ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1236 (11/2023)

SERIES X: Data networks, open system communications and security

Cyberspace security – Countering spam

Security requirements and countermeasures for targeted email attacks

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	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
Cybersecurity	X.1200-X.1229
Countering spam	**X.1230-X.1249**
Identity management	X.1250-X.1279
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	X.1800-X.1819

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

Recommendation ITU-T X.1236

Security requirements and countermeasures for targeted email attacks

Summary

Recommendation ITU-T X.1236 specifies requirements for security features to block inbound and outbound email attacks in the form of multilevel management that includes countermeasures against targeted email attacks. This approach is necessary to integrate or deploy a new framework to improve Internet user defence against such attacks. Recommendation ITU-T X.1236 forms a reference on the direction and objectives of designing an email security diagnostic framework or developing email security solutions with those security functional requirements for information technology (IT) security managers, especially in those countries beginning to be actively engaged in IT development and implementation.

Targeted email attacks are designed to damage or compromise information assets of an entity by establishing a connection with the targets after gathering sufficient resources to conduct an attack and then enticing them to take certain actions that eventually create a security loophole. These targeted attacks used in inbound and outbound emails are evolving into more sophisticated and unknown types, such as using unknown malicious files or capitalizing on the target's social relationships. However, so far there are no security requirements proposed to effectively prevent or block them.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1236	2023-11-13	17	11.1002/1000/15710

Keywords

Countermeasure, security requirement, targeted email attack.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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 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

Cyberattacks via email have gradually evolved in parallel with network attack techniques in modern society. Active Internet users and businesses around the world are being harmed by the increasing number of malicious specifically targeted email attacks, through complex cyberattack tactics using malware and social engineering.

These targeted email attacks are conducted on a specific person after setting an individual or company as a target, unlike spam phishing attacks launched on an unspecified number of people, to damage or compromise the information assets of the target entity. To conduct a targeted attack, threat actors gather information to craft a personalized email message that appears authentic to convince the target to respond to it, which eventually creates a security loophole. Targeted attacks used in inbound and outbound emails employ sophisticated and unknown methods such as attaching unknown advanced malware or impersonating normal senders whom the target trusts, by use of forged headers, similar email address, or account take-over.

As threat actors have such motives as misdirected money transfer, data breach and computer system failure, a target responding to their email by, for example, clicking on an attachment or sending a reply with personal information included, as intended by the threat actor, poses a hazard to the target's information assets.

Despite the severity of the risk posed, no security requirements are proposed to effectively prevent or block them. Therefore, this Recommendation specifies requirements for security features to block inbound and outbound email attacks in the form of multilevel management, which may be the most fundamental countermeasures against targeted email attacks.

Recommendation ITU-T X.1236

Security requirements and countermeasures for targeted email attacks

1 Scope

This Recommendation provides security requirements and countermeasures for targeted email attacks, and includes the following information:

- the characteristics of targeted email attacks;
- the technical procedure of inbound and outbound targeted email attacks;
- threats for targeted email attacks;
- security requirements for types of inbound and outbound emails involving elements of malware, social engineering, and threats by user and attacker to counter targeted email attacks;
- countermeasures against each type of email threat coming from inbound and outbound emails.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 targeted email attack: A sophisticated email attack that is delivered against a specific person after setting an individual or company as a target for defrauding and by having the person take a specific action that seems innocuous.

3.2.2 malware email filter: A set of email filtering functions to examine inbound emails including malware code for detecting and preventing parts of targeted email attacks through traditional techniques such as attachment file examination, examination utilizing virtual space and advanced malware examination.

3.2.3 social engineering email filter: A set of email filtering functions to examine inbound emails not including malware code for detecting and preventing parts of targeted email attacks through similarity examination based on training data and checking the change history for changed sender location, current and previous route, etc.

3.2.4 email security reporting system: A set of email security systems to provide security managers or users with an overview of inbound emails related to user email activity and status, such as, risk factors of email security threats.

3.2.5 outbound approval system: A set of email security functions through which an email transmission is approved by the designated assessor or based on pre-registered conditions set by the user.

