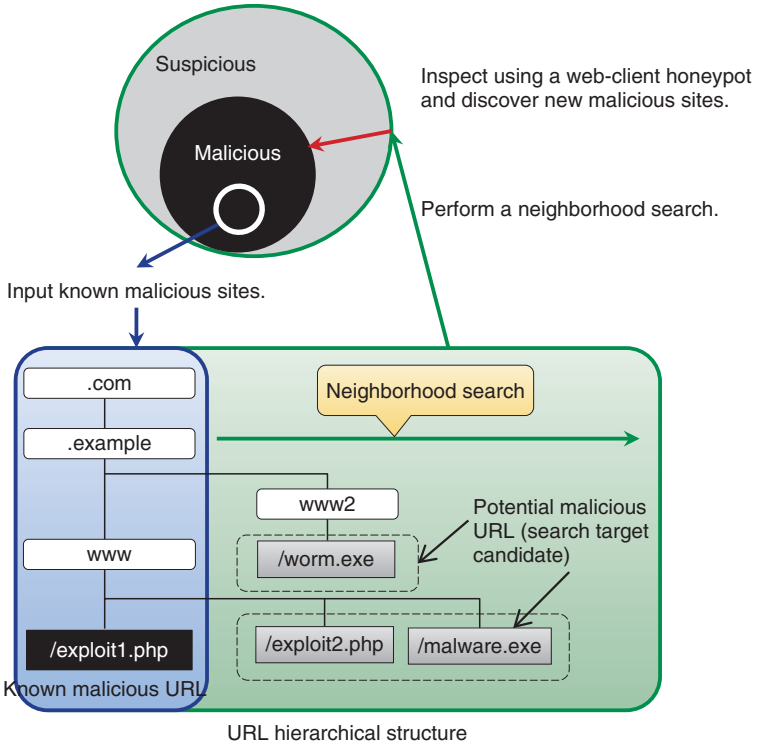

Fig. 4. Neighborhood search technology.

neighborhood search technology (**Fig. 4**) is an original development by NTT. It can discover information about malicious sites that has until now not been included in ordinary blacklists because of the difficulty of uncovering it. NTT has received a commendation for this technology at an IEEE international meeting.

The information obtained by these detection and analysis technologies is stored in a cyber attack information database (4). The idea is to continuously expand the information in the database by coordinating the detection and analysis technologies and repeating the information-collection and analysis processes. In addition to blacklist generation, the information stored in this database can be used to survey attack trends and develop new anti-malware technologies.

The information stored in this cyber attack information database is now used to generate specific blacklists, which are stored in the blacklist database (5). These include a list of URLs of malicious websites that, if accessed, will result in a malware infection, and a list of IP addresses of attack origins.

These blacklists are used to protect users, datacenters, and clouds (6). For example, they can be installed and used as filters in anti-attack equipment composing a firewall, intrusion detection system (IDS), or intrusion prevention system (IPS). They can also be applied to the monitoring of traffic logs and other information to aid in discovering attacks and used as reference information in incident response. Section 4 describes methods for using these blacklists.

4. Methods for using blacklists

4.1 Methods

As shown in **Fig. 5**, the blacklist database stores four types of information, A–D, as effective data for an IDS/IPS to defend against attacks as well as two types, E and F, that will be provided to users. As an example of using type-A information, consider a list of URLs of malicious websites that would infect a client with malware if accessed by a vulnerable web browser. This list can be installed in an IDS/IPS filter on a user network to block access to malicious websites and protect the user's PC. Next, as an example of using type-B information, consider a list of URLs of malicious websites that web servers accessed at the time of a malware infection caused by an attack. This list can be installed in an IDS/IPS filter in a cloud

