NTT Com Security

Tetsuo Someya, Chief Business Development Officer and Chief Governance Officer

Abstract

NTT Com Security, the successor to security specialists Integralis (Germany) and Secode (Sweden), launched its comprehensive risk management service called WideAngle in June 2013. This article introduces the work of NTT Com Security while describing the information security environment surrounding today's corporations.

1. Introduction

NTT Com Security provides information security services. Its main office is located in Germany, and the company is listed on the German stock exchange. Its parent companies are Integralis, a German company founded in 1988, and Secode, a Swedish company founded in 1986, both of which were acquired by NTT Communications—the former in 2009 and the latter in 2010. The two companies merged in 2011 and changed their name to NTT Com Security in October 2013. NTT Com Security has just started afresh as a company at the core of the security services business in the NTT Communications Group (**Fig. 1**).

NTT Com Security has been a leading company in the security field for over 25 years since its initial founding. It has been expanding its business with a focus on Europe and the United States and is now developing its business in the Asia Pacific region (**Fig. 2**).

NTT Com Security employs about 870 people worldwide, of which more than 500 are skilled personnel such as consultants specializing in security or security analysts prominent in the field. It consists of a main office and branch offices in 15 countries around the world. More than 200 of these employees are working as security engineers or risk analysts at Global Risk Operations Centers in seven countries. Their job is to perform security monitoring for NTT Com Security customers 24 hours a day, 365 days a year and to keep track of global security trends.

2. Current state of security market

A common theme today is that security is something that cannot be ignored in an environment of advanced communications technologies, BYOD (Bring Your Own Device) policies, and big data applications. Hacking of information related to financial, government, and military institutions, as well as hacking of confidential information to conduct electronic commercial transactions (e-commerce), and hacking simply for financial gain, occur on a daily basis in an increasingly organized and sophisticated manner. Another side of technological progress is the numerous examples of commonly used services that are being exposed to security threats, which results in a less reliable social infrastructure. Specifically, it has become clear that serious vulnerabilities such as Heartbleed, which was uncovered in the OpenSSL cryptographic library, and those in Apache Struts 2, a widely used open-source framework for creating web applications, have exposed many transactions on the web to the risk of information leaks, resulting, for example, in the temporary closure of a website used

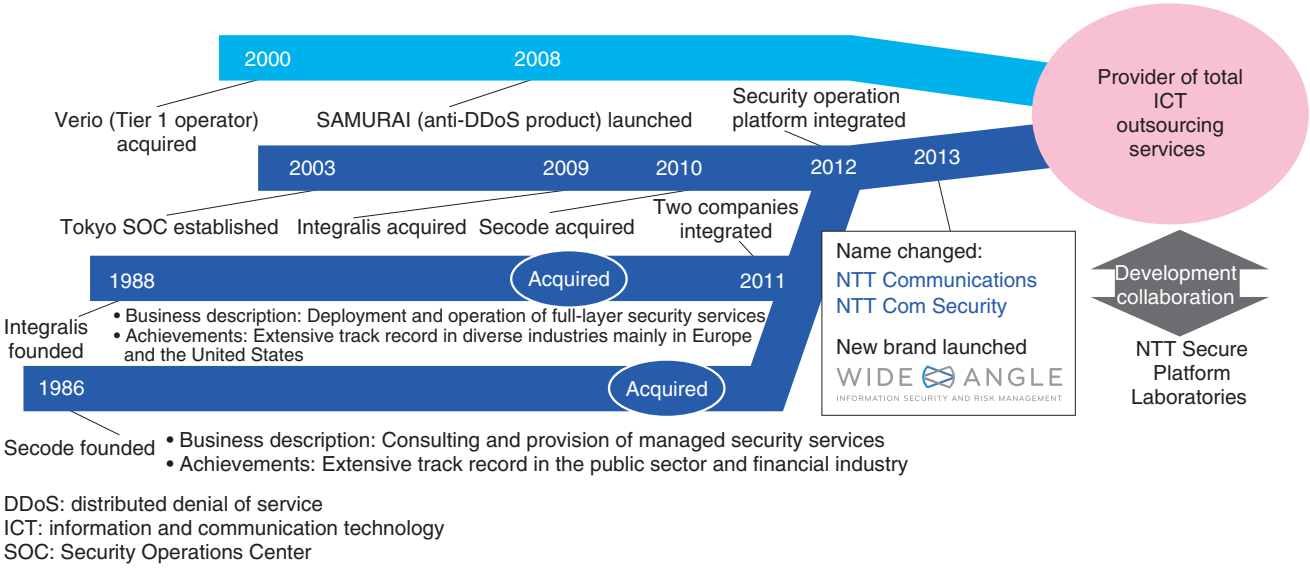

Fig. 1. History of NTT Com Security.

Fig. 2. Global expansion of NTT Com Security business.

for filing income tax returns.

