A low-risk, high-profit criminal activity, payment card fraud can be split into two distinct types: card-not-present fraud, which occurs largely online, and card-present fraud, which typically occurs at retail outlets and ATMs.

As a form of cybercrime, card payment fraud is one of the EMPACT priorities, Europol's priority crime areas, under the 2018-2021 EU Policy Cycle.

Card-not-present fraud involves the unauthorised use of credit or debit data (the card number, billing address, security code and expiry date) to purchase products and services in a non-face-to-face setting, such as via e-commerce websites or over the telephone. In the majority of cases, the victims are unaware of the unauthorised use of their cards, which remain in their possession.

Often referred to as carding, this type of illegal activity has grown steadily, as compromised card details stolen by means of data breaches, social engineering attacks, data-stealing malware and phishing tools become more readily available on forums, marketplaces and automated card shops in the deep web and Darknet.

According to the most recent (2013) data, card-not-present fraud accounted for 66 % of the EUR 1.44 billion in fraudulent card transactions in the 35 countries of the Single Euro Payments Area (SEPA).

Card-not-present fraud is found across all sectors but the purchase of physical goods, airline tickets, car rentals and accommodation with compromised cards have generally seen an increase throughout the EU.

The fraudulent purchase of airline tickets in this way is at the focus of Europol's successful Global Airline Action Days.

SKIMMING

The growth in card-not-present fraud is also driven by the effectiveness of measures against the more traditional card-present fraud. Card-present fraud requires an offender to present a physical card at an automated teller machine (ATM), point of sale (POS) or other terminal.

This fraud has two stages: obtaining a card and the use of the card. The cards used are either lost or stolen genuine cards, or counterfeit cards. Counterfeit cards are often the product of skimming, which involves the duplication of a card's magnetic strip, often through devices hidden within compromised ATMs and point-of-sale terminals.

Cardholders' confidential data is more secure on a chip-embedded payment card than on a card with a magnetic strip.

Thus, fraud using counterfeit cards is typically committed outside the Single Euro Payments Area (SEPA). As some parts of the world have been slow to embrace EMV, card-present fraud has migrated, chiefly to the Americas and Southeast Asia, Indonesia and the Philippines in particular, where criminals use cards cloned in Europe to cash out counterfeit cards. The rollout of EMV technology in the United States is likely to increase the focus of criminals on card-not-present fraud.

Did you know? Payment card transactions are the most widespread form of non-cash payment in the EU. In 2012, the total value of transactions made by debit and credit cards issued within the Single Euro Payments Area (SEPA) amounted to EUR 3.5 trillion. In the same period, criminals acquired EUR 1.33 billion [2013: 1.44 billion] from payment card fraud. This represents EUR 0.38 lost to fraud for every EUR 1 000 worth of transactions.

TRENDS

The growing e-commerce industry will result in a parallel growth of card—not-present fraud, especially as industry measures at preventing card-present fraud become more effective. Criminal modus operandi will be shaped by industry measures to counter payment card fraud.

Emerging and alternate payment options such as contactless payment using near field communication (NFC) will drive innovation within organised crime groups to enable them to abuse new technologies. New electronic/card-less payment methods may, however, ultimately result in a downwards trend in card fraud.

INTERNATIONAL COOPERATION

In most of the card-not-present fraud investigations Europol has supported, the primary source of illegal data is breaches within private industry, often facilitated by insiders, malicious software, or both.

Europol has organised courses on the forensics of payment card fraud. Topics include the examination of skimming devices, ATM logical attacks and, especially, malware attacks, which are a developing threat.

Europol's Joint Cybercrime Action Taskforce (J-CAT) has supported several high-profile cybercrime operations, such as in May 2017, when 27 individuals linked to ATM "black box" attacks were arrested across Europe. The operation also involved a number of EU Member States and Norway, supported by Europol's European Cybercrime Centre (EC3).

In addition, Europol's Analysis Project Terminal provides support for hundreds of investigations into international electronic and online payment fraud.

NUMBER OF ITEMS FOUND: 128

SEARCH

TYPE

Article/Story, Event, How-To Guide, Landing Page, Multimedia, News/Press Release, Operation, Page, Publication/Document

TARGET GROUP

SEARCH

CLEAR ALL

PROJECT SANDPIPER

OPERATION

18 Dec 2014

FUEL CARD INDUSTRY MEETS AT EUROPOL TO TACKLE PAYMENT CARD FRAUD

NEWS/PRESS RELEASE

GLOBAL AIRPORT ACTION DAYS (GAAD)

OPERATION

OPERATION ONYMOUS

OPERATION

OPERATION IMPERIUM

OPERATION

29 Sep 2014

ORGANISED CRIME GROUPS EXPLOITING HIDDEN INTERNET IN ONLINE CRIMINAL SERVICE INDUSTRY

NEWS/PRESS RELEASE

24 Sep 2014

ORGANISED CRIME NETWORKS TARGETED IN HUGE LAW ENFORCEMENT OPERATION IN EUROPE

NEWS/PRESS RELEASE

OPERATION ARCHIMEDES

OPERATION

17 Jul 2014

INTERNATIONAL NETWORK OF ROMANIAN CYBERCRIMINALS DISMANTLED

NEWS/PRESS RELEASE

OPERATION ROMEX2

OPERATION

22 May 2014

JOINT OPERATION TAKES DOWN BULGARIAN ORGANISED CRIME NETWORK AFFECTING EUROPEAN ELECTRONIC PAYMENTS

NEWS/PRESS RELEASE

OPERATION ECHO

OPERATION