2 Summary of Research and Development Activities

2-1 Overview of Research and Development Activities on Cyber-Security

Daisuke INOUE

In order to cope with cyber-attacks which had been continuously growing in sophistication, in 2011, in the Cyber Security Laboratories, we started our studies on cyber-security technologies, constructing the world most advanced technology-infrastructure that enables the observations, analyses, counter-measures, and prevention of cyber-attacks: as the abovementioned example shows, for the purpose of contributing to the solution-provision of social issues, we have been conducting the activities on cyber-security research and development by taking practical approaches. In 2013, under the Cyber-Attack Counter-Measure Research Center, Cyber-Attack Protection-Tactics Research Laboratory and Cyber-Attack Detection and Analysis Laboratory were established. Their missions are to conduct the studies for the establishment of cyber-attack protection tactics which are derived from the fundamental studies on cyber-attack mechanisms and the studies on the recreation of attacks—of course safely—for attack-evaluation and test. In this article, we show the overview of NICT's research and development activities on the cyber-security technologies conducted during the five years from FY2011 that were conducted following the 3rd Medium- to Long-Term Plan.

1 Introduction

We have been receiving so many benefits in our social and economic activities from the Internet that we could not get back to the era where no Internet is available; the Internet has made irreversible changes in every corner of our modern society. However, on the other hand, the threats of cyber-attacks in the Internet have become more and more severe at the same pace as the growth of the Internet. Of course, cyber-attacks are caused by human "crackers"—carrying out hacking with bad intentions, but it is true that the tools available exist—illegal programs called malware. Malware in the earlier half of 1990s or earlier was mainly created, used and provided by offenders for pleasure or for self-promotion. However, since the latter half of 1990s when organized criminals began to use malware as tools for stealing money, malware has drastically advanced in performance and sophistication.

We, for the purpose of coping with the cyber-attacks using such advanced malware, have been conducting our research and development activities on the following; the technologies of the real-time observation, analysis, and counter-measure-taking against cyber-attacks or advanced persistent threats (APR); infrastructure technologies for detecting attack-signals to take preventive actions. In parallel, we, for the purpose of utilizing the data we obtained on malware attacks and attack traffic for the promotion of researches or the development of human resources, have been focusing our efforts on the development of cyber-attack protection technologies.

In this section, we introduce the following four research themes on which the research activities were conducted in

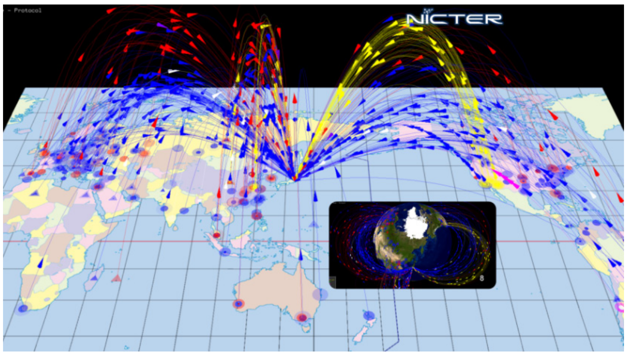


Fig. 1 Network Incident analysis Center for Tactical Emergency Response, NICTER

Cyber Security Laboratories, following the 3rd Medium- to Long-Term Plan: the construction of the world largest cyber-attack observation network; the infrastructure technologies for the cyber-attack analysis and prevention; IPV6 security-evaluation and protection technologies; and the cyber-security research infrastructure.

2 Construction of Cyber-Attack Observation Network

2.1 Indiscriminate Cyber-Attack

We had been placing efforts on the construction of our incident-analysis center, NICTER[*1] (Fig. 1) as a countermeasure against indiscriminate attacks, enhancing it in FY2015 by doubling the dark-net (unused IP address) coverage to the world’s largest scale of 300,000 IP addresses through deploying our sensors to external domestic / overseas organizations; such expansion of our observation network has enabled us to construct such systems that are able to quickly detect the signals of forth-coming attacks such as suspicious activities preparing Reflection DoS Attacks[*2] (DRDoS) or large-scale virus-infections of IoT devices. We promoted the deployment of our sensors to the organization in the U. S. and EU as one of our international collaboration activities in the security-field.

We introduce below one of the significant findings by NICTER. Statistical summaries of our observations indicate interesting events.

NICTER Dark-Net Observation Statistics of 2014 and 2015 indicates the following; the total annual number of observed packets per IP address had increased drastically—doubled year by year—, and furthermore the analysis of the number of packets by destination port-number shows that the number of service-packets on the 23rd port (TCP) had grown. The investigations conducted by Yoshioka Laboratory, Yokohama National University suggest that IoT devices actually-working in business operations including Web cameras or broadband-routers have been infected by malware to work as attackers. For the details of NICTER Observation Statistics, we recommend readers refer to the reference documents listed in “**3-1** NICTER’s Long Term Analysis of the Dark-Net.”