3.2.6 outbound email filter: A set of email filtering functions to examine outbound emails and prevent their transmission if malicious elements such as malware or social engineering are detected.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ATO	Account Take-Over
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IP	Internet Protocol
IT	Information Technology
POP3	Post Office Protocol version 3
SMTP	Simple Mail Transfer Protocol
TLD	Top-Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator

5 Conventions

This Recommendation uses the following conventions:

The phrase **"is required"** indicates a requirement that must be followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The phrase **"is recommended"** indicates a requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the implementation must provide the option, and the feature can be optionally enabled. Rather, it means the feature may optionally be provided to information technology security managers while still claiming conformance with the specification.

6 Introduction of targeted email attacks

In this clause, general and detailed characteristics of targeted email attacks are described, and security technical procedures of targeted email attacks are illustrated. The types of targeted email attacks are those of email impersonation, zero-day malware, post malware and outbound email via account take-over (ATO). The security technical procedures of inbound and outbound targeted email attacks are shown.

6.1 General characteristics

Targeted email attacks include threats with or without malware. The detailed types of targeted email attack are described in clauses 6.1.1 to 6.1.4.

6.1.1 Zero-day malware attacks

Targeted email attacks mainly include using new malware that may be difficult to detect with general pattern recognition. For instance, through utilizing a zero-day vulnerability, malicious developers can create malware that uses a vulnerability before the corresponding security program can be developed and deployed. This means that malware exploiting vulnerabilities can spread widely before organizations can prevent the threat.

6.1.2 Post receipt malware attacks

An attacker sends an email to a recipient that includes attachments with an embedded malicious uniform resource locator (URL) [b-IETF RFC 2396], which may appear as legitimate during inspection. The malware within the URL becomes active upon the recipient clicking on it, when a virus or malicious software, such as spyware, can be installed without the user's knowledge. The email passes the inspection because the attacker inserts the malware after the email has been received. This can potentially enable the attacker to compromise sensitive information, destroy data and cause damage to hardware.

6.1.3 Outbound email attacks via account take-over

ATO is another type of targeted email attack stealing a user's account through inbound email attacks and leaking confidential information by sending email through the accounts. For example, say company A and company B exchange confidential information. If attackers steal company A's employee account using malware, then they could compromise both company A's and company B's confidential information that is stored in company A's account. However, company B cannot recognize that company A's employee account has been compromised.

6.1.4 Email impersonation attacks

Targeted email attacks can take place in a form that impersonates legitimate senders. Examples include an ATO attack, the action with a stolen account directly to impersonate a legitimate sender or modifying the address of receiving replies in the header after falsifying the originating address to make it look like a domain with which the user is used to exchanging emails. This might mislead users into sending emails to an address that looks like one that is familiar.

6.2 Security technical procedure for targeted email attacks

Figure 1 is a conceptual diagram of a multilevel management security system applicable to inbound emails. This system blocks targeted email attacks, including those involving malware and social engineering, through the use of a malware email filter, social engineering email filter and an email security reporting system.

