International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1217

(01/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cybersecurity security – Cybersecurity

Guidelines for applying threat intelligence in telecommunication network operation

Recommendation ITU-T X.1217

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	**X.1200–X.1229**
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1217

Guidelines for applying threat intelligence in telecommunication network operation

Summary

Threat intelligence from a telecommunication operator's point of view is a collection of organized, analysed, and refined information about potential and current attacks that may threaten an organization. This information can also include attackers' motivations, intentions, characteristics, and methods, along with their modus operandi or techniques, tactics, and procedures.

In the network and information security area, the occurrence of large-scale and unexpected cybersecurity incidents has triggered the urgent need for threat intelligence. Threat intelligence can help an organization to reduce risk and improve its overall security. A unified taxonomy, grammar, and presentation of threat intelligence has been defined so that threat intelligence can be shared between different organizations.

Recommendation ITU-T X.1217 specifies guidelines for applying threat intelligence in telecommunication network operation after an overview analysis.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1217	2021-01-07	17	11.1002/1000/14443

Keywords

Security, threat intelligence.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Threat intelligence from a telecommunication operator's point of view is a collection of organized, analysed and refined information about potential and current attacks that may threaten an organization. This information can also include attackers' motivations, intentions, characteristics and methods, along with their modus operandi or techniques, tactics and procedures.

In the area of network and information security, the occurrence of large-scale and unexpected cybersecurity incidents has triggered the urgent need for threat intelligence. Threat intelligence can help an organization reduce risk and improve overall security by understanding who is most likely to attack, what they will attack, what they want to accomplish, why they want it, and how they plan to do it.

[OASIS STIXv2] defines a language and serialization format used to exchange cyberthreat intelligence. [OASIS TAXIIv2] specifies a protocol used to exchange cyberthreat intelligence over HTTPS. [ITU-T X.1215] describes how the structured threat information expression (STIX) language may be used to support cyberthreat intelligence and information sharing.

A unified taxonomy, grammar and presentation of threat intelligence has been defined so that threat intelligence can be shared between different organizations. The next problem that needs to be taken into consideration is how to use the threat intelligence to solve security problems in the network.

[OASIS OpenC2-L] specifies a command and control (C2) language for controlling cybersecurity functions. [OASIS OpenC2-H] specifies a HTTPS application programming interface (API) to transport OpenC2 commands to cybersecurity devices. [OASIS OpenC2-P] specifies the use of the OpenC2 language for controlling stateless firewalls. Profiles for other cybersecurity functions are under development in OASIS.

This Recommendation specifies the guidelines for the application of threat intelligence after an overview analysis.

Recommendation ITU-T X.1217

Guidelines for applying threat intelligence in telecommunication network operation

1 Scope

This Recommendation proposes guidelines for applying threat intelligence in telecommunication network operation after an overview analysis.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1215] Recommendation ITU-T X.1215 (2019), *Use cases for structured threat information expression*.

[OASIS OpenC2-H] OASIS Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0.
<https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html

[OASIS OpenC2-L] OASIS Open Command Open Command and Control (OpenC2) Language Specification Version 1.0.
<https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html>

[OASIS OpenC2-P] OASIS Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0.
<https://docs.oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0.html>

[OASIS STIXv2] OASIS STIX 2.1 specifications.
<https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>

[OASIS TAXIIv2] OASIS TAXII 2.1 specifications.
<https://docs.oasis-open.org/cti/taxii/v2.1/cs01/taxii-v2.1-cs01.html>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 botnet [b-ITU-T X.1231]: Remotely controlled malicious software robots (bots) that are run autonomously or automatically on compromised computers together with a command-and-control server owned by bot masters.

3.1.2 fraud [b-ITU-T Y.140.1]: The act of acquiring pecuniary advantage by misrepresentation or unauthorized action.

3.1.3 malware [b-ITU-T X.1211]: Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

3.1.4 phishing [b-ITU-T X.1244]: An attempt to acquire criminally and fraudulently sensitive information, such as usernames, passwords and financial account details, by masquerading as a trustworthy entity in an electronic communication.

3.1.5 vulnerability [b-ITU-T X.1524]: Any weakness in software that could be exploited to violate a system or the information it contains.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 data cleaning: A process to delete irrelevant data and duplicate data in the original data set, to smooth the noise data, and process missing values and outliers.

