Security Intelligence for Malware Countermeasures to Support NTT Group's Security Business

Takeo Hariu, Keiichi Yokoyama, Mitsuhiro Hatada, Takeshi Yada, Takeshi Yagi, Mitsuaki Akiyama, Tomonori Ikuse, Yuta Takata, Daiki Chiba, and Yasuyuki Tanaka

Abstract

Cyber-attacks caused by malware (malicious software) are becoming a serious social problem in many parts of the world. In this article, we introduce the security intelligence technology behind our WideAngle global integrated security service.

Keywords: malware, security intelligence, WideAngle

1. Introduction

Cyber-attacks have been causing a number of social problems in recent years. In particular, malware infections inflict severe damage and can cause leakage of information at a national level. An example of a malware attack on a personal computer (PC) is shown in **Fig. 1**. When a PC with vulnerabilities in its web browser or plugins visits a portal or relay site that has been created by an attacker to automatically forward content, it is automatically transferred to an attack site containing attack codes that cause the browser to become infected by downloading malware. A PC that has been infected with malware by accessing a series of malicious sites in this way will exchange information with a command site created by the attackers for purposes such as information theft.

At NTT's laboratories, we have been researching and developing technology to detect infection activity, collect malware, and analyze the infection pathways and malware behavior [1]. By continuously collecting and analyzing attacks, we have created techniques for efficiently and accurately characterizing the latest malware infections. Recently, however, it has become difficult to create services that lead to effective countermeasures using a single technology alone due to the increasing complexity of attacks and the emergence of malware attacks with a very short cycle.

From empirical knowledge obtained in previous research and development (R&D) and from observing attacks, we realized the importance of the security intelligence and its effect on malicious activity. The security intelligence includes the destinations of traffic related to malware infections, which are obtained through cross-sectional analysis of traffic data and attacks occurring up to and beyond the point of malware infection. Therefore, we began conducting R&D on world-leading intelligence creation techniques [2]. Furthermore, in partnership with NTT Communications, which is a world leader in the global security business, we expanded our security intelligence efforts into the WideAngle managed security service [3].

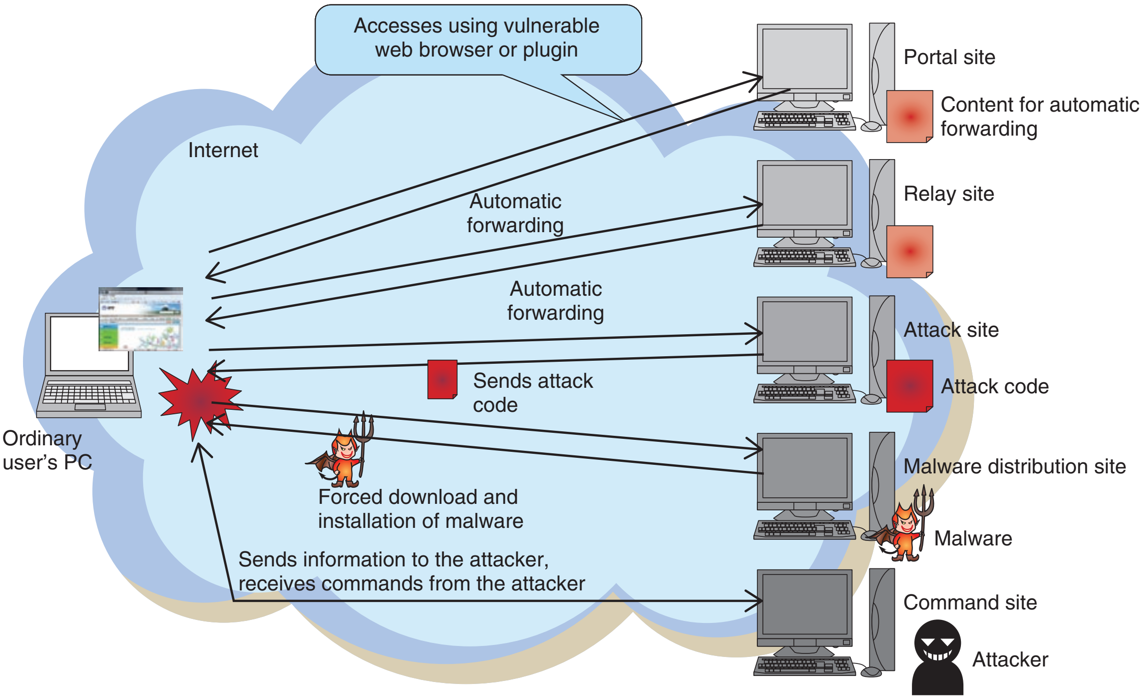

Accesses using vulnerable web browser or plugin
Internet
Portal site
Content for automatic forwarding
Relay site
Automatic forwarding
Automatic forwarding
Attack site
Attack code
Sends attack code
Ordinary user's PC
Malware distribution site
Forced download and installation of malware
Malware
Sends information to the attacker, receives commands from the attacker
Command site
Attacker