Fig. 2 Long-Duration Operation Test of Sensors for GHOST, Active Cyber-attack Observation System

Also, in order to share information, we have been providing the observation and analysis results by NICTER to the following organizations; JPCERT / CC; IPA; @Police; SIGMON (a group of volunteers for stationary-observation), participated in by national universities and others; a working group of domestic ISPs established for ensuring prompt collaborative counter-actions to DoS attacks; ACTIVE PROJECT in the Ministry of Internal Affairs and Communications. Furthermore, in FY2012, we started the development project of DAEDALUS[*3]—a mechanism to raise alerts when a communication from a private address to the NICT Observation Network is detected, and NIRVANA[*4]—a visualization and analysis system of real networks.

In addition, for the purpose of utilizing the information derived from the observations in a disaster situation to ensure the quick and prompt grasp of the network damage-situations, we have conducted research and developments, constructing a system named ACTIVATE—estimating the live-or-dead situation of networks.

In addition, for the purpose of the construction of an cyber-attack active observation network—enabling flexible and dynamic allocation of cyber-attack observation sensors—, we promoted the research and developments on the GHOST[*5] Sensor—cyber-attack active observation system where the groups of virtual sensors (tunneling nodes using virtualization technologies) that are deployed in a distributed way to a number of organizations, and the censor-side various types of sensors with different operation-modes are integrated and operated through switching—, successfully conducting in FY2015 the long-duration experiments (Fig. 2) on a large scale dark-net augmented by about 16,000 addresses, showing that the system was able to detect malware at an improved rate.

We recommend the readers refer to the reference

[*1] NICTER: Network Incident analysis Center for Tactical Emergency Response

[*2] A DNS Reflection Attack is an attack using “packet-reflections,” where a large number of DNS packets with false sender addresses are sent to a target of attack.

[*3] DAEDALUS: Direct Alert Environment for Dark-net and Live-net Unified Security

[*4] NIRVANA: NIcter Real-network Visual ANAlyzer

[*5] GHOST: Global, Heterogeneous, and Optimized Sensing Technology

documents listed in Section **3** for the details of how NICT will use its systems in disaster situations or the details of DAESALUS—it is an anti-indiscriminate-cyber-attack system, and it is a spin-off system out of NICTER.

2.2 Counter-Measures Against Indiscriminate Attacks

As for counter-measures against advanced persistent threats (attack on a specified target), we have been placing our efforts on the development of a technological framework design for preventing malware-infected computers from leaking information and the implementation of the prototype system to realize a part of the framework.

As for the establishment of the counter-measure technologies against advanced persistent threats, we have attained so far the following achievements through extending research and development activities we have been conducting: the development of correlation-analysis engine that enables cross-relational analyses of a number of alerts of different types, by promoting the development of "NIRVANA-Kai" (Advanced NIRVANA)—it is a comprehensive cyber-attack analysis platform that performs the real time observations (of real traffic) and analyses of in-organization (internal) networks, integrates alerts raised by individual security-appliances of different types, and at the same time helps us drill-down to the alert sources by using a real-time visualization interface—, the development of the functions for end-host-collaboration and the functions for automatic protection. We deployed NIRVANA to the Interop TOKYO Exhibition site to perform demonstrations of live-net observation and analysis on ShowNet—it is composed of the most advanced network devices—and, in collaboration with a number of domestic / overseas companies related to security, conducted proof-of-concept experiments on the integration of the alerts raised by different types of security-appliances. Also, at the latest exhibition (Interop Tokyo 2016), such proof-of-concept experiments were conducted.

Furthermore, we have promoted the research and development of a high-speed analysis infrastructure which enables us to analyze a very large number of live-nets; proving its real-time processing performance by a large-scale on-memory processing of 200,000 packets/sec through conducting experiments on NICT's live-network. Also, in addition to developing the Across-Network-Boundary Intrusion Detection Engine, in parallel we developed different types of live-net analysis engines of different methods including the black-list method, white-list method and slow-scan detection method.

Also, we have promoted the development of end-host software-solutions including anti-virus solutions (network-based intrusion-detection solutions) by developing a system for NIDS[*6]-HIDS[*7] collaboration. Such activities led to the development of the following; the mechanism for the centralized process-status monitoring or security-level adjustment of end-hosts; the functions for the information-collection from end-hosts and the collaboration with end-hosts; and the functions for the automatic protection of end-hosts (Fig. 3).

