Meeting the Challenge of Targeted Threats

ISHIHARA Kenji, KOBAYASHI Youhei, KUSUDA Toru

Abstract

Targeted threats represent today's greatest challenge to information security and have become increasingly prevalent in Japan since 2011. As cyber threats become ever more sophisticated and advanced, their perpetrators have begun to direct their attacks at a wider range of targets including government and municipal offices, universities, and public organizations, as well as enterprises. In this paper, we focus on the damage that can be wrought by targeted attack email - one of the most common techniques used to launch a cyber attack - and discuss how to identify and protect against these threats.

Keywords
cyber attack, cyber security, targeted threat, information leakage, mail, malware, "My Number", defense in depth, sandbox, SOC, SIEM, forensics

1. Introduction

Cyber attacks pose an increasing challenge for enterprises today, as well as governments and other organizations. Striking corporate IT infrastructures via networks and the Internet, these attacks are increasing in both number and effectiveness every year. Nor are these attacks limited to random, exploitative hacks; today's cyber threat environment is dominated by targeted threats - that is, persistent attacks targeted at particular industries and companies.

Because targeted threats are carefully premeditated and adroitly executed using sophisticated methodology, it is difficult to prevent them with conventional security measures. Countering these threats requires not only improvements in security, but more effective threat monitoring to identify threats both within and beyond local networks and new tools, tactics, and procedures to deal with those threats. This paper discusses those measures using real-life examples to show how cyber threats can be most effectively countered.

2. Overview of Targeted Threats

In many cases, targeted treats begin with the execution of what is called malware - a foreign program or a set of codes that inserts itself into the targeted computer and performs malicious behaviors. The most common way to insert malware into a computer and have it executed there is to attach it to an email called targeted attack email.

Targeted attack emails often pretend to be relevant to the daily operations of targeted users and critical to important procedures inside and outside their organization. They are designed so that users open them without any suspicion. Once the email has been opened, the user's computer can be infected with the malware.

Infection by malware is most commonly achieved by having the user open an attached file embedded with the malware. However, there are now an increasing number of cases in which the email text contains a URL that pretends to be an actual site and clicking the URL causes infection.

Once the user's PC has been infected by the malware, that PC is used as a springboard to the company's servers and other computers, allowing the attacker to steal confidential information, defraud the company of money, or destroy the systems - whatever is the intended goal of the attack.

As soon as the attacker's goal has been accomplished, all traces of the attack are covered up by deleting or altering logs

and the attack or series of attacks is terminated.

As we have seen, the most notable characteristic of targeted threats is that routine computer operations can lead to confidential information theft and money fraud, as well as system destruction. Because access is gained by deception, these attacks cannot be dealt with using conventional security measures such as firewalls and antivirus software.

3. Targets of Targeted Threats

A decade has passed since 2005 when the first targeted attack email was confirmed in Japan. During that period, the nature of the targets and the objectives of targeted threats have continued to evolve. Today, the major targets are government agencies and public service organizations that store huge amounts of confidential information, as well as manufacturers that have highly valuable intellectual property. The objectives of current targeted threats can be classified as follows.

(1) Personal information theft

As is evident in recent incidents of information leakage, personal information including names, addresses, and phone numbers themselves have monetary value, so such information is stolen for the purposes of selling to list brokers or to use in schemes to defraud the victims whose information has been stolen.

The introduction of the "My Number" social security and tax identity system in Japan has led to increased concern about the potential for information being lost or stolen.

(2) Confidential information theft

By stealing product planning, R&D, and patent information, the perpetrators can sell it to the victim's competitors and make prior patent applications. Confidential information about government and other important buildings can be used for planning terrorist attacks. Other confidential information can be used for espionage activities.

(3) Money fraud

In the past few years, there have been countless reports on cases of money fraud by unauthorized access and operation of Internet banking systems. In the United States, in particular, the number of incidents in which credit card numbers are stolen in attacks targeted at POS systems is increasing. Once obtained, the credit card numbers can be used to fraudulently obtain money and goods. It is now feared that this type of attack will also spread to Japan.

(4) Unauthorized access and destruction of control systems

Today, even control systems used in factories and various energy plants are increasingly connected to open and network-connected systems - which increases vulnerability to malicious attacks.

While attacks targeted at control systems can cause devastating damage to the production activities of a company by destroying the systems in the factories, the destruction of systems in energy and chemical plants can disrupt lifelines and can even threaten human life under certain circumstances.

4. Trends in Targeted Threats

The increasingly sophisticated nature of targeted threats is making it more and more difficult to counter them with conventional measures. Nor, in many cases, does a single measure provide adequate protection. In order to provide an IT infrastructure with comprehensive protection against targeted threats, a "defense in depth" is recommended, in which separate measures are taken at different key access points, such as firewalls for Internet connection, intranets, servers, and PCs.

In addition to the introduction of protection solutions and products, mutual collaboration between various relevant menus of systems, administration, organization, education, and training for early detection of attacks, management to minimize damage, the introduction of procedures and structures to cope with emergencies and ongoing user training are required in order to build systems that can lead to a solution.

