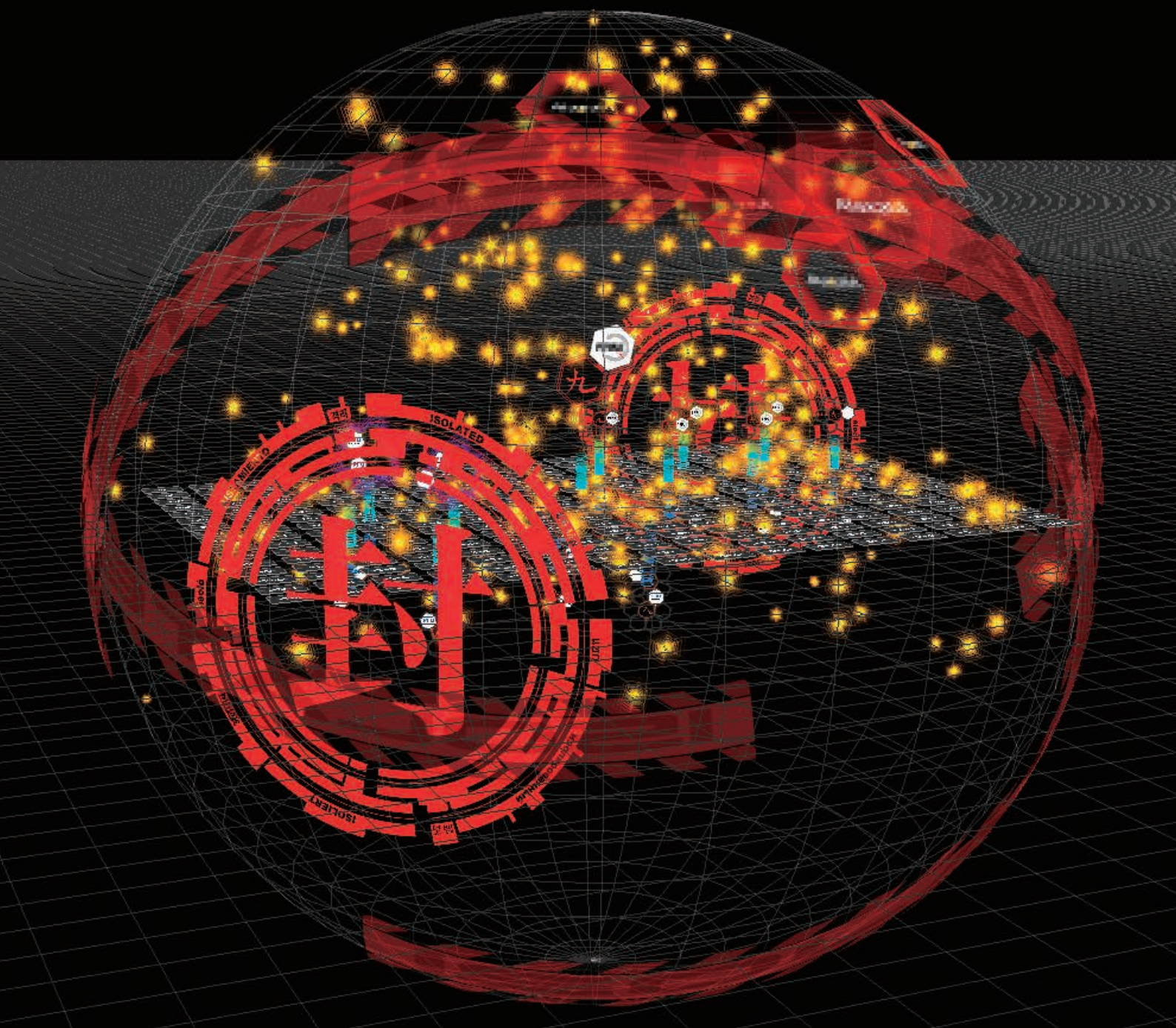
National Institute of
Information and Communications Technology

NICT NEWS

2018
No. 6
Vol. 472

FEATURE

A State-of-the-Art R&D on Cybersecurity



NICT NEWS 2018 No.6 Vol.472
National Institute of Information and Communications Technology

CONTENTS

FEATURE

TOPICS

Cover photo: "Screenshot of the Visualization of NIRVANA KAI"
The screen shown is a visualization of the status of the network segment isolated from the Internet following the actuation of NIRVANA KAI automatic protection functions for security and network devices.
The white panel at the center represents an IP address for the organization's network segment. The sphere surrounding the panel represents networks outside the segment. The yellow light indicates communications isolated and contained within the segment.
Upper left photo: This shows the NICTER Operation Room, where threats of cyberattacks are detected and analyzed.

INTERVIEW

How Can We Protect Ourselves from Sophisticated Cyberattacks?

What's the Cybersecurity Laboratory's mission?

Daisuke INOUE
Director of Cybersecurity Laboratory, Cybersecurity Laboratory
After completing a doctoral course in 2003, he joined Communications Research Laboratory (currently NICT). He has been engaged in research and development of network security focusing on Network Incident analysis Center for Tactical Emergency Response (NICTER) since 2006. Ph.D. (Engineering).

With cyberattacks intensifying by the day and a mere two years to go until the Tokyo 2020 Olympic and Paralympic Games, cybersecurity is also gaining importance. Another concern is attacks on the IoT (Internet of Things), whose societal profile and deployment have rapidly grown in recent years.

So how does the Cybersecurity Laboratory at NICT intend to counter these threats? We put this question to Dr. Daisuke INOUE, Director of the Cybersecurity Research Institute's Cybersecurity Laboratory.

— What do you see as the Cybersecurity Laboratory's research themes?

Dr. INOUE: The research at our laboratory addresses practical measures to strengthen security in cyberspace. We do research and development to build security technologies unique to Japan by examining the technologies needed in everyday society and by studying the most advanced technologies available in the world today.

NICTER, Monitoring Japan's Largest Darknet

— Your laboratory is developing cybersecurity systems. Can you give some examples?

Dr. INOUE: I can position the systems we're developing on a two-dimensional map (Figure: Cybersecurity Laboratory Research Map). Along the vertical axis, measures positioned toward the top tend to be more passive. Measures toward the bottom tend to be more active. The horizontal axis indicates scale: the left side is more global; the right side is more local.

Passive here means basically characterized by silent observation and analysis of cyberattacks. Active refers to interactive countermeasures.

The horizontal axis shows the scale of the monitoring of cyberattacks. Global systems perform wide-range monitoring of networks. Local systems monitor networks within organizations.

The systems classified as global and passive include NICTER*1 and DAEDALUS.*2 NICTER is an incident analysis center, which could be described as the starting point of all of our research and development activities. It monitors and analyzes communications reaching the approximately 300,000 IP address spaces called the darknet.

— What's the darknet?

Dr. INOUE: The darknet refers to a group of IP address spaces that aren't used on the Internet. In indiscriminate cyberattacks, scans are transmitted to identify devices that would make suitable attack targets. Since the scans are transmitted over the entire Internet, they reach all IP addresses, even unused IP addresses, i.e., the darknet. So, by using NICTER, we can get an idea of the global trend of indiscriminate cyberattacks. NICTER is the only system in Japan that monitors the massive darknet of nearly 300,000 IP address spaces.

— Can you describe the cyberattacks in more detail?

Dr. INOUE: According to NICTER monitoring data from 2017, the most common type of attack targets TCP port 23. These attacks accounted for a third of all cyberattacks. The port number determines the type of service being accessed on the Internet. Port 23 is used for Telnet, a communication protocol established in the 1980s that lets a user access a server over a network. Cyberattacks gain access to IoT devices via this port.

Recent trends indicate attacks on IoT devices are on the rise. What's more, these attacks are growing more ingenious. Up to around 2016, most attacks involved penetrating devices using simple IDs and passwords. From 2017, some began to target vulnerabilities (flaws in programs) in the IoT devices. Now, in 2018, we've seen even multistaged attacks on the Android terminals linked to IoT devices.

— How is NICTER's monitoring data being applied?