3.2.2 data clipping: A process to clip useless or abnormal data.

3.2.3 data deduplication: A process to delete duplicate data in the original data set.

3.2.4 data desensitization: A process to hide the sensitive data.

3.2.5 data filtering: A process to delete irrelevant data and filter the unrelated data in the original data set.

3.2.6 data mapping: A process to map data elements from the source data system to the destination data system.

3.2.7 data merging: A process to merge the similar data records into one record.

3.2.8 data mining: A computational process to discover patterns in large data sets involving methods of artificial intelligence, machine learning, statistics, and database systems.

3.2.9 data noise reduction: A process to smooth the noise data.

3.2.10 data sampling: A statistics technique used to process missing values and outliers.

3.2.11 data segmentation: A process to segment data from different levels.

3.2.12 data sorting: A process to sort data in a certain order or category.

3.2.13 data transforming: A process to transform data to a certain format and scale the data to a specified range.

3.2.14 incidents collecting: A process to collect data about security incidents.

3.2.15 situation awareness: A process to display the overall situation and predict possible threats and attacks.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CVE	Common Vulnerabilities and Exposures
C&C	Command and Control
DDoS	Distributed Denial of Service
DNS	Domain Name System
FW	Firewall
GW	Gateway
HTTPS	Hypertext Transfer Protocol Secure
ID	Identity
IDS	Intrusion Detection System
IP	Internet Protocol

MD5	Message Digest Algorithm 5
IPS	Intrusion Prevention System
O&M	Operations and Maintenance
SDN	Software Defined Network
SIEM	Security Information and Event Management
SoC	Security Operation Centre
STIX	Structured Threat Information expression
TAXII	Trusted Automated exchange of Intelligence Information
URL	Uniform Resource Locator
WAF	Web Application Firewall

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of threat intelligence

Threat intelligence from a telecommunication operator's point of view is a collection of organized, analysed and refined information about potential and current attacks that may threaten an organization. This information can also include attackers' motivations, intentions, characteristics and methods, along with their modus operandi or techniques, tactics and procedures.

In telecommunication network operation, threat intelligence is knowledge that is used to prevent or mitigate cyberattacks, including attackers' motivations, intentions, characteristics, methods, operandi, techniques, tactics and procedures. It is not related to personal identifiable information.

In the area of network and information security, the occurrence of large-scale and unexpected cybersecurity incidents has triggered the urgent need for threat intelligence. Threat intelligence can help an organization reduce risk and improve overall security by understanding who is most likely to attack, what they will attack, what they want to accomplish, why they want it, and how they plan to do it.

[OASIS STIXv2] defines a language and serialization format used to exchange cyberthreat intelligence. [OASIS TAXIIv2] specifies a protocol used to exchange cyberthreat intelligence over HTTPS. [ITU-T X.1215] presents how the structured threat information expression (STIX) language may be used to support cyberthreat intelligence and information sharing.

A unified taxonomy, grammar and presentation of threat intelligence has been defined so that threat intelligence can be shared between different organizations. The next problem that needs to be taken into consideration is how to use the threat intelligence to solve security problems in the network.

[OASIS OpenC2-L] specifies a command and control (C2) language for controlling cybersecurity functions. [OASIS OpenC2-H] specifies a HTTPS API to transport OpenC2 commands to cybersecurity devices. [OASIS OpenC2-P] specifies the use of the OpenC2 language for controlling stateless firewalls. Profiles for other cybersecurity functions are under development in OASIS.

7 Overview of applying threat intelligence in telecommunication network operation

Figure 7-1 shows how threat intelligence is applied in telecommunication network operation.

