Cyber Security Factory - Our Commitment to Help Developing More Effective Methods of Coping with Today's Increasingly Sophisticated Cyber Threat

YANO Yukiko, TAKAHASHI Hiroki, HIGUCHI Ken, ARIMATSU Tatsuhiko

Abstract

In order to respond quickly and effectively to cyber attacks that are becoming more sophisticated, NEC established the "Cyber Security Factory," a specialized unit dedicated to developing countermeasures against cyber attacks. Concentrating our technical resources, technologies, knowledge, and expertise to provide advanced and comprehensive cyber protection services in cooperation with Japanese security top vendors, the Factory became fully operational in June 2014. We will continue to develop services and technologies, expand cyber intelligence functions, and train security professionals to combat this ever-evolving threat.

Keywords

cyber security, cyber attack, targeted attack, security monitoring, cyber intelligence, Cyber Security Factory, INTERPOL

1. Introduction

In recent years, cyber attacks by professional organized cyber criminal groups have resulted in the theft of massive amounts of critical data. These attacks have been increasing both in frequency and effectiveness, focusing on sensitive government data, corporate latest technical data, and personal information. These attacks can have devastating effects, ranging from loss of public trust to severe financial losses caused by damages and compensation. In some cases, these attacks can even prevent a company's ability to continue to do business. Preventing these attacks and responding quickly to them when they do occur is vital to the continued success of any business today.

Photo Cyber Security Factory.

NEC's Cyber Security Factory was established as a specialist organization dedicated to countering these threats and attacks (**Photo**).

This paper introduces the current operations of the Cyber Security Factory, as well as its direction for the future.

2. Current Situation of Cyber Attacks

Over the past decade, cyber attacks have evolved from juvenile hacking exploits aimed at random targets with no real goal other than to show off the perpetrator's technical skills to much more serious attacks, targeting specific organizations such as governments, critical infrastructure, intellectual property and confidential data, website spoofing and service denial, etc. When exposed to a cyber attack, an organization not only suffers temporary and costly system downtime, its corporate responsibility can also be severely damaged, leading to a social problem.

Cyber attacks reported in the news are only the tip of the iceberg. Many incidents are never disclose public, and many more continue silently and unnoticed with executives and system administrators not even aware that they are happening (**Fig. 1**).

Cyber attacks in recent years have made use of a number of different techniques - some are at vulnerabilities in web servers, networks, operating systems, gateway products, and applications, others take advantage of people's interests by spoofing respectable organizations. Constantly evolving and becoming ever more sophisticated, cyber attacks demand an equally adaptive and sophisticated response (**Fig. 2**).

Before striking a database, hackers can spend up to a year getting ready, first engaging in reconnaissance activity to identify what information they want and which organizations to target, and then examining various attack scenarios and methods. The hackers penetrate the target systems, send attacking codes while communicating with external C&C (command and control) servers, and attempt to steal data or shut down systems. Subsequently, they may delete system logs, attacking codes in terminals, and compressed data used for the data theft in order to delay discovery (**Fig. 3**).

Because these attacks are so hard to defend against, vulnerable government agencies, critical public infrastructure, and private companies need to develop new and more effective countermeasures. Conventional protection methods are no longer sufficient to protect an organization from today's rapidly evolving and highly sophisticated attacks.

