Recognizing the Importance of Dissemination Skills after 10 Years of Combating Malware

Makoto Iwamura
Distinguished Researcher,
NTT Secure Platform Laboratories

Combating malware has become a global issue. The black market for malware, which threatens the integrity of even state secrets, is turning into a robust organization that presents an ongoing challenge to researchers. Since 2005, when the word *malware* came into common use, NTT Secure Platform Laboratories has been working around the clock to collect, analyze, and combat malware. We asked Dr. Makoto Iwamura, NTT Distinguished Researcher, to tell us about research achievements to date, future issues, and approaches to establishing an anti-malware system and training program for security personnel.

Keywords: cyber security, malware, honeypot

Wide-ranging need for cyber security, from personal information to state secrets

—Dr. Iwamura, please tell us about your research activities.

My work involves the collection and analysis of malware and the creation of mechanisms for solving malware-related problems. Malware is a portmanteau of the words *malicious* and *software* and refers to software with malicious intent. For example, when malware infects a computer, it may result in unintended operations or information leaks and can even disable the computer itself.

It has become commonplace to hear about damage caused by malware attacks, such as the leak of confidential documents from a personal computer or monetary loss from a transfer of funds to an unintended account during an Internet banking transaction. Today, however, malware is also coming to be known as a cyber weapon that can be used as a means of mounting a military-like attack on a foreign government.

In the past, malware was mainly used to mount attacks indiscriminately on an unspecified number of people. Recently, however, malware that mounts targeted attacks on specific individuals or organizations has come into existence. These types of attacks may infect a personal computer by attaching a document to email or by exploiting vulnerabilities in a web browser to direct the user to visit a specific URL (Uniform Resource Locator).

Malicious scanning that exhaustively attacks vulnerable computers in Internet space (by *knocking on doors* to find vulnerable areas of computers) and spreads an infection if successful was reported to

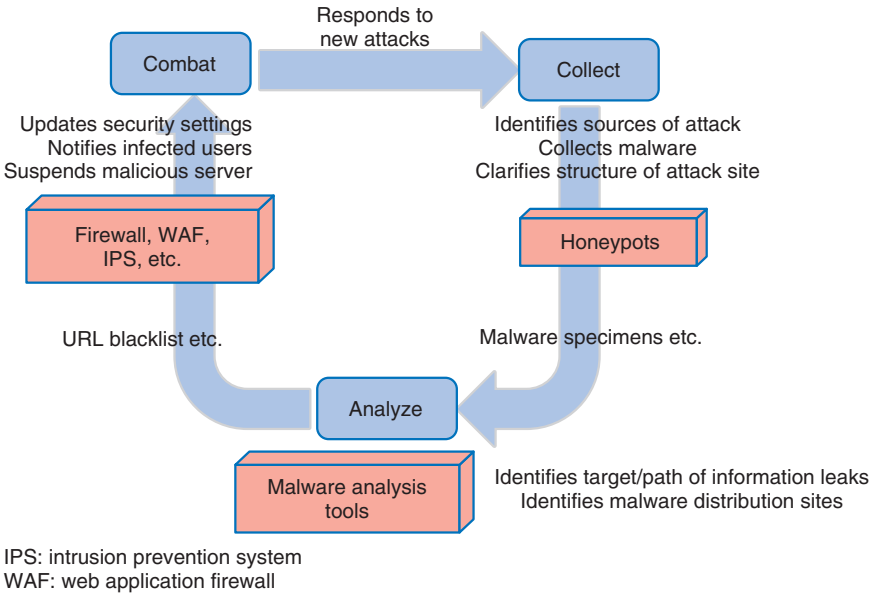

Fig. 1. Anti-malware approach using honeypots.

have occurred about 25.6 billion times in 2014.

These attacks have been mounted to obtain personal information, confidential corporate information, and state secrets, and when such information is obtained, it has consequently been traded on the black market, resulting in undeserved profits for perpetrators. We researchers combat cyber attacks day and night to prevent such damage from becoming a daily occurrence, but the truth is that there are more than a few countries and companies that have been the victim of malware.

—What specifically does your work entail?