Dr. INOUE: We're sharing information with security organizations like the JPCERT Coordination Center, IPA (Information-Technology Promotion Agency), and @police of the Na-

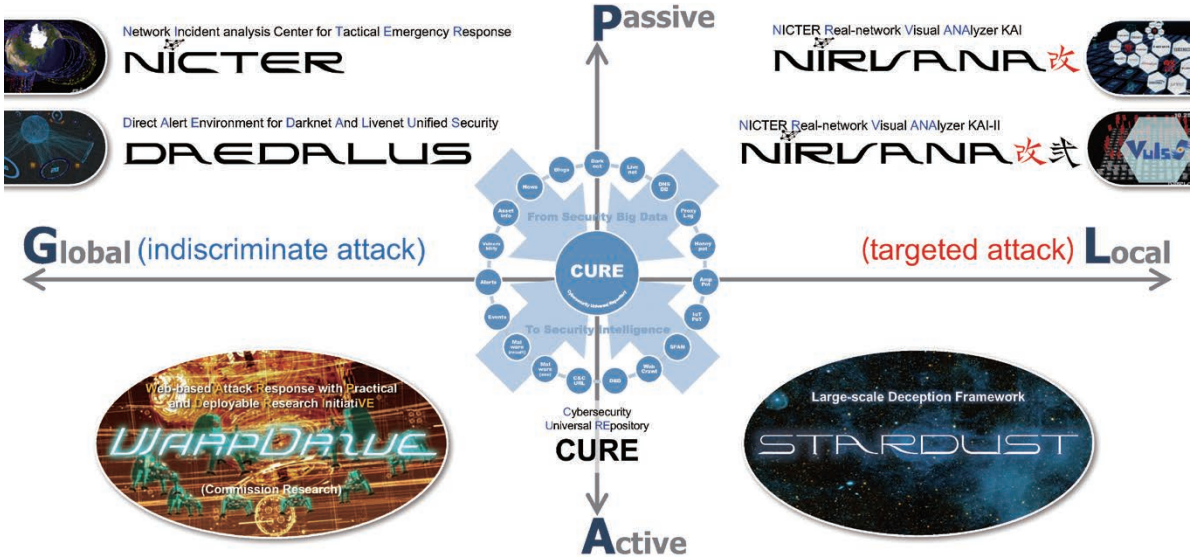


Figure Cybersecurity Laboratory research map

tional Police Agency. We're also cooperating with the National Center for Incident Readiness and Strategy for Cybersecurity (NISC) and the Tokyo Organizing Committee of the Olympic and Paralympic Games. For the general public, we provide information through NICTER Web (https://www.nicter.jp/) and the NICTER Blog (https://blog.nicter.jp/).

DAEDALUS and NIRVANA KAI/ NIRVANA KAI-II

— And what does DAEDALUS do?

Dr. INOUE: DAEDALUS is a cyberattack alert system. When NICTER detects a communication sent from a specific organization within the large-scale darknet monitoring network, it issues an alert to the organization to notify them of potential malware infections. The alert information is currently provided free of charge to approximately 600 municipal governments. We've also transferred DAEDALUS's technologies to companies. That's already led to some commercial alert services becoming available.

— What are NIRVANA KAI and NIRVANA KAI-II?

Dr. INOUE: NIRVANA KAI*[3] is an integrated platform for analyzing cyberattacks. To enable countermeasures to localized cyberattacks, including targeted attacks, we install sensors from the top level down to the network branches deployed within an organization. This makes it possible to monitor, analyze, and visualize traffic. NIRVANA KAI also functions as a security operations assistance tool within the organization; it collects alerts sent from various security devices, performs triage (prioritizes response), and enables automatic response to security threats.

NIRVANA KAI-II is a vulnerability management platform. It gathers information in advance, like OS architecture and software on server devices on the organization's network, to allow rapid response whenever a new vulnerability comes to light. We use Vuls, a Japanese-made open source vulnerability scanner, to assess the vulnerability of server devices.

Both NIRVANA KAI and KAI-II are designed to allow use with security devices deployed by domestic and foreign companies. Technological transfers to private industry is currently underway to allow implementation of these systems in the real world.

WarpDrive, Using a Character from SF Anime

The system in the active and global quadrant is WarpDrive,*[4] a framework for web-based attack response. With certain types of cyberattack, simply browsing a website can result in a malware infection. The system involves installing an attack monitoring sensor as a browser extension, which then collects web access data for users on a massive scale. The sensor also has an actuator function that blocks attempts to access malicious websites.

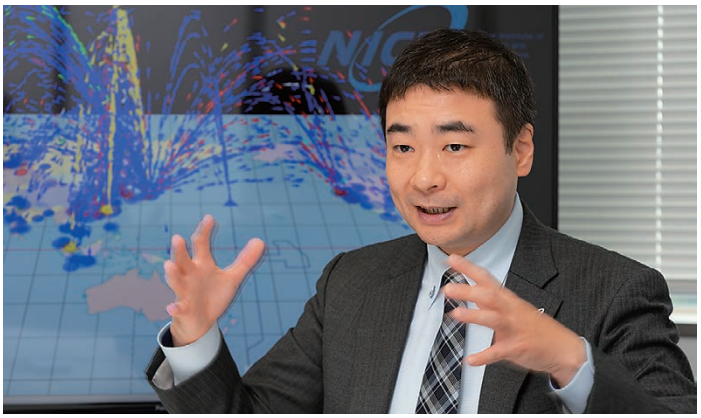
The browser extension is represented by Tachikoma, an artificial intelligence (AI) robot character from the Ghost in the Shell SF anime series, which has a world-wide following. This emerged from a joint project with the Ghost in the Shell REALIZE PROJECT. The idea is that having Tachikoma play the role of messenger to users will help make the system more friendly and immediate. More users mean more data and better identification of malicious sites. An experiment began June 1, 2018. It's already enrolled several thousand participants.

STARDUST and CURE

In the active and local quadrant is STARDUST, an infrastructure for luring cyberattacks. In a targeted attack, the adversary uses computers infected with malware as stepping stones from which the adversary seeks to penetrate the target organization. The conventional approach, which involves simply analyzing the malware program, doesn't provide a complete picture of the activities of the actual adversary, the person at the core of the attack.

STARDUST involves building a dummy network environment that mimics that of an organization. The adversary is then lured into this environment. The environment is recreated in such detail that the adversary doesn't realize he's penetrated a dummy network. This lets the observer monitor the behavior of the adversary over an extended period and analyze the attack methods and intent.

One achievement already made possible by STARDUST is that we've been able to uncover the true nature of the adversaries. Surprisingly, most targeted attacks deploy methods so similar suggesting that the various adversaries seem to be working from the same manual. The skills of the adversaries weren't necessary remarkable,



which contrasts with the conventional idea that attacks like this are perpetrated by incredibly skilled black-hat hackers. The latter cases turned out to be far outliers. Based on this data, we expect to establish technologies that will generate reasonable countermeasures to targeted attacks.

Last, positioned at the center of the research map, is the Cybersecurity Universal Repository (CURE).*5 This collects information from all directions—passive, active, local, and global. We're pursuing research and development on a scheme for mutually linking and analyzing the collected data. By collecting and analyzing massive volumes of data with CURE, we hope to generate a comprehensive intelligence picture from the dispersion of big data. The key to achieving this goal will be automatic analysis technologies based on machine learning.

NICT's Role

— What role does NICT play as a national research and development institute?

Dr. INOUE: Our principle is to return to society the technologies developed at our laboratory and the data obtained using these technologies. To do this, we promote technology transfers to industry and information sharing with security organizations. For example, during a recent large-scale malware infection incident in Japan, our analysis team participated in the containment effort by working to identify the cause, then issuing warnings alongside associated organizations.

— Where do Japan's security technologies rate on a global scale?

Dr. INOUE: It's hard to make simple comparisons. During Japan's so-called lost 20 years, investment in research and development on security technologies was really low. Research and development progressed at a solid pace in Europe and USA during that time, eventually creating the current global security industry. But we've seen a significant change in awareness among Japanese businesses. With news of cyberattacks reported in the media every day and following several incidents of massive information leaks from companies, management leaders now fully grasp the importance of security. Most of all, there's increased awareness that the need for security presents business opportunities.

The term *security self-sufficiency ratio* has emerged in recently years. This refers to how big a share of the domestic market is held by the country's own security products. Sadly, in Japan right now, no domestic security product holds a major share. Most government offices and companies in Japan are protected by foreign security products. The security is one whose internal logic can't be fully accessed—security provided by a black box, so to speak. From the viewpoint of national security, we know we have to increase Japan's security self-sufficiency ratio.

— What practical strategies are you planning to adopt?