5. A Real-World Example of Defense in Depth

An example of protection systems that achieve defense in depth is shown in **Fig**. below. Along with the flows of data in targeted threats, defense in depth can be accomplished by installing protection solutions at various key points.

(1) Gateway protection

It is extremely important that targeted threats from outside be detected at the perimeter of an enterprise - to stop any damage at the water's edge, so to speak. This is generally called gateway protection.

Gateway protection typically involves firewalls, antivirus programs, and antispam programs, which are installed at points where the enterprise's systems connect with the outside world to protect the in-house systems from unauthorized communications, viruses, and spam mails. However, the majority of the threats today consist of targeted attack emails that pretend to be ordinary emails. Keeping these threats from penetrating the company's systems is difficult for conventional protection systems as these generally operate by comparing current activity with known patterns of attacks and viruses, none of which is helpful in dealing with what may appear to be a harmless email.

Today products are available that detect targeted threats by executing access to URLs in attached files and email texts in the virtual space inside security mechanisms called sandboxes and examining their behaviors. These products can help strengthen protection against unknown malware which does not resemble any known conven-

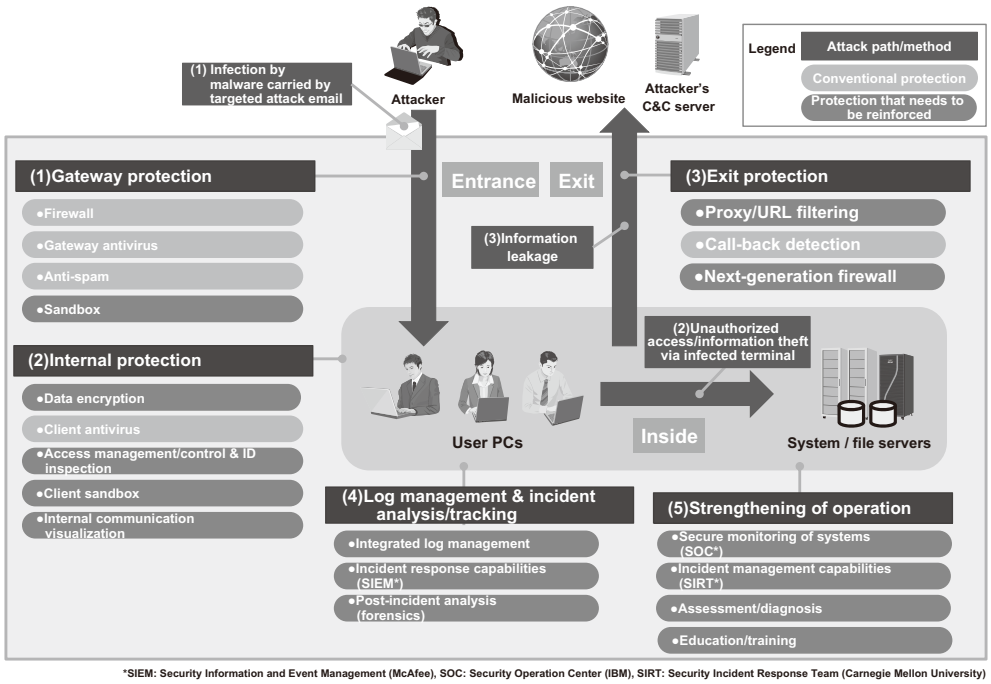

Fig. Example of defense in depth model for targeted threats.

tional attacks or viruses.

(2) Internal protection

As targeted threats become more sophisticated. It is becoming more common for an attack to penetrate the outer layer of defenses, even when these have been properly set up.

The second key to defense in depth is to protect PCs and networks inside the company. Once the targeted attack email has passed through the gateway protection, it reaches each user's PC. When the user opens the attached file or accesses the URL in the mail text, malware infection takes place.

Because the attacker can use the infected PC as a springboard to gain unauthorized access to various internal systems and file servers and then steal information or destroy systems, it is important to prevent the PCs from being infected by malware and to be able to detect unauthorized access and communication of the infected PC.

These measures are usually called internal protection. In particular, effective measures include interruption of malware trying to infect PCs by monitoring the memories and processes on the PCs, as well as, on the assumption that the PCs have already been infected by the malware, access management, ID inspection, and internal communication visualization to detect suspicious requests for unauthorized login to various systems and servers from the PCs and to detect unauthorized communication and prevent it from reaching the exit.

Encryption of data stored in PCs and file servers is also effective. Once that has been done, even if data is disclosed outside the company, its content cannot be decrypted, preventing confidential information from being leaked externally.

(3) Exit protection

Typically, the main objective of targeted attacks is to steal information. This is usually achieved by concealing information transmission as web communication with the outside initiated by the PC infected with the malware. By detecting communication with the outside, it is possible to prevent the information from being leaked.

Specifically, effective measures include (1) blocking access to malicious websites by filtering URLs and (2) blocking unauthorized communications with the outside by filtering according to the behaviors of communications and types of applications.