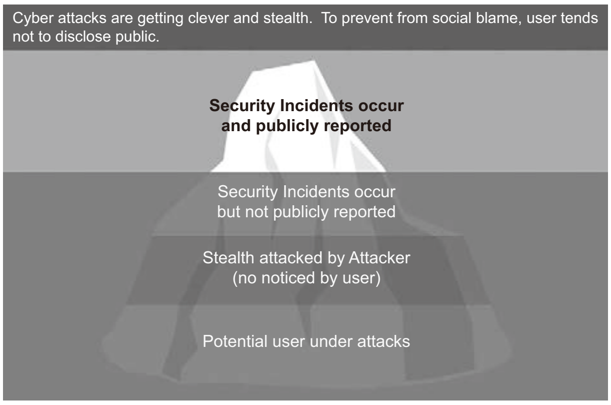
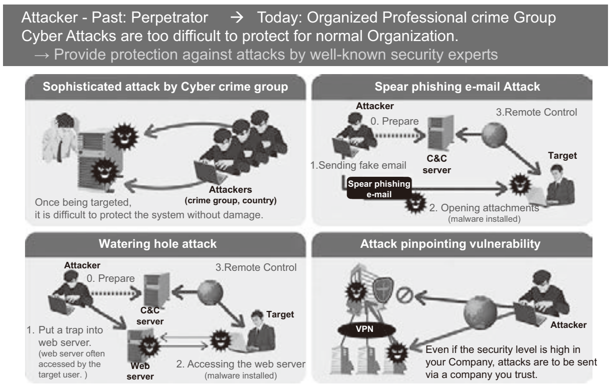
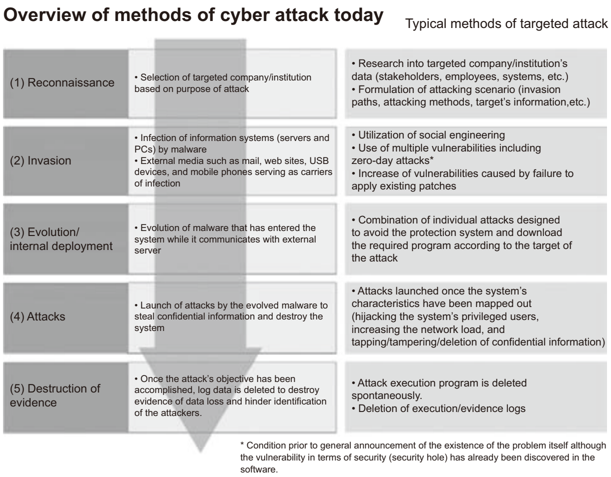

Cyber attacks are getting clever and stealth. To prevent from social blame, user tends not to disclose public.
Security Incidents occur and publicly reported
Security Incidents occur but not publicly reported
Stealth attacked by Attacker (no noticed by user)
Potential user under attacks

Fig. 1 Actual cases of cyber attacks.


Attacker - Past: Perpetrator → Today: Organized Professional crime Group
Cyber Attacks are too difficult to protect for normal Organization.
→ Provide protection against attacks by well-known security experts

Sophisticated attack by Cyber crime group
Attackers (crime group, country)
Once being targeted, it is difficult to protect the system without damage.
Spear phishing e-mail Attack
Attacker
0. Prepare
C&C server
3.Remote Control
Target
1.Sending fake email
Spear phishing e-mail
2. Opening attachments (malware installed)
Watering hole attack
Attacker
0. Prepare
C&C server
3.Remote Control
Target
1. Put a trap into web server. (web server often accessed by the target user.)
Web server
2. Accessing the web server (malware installed)
Attack pinpointing vulnerability
VPN
Attacker
Even if the security level is high in your Company, attacks are to be sent via a company you trust.

Fig. 2 Cyber attacks are becoming increasingly sophisticated.


Overview of methods of cyber attack today

		Typical methods of targeted attack
(1) Reconnaissance	• Selection of targeted company/institution based on purpose of attack	• Research into targeted company/institution's data (stakeholders, employees, systems, etc.) • Formulation of attacking scenario (invasion paths, attacking methods, target's information,etc.)
(2) Invasion	• Infection of information systems (servers and PCs) by malware • External media such as mail, web sites, USB devices, and mobile phones serving as carriers of infection	• Utilization of social engineering • Use of multiple vulnerabilities including zero-day attacks* • Increase of vulnerabilities caused by failure to apply existing patches
(3) Evolution/ internal deployment	• Evolution of malware that has entered the system while it communicates with external server	• Combination of individual attacks designed to avoid the protection system and download the required program according to the target of the attack
(4) Attacks	• Launch of attacks by the evolved malware to steal confidential information and destroy the system	• Attacks launched once the system's characteristics have been mapped out (hijacking the system's privileged users, increasing the network load, and tapping/tampering/deletion of confidential information)
(5) Destruction of evidence	• Once the attack's objective has been accomplished, log data is deleted to destroy evidence of data loss and hinder identification of the attackers.	• Attack execution program is deleted spontaneously. • Deletion of execution/evidence logs

* Condition prior to general announcement of the existence of the problem itself although the vulnerability in terms of security (security hole) has already been discovered in the software.