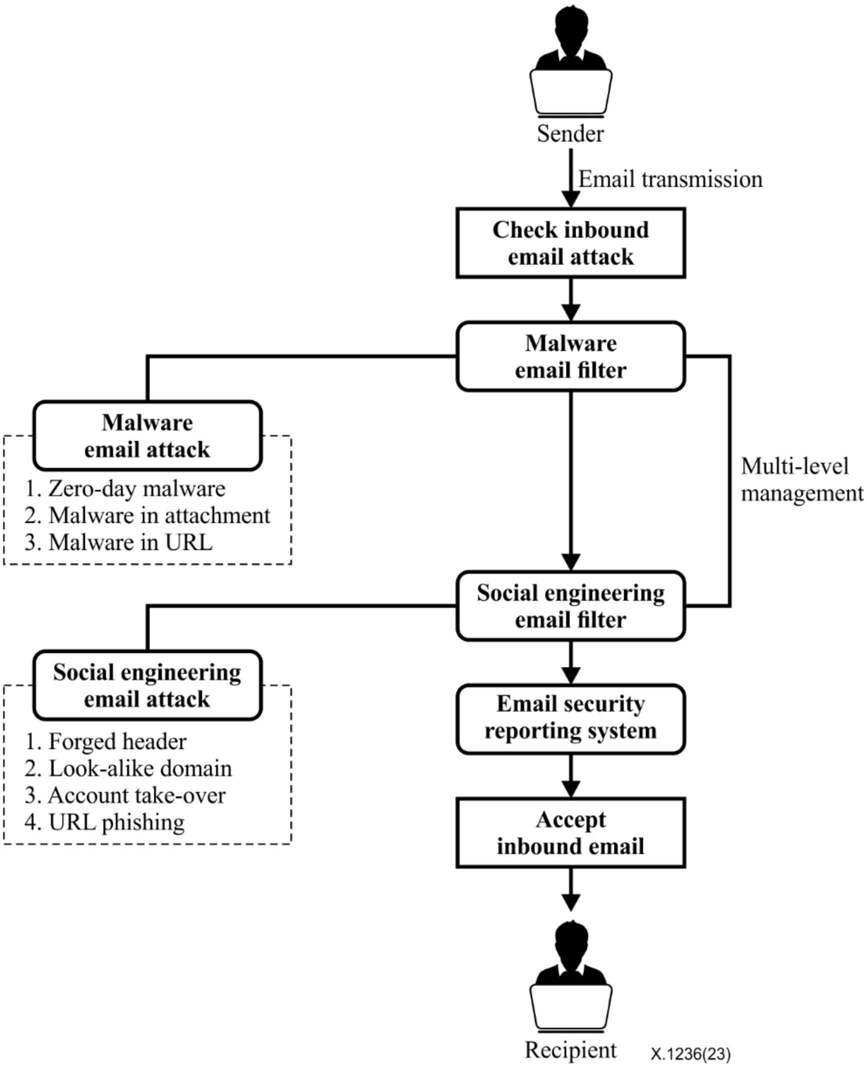

Figure 1 – Security technical procedure of inbound targeted email attack

Figure 2 illustrates a conceptual diagram of a security system applicable to outbound emails. This system performs several types of inspection and blocks targeted email attacks through an outbound approval system and an outbound email filter.

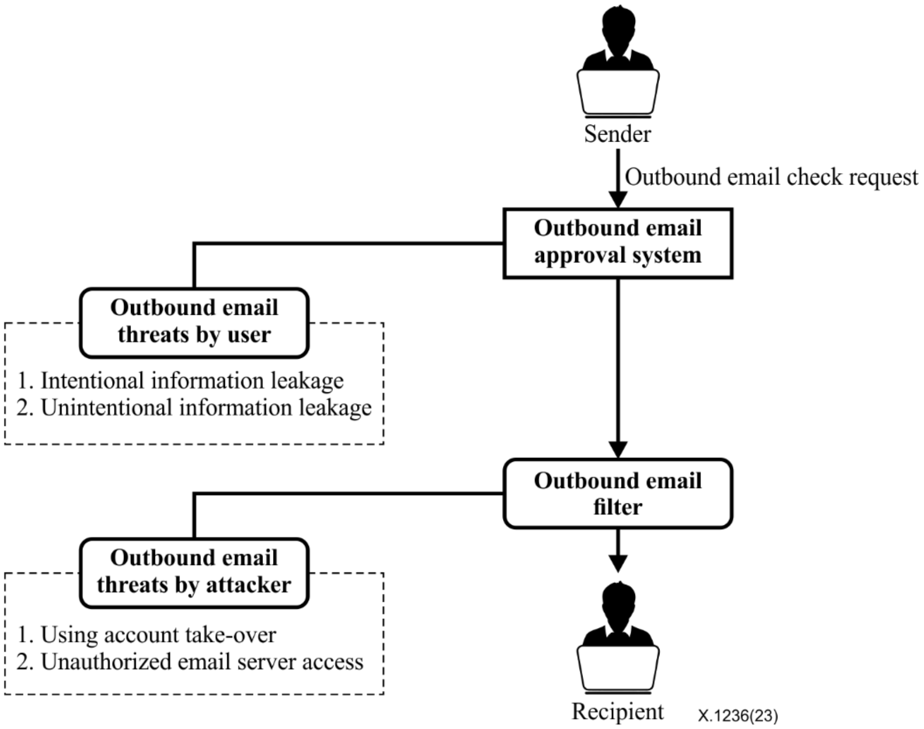
Sender
Outbound email check request
Outbound email approval system
Outbound email threats by user
1. Intentional information leakage
2. Unintentional information leakage
Outbound email filter
Outbound email threats by attacker
1. Using account take-over
2. Unauthorized email server access
Recipient
X.1236(23)