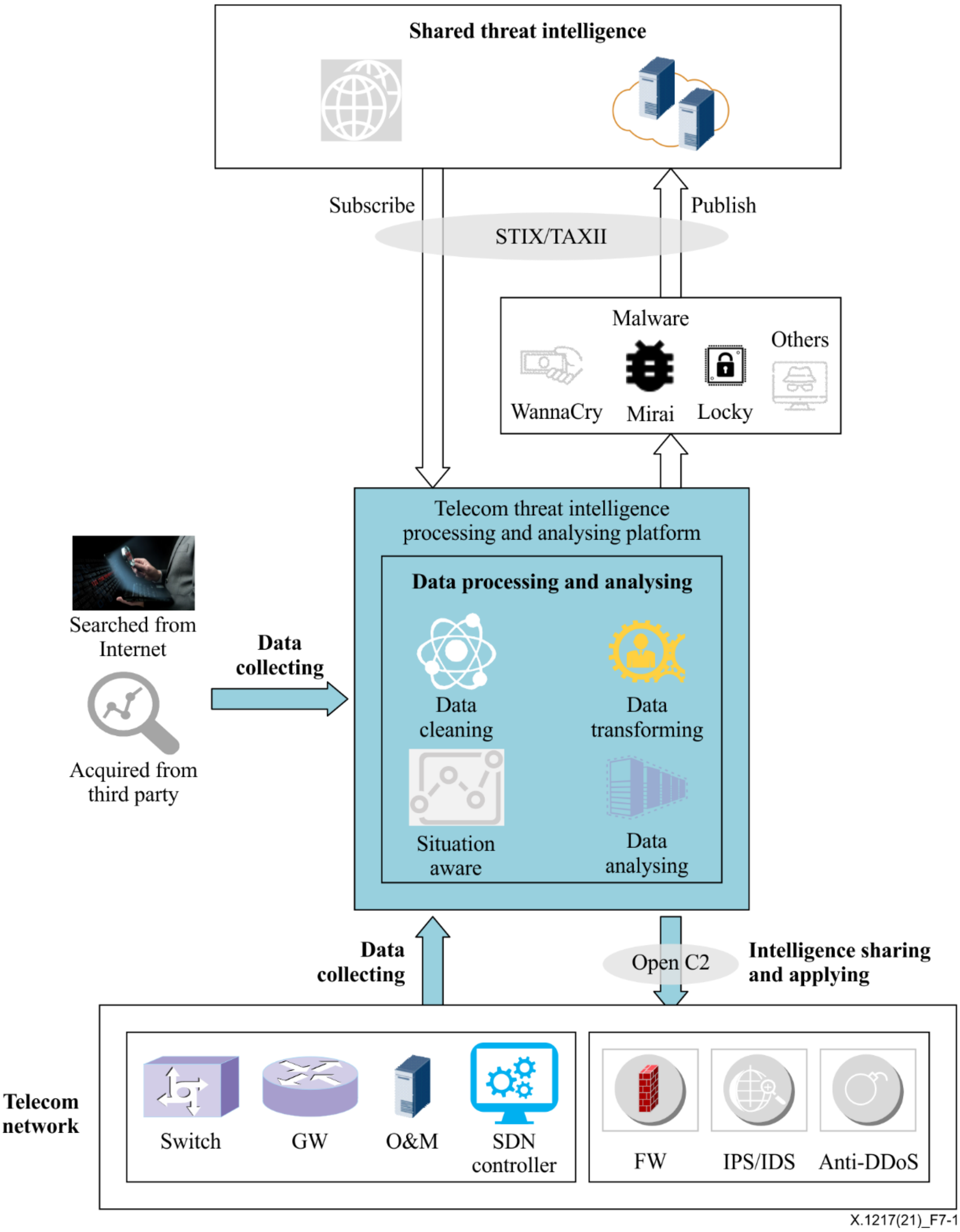

Figure 7-1 – Applying threat intelligence in telecommunication network operation

According to Figure 7-1, applying threat intelligence in telecommunication network operation includes three main processes: data collecting, data processing and analysing, and intelligence sharing and applying.

7.1 Data collecting

There are two kinds of threat intelligence data sources:

- data from internal network elements and security devices;
- data from outside sources.

The data from internal network elements and security devices mainly includes the logs, alerts and security policies, such as incident logs, domain name system (DNS) logs, firewall logs, etc.

There are some specific sources to collect data from outside, such as searching via the Internet, acquisition from third parties via STIX/TAXII, etc. The shared data mainly includes IPs, domains, URLs, incidents, vulnerabilities, etc.

Data desensitization is required to be performed before the data is collected.

7.2 Data processing and analysing

Data processing and analysing includes four function components: data cleaning, data transforming, data analysing, and situation awareness.

Figure 7-2 illustrates the function components of data processing and analysing.

