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.

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 even 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.

### 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.
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.

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
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

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

Remarks for Special Issue on Solutions for Society - Creating a Safer and More Secure Society
NEC’s Vision for Public Solutions
NEC’s Public Safety Initiative

For a life of efficiency and equality
New Services Realized with the “My Number” System
‘NEC Stadium Solutions’ Played a Critical Role in Construction of the World Cup
Deployment of Eye-Catching, Visually Appealing Flight Information Systems
NEC SDN Solutions Accelerate New Service Implementations for Railway Stations
Cloud-Based Interpreting Service Using a Videoconference Telephone Compatible with Multiple Devices
Easy-to-Use, Smartphone-Oriented Internet Banking, featuring Color Universal Design
The World’s Best Face Recognition System to Achieve Safety and Security in Our Society
Product Line-up for Face Recognition Solutions and its Social Applications

For a safer and more secure life
Healthcare challenge with ICT (Information and Communication Technologies)
Information Governance
Safety Awareness Network
Building a Safer City in Singapore
Securing the Future in Tigre
New Congestion Estimation System Based On the “Crowd Behavior Analysis Technology”
Speech/Acoustic Analysis Technology - Its Application in Support of Public Solutions
High-Sensitivity Camera for Round-the-Clock Surveillance
Imaging Solutions for Search & Rescue Operations
Emergency Mobile Radio Network based on Software-Defined Radio

For the security and safety of critical infrastructure
Centralized Information Control System Supporting Safe and Stable Shinkansen Transportation
Smart Water Management Technology with Intelligent Sensing and ICT for the Integrated Water Systems
A Water Leak Detection Service Based on Sensors and ICT Solutions
Harbor Monitoring Network System for Detecting Suspicious Objects Approaching Critical Facilities in Coastal Areas
Failure Sign Monitoring System for Large-scale Plants Applying System Invariant Analysis Technology (SIAT)
Infrared Camera Image Processing Technology and Examples of Applications
Cyber Security Factory - Our Commitment to Help Developing More Effective Methods of Coping with Today’s Increasingly Sophisticated Cyber Threat

Advanced technologies for a Safer and More Secure Society
Technologies for Improving the Speed and Accuracy of Fingerprint Identification Systems in Support of Public Bodies
Compression Technologies Supporting Next Generation Broadcasting Services - Ultra-HD Digital Video Compression Technology and Real Time HEVC Compression Unit Corresponding to 4K HD Images

NEC Information

NEWS
NEC Starts Operation of Satellite Integration Center
Development of Water Purification System Type2 Reverse Osmosis (WPS RO2) for Japan Ground Self-Defense Force