In March 2014, the NTT Group published the Global Threat Intelligence Report (GTIR) based on recent attacks and a massive security-monitoring log (**Fig. 3**). This report was prepared and released by NTT Innovation Institute, Inc. (NTT I^3) in cooperation with NTT Group security companies (Solutionary, NTT Com Security, Dimension Data, and NTT DATA) and NTT laboratories. Through an analysis of more than 3 billion recent security attacks and security log data covering several trillion cases obtained through monitoring at 16 Security Operations Centers (SOCs) worldwide, this report provides useful information on what information assets attackers are aiming for and what methods they are using, and on how an organization can protect itself.

According to this report, 34% of all known attacks are related to client botnet activity and 15% to

anomalous behavior, i.e., unnatural or abnormal communications (**Fig. 4**). This means that, for about half of all attacks, users' internal terminals or users themselves are either knowingly or unknowingly complicit in the attacks. An enterprise must take countermeasures against the risk of becoming a victim and of simultaneously becoming a perpetrator. Furthermore, it goes without saying that individual employees can expose the enterprise they work for to major lawsuits or compensation claims by causing internal or external damage.

There are cases in which a system manager's terminal within a corporate network becomes infected with malware that then spreads throughout the network unbeknown to that manager. It is clear from survey materials that most such cases result in large monetary losses. The GTIR states that the monetary damage per incident of this type is estimated to be about US$110,000.

Malware is continuously evolving to evade system managers and diverse security measures. The same survey revealed that 54% of new malware gathered by honeypots set up by the NTT Group for research purposes could not be detected by existing anti-virus software and similarly that 71% of malware gathered in a sandbox environment could not be detected by up to 40 existing virus countermeasures.

New types of attacks that are mounted from either inside or outside a company directed at information assets appear daily, so it is impossible to protect oneself by simply introducing security devices and security software. It is important to have a security maintenance mechanism that can defend against both external and internal attacks and deal with new attack techniques on a continuous basis. Furthermore, when selecting a security service or vendor, it is important to consider whether the service or company can provide a mechanism not just for end-point security but also for detecting malware throughout the corporate network and cloud and whether that mechanism can uncover vulnerabilities and understand the nature of attacks. It must also be considered whether a security service or vendor can provide resources for keeping up with the latest security trends.

Fig. 3. Global Threat Intelligence Report.

3. New service brand—WideAngle

The market focused on by NTT Com Security is mainly corporate information security management consisting of three business domains: (1) professional services, (2) sales and deployment of security devices, and (3) managed security services (MSS).

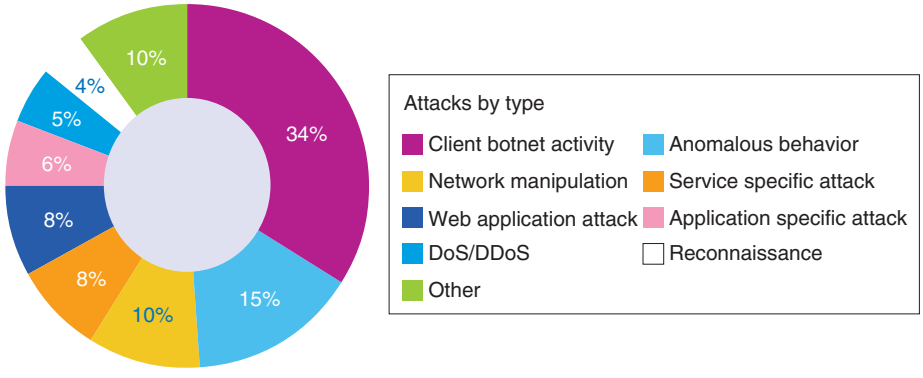

Fig. 4. Breakdown of security attacks.

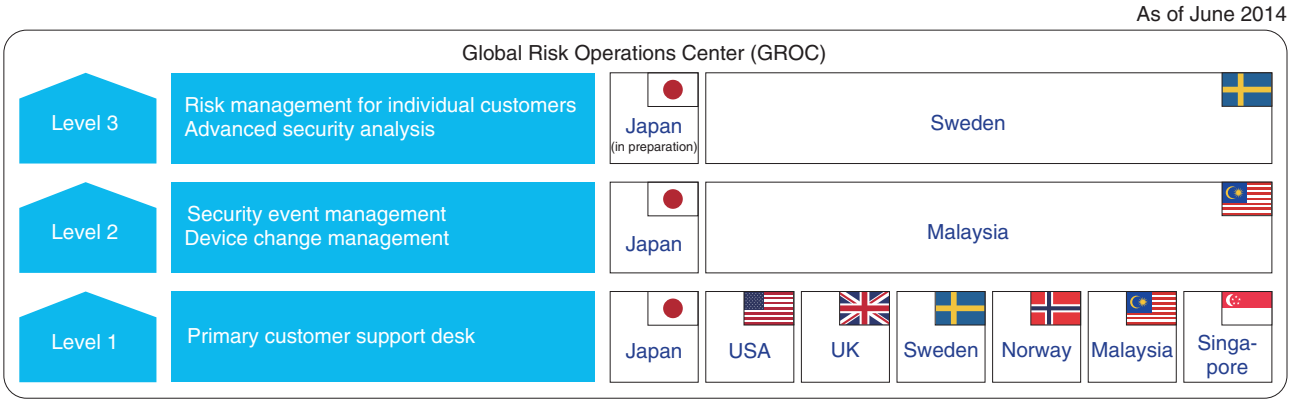

Fig. 5. Security monitoring operations system.

