Detection, Auto Analysis of Cyber Threats Using Open Source Intelligence

KAWAKITA Masaru, SHIMA Shigeyoshi

Abstract

Threat information such as cyberattack techniques and responsibility claims is distributed via social media and the deep web. However, the explosion of information and an insufficiency of security analysts make it difficult to detect such information at an early stage. This causes the problem of delayed preparation against attack damage. This paper introduces an automated proactive attack prevention technology that employs a technical analysis technique used in financial engineering to identify signs that a threat trend is reaching a peak. At the same time deep learning is employed to analyse the overall evidence of a cyberattack.

Keywords

cybersecurity, open source intelligence, threat information, social media, deep web, STIX/TAXII

1. Introduction

Cyberattacks have recently become a social problem by causing damage in many countries worldwide. The security analyst protecting each organization should always collect and analyse the huge amount of threat information showing signs of cyberattacks and take prompt action when the occurrence of an event is predicted. This will ensure the smooth operation of the targets that are frequently attacked; such as critical infrastructures, government institutions and private enterprise entities.

If a new vulnerability discovered in a piece of software or hardware used in an organization is left without taking appropriate action, there is a risk that a cyberattack will occur that exploits the vulnerability. Damage such as confidential information theft may then ensue and malware infection may be caused not only within the organization but also among customers and even in organizations unrelated to the original target. For example, the ransomware “WannaCry” that produced worldwide damage in mid-May 2017 was spread by the “EternalBlue” attack tool that targets OS vulnerabilities.

An attacker who brings a cyber threat executes cyberattacks in an organized manner by collecting information on the attack tools and unreleased vulnerability from social media and black markets. Services that will undertake cyberattacks are also now being developed. Some of the typical example of these are Booters and Stressers that are also known as DDoS-for-hire services and the RaaS (Ransomware as a Service) that distribute ransomware widely in order to take a victim’s files hostage. If the victim pays the ransom, RaaS pays part of it to the client that ordered the attack. The characteristics of these services are that the series of attack actions are automated and the attacks are low cost procedures.

On the other hand, on the protection side, analyses of the cyber threats caused by 100% human labor have already reached a limit for the following reasons.

- The advent of Industry 4.0 has expanded the target of protection from IT equipment to OT equipment.
- The numbers of arrests and consultations related to cybercrimes are increasing every year.
- The amount of information distributed through social media as means of threat information circula-

tion has increased by about 9 times in nine years from 2005 to 2014.

- While the insufficiency of security engineers has already become a problem, these human resources cannot be cultivated in a short space of time due to the necessity of a wide range of knowledge on the system construction.

The background described above is increasing the social need for an efficient means of cyber threat analyses.

In the rest of this paper, in section 2 we describe a cyberthreat information analysis technique based on OSINT (Open Source Intelligence) proposed by NEC and in section 3 we report on an evaluation test, before providing an overall conclusion in the final section.

2. Cyber Threat Information Analysis Based on OSINT (Open Source Intelligence)

At NEC, we have attempted to automate the cyber threat analysis in five phases shown in **Fig. 1**. The key technology element used in each phase will be described in the following subsections.

2.1 Data Collection

For the purpose of research, threat information is collected permanently and saved from more than three million social media, blogs and underground sites on the Internet. The collection targets are expanded autonomously by tracing malicious sites moving across data centres worldwide by detecting the attacker communities. The targets of collection also include the websites located on the deep web that are usually unsearchable by ordinary search engines.

2.2 Prediction

After the presence of malware that expands infections via routers under certain conditions was confirmed in mid-September 2015, cyberattacks targeting such routers occurred frequently from mid to late September of the same year.

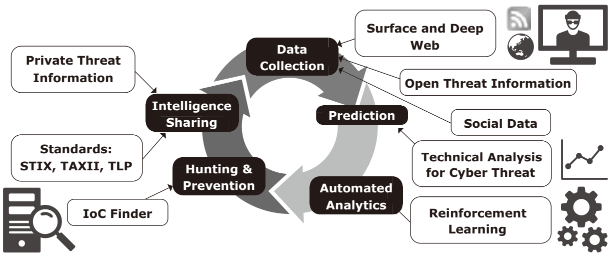


Fig. 1 Flow of automated cyber threat analysis.