Figure 2 – Security technical procedure of outbound targeted email attack

The technical security procedures shown in Figures 1 and 2 consider targeted email attacks and their countermeasures for both incoming and outbound emails. Figures 1 and 2 also give extended information applicable to approved ITU-T Recommendations related to security requirements for countering targeted email attacks. The Recommendation has been developed to identify whether individuals can utilize technical countermeasures against sophisticated forms of email attack recognizable because of the use of various types of patterns of malware and social engineering shown in Figures 1 and 2.

7 Threats for targeted email attacks

7.1 Malware email attacks

7.1.1 Zero-day malware

As zero-day malware is not registered in a big data database, unknown malware used by an attacker is difficult to detect in a security system. The vulnerability of zero-day is exploited to insert an attachment or a clickable link containing unknown malware that the security system cannot detect, and send an email that induces users to click when they should not. Zero-day malware may access memory on a victim's computer system to damage or delete files and programs.

7.1.2 Malware in an attachment

A malicious attachment is one type of threat in which attackers conceal malware inside commonly emailed files. The attachments within these malicious emails can be disguised as documents, executable files or even image and video files. These files can also be encrypted with other extensions. Attacks using executable files may involve spoofing the sender's address to deceive the recipient into opening emails with malicious documents.

7.1.3 Malware in uniform resource locator

A malicious URL attack is made by inserting a clickable link containing malware in emails for the purpose of inducing users to visit malicious websites. Also, malicious URLs can be contained in a large attachment or in the body of an email. This can be an attack that causes malware to be executed when a user clicks on a URL in an email or regular attachment, not only at the time of delivery.

7.2 Social engineering email attacks

7.2.1 Forged header

One type of social engineering attack involves scammers dodging detection by forging account information in a header. Attackers use email header forgery to bypass the destination of emails when a user sends a reply. Through a forged header attack, attackers are able to intercept emails from normal users that may contain information relating to a company's credentials and personnel.

7.2.2 Look-alike domain

A look-alike domain is a type of attack where attackers send a malicious email from an email address that on cursory visual examination is remarkably similar to that of a normal, familiar sender. For example, capital 'I' and lower case 'l' letters are similar in appearance and this similarity can be abused in an attack.

7.2.3 Account take-over

ATO is a social engineering attack that uses the account of a real user. After attempting to log in to the stolen email account to browse the email history of the user, the attacker finds confidential information and potential secondary victims. For example, account information stolen from a phishing site can be used by an attacker to send an email asking for remittance account changes or to deliver confidential information stored in the account to an external party.

7.2.4 Uniform resource locator phishing

URL phishing is the theft of the identifier (ID) and password of a victim, in which the attacker creates a phishing page or website to induce the victim to enter account information through the use of a malicious URL or file embedded in an email.

7.3 Outbound email threats by user

7.3.1 Intentional information leakage

Intentional information leakage is a method in which employees purposely leak corporate confidential information or employee personal information to external parties through business or personal email due to the absence of in-house security policies.

7.3.2 Unintentional information leakage

Unintentional information leakage can be caused by carelessness or negligence of employees. When account users send emails with a large attachment from an isolated internal network to an external party, if the attached files contain crucial corporate or personnel information by mistake, this can cause serious information leakage issues.

7.4 Outbound email threats by attackers

7.4.1 Using account take-over

The method of outbound email attack generally begins after a user's account is stolen. Attackers randomly send follow-up emails exploiting the personal information of others in the user's inbound and outbound emails through the stolen account. Accounts related to attacked users will potentially be secondary victims and later reused in phishing attacks.

7.4.2 Unauthorized email server access

Unauthorized email server access is a method of outbound attack where an attacker gains control of the server. The attacker may gain unauthorized access to a user company email account with stolen account credentials. For example, once an email server is compromised, the attacker can retrieve user passwords, which may grant the attacker access to other hosts on the organization's network.