Well, to begin with, we create decoy computer systems called *honeypots* to collect malware (**Fig. 1**). Honeypots are placed at a variety of locations to make malware collection more efficient such as on a customer's network or in Internet space where vulnerable software or browsers are present. Honeypots can be broadly divided into four types: high-interaction honeypots and low-interaction honeypots based on the level of interaction, and server honeypots and client honeypots based on the path of infection. I am particularly involved with two high-interaction honeypots called DenDenHoney and Marionette that have high camouflaging ability.

DenDenHoney uses technology for identifying and safely collecting the sources of attacks by accurately detecting attacks that exploit vulnerabilities in Windows OSs (operating systems) (**Fig. 2**). It can also collect the malware itself in a restricted environment called a *sandbox*.

Marionette, on the other hand, is technology for detecting malware via the web and for discovering malicious websites. Using a web browser with vulnerabilities, Marionette crawls through Internet space actively collecting information on malicious websites and capturing malware itself.

Next, in terms of malware analysis, there are two types of analysis techniques: dynamic analysis that actually executes the collected malware and analyzes its behavior, and static analysis that analyzes only the program code of malware without running it. The former monitors malware behavior in detail and clarifies its communication patterns and functions. The latter, meanwhile, disassembles program code to obtain an overall view of the malware including latent functions that operate only under certain conditions. The above malware analysis is conducted manually and consequently requires considerable labor, but it can be made more efficient by identifying similarities with past malware and concentrating on those elements that are different.

Through my involvement in developing cyber security measures over a period of about ten years, I have found that attackers are continuously thinking up and implementing new attack techniques reflecting a very

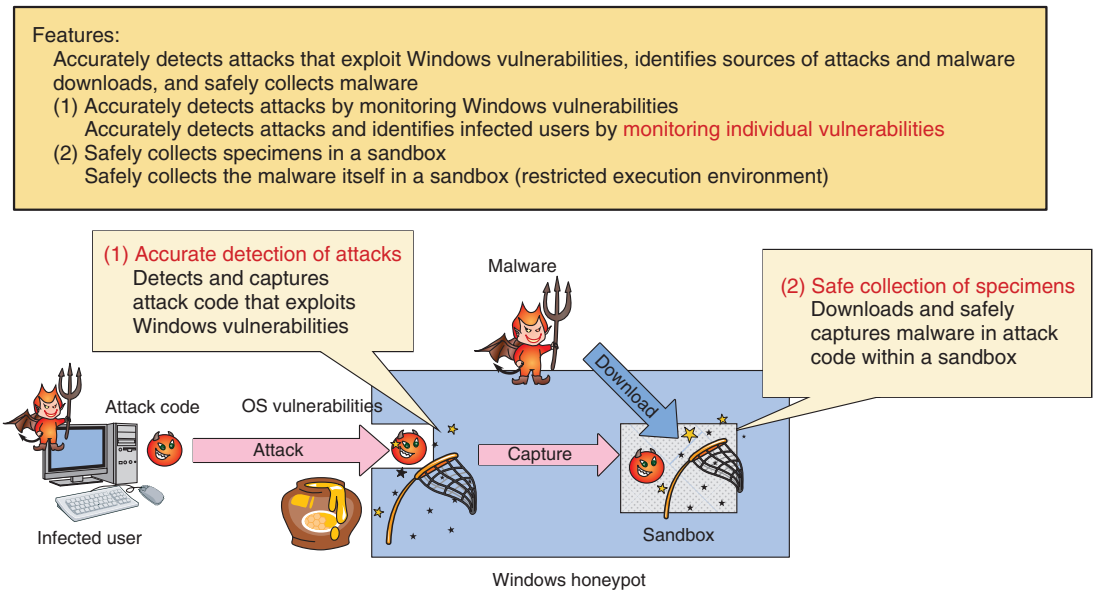

Fig. 2. Malware attack detection approach of DenDenHoney.

high level of creativity.

In contrast, the side that provides security has been taking a more passive stance in which it tries to determine how best to respond to a customer that has been infected by malware. With this approach, however, I cannot help but feel that we are simply chasing after malware endlessly, so I would like to promote research and development on techniques for anticipating and preempting malware.