Fig. 3 Overview of methods of cyber attack today.

3. Cyber Security Factory

Equipped with all the latest techniques, resources and others for detecting, preventing, and combating cyber attacks, NEC's Cyber Security Factory (**Fig. 4**) is staffed by cyber security experts who work closely with NEC Group companies and external security vendors to provide services such as security monitor operation to detect potential cyber attacks and deep analysis of each incident. The Cyber Security Factory collects and analyzes data on cyber attacks and develops technologies and methods to deal with cyber attacks.

3.1 Security Monitoring

Security analysts monitor our customers' networks and websites on a 24 hours a day, 365 days a year basis. If an attack is detected, it is analyzed and reported to the customer affected (**Fig. 5**).

When an attack is detected, the customer is not alerted by unfiltered alarms delivered by security equipment; instead those alerts are first filtered through analysis engines and then carefully analyzed by our security analysts. This allows us to inform the customer of the precise nature of the attack and appropriate countermeasures. As attacks become increasingly sophisticated, countermeasures need to be improved and refined on an ongoing basis.

3.2 Incident Response

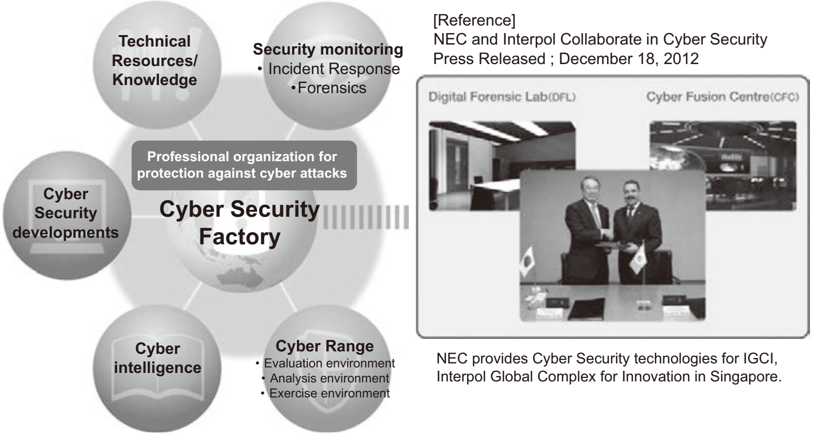

Technical Resources/ Knowledge
Security monitoring
• Incident Response
•Forensics
Professional organization for protection against cyber attacks
Cyber Security Factory
Cyber Security developments
Cyber intelligence
Cyber Range
• Evaluation environment
• Analysis environment
• Exercise environment
[Reference]
NEC and Interpol Collaborate in Cyber Security
Press Released ; December 18, 2012
Digital Forensic Lab(DFL)
Cyber Fusion Centre(CFC)
NEC provides Cyber Security technologies for IGCI, Interpol Global Complex for Innovation in Singapore.

Fig. 4 Overview of Cyber Security Factory.

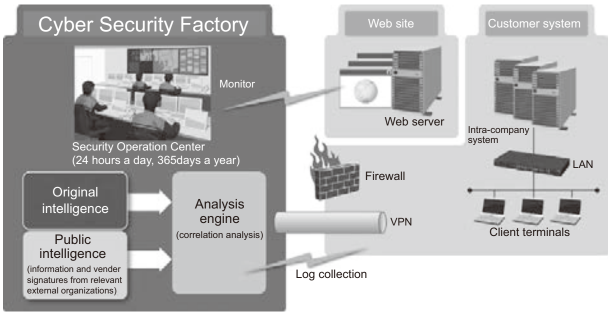
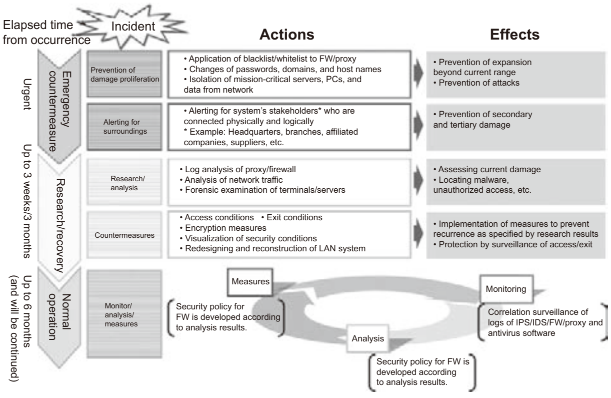


Fig. 5 Security monitoring architecture.