Fig. 1. Malware infection attack.

2. NTT security intelligence

In general, security intelligence refers to information used to defend against cyber-attacks. For example, this includes the originating Internet protocol (IP) addresses of DDoS (distributed denial of service) attacks or spam emails, or the IP addresses of botnet C&C (command & control) servers or collection sites for stolen data, and the Uniform Resource Locators (URLs) of phishing sites and fake websites.

A wide variety of cyber-attacks originate from PCs and servers that have been compromised by attackers via malware infection. Therefore, to fundamentally solve the problem of cyber-attacks, it is absolutely essential to have security intelligence for deploying malware infection countermeasures. Also, to develop security intelligence into a business, it is important to have clear documented information on which to base malignancy decisions, as well as information on how it is used.

At NTT's laboratories, security intelligence includes information such as the destination IP addresses and URLs of traffic at the time of malware infection and the destination of traffic from the infected victim, as shown in **Fig. 2**.

Each item of information is associated with evidence identified using proprietary techniques such as decoy systems (*honeypots*) and dynamic malware analysis systems. These techniques are applied in parallel to identify the URLs of malware sites that cannot be collected by other companies. Furthermore, the URLs of these malware sites are analyzed to identify unknown malware site URLs.

2.1 Honeypots

Malware is collected by using decoy systems called honeypots to accept attacks. By analyzing the communication with honeypots, we can gather evidence about the vulnerabilities that are being used by attackers to spread their malware, and to identify information that is effective for preventing infection.

We are conducting R&D on honeypots that keep up with the trends in malware infection activity. We are currently researching and developing web server honeypots to attract attacks that exploit vulnerabilities in web applications, and *honeyclients* to attract attacks that exploit vulnerabilities in web browsers and plugins. Here, we introduce a honeyclient that performs a key role in intelligence creation.

In general, honeypots are classified into two categories: low-interaction honeypots that securely gather the minimum amount of information by simulating a

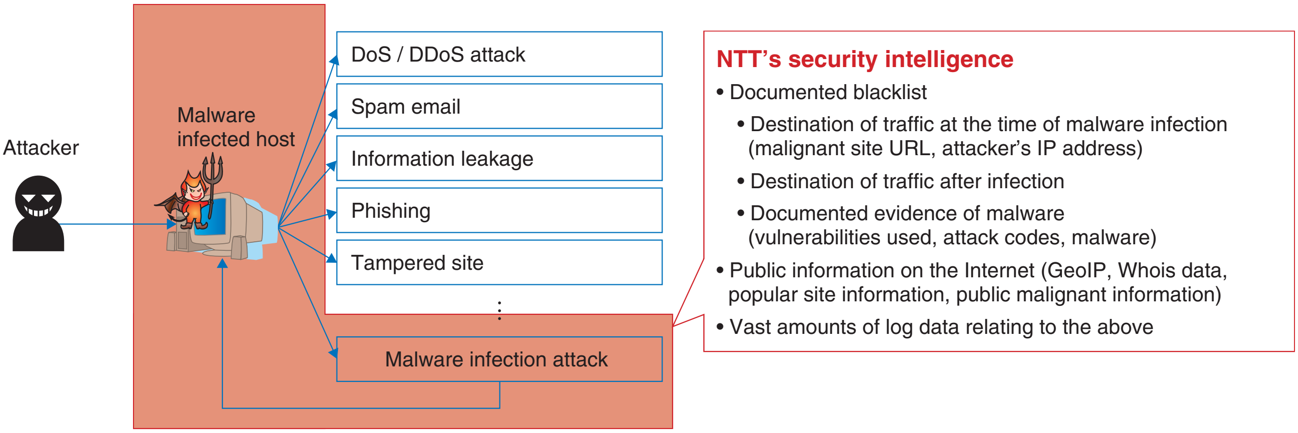

Attacker
Malware infected host
DoS / DDoS attack
Spam email
Information leakage
Phishing
Tampered site
⋮
Malware infection attack
NTT's security intelligence
• Documented blacklist
• Destination of traffic at the time of malware infection (malignant site URL, attacker's IP address)
• Destination of traffic after infection
• Documented evidence of malware (vulnerabilities used, attack codes, malware)
• Public information on the Internet (GeoIP, Whois data, popular site information, public malignant information)
• Vast amounts of log data relating to the above