Just like magic! Continuing the never-ending battle against cyber attacks after hearing the words of a fellow student

—In your ten years of combating highly creative attackers on a daily basis, have there been any momentous events?

We started our work on DenDenHoney in 2005, around the time when malware was turning into a social problem. Since then, publicly available honeypots in open source or other formats have existed, but most of them have been easily recognizable to attackers. As a result, they are not useful for malware collection, and we therefore took it upon ourselves to develop our own honeypots.

The inspiration for this idea came early, but it took us more than a year to implement the idea. The mechanism itself for collection was very simple, but there were very high technical hurdles that we had to overcome to implement it, and the entire team had to improve its skills in this field. However, once malware issued by attackers began to flow into our honeypot, indicating that our collection mechanism was working, we responded joyously by exclaiming "We've done it!"

If malware is analyzed in a haphazard manner, such analysis can become noticeable to attackers. To prevent this from happening, our team created virtual software specialized for malware called Stealth Debugger, which was another momentous experience for me. This software is currently becoming a base technology for a mechanism that can quickly identify malware that causes information leaks.

—Why did you choose the life of a researcher?

When I was in elementary school, I loved inventions. At that time, there was no such thing as a *staple-free* stapler, so I wanted to create one, and I devoted myself to that task. Additionally, because my family home had a bicycle shop, I also developed an interest in mechanical things. If I weren't doing what I'm doing now, I would probably be a watchmaker. Later, however, on encountering computers, I felt that "You can do anything with a computer!" and I became seriously committed to computing. Then, during my university studies, I heard a senior of mine say "You

can wrest control from a server by causing its buffer to overflow." At that time, I had no idea what that meant—I could not understand how a commonplace event like a buffer overflow could be used to rob control from a server. It seemed like magic to me!

In an attempt to understand the mechanism behind this, I turned my attention to operating systems, compilers, and machine language and became captivated by discovering countermeasures to security holes. Needless to say, buffer-overflow attacks still exist, and countermeasures to them are in force, but attackers continue to come up with ever-ingenious attacks of this type. Technically speaking, I believe there are still elements of these attacks that we have to investigate further.

The need for dissemination skills in an unexplored field

—What kind of stance must the security-provision side take from here on?

I believe that the side that provides cyber security must be knowledgeable about social trends, that is, about the likes and preferences of people, and it must also strive to build relationships based on trust. In this regard, dissemination skills are essential. By this, I mean one must be able to communicate information to a wide audience. Now, after ten years, I feel strongly that the cyber security business cannot fully function if the people involved simply focus on their own research.

Although the need for a system of mutual information-sharing is recognized, it will be difficult for the security-provision side to become united if some of us are hesitant about admitting a breach into one's system and revealing a flaw in one's security measures. However, if we do not change this mindset and we refuse to cooperate, we will not be able to stand up to the cyber-attacking side. It is said that "Information accumulates around people that disseminate information," and I would like to expand cooperation by disseminating information myself.

For my part, to help expand the security network both inside and outside the NTT laboratories, I am involved in bringing together talented researchers and security engineers on the security-provision side while also helping to train the next generation of security engineers. I also actively participate in outside activities such as speaking at national security camps held by the Information-Technology Promotion Agency (IPA), supervising security contests, and giving lectures at universities (**Photo 1**).