8 Security requirements to counter targeted email attacks

– Email body examination in security requirements should be done with user permission when necessary.

– Email security aspects relating to users or /attackers in clause 7 are covered in this clause.

8.1 Security requirements to counter malware email attacks

8.1.1 Security requirements to counter zero-day malware attacks

– It is required to conduct a behaviour-based analysis inspection to detect new viruses that are not registered in patterns in order to counter threats of new malware attacks.

– It is required to report an explanation of the behaviour of the newly found or detected malware, via a manual or automated process.

8.1.2 Security requirements to counter malware in attachment attacks

– It is recommended to detect a forged file extension in various file formats.

– It is recommended to provide email reputation analysis.

8.1.3 Security requirements to counter malware in uniform resource locator attacks

– It is required to trace the final destination of URLs within multiple linked URLs while checking all URLs for malware.

– It is required to check a post-URL to prevent malware attacks when users execute URLs after receiving email.

– It is recommended to disable opening a URL link to prevent a user from clicking on malicious URLs by mistake.

8.2 Security requirements to counter social engineering email attacks

8.2.1 Security requirements to counter forged header attacks

– It is required to block or warn users if the email address to be replied to is different when replying to an inbound email.

– It is recommended to verify compliance with the email communication protocol.

8.2.2 Security requirements to counter look-alike domain attacks

– It is required to inform a user of the level of risk similarity when the sender's domain is detected as a similar domain based on accumulated email history and to block such emails.

– It is required to apply the difference in the number of email addresses as a criterion for judging fraudulent look-alike email attacks.

– It is required to manage it separately if the top-level domain (TLD) is different.

– It is recommended to enable security managers to directly register fraudulent look-alike email addresses that look suspicious.

8.2.3 Security requirements to counter account take-over attacks

– It is required to warn users or block emails when the sender location is different from that of emails previously received.

– It is required to warn users or block emails when the Internet protocol (IP) [b-IETF RFC 6864] address of the email server is different from that of emails previously received.

- It is recommended to warn users or block emails when the sending route of emails is different from that of emails previously received.

8.2.4 Security requirements to counter uniform resource locator phishing attacks

- It is required to continuously track the final destination of an URL that contains a web page inducing personal information input.

8.3 Security requirements to counter outbound email threats by user

8.3.1 Security requirements to counter intentional information leakage

- It is recommended that security managers be able to set conditions for email dispatch.
- It is recommended to have the ability to reconsider email sending if the condition set is not satisfied.

8.3.2 Security requirements to counter unintentional information leakage

- It is required to issue a warning or automatically block users from replying to or sending emails to an email address that has been classified as malicious.
- It is required to convert large attachments within an email to regular ones when transmitting the email from the isolated internal network to the external network.
- It is required to retrieve converted emails with large attachments after safe delivery from an isolated internal network to an external network.
- It is required to allow senders to recall sent emails in order to prevent data leakage.
- It is recommended to encrypt contents of outbound emails that meet certain conditions, such as the IP address that checked emails and the number of times emails were opened.

8.4 Security requirements to counter outbound email threats by attacker

8.4.1 Security requirements to counter attacks using account take-over

- It is recommended to allow security managers and users to configure specific IP addresses and countries for accessing email accounts.
- It is recommended to implement malware detection in the same way as the inbound email security requirements are implemented in the clause 8.1 when sending an email.

8.4.2 Security requirements to counter unauthorized email server access attacks

- It is required to block unregistered simple mail transfer protocol (SMTP) [b-IETF RFC 2821] and country access to webmail services.
- It is required to ascertain detailed information about access in order to detect unauthorized email server attacks, and prevent the unauthorized email server from forwarding access requests to the email server.
- It is required to block mail delivery if sender SMTP information does not match that of the recipient.

8.5 General security requirements to counter targeted email attacks

8.5.1 Common security requirements to counter targeted email attacks

- It is required to synchronize between inbound and outbound inspections for collected malicious files and account data.
- It is required that the folder structure of the email security system be periodically changed manually or automatically.
- It is recommended to inspect emails for malware detection, even if the emails are included in whitelists.

- It is recommended to monitor malicious ATO attempts for users, security managers and the web.

