# INTERNATIONAL CRIMINAL GROUP BEHIND ATM SKIMMING ATTACKS DISMANTLED

24 May 2016

Press Release

On 18 May 2016, the French Gendarmerie of Pau[1], in close cooperation with the Investigative Unit of the Italian State Police of Imperia[2] and Europol, disrupted an international criminal group responsible for large-scale ATM skimming and money laundering. Composed mainly of French-Italian nationals, the criminal network used sophisticated ATM skimming devices which allowed them to compromise ATMs and perform fraudulent withdrawals outside the EU. Estimated losses incurred by the criminals' activities amount to more than half a million euros.

This operation resulted in multiple house searches and the final arrest of nine individuals in France. Micro camera bars, card readers, magnetic strip readers and writers, computers, phones and flash drives, two hand guns, five vehicles, as well as thousands of plastic cards ready to be encoded, were seized in several locations between France and Italy as part of this operation.

The primary modus operandi of the criminals was to harvest financial data from ATMs in different areas of France. The compromised card data, which was used to create fake payment cards, was stored on a cloud server managed by the members of the criminal organisation. These fake cards were used to withdraw large amounts of cash from ATMs outside the European Union (Asia and the US).

Europol's European Cybercrime Centre (EC3) initiated the case early this year and supported the involved law enforcement authorities in their efforts to identify the suspects. Operational meetings were held at Europol's headquarters in The Hague and EC3 provided analytical and forensic support throughout the investigation including the deployment of a mobile office and a forensic expert during the final action day to assist the French authorities.

In addition, Europol's information and analysis systems were used to exchange and cross-check intelligence received from EU Member States and non-EU countries with which Europol has operational agreements.
Background

ATM skimming refers to the use of highly advanced devices which target an ATM, thus allowing the attackers to copy and store magnetic strip card data and confidential PIN codes.

To reduce the risk of becoming a victim of this type of electronic crime, check your banking

transactions regularly and immediately inform your bank of anything suspicious, which could also include a transaction not being debited from your account after you have used your card.

① Section de Recherches de Pau.

② Squadra Mobile della Questura di Imperia.

CRIME AREAS    Economic Crime  •  Cybercrime  •  Payment Fraud
TARGET GROUPS    General Public  •  Law Enforcement  •  Academia  •  Professor  •  Students  •  Researcher  •
Press/Journalists  •  Other
ENTITIES    European Cybercrime Center (EC3)

**Source URL:** https://www.europol.europa.eu/newsroom/news/international-criminal-group-behind-atm-skimming-attacks-dismantled