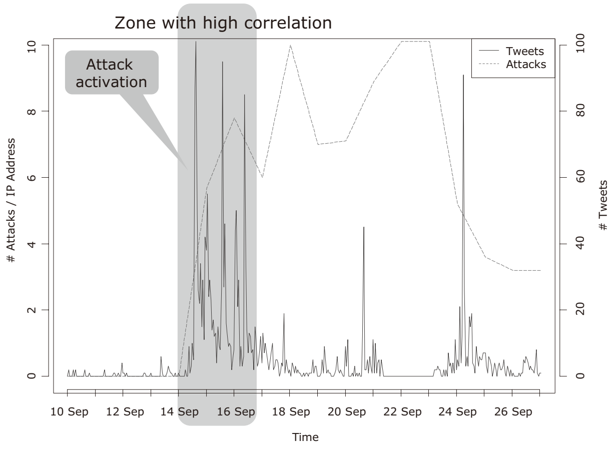


Fig. 2 Numbers of attacks of routers and tweets in social media.

Fig. 2 shows the daily changes in the numbers of attacks per IP address and tweets posted in social medium "Twitter." The multiple regression analysis over the entire period of attacks showed little correlation between them. Nevertheless, high correlation and a certain interlocked property was observed with the analysis focused only on the first peak in the numbers of attacks and tweets around noon of September 15th. This means that identifying signs of a sudden increase in the number of tweets as early as possible would make it possible to detect signs of an attack occurrence.

Traders engaged in investment operations of the financial industry gain profits by predicting issues that will arise and affect stocks and by buying stocks at low prices and selling at high prices.

On the other hand, security analysts also wish to predict vulnerability attacks that become prevalent or the arrival of malware from the trends of threat information and to prepare for cyberattacks in advance so as to minimize the period of potential damage.

This shows that traders and analysts share the same purpose of predicting future trends, except that the objectives are different.

One of the means of predicting the stock price movements used in the financial industry is the technical analysis that predicts the future price movements from changes in prices from the past to the present. Considering that the purpose has similarities, we assume that the technical analysis technique will also be applicable to the prediction of cyber threats.

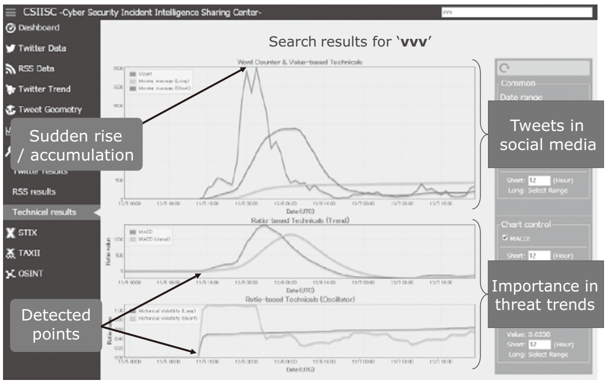
Technical analysis can be divided roughly into the trend and the oscillator analyses. The known trend indicators include the EMA (Exponential Moving Average), which is suitable for identifying the mid- and long-term trends. While the known oscillator indicators include the Historical Volatility and RSI (Relative Strength Index) suitable for identifying short-term trends. There is also the MACD (Moving Average Convergence Divergence), which is an intermediate indicator with the characteristics of both of the above. This identifies the market cycle and sale/purchase timings based on the short- and long-term movement averages of lines. We have clarified that the MACD technique is particularly effective for the analysis of cyber threat trends.

As seen in **Fig. 3**, we analysed each of the characteristic terms contained in the threat information using an original algorithm based on the MACD technique and calculated the degree of causing serious consequences. The results are output as the importance ranking in **Fig. 4** for providing security analysts with the opportunity of noticing signs of threats as well as for use as information for the overall image analysis in the next step.

2.3 Automated Analytics

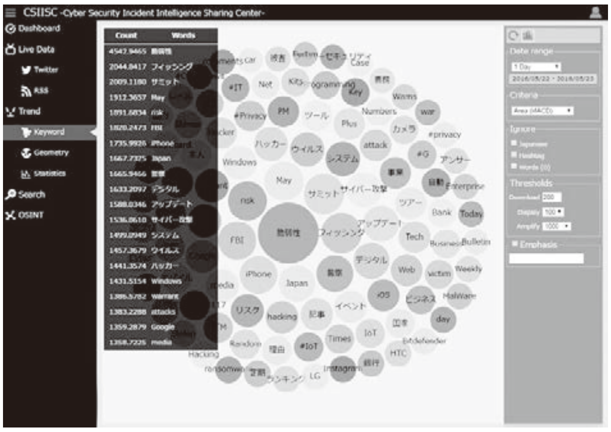
We have developed a technology that uses the deep learning method to promote expertise in overall cyber threat image analysis by skilled security analysts of existing analysis results and of terminal operations histories. If a new clue is found, the entire view of the threat is thereby exposed based on the acquired knowledge (**Fig. 5**).

Since a threat does not necessarily imply a cause of immediate damage, the judgment whether or not a threat will lead to system damage varies depending on the organization's system configuration and workflow as well as the analyser's interpretation and the reliability of the information sources. In addition, the volume of the threat information is very large and simple association of information could result in the enumeration of thousands of elements that include malicious IP addresses.