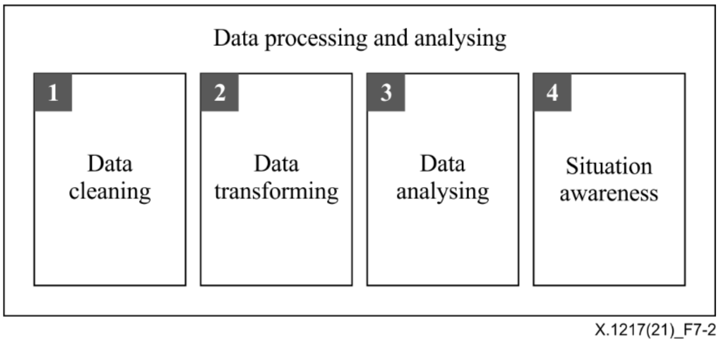

Figure 7-2 – Function components of data processing and analysing

- Data cleaning deletes irrelevant data and duplicate data in the original data set, smooths the noise data, and processes missing values and outliers.
- Data transforming includes data integration and data normalization:
  - Data integration is to unify storage of multiple data sources in a certain format.
  - Data normalization is to eliminate the influence of the dimension and the range of values between indicators, and scale the data to a specified range, including function transformation and attribute construction, etc.
- Data analysing uses various algorithms to analyse the data, extract keywords, clear rules, correlate analysis to obtain threat intelligence information, and analyse the corresponding countermeasures.
- Situation awareness includes visualization and predictive warning:
  - Visualization is a visual display of the overall situation through the analysed data, such as categorization, sorting, and so on.
  - Predictive warning refers to predicting the possible range of threats, attack paths, attack methods, etc., through data analysis and overall situation, and issuing early warnings to give security strategies to defend against possible attacks.

7.3 Intelligence sharing and applying

Intelligence sharing and applying includes two aspects:

- According to the threat intelligence, operation and maintenance administrators can deploy security policies to network elements and security devices.
- The threat intelligence can be shared with third parties.

Threat intelligence for sharing and applying in telecommunication network operation includes threat intelligence information, predictive warning information, network security countermeasures, etc.

The objects of intelligence sharing and applying in telecommunication network operation include network elements and security devices, such as intrusion detection system (IDS), intrusion prevention system (IPS), firewalls and anti-DDoS devices. When it comes to applying security command and control in security devices, it is recommended to use OASIS OpenC2 specifications.

The goal of intelligence sharing and applying in telecommunication network operation is to prevent and reduce security incidents and at the same time achieve a prompt and efficient response to each security incident in the telecommunication network.

8 Guidelines for applying threat intelligence in telecommunication network operation

Clause 7 describes three main processes, data collecting, data processing and analysing, intelligence sharing and applying for applying threat intelligence in telecommunication network operation. Guidelines for applying threat intelligence in telecommunication network operation are specified accordingly in clauses 8.1 to 8.3.

8.1 Data collecting

Data collecting is the precondition of applying threat intelligence, and the purpose is to collect all the threat intelligence related information and data. The data is recommended to include data from internal network elements and security devices, e.g., logs, alerts and security policies. Meanwhile, the data is recommended to include data from outside sources, such as data searched via the Internet, data acquired from third parties, and so on. The shared data mainly includes IPs, domains, URLs, incidents, vulnerabilities, and so on.

Active data collecting is recommended to be implemented to collect data such as DNS logs, firewall logs, and so on. Incidents collecting is recommended to be taken to collect data about security incidents. Intelligence collecting is recommended to be taken to collect critical intelligence, such as IPs, domains, URLs, incidents, vulnerabilities, and so on.

If the data is collected from internal network elements and security devices, data collecting can be implemented according to different types such as incident information or botnet activity.

The incident information can be collected from an IDS device, IPS device, web application firewall (WAF), anti-DDoS device, security information and event management (SIEM) platform and security operation centre (SoC) platform. The collected incident information is recommended to include the name, description, category, and affected assets of the incident. The time when the incident happens is recommended to be included. The botnet activity can be collected from DNS devices, IDS, WAF, anti-DDoS devices, etc. The collected botnet activity information is recommended to include the name, description, category and affected assets of the botnet activity. The time when the botnet activity happens is recommended to be included.

If the data is collected from the Internet, data collecting can be implemented according to different types such as vulnerabilities information, malicious domains, malicious URLs, malicious IP addresses, incident information, etc.