Furthermore, in collaboration with the Cyber-Attack Evaluation Laboratory, we implemented, on StarBED, a simplified model network-environment of an in-house network, and prepared a command-and-control (C&C) server and remote access tools (RAT)—offense-side players use those tools—, conducting, by using the environment, attack-simulation experiments to make evaluations of the attack observation / analysis technologies that are used on the defender-side and analyze the various-types of logs generated and left on the occasions of advanced-persistent-threats.

On the other hand, we developed, by using NIRVANA-Kai as a base, the following systems / tools for "Capture The Flag (CTF)", which is a game developed for the purpose of the enhancement of the technologies for cyber-attack protection; the dedicated engine "NIRVANA-Kai SECCON Custom" which visualizes the actions by defense-player and offense-player "NIRVANA-Kai SECCON Custom Mk-II"; AMATERAS". We developed and improved those tools every year following the CIF schedule. On the SECON National Convention—the contest-event of information

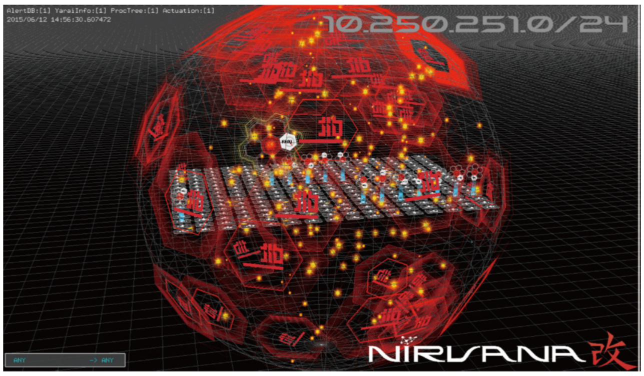


Fig. 3 NIRVANA-Kai's Automatic Protection Functions

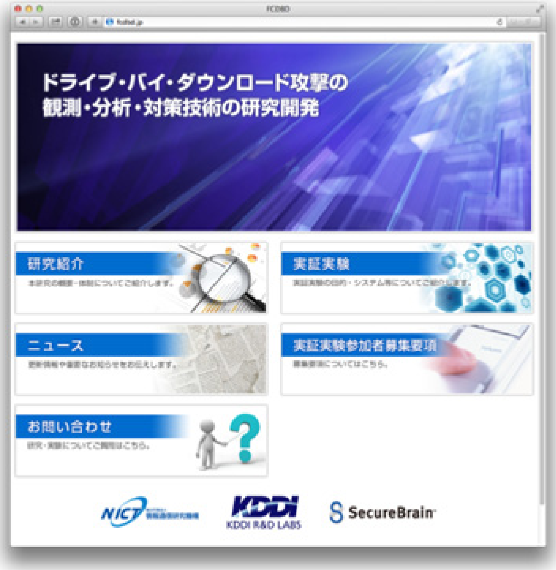
[*6] NIDS: Network-based Intrusion Detection System
[*7] HIDS: Host-based Intrusion Detection System

security—we successfully visualized the CIF Final Battle, fought by the CIF top teams from countries around the world.

3 Cyber-Attack Analysis and Prevention Infrastructure Technologies

We have been conducting the research and development of observation / analysis technologies against the attacks abusing Web or SNS that have newly arisen, focusing on the anti-cyber-attack analysis / prevention infrastructure technologies using diversified inputs from different types of sensors and data-mining methods.

For the purpose of developing the prevention measures against drive-by-down-load (DBD) attacks via websites, we developed the DBD-attack counter-measure technology, which enables protection against Web-based attacks through broadly deploying web-browser-plug-in sensors to users, macroscopically observing users' behaviors at the observation-center to detect illegal sites including malware-pushing sites, and furthermore directly blocking users' accesses to those illegal sites. We conducted a small-scale experiment on those technologies in FY2014, and a large-scale proof-of-concept experiment participated in by about 1,600 users in FY2016 (Fig. 4). Along with the validity evaluation, we also have been conducting the legal and technological studies on the proper management of personal information, holding a workshop on what to do in the above mentioned experiment held prior to the conduction of the experiment.



