Абсолютно все дыры обязаны быть пропатчены, а также обязаны быть установлены последние обновления. Это даст возможность сдержать Dos-атаки, эксплуатирующих баги на сервисах.

Все сетевые сервисы, назначенные с целью административного применения, обязаны быть скрыты brandmouer от абсолютно всех недоброжелателей. В таком случае атакующий никак не сумеет применять их с целью выполнения Dos-атаки либо bruteforce.

На подходе к серверу обязана быть система слежения за трафиком, чтобы отследить любую начинающиеся атаку на систему, а также принять меры её предотвращения.

Спиок використаних джерел:

1. Классификация DDoS-атак; краткий обзор современных технологий: Режим доступа: http://surl.li/hhmc
2. Атака сетевых зомби: Режим доступа: http://surl.li/hhme

Ключевые слова: Кибербезопасность, Атака, Взлом, Афера.
Ключові слова: Кібербезпека, Атака, Злом, Афера.
Keywords: Cybersecurity, Attack, Breaking, Scam.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Лоза Илья Олегович
Национальный университет «Одесская юридическая академия»,
студент 2-го курса факультета кибербезопасности
и информационных технологий

КАРДИНГ

С момента появления пластиковых банковских карт жизнь людей стала в разы проще. Больше не нужно ходить за зарплатой к «начальству», думать где хранить свои денежные средства, а также удобное осуществление покупок. Но преступники не дремлют, и они также начали активно использовать эти возможности в своих не совсем законных целях. А именно

зарождение нового вида мошенничества, что получило название «Кардинг».

Кардинг – это вид мошенничества, в котором напрямую задействуются платежные карты пользователей, либо же реквизиты этих карт для дальнейшего их использования. В простонародье можно именовать, как воровство, только в основном это происходит в цифровом виде, но всё же на некоторых этапах мошенник также обращается к так называемой «Социальной инженерии», но где, и как она используется будет описано немного далее.

Для начала ознакомимся с неким словарём «кардера», и далее пойдём по порядку.

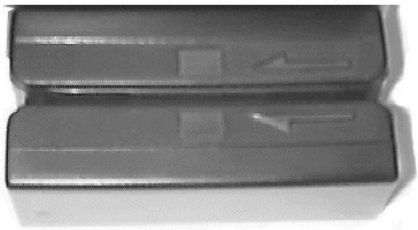
Словарь «кардера»

- **Track(трек)** – информация с магнитной полосы платежной карте.
- **дроп** – человек, который будет заниматься обналичиванием «картона».
- **Credit Card** – собственно сама кредитная карта.
- **White Plastic(белый пластик) –** служит для изготовления банковских карт, в основном тип пластика CR-80.
- **Кард-холдер –** реальный держатель (владелец) карты.
- **Dump –** трек код и пин код карты.
- **Голубь / Глобус –** на каждой кредитке есть голограмма, на Visa – это голубь, на Mastercard – полушарие.
- **Скарженный**- украденный с помощью «кардинга»

Где кардеры берут информацию о картах (CC)

1. Ридеры – устройство выполняет считывание информации с магнитной полосы. Бывают как стационарные, так и портативные на батарейках (прим. Рис 1). В свою очередь у «кардеров» есть специальные агенты, которые устроены кассирами в крупных магазинах, работниками гостиниц, ресторанов. Вкратце, они устроены в тех местах, где есть оплата картой, и с помощью «ридера», они передают информацию непосредственно самому «кардеру». Цена такого труда варьируется от

20$ и до 250$ в зависимости от того, сколько «агент» раздобыл информации.



Mini-Mag Magstripe reader (PMR 102)

Рис. 1. Портативный ридер PMR102

2. Взлом баз данных – этот способ является одним из самых распространенных в наше время, злоумышленнику достаточно сломать процессинговую сеть, через которую проходят физ. платежи (не виртуальные), откуда и берется база данных. Также это работает и с виртуальными магазинами, в которых незащищенное соединение, и имеется способ оплаты картой, здесь же все происходит гораздо проще, нежели в первом варианте, ибо такие магазины в основе своей очень легки на взлом.

3. Покупка дампов – очень актуальный способ, есть достаточно большое количество сервисов «.onion», которые за определенную плату предоставляют вам краденые реквизиты банковских карт. В среднем цена за единицу 1-3, за Американские карты просят до 25$. Они же в свою очередь пользуются одним из вышеперечисленных методов получения этих данных. Способ является самым легким, но также есть БОЛЬШОЙ риск быть обманутым, за счёт того, что сервисы эти расположились под надежной маской TOP.

4. Скимминг – на сегодняшний день почти неосуществимый способ. На приёмник карт банкомата ставится дополнительный пластиковый ридер, который не особо сильно бросается в глаза. А клавиатуру накрывает очень тонкая клавиатура, кото-

рая будет перехватывать ПИН-код держателя карты (кардхолдэра). По итогу выходит банкомат «бабломёт», который полностью перехватит данные вашей карты, и сольет их мошеннику. Неосуществимый этот способ из-за того, что банкоматы периодически обслуживаются работниками банков, и находятся под беспрерывным наблюдением камер.

С помощью всех вышеперечисленных способов мошенник получает дампы карты, далее следует сложный этап кардинга (снятие средств).

Перевод данных на белый пластик

Для дальнейшей работы с дампами мошенниками потребуется «белый пластик» и «энкодер».

1. Используется для этого специальный пластик с маркировкой «**CR-80»**. Раздобывают кардеры такой пластик также на **теневых ресурсах** сети интернет.

2. Далее в ход идёт **Энкодер**.

Энкодер – это специальное устройство, которое из обычной белой карты делает готовую магнитную копию. Для этого достаточно разобраться с несложной программой энкодера, после чего провести белый пластик через устройство. Современные Энкодеры также предоставляют возможность устанавливать на белый пластик магнит для бесконтактной оплаты.

Рис. 2. Энкодер

3. С помощью определенной махинации, мошенник получает ПИН-код карты, либо если дамп куплен, в основном код к нему прилагается. После чего мошенник может снимать деньги с помощью магнитной копии с практически любого банкомата.

Также есть способы получения средств со «скарженных» карт методом нахождения дропа.

Пример: «Дроп» хочет себе новый телефон, который стоит 10к. «Кардер» покупает этот телефон онлайн с помощью оплаты картой на адрес заказчика. Заказчик в свою очередь отправляет 30% суммы мошеннику, по итогу «кардер» обналичил 3к без каких-либо рисков, а заказчик получил новый телефон за 30% от его стоимости. Обе стороны остались довольны, только вот сторона заказчика не учла, что его адрес засветился, и в случае дальнейших разбирательств крайним останется он.

Методы защиты от кардинга

- Быть бдительным при использовании банкоматов, на наличие посторонних устройств.
- Никогда не передавать карты третьим лицам.
- При осуществлении покупок смотреть за тем, чтобы карта использовалась по назначению
- Не сообщать никому трехзначный код, и ПИН-код
- Работники банка не будут у вас спрашивать CVV или PIN, это конфиденциальная информация.

«Корысть дает новые идеи.
Идеи дают новые способы Теневого заработка.
Кардинг не умер.»

Список использованных источников:

1. Рисунок 1 [Источник фотографии]. URL – http://www.e-scan.com/profiles/miniportable.htm

2. Рисунок 2