8.5.2 Security requirements for an email security reporting system

- It is required to provide to users a report to verify whether emails received are secure before opening.
- It is required to provide a diagnostic report based on the data collected on the current status of email security of domains or servers.
- It is required to provide calculated risk results of all inbound emails as well as to display the result with the email.
- It is recommended to provide security managers and users of information about blocked fraudulent emails on a regular basis.
- It is recommended to include a warning message in the subject line to users when forwarding an email with security issues.
- It is recommended to restore emails detected as false-positives in the security inspection process.

9 Countermeasures for targeted email attacks

Security requirements for targeted email attacks as described in clause 8 can be implemented through the methods and processes described in clauses 9.1 to 9.5.

9.1 Countermeasures for malware email attacks

9.1.1 Countermeasures for zero-day malware

- **Malware classification management** allows security managers to configure emails identified as malicious files and viruses cannot be delivered even if the user requests retransmission.
- **Multianalysis inspection** detects unknown malware that is not detected in primary testing by environmental operating system change testing, which scans the behaviour of malware against the system with a combination of static and dynamic testing. Behaviour results are, for instance, divided into: forgery; memory access; hooking warning; create file; delete file; or run process.

9.1.2 Countermeasures for malware in attachment

- **Big data-based inspection** scans all inbound and outbound email data of users on a regular basis via cloud service to extract malicious attachments that require further inspection. It determines whether there is a risk of targeted email attacks based on the data stored in the big data system. This feature identifies and detects a forged file extension.

9.1.3 Countermeasures for malware in uniform resource locator

- **URL image conversion** disables opening a URL link in a perceived dangerous environment where the attached malicious URL is recognized.
- **Endpoint URL monitoring** continuously tracks the final destination of all URLs within the body or document file of email by monitoring potential hazards. For instance, large attachments that are downloaded by bypassing the URL in the body of the email should be able to track down all URLs for malicious attachments or document files after download.
- **URL post testing** re-inspects the access of URL in real time through file and endpoint scanning when the user attempts to click the URL links after receiving the email, and restricts access when a risk is detected.

9.2 Countermeasures for social engineering email attacks

9.2.1 Countermeasures for forged header attacks

- **Email header information** analyses to check whether the sender header value (From: <id@domain>) and the reply address header value (Reply-To: <id@domain>) of the inbound email are the same or different. It determines which part of each header value is different and provides a filtering result.
- **Communication protocol authentication** detects forged sender addresses in email through validation of the sender's email as to whether it complies with communication protocols (e.g., sender policy framework, domainkeys identified mail [b-IETF RFC 6376]). It manages the sender reputation of the IP address and domain, as well as validating whether the email addresses have a reliable domain.

9.2.2 Countermeasures for look-alike domain attacks

- **Domain similarity calculation** accumulates the sender domain of inbound emails and then compares and analyses the newly received email with it. It could be able to block similar domains of three characters or fewer that are difficult to identify. Inbound emails are suspended or blocked when the TLD is modified or when there is reordering in an array of strings or change with one of the strings into a similar letter or character, creating a set of strings. Determination of domain similarity based solely on a simple difference in the number of characters is not recommended, as this can lead to false positives.

9.2.3 Countermeasures for account take-over attacks

- **Email data for the same sender** should be learned and then learning data and validation should be performed by analysing the received email in real time.
  a) Learning data validation: Learn the configured header structure and social graph, and compare and analyse past learning records and current data when sending an email.
- **Sender location change detection** analyses the header information of the inbound email to accumulate the sender location IP history, and compares the newly received email with the sender location IP country of the accumulated history. The email header includes the IP where the email was first written, the IP of the server through the time of delivery, and the IP information of the server where the email was finally sent. It accumulates the IP history of destinations of all inbound emails (first destination, waypoint, final destination) and detects the authenticity of the sender if the country of the new inbound email sender location IP differs from the previous inbound email.

9.2.4 Countermeasures for uniform resource locator phishing attacks

- **Endpoints of URL tracking**: The potential for information input guidance should be monitored by tracking to the final destination of all URLs.
- The **hypertext markup language source code** of a web page should be analysed to check whether there is an input text box that induces users to provide their personal information or account information such as IDs and passwords, and inspect whether the input information is delivered to a third-party server.