Fig. 2. NTT's security intelligence.

vulnerable system, and high-interaction honeypots that collect a lot more information by using an actual vulnerable system. Although high-interaction honeypots are said to run the risk of being infected with malware, we have managed to develop a secure high-interaction honeyclient. Also, low-interaction honeypots are said to be only capable of collecting limited information, but we have managed to develop one with improved information-gathering capabilities. With a honeyclient, it is possible to detect malware infections and identify the URLs of malware sites that infect visitors with malware. Then malware infections can be prevented by prohibiting access to such URLs.

2.2 Dynamic analysis of malware

Malware collected by honeypots is analyzed to shed light on its latent threats by investigating its functions in detail. Furthermore, by analyzing the traffic generated by malware infections to discover information such as the servers they communicate with when obtaining additional malware and the command servers set up by the attackers, it is possible to identify information that is effective for suppressing the damaging effects of malware.

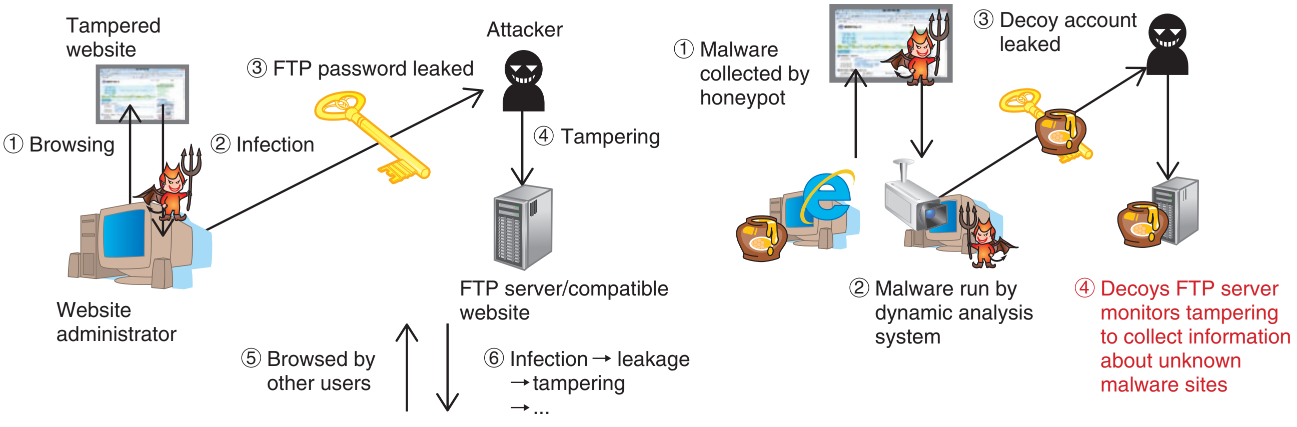
Malware analysis includes dynamic analysis, which clarifies the behavior of malware by actually running it, and static analysis, which deciphers the malware's program code. Dynamic analysis is introduced here.

Dynamic analysis can be performed either in a closed environment, where the malware is operated in complete isolation, or in an open environment, where the malware can connect to the Internet. In both types of environment, a debugger can be used to closely monitor the malware's behavior. Furthermore, taint analysis techniques can be used to track the flow of data handled within a system and identify servers prepared by the attackers to send data causing malicious behavior. For example, PCs that have been infected with malware can be discovered by identifying the PCs that access the command server or destination server when acquiring additional malware.

2.3 Honeytokens

During the dynamic analysis of malware collected by a honeypot, it is possible to allow the attacker to tamper with a controlled decoy website by deploying false information for the website administrator's account in the analysis environment. This makes it possible to collect the latest attack information.