CSIISC -Cyber Security Incident Intelligence Sharing Center-
Dashboard
Twitter Data
RSS Data
Twitter Trend
Tweet Geometry
RSS results
Technical results
STIX
TAXII
OSINT
Search results for 'vvv'
Word Counter & Value-based Technicals
Ratio-based Technicals (Trend)
Ratio-based Technicals (Oscillator)
Date (UTC)
Common
Date range
Chart control
Sudden rise / accumulation
Tweets in social media
Detected points
Importance in threat trends

* Example of prediction: TestaCrypt (alias VVV virus) case (Early Dec. 2015)

Fig. 3 Example of threat information trend analysis using original MACD-based algorithm.



Count	Words
4542.9465	脆弱性
2044.8417	フィッシング
2009.1180	サミット
1912.3657	May
1891.6834	risk
1820.2473	FBI
1735.9926	iPhone
1667.7375	Japan
1665.9466	[illegible]
1633.2097	デジタル
1588.0346	アップデート
1536.8610	サイバー攻撃
1499.2949	システム
1457.3679	ウイルス
1441.3574	ハッカー
1431.5154	Windows
1386.5782	warrant
1383.2288	attacks
1359.2879	Google
1358.7226	media

Fig. 4 Display of threat prediction result rankings.

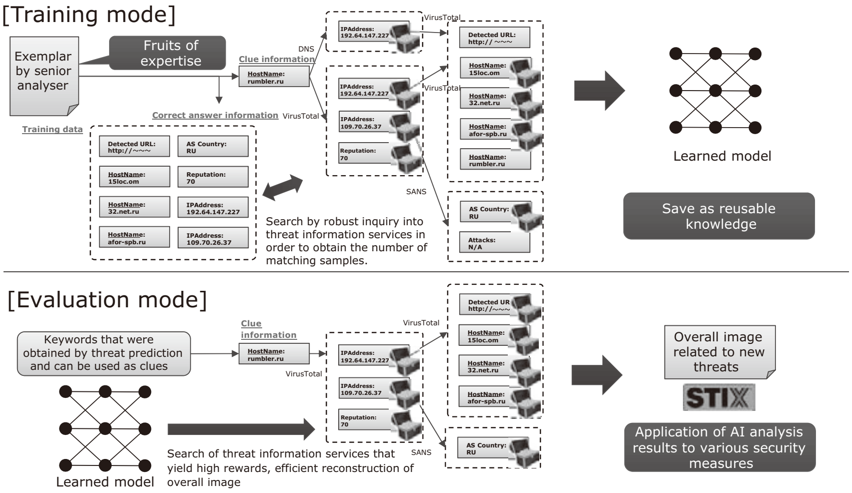

[Training mode]
Exemplar by senior analyser
Fruits of expertise
Training data
Clue information
DNS
HostName: rumbler.ru
Correct answer information
VirusTotal
SANS
IPAddress: 192.64.147.227
IPAddress: 109.70.26.37
Reputation: 70
Detected URL: http://~~~
AS Country: RU
HostName: 15loc.com
HostName: 32.net.ru
HostName: afor-spb.ru
Attacks: N/A
Search by robust inquiry into threat information services in order to obtain the number of matching samples.
Learned model
Save as reusable knowledge
[Evaluation mode]
Keywords that were obtained by threat prediction and can be used as clues
Search of threat information services that yield high rewards, efficient reconstruction of overall image
Overall image related to new threats
STIX
Application of AI analysis results to various security measures

Fig. 5 Overall cyber threat image analysis using the deep learning technique.

Direct application of the obtained results as security countermeasures may also affect routine operations due to excessive protection.

Overall threat image analysis of an appropriate amount and based on a standard specific to each organization is possible by learning the procedures used from previous analyses of cyber damage events. If a new threat is detected it is automatically analysed based on the learned results.

2.4 Hunting & Prevention

The importance of "threat hunting" is increasing as a methodology for coping with targeted attacks that threaten specific organizations via E-mails, etc.

For example, endpoints detect the presence of malware using pattern files provided by anti-virus software. However, there are cases in which damage is caused by malware before completion of the delivery of the pattern file and damage may be detected when using it. Specific organizations are particularly prone to damage by targeted attacks. Such attacks often use malware with malicious devices which can avoid detection by the anti-virus software used by the targeted organizations.

Threat hunting inspects an entire system by using the signs obtained by threat information analysis as a hypothesis to verify the presence of damage and the degree of risk. Its automation enables proactive security measures such as identification of damage and future attack potential immediately after a cyberattack group claims responsibility for an attack (i.e. before the pattern file is delivered).

