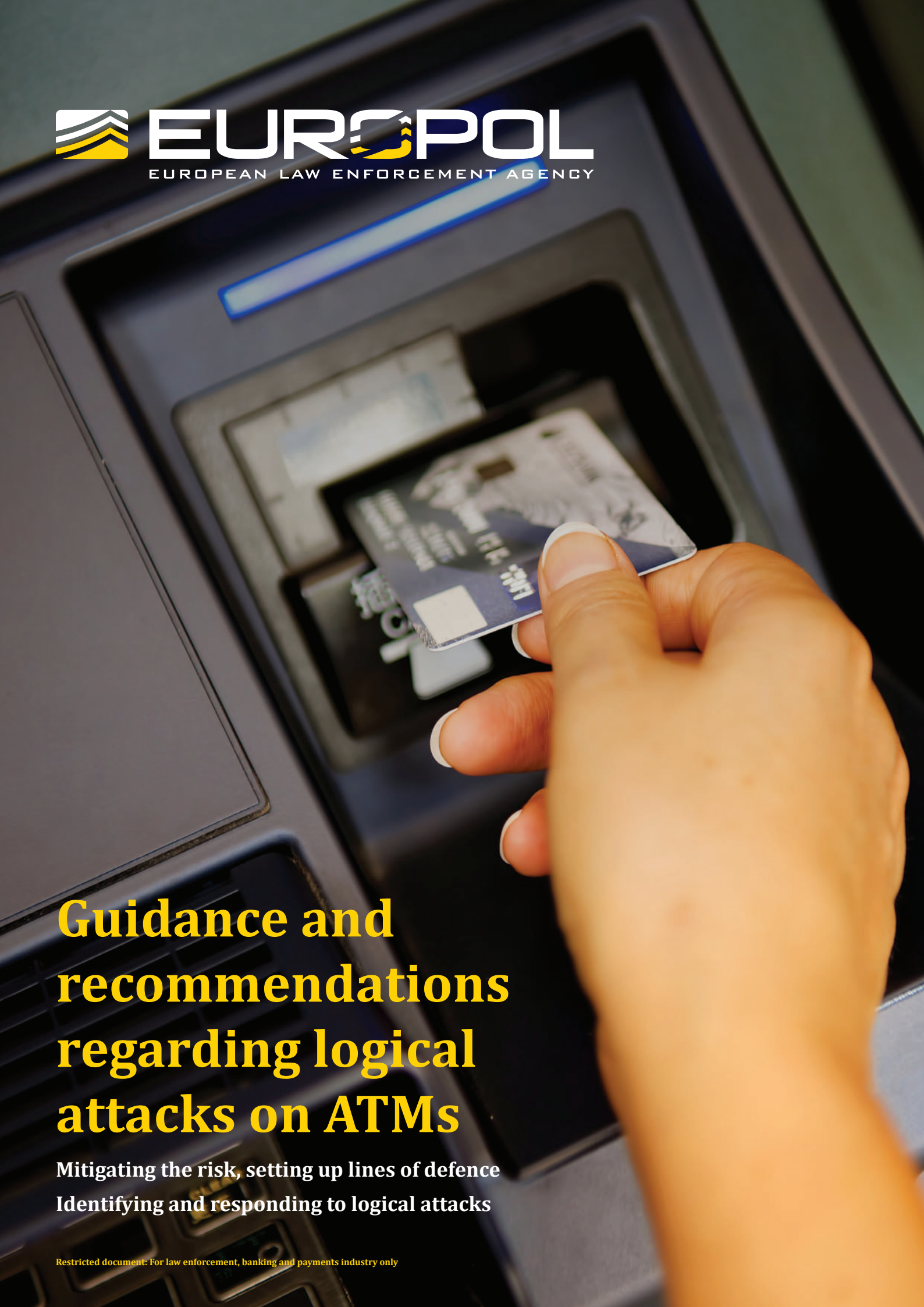


EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

# Guidance and recommendations regarding logical attacks on ATMs

## Mitigating the risk, setting up lines of defence
## Identifying and responding to logical attacks

# CONTENTS





# FOREWORD

Logical attacks on ATMs are recognised as a developing threat by the industry, as other threats, notably card skimming, are increasingly being contained. Since 2013, ATM malware attacks have significantly increased, thereby causing substantial economic damage, and become more widespread geographically. There are no central records of such attacks and in many cases, such attacks could have been prevented by implementing basic countermeasures.

Europol recognises the severity of the threat presented by ATM malware attacks, and has been actively cooperating over the past decade with all the payment and banking industry sector representatives collected under the umbrella of the European ATM Security Team (EAST). I would like to highlight the very successful cooperation Europol and in particular Focal Point Terminal has had with EAST since its inaugural meeting in 2004.