As mentioned previously, the greatest threat of malware infection in recent years has been caused by users unknowingly visiting malware sites. Parts of the malware deployed in these attacks have functions that collect and send out various kinds of account information. Therefore, when a website administrator's account information is recorded on an infected PC, this information is leaked to the attacker so the website can be manipulated by the attacker, as shown in **Fig. 3(a)**. A honeytoken shows nothing but decoy information. Since the content of a website is often managed via a File Transfer Protocol (FTP) server, fake FTP account information is prepared as a honeytoken. The attacker uses the honeytoken information to log in to a separate fake FTP server and tampers with its content. Checking the falsified content in the honeypot makes it possible to collect security intelligence about the latest attacks initiated by the attacker


Tampered website
Attacker
③ FTP password leaked
① Browsing
② Infection
④ Tampering
Website administrator
FTP server/compatible website
⑤ Browsed by other users
⑥ Infection → leakage → tampering → ...
① Malware collected by honeypot
③ Decoy account leaked
② Malware run by dynamic analysis system
④ Decoys FTP server monitors tampering to collect information about unknown malware sites

(a) Typical attack on a PC

(b) Our original observation technique using honeytokens

Fig. 3. Honeytokens.

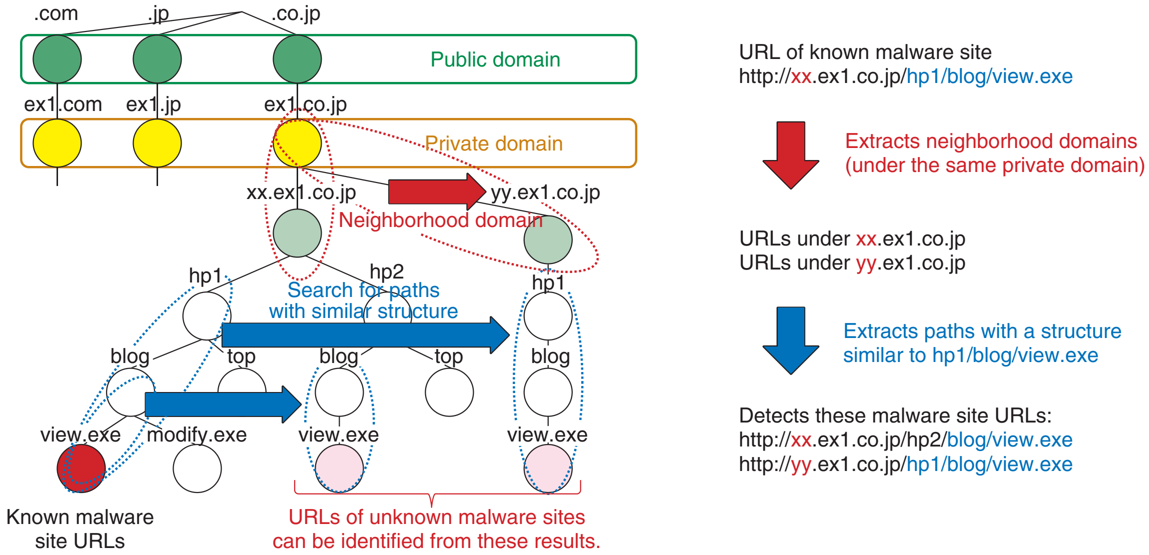

.com
.jp
.co.jp
Public domain
ex1.com
ex1.jp
ex1.co.jp
Private domain
xx.ex1.co.jp
yy.ex1.co.jp
Neighborhood domain
hp1
hp2
hp1
Search for paths with similar structure
blog
top
blog
top
blog
view.exe
modify.exe
view.exe
view.exe
Known malware site URLs
URLs of unknown malware sites can be identified from these results.
URL of known malware site
http://xx.ex1.co.jp/hp1/blog/view.exe
Extracts neighborhood domains (under the same private domain)
URLs under xx.ex1.co.jp
URLs under yy.ex1.co.jp
Extracts paths with a structure similar to hp1/blog/view.exe
Detects these malware site URLs:
http://xx.ex1.co.jp/hp2/blog/view.exe
http://yy.ex1.co.jp/hp1/blog/view.exe

Fig. 4. Neighborhood search of malware sites.

(**Fig. 3(b)**).

A paper summarizing this technique [4] was the first Japanese-authored paper in ten years to be accepted at one of the highest-level international conferences and was highly rated all over the world.

