Finnish Transport and Communications Agency
National Cyber Security Centre

Instructions – Leaked IDs

Traficom Publications

22/2022

Contents

1 Introduction

1.1 Purpose of the instructions

The purpose of these instructions drawn up by the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency Traficom is to offer advice to organisations in situations in which it is suspected that IDs have leaked to unauthorised persons or parties and that they have been exploited in a cyber attack. The instructions are focused on how to deal with the special characteristics of this type of information security incident. In order to resolve the situation completely, the organisation should maintain the incident response plan it has drawn up in case of information security incidents and follow it.

These instructions offer guidance on a general level on how to act in case of an information security breach and recover from it. It is recommended that the organisation should draw up a separate guide for its own use that takes its technological and operational environment into account in more detail. The project is funded by the National Emergency Supply Agency.

1.2 What do leaked IDs mean?

Leaked IDs are one of the most common ways attackers can use to penetrate the information systems of your organisation. Leaked IDs are often used to gain the first foothold in attacks. User IDs are traded on marketplaces used by criminals, and they are shared publicly as large databases.

IDs most commonly fall into the wrong hands due to a third-party data leak, reuse of passwords or phishing messages. It is extremely important that the password practices of your organisation are up to date and that the personnel are trained to minimise the risks.

1.2.1 CEO fraud

In CEO fraud (business email compromise), an employee in charge of the financial transactions of the company is deceived into paying an invoice or making another kind of bank transfer from the company’s fund to the account of the criminals. Cyber criminals buy user IDs from darknet markets and exploit them to log in to an employee’s email and monitor the email traffic, looking for opportunities to do things like change the content of existing email threads, such as account numbers. They can also create completely new invoices and direct the payments to their own accounts.

2 Preparation

Preparing for security incidents is a good way to reduce their severity and make it possible to recover quickly and continue the business. Organisations can assess their own readiness by using the Kybermittari (Cybermeter) cyber security evaluation tool of the National Cyber Security Centre Finland, for instance[1]. An incident response plan that has been drawn up in advance is a good starting point for what to do in case of a security incident. The organisation must also ensure that measures such as locking user IDs, isolating servers and terminal devices from the network and restricting network traffic to harmful IP addresses or domain names are technically possible and that the personnel have the expertise required to carry them out.

Gathering, compiling and monitoring log data is important in order to detect incidents in time. Log data also make it possible to investigate incidents thoroughly, which speeds up the cleaning and restoration of the environment, if necessary. The National Cyber Security Centre Finland has drawn up a guide on how to collect and use log data.[2] Depending on the systems used by the organisation, comprehensive monitoring typically also requires network- and system-level solutions in addition to this.

A common password policy of the company, imposing restrictions on login sources and multifactor authentication are excellent ways of preventing the exploitation of leaked IDs.

2.1 Administrative measures

- In case of security incidents related to a data leak containing user IDs, implement an incident response plan that has clear instructions for the personnel on what to do.
- Design a password policy for your organisation that defines the minimum requirements for a password.
- Train the personnel to identify phishing messages.
- Find out in advance how you can report an information security breach to the National Cyber Security Centre Finland[3]. Start monitoring the news by the National Cyber Security Centre Finland.[4]
- Review attack scenarios together with the company’s management and agree on the practical measures as well as management responsibilities and authority in case of an information security breach.
- Develop[5] the incident response plan and practice it regularly with tabletop exercises, in which responsible persons and interest groups practice the information security incident response process in imaginary scenarios.
- Specify the necessary access rights carefully based on the needs of the users and the technical functionalities.
- Consider establishing a security operations centre or purchasing a similar service. The purpose of the security operations centre is to monitor the network traffic of your company and information security events in the systems.

[1] https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter

[2] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/collecting-and-using-log-data

[3] https://www.kyberturvallisuuskeskus.fi/en/report

[4] https://www.kyberturvallisuuskeskus.fi/en/ncsc-news

[5] https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

2.2 Technical measures

- Enable multi-factor authentication.
- Restrict login sources from countries in which your organisation does not do business.
- Implement identity and access management (IAM) controls.
- By using a virtual private network (VPN), you can prevent login attempts from outside the network to the most critical systems.
- Aim to detect attacks as early as possible with different kinds of centralised monitoring solutions and test their functionality regularly.
- Implement features of existing systems or purchase an information security product capable of filtering emails with harmful content, spam and unwanted network traffic.