NTT Com Security began its security business in 1986 at overseas locations and in 2003 at the Tokyo SOC as a base within Japan. The company continues in its role of monitoring corporate network security. At present, a total of about 200 employees work at customer support desks at seven bases around the world (**Fig. 5**). This support includes security event management and device change management in Japan and Malaysia and advanced security analysis and risk management for individual customers in Japan and Sweden.

The company began providing Biz Managed Security Services as MSS for the Japan market in June 2012. In 2013, it upgraded its service platform under a new service brand called WideAngle to provide information security services for customer systems in a seamless manner across international and domestic cloud services and on-premise corporate systems. In this way, NTT Com Security can provide both corporate information security platforms and operations services as a trusted advisor. In MSS, the company provides total security outsourcing services on various layers to uncover vulnerabilities and deal with new types of threats such as targeted attacks that aim to exploit user psychology. NTT Com Security has come to manage over 11,000 security devices in about 3000 companies (as of May 2014).

At NTT Com Security, security consulting is the pillar of professional services, and the company has a record of providing consulting in more than 8000 cases over the last 25 years. Based on this extensive experience accumulated since its initial founding, the company is now providing a new consulting program called Global Enterprise Methodology (GEM). This program has established a globally uniform evaluation technique and systematized the company's know-how. It quantifies the security level of a client company, determines the optimal security level that the company should have given the client's business and industry and the requirements to attain that level, and makes proposals for overall improvement.

In information security, the defending side must be optimized in the face of ever-changing attacks. The attacker, meanwhile, may not necessarily be aiming to exploit information or engage in fraud through only one attack. A more likely scenario is that the attacker shifts to full execution only after making some preparations and performing a preliminary investigation of the target site. Detecting such signs of prior activity can only be accomplished through managed services that perform continuous security monitoring. An effective defense against attacks cannot be achieved by only implementing a countermeasure once, by only deploying security devices, or by only using a detection system engine.

It is extremely difficult for a company to thoroughly defend itself from threats by implementing such measures on its own or by keeping an eye on numerous devices.

The new WideAngle service platform provided by NTT Com Security features a newly developed security information and event management (SIEM) engine in addition to monitoring and analysis by expert risk analysts. It also provides the customer with a portal for integrated viewing of the state of various security devices.

In providing total managed services for client companies and public institutions, NTT Com Security is working with NTT laboratories, NTT DATA, and Solutionary to assemble knowledge and know-how

related to NTT Group security technology. It researches how to identify threats that are continuously changing, how to protect information assets, and how to make the use of such assets safe. It then promptly incorporates the results of this research into actual services.

4. NTT Group's approach to security solutions

The NTT Group added Solutionary in North America as a new security service provider in 2013, and together with NTT Com Security (born out of Integralis and Secode), Earthwave, a subsidiary of Dimension Data, and NTT I^3, the Group's research and development center in North America, it has been making its presence felt in the global security market and receiving high marks from client companies.

The NTT Group was evaluated as a "Challenger" in Gartner's 2014 Magic Quadrant for Global MSSPs*, which positions MSS providers in the global market, and was positioned in the same quadrant as the vendor with the highest "ability to execute."

At NTT Com Security, we believe that the reason for this high evaluation is due to our provision of high-quality MSS services, our development of a wide variety of novel technologies in support of those services, our globally uniform system of providing services and operating SOCs, and our sophisticated information exchange network within the NTT Group for keeping up with the latest security trends and threats.

Going forward, we aim to create a synergetic effect through even further interaction and collaboration among the NTT Group companies while providing solutions in diverse domains such as network services, datacenters, and cloud services. Our desire is to provide cutting-edge security solutions at the forefront of the industry by working together as a unified group.

* Gartner, "Magic Quadrant for Global MSSPs," Kelly M. Kavanagh, 26 February 2014.
Gartner does not endorse any vendor, product, or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Tetsuo Someya
Chief Business Development Officer and Chief Governance Officer, NTT Com Security.

He has an MBA from Yale School of Management and a BA in law from Waseda University in Japan. He was appointed Chief Business Development Officer and Chief Governance Officer in January 2013. As Chief Business Development Officer, he is responsible for developing the relationship between NTT Com Security and NTT Communications and its affiliates. In his role as Chief Governance Officer, he looks after key group governance functions, including those concerning legal, procurement, information security, internal auditing, and group IT issues.

Prior to this, he worked in a variety of roles across NTT Communications for over 20 years, including service planning and development, public relations, global business strategy, and global human resources management, and spent time at NTT Europe leading the Düsseldorf office. He also played an important role in overseas investment management at NTT (holding company) from 2001 to 2005.