Dr. INOUE: NICT can't tackle this whole issue by itself. We're planning to work with industries and academic partners in our research and development efforts. For example, NICT's own network has been turned into a security testbed. Security technologies developed not just by our laboratory but by other companies and universities can be brought in and tested here. Various evaluation tests are already underway. Another advantage NICT offers is the massive volumes of data we've accumulated. We plan to provide this to researchers and engineers outside NICT to maximize their utility.

— What do you see as future prospects?

Dr. INOUE: The first thing is to make sure nothing happens to disrupt the Tokyo Olympics and Paralympics in 2020. We hope to do this by improving domestic security technologies and helping train a highly-skilled security workforce. Success in this endeavor should help Japan to become a player in the global security business in the years to follow.

---

*1 NICTER (Network Incident analysis Center for Tactical Emergency Response)

*2 DAEDALUS (Direct Alert Environment for Darknet And Livenet Unified Security)

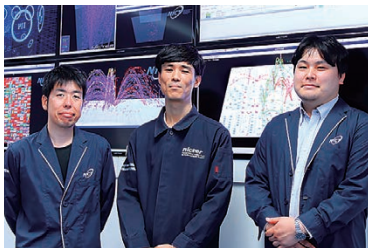
*3 NIRVANA (NICTER Real-network Visual ANAlyzer)

*4 WarpDrive (Web-based Attack Response with Practical and Deployable Research InitiatiVE)

*5 CURE (Cybersecurity Universal Repository)

Current State of Cyberattacks as Revealed by Large-Scale Monitoring

Research and development to detect threats in the age of IoT



From the left: Ryoichi ISAWA, Masaki KUBO, Takahiro KASAMA.

Masaki KUBO
Executive Technical Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

Joined NICT in 2017 after working for JPCERT/CC, leading secure coding initiative and vulnerability handling operations. NICTER analysis team leader.

Takahiro KASAMA
Senior Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

Joined NICT in 2011. Engaged in NICTER project as well as other cybersecurity related R&D. Ph.D.(Engineering).

Ryoichi ISAWA
Senior Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

Joined NICT in 2012 after working for an IT security startup. Research area includes malware analysis using OS kernel modules or virtualization technologies. Ph.D.(Engineering).

We have pursued real-time monitoring and analysis of cyberattacks over the Internet for more than 10 years in the NICTER Project. In this article, we present the state of cyberattacks uncovered in recent years by our efforts, with a special emphasis on cyberattacks targeting IoT devices.

Large-Scale Monitoring of Approximately 300,000 Addresses

In the NICTER Project, we assess the current state of cyberattacks by monitoring communications that reach IP address spaces unused on the Internet (i.e., the darknet). Under ordinary conditions, no communication will reach the darknet; in reality, search messages (scans) sent out by computers infected by malware to find the next target have been arriving in volumes. Through large-scale monitoring and analysis of such communications, we can spot indications of a potential malware outbreak in its early stages, enabling fast response. Working jointly with organization both in Japan and abroad, we're carrying out darknet monitoring of approximately 300,000 IP addresses, one of the largest such efforts anywhere in the world (Figure 1).

Increased Activity of Attacks Targeting IoT Devices

Within the past few years, the number of scans observed in the darknet has grown. In 2017, we detected approximately 560,000 packets per IP address. Figure 2 is a graph showing the number of detected packets counted for each type of port to which it was addressed. The graph shows that packets targeting TCP port 23 (Telnet) and TCP port 22 (SSH) comprise the majority. Recent years have seen countless incidents of malware infections of IoT devices with improper User ID/password settings (mainly web cameras and Wi-Fi routers). According to the results of our survey, the section of the graph colored in blue (comprising over 50%) are all attacks targeting IoT devices. Note that these attacks are taking place not just abroad, but in Japan. The results of our monitoring and analysis have uncovered cases of malware infection of devices (Wi-Fi routers) marketed and distributed mainly in Japan. We provided this information to relevant organizations such as JPCET/CC.

Automatic Categorization of Infected IoT Devices

The devices from which the attacks originate, monitored on the darknet, are believed

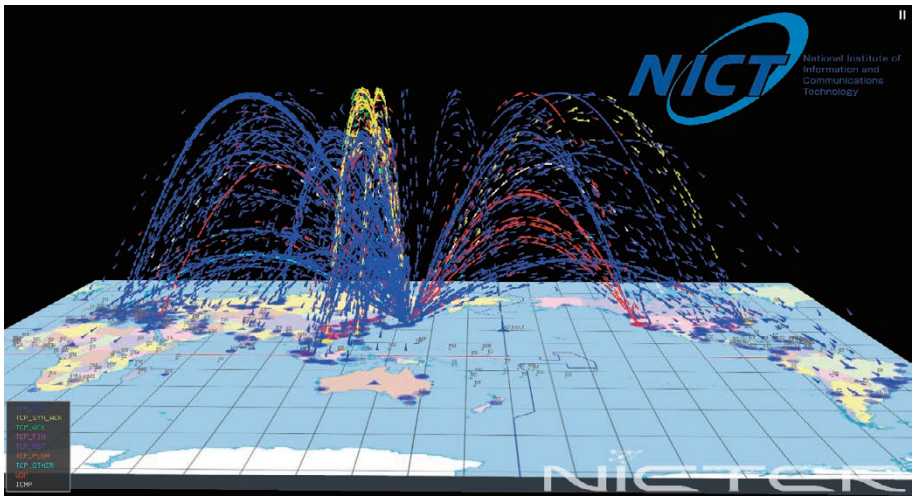


Figure 1 A schematic illustration showing how communications reach the NICTER darknet (visualization using Atlas)

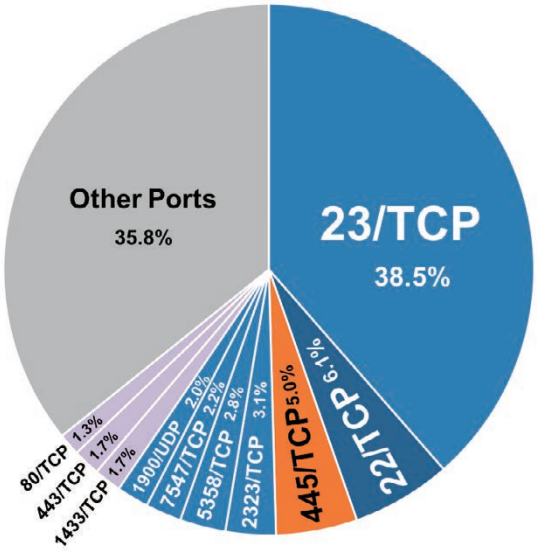


Figure 2 Breakdown of number of monitored packets according to port number (2017)

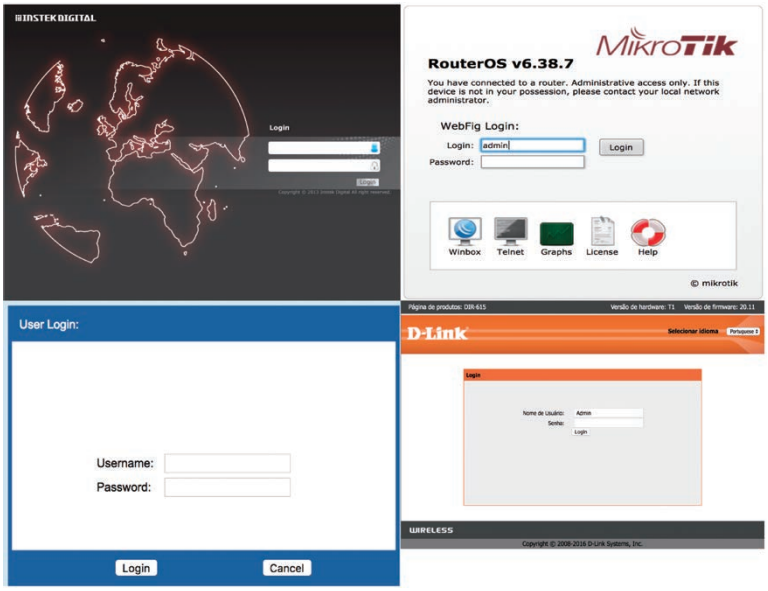


Figure 3 The login screen of the web interface for IoT device management

to be already infected by malware. It's difficult to determine whether a device is an IoT device based only on a scan packet obtained through monitoring. Thus, we're conducting research and development on technologies that will actively access the device from which an attack originated and perform automatic identification and categorization of the device, based on the response obtained. For example, when the device is accessed via the web, a login screen for the device, like the one shown in Figure 3, may appear. Because login screens differ from device to device, the information collected can be used to categorize each device from which an attack originated. Through these efforts, we're working to identify the devices that function as the source for large volumes of malware infections.