Europol's Guidelines regarding logical attacks on ATMs, the production of which has been coordinated by the EAST Expert Group on ATM Fraud (EGAF), is a first of its kind. This advisory document provides vendor-neutral guidance on countermeasures as well as a collection of indicators that can be used to detect when a malware incident may have occurred. The document will be updated periodically as malware attacks further evolve.

I take this opportunity to recognise the work of FTR Solutions, ING, RBS, GMV, Diebold, NCR, Wincor Nixdorf and EAST. Their valuable contributions were indispensable for the production of these Guidelines. I look forward to Europol's continued engagement and cooperation with EAST and its stakeholders combating new payment industry threats, and I am confident that Europol will continue to succeed in this field.

**Wil van Gemert**
Deputy Director of Operations
Europol

Chapter 1

# DESCRIPTION OF MODUS OPERANDI

## Malware attacks on ATMs can be divided into two different categories, based on how the attack is performed

### Definition of ATM Logical & ATM Malware attack

A logical attack on an ATM or ATM network is a coordinated set of malicious actions performed by criminal individuals or organisations to gain access to ATM computer systems or components with the purpose of obtaining cash or sensitive data from ATMs. Malware attacks are a sub-category of logical attacks. In these attacks the goal is to deploy software in the ATM PC so that the software will be running in the background when the ATM is operating normally.

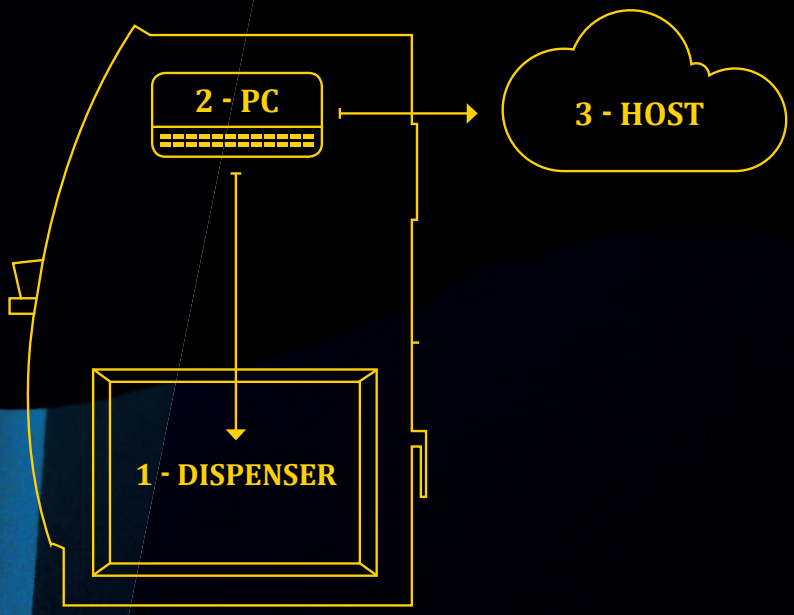
With some exceptions, each ATM has the same functionality, a cash dispensing mechanism that is controlled by an operating system using a computer (*PC*) - and therefore all ATMs (*regardless of vendor*) are at risk from malware attacks.

**Offline attacks** are conducted while the operating system of the ATM PC is not running. These could be attacks where a fraudster connects a notebook or mini PC to components of the ATM, or by running his own operating system on the original ATM PC. An offline attack can also be used to prepare an online attack e.g. by disabling security features.

**Online attacks** are conducted while the operating system of the ATM PC is running e.g. by connecting a USB stick with malware.

The timeline of a logical attack can be very different. For example the infection with malware and its usage can be performed at the same time or with a significant delay. Moreover the malware can stay on the system or may be deleted directly after usage. This mainly depends on the used modus operandi.

The vast majority of currently observed attacks have required some physical access to the ATM. The drawing below shows a typical architecture of current ATMs. The PC is placed in the head compartment, connected to an external host and the cash dispenser or recycler within the safe.




## BASED ON THIS ARCHITECTURE, THERE ARE THREE COMMON POINTS WHERE A FRAUDSTER TRIES TO ATTACK THE SYSTEM:

1) The communication line between the PC and the dispenser unit. In most cases a serial RS232 or USB connection. It is typically offline attacks with additional hardware.

2) The ATM PC using its interfaces like USB for external keyboards and memory sticks or the CD/DVD drive. This could be done offline, online or with a combination of both.

3) The communication line between the ATM PC and the host. Besides the PC there could be additional network components inside the ATM like a virtual private network (VPN) router. This could be carried out online or offline with additional hardware.

