Enhancing Security Analysis at NTT I3

Shin Adachi
CISSP, CISM, CISA, PMP
Lead Security Analyst,
NTT Innovation Institute, Inc.

Abstract

NTT Innovation Institute, Inc. (NTT I3) has been analyzing security intelligence in collaboration with the NTT Computer Security Incident Response and Readiness Coordination Team, also known as NTT-CERT, and other CSIRTs, or Computer Security Incident Response Teams, and it aims to apply this know-how to the research and development of advanced security technologies. We asked Shin Adachi, the Lead Security Analyst at the center of security-related work at NTT I3, about the current status of information security and the benefits of establishing NTT I3 as a center for research and development in North America.

Keywords: security, CSIRT, security research

Introduction

A Computer Security Incident Response Team (CSIRT) works to prevent (if possible), detect, respond to, and mitigate security incidents, including cyber attacks on companies and organizations. In large corporations or in companies operating a critical infrastructure, it may be a dedicated organization consisting of a full-time staff or team whose members hold concurrent posts in the company. The NTT Computer Security Incident Response and Readiness Coordination Team, also known as NTT-CERT, was launched in 2004 within NTT R&D (research and development) of NTT Holding Company as the CSIRT representing the NTT Group. It supports the NTT Group in security-related matters, including the provision of up-to-date information, and acts as an NTT Group contact point for interacting with outside security organizations and collecting information.

NTT I3 has been supporting the monitoring functions of NTT-CERT since 2012 originally in the form of its predecessor, NTT Multimedia Communications Laboratories (NTT MCL). Specifically, it has been in charge of surveying security conditions especially outside Japan and of maintaining and boosting interaction with outside organizations (**Fig. 1**). Given that security and cloud computing are major areas of R&D at NTT I3, this work can be expected to take on an increasingly important role in the years to come.

Shin Adachi, the Lead Security Analyst at the center of this work, is well known for his activities in major security-industry organizations including the Forum of Incident Response and Security Teams (FIRST)—the global forum of CSIRT organizations—and is recognized internationally as a security expert. Last year, he was elected co-chair of the FIRST Education Committee, one of the oldest committees in FIRST, succeeding his predecessors from the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, which is known as the first

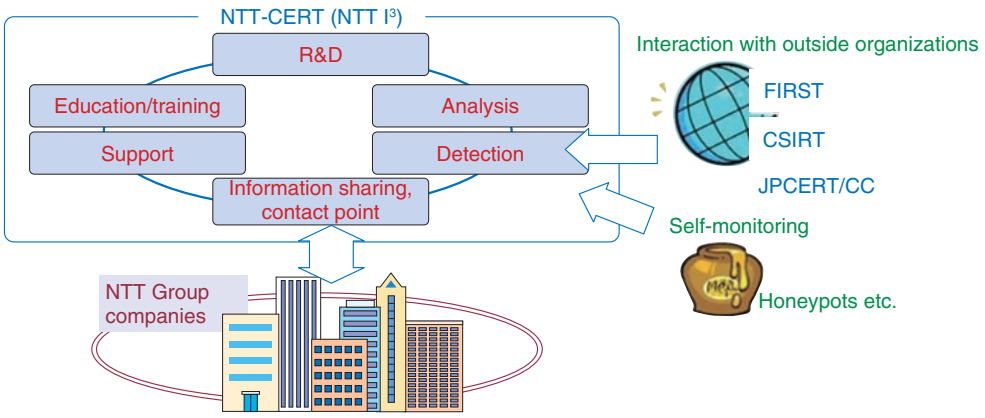


Fig. 1. Overview of NTT-CERT (NTT I^3) activities.

CSIRT. Mr. Adachi was elected as co-chair together with Franz Lantenhammer, head of Computer Emergency Response Team Bundeswehr (CERTBw) of the German Federal Armed Forces. He is the first Committee Chair elected from a company based in Asia.