Categorization of IoT Malware

We're also pursuing research and development to obtain malware binaries and determine the infection method and intentions. In addition to notorious examples of malware such as Mirai and Bashlite, we're seeing a boom in IoT malware that mines cryptocurrency (mining malware). The intent is to make money by infecting IoT devices with mining malware and using them to mine for cryptocurrency. Because the volume of cryptocurrency that a single IoT device can mine per day is relatively modest, the adversaries attempt to hijack as many IoT devices spread out all over the world to maximize their profits. This means protecting your IoT devices from adversaries will help prevent their illegal mining activities.

If a system can be designed to identify the type of malware immediately upon detection—for example, as Mirai or mining malware—the subsequent malware analysis can be performed more efficiently. We're pursuing research and development to establish a method for categorizing malware type. The important thing is calculating the degree of similarity (how similar two things are) between one malware program and another. In our study, we've focused on the machine code that constitutes the malware program and developed a program that compares the machine code of two malware programs by examining the number of shared commands. The greater the number of shared commands, the greater the similarity. In practice, commands are first extracted from assembly codes obtained by decompiling the malware programs, then calculations are performed so that higher similarity scores are produced for two programs that have higher number of shared sequence of instructions based on the combination of N-grams. Figure 4 shows the results of actual degree-of-similarity calculations performed on 2,000 malware samples mapped on a two-dimensional plane. This figure shows, for example, a high probability that unknown samples (presented using red crosses) mapped near Bashlite are Bashlite. Through the automatic categorization of the malware programs by applying machine learning methods after determining the degree of similarity between each malware program, we can identify the type of malware to which the captured program belongs.

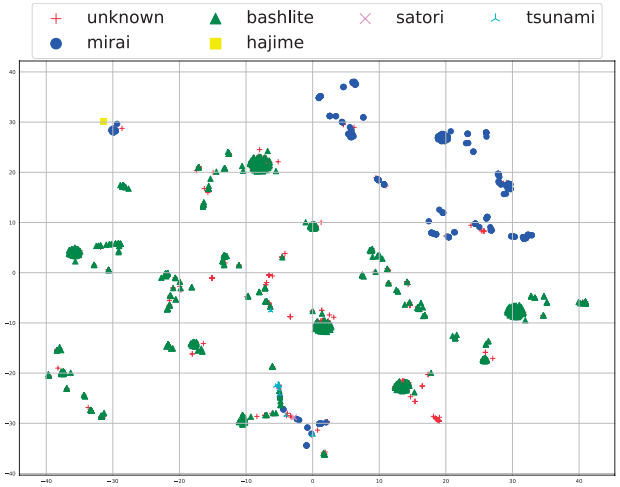


Figure 4 Result of malware categorization based on degree of similarity

Summary

While the number of Internet-connected devices will increase in the age of IoT, attacks on such IoT devices will also rise. We're even seeing attacks that target vulnerabilities specific to IoT devices. The attacks themselves are becoming more complex. We will continue to monitor and analyze the darknet, searching for new threats at the early stages to devise countermeasures based on the actual state of these threats.

NIRVANA KAI/NIRVANA KAI-II

For next-generation cybersecurity operations

Koei SUZUKI
Executive Technical Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

After working for a private company, he joined NICT in 2009. He has been engaged in research and development of NICTER, DAEDALUS, NIRVANA, and NIRVANA KAI-II.

Daisuke INOUE
Director of Cybersecurity Laboratory
Cybersecurity Research Institute

Developing countermeasures to cyberattacks has become a never-ending struggle against a daily tide of security alerts and vulnerability information. The Cybersecurity Laboratory is currently pursuing research and development on NIRVANA KAI, an integrated analysis platform intended to counter cyberattacks, and on NIRVANA KAI-II, a vulnerability management platform. Based on the goal of implementing efficient security strategies for networks within organizations, the Laboratory is also at work with the actual deployment of these platforms.

NIRVANA KAI

To combat cyberattacks, many organizations have installed and operate multiple cybersecurity products, including firewalls, intrusion detection systems, and endpoint security software. These security products generate a daily flood of security alerts. The burden of processing these alerts entails significant human resource costs.

As an integrated analysis platform designed to counter cyberattacks for efficient security operations based on centralized management and triage of security alerts, NIRVANA KAI can be described as a real-time graphical SIEM *[1] engine equipped with four functions: security alert aggregation and analysis; actuation; network traffic monitoring; and real-time visualization (Figure 1).

Security Alert Aggregator and Analytical Functions

The security alert information generated by security appliances and endpoint security software installed inside an organization is managed in a centralized manner using the security alert aggregator and analyzed via the NIRVANA KAI user interface. The operator categorizes the alert information and performs triage to prioritize incident response.

If a PC gives signs of a malware infection, the host information aggregator collects detailed information from inside the PC. This information is then used to swiftly identify the malware and confirm the communication status.

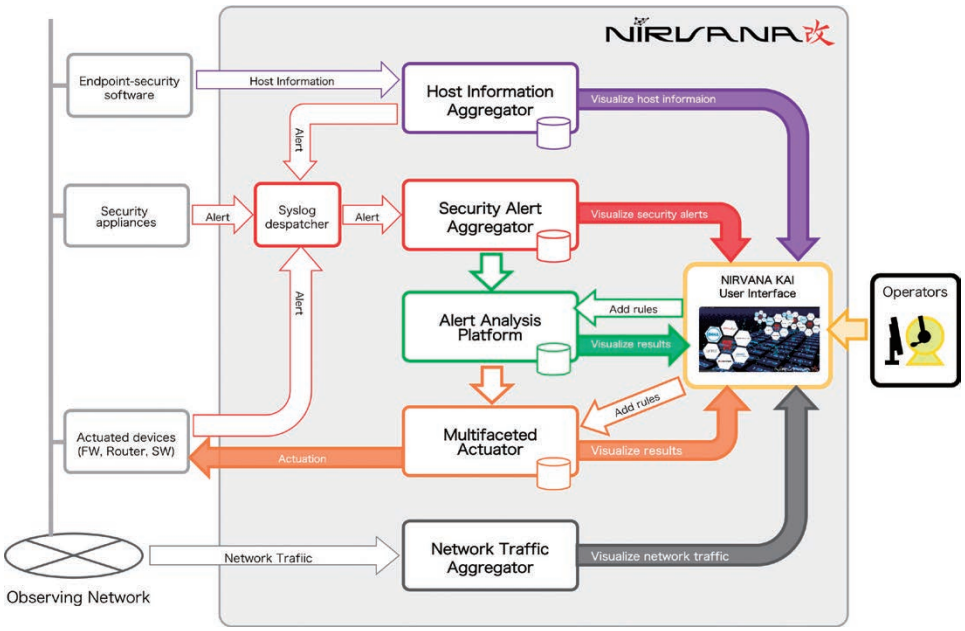


Figure 1 The NIRVANA KAI system architecture

Figure 2 Using the NIRVANA KAI auto-actuation function to block network access

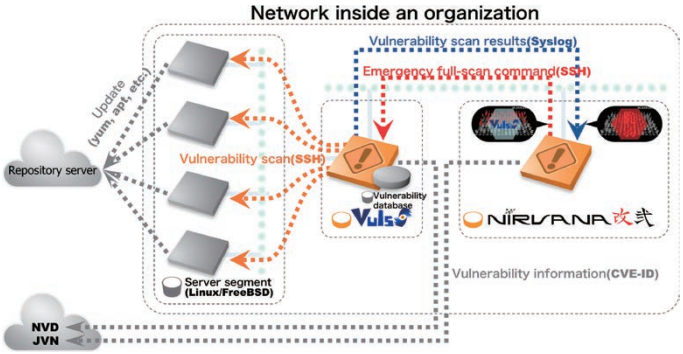


Figure 3 The NIRVANA KAI-II system architecture

The system also allows seamless associations with security alerts issued for networks, significantly reducing the time required to identify root causes.

Auto-Actuation Function

Based on analytical rules set by the operator, the alert analysis platform automatically extracts important incidents that must be handled as emergency events from alert information accumulated to the security alert aggregator database.

Within the actuator, security measures can be defined and automatically (or manually) executed for events detected by the alert analysis platform—for example, blocking communication. The actual command issued to the target actuating device can be user-defined to suit the specific device interface.