FCDBD

fcdbd.jp

ドライブ・バイ・ダウンロード攻撃の
観測・分析・対策技術の研究開発

研究紹介
本研究の概要・体制についてご紹介します。

実証実験
実証実験の目的・システム等についてご紹介します。

ニュース
最新情報や重要なお知らせをお伝えします。

実証実験参加者募集要項
募集要項についてはこちら。

お問い合わせ
研究・実験についてご質問はこちら。

Fig. 4 Proof-Of-Concept Experiment Site for DRDoS-Attack Counter-measure Framework

As for the basic studies on SNS-security technologies, we have conducted the following; studies on the detection methods of spam-message diffusion or malware-infections, using a model we developed to express a target SNS as a structure of user-account-to-user-account links and user-account-to-related-resource links: prototype development of SNS observation / analysis technologies; proposals and proof-of-concept experiments and validity-evaluations of illegal user detection methods based on users' mutual co-operation / collaboration which could be used as a counter-measure against illegal users on SNS including those engaged in impersonation.

On the other hand, for the purpose of the establishment of cyber-attack analysis / prevention infrastructure technologies, we have conducted the research and development on the multi-modal analysis to find-out the correlations between the different types of cyber-attacks, thus revealing that there exist correlations between the different types of cyber-attacks which conventionally had been analyzed separately. In addition, for the purpose of the realization of cyber-attack prediction, we have developed the detection method of BOT traffic by applying data-mining— the method, by eliminating the impacts of human-induced / abrupt surges on traffic, ensures the extraction of the trends which are signaling the activities caused by malware infections. In FY2012, we conducted proof-of-concept experiments on in-NICT networks; we applied the previously-mentioned technologies as the anti-APT-countermeasure technologies to use them as the prototypes of the analysis engines for detecting abnormal events from the in-house communications and the outbound communications.

Furthermore, we have been operating a DRDoS honey pot cooperatively with MIC's PRACTICE Project (cyber-attack-prediction / quick response project by international collaboration), developing the DRDoS alert raising system, and successfully detecting DRDoS attacks on the organizations in Japan with a high degree of accuracy.

4 Technologies for IPv6 Security Evaluation and Protection

For the purpose of securing new-types of network infrastructures including IPv6, we have been conducting the research and development of security-evaluation and protection of the IPv6 environments, as introduced below.

We have designed and developed the technical environments—simulating in-corporate environments— for evaluating IPv6 security, under the IPv6 Technical Evaluation Conference, which is participated in by NICT, OS-venders, communication business operators, and network-appliance vendors. Under these environments, we conducted experiments following the 40 attack-scenarios, making a judgment on the go / no-go of each of the attack scenarios, studying how an attack failed or succeeded. Furthermore, we discussed, at the conference, the protection-measures, studying the protection against each of the attack scenarios. In FY2011, we finalized the studies of protection-measures, releasing the final report, which listed the 100 protection measures. The evaluation results and protection measure were submitted as an international recommendation to ITU-T and approved in December 2013 as X.1037. Furthermore, 23 out of 40 attack-scenarios used the Neighbor Discovery Protocol (NDP), so we developed BDP Guard—protection technology against the attacks abusing NDP—, conducting validity evaluations of the technology in experimental environments.

5 Research Infrastructure of Cyber Security

NICT, as a neutral and public institution, has been able to collect the information on security including attack traffic and malware specimens. For the purpose of promoting the utilization of such information in a safe and secure manner and advancing the network-security research in Japan, we have conducted the research and development of filtering technologies for preventing security information from being leaked; and in parallel, we constructed the cyber-security research infrastructure (NONSTOP[*8]), conducting its production-level operations, in collaboration with universities and businesses.

In FY2011, we implemented the following functions in NONSTOP as its filtering tools: malware detection function; packet capture (PCAP) functions; compressed file detection functions; cryptogram detection functions based on FIPS130-2 randomness test; communication-volume control functions. At the same time, we introduced into the infrastructure the technologies for sanitizing sensor IP addresses in real-time on the occasions when attack-traffic arrives; subsequently, we enhanced the functionality of the infrastructure, by adding functions— for instance, implementing debug functions into the virtual machines handling malware specimens, and adding information on spam-mails.

In addition to the above-mentioned activities, we also conducted the following activities; we conducted the test-operations of NONSTOP in collaboration with the universities in Japan: originally with three universities and later with eight universities and other organizations; we have promoted the utilization of the security information collected by NECTER, through providing since 2012 via NONSTOP the darknet traffic data as a data-set to be used in the malware counter-measure research workshop, the largest workshop in Japan dedicated to anti-malware measures research human-resource development. Through those activities, we have contributed to the human resources development on security research or engineering, which is the most urgent issue. The data we provide are used in a number of domestic organizations for their researches.

Daisuke INOUE, Ph.D. (Eng.)
Director of Cybersecurity Laboratory,
Cybersecurity Research Institute
Cybersecurity, Network Security, Information Security

[*8] NONSTOP: NICTER open network security test-out platform