The CSIRTs belonging to individual companies or organizations form human networks to create mutually trustworthy relationships, which are often reflected in daily activities such as obtaining reliable, up-to-date information from that network and working together to deal effectively with security incidents. Mr. Adachi has a large network of personal relationships and extensive experience in the security industry, and his NTT I^3 colleagues often refer to him as "our treasure" for this reason.

—Mr. Adachi, can you tell us about the present state of cyber attacks?

To begin with, let me say a few things about these incidents that we call "cyber attacks" considering that we don't usually know from whom or where, or how an attack will be mounted.

The first thing that probably comes to mind when hearing the words "cyber security" is attacks on personal computers (PCs). However, it was not so long ago that an attack was made on the Subway restaurant chain in the United States in which a vulnerability in their POS (point-of-sale) terminals was exploited. This attack caused considerable damage and was later found to have originated in Romania.

If we look at recent trends, survey reports and security-related literature tell us that there is a considerable time lag between the first occurrence of a malware attack and its detection, specifically, from 240 days to more than 365 days. Conditions such as these make it difficult to obtain an accurate number of malware incidents. The literature indicates that at least 200 days are now needed to detect that something has occurred. It can therefore be said that, at any point in time, we just don't know what is going on where.

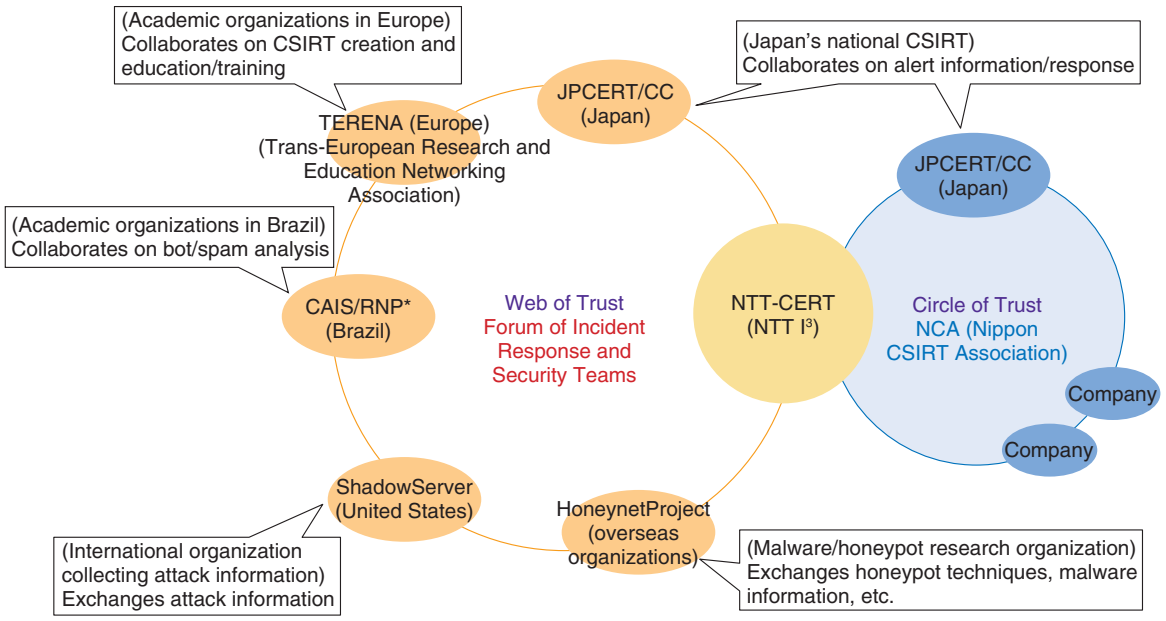
Japan is the home of many globally known corporations that have a high probability of being targeted by malware attacks, so it should be acknowledged that attacks are occurring here and there on a daily basis.

Reports from Microsoft and elsewhere state that the risk of PC malware in Japan is not that high compared to other countries, but I believe that it is only a matter of time before Japan too is affected by some global-wide incident.