Traffic Monitoring Function

Using port mirroring or network TAP techniques, the traffic monitoring system aggregates traffic data from networks within an organization. The traffic data thus gathered is represented visually on the user interface in real time to help operators rapidly assess the current network status.

Real-Time Visualization Function

Using the real-time visualization feature of the NIRVANA KAI user interface, an operator can swiftly and efficiently perform a sequence of security operations ranging from analyzing the security alert, to triage, and finally to actuation of a response (Figure 2).

NIRVANA KAI-II

Eliminating vulnerabilities—flaws in the OS and/or software—is essential to preventing damage from cyberattacks. However, vulnerability management processes have conventionally relied on a manual approach that entails significant costs in terms of human resources and poses roadblocks to improving the security of the organization.

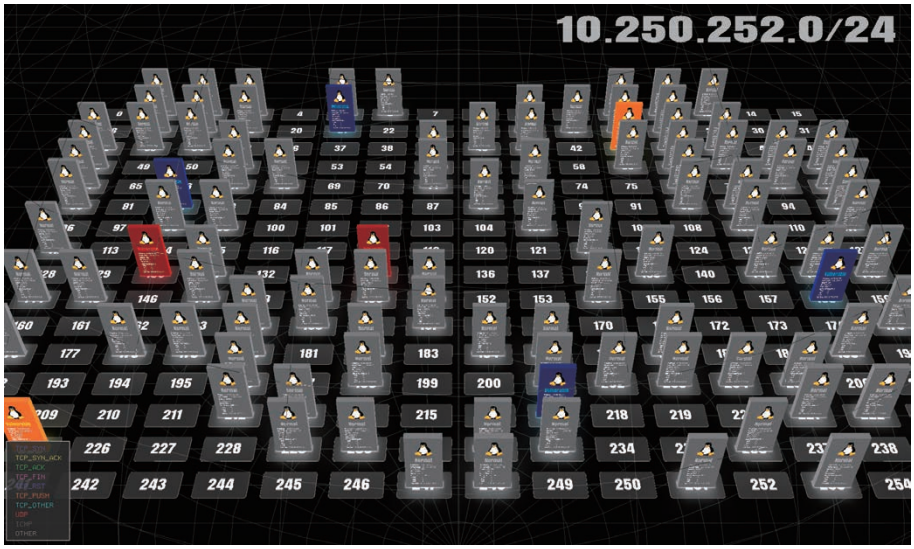


Figure 4 A wide-angle bird's-eye view of the vulnerability management status of server devices generated by NIRVANA KAI-II

NIRVANA KAI-II works in tandem with Vuls,*2 a domestically-developed vulnerability scanner, to create a vulnerability management platform that allows integrated management of vulnerabilities within the organization. Vuls, an agentless vulnerability scanner, performs vulnerability scans of each server by periodically accessing Linux/FreeBSD servers on the organization's internal networks. The results of the scans are visualized in real-time by NIRVANA KAI-II (Figure 3).

On the NIRVANA KAI-II user interface, an organization's internal network servers are represented as monolith icons whose colors change based on the severity of the vulnerabilities identified. This gives operators a bird's-eye view of the vulnerability management status of these devices (Figure 4). Whenever a vulnerability with potentially serious impact comes to light, NIRVANA KAI-II can be configured, using the auto-actuation function, to automatically issue a command that executes an emergency complete scan to identify server devices affected by a vulnerability.

If a vulnerability is discovered on an internal server, the operator can access vulnerability information available on external networks via NIRVANA KAI-II to retrieve detailed information on the vulnerability. Additionally, the servers can be updated based on security policies set by the organization to ensure swift and efficient vulnerability management, improving organizational security while reducing human resource costs.

Future Prospects

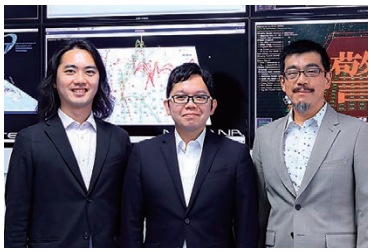
We've been promoting the transfer of technologies related to NIRVANA KAI to the private sector, with steady growth of implementation in Japan. In the future, drawing on feedback from the sites where actual security operations occur, we hope to continue advancing the NIRVANA KAI and NIRVANA KAI-II systems and to contribute to enhanced security for society.

*1 SIEM: Acronym for Security Information and Event Management, or technologies to achieve integrated storage and management of event information from security devices and software to assess events that pose security threats

*2 Vuls: An OSS vulnerability scanner developed in Japan by Future Corporation (Chairman and President, Group CEO: Mr. Yasufumi Kanemaru)

STARDUST: A Large-Scale Infrastructure for Luring Cyber Adversaries

Luring cyber adversaries and revealing their actual activities



From the left: Takashi TOMINE, Yu TSUDA, Nobuyuki KANAYA

Yu TSUDA
Senior Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

He was completed Ph.D. program without a Ph.D. degree, and then he joined NICT in 2013. He is interested in countermeasures against targeted attacks, information security operation, Capture the Flag (CTF). Ph.D. (Informatics).

Takashi TOMINE
Fixed Term Technical Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

He was completed Ph.D. program without a Ph.D. degree in 2012, and then he joined NICT in 2013. He is interested in network operation, internet, and countermeasures against targeted attacks.

Nobuyuki KANAYA
Senior Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

After master's degree, he works on a private company's research institution. He then joined NICT in 2013. He is interested in countermeasures against targeted attacks.

Although targeted attacks aimed at specific organizations have become a social issue, it is difficult to assess the status of targeted attacks based on monitoring by NICTER, which is designed to monitor for indiscriminate cyberattacks. For this reason, we have pursued research on a platform for luring cyber adversaries partaking in targeted attacks and stealthily monitoring their activities.

Difficulties in Research on Targeted Attack Countermeasures

Cyberattacks refer to activities that inflict damage via computer networks. The attacks of this kind that have severely serious social impact are targeted attacks. Targeted attacks are literally cyberattacks executed against specific organizations, such as companies and public offices. The adversary makes a reconnaissance of the characteristics of his target organization and seeks to penetrate intra-organization networks using various attack techniques tailored to these characteristics. The adversary then remains active for extended periods until his purpose (for example, stealing classified information) is fulfilled.

Japan has seen significant damage caused by targeted attacks. The incident made public in June 2015, in which 1,250,000 cases of personal data were leaked from the Japan Pension Service, was attributed to an attack campaign called Blue Termite. The targeted organization in this case was the Japan Pension Service. The malware known as Emdivi was involved in this attack. By attaching Emdivi to emails written in Japanese, the adversary gained entry into the organization and proceeded to undertake various malicious activities via a command and control server (C2 server).

An overview of these attacks can often be realized from information on mass media, social media, or the results of malware analysis published by security companies. However, in most cases, these sources of information fail to include detailed information on the actual activities involved in the attacks. What procedures and methodology did the adversary actually use to attack and infiltrate the targeted organization? What information is retained in network system logs? These traces left behind by the attack are vital for research and development on countermeasure technologies. Yet, this information is rarely released because they contain volumes of classified information of the victim organization.

STARDUST: A Large-Scale Infrastructure for Monitoring Adversaries' Activities

To overcome this problem and collect data associated with targeted attacks, we're pursuing research and development on a large-scale infrastructure for monitoring the activities of adversaries, called STARDUST (Figure 1). STARDUST automatically creates parallel-world networks that mimic in precise detail the ICT environment of an organization