2.3 Preparation and training in practice

One important part of preparation is practicing threat scenarios. By practicing scenarios such as the one found in these instructions in advance, your organisation can make sure that it is ready to meet situations like the one described. Training ensures, among other things, that the personnel of your organisation understand what the different parts of the workflow and checklist in the instructions mean and they have the capability to act according to the instructions.

It is also recommended that you study the materials of the National Cyber Security Centre Finland related to exercises.[6]

One example scenario is a situation in which the IDs of one of the company's employees have ended up in the hands of cyber criminals. The IDs have been used to log in to email, which has then been used to send forged invoices. The information security breach is revealed when a partner notices that the invoices they have received contain suspicious details.

How would your organisation act in a situation like the one described? Practice at least the following steps of these instructions:

- Reporting the security breach and escalating the situation.
- Locking down the infected IDs and disconnecting active sessions.
- Gathering identification information of login events and log analysis.
    - Is it possible to find out how the user IDs leaked?
    - Which user IDs have been compromised?
- Using the identification information gathered to check other user IDs in case of infection.
- Finding out the recipients of the phishing message.
- The post-incident review process.

In connection with all of the steps being practiced, you should think about how the organisation leads the information security breach management, how the internal communications work and who the person responsible or their deputy are at which stage.

[6] https://www.kyberturvallisuuskeskus.fi/en/our-services/exercises

3 Detecting an information security breach

An information security breach caused by leaked IDs can be detected in the following ways, for instance:

- The organisation is notified about a suspicious activity or email via social media, customers, partners or the authorities, for example.
- An alarm is sent by an information security product or a service provider.
- A threat information service issues a notification of the leaked IDs.

Report the information security breach to the National Cyber Security Centre Finland.[7] We advise you confidentially and free of charge on how to limit the damage, analyse the incident and take recovery measures. At the same time, you support the national information security situation awareness and make it possible to help and warn other potential victims.

See the guide on how to detect data breaches by the National Cyber Security Centre Finland (in Finnish).[8]