9.3 Countermeasures for outbound email threats by user

- **Secure email**: Instead of sending an actual email to the recipient, the system sends a secure message with a link to view the email information (e.g., sender, title) in advance, e.g., on a secure web portal. At this time, the user should be able to manage the sent secure email.
- **Approval email** enables approvers to configure identity applications to send an email that notifies users when there is a pending task to approve or reject permission requests. If a specific keyword and attachment type are included in the email, the approver sets up an

approval process according to the organization chart. Such emails can be sent when approvers allow or reject the transmission of emails containing a particular keyword that requires approval in the subject, attachment or file extension.

- **Email delivery restriction** allows a limit to be set for the maximum number of emails that can be sent at once to maintain the email server status and security of account by limiting the number of emails users can send per day and the number of recipients per email.

9.3.1 Countermeasures for intentional information leakage

- **Outbound blocking policy** establishes an outbound policy tailored to the enterprise to block attempts to leak information and data through email. The blocking policy conditions are as follows:

  a) capacity limitations: attachments, outbound email capacity (block large data leakage attempts), large files;

  b) limitation of image size within email body;

  c) potential set target exception sender list;

  d) keyword: forms of numbers or words reflect personal information;

  e) attachment: filename, file extension.

- **Outbound email delay and retrieval or deletion**: a delay is recommended to be set between the time of email dispatch and delivery, and it should be possible to cancel email dispatch during the delay period. The right to cancel email within the delay time is granted to security managers and users; once cancelled the sent email cannot be re-delivered, and the email must be rewritten.

9.3.2 Countermeasures for unintentional information leakage

- **Email encryption** protects sensitive information from being read by anyone other than the intended recipient by encrypting or disguising the contents of email and attachments.

- **Email convert conditions**: To safely transmit emails with large attachments from an isolated internal network to an external network, it is necessary to meet the following conditions for converting those emails.

  a) Examination of security risks for large attachments inserted to be classified as general attachments according to pre-set email transmission policies.

  b) Enablement of the ability to forward converted emails after approval.

- **Email retrieve conditions**: To safely transmit emails with large attachments from an isolated internal network to an external network, it is necessary to meet the following conditions for retrieving converted emails.

  a) Examination of security risks for large attachments inserted to be classified as general attachments according to pre-set email transmission policies.

  b) Encryption of external network path information of large attachments restored from converted emails should be attached as URL information.

  c) A web page file accessible to encrypted external network path information of large attachments should be attached as general attachments.

9.4 Countermeasures for external outbound email attack

9.4.1 Countermeasures for attacks using account take-over

- **IP permission setting** allows security managers and email users to register specific IP addresses and countries that are accessible by secure IP registration or permitted country registration for blocking email attacks by receiving emails from the permitted IP addresses and countries.

9.4.2 Countermeasures for unauthorized email server access

– **Email server or IP access control** allows security managers to control secure email links sent by restricting access to web mails or mail clients. Webmail can be blocked through registered IPs, and communication access based on client server post office protocol version 3 (POP3) [b-IETF RFC 1939] or SMTP [b-IETF RFC 2821] is controlled to block mail client communication. Emails can be sent from registered IP addresses and countries and provide logs of email server access restrictions such as IP addresses and dates.

– **Email server access log** allows the determination of whether user access is authorized.

9.5 General countermeasures for targeted email attacks

9.5.1 Common countermeasures for targeted email attacks

– **Email whitelist or blacklist registration** allows security managers manually to enter allowed and disallowed specific email addresses, IP addresses and domains. This automatically filters user access by approving or discarding emails. Additional inspections should be carried out for whitelisted email accounts or IP addresses, to block malware inflow from inbound and outbound emails.

– **Email security data synchronization** can be used to synchronize and block incoming and outgoing data by collecting and analysing new and existing data on inbound and outbound email. Detailed information on email security data includes zero-day malware, look-alike domain, and delivery routeing information (i.e., email server and sender location).

– **Login log** enables the monitoring of malicious ATO attempts within the email server by displaying login attempts for users, security managers and the web with detailed log information such as ID, location (country), IP address, date and status (e.g., success or failure).