2.4 Searching the neighborhood of malware sites

To avoid defenses set up based on security intelligence, attackers construct numerous malignant sites. Since they are reluctant or unable to spend much money on each site, they adopt configurations that enable new malware sites to be set up without incurring much additional cost. In anticipation of this trend, we identify malware sites by searching for web spaces that are highly likely to have been created by attackers.

This search technique is shown in **Fig. 4**. We first extract URLs with the same path structures as existing malware site URLs in URL groups that exist in the same private domains as the URLs of known malware sites, and then we investigate these URLs using

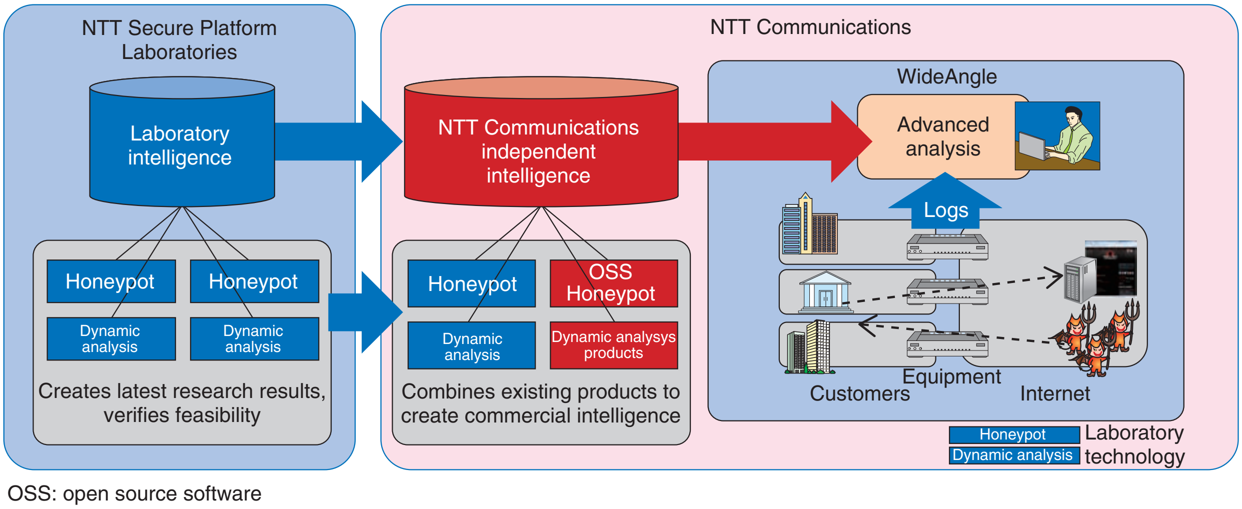

NTT Secure Platform Laboratories
Laboratory intelligence
Honeypot
Honeypot
Dynamic analysis
Dynamic analysis
Creates latest research results, verifies feasibility
NTT Communications
NTT Communications independent intelligence
Honeypot
OSS Honeypot
Dynamic analysis
Dynamic analysys products
Combines existing products to create commercial intelligence
WideAngle
Advanced analysis
Logs
Equipment
Customers
Internet
Honeypot
Dynamic analysis
Laboratory technology
OSS: open source software

Fig. 5. Global business development.

honeypots. An attacker who manages a known malignant site URL will be able to generate such URLs without incurring any cost burden, so with this search technique it is possible to discover malignant URLs prepared by attackers that are intended to avoid security intelligence. This technique was summarized in a paper that achieved global recognition [5] and received the best paper award at a major international conference.

3. Global business development of security intelligence

The honeypot and analysis techniques and the security intelligence services created at NTT's laboratories are being put to use in the services offered by NTT Communications. By implementing a combination of laboratory techniques, security intelligence, and existing products, NTT Communications is creating its own independent security intelligence, as shown in **Fig. 5**.

In business applications, we envisage that security intelligence could be deployed in services such as log auditing, user access filtering, or monitoring user websites. We have been using security intelligence in NTT Communications' managed security services for log auditing since February 2013. In this service, security intelligence is used to detect security risks by employing advanced correlation analysis and to automatically assess threat levels. In this way, correlation analysis is done automatically on vast amounts of security information such as communication log files collected using ICT (information and communication technology) equipment, enabling an advanced and rapid response to any detected threats.

Our managed security services are currently marketed under the WideAngle brand name, and they provide globally seamless comprehensive security countermeasures to users by conducting advanced security monitoring all day, every day based on a security provider system that includes over 900 specialists in 14 countries worldwide.