## THE FOLLOWING MODI OPERANDI HAVE BEEN OBSERVED IN RELATION TO ATM MALWARE ATTACKS.

**Jackpotting or cash out attack**
Jackpotting is a term for attacks where malware takes control of the ATM PC (2) and the cash dispenser function, thereby allowing the fraudster to directly cash out money. In most cases the malware is adapted to a specific environment, but the concepts can be easily migrated to different systems.

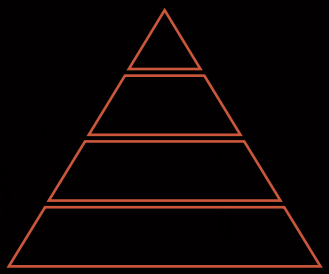
**Black Boxing**
Black Boxing is a variant of Jackpotting, where the ATM PC is not used. Instead the fraudster brings his own PC with him and targets the communication between the PC and the dispenser unit (1). As the malware communicates directly with the dispenser, each Black Box attack is only valid for one type of dispenser.

**Man-in-the-Middle**
Man-in-the-Middle attacks focus on the communication between the ATM PC and the acquirers host system. The malware can, for example, fake host responses to withdraw money without debiting the fraudster's account. Typically the malware is triggered during transactions with pre-configured card numbers. It can be implemented at a high software layer of the ATM PC (2) or somewhere within the network (3).

**Software Skimming – Skimming 2.0**
Software skimming malware intercepts card and PIN data at the ATM, allowing the fraudster to copy it and to create counterfeit cards for the usage at non-EMV compliant ATMs. Once infected the malware is active on the ATM PC (2) during the normal operation. A non-PCI compliant EPP firmware is a precondition for the malware to intercept PIN data.

## Chapter 2

# MITIGATING THE RISK OF ATM LOGICAL AND MALWARE ATTACKS, SETTING UP LINES OF DEFENCE



A Layered Approach, the four lines of defence

**A layered approach is recommended to protect ATMs from malware and logical attacks. When combined these layers work together to substantially reduce the risk of malware attacks on an ATM. The lines of defence are:**

1. Physical access to the ATM
2. Offline protection
3. Online protection
4. Additional measures

The First Line

## Physical access to the ATM

Only authorised personnel should be allowed to carry out work on an ATM. In particular:

1. Ensure that authorised service providers carry accreditation documents and that there is a procedure for ATM site personnel to authenticate their authorisation to work on the ATM.
2. Usually the top compartment (top box) of an ATM contains the PC. This area should be secured by an intruder alert to prevent unauthorised opening, or the access lock to the top box should be changed to avoid the usage of default master keys provided by the manufacturer.
3. Surveillance monitoring (cameras) should be in place, which will also detect and record suspicious activity around the ATM. If surveillance monitoring is used, then camera/video images should be stored externally to the ATM, and operations of the cameras should not be interrupted by an ATM reboot.
4. There should be adequate lighting in and around the ATM.

The Second Line

## Offline protection

Logical attacks can be performed without the usage of the ATM operating system.
Therefore:

***BIOS configuration***

BIOS configuration editing should be password protected, the latter differing from the default password provided by the ATM vendor.

1. Consider robust password management policies. Best practice indicates that these passwords should be as complex as the BIOS can support.
2. Set the BIOS to boot only from the ATM hard drive.
3. Booting from removable media should be disabled by default.
4. Apply a robust operating system administrator password.
5. Ensure AUTORUN has been fully and effectively disabled.

***Hard disk encryption***

Hard disk encryption should be deployed to prevent unauthorised changes to the content of the hard drive.

***Cash Dispenser Communications***

The USB/serial communication between the dispenser and the PC should be protected and secured against message manipulation and injection.

1. To prevent unauthorised devices from sending commands to the cash dispenser, the initial communication should require authentication at the cash dispenser. e.g. by physical access to the safe.
2. It should not be possible to circumvent the communication's protection e.g. by rolling back firmware, or by replaying messages.

The Third Line

## Online protection

***Network***

Communication authentication and encryption protections should be applied to all ATM network traffic. The recommendation is to use TLS 1.2 or a VPN, and by implementing MACing to provide cryptographic authentication of sensitive messages.

***Firewall***

A firewall should be established to restrict all inbound communication to the ATM.

***Operating system***

An operating system should be hardened or parameterised so as to prevent abuse of privileges, default accounts, installation of malicious software, and unauthorised access to resources like USB ports/CDs/DVDs/hard disks. Therefore the following should be applied.

1. The OS is to enforce strict application separation. For example the unauthorised use of various services (OS, Platform, including XFS and Applications) is to be prevented at all times e.g., runtime, service and administration.
2. Unused services and applications are to be removed.
3. Establish a policy for secure software upgrades.
4. Ensure the application runs in a locked down account with the minimum required privileges not being root or administrator.

***Anti-malware and logical protection***

An ATM specific anti-malware and logical solution based on the "whitelisting" or "sandboxing" principles should be employed.