The vulnerability information can be collected from vulnerability websites, such as common vulnerabilities and exposures (CVE) websites. The collected vulnerability information is recommended to include the ID, name, description, type, affected versions, affected vendors, affected products of vulnerability, etc.

The malicious domain and URL information can be categorized as different threat types of command and control (C&C), botnet, malware, trojan code, phishing, fraud, etc. The malicious domain and URL information can be collected from websites, vendors' reports, third party's security reports, etc. The collected malicious domain and URL information is recommended to include domain name server, DNS type, threat type, credit level, etc.

The malicious IP address information can be collected from various websites and some vendors and security companies, etc. Malicious IP addresses can be categorized as different threat types of DDoS, exploits, spam source, web attack, botnet, malware, C&C, etc. The collected malicious IP information is recommended to include IP, threat type, credit level, etc.

The incident information can be collected from security news or vendors' reports. The collected incident information is recommended to include the name, description, category and affected assets of incident.

The data acquired from third parties mainly includes IPs, domain names, URLs, incidents, vulnerabilities, and so on. The information of each type is the same as that of the above.

Data collecting is recommended to be implemented by automated tools or scripts, when the data is collected from internal network elements and security devices. Data collecting is recommended to be obtained by using scripts or by a data exchanging and sharing mechanism, when the data is collected from outside sources. Subsequent processing of the collected data is recommended to follow the standard format defined by [OASIS STIXv2] and [OASIS TAXIIv2]. For the shared threat intelligence, data collecting is recommended to follow the standard format defined by [OASIS STIXv2] and [OASIS TAXIIv2].

Data desensitization is recommended to be performed before data collecting, as data desensitization is the process of hiding the original sensitive data with characters or data, for the purpose of protecting the sensitive data.

8.2 Data processing and analysing

8.2.1 Data cleaning

Data cleaning is one of the main steps of applying threat intelligence, and the purpose is to clean the collected data to make it uniform and useful data and to get prepared for the data transforming and data analysing part.

– It is recommended to implement data filtering, data noise reduction and data deduplication.

– It is recommended to implement data filtering, delete irrelevant data and filter the unrelated data in the original data set.

– It is recommended to implement data noise reduction and data deduplication to smooth the noise data and delete duplicate data in the original data set.

Since the collected data contains different kinds of data, such as the IPs, domains, URLs, incidents, vulnerabilities, and so on, data cleaning can be different according to the collected data.

The data deduplication mainly deletes the duplicate data to save storage space. The criteria for different data types are different. For the data of IP information, if IP address is the same and the other parts of the record such as threat type, credit level are the same, then it is duplicate data and needs deduplication, otherwise it needs merging. As for domain information, if all the records of domain name server, DNS type, threat type and credit level are the same, then it is duplicate data and needs deduplication, otherwise it needs merging. For the vulnerability information, if the vulnerability ID is the same, then it is duplicate data and needs deduplication. For the data of some other types, the similarity rate is recommended to be computed, if the similarity rate is higher than the threshold, then it needs deduplication.

The similar information is recommended to be merged into one record. For the types of IP, domain, URL and incident information, if the IP, domain name server, URL and incident description is the same as another one, then they can be merged into one record. For some other data types, the similarity rate can be computed. If the similarity rate is within the threshold, then the information needs to be merged.

– It is recommended to implement data sampling, data merging and data sorting to process missing values and outliers and to make data more useful for the latter process.

– It is recommended to use automated tools for data filtering and data deduplication.

8.2.2 Data transforming

Data transforming is to eliminate the influence of the dimension and the range of values between indicators, and scale the data to a specified range, including function transformation and attribute construction, etc., and to transform the cleaned data to the unified format data, getting prepared for data analysing.

To implement data transforming, it is recommended to use data mapping, data clipping and data segmentation to change the data to useful data with value. Spelling conversion is recommended to convert different spellings to the unified spelling. Format standardization is recommended to make the data of multiple data sources in a certain format. Data convergence is recommended to make unified storage of multiple sources.

The data transforming procedures for each type of IP, domain, URL and incident vulnerability are similar. Data mapping rules are recommended for each type, which can be different according to the data type. For example, the data mapping rule for the incident information is to transform the name, description, category and affected assets field into standard format fields. The firewall (FW) information such as map timestamp, request URL, host name, attack type, attack content are recommended to be mapped to the defined format.

