Latest Cyberattack Trends 2017 - Model Applying NEC Cyber Threat Intelligence -

ISODA Koji, KAKUMARU Takahiro

Abstract

Traditional security measures have experienced difficulty in protecting against recent cyberattacks. This is because the attacks no longer consist of malware alone but have now acquired the capability of avoiding detection by the sophisticated use of management tools in their targeting systems. In order to deal with attack techniques that are continuing to advance, the use of Cyber Threat Intelligence (CTI) such as via cyberattack technique analysis, is currently attracting attention. This paper describes the cyberattack techniques recently discovered by using CTI.

Keywords

cyberattack countermeasures, Cyber Threat Intelligence, malware, ransomware

1. Introduction

In March 2017, NEC participated in the Automated Indicator Sharing (AIS), a framework promoted by the U.S. Department of Homeland Security (DHS) for quick sharing of cyberattack threat information across governmental and private sectors. Its aim was to enhance the information (CTI) which is critical for its cybersecurity business, together with its technologies and human resources. Based on analyses of mutual relationships, mechanisms and indicators of threat elements, the CTI provides the criteria to respond to various threats with the aim of enhancing security countermeasures and reducing the operations costs.

2. Enhancement of Cyberattack Defence Utilizing CTI

2.1 “URSNIF/DreamBot” Targeting Japanese Enterprises and Organizations

A variety of spam mails written in the Japanese language have been distributed since around June 2016 with the aim of causing infections via the URSNIF banking malware. When the addressee opens the file attached to such a mail, illegal codes are downloaded from an illegal site, causing risk of theft of confidential information. Although warnings calling for attention have been issued frequently from the Japanese National Policy Agency, Tokyo Metropolitan Police Dept. and Japan Cybercrime Control Center (JC3), damage still continues to occur. **Fig. 1** shows an example of the results of piv-

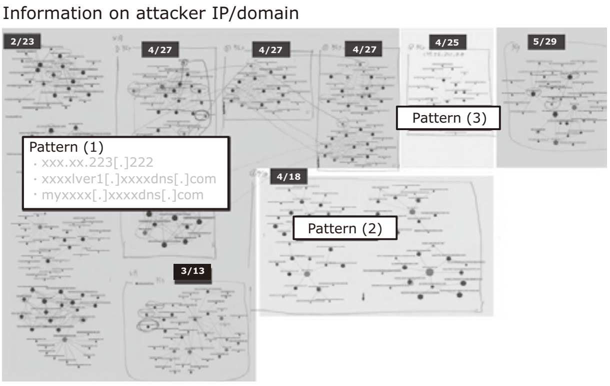


Fig. 1 Results of attack source analysis 1.

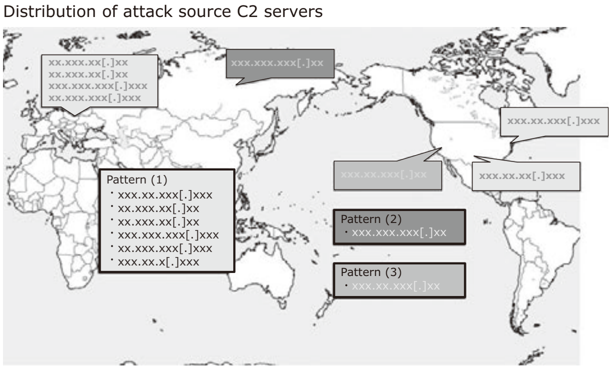


Fig. 2 Results of attack source analysis 2.

Fig. 3 NEC Cyber Threat Map.

ot-table data analysis of spam mail information sent to specific organizations from January to June 2017.

Pivot analysis is used to study the correlations between scattered individual events by collecting and sorting them. In the case of Fig. 1, it was found that the domains and IP addresses of attackers are used in three patterns depending on the time period.

The same results are expressed using the world map in **Fig. 2**.

In addition, it is also possible to sort out the ranges of IP addresses used by attackers and the cycle they use and prepare a defence system accordingly. NEC collects the latest cyberattack information from various sources, analyses them and views the results as shown in **Fig. 3**, to be then applied actively as the basis of security measures.

2.2 How to Defend against Increase of Malware Utilizing PowerShell

Recently media has reported frequently regarding fileless malware that does not use execution files directly. But this is not a new threat concept. For example, the Code Red in 2001 and SQL Slammer in 2003 ran only via memory and without writing anything on the disk. Similarly, IoT malware Mirai and the backdoor DoublePulsar recently leaked from the U.S. National Security Agency (NSA) do not leave any trace on the disk. They remotely abuse the WMI or PowerShell installed in the attack target system as Windows standard functions, minimize the files used in the attacks and clear the illegal files and logs after achieving their goals. The following characteristics are explained as of the time of the compilation of this paper. The actual cases are introduced in JPCERT/CC.