		Actions	Effects
Emergency countermeasure	Prevention of damage proliferation	• Application of blacklist/whitelist to FW/proxy • Changes of passwords, domains, and host names • Isolation of mission-critical servers, PCs, and data from network	• Prevention of expansion beyond current range • Prevention of attacks
	Alerting for surroundings	• Alerting for system’s stakeholders* who are connected physically and logically * Example: Headquarters, branches, affiliated companies, suppliers, etc.	• Prevention of secondary and tertiary damage
Research/recovery	Research/ analysis	• Log analysis of proxy/firewall • Analysis of network traffic • Forensic examination of terminals/servers	• Assessing current damage • Locating malware, unauthorized access, etc.
	Countermeasures	• Access conditions • Exit conditions • Encryption measures • Visualization of security conditions • Redesigning and reconstruction of LAN system	• Implementation of measures to prevent recurrence as specified by research results • Protection by surveillance of access/exit
Normal operation	Monitor/ analysis/ measures	Measures: Security policy for FW is developed according to analysis results. Analysis: Security policy for FW is developed according to analysis results.	Monitoring: Correlation surveillance of logs of IPS/IDS/FW/proxy and antivirus software

Fig. 6 From occurrence of cyber incident to normal operation.

In case an attack code is installed within own organization and causes cyber incident, it is necessary to neutralize the attack, analyze the cause of the incident, recover the damaged system, and prevent any recurrence.

As shown in **Fig. 6**, countermeasures are divided into three phases (emergency countermeasure, research/recovery, and normal operation). By performing the actions listed in the chart, damage can be prevented from proliferating, and measures can be implemented to prevent future attacks.

If the organization do not have the tools or the skills to effectively counter an attack, it is also possible to conclude NDAs with JPCERT/CC and security vendors to implement appropriate measures. There are also companies that establish a CSIRT (Computer Security Incident Response Team) within their own organizations to protect themselves, who can also be asked to provide support as a contribution to the social good.

3.3 Cyber Intelligence

As cyber attacks continue to evolve and mutate, becoming ever more sophisticated and difficult to detect, security measures must be able to adapt to an evolving threat environment. This requires the collection and analysis of an enormous amount of data from a wide variety of sources. The data includes trends in hacker communities, warning signs of potential attacks, information on the latest attack techniques and attack tools, information on attackers (blacklists), information on unknown vulnerabilities, and attack detection methods (signatures). Generically, this data is called “cyber intelligence.”

In addition to working closely with law enforcement agencies in various countries via the International Criminal Police Organization (INTERPOL) and cooperating with the Japanese government, NEC has also formed close alliances with overseas intelligence information companies.

3.4 R&D

In order to counter cyber attacks, it is necessary to gather all the latest information from the fields of security monitoring and cyber intelligence and build a knowledge base that can be put to practical use. However, because there is such a vast amount of data, we are developing technologies to automate analysis and knowledge development performed by analysts. By supporting analysts with automated analysis tools, this technology makes it possible for the analysts to concentrate on more advanced analyses. We are also developing technologies to improve detection accuracy, enhancing our ability to respond effectively to more sophisticated attacks.

3.5 Technical Resource Training

We are also working to develop more effective training methods by using our actual operational experience as the basis for cyber training scenarios. We also train personnel in security monitoring operations and in the various other activities performed at the Cyber Security Factory.

The opportunity to get actual hands-on experience of a cyber attack is rare, so we create a virtual environment similar to an actual corporate ICT environment to enable engineers to try out different countermeasures and get a feel for what will work in actual practice. In FY 2013, we ran ten cyber attack practice sessions as part of a project sponsored by the Ministry of Internal Affairs and Communications called “CYDER:Cyber Defense Exercise with Recurrence.” Altogether, several hundred people attended these exercises, primarily system administrators and information security specialists.

We also plan to package the various training programs we have developed as part of our cyber security technical resource - including the cyber training scenarios discussed above.