Obviously, malware targets things of high value. There are numerous cases of financial crimes and fraudulent uses of information in North America, and case studies from South America reveal that the methods used in committing financial crimes can be quite skillful and varied. Each country, region, and business field features particular methods of deception.

It appears that attack techniques that originate in South America and elsewhere arrive in Japan about one or two years later. The good news here is that understanding and analyzing incidents that are occurring in other regions in the world should enable us to anticipate and prevent to some extent security incidents in Japan. Case studies can help us make advanced preparations and take appropriate actions.

—Given this state of affairs, what specific activities are you involved in?



*The full name is Centro de Atendimento a Incidentes de Segurança / Rede Nacional de Ensino e Pesquisa (in Portuguese)

Fig. 2. Collaboration between NTT-CERT (NTT I^3) and key CSIRTS inside/outside Japan.

I am involved in incident monitoring work in conjunction with NTT-CERT. The term "monitoring work" may convey the idea of real-time incident monitoring, but it also involves the important work of releasing new information on which companies have experienced vulnerabilities and when, and of updating previously released, beneficial security information.

I also act as a liaison to other organizations involved with information security.

In fact, in addition to issues involving attacks and vulnerabilities, my work spans the full breadth of the IT industry. I must consider, for example, judicial and legal matters, service providers, incident responders, universities, other CSIRTs, vendor information, and endorsements.

My job is to uncover important information from a complex web of data from which I need to determine what type of information lies hidden and where, and what kind of impact that information might have. So it's not just a matter of keeping myself glued to a screen 24 hours a day to collect information.

I also exchange information with organizations in other industries and with security activists in the same industry via teleconferencing as the need arises. In short, security work covers a wide range of activities—the day is over before I know it!

—You have participated in conferences and meetings throughout the world. What are your prime objectives here?

First of all, NTT became a member of the Forum of Incident Response and Security Teams, or FIRST, the global consortium of CSIRTs, in 2005, which was relatively early as a CSIRT in Japan (**Fig. 2**).

Being a member of FIRST helps NTT-CERT facilitate trustworthy interaction with other members and strengthen all sorts of relationships, human or otherwise. It also ties in with incident response. For example, there was a case in which we were able to track an actual incident by receiving exceptional cooperation from a CSIRT in another country. The feeling is that we can get our hands on important facts from reliable information sources in FIRST and reflect those facts in our response. There are also cases in which incident reports from FIRST sources are submitted prior to any problems occurring on our side. All in all, becoming a FIRST member promotes bidirectional problem solving.

I recently attended a number of conferences held in Brazil, Argentina, Malta, and other countries either for FIRST members or general participants (**Photo 1**).

I've also attended non-FIRST conferences on an

Photo 1. Participants at a FIRST meeting held in Thailand June 16–21 (Lead Security Analyst Shin Adachi is second from the left).

invitation basis, for example, those sponsored by the National Cyber Security Center of The Netherlands (NCSC.NL). These conferences and meetings help me to build up my knowledge and expand my network of contacts.

Of course, collecting information is an important task here, but raising one's profile and obtaining the trust of others is also an important activity. I also accept invitations to lecture to increase my exposure to the outside world. Speaking out in this way enables me to disseminate the strengths of NTT I^3 and NTT-CERT. Through these activities, I hope to increase the number of colleagues I have in this field and to decide on what direction I should take.

Just recently, for example, NTT I^3 applied for and received approval for membership in the Cloud Security Alliance (CSA), thereby joining ranks with well-known companies such as AT&T and Verizon.

I believe that the CSA is the only global industry body taking on both cloud computing and security. Its activities include drafting white papers, so I believe that offering our help in such work is a good way for others to learn about the highly talented staff, activities, and core competencies of NTT I^3. I also think that we can engage in effective PR through advertising and other activities targeting specialized fields.

Establishing a name will take several stages, but at first, our aim is just to increase recognition of the NTT I^3 name and to signal to the industry that our top priorities are cloud computing and security.

To spread the word about NTT I^3's capabilities, I think the best approach is to combine such efforts with other activities.