- No log is left even after illegal PowerShell execution.
- No trace of illegal codes is left after the OS reboot.
- Detection is difficult because of direct loading in memory.
- Network detection is difficult if executed via HTTPS communication.
- The attack techniques are difficult to be clarified or discovered.

Some enterprises and organizations currently consider that "attacks making use of PowerShell are difficult to detect." While PowerShell 2.0 packaged in Windows 7 was capable of logging only start-up and exit, the updated 5.0 version can log the actions of attackers including the executed PowerShell commands and scripts, by enabling the logging function. When Windows Module Logging or Windows Sysmon is used, it is also possible to output and view the logs of PowerShell, etc. By considering what kind of operation design can enhance security while using the existing environment and verifying the threats that occur on a daily basis the future generation of intelligence of higher accuracy will contribute to "secure operations."

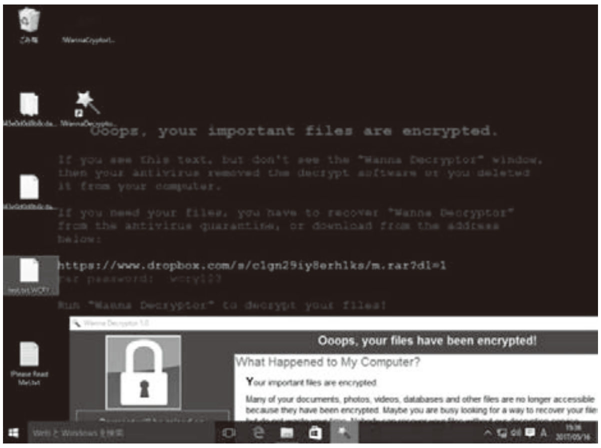
2.3 Threat of WannaCry cannot be Defended with Vulnerability Countermeasures Alone

On May 12, 2017 (U.S. time), damage due to "WannaCry" ransomware (aka. WannaCrypt, WannaCryptor, Wcry, etc.), was produced in enterprises and organizations including in the British medical institutions (**Table**).

Media have been reporting that the damage can be prevented by applying the security patch of MS17-010.

Table Time line of damage occurrences by WannaCry ransomware.

2016 Sept.	Microsoft recommends disuse of SMBv1.
2017 Jan.	US-CERT proposes invalidation of SMBv1.
May 14	Microsoft releases MS17-010.
Apr. 14	Shadow Brokers discloses attack tool EternaBlue.
Apr. 25	WannaCry misusing the URL of Dropbox.
May 12	Cyberattacks using WannaCry occur in countries worldwide.
May 14	IPA calls for attention against WannaCry.
May 23	Symantec announces the potentiality of North Korean involvement.



```
Ooops, your important files are encrypted.

If you see this text, but don't see the "Wanna Decryptor" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.

If you need your files, you have to recover "Wanna Decryptor"
from the antivirus quarantine, or download from the address
below:

https://www.dropbox.com/s/clgn29iy8erhlks/m.rar?dl=1
rar password:  wcry123

Run "Wanna Decryptor" to decrypt your files!
```

Wanna Decryptor 1.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your file

Fig. 4 Infection with Windows 10 applying MS17-010.

However, NEC promptly obtained and verified samples and, as a result, found that the worm function that diffuses using the vulnerability of Windows file sharing protocol SMBv1 and the ransom function can work independently in WannaCry. The verification results indicating the absolute necessity of ransomware countermeasures, even after application of MS17-010 were communicated to the persons in charge of CSIRT and SE in the NEC Group (**Fig. 4**).

2.4 Threat of the "Wiper Type" Ransomware Petya and Its True Purpose

On June 27, 2017 (local time), damage by ransomware (NotPetya, PetrWrap, GoldenEye, etc.) was confirmed mainly in European countries, as causing serious damage in many enterprises and organizations.

The damage situations as of June 28, 2017 were as follows.

- Ukraine: About 1/3rd of government, enterprise and banking systems and 1/10th of domestic PCs were infected, causing a fault in the radiation measuring system at the Chernobyl power plant.
- Russia: National Oil Company and middle range oil companies infected.
- Denmark: Major shipping businesses.
- USA: Major pharmaceutical manufacturers, major confectionary makers.

Infections took the following routes:

- Accounting software MeDoc used by Ukrainian businesses
- Misuse of a vulnerability of Microsoft Office (CVE-2017-0199)
- Watering hole attacks falsifying major Ukrainian sites

Although this malware partially used the codes of the Petra ransomware in 2016, it is called "NotPetya" because it destroys the key that encrypts the MFT (Master File Table) that manages the information on all files in Windows and renders it unrecoverable. The infections were spread using the hacking tool "EternalBlue," Windows official tool PsExec or by WMI commands like WannaCry. While WannaCry expands infections in the external networks by misusing a vulnerability of SMBv1, Petya attempts to spread infections inside the target organization. Its attack has the following properties.