[7] https://www.kyberturvallisuuskeskus.fi/en/report

[8] https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

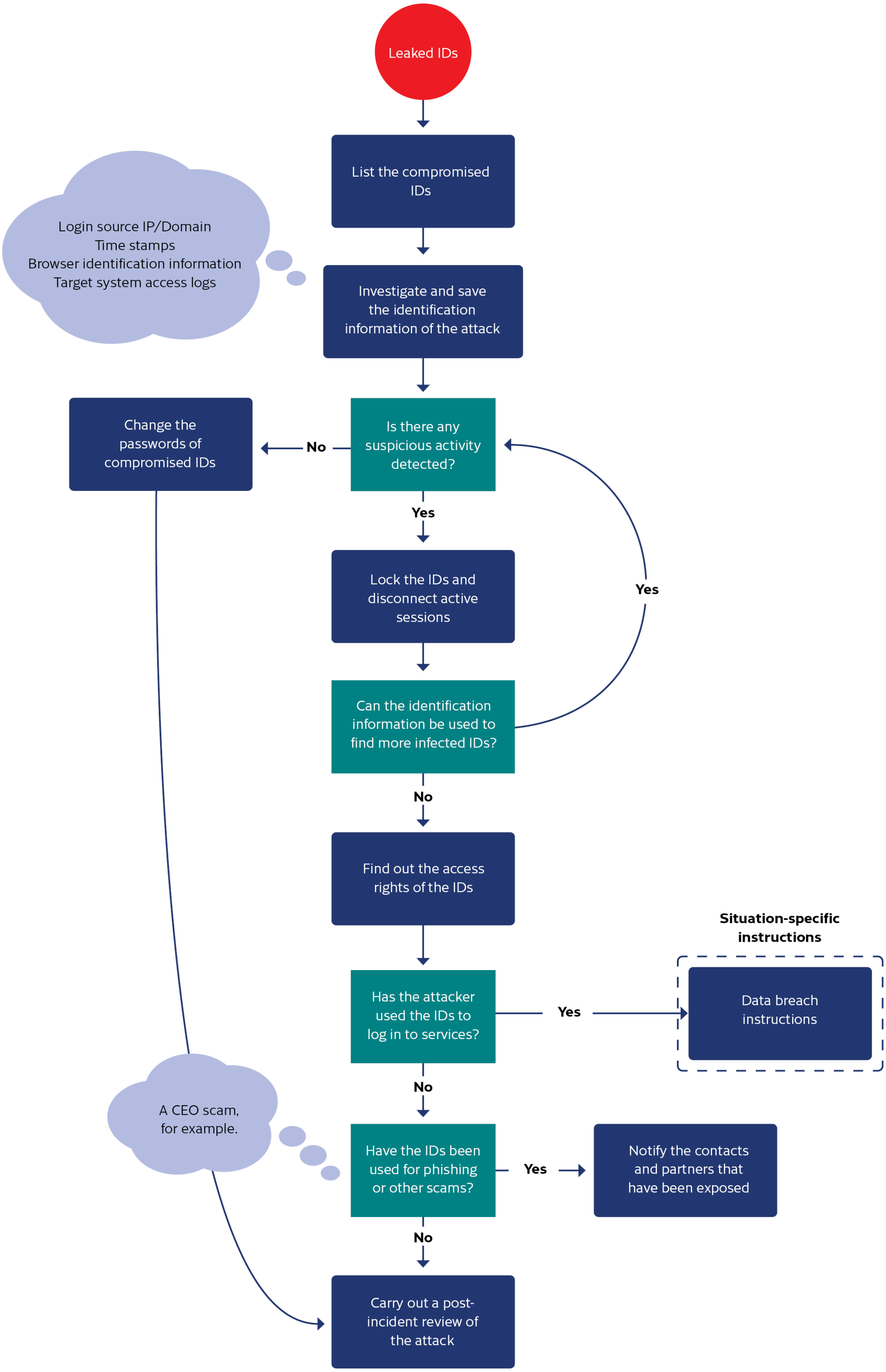
4 Instructions

Use the attached checklist to find measures to help you when you detect an information security breach related to user IDs. The checklist helps organisations to prioritise and use a phased approach when investigating the security breach.

4.1 Workflow of an information security breach investigation

The flow chart below describes the right order of measures when investigating the security breach. The flow chart supports the use of the checklist. During the investigation, it is also crucially important to keep an accurate event log of the measures taken. The log should show the measure taken, the timestamp and the party that implemented the measure.

The gathering of potential evidence should also be documented carefully. You should record who gathered the data, what it was, and when and how it was gathered. A carefully drawn up event log makes the investigation as well as the cooperation with the police and information security investigators significantly easier.


Leaked IDs
List the compromised IDs
Investigate and save the identification information of the attack
Login source IP/Domain
Time stamps
Browser identification information
Target system access logs
Is there any suspicious activity detected?
No
Change the passwords of compromised IDs
Yes
Lock the IDs and disconnect active sessions
Can the identification information be used to find more infected IDs?
Yes
No
Find out the access rights of the IDs
Has the attacker used the IDs to log in to services?
Yes
Situation-specific instructions
Data breach instructions
No
Have the IDs been used for phishing or other scams?
A CEO scam, for example.
Yes
Notify the contacts and partners that have been exposed
No
Carry out a post-incident review of the attack

4.2 Immediate measures

Goals of the phase	The accuracy and speed of the measures are both important. The goal of the immediate measures is to stop the malware from spreading, prevent the attackers from gaining a foothold in the network and prepare for the start the recovery process.