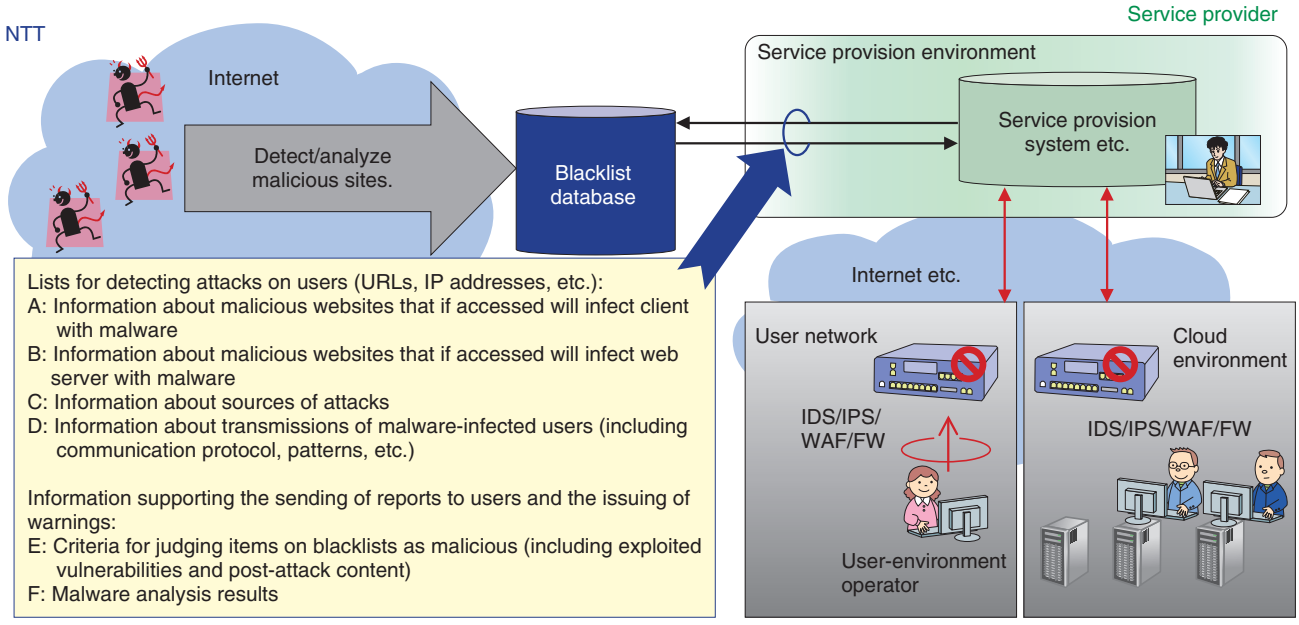

Fig. 5. Use of blacklists.

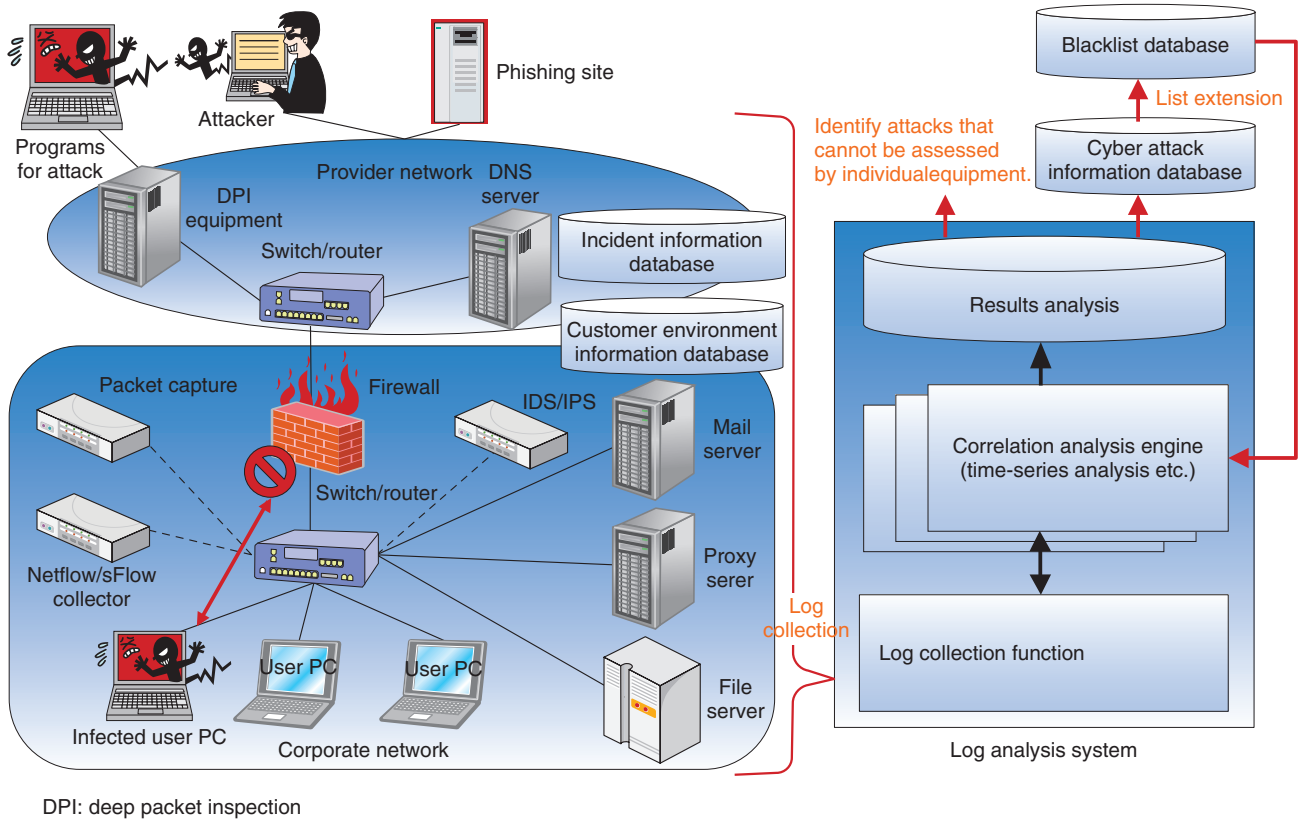

Fig. 6. Concept of log analysis.

environment to block further access to malicious websites and protect web servers. At this time, a list of IP addresses from which attacks are mounted against web servers (type-C information) can also be used in a filter to block access from IP addresses from which an attack is possible. Moreover, a list of access destinations uncovered during malware analysis (type-D information) can be installed in an IDS/IPS as a monitoring target to discover users susceptible to a malware infection. Information of types E and F can be used for services that create reports for users and issue warnings at the time of a security incident.