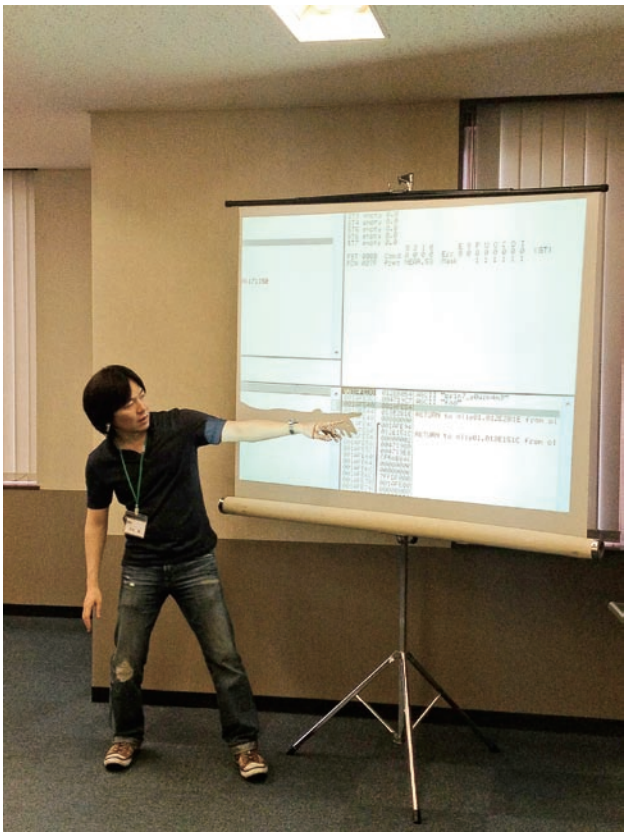

Photo 1. Delivering a lecture at a national security camp.

Additionally, I recently participated in a DEF CON CTF (Capture the Flag) contest, in which participating teams use their cyber security-related skills, that is, hacking skills, to compete against each other. In this contest, I competed shoulder-to-shoulder with young engineers I had mentored at security camps. My aim here was to grow as an engineer above and beyond what I could accomplish by simply disseminating information. For a full two days and two nights, these young engineers were faced with very challenging problems, and I found them clinging to their computers even while I was taking a break. In my daily work, I am usually involved in several tasks and have few opportunities to devote all my energy to one endeavor, so seeing the way they approached these problems reminded me of the importance of facing a technical problem head-on until a solution is reached.

In my free time, I enjoy playing popular computer games and watching hit movies, but I've come to realize that what I'm really interested in is keeping up

with social trends. In other words, I have been unconsciously following what people like and dislike in the real world as opposed to the closed world of the cyber security industry.

—I assume that a wide range of measures are required for solving unprecedented problems such as cyber attacks.

Today, we may be entering a period in which people that create programs will be required to have essential skills and be responsible for creating safe and secure programs. There may be a need for establishing certifiable qualifications in much the same way as a medical license. This is not simply a matter of teaching an engineer the technical skills needed for analyzing malware. It is also important to develop programmers who have a good understanding of security while simultaneously educating managers who have decision-making power in implementing countermeasures to cyber security-related problems.

Furthermore, through my daily work and on-site activities in training security personnel, I strongly feel that we have a shortage of qualified personnel. A genuine problem today is that companies that have suffered damage from malware, while recognizing the importance of security engineers, nevertheless tend to respond to the occurrence of problems with stopgap measures. The placement of qualified personnel and the development of personnel with a forward-looking mindset tend to receive low priority.

It is said that personal happiness comes about through engagement, relationships, meaning, and achievement. For me, I can say that I am truly happy when I am completely engaged in creating something or in collecting or analyzing malware. Many of the young engineers I encounter at DEF CON and security camps feel joy in much the same way.

To counter the creativity of attackers, we must be able to make best use of this special character in young researchers who excel in combating cyber attacks. This, I believe, is the responsibility of those of us in corporate organizations whose job is to nurture people with talent.

Young researchers such as these find value in devoting themselves to research without focusing on its meaning or significance. For those of us who supervise such talent, we should perhaps set up environments for them in which they can discover at least some minor goals to aim for. Looking 10 or 20 years into the future, I myself plan to devote more energy to developing personnel for an active career in the cyber security industry and setting up venues for security-related activities.

First and foremost, I would like to be actively involved in disseminating information to gain the trust of people so that they too will share information. In addition, I hope to increase the number of my colleagues on the security-provision side both inside and outside NTT and collaborate with them in developing countermeasures to cyber attacks.

■ **Interviewee profile**
Makoto Iwamura
Distinguished Researcher, Senior Research Engineer, Cyber Security Project, NTT Secure Platform Laboratories.

Dr. Makoto Iwamura received his B.E., M.E., and D.Eng. in science and engineering from Waseda University, Tokyo, in 2000, 2002, and 2012, respectively. He joined NTT in 2002. He is currently with NTT Secure Platform Laboratories, where he is engaged in the Cyber Security Project. His research interests include reverse engineering, vulnerability discovery, and malware analysis.