Phase	Purpose	Measures
Lock the user ID	By locking the user ID and disconnecting active sessions you can prevent the user IDs from being exploited.	Lock the user ID so that it cannot be used. Disconnect all active sessions.
Find out what rights the user IDs have	User IDs can be exploited in different ways depending on what rights they have. Find out the answers to the questions: • Which systems can you log in to with the IDs? • Do the IDs have administrator rights to systems or other user IDs?	Find out what rights the user IDs have.
Evaluate whether you need external help to handle the information security breach or not	The organisation may need help with organising measures, managing the security breach and technical measures. If your own organisation or IT service providers do not have the necessary expertise, you should consider getting external help.	Technical measures to handle the incident may require external expertise. Such measures may include collecting identification information and investigating the threat based on it. The National Cyber Security Centre Finland can help organisations especially during the first response to the incident as well as by offering additional information on similar cases in Finland and abroad. You can find Finnish service providers in the resources listed in the footnote.[9]
Report the information security breach to the authorities	Report the incident to the authorities. The organisation may have an obligation to report the information security breach based on regulations or the terms of the cyber insurance.	File a report of an offence about the incident with the police.[10] Also notify the National Cyber Security Centre Finland of the incident[11] to maintain situation awareness and get help. If personal data or other information subject to data protection legislation (GDPR) may have ended up in the hands of the attacker, report the incident to the Office of the Data Protection Ombudsman[12]. The infrastructure operators and service providers critical to the security of supply that are subject to the NIS directive of the

[9] https://dfir.fi/
https://www.fisc.fi/fi/about-us
https://www.hansel.fi/yhteishankinnat/tiedonhallinnan-ja-digiturvallisuuden-asiantuntija/ (in Finnish)

[10] https://poliisi.fi/en/report-a-crime

[11] https://www.kyberturvallisuuskeskus.fi/en/report

[12] https://tietosuoja.fi/en/data-breach-notification

		EU on the security of network and information systems must notify the supervisory authorities about information security breaches in network and information systems[13].

[13] https://www.kyberturvallisuuskeskus.fi/en/services/report-security-incident-nis-notification-obligation

4.3 Investigating an information security breach

Goals of the phase	The goal of investigating the security breach is to determine the extent of the attack and its impact on the organisation. A careful investigation ensures that the attacker no longer has access to the system and that all compromised IDs have been brought under control again.

Phase	Purpose	Measures
Identify harmful activity and collect identification information	Identification information is used to find infected devices and IDs. Collecting identification information carefully and using it to investigate the incident is vitally important for cleaning the environment to a sufficient level so that the recovery can start safely.	Look for abnormalities in the available log data to determine if the leaked IDs have been exploited. Such abnormalities may include: • Time of the login • Source IP address • Version of the operating system or browser Verify the observations by interviewing the owner of the IDs to ensure that they did not carry out the measures. Save the identification information discovered in the abnormalities so that you can use them to look for other user IDs whose information may have leaked.
Use identification information to find all leaked IDs	The identification information can be used to find out how far into the organisation the attacker was able to penetrate. By collecting identification information and searching for it in the target systems, it is possible to ensure that all infected devices and identifiers are found and cleaned.	You can use centralised monitoring software to look for leaked IDs. The software often offers the option of searching for events on terminal devices by using the desired identifiers. If the organisation has also implemented centralised log management, it can be used to search for events efficiently from several different sources at the same time. If neither of the solutions mentioned above is available, identifiers should be searched manually from all terminal devices and servers. There is a risk that the attackers have attempted to cover their tracks by disabling logging after gaining access to a device, in which case their activities have left no trace. For this reason, it is important to review identification information collected from all of the different sources and use it to try and establish an overview of the attackers' activities.
Save all available log files and other evidence on a hard drive isolated from the network for later investigation	The aim of collecting and storing evidence is to guarantee a high-quality investigation after the incident so that the root causes of the incident can be determined. Evidence may be needed for filing a report of an offence and the court proceedings. If the organisation has a cyber insurance policy, the insurance company may also re-	Save log files that contain information relevant to the investigation of the incident on a hard drive isolated from the network. Also collect harmful email and other messages, if any. Aim to keep the evidence, such as complete disk images and memory samples, as intact as possible. Extract integrity

	quire more detailed information on the security incident as well as evidence for the investigation.	hashes from them to ensure this. Try to take samples of the malware detected and store them. They should be handled with extreme care. Professional expertise is often required to store them safely. Send the samples to the National Cyber Security Centre Finland.[14]
Interview the user	Confirm the observations by interviewing the user that owns the leaked IDs. The user may be able to provide information on how the IDs leaked. For example, the user may have downloaded files on their computer, clicked a link in an email message or opened a remote connection to an attacker impersonating an IT support person. When interviewing the user, they should not be made to feel guilty about what happened, because their actions may not have played any part in the data leak, and the user may not necessarily have noticed anything unusual.	Interview the user whose user IDs were found to be linked to unusual activity and try to find out why the IDs leaked.