—There are security risks in all regions of the world, with researchers there to pursue them. Therefore, what are the benefits of working out of Silicon Valley?

One advantage of establishing an R&D center in North America is that the time difference with Japan can be put to good use. Specifically, in the case of California, our colleagues in Japan can send us messages and inquiries before they leave for the day, and since we are working while they are resting, we can reply to their messages by the early evening in our time. This means that they will receive our responses, results, or progress reports first thing in the morning the following day in Japan.

At the same time, working in just any location in the United States is not necessarily beneficial. For example, New York and Washington D.C., though being the respective centers of American finance and government and being located on the East Coast three hours ahead of California, are disadvantageous in the sense that software vendors tend to be located in California.

Let me explain using a specific example, which occurred some time ago. A new type of malware began to infect computer systems on a certain weekend, and as dawn broke around the world, the malware infections spread from New Zealand and Australia to Japan and Europe, and eventually infected computers on the East Coast of the United States. As a result, one financial institution after another fell victim to this malware and suffered damage. However, because major antivirus software vendors are concentrated on the West Coast, no effective countermeasure to stem the effects of that damage could be taken until the start of the business day on Monday in California. Such a situation would probably not occur today, but there are still various reasons why time differences can sometimes be a major problem. It can also be said that there are both good aspects and bad aspects to having a concentration of vendors in the California area, but understanding both sides also has its benefits.

At present, I make an effort to get up before 4:00 AM Pacific Time in California every morning to collect information on security matters affecting financial and government institutions, but looking forward, I would like to enhance and fortify the way we cover East Coast problems.

At the risk of repeating myself, I'll say that the present situation is such that I don't know what is going on security-wise at all points around the world.

But I do know that a new day begins with New Zealand and Australia—that will never change!

—What types of activities does NTT I³ intend to focus on going forward?

As a new direction from a business point of view, NTT I³ aims to support the datacenters and security services of three NTT companies doing business in North America, namely, Dimension Data, NTT America, and NTT DATA, Inc. Our mission is twofold: to protect the business operations of these companies and to determine which technologies are needed to protect their customers.

Furthermore, to expand NTT's cloud business, we must keep two questions in mind: how do we protect the security of the cloud business, and conversely, how do we leverage the power of the cloud to protect security?

The business of the NTT Group differs greatly between Japan and North America in the services provided to customers, the temperament and characteristics of customers, the business environment, and the regulatory environment. This difference has a big impact on security, the form of attacks referred to as the "attack vector," the way of dealing with vulnerabilities, and the incident response. I would like to apply the experience and achievements that we have built up so far as a CSIRT to develop intellectual property (IP) that can effectively support managed security services.

To this end, I am beginning to exchange information on a face-to-face basis while also investigating the specifics of how best to proceed from here on. I am currently at the stage of establishing a firm foundation, and the key to this process is conducting interviews and meetings with the relevant players.

I also think that there is a wealth of talented, hard-working people in NTT R&D who are a true asset to the company. In addition to being responsible and loyal professionals, their knowledge extends beyond their specialized technologies to a broad range of peripheral technologies, too. I believe it's the duty of NTT I³ to inform the outside world about the high level of R&D activities underway in the NTT laboratories.

If we remain silent about this, nothing will get off the ground. Other Japanese firms may be involved in similar activities, but I believe that NTT is at the forefront of security technologies. I would like the vast capabilities of NTT to become well known.

Interviewee profile

■ Career highlights

Shin Adachi brings experience and expertise on information security gained over many years to NTT I³, as the Lead Security Analyst. He currently represents and serves NTT-CERT in the Americas. In addition, he has spoken at, played significant roles at, and/or contributed to, well recognized organizations such as FIRST, NIST Cloud Computing Program, Liberty Alliance, Kantara Initiative, APEC TEL eSecurity, Asia PKI Consortium, and ITU-T. Currently, he is serving FIRST as CoChair of its Education Committee and as a senior member of its Program Committee.