2.5 Intelligence Sharing

The results of threat analyses are saved with STIX[*1], which is an open structured threat information expression description language elaborated by the OASIS standardization organization. It is from this point that the information required for firewalls and IDS setting changes is generated in order to enforce security measures such as the blocking of the cyberattack transmission source.

The threat analysis results can be shared with other departments, organizations and countries using TAXII[*2], which is an automated detection indicator information exchange procedure elaborated also by OASIS. Cooperative relationships are built so as to service the knowledge obtained from external organizations in the security measures of specific organizations.

Table Early report rate of cyber threats.

Year/Month	Early detection	Total # of threats	Early report rate
2015/July	66	128	51.6%
2015/Aug.	47	78	60.3%
2015/Sep.	34	60	56.7%
2015/Oct.	30	59	50.8%
2015/Nov.	30	62	48.4%
2015/Dec.	40	58	69.0%
Average			56.1%

NEC has joined the AIS, an initiative promoted by the U.S. Department of Homeland Security for sharing cyber threat information among governmental and private sectors, so that we will bolster cyber intelligence and technologies and also human resources in its cyber security businesses.

3. Evaluation Test

The authors measured the number of mentions of cyber threats from the tweets posted in social media every other hour in the period from July to December 2015. From the changes in the number of tweets, the date/time at which sudden rises were detected were obtained by using an original MACD-based algorithm. In addition, the authors also surveyed the date/time of publication of the earliest article by a public institution mass media source or vendor of each cyber threat. As a result, it was confirmed that the original algorithm is capable of detecting cyber threats 56.1% earlier on average (**Table**).

4. Conclusion

In the above, the authors first describe the expansion of cyberattacks and the circulation of threat information via social media and the deep web which may cause the cyberattacks. It was noticed that the first peak in the number of tweets related to cyber incidents on the social media is linked to the number of associated attacks. The authors then proposed a method of extracting threat information with a high potential of damage by using a technical analysis technique as used in financial engineering. In addition, the authors also conducted an evaluation test and demonstrated that the proposed technique can detect the threat information 56.1% earlier on average

[*1] Structured Threat Information eXpression, which is a technical specification for description of items associated with cyberattack activities by incorporating events characterizing cyberattacks. http://stix.mitre.org/

[*2] Trusted Automated eXchange of Indicator Information, which is a technical specification for exchange of threat information associated with cyberattack activities. http://taxii.mitre.org/

than via announcements by public institutions, etc.

The introduction of the proposed procedure can detect the signs of attacks from a huge amount of threat information and apply early and accurate measures so that the period of a potential attack and damage may be decreased.

In the future, too, the authors intend to promote the threat hunting procedure, which takes preventive action before incurring damage from cyberattacks, and they will continue their research activities aiming at the implementation of safe, secure and efficient social infrastructures.

* Twitter is a registered trademark or trademark of Twitter, Inc.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Authors' Profiles

KAWAKITA Masaru
Senior Researcher
Security Research Laboratories

SHIMA Shigeyoshi
Principal Researcher
Security Research Laboratories

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 -

Remarks for Special Issue on Cybersecurity
Developing Fundamental Solutions to Combat the Rise in Cybercrime: What role can a third-party all-Japan industry-academia-government organization play in containing the threat posed by cybercrime?
Trends in Cybersecurity and NEC’s Commitment to Developing Solutions

Social trends & NEC’s approach

An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures
Latest Cyberattack Trends 2017 - Model Applying NEC Cyber Threat Intelligence -
The Measures Applied Internally by the NEC Group to Forestall and Prevent Cybersecurity Incidents

Cybersecurity solutions

Security Operations Center (SOC) and Security Monitoring Services to Fight Complexity and Spread of Cyber Threats
Incident Response Solution to Minimize Attack Damage
Enhancement of Incident Handling Capabilities by Cyber Exercise
Integrated Security Management/Response Solution – “NEC Cyber Security Platform”
Cloud-based File Encryption Service – ActSecure Cloud Secure File Service –
Security LCM Services
Secure Mobile Work Solutions That Exploit EMM
Cybersecurity Consulting Services in the World of IoT

Applications of AI technology to cybersecurity

Countermeasures against Unknown Cyberattacks Using AI
The Potential of AI to Propose Security Countermeasures
Detection, Auto Analysis of Cyber Threats Using Open Source Intelligence
Cyber-Physical Integrated Analysis Technology for Criminal Investigation Support

In-house efforts provide safety and security for customers

Efforts to Provide Safe, Secure Products and Services for Customers – Secure Developments/Operations –
Talent Management: Managing Cybersecurity Human Resources

\Orchestrating a brighter world NEC
NEC Technical Journal
Cybersecurity
- Building Futureproof Security to Support Business Safety and Reliability -
Vol.12 No.2

Vol.12 No.2

January 2018

Special Issue TOP