Collecting, Analyzing, and Leveraging Threat Intelligence at NTT-CERT

Shunichi Konno

Abstract

The use of threat intelligence is progressing in corporate-based security frameworks typified by computer security incident response teams (CSIRTs) in order to defend networks and systems against increasingly sophisticated cyberattacks. It is becoming necessary to obtain a deeper understanding of threat intelligence and to deal with more advanced forms of such information. This article presents an analysis of attacker motivation using threat intelligence. The usefulness of threat intelligence in actual on-site CSIRT activities is also explained.

Keywords: NTT-CERT, CSIRT, threat intelligence

1. Introduction to NTT-CERT

The NTT Computer Security Incident Response and Readiness Coordination Team (NTT-CERT) is involved in various activities associated with computer security incidents within the NTT Group as a computer security incident response team (CSIRT) in the NTT laboratories [1]. These activities include response, analysis, education and monitoring, and research and development (R&D) and were initiated on October 1, 2004, within NTT Information Sharing Platform Laboratories, the predecessor to NTT Secure Platform Laboratories. NTT-CERT is a member of the Forum of Incident Response and Security Teams (FIRST)* and a founding member of the Nippon CSIRT Association. It is involved in a variety of initiatives in conjunction with CSIRTs and security teams inside and outside NTT. The parent organization of NTT-CERT was moved to NTT Secure Platform Laboratories on April 1, 2012.

NTT-CERT has the following functions in its diverse activities in the NTT laboratories:

(1) Acts as an R&D organization for disseminating know-how and tools to NTT Group companies and customers based on its history of setting up and operating an advanced CSIRT in the NTT Group
(2) As the representative CSIRT in the NTT Group, serves as a point of contact for outside CSIRTs who wish to access the NTT Group
(3) Extracts needs from the field, feeds them back to the NTT laboratories, and conducts trial applications of research deliverables

With the huge scale of the NTT Group, NTT-CERT on its own is unable to provide technical support for all of the diverse incidents that occur within the group. There are presently more than ten CSIRTs within the NTT Group companies, all of which work in collaboration to prevent incidents and to minimize any incident-related damage.

2. Threat intelligence and CSIRT

Various types of information can be called *threat intelligence*. Simple examples are the source IP (Internet protocol) address of an attack observed in the past, characteristic character strings in transmissions at the time of an attack, and the targets of

* FIRST: An international confederation of CSIRTs and security teams founded by 11 organizations in 1990 as a framework spanning organizations, countries, and regions.

transmissions from a host infected with malware. There is also threat intelligence that compiles a series of attacks as a cyberattack campaign or that draws a correlation between an attack and a political event such as an election. In any case, threat intelligence constitutes knowledge extracted and processed in a variety of stages from basic data such as a network log in order to determine whether a threat is being posed to the recipient. For this reason, NTT-CERT devotes its efforts to analyzing and integrating a wide array of threat intelligence.

The main roles of a CSIRT are to provide security quality management services, proactive services, and reactive services [2]. In quality management, a CSIRT is involved in such activities as risk analysis, security consulting, and education, but the use of threat intelligence can improve the quality of quality management activities themselves. For example, analyzing the risk to one's company's security based on threat intelligence that has been obtained and reporting the analysis results to corporate management can produce a steering effect from the management layer. Here, to prevent this risk analysis from becoming just a *pie in the sky*, or an illusion, it is important that threat intelligence obtained from multiple routes be compared with examples of past incidents and with homemade threat intelligence obtained from Internet sensors and other sources to improve its reliability.

Threat intelligence used in quality management activities can also be useful in proactive services before the occurrence of incidents. For example, in addition to using it in filtering to prevent incidents from happening in the first place, threat intelligence can be used as input in efforts to hunt for undetected attacks in large volumes of log data.

3. Examples of using threat intelligence in reactive services: cyberattacks and motivation

Threat intelligence can also be quite useful in CSIRT reactive services if an incident should actually occur since it can facilitate a response to a sophisticated cyberattack and make incident response more efficient.

Cyberattacks are motivated for various reasons. Paolo Passeri, a Solutions Architect at Netskope, investigated the motivations for cyberattacks that occurred worldwide in 2016 as a percentage of incidents using the results of cyberattack analysis released by HACKMAGEDDON [3]. The results are given in **Fig. 1**.

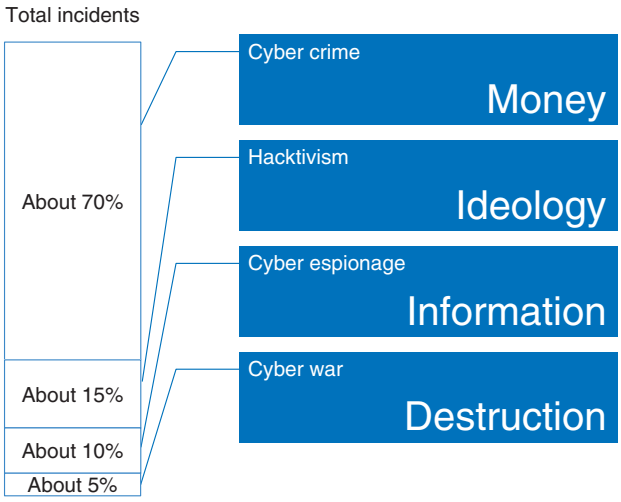

Fig. 1. Motivation behind cyberattacks.