4. Future prospects

In the future, we plan to work on making our global business more competitive and on developing our security business while prototyping NTT's leading-edge security technology.

References

[1] M. Ito, 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. Hariu, M. Akiyama, K. Aoki, T. Yagi, M. Iwamura, and H. Kurakami, "Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa2.html

[3] Website of WideAngle,
http://www.ntt.com/wideangle_security_e/

[4] M. Akiyama, T. Yagi, K. Aoki, T. Hariu, and Y. Kadobayashi, "Active Credential Leakage for Observing Web-based Attack Cycle," Proc. of RAID2013 (the 16th International Symposium on Research in

Attacks, Intrusions and Defenses), Vol. 8145, pp. 223–243, Rodney Bay, St. Lucia, Oct. 2013.

[5] M. Akiyama, T. Yagi, and M. Itoh, "Searching Structural Neighborhood of Malicious URLs to Improve Blacklisting," Proc. of SAINT2011 (the 11th IEEE/IPSJ International Symposium on Applications and the Internet), pp. 1–10, Munich, Germany, Jul. 2011.

Takeo Hariu

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

He received his M.S. 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. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Institute of Electrical Engineers of Japan (IEEJ).

Keiichi Yokoyama

Senior Manager, Security Operation Center, NTT Com Security Corporation.

He joined NTT in 1997 and worked on the development of security services for the OCN Internet service. He has led various Ministry of Internal Affairs and Communications projects involving NTT R&D technology, including the Cyber Clean Center project from 2006 to 2010 and the Reputation Database Project from 2009 to 2011. He has been with NTT Com Security since 2012.

Mitsuhiro Hatada

Senior Manager, Technology Development/ NTT Com-SIRT, NTT Communications Corporation.

He received his B.E. and M.E. in computer science and engineering from Waseda University, Tokyo, in 2001 and 2003. He joined NTT Communications in 2003 and has been engaged in R&D of computer and network security. He is a member of the Information Processing Society of Japan (IPSJ) and IEICE.

Takeshi Yada

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

He received an M.S. in engineering from Tokyo Institute of Technology in 1991. Since joining NTT in 1991, he has been conducting R&D on network architecture, measurement, and inference for network traffic, and network management. His current research interests include network security. He is a member of IEICE, the Operations Research Society of Japan, and the Japan Statistical Society.

Takeshi Yagi

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

He received a B.E. in electrical and electronic engineering and an M.E. in science and technology from Chiba University in 2000 and 2002. He also received a Ph.D. in information science and technology from Osaka University in 2013. Since joining NTT in 2002, he has been engaged in research and design of network architecture and traffic engineering. His current research interests include network security, especially honeypots and security-data analysis based on machine learning. He is a member of IEICE, the Institute of Electrical and Electronics Engineers (IEEE) and IEEJ.

Mitsuaki Akiyama

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

He received his M.E. and Ph.D. in information science from Nara Institute of Science and Technology in 2007 and 2013. Since joining NTT in 2007, he has been involved in R&D of network security, especially honeypots and malware analysis.

Tomonori Ikuse

Researcher, Cyber Security Project, NTT Secure Platform Laboratories.

He received an M.E. in information science from Nara Institute of Science and Technology in 2012. Since joining NTT in 2012, he has been engaged in network security R&D. He is a member of IEICE.

Yuta Takata

Researcher, Cyber Security Project, NTT Secure Platform Laboratories.

He received his B.E. and M.E. in computer science and engineering from Waseda University, Tokyo, in 2011 and 2013. He is currently a Ph.D. student in the Department of Computer Science and Communications Engineering, Waseda University. Since joining NTT in 2013, he has been engaged in R&D of network security, especially honeyclients and malicious code analysis.

Daiki Chiba

Researcher, Cyber Security Project, NTT Secure Platform Laboratories.

He received his B.E. and M.E. in computer science and engineering from Waseda University, Tokyo, in 2011 and 2013. He is currently a Ph.D. student in the Department of Computer Science and Communications Engineering, Waseda University. Since joining NTT in 2013, he has been conducting research on cybersecurity through data analysis.

Yasuyuki Tanaka

Manager, Technology Development/NTT Communications Corporation.

He received a B.E. in physics from Rikkyo University, Tokyo, in 1995 and an M.E. in informatics from the Institute of Information Security, Kanagawa, in 2015. He joined NTT in 1995 and has been engaged in R&D of computer and network security. He is a member of IPSJ.