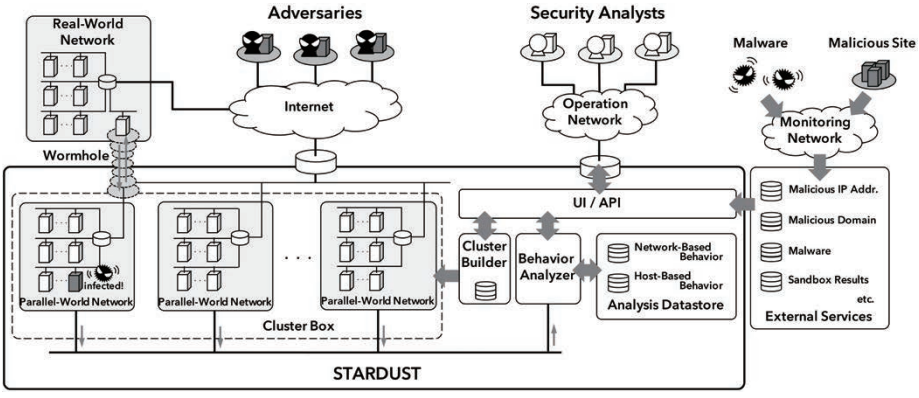


Figure 1 Architecture of STARDUST

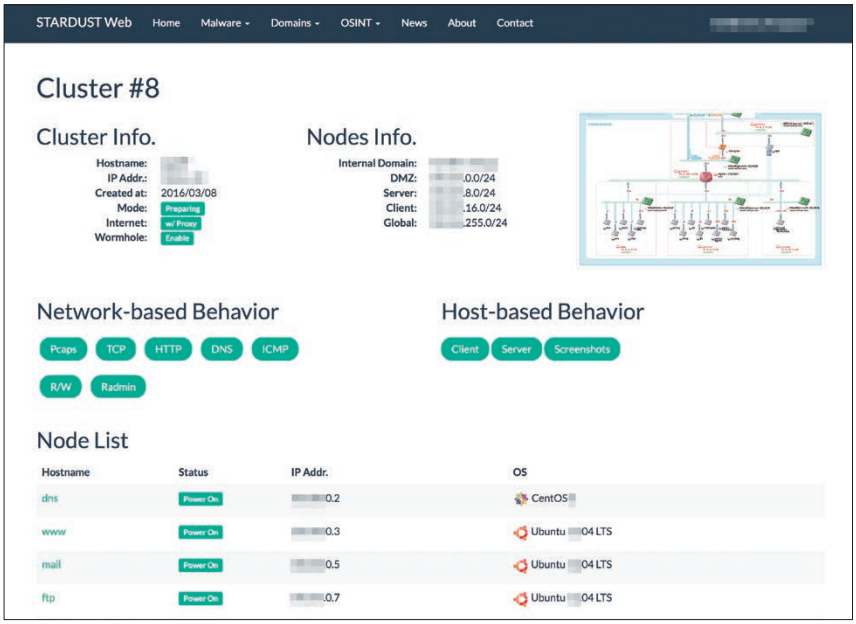


Figure 2 Web interface of STARDUST

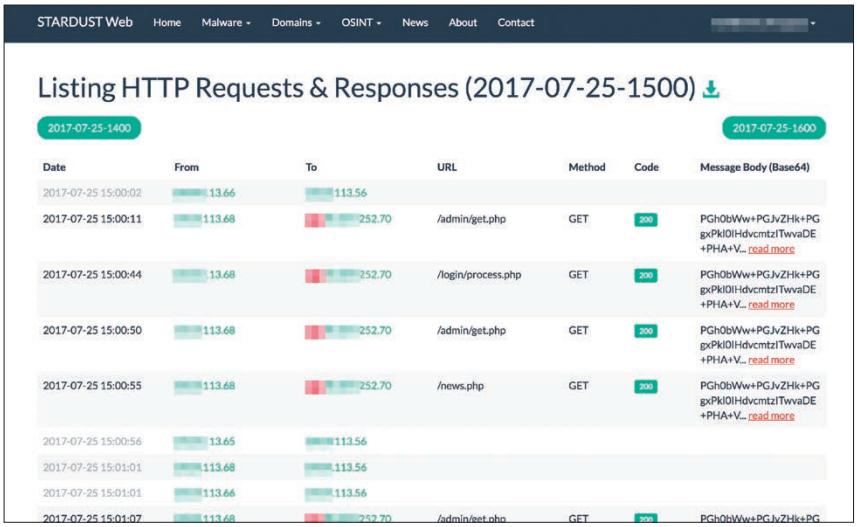


Figure 3 HTTP communication obtained using STARDUST, including the communication between C2 server and malware

```
1  net view
2  systeminfo
3  whoami
4  tasklist
5  dir c:¥users¥nito¥desktop¥
6  dir "c:¥program files¥"
7  dir d:¥
8  dir c:¥users¥nito¥
9  dir c:¥users¥nito¥documents¥
10 dir c:¥users¥nito¥downloads¥
11 dir "c:¥Program Files (x86)¥"
12 netstat -an
13 dir c:¥users¥nito¥documents¥Credential
14 ipconfig /all
15 whomai /groups | find /i "level"
16 whoami
17 whoami /groups
18 net group
19 net view
20 arp -a
21 netstat -ano
22 ping ***.***.8.4 -n 1 （プロキシサーバのIPアドレス）
23 tasklist
24 netstat -an
25 net view
26 tracert
27 net view ¥¥win05
```

Figure 4 An example of an attack

that acts as bait for an adversary. The malware used by a targeted attack is executed on a personal computer (PC) within the parallel-world network to establish an actual connection with the C2 server, thereby luring the adversary.

To persuade the adversary attracted in this way to stay as long as possible, STARDUST is equipped with a function for simulating various activities: creating documents, using email, adding bookmarks to web browsers, and setting user information. This function gives the adversary the impression that the parallel-world network is in actual use. Additionally, using a "wormhole," a connection is established with the C2 server via the real-world network of the organization targeted by the adversary. These actions convince the adversary that the attack was successful.

Traces left behind by an adversary while searching the PCs of the parallel-world network can be acquired through communications within the PC or over the network. High stealth methods have been adopted for STARDUST to ensure the adversary remains unaware that he is being watched. The acquired data can be referenced in real-time via the web interface (Figures 2 and 3). It's also possible to operate each PC based on the acquired data while monitoring is underway.

What We've Learned So Far on the Activities of Adversaries

At the NICT Cybersecurity Laboratory, we've used various types of malware associated with targeted attacks to lure in adversaries. Here in this report, we introduce an example of an activity revealed for an adversary group known as DragonOK (Figure 4).

This is a list of built-in OS commands actually executed by an adversary on a PC in a parallel-world network. These commands are used by the organization's network administrators and are rarely used by common workers. The results show the adversary used these commands to investigate the organization's network. Take a look at the command in line 15: The adversary has entered "whomai" and tried to execute it. But a command by that name isn't found in the OS. On the next line, he entered the correct commands, "whoami" and added an option, "whoami /group," then went on to execute them. The former was most likely a typographical error. This finding shows the activities were likely executed manually, not automatically.

By attracting adversaries in this manner, we were able to monitor and reveal the actual state of adversarial activities. By accumulating such data from actual adversaries, we can expect to obtain an understanding of targeted attacks for subsequent use in data in various applications.

Future Prospects

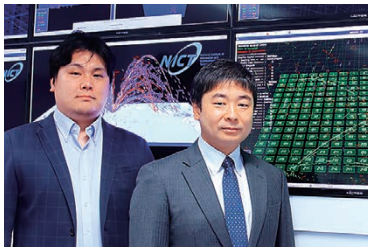
Ever since the launch of STARDUST to the public in May 2017, the number of users has gradually increased. STARDUST is now being used by numerous organizations including companies and universities. NICT has also been accumulating data by luring and analyzing actual targeted attacks of STARDUST. The accumulated data is not from a simulated attack; it represents invaluable data on real adversaries. We believe this data can be used to generate a scenario of a cyberattack for realistic tactical exercises. Moreover, we hope to create a dataset to promote future research and development.

WarpDrive: Web-Based Attack Response with Practical and Deployable Research Initiative

A user participation approach to build countermeasures to web-based attacks

Akira YAMADA
KDDI Research, Inc.

He received the M.E. degree in 2000. He joined KDDI Corporation in 2000 and had been engaged in the research on network security, intrusion/anomaly detection and DDoS attack defense in KDDI Research, Inc. He received the Ph.D. degree in computer science, in 2010.



From the left: Takahiro KASAMA, Daisuke INOUE

Takahiro KASAMA
Senior Researcher
Cybersecurity Laboratory
Cybersecurity Research Institute

Daisuke INOUE
Director of Cybersecurity Laboratory
Cybersecurity Research Institute

In light of the serious damage that can be inflicted by malware infections via web browsers, a major current issue is to assess the actual state of an infection and to devise appropriate countermeasures. The malicious web sites designed to launch such attacks typically also seek to often evade monitoring efforts, to hide their attack code, and discontinue their activities after very brief intervals. In response, we've pursued research and development on a framework for monitoring and designing countermeasures for web-based attacks based on a user participation approach. With this framework, monitoring is implemented by gathering web browsing histories from user terminals. To involve as many users as possible, we launched a demonstration experiment in collaboration with the Ghost in the Shell REALIZE PROJECT. These efforts have begun to generate an overview of such attacks.