4. Global Commitment

INTERPOL is proceeding with the establishment of a new center in Singapore for study and analysis of leading-edge issues in crime and policing, the Interpol Global Complex for Innovation (IGCI). The primary focus at IGCI is cyber crime and the Interpol Digital Crime Center (IDCC) is supposed to play a primary role in dealing with actual cybercrime. IDCC is scheduled to implement the system infrastructure and start actual operation by the end of FY 2014.

NEC is playing a leading role in supporting INTERPOL’s efforts to battle cybercrime. Our activities range from setting up IDCC’s data analysis systems to providing training and technology. As IDCC gears up to go into full operation, it is expected that there will be many opportunities to collaborate in the cybercrime, including working with law enforcement agencies in surrounding countries.

The same analysis systems used by INTERPOL have been installed in NEC’s Cyber Security Factory, allowing us to support them on the back end, while taking advantage of our knowledge bases and strengthening our ties through training and personnel exchanges.

5. Cyber Security Comprehensive Support Service

In order to prevent theft of information via cyber attacks, our Cyber Security Comprehensive Support Service offers a one-stop support system that covers end-to-end from the design and installation of systems to prevent cyber attacks to administration and monitoring of security systems and threat response (**Fig. 7**).

Each customer is provided with an optimal solution tailored to their specific needs based on diagnosis of vulnerability and penetration testing. We are also working to improve administrative services such as monitoring of terminals and periodic inspections. Whenever something suspicious is detected, our Cyber Incident Emergency Response service enables to take the most appropriate initial response as soon as the incident occurs.

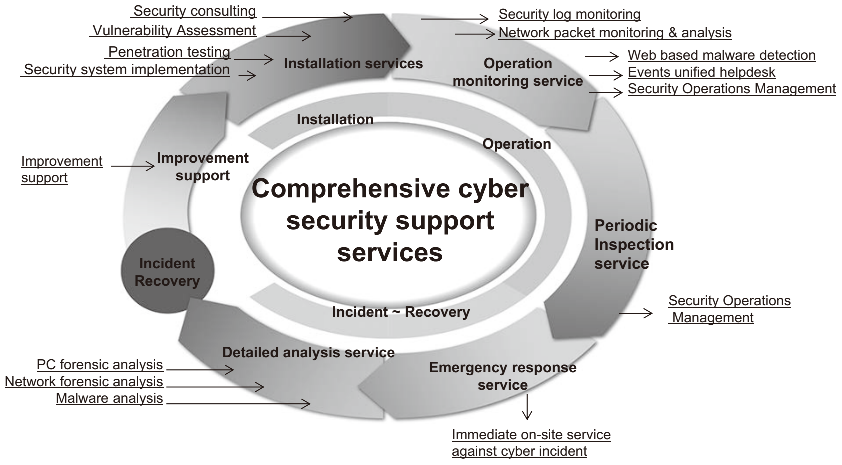

Security consulting
Vulnerability Assessment
Penetration testing
Security system implementation
Installation services
Security log monitoring
Network packet monitoring & analysis
Operation monitoring service
Web based malware detection
Events unified helpdesk
Security Operations Management
Installation
Operation
Improvement support
Improvement support
Comprehensive cyber security support services
Periodic Inspection service
Incident Recovery
Incident ~ Recovery
Security Operations Management
Detailed analysis service
PC forensic analysis
Network forensic analysis
Malware analysis
Emergency response service
Immediate on-site service against cyber incident

Fig. 7 Overview of Cyber Security Comprehensive Support Service.

6. Conclusion

At Cyber Security Factory, we will continue to concentrate our efforts on developing and providing optimal solutions to detect and prevent cyber attacks. By leveraging the multiplier effects derived from information sharing, R&D, and technical resource training we can better address the dangers posed by a constantly evolving threat environment.

Authors’ Profiles

YANO Yukiko
Project Director
National Security Solutions Division

TAKAHASHI Hiroki
Manager
National Security Solutions Division

HIGUCHI Ken
General Manager of Sales Division
Infosec Corporation

ARIMATSU Tatsuhiko
General Manager
Cyber Intelligence Center
Infosec Corporation

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.9 No.1 Special Issue on Solutions for Society - Creating a Safer and More Secure Society

NEC
NEC Technical Journal
Special Issue on Solutions for Society - Creating a Safer and More Secure Society

Vol.9 No.1

January, 2015

Special Issue TOP

NEC Information