EAST Publishes European Fraud Update 2-2018

association-secure-transactions.eu/east-publishes-fraud-update-2-2018/

05/07/2018

EAST has published its second European Fraud Update for 2018. This is based on country crime updates given by representatives of 18 countries in the Single Euro Payments Area (SEPA), and 3 non-SEPA countries, at the 45th EAST meeting held in The Hague on 6th June 2018.

Payment fraud issues were reported by fifteen countries. Seven countries reported card-not-present (CNP) as a key fraud driver. Two countries reported attempted 'Forced Post' fraud, possible when some point of sale (POS) terminals allow the 'force sale' functionality. One country reported a new form of malware on android mobile phones, distributed with a fake application uploaded from third-party android stores. Another country reported cases of SIM swap fraud, where fraudsters authorise a bank transfer by switching the customer's mobile phone number over to a new SIM and intercept the authorisation message. To date in 2018 the EAST Payments Task Force (EPTF) has published five Payment Alerts covering phishing, malware on mobile phones, fraudulent mobile Apps and CNP fraud.

ATM malware and logical security attacks were reported by nine countries. Five of the countries reported ATM related malware. In addition to Cutlet Maker (used for ATM cash-out) a new variant called WinPot has been reported – this is used to check how many banknotes are in an ATM. Six countries reported the usage (or attempted usage) of 'black-box' devices to allow the unauthorised dispensing of cash. To date in 2018 the EAST Expert Group on All Terminal Fraud (EGAF) has published seven related Fraud Alerts. To help counter these threats Europol, supported by EAST EGAF, has published a document entitled

‘Guidance and Recommendations regarding Logical attacks on ATMs’. It covers mitigating the risk, setting up lines of defence and identifying and responding to logical attacks. This is available in four languages: English, German, Italian and Spanish.

Card skimming at ATMs was reported by fourteen countries. For the first time one country reported the arrest of a Chinese national in connection with such attacks. The usage of M3 – Card Reader Internal Skimming devices remains most prevalent. This type of device is placed at various locations inside the motorised card reader behind the shutter. Six countries reported such attacks. One country reported the use of M2 – Throat Inlay Skimming Devices. Skimming attacks on other terminal types were reported by five countries, four of which reported such attacks on unattended payment terminals (UPTs) at petrol stations. To date in 2018 EAST EGAF has published ten related Fraud Alerts.

Year to date International skimming related losses were reported in 31 countries and territories outside SEPA and in 3 within SEPA. The top three locations where such losses were reported remain Indonesia, the USA and India.

Three countries reported incidents of Transaction Reversal Fraud (TRF), two of which reported new attack variants. To date in 2018 EAST EGAF has published four related Fraud Alerts.

Ram raids and ATM burglary were reported by eight countries. Six countries reported explosive gas attacks, one of which reported such attacks against ATS machines for the first time. Another reported that explosive gas attacks against ATMs have started for the first time. Five countries reported solid explosive attacks. The spread of such attacks is of great concern to the industry due to the risk to life and to the significant amount of collateral damage to equipment and buildings. To date in 2018 the EAST Expert Group on ATM & ATS Physical Attacks (EGAP) has published five related Physical Attack Alerts.

The full Fraud Update is available to EAST Members (National and Associate).