For data clipping and data segmentation, the process of data transforming is recommended to be implemented by automated tools. For spelling conversion, the process of data transforming is recommended to be implemented by automated tools. For format standardization, the process of data transforming is recommended to follow the standard format defined by [OASIS STIXv2] and [OASIS TAXIIv2].

8.2.3 Data analysing

Data analysing is the critical step for applying threat intelligence to use various algorithms to analyse the transformed data, extract keywords, clear rules, correlate analysis, etc., to obtain threat intelligence information, and analyse the corresponding countermeasures.

To implement data analysing, data retrieval and data mining is recommended to obtain key threat intelligence information so as to create warnings or the corresponding countermeasures. Behaviour analysis and incident correlation analysis is recommended to be taken, so as to find the useful threat intelligence, such as IP address, domain name, hash digest, attacker information, response action, and so on. Knowledge mapping and threat hunting is recommended to be taken to hunt deep threat intelligence information and take countermeasures and responses.

For example, the machine learning algorithm for DNS logs can be used to detect botnet C&C. The FW logs are recommended to be combined with the threat source, type, attack time and other information to compute threat level. The URL and IP information can be used to compute the reputation level.

The data analysing algorithms are recommended to be conducted automatically. The result of data analysing is recommended to follow the standard format defined by [OASIS STIXv2] and [OASIS TAXIIv2].

8.2.4 Situation awareness

Situation awareness uses the analysed data to make trend predictions and warnings and at the same time display the overall situation.

To implement situation awareness, situational visualization is recommended to make the display of the overall situation through the analysed data. Trend prediction and warning is recommended to be used to predict the possible range of threats, attack paths, attack methods, etc., through data analysis and the overall situation, and for issuing early warnings to provide security strategies to defend against possible attacks. The situation awareness method is based on algorithms including machine learning, linear analysis, probability statistics and artificial intelligence.

Trend prediction and warning is recommended to be conducted automatically. The trend prediction and warning results are recommended to follow the standard format defined by [OASIS STIXv2] and [OASIS TAXIIv2]. For situational visualization and display, it is recommended to display the overall data situation using visualization tools.

8.3 Intelligence sharing and applying

The purpose of intelligence sharing and applying is to prevent or reduce security incidents, and to achieve a prompt and efficient response to each security incident in the telecommunication network.

The intelligence obtained from the data processing and analysing phase, including threat information, predictive warning information, network security countermeasures, security policies, etc., could be shared with different departments and communities of telecommunication operators. The intelligence could be shared in several forms. For example, it could be shared in the form of reports and advisories or it could also be shared in the form of detection indicators.

It is recommended to obtain intelligence from network elements, security devices and warning centres, etc. The operation and maintenance administrators could generate security policies according to the intelligence obtained, and deploy these security policies into network elements and security devices. The administrators could also update software versions, and modify the configuration of the network elements and security devices, if necessary.

The URL type intelligence is recommended to be applied to the gateway, and then the gateway could update its security policy by filtering malicious URLs to a blacklist. It is recommended to be applied to IDS or IPS by updating protection rules using corresponding URLs.

The malicious domain type intelligence is recommended to be applied to the DNS server, which could update the configuration by setting the malicious domain to a blacklist.

The malicious IP type intelligence is recommended to be applied to the firewall and the firewall could update its security policy by filtering the malicious IP address. It can also be applied to IDS or IPS by updating protection rules using corresponding IP address.

The vulnerability type intelligence is recommended to be applied to network elements, which could fix the vulnerabilities by updating the software or hardware. Meanwhile, it can optionally be used for making detection plug-ins, and then be used to update the detection scanner. The intelligence can optionally be applied in an emergency response system to identify the incidents and help to take action to prevent attacks.

The intelligence is recommended to follow the standard format defined by [OASIS STIXv2] and [OASIS TAXIIv2]. Security command and control is recommended to use OASIS OpenC2 specifications.

Bibliography

[b-ITU-T X.1211] Recommendation ITU-T X.1211 (2014), *Techniques for preventing web-based attacks*.

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam*.

[b-ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

[b-ITU-T X.1524] Recommendation ITU-T X.1524 (2012), *Common weakness enumeration*.

[b-ITU-T Y.140.1] Recommendation ITU-T Y.140.1 (2004), *Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021