9.5.2 Countermeasures for email security reporting systems

– **Warning message** alerts users about the risk of targeted email attacks using terms such as "look-alike domain" and "forged header" along with the subject of the email in their mailbox, to provide recognition on what sort of malicious emails the user received. It is possible for a security manager to configure any suspicious email to be delivered or not. Warning words or phrases in messages can also be managed by setting them on a group basis.

– **Email risk score determination criteria** provide a basis for users to easily and intuitively judge or recognize email risks. The basis can be divided into a method of calculating the email risk score and the implementation conditions.

– **Email security report (for users)** appears as a notification before the user opens an email, and identifies the riskiness of received email. It is recommended to display at least the following information.

a) **Received history**. History of previously received messages from the email address of a look-alike domain verification.

b) **Delivery route**. Current delivery route and change of delivery route history of email transmission.

c) **Header forgery**. The status of the sender header forgery.

d) **URL inspection**. The number of detected malicious URLs.

e) **Similar domain**. The risk level of a look-alike domain (i.e., TLD, low, high and danger).

– **Status board** provides an overview of the real-time technical status of inbound and outbound emails that affects operations for the selected technical objects such as operational status, configuration and operating environment. Fully functioning panels of real-time information, such as the total number and status of emails, the reason for failure of inbound and outbound emails and the number of targeted email attacks received, are viewed to be controlled by internal security managers to recognize risks and disruptions to email security.

Appendix I

Use case of targeted email attacks and countermeasures

(This appendix does not form an integral part of this Recommendation.)

I.1 Use case of targeted email attacks

This appendix describes ATO of social engineering attacks through password reset poisoning, weak transport layer security (TLS) protocol [b-IETF RFC 8446] and phishing site.

Attackers can construct a password reset poisoning attack in an instance where the host server generates a reset password URL based on a user controllable host header. The form of a password reset poisoning attack goes through the following steps.

– The attacker obtains a specific user's email address or username and submits a password reset request on their behalf.

– The attacker interjects the hypertext transfer protocol [b-IETF RFC 2616] request and modifies the host header to point towards a malicious domain controlled by the attacker.

– The site checks whether the user is present in its database and creates a unique temporary password token that is associated with the user's account.

– The site sends a reset password email to the legitimate user, which contains a password reset link and a valid password reset token. The domain name in the token's URL points to the host controlled by the attacker.

– If the user clicks the link embedded in the email, a password reset token is sent to the attacker's host.

– The attacker visits the vulnerable site and uses the relevant query parameter to submit the password token. The attacker can then reset the user's password to their chosen value and take over the registered user's account.

When the site is protected by the hypertext transfer protocol secure (HTTPS), the browser does not exchange data with the web server until it has ensured that the digital certificate of the site is valid. However, attackers can exploit a weakness to redirect TLS traffic from the intended server and protocol to another, substitute endpoint and protocol. The form of weak TLS protocol attack goes through the following steps.

– When the domain name of the site matches the domain name in the email server, the attacker sets the browser to establish a TLS connection with one of servers rather than the site the user intended to visit.

– The attacker redirects traffic intended for one service to another.

– When the browser is communicating in HTTPS and the email server is using SMTP and POP3, a decrypted authentication cookie is sent to the attacker, or an attacker executes malware on the visiting site.

When it is impossible to decrypt HTTPS packets, attackers can create a phishing site that is identical to a real site.

– The attacker uses a tool to create a fraudulent site that is difficult for the user to distinguish from a genuine site and sends an email with an embedded URL to the user.

– The user opens the email and clicks the embedded URL within it.

– The user visits the phishing site and enters a username and password.

– The attacker receives the user's username and password.

Bibliography

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post office protocol – Version 3*.

[b-IETF RFC 2396] IETF RFC 2396 (1998), *Uniform resource identifiers (URI): Generic syntax*.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*.

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple mail transfer protocol*.

[b-IETF RFC 6376] IETF RFC 6376 (2011), *Domainkeys identified mail (DKIM) signatures*.

[b-IETF RFC 6864] IETF RFC 6864 (2013), *Updated specification of the IPv4 ID field*.

[b-IETF RFC 8446] IETF RFC 8446 (2018), *The transport layer security (TLS) protocol version 1.3*.

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

Published in Switzerland
Geneva, 2024