Challenge in Monitoring Web-Based Attacks

Web browsers have become the mainstream attack route for cyberattack infections. Cyberattack monitoring typically is by the passive honeypot method and the active web crawler method. However, since actual web-based attacks occur at user terminals, monitoring the attacks themselves has been challenging. The sheer difficulty of an exhaustive search of web sites with embedded attack code has hindered efforts to assess the actual state of such attacks. Monitoring is often made even more difficult by the stratagems adopted by these sites, which seek to hide attack code when any web crawler used for cyberattack monitoring is identified.

Countermeasure to Web-Based Attacks Based on a User Participation Approach

Confronted by these challenges, we began to research and develop WarpDrive,*1 a countermeasure to web-based attacks based on a user participation approach. As its main feature, WarpDrive creates a monitoring environment based on participation from ordinary users. Figure 1 presents the architecture of the WarpDrive system, which consists of web browser sensors and data analysis platforms. Users taking part in monitoring efforts are asked to install a software called a web browser sensor at their terminals. The data analysis platform collects information through these sensors to assess the actual status of any attacks that occur at the user terminals. Based on this assessment,

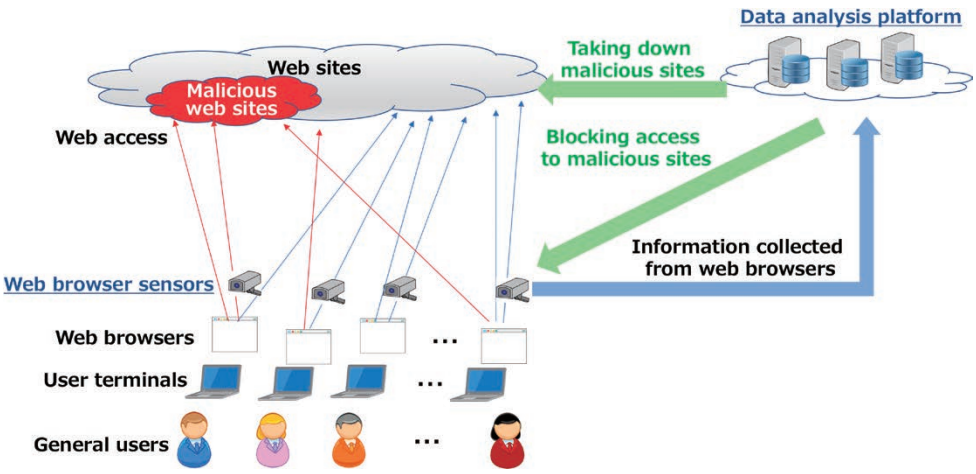


Figure 1 Countermeasures to web-based attacks based on a user participation approach

Figure 2 Visualization of web browsing history

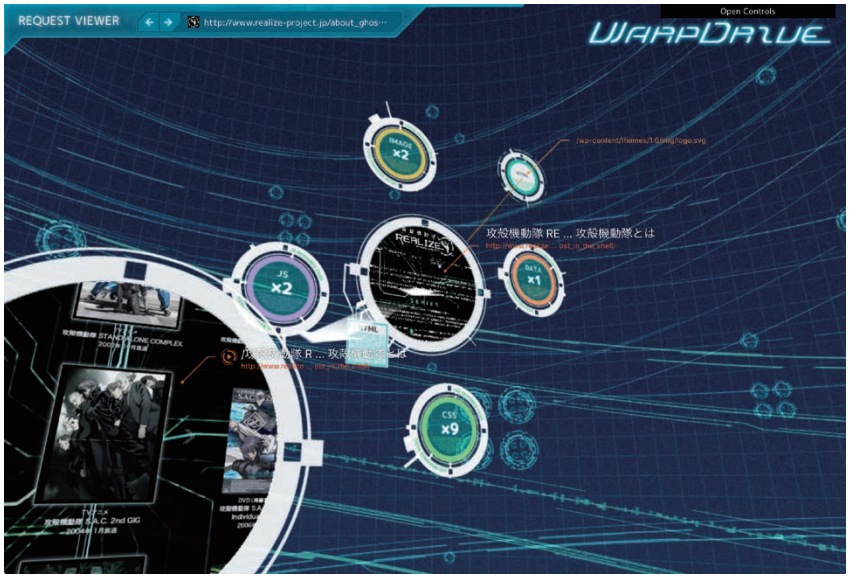


Figure 3 Visualization of web content

Table Continual changes in the URL address of a malicious site (Rig Exploit Kit) (August 7, 2018)

Malicious site URL	Start	End	Duration	Number of Times
http://aaa.aaa.213.226?MjczMDQ < omitted below >	01:33:27	05:40:53	4.1	7
http://bbb.bbb.124.190?NTM2NTE < omitted below >	07:56:01	14:20:56	6.4	10
http://ccc.ccc.213.216?MTc1NTg < omitted below >	16:43:38	20:34:27	3.8	8
http://ddd.ddd.120.59?NDY2MTg < omitted below >	20:54:58	22:47:59	1.9	5
…	…	…	…	…

WarpDrive either takes down the malicious site or blocks access to the site whenever a user attempts to access it. Involving more participants refines the overall picture of the attack and improves detection and protection performance.

Demonstration Experiment in Collaboration with Ghost in the Shell REALIZE PROJECT

To deploy this system, we worked with the Ghost in the Shell REALIZE PROJECT to launch a demonstration experimental phase. We developed a Tachikoma Security Agent ("Tachikoma SA" hereafter) based on the character Tachikoma from the *Ghost in the Shell* anime series. In the anime, Tachikoma is a sophisticated artificial intelligence (AI) robot that offers essential support to the main characters. The Tachikoma SA incorporates various security functions, including attack monitoring and protection, and allows users to work within a visualized web space that draws on *Ghost in the Shell* motifs (Figures 2 and 3).

The demonstration experiment was launched on June 1, 2018. Within the three months that followed, we registered over 5,000 users to the system, making it possible to collect some 1.5 billion site visits on a daily basis. Tachikoma SA has blocked access to malicious sites at an average rate of 11.7 cases per day. The system has collected detailed analysis for an average of 140.1 URL addresses per day it deems highly malicious. The project revealed that malicious web sites change their URL addresses within a short span of time (Table). This table shows how the URL address for an attack tool named Rig Exploit Kit changes.

Future Prospects for WarpDrive

The demonstration experiment currently underway for WarpDrive is gathering a stream of invaluable data. We plan to make further efforts on assessing the state of web-based attacks based on the collected data and to consider how user security may be improved based on the environment created by the experiment. We will also strive to develop practical applications for the knowledge and technologies gained through this R&D effort. The Tachikoma SA is available for downloading and installation from the portal site*2 while the experiment is underway. We invite all those interested to join us in our efforts.

*1 WarpDrive (Web-based Attack Response with Practical and Deployable Research InitiatiVE)

*2 https://warpdrive-project.jp

Launching a Demonstration Experiment on a Multi-Parameter Phased-Array Weather Radar —From an NICT Press Release—

A research group in which NICT is a member has developed the world's first, practical multi-parameter phased-array weather radar (MP-PAWR) as a part of the Cross-Ministerial Strategic Innovation Promotion Program (SIP): "Enhancement of Societal Resiliency against Natural Disasters" promoted by the Council for Science, Technology and Innovation, the Cabinet Office of Japan. The MP-PAWR is a new type of weather radar capable of both rapid, three-dimensional observations of rain clouds and accurate observations of rainfall. The radar can continuously observe at 30-second intervals within a 60 km radius of the radar station from near ground level to the skies above, allowing it to monitor rainfall caused by rapidly developing cumulonimbus. The observation data is assimilated into a weather forecasting model run by the National Research Institute for Earth Science and Disaster Resilience. Demonstration experiments have been underway since July 2018. Eventually, rainfall predictions within subsequent 30-minute windows will be provided to 2,000 monitors, including citizens and personnel in charge of disaster prevention at municipal governments.