Blacklist generation technology can also be used for inspecting whether a specific website is malicious. For example, the logs of a user's proxy server or DNS (domain name system) server can be analyzed and websites found to be frequently accessed by the user can be periodically inspected so that malicious websites having a high possibility of being accessed by the user can be put on a blacklist early.

There are plans to extend the types of information stored in the blacklist database. Functions will eventually be extended with the aim of applying the data collected by honeypots and malware analysis to incident response.

4.2 Log analysis using blacklists

As shown in **Fig. 6**, blacklists can be used to perform correlation analysis with firewall, IDS, and IPS security-equipment logs, proxy/file server logs, logs output from client PCs, and logs of packet information to extract the behavior of attacks and information leaks on the network. Performing long-term log correlation analysis through a log analysis system makes it possible to isolate abnormal behavior that cannot be identified by firewalls or IDS/IPS equipment alone. In this way, countermeasures to many types of attacks including targeted attacks can be formulated.

5. Future developments

NTT Secure Platform Laboratories plans to construct prototype tools for implementing detection, analysis, and countermeasure technologies and conduct diverse evaluation experiments to keep pace with quickly evolving cyber attacks.

References

[1] M. Itoh, T. Hariu, N. Tanimoto, M. Iwamura, T. Yagi, Y. Kawakoya, K. Aoki, M. Akiyama, and S. Nakayama, "Anti-Malware Technologies," NTT Technical Review, Vol. 8, No. 7, 2010. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201007sf3.html

[2] T. Yagi, N. Tanimoto, T. Hariu, and M. Itoh, "Intelligent High-interaction Web Honeypots Based on URL Conversion Scheme," IEICE Trans. Commun., Vol. E94-B, No. 5, pp. 1339–1347, 2011.

[3] M. Akiyama, M. Iwamura, Y. Kawakoya, K. Aoki, and M. Itoh, "Design and Implementation of High Interaction Client Honeypot for Drive-by Download Attacks," IEICE Trans. Commun., Vol. E93-B, No. 5, pp. 1131–1139, 2010.

[4] K. Aoki, T. Yagi, M. Iwamura, and M. Itoh, "Controlling Malware HTTP Communications in Dynamic Analysis System Using Search Engine," Proc. of the 3rd International Workshop on Cyberspace Safety and Security (CSS2011), Milano, Italy, 2011.

[5] Y. Kawakoya, M. Iwamura, and M. Itoh, "Memory Behavior-based Automatic Malware Unpacking in Stealth Debugging Environment," Proc. of the IEEE International Conference on Malicious and Unwanted Software (MALWARE2010), Nancy, France, 2010.

[6] M. Akiyama, T. Yagi, and M. Itoh, "Searching Structural Neighborhood of Malicious URLs to Improve Blacklisting," Proc. of the 12th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT 2011), Munich, Germany, 2011.

Takeo Hariu

Senior Research Engineer, Supervisor, Network Security Project, NTT Secure Platform Laboratories.

He received the M.S. degree in electro-communications from the University of Electro-Communications, Tokyo, in 1991. Since joining NTT in 1991, he has been engaged in network security R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Institute of Electrical Engineers of Japan (IEEJ).

Mitsuaki Akiyama

Network Security Project, NTT Secure Platform Laboratories.

He received the M.E. degree in information science from Nara Institute of Science and Technology in 2007. Since joining NTT in 2007, he has been engaged in network security R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of IEICE.

Kazufumi Aoki

Network Security Project, NTT Secure Platform Laboratories.

He received the M.S. degree in information science from Tohoku University, Miyagi, in 2006. Since joining NTT in 2006, he has been engaged in network security R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. He is a member of the Information Processing Society of Japan (IPSJ) and IEICE.

Takeshi Yagi

Research Engineer, Network Security Project, NTT Secure Platform Laboratories.

He received the B.E. degree in electrical and electronic engineering and the M.E. degree in science and technology from Chiba University in 2000 and 2002, respectively. Since joining NTT in 2002, he has been engaged in network architecture R&D. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. His current research interests include network security and web security. He is a member of IEICE and IEEJ.

Makoto Iwamura

Research Engineer, Distinguished Researcher, Network Security Project, NTT Secure Platform Laboratories.

He received the B.E., M.E., and D.Eng. degrees in science and engineering from Waseda University, Tokyo, in 2000, 2002, and 2012, respectively. He joined NTT in 2002. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories. His research interests include reverse engineering, vulnerability discovery, and malware analysis.

Hiroshi Kurakami

Senior Research Engineer, Network Security Project, NTT Secure Platform Laboratories.

He received the B.S. degree in physics from Tohoku University, Miyagi, in 1991. Since joining NTT in 1991, he has been engaged in R&D of ATM networks, IP VPNs, and network security. As a result of organizational changes in July 2012, he is now in NTT Secure Platform Laboratories.