***USB protection***

The use of unknown USB devices should be blocked.

The Fourth Line

## Additional Measures

Other measures can be put in place as follows:

***ATM installation***

It is recommended to start with a clean install at the ATM or perform an antivirus check before the approved installation.

***Secure Software delivery***

A policy should be established for secure and regular software updates for all software installed on the ATM.

***Fraud monitoring***

- Deploy a responsive, real-time fraud system.
- Ensure your fraud system identifies suspicious patterns of behaviour to stop fraud.

***ATM Monitoring***

- Make sure that effective ATM monitoring is in place, that every opening of an ATM is recognised centrally.
- Alerts generated by security solutions should be monitored and acted upon.

***Cash refilling cycles***

Consider filling the ATM with just enough cash for a shorter period.

***Test vulnerability***

Conduct a regular ethical hacking testing and vulnerability scanning on the ATM and the ATM's network which includes wireless access point presence testing.

***Look for abnormalities***

During ATM maintenance and cash replenishment random checks can be conducted by employees to inspect the ATM for abnormalities on the fascia of the ATM or inside the operating area of the ATM.

***Segregation of duties***

Individual employees are not to have full access to the ATM (segregation of duties)

***Host integrity check***

The ATM is recommended to prove to the host that the ATM security can give the same hash over the SW in the ATM back to the host.

# Chapter 3

# IDENTIFYING AND RESPONDING TO LOGICAL AND MALWARE ATTACKS

## Part 1: Identification of logical and malware attacks

There are no specific features of malware or logical attacks that can be used to uniquely distinguish them from other types of attack. Diagnosing a particular incident as a malware attack must therefore use a process of elimination to reduce the possible causes for the incident until only the possibility of a malware attack remains. This problem is compounded by the fact that certain of the observed ATM malwares have been quite effective at removing traces of their presence once the fraud has been completed.

The following list of indicators can be used to help in the determination of whether or not a particular incident represents a logical or a malware attack. The presence of one or more of the indicators listed here does not necessarily imply the presence of malware. Rather, a confluence of indicators may lead an investigator to conclude that a logical or a malware attack has taken place.

The following behaviours or patterns may indicate the presence of malware on an ATM:

- Unexpected reboots.
- Unexpected “cash out” events.
- Unexpectedly empty cash cassettes.
- Gaps in audit logs where there ought to be records of transaction activity.
- Transaction records on the ATM that do not correlate with the value of cash apparently dispensed.
- Transaction records on host servers that do not correlate with the value of cash apparently dispensed.
- Discrepancies in device status messages reported by the ATM between consecutive legitimate transactions.
- Legitimate files in incorrect locations.
- Loss of communication with security solutions running on the ATM.
- Unexpected gaps in CCTV footage.
- Unexpected physical access to the ATM top box, including physical breaches such as lock picking or removal.
- Relatively minor incidents, such as the theft of lock barrels from top boxes, may be a component of a systematic process of gaining access to ATM PC cores, for example, the manufacture of relevant keys.
- Physical security, information security, operational and fraud teams may all have possession of pieces of the information that would allow an organisation to conclude that a malware attack has taken place. However, taken in isolation these various aspects of the attack may not allow any one of the individual groups to draw the necessary conclusion. Therefore, organisations should review their incident response procedures to ensure effective cooperation between physical, information security, operational and fraud staff as required.

## Part 2: Responding to Logical or Malware Attacks

As mentioned in part 1, any one or more of the indicators above could have alternative legitimate or fraudulent explanations. Therefore, at the time of the initial response to an incident it can be very difficult to determine whether that incident is a malware incident. Any institution planning a response to malware incidents must consider balancing the requirement of the need to return the ATM to service as quickly as possible with the need to preserve as much evidence as possible.

The difficulty of identifying malware incidents as well as the delicacy of forensic evidence means that the best practice for responding to malware incidents is currently an evolving topic. In general terms, institutions should bear in mind the following points:

- Create and establish plans and procedures for managing and responding to logical or malware attacks.
- Include procedures for collection and preservation of physical evidence, such as fingerprints or DNA, present at the ATM.
- Include procedures for collection of logical evidence, such as traces of the malware. A "forensic image" should be taken as soon as possible.
- There may be CCTV evidence. Correct procedures must be followed for the collection and preservation of this evidence.
- Engage with the appropriate local law enforcement agencies in your jurisdiction as soon as possible.
- Keep accurate records of all action taken from the beginning of the incident to keep the chain of custody.

EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands
PO Box 90850
2509 LW The Hague
The Netherlands

**Website:** www.europol.europa.eu
**Facebook:** www.facebook.com/Europol
**Twitter:** @Europol_EU and @EC3Europol
**YouTube:** www.youtube.com/EUROPOLtube