(1) Cyber crime

The highest number of incidents falls within the category of cyber crime, at about 70% of all incidents. In general, these are attacks motivated by money. Ransomware such as WannaCry and NotPetya, which caused major issues in 2017, achieves the attacker's purpose by using encryption to make it difficult to read the content of the infected computer and intimidating the owner to pay a ransom to free up the data. In addition to ransomware, there are examples where money is demanded in the form of blackmail denial-of-service (DoS) attacks directed at Internet businesses whose continuous operation constitutes a lifeline. For example, an Internet-based foreign-exchange operator would be unable to profit from commissions if its website services came to a halt as a result of a DoS attack. Such an outcome would be a major blow to business.

(2) Hacktivism

The second type of motivation is hacktivism, accounting for about 15% of all incidents. This type of attack is carried out to proclaim the attacker's ideology. It may take the form of defacement of a website to display messages from the attacker or obstruction of the cyberspace activities of an organization at odds with the attacker's way of thinking. In Japan, well-known attacks of this type are associated with memorial days such as the *9/18 attack* that is mounted around September 18 every year recalling the Manchurian Incident of 1931. In addition, elements within the worldwide hacktivist group Anonymous have halted the website services of certain aquariums

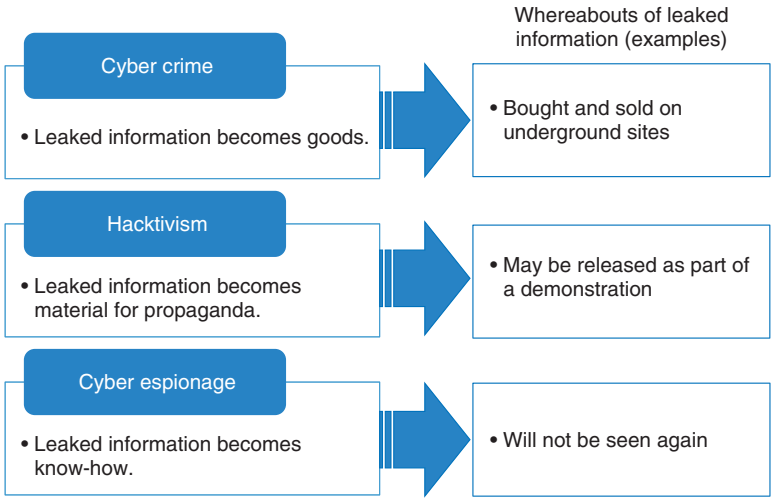

Fig. 2. Whereabouts of leaked information.

by mounting a series of attacks as an operation called OpKillingBay, leveraging the strong opposition to dolphin hunting in Japan.

(3) Cyber espionage

The third type of motivation is cyber espionage, accounting for about 10% of all incidents. As the word *espionage* implies, this type of attack attempts to surreptitiously steal information. While the number of incidents of this type of attack is only one-seventh that of cyber crime, such attacks may involve the stealing of design information on developed products or equipment, so they cannot be disparaged simply because of the low number of incidents. One feature of this type of attack is that the victim may be completely unaware of the attack.

(4) Cyber war

The fourth type of motivation is cyber war, accounting for about 5% of all incidents. The purpose of such an attack is destruction of critical infrastructures. Such an attack, if mounted, could have a major impact on society.

In the above way, collecting examples of past attacks is advancing the analysis of attackers throughout the world, and accumulating information on TTP (tactics, techniques, and procedures), on attacker tools, and on evidence of attacks is proving useful for responding to incidents within a CSIRT.

4. Attacker motivation and CSIRT activities

Attacker analysis can also be important in cases where a CSIRT conducts a survey to determine how an organization's roster leaked to the outside may be used for malicious means. Even for incidents in which the same kind of information has been leaked, for example, a roster from company A and a roster from company B, the whereabouts of that leaked information may be completely different depending on the attacker's motivation (**Fig. 2**).

For an incident suspected of being a cyber crime, the leaked information may come to be bought and sold on underground sites on a darknet. In such cases, a CSIRT will conduct an investigation of underground spaces.

For an incident motivated by hacktivism, there should be concern that the leaked information could be leaked to the world as propaganda in support of the attacker's ideology.

Meanwhile, for an incident motivated by cyber espionage, a survey conducted by a CSIRT will often come to a dead end. For an attacker involved in cyber espionage, the stolen information is the embodiment of desperately needed know-how and constitutes secret information for which there is no desire to pass it on to another party.

It can be seen from the above that the approach taken in an investigation of leaked information will differ depending on the motivation of the attacker, which can often be inferred based on tools used in an attack or evidence left on a damaged terminal.

In this way, NTT-CERT collects and analyzes threat intelligence from a variety of information sources to enable more advanced responses to attacks and more efficient surveys.

References

[1] Website of NTT-CERT, https://www.ntt-cert.org/index-en.html
[2] Software Engineering Institute, “CSIRT Services,” 2002. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=53046
[3] HACKMAGEDDON, http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/

Shunichi Konno
Threat Intelligence Team Leader of NTT-CERT, and Senior Research Engineer, NTT Secure Platform Laboratories.
He received a Master of information science and technology from the University of Tokyo in 2003 and joined NTT the same year, where he studied operating system security, CSIRT operation, and virtualization. He is one of the founding members of NTT-CERT, which offers CSIRT services to the entire NTT Group throughout the world.