[14] https://www.kyberturvallisuuskeskus.fi/en/news/transmitting-e-mail-and-sending-samples-national-cyber-security-centre-finland

4.4 Recovery

Goals of the phase	The aim is to regain control of all of the leaked IDs and ensure that the IDs are safe again. Operating models are improved so that such an incident could be avoided in the future.

Phase	Purpose	Measures
Change the password of the user ID	Ensure that the login information of all of the infected IDs is changed so that the attacker can no longer use the IDs to access the organisation's systems.	Change the password and ask the user to change the password again themselves when they log in for the first time. Deliver the new passwords to users either verbally in person, in a text message or by telephone, but do not use email or the instant messengers used in the organisation, because the attacker may still have access to them. Consider adding two-factor authentication to administrator accounts as well as the IDs that were exploited in the attack. In addition, monitor the IDs used in the attack more carefully after they have been restored in case the attacker gains control of them again. If it is still unclear how the attacker was able to gain control of certain IDs, consider destroying them and creating completely new IDs. In this way, you can ensure that the attacker cannot use this unidentified method to gain control of the IDs again. Also consider issuing a new workstation to the owners of the leaked IDs.
Check the redirect rules of email accounts	CEO fraud often involves setting redirect rules for email accounts that the criminals can use to monitor the email traffic of the organisation.	Check the redirect rules of email accounts related to the leaked IDs and remove any harmful rules you find.
Impose stricter login requirements on users	The exploitation of leaked user IDs can be restricted by imposing stricter login requirements.	Set the login requirements to a suitable level by implementing the following: • Multi-factor authentication • Certificate-based login • Domain-linked terminal device or one that is otherwise controlled by the company • Restrictions based on the source IP address
Evaluate the current password practices	By maintaining password practices, you can set minimum requirements on the complexity of the password.	Evaluate and update the instructions related to password practices.

5 Post-incident review of an information security breach

When the crisis is over and business operations have returned to normal, it is important to start the post-incident review of the attack and learn as much as possible about what happened for the future. At the same time, crisis management systems should be updated based on the observations made. The organisation may become a victim of a similar attack again, if the root causes of the incident cannot be determined and no lessons are learned from it.

During the post-incident review, the activities during the crisis are studied: what measures were done well, what could have been done better, and how the plans and the security level could be improved. A report should be drawn up on the post-incident review that examines at least the following questions in addition to the course of the events:

- Root causes of the incident
  - What technical or functional weaknesses led to the situation?
- Effectiveness of the organisation’s own protection
  - Were the controls used to detect attacks sufficient?
  - Did the attacker’s actions raise any alarms?
  - What was the reaction to the alarms like? Was the information about alarms transmitted to the right responsible persons?
- Actions during the crisis
  - Was the crisis plan followed? How usable was it?
  - Were the responsibilities of the crisis management team assigned to the right people?
  - How successful was limiting the scope of the attack and removing the attacker?
  - How successful were the communications of the crisis management team? How were the interest groups taken into account?
- Recovery
  - How did the recovery of critical information and services go?
- Post-incident review
  - Have the course of events and the investigation work been documented?
  - Was the technical investigation of the incident sufficient? Has it been possible to submit sufficient data on the attack for the use of the authorities, for example?
  - Evaluate the actions of the service providers. Were the response time and the services that were agreed upon sufficient for the investigation of the incident?

The organisation should update its own incident response plan and more detailed playbooks designed for combating different types of security incidents after the fact. Practicing different scenarios at regular intervals is also recommended to ensure that you can benefit from them in crisis situations.

The National Cyber Security Centre Finland hopes that the companies and organisations share the most important lessons they have learned from the incident with the Centre, too. With incident reports, the National Cyber Security Centre Finland can help other organisations in Finland as well as internationally to investigate similar cases. The lessons learned from recovery help with developing the preparedness of all organisations.

Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland
PO Box 320, FI-00059 TRAFICOM
tel. +358 29 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-814-0

NATIONAL EMERGENCY SUPPLY AGENCY

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre