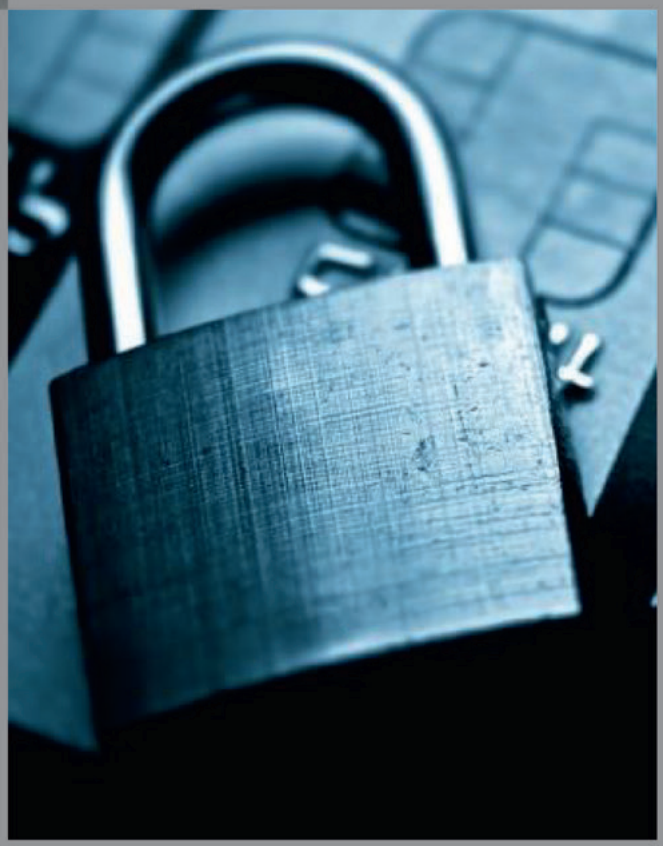
МОШЕННИЧЕСТВО В ТЕРМИНАЛАХ (ATM, UPT И POS). ОПРЕДЕЛЕНИЯ И ТЕРМИНЫ.

ЭКСПЕРТНАЯ ГРУППА EAST ПО МОШЕННИЧЕСТВУ В ТЕРМИНАЛАХ (EGAF)



Версия 1.6. Изданная

Авторы:
Christian Beine – Diebold Nixdorf
Ben Birtwistle – NatWest Bank plc
Otto de Jong – ING
Lachlan Gunn – EAST
Claire Shufflebotham – TMD Security

Дизайн: Niek Westendrop – TMD Security

12/12/2018

ПОДГОТОВЛЕНО: THE EUROPEAN ASSOCIATION FOR SECURE TRANSACTIONS

www.association-secure-transactions.eu

ПЕРЕВЕДЕНО: Украинская межбанковская Ассоциация членов платежных систем «ЕМА» – национальный представитель Украины в EAST с 2012 года

www.ema.com.ua

ПРИ УЧАСТИИ:
Николай Дош – Ассоциация участников Мастеркард
Александр Пекшеев – Банк Пивденный

Про EAST

EAST – неприбыльная организация, основанная в 2004 году, национальные представители которой осуществляют сбор и обмен информацией о мошенничестве в банкоматах, терминалах и о платежном мошенничестве в своих странах/регионах. Была основана как Европейская команда безопасности банкоматов (European ATM Security Team – EAST) – трансграничная рабочая группа, объединяющая профессионалов из индустрии банкоматов (и других терминалов, близких к банкоматам в вопросах безопасности) и правоохранительных органов. В 2017 EAST изменил свое название на Европейская Ассоциация Безопасных Транзакций.

Миссия EAST – собирать и предоставлять информацию для платежной индустрии, а также поддерживать эффективное рассмотрение вопросов безопасности платежей и банкоматов в профильных центральных институтах Европы, благодаря координации совместных европейских инициатив.

EAST внедрила процедуры, улучшающие сотрудничество производителей терминального оборудования, финансового сектора и правоохранительных органов, в частности, Европола, для того, чтобы повысить осведомленность и улучшить результаты борьбы с организованными трансграничными преступлениями. Национальные представители EAST представляют 35 стран.

EAST Expert Group on ATM Fraud (EGAF) создана в мае 2013, – комиссия, в состав которой входят ведущие европейские эксперты, исследующие тенденции банкоматного мошенничества в Европе, методологию совершения преступлений и осуществляющие разработку мероприятий противодействия, а также создание регламентирующих документов для индустрии и правоохранительных органов. Через систему Fraud Alert может доносить важную и срочную информацию до своих Национальных и Ассоциированных членов.

EAST Expert Group on ATM Physical Attaks (EGAP) создана в мае 2014, – комиссия, в состав которой входят ведущие европейские эксперты, которые исследуют тенденции развития физических атак на банкоматы в Европе, методологию осуществления атак и разрабатывают мероприятия по противодействию. Также администрирует и регулярно обновляет список средств по защите банкоматов от физических атак. Через систему Fraud Alert может доносить важную и срочную информацию до своих Национальных и Ассоциированных членов.

EAST Payments Task Force (EPTF), создана в январе 2016, – комиссия, в состав которой входят ведущие европейские эксперты, которые исследуют тенденции развития платежного мошенничества Европе и формируют обобщённую статистику. Через систему Fraud Alert может доносить важную и срочную информацию до своих Национальных и Ассоциированных членов.

Содержание:

Официальные уведомления и отказы от ответственности

EAST предприняты разумные усилия для представления информации в корректном, открытом и объективном изложении. Тем не менее, EAST не обещает и не гарантирует полноту приведённых определений.

К тому же информация в этом документе разрабатывалась EAST совместно с другими участниками, потому в нем не исключены ошибки или вероятность представления ошибочной информации. Ответственность за прямой, непрямой и последующий ущерб, категорически отрицается и исключается.

МОШЕННИЧЕСТВО В ТЕРМИНАЛАХ (ATM, UPT & POS). ОПРЕДЕЛЕНИЯ И ТЕРМИНЫ

Введение

В этом документе даны определения терминам мошенничества, которые используются EAST при выпуске Fraud Alert-ов, при сборе статистики для European Payment Terminal Reports и European Fraud Updates. Они разработаны членами экспертной группы EAST по мошенничеству в терминалах. Типы терминалов, для которых сформулированы эти определения:

- ATM – Automated Teller Machine – банкоматы
- POS – Point of Sale Terminal – терминалы в торгово-сервисных предприятиях
- UPT – Unattended Payment Terminal – терминалы самообслуживания (в т.ч. транспортные и по продаже билетов для парковки)

Каждый вид мошенничества в терминалах имеет специфический преступный умысел. Для их понимания EAST EGAF определила 6 разновидностей преступных целей. Эти цели являются ключом к пониманию методов, с использованием которых злоумышленники реализуют преступный умысел и с их помощью в документе определены все виды терминального мошенничества.

Целью определения видов мошенничества и соответствующего преступного умысла является внедрение общей для всей индустрии и правоохранительных органов терминологии по мошенничеству в терминалах.

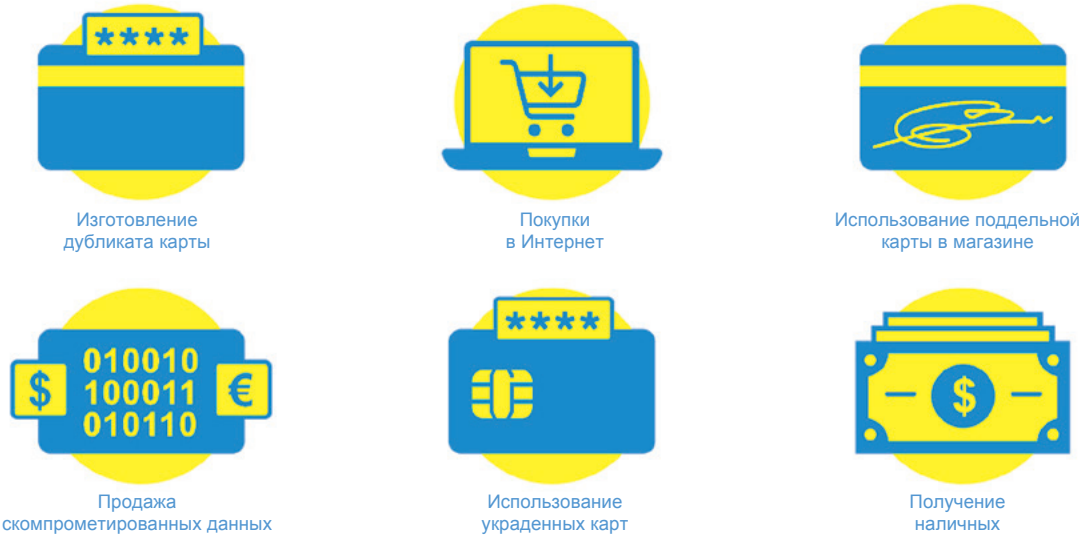
В этом документе представлена только базовая классификация терминологии. Более полная информация представлена в документе с ограниченным доступом «Стандартизация терминологии по размещению устройств компрометации данных в банкоматах». Этот документ предназначен для внутреннего использования членами EAST, как Национальными, так и Ассоциированными, в т.ч. сотрудниками правоохранительных органов – представителями тех организаций, которые еще не являются Ассоциированными членами EAST.

Базовые определения типов мошенничества и терминологии по размещению устройств компрометации данных также доступны на сайте EAST
https://www.association-secure-transactions.eu/

Использование документа

Преступный умысел

У мошенников существуют следующие возможности для реализации преступного умысла. Существующие шесть возможностей изображены в виде иконок на рисунке ниже (CNP – card-not-present), в дальнейшем они будут использоваться для визуализации определений типов мошенничества в терминалах.



Определение видов мошенничества в терминалах

Skimming

Определение
- Установка неавторизованных устройств для получения данных магнитной полосы платежной карты.

Реализация
- Преступники атакуют слот для чтения карт, устанавливая внешние устройства поверх отверстий для вставки карт или внутренних устройств в кардридер.
- Дополнительно устанавливается ПИН-камера или накладная клавиатура для компрометации ПИНа карты.
- Обычно оба устройства демонтируются спустя некоторое время.

Характеристики
- Устройство содержит, как минимум, одну считывающую магнитную головку и установлено поверх отверстия для введения карт или непосредственно в кардридер.

Последствия для владельца банкомата
- Финансовые: Нет
- Операционные: Повреждения, недоступность сервисов
- Репутационные: Компрометация данных и потери у эмитентов карт.

Последствия для Картодержателей
- Клиент проводит обычную транзакцию и забирает карту.

Shimming

Определение
- Перехват («пассивный») и/или изменение («активный») информации, которая передается от EMV карты к чиповому интерфейсу кардридера.

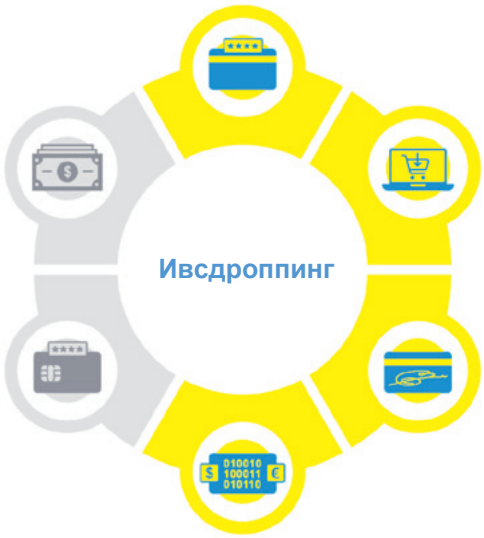
Реализация
- Преступник размещает устройство в кардридере.
- Дополнительно устанавливается ПИН-камера или накладная клавиатура для компрометации ПИН-кода карты.
- Обычно оба устройства демонтируются спустя некоторое время.

Характеристики
- Устройство устанавливается в кардридере и находится между чипом карты и чиповым интерфейсом кардридера.

Последствия для владельца банкомата
- Финансовые: Нет
- Операционные: Повреждения, недоступность сервисов
- Репутационные: Компрометация данных и потери у эмитентов карт

Последствия для Картодержателей
- Клиент проводит обычную транзакцию и забирает карту.

Eavesdropping



Определение
- Установка неавторизованных устройств для получения данных платежной карты.

Реализация
- Преступники устанавливают устройство внутри банкомата, чаще всего высверливая отверстие возле кардридера на лицевой части банкомата.
- Дополнительно устанавливается ПИН-камера или накладная клавиатура для компрометации ПИН-кода карты.
- Обычно оба устройства демонтируются спустя некоторое время.

Характеристики
- Устройство использует легальную функциональность кардридера банкомата по считыванию данных карты.
- Как правило, это достигается путем «прослушивания», в процессе которого крадутся карточные данные, которые проходят через кардридер, или соединение считывающей (или пре-считывающей) магнитной головки с кардридером.

Последствия для владельца банкомата
- Финансовые: Нет
- Операционные: Повреждения, недоступность сервисов
- Репутационные: Компрометация данных и потери у эмитентов карт

Последствия для Картодержателей
- Клиент проводит обычную транзакцию и забирает карту.

Card Trapping

Определение
- Незаконные физические манипуляции с банкоматом, которые не позволяют клиенту получить свою карту после выполнения операций.

Реализация
- Преступники устанавливают устройство поверх или внутри картоприемника перед тем, как клиент проведет операцию, и забирают его после операции.
- ПИН-код может быть получен путем подглядывания через плечо, ПИН-камеры или накладки на ПИН-клавиатуру.

Характеристики
- Устройство позволяет карте зайти в банкомат и удерживает ее в момент возврата, предотвращает возврат карты банкоматом механическим путем.

Последствия для владельца банкомата
- Финансовые: Нет – все финансовые потери будут у банка-эмитента
- Операционные: Повреждения, недоступность сервисов
- Репутационные: Могут возникнуть, так как клиенты думают, что банкомат изъял карту, а потом узнают, что по карте прошли мошеннические транзакции.

Последствия для Картодержателей
- Клиент остается без карты.

Cash Trapping

Определение
- Незаконные физические манипуляции с окном для выдачи наличных в банкомате, которые препятствуют получению наличных Держателем платежной карты.
- Два типа: Внешний захват наличных (захватывающее устройство расположено поверх заслонки отверстия для выдачи наличных) и Внутренний захват наличных (улавливающее устройство расположено в механизмах выдающей части диспенсера – презентере банкомата.

Реализация
- Внешнее устройство для захвата наличных устанавливается перед каждой транзакцией клиента и демонтируется сразу после нее.
- Внутренние захватывающие устройства могут быть установлены злоумышленниками путем принудительного открытия заслонки отверстия для выдачи наличных или путем получения доступа к диспенсеру при выполнении транзакции на небольшую сумму по картам, которые они контролируют.
- Внутреннее устройство захвата наличных может использоваться для нескольких последовательных транзакций.

Характеристики
- Устройство должно располагать функционалом для захвата наличных и предотвращать возврат пачки банкнот назад механизмами «презентерной» части диспенсера.

Последствия для владельца банкомата
- Финансовые: Будут понесены финансовые убытки
- Операционные: Повреждения, недоступность сервисов
- Репутационные: Могут возникнуть в случае, если Держатель платежной карты считает, что банкомат не выдал наличные по технологическим причинам, а позже обнаруживает, что прошло списание средств по счету.

Последствия для Картодержателей
- Клиент не получает деньги.

Transaction Reversal Fraud

Определение
- Незаконные физические манипуляции с процессом выдачи наличных в банкомате.

Реализация
- Необходимо наличие активной платежной карты для использования в банкомате, открытой к счету, на котором есть необходимая денежная сумма.
- Выполняется транзакция, затем физически нарушается последовательность выдачи наличных, как с использованием, так и без использования мошеннического устройства.
- Злоумышленники забирают купюры таким образом, чтобы банкомат зафиксировал, что они не были получены клиентом, и передал сообщение эмитенту о отмене транзакции.

Характеристики
- Когда выполняется без дополнительного устройства, преступникам нужна сноровка и синхронность.
- Когда используется дополнительное устройство, тогда так же, как при внутреннем захвате наличных, устройство должно быть способным захватывать наличные и противостоять механическим попыткам банкомата изъять его.

Последствия для владельца банкомата
- Финансовые: будут понесены финансовые убытки
- Операционные: Повреждения, недоступность сервисов
- Репутационные: Нет

Последствия для Картодержателей
- Нет

Malware

Определение
- Нелегальное ПО, или легальное ПО, используемое с преступной целью на компьютере банкомата:
- Jackpotting: Цель – контроль функции выдачи наличных для получения всех банкнот из кассет банкомата.
- MitM: Цель – коммуникации между компьютером банкомата и хостовой системой эквайера для фальсификации ответов хоста и получения денег при их фактическом отсутствии на счете.
- Программный скимминг: Цель – данные карт и ПИН-коды для изготовления дубликатов карт для последующих мошеннических транзакций.

Реализация
- Злоумышленники устанавливают вредоносное ПО на компьютер банкомата локально или удаленно через сеть.
- Контроль работы вредоносного ПО выполняется локально или удаленно через сеть.
- Локальная инсталляция может быть выполнена через незащищенные коммуникационные интерфейсы, например, USB, и/или путем загрузки неавторизованной операционной системы.

Характеристики
- Вредоносное ПО может содержать функционал для исключения его обнаружения, обратного инжиниринга и неавторизованного использования, также может содержать функцию безопасного удаления.

Последствия для владельца банкомата
- Финансовые: Да, сразу же, в случае прямого диспенса и атак MitM, или в будущем, как источник компрометации данных при программном скимминге.
- Операционные: Повреждения, недоступность сервисов.
- Репутационные: Программный скимминг и MitM могут привести к компрометации данных и финансовым потерям эмитентов.

Последствия для Картодержателей
- Зависят от типа вредоносного ПО. При программном скимминге и MitM для клиента транзакции проходят как обычно, в случае прямого диспенса банкомат может оказаться в нерабочем состоянии или поврежденным.

Замечание:

MitM – сокращение от **Man-in-the-Middle.** MitM EAST Payments Task Force (EPTF) определяет как:

В криптографии и компьютерной безопасности атака MitM – атака, при которой атакующий тайно проникает в коммуникации между двумя участниками, которые уверены, что они общаются друг с другом.

Black Box

Определение
- Разновидность атак типа Jackpotting (прямая выдача наличных, так называемый прямой диспенс)
- Подключение неавторизованного устройства, которое отправляет диспенсеру банкомата команду на выдачу всех банкнот из кассет банкомата.

Реализация
- Преступники открывают верхнюю часть банкомата или делают отверстия в лицевой части для того, чтобы подключить неавторизованное устройство и дать с его помощью команду прямого диспенса .

Характеристики
- Устройство должно иметь возможность быть физически и логически подключенным к диспенсеру непосредственно через USB или другие аппаратные интерфейсы.
- Преступники отсоединяют системный блок компьютера банкомата от кабеля, ведущего к диспенсеру банкомата, и подключают этот кабель к своему переносному компьютеру – ноутбуку/планшету. Таким образом, компьютер преступников подключен к системе выдачи банкомата.

Последствия для владельца банкомата
- Финансовые: Будут понесены финансовые убытки.
- Операционные: Повреждения, недоступность сервисов.
- Репутационные: Нет

Последствия для Картодержателей
- Нет

Термины, определяющие места расположения устройств компрометации данных в терминалах

Ниже выдержка из опубликованного Справочника «Стандартизация терминологии по определению мест расположения устройств компрометации данных в банкоматах».

Тип устройства	Описание
M1 Overlay Skimming Device (накладное устройство для скимминга, накладка)	Считывающая головка этого накладного устройства расположена вне корпуса банкомата перед отверстием картоприемника, устройство может накрывать весь слот моторизованного кардридера.
M2. Throat Inlay Skimming Device (вставное устройство для скимминга, вставка)	Считывающая головка этого типа устройства находится внутри слота для введения карт перед шаттером кардридера.
M3. Card Reader Internal Skimming Device (внутреннее устройство для скимминга)	Считывающая головка этого типа устройства размещается в разных местах внутри моторизованного кардридера за шаттером. Этот тип устройства иногда называют устройством «глубокой вставки» («deep insert»).
D1 Overlay Skimming Device (накладное устройство для скимминга, накладка)	Считывающая головка этого накладного устройства находится вне корпуса банкомата перед слотом DIP кардридера и устройство может накрывать весь слот DIP кардридера.
D2 Throat Inlay Skimming Device (вставное устройство для скимминга, вставка)	Считывающая головка устройства этого типа находится внутри DIP кардридера перед считывающей головкой кардридера.
D3 Card Reader Internal Skimming Device (внутреннее устройство для скимминга)	Считывающая головка устройства этого типа находится внутри DIP кардридера за считывающей головкой кардридера.
E1 Pre-read Head Eavesdropping Device (устройства для подслушивания, присоедененное к головке предварительного считывания).	Этот тип устройства прикрепляется к головке предварительного считывания моторизованного кардридера.
E2 Read Head Eavesdropping Device (устройства для подслушивания, присоедененное к головке считывания).	Этот тип устройства прикрепляется к головке предварительного считывания кардридера.
E3 PCB Eavesdropping Device (устройства для п подслушивания, присоедененное к электронной плате кардридера).	Этот тип устройства присоединяется к разъемам электронной платы контроллера кардридера.
E4 Communication Eavesdropping Device (устройства для подслушивания, присоедененное к коммуникационному интерфейсу).	Этот тип устройства прикрепляется к коммуникационному (например, USB) интерфейсу кардридера.
S1 S1 Card Reader Internal Shimming Device (шиммингговое устройство) :	Этот тип устройства размещается в середине кардридера.