- Files are overwritten by other files after encryption.
- The Salsa20 key used in encryption is destroyed and made unrecoverable.
- Tor, the common trick of other ransomware, is not used.
- The contact destination is limited to a blocked mail address.
- Administrator information is exploited and a similar tool to Mimikatz is used.
- Attacks were done on the day previous to the Ukrainian Constitution Day.
- Unlike Petya in 2016, decryption was not possible.

The fact of the situation described above suggests that the ransomware is not intended for ransom but that it is an act of destruction at a national level. Ransomware "Xdata" used in Ukraine in May 2017 also misused the updating function of accounting software MeDoc, which is popular in Ukraine, and caused damage using the Mimikatz tool that steals the authentication information. In addition, large-scale power outages occurred in December 2015 and in December 2016 in Ukraine. Russian company Kaspersky reported that these outages are caused by an attacker group called the BlackEnergy APT. After them, a pro-Russian group in Ukraine declared a "new nation" and military tension has been continuing since then, as seen with the joint exercise of the U.S. Navy and the Ukrainian military forces. The CTI should not be regarded simply as a technical matter but it is also important to consider it from the viewpoints of international circumstances and of the political background becoming the motive of the attacks.

2.5 BRONZE BUTLER Relentlessly Targets Japanese Organizations

The BRONZE BUTLER (aka. Tick) is the name given to an attack group by security vendor DELL SecureWorks. This group relentlessly targets specific Japanese organizations via its high technical ability. Once it succeeds in an intrusion, it continues to execute cyber-espionage for several hours.

Reference information:
Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+6.1;+Trident/4.0;+SLCC2;+.NET+CLR+2.0.50727;+.NET4.0E)

An example of a log analysis by Splunk, the data analysis application:
host=ISC_Proxy UserAgent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; SV1)" | eval MalType = if(match(URL,".*¥.(gif|asp|jpg)$"),"Daserf", MalType)

Fig. 5 Example of a conducted log analysis investigation.

- **Purposes of attacks**
  “Technical and intellectual property information” of Japanese businesses.
- **Targets of attacks**
  Key infrastructures and associated businesses.
- **Spear Phishing mails**
  Infected by an attached malicious file in a mail.
  Targeted mail disguising a seasonal greetings mail.
  Watering hole attack
- **RATs (Remote Access Tools, or Remote Administration Tools)**
  Daserf, Datper, xxmm, etc.

Symantec named the attack “Tick” and reported that its activities have been developing over more than a decade.

The attack in question contained more than 50 MB of garbage data and it had the potential of slipping by without being verified by existing security appliance products. When the log information of a specific organization was investigated by referring to the SecureWorks analysis below, four terminals were seen to be infected and their infections were deployed horizontally to tens of terminals. However, as the attack was found to be at an early stage, serious damage was able to be avoided.

Fig. 5 shows an example of a log analysis made in the investigation.

3. Conclusion

At NEC, we are trying to enhance various kinds of intelligence to support our customers via CTI. The threat information data used as the indicators of attacks by malware is generated based on the structured expression language called STIX (Structured Threat Information eXpression). The data includes the threat information viewed by people and that set to various security products and services for automated defence (illegal domain names, IP addresses, hash values, etc.) and is verified daily in order to improve accuracy (**Fig. 6**).

We are also advancing improvements in our analysis capabilities by automating systems and utilizing AI. However, the results and judgments made via the optimum analyses of human labor are indispensable for packaging the training data. It is also important to constantly enhance the countermeasures in order to deal with cyberattack techniques that are continually evolving.

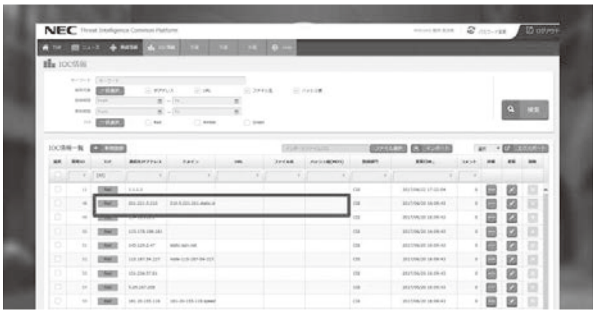


Fig. 6 Image of display of NEC Cyber Threat Intelligence.

* Windows and Microsoft are registered trademarks of Microsoft Corporation in the U.S. and other countries.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Authors’ Profiles

ISODA Koji
Senior Expert
Security Engineering Center
Cyber Security Strategy Division

KAKUMARU Takahiro
Assistant Manager
Security Engineering Center
Cyber Security Strategy Division
CISSP

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.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Vol.12 No.2
January 2018

Special Issue TOP