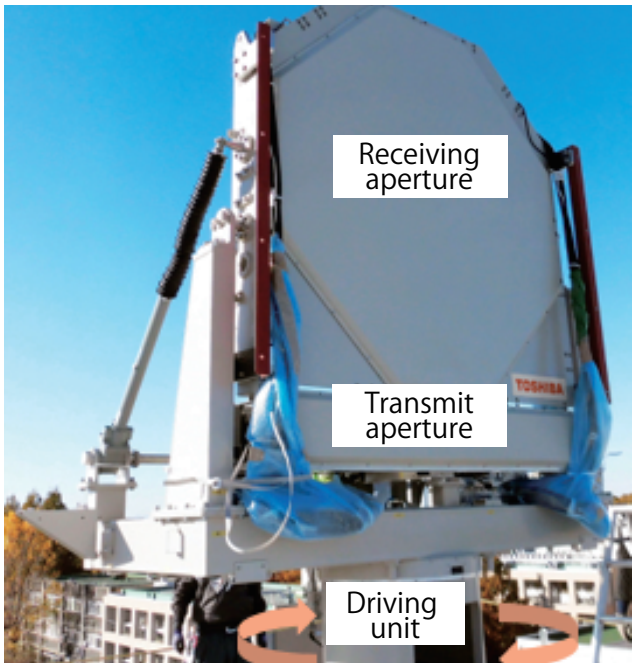


Figure 1 Antenna part of MP-PAWR (Rooftop of Bldg. No.3, Department of Civil and Environmental Engineering, Saitama University)

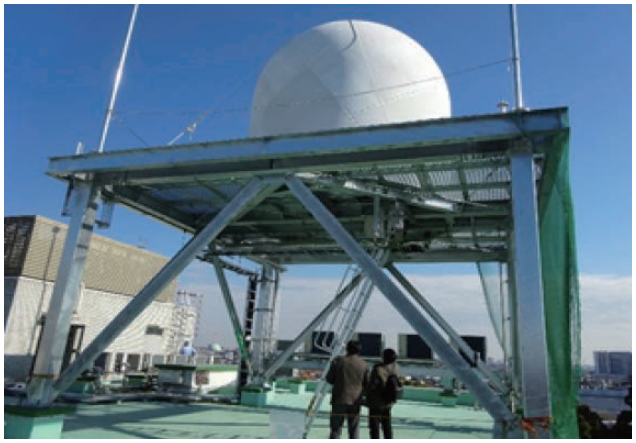


Figure 2 MP-PAWR installed in Saitama University

What is MP-PAWR?

The MP-PAWR is a phased-array weather radar, or PAWR, capable of rapid three-dimensional observations and equipped with a function that allows accurate observations (multi-parameter; MP) using horizontally and vertically polarized radio waves. Small raindrops are nearly spherical in shape; as they grow, the resistance from surrounding air during their fall causes them to flatten and to take on an ellipsoid shape (similar to a hamburger bun). This shape generates specific scattering and propagation characteristics when horizontally and vertically polarized radio waves pass through the flattened raindrops. The radar uses this difference to identify the type of rain—for example, whether the raindrops indicate a drizzle or are more characteristic of raindrops found in thunderstorms—allowing the system to accurately determine rainfall intensity distributions. The MP-PAWR system achieves rapid three-dimensional observations by combining wide-angle transmitter beams and narrow receiver beams using digital beamforming (DBF), allowing observations in multiple directions simultaneously. To make instantaneous observations of vertical rainfall profiles, the transmitter and receiver beams are electronically scanned at high-speed from the horizontal direction to the vertical direction. For azimuthal observations, the radar antenna is rotated mechanically (30 seconds per rotation).

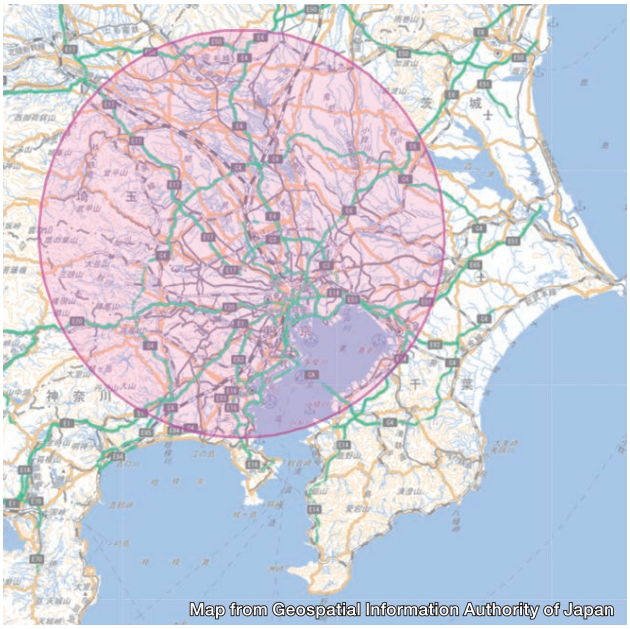


Figure 3 The observation range of MP-PAWR (60 km radius)
The radius of 60 km is overlain here on an electronic map from the Geospatial Information Authority of Japan.

Related press release

- **Demonstration experiment of world's first practical "Multi Parameter Phased Array Weather Radar (MP-PAWR)" started.**
  (released on July 19, 2018 http://www.nict.go.jp/press/2018/07/19-1.html)

Tackling Malware Analysis for Identifying Malware Infecting Web Cameras and other IoT Devices

Ryoichi ISAWA

Senior Researcher
Cybersecurity Laboratory, Cybersecurity Research Institute

Having a desire to realize a secure Internet society, I had already been researching on malware analysis before I entered NICT in 2012. Those days, malware programs particularly targeted Windows, and researchers in general focused on Windows malware. Partly because I was interested in machine language of programs, I focused on the machine code of malware programs, for example, to develop an automated system for identifying their malicious behavior, together with laboratory members of the graduate school. We also developed a system for categorizing malware programs, based on their code. Since around 2013, there's been gradual growth in malware infections affecting IoT devices like web cameras and home routers (simply "IoT malware" hereafter), and they have become threat in parallel with Windows malware. Reflecting these circumstances, I shifted my research theme from Windows malware to IoT malware and am currently involved in research for analyzing malware programs.

As I shifted my research theme from Windows malware to IoT malware, I noticed there are several differences between Windows and IoT devices, which I struggled with. For example, the CPU (central processing unit) of PC, which Windows runs on, is based on CPU architecture called Intel x86_64, and Windows malware programs are also composed of Intel x86_64 machine language. Meanwhile, in IoT devices, CPU with a variety of architectures such as ARM or MIPS is employed. Thus, machine languages for IoT malware are different, depending on the architecture of the CPU. So, I began with studying machine languages like ARM or MIPS and carried out R&D of categorization method of IoT malware programs based on machine language. This method helps to provide analytical support because resembling malware programs are detected in advance by categorizing the analysis target. Regarding this method, please refer to Section "Categorization of IoT Malware" on Page 5.

This categorization method currently cannot treat with malware programs running on different CPU architectures all together. I'm planning to find out a method to absorb the difference in machine languages and will tackle categorizing malware programs beyond the CPU architectures. By categorizing all IoT malware programs captured in advance, a global trend of malware programs will be more effectively identified. I will advance research on corresponding swiftly to the threat of IoT malware.

Q&As

Q: What are some of your current interests?
A: I've recently begun reading books on philosophy at home. I have the idea that thought processes related to resolving philosophical questions will help me in my own research.

Q: What would you want to be in your next life?
A: A cat. After getting over the sheer joy of having paw pads, I'd spend my time lolling about a window. In a little while I'd casually turn to look out the window, and if some birds were there, I'd begin cat chattering towards them as I would have a hunting instinct. I'll look forward to realizing how cats feel at the time they are chattering.

Q: What advice would you like to pass on to people aspiring to be researchers?
A: (This piece of advice is for people who have certain anxieties.) If you don't find writing research papers burdensome, you might just make it as a researcher.

Background

2004: Graduated from Department of Information Science and Intelligent Systems, Faculty of Engineering, Tokushima University
2006: Completed master's program at the Graduate School of Faculty of Engineering, Tokushima University; subsequently joined cybersecurity startup while concurrently enrolling in doctorate program at the Graduate School of Kobe University
2012: Completed doctorate at Graduate School of Kobe University, earning a Ph.D. in engineering; joined NICT the same year
2018: Current position as shown above

Awards

- Best Paper Award (The 13th Asia Joint Conference on Information Security)
- FIT 2011 Young Researcher Award

In this column "NICT's Challengers" you will find a profile of NICT staff tackling a variety of things.

NICT NEWS 2018 No.6 Vol. 472
Published by **Public Relations Department, National Institute of Information and Communications Technology**
Issue date: Nov. 2018 (bimonthly)

4-2-1 Nukui-Kitamachi, Koganei, Tokyo
184-8795, Japan
TEL: +81-42-327-5392 FAX: +81-42-327-7587

URL: http://www.nict.go.jp/
@NICT_Publicity
#NICT

Subscription applications accepted by
E-mail or on the Web site.
ISSN 2187-4050 (Online)