(4) Log management and incident analysis/tracking

Although the measures introduced in (1) to (3) can significantly reduce the risk of damage from targeted attacks, there are no measures available at this time that can provide assurance of one hundred percent safety when the nature and methodology of attacks are being constantly evolving, becoming ever more sophisticated and difficult to defend against.

To bring the risk down as close to zero as possible, it is critical that the log be assiduously managed at all times, regardless of whether a threat is suspected, in order to en-

sure that any signs of abnormality are detected at an early stage.

Many of the products designed to protect against targeted threats feature the ability to record system logs, access logs, and operation logs themselves, so it is possible to detect abnormal conditions from individual logs. Recently, however, a growing number of organizations are looking at the possibility of introducing integrated log management, as well as security information and event management (SIEM). Analyzing the collected logs from devices makes it possible to analyze symptoms related to an incident across different devices and perform a comprehensive forensic investigation of the incident.

(5) Improved operation

No matter how sophisticated the software or hardware countermeasures deployed, human capabilities remain a key variable in order to prevent advanced targeted threats. Without a thorough grounding in data security and a comprehensive understanding of the functions and features of the various anti-malware products and defensive systems employed, operators may make errors that can leave the system vulnerable. It is also essential that operators know what countermeasures to deploy as soon as the damage from an attack has been confirmed, understand the meanings of the alerts and logs issued by the anti-malware software, and be able to confidently implement countermeasures.

To function effectively, operators need to be up to date on the very latest in vulnerability and targeted threat information, as well as possessing operation know-how in protection systems. Also required are a security operation center (SOC) that can immediately respond to an emergency by performing security monitoring 24 hours a day, 365 days a year, and a security incident response team (SIRT) that can perform a full investigation of any incidents that occur. These responsibilities can be handled by in-house organizations or outsourced to other companies.

It is also necessary to perform periodic self-evaluations, reviews, and improvements in order to ensure that the maximum level of protection is maintained. It is recommended security assessment and diagnosis be used to track that the overall protection environment and single out any areas that require improvement. Employee security consciousness should be enhanced by education and training.

6. Conclusion

Countermeasures against targeted threats are very wide-ranging and require advanced experience and know-how to implement effectively, making it impossible to build perfect structures and measures in a short time.

We believe that the quickest way to strengthen the countermeasures against targeted threats is to introduce the key protection measures discussed in this paper step by step and to accumulate operation so that the level of the countermeasures can continue to be improved.

Authors' Profiles

ISHIHARA Kenji
Manager
Global Products and Services Development Division

KOBAYASHI Youhei
Assistant Manager
Global Products and Services Development Division

KUSUDA Toru
Assistant Manager
Global Products and Services Development Division

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.10 No.1 Special Issue on Enterprise Solutions to Support a Safe, Secure and Comfortable Life
- Value Chain Innovation Linking "MAKE," "CARRY" and "SELL" -

Remarks for Special Issue on Enterprise Solutions to Support a Safe, Secure and Comfortable Life
NEC's Approach to Value Chain Innovation
- Safer, More Secure and More Comfortable Living Through Value Chain Innovation -

Value chain innovation: "MAKE"
Making the Manufacturing Industry More Responsive – NEC Manufacturing Co-creation Program
NEC Industrial IoT - Building the Foundation for Next-Generation Monozukuri
Industrie 4.0 and the Latest Trends in Monozukuri Innovation in the Auto Industry

Value chain innovation: "CARRY"
Logistics Visualization Cloud Services in Asian Developing Countries

Value chain innovation: "SELL"
ICT and the Future of the Retail Industry - Consumer-Centric Retailing
An Advanced Electronic Payment System to Support Enhanced Service Provision
NEC's "NeoSarf/DM" E-Commerce Solution and the Omni-Channel Era
NEC Smart Hospitality Solutions - Deploying OMOTENASHI or the Unique Japanese Way of Entertaining Guests

Sustainable living/Sustainable lifestyles
Transit System Smart Card Solutions and Future Prospects
NEC's Commitment to Smart Mobility
EV Charging Infrastructure System That Facilitates Commercialization of EV Charging
IoT Device and Service Platforms Development and Realizing IoT Business

NEC's advanced ICT/SI for the enterprise domain
NEC's Approach to Big Data
Demand Forecasting Solution Contributing to Components Inventory Repair Optimization
Predictive Analytics Solution for Fresh Food Demand Using Heterogeneous Mixture Learning Technology
Global Deployment of a Plant Failure Sign Detection Service
Application of Big Data Technology in Support of Food Manufacturers' Commodity Demand Forecasting
Contributing to Business Efficiency with Multi-cloud Utilization and Migration Technology
Integrated Group Network Using SDN Case Study: Toyo Seikan Group Holdings
Meeting the Challenge of Targeted Threats
Security Assessment Ensuring "Secure Practice" Against Escalating Cyberattacks
Control System Security Anticipating the Coming Age of IoT
NEC's Approach to VCA Solutions Using Image Identification/Recognition Technology
Quick-Delivery, Low-Cost Web Development Architecture born from Field SE
Embedded System Solutions for Creating New Social Values in the Age of IoT
NEC's Advanced Methodologies for SAP Projects

Vol.10 No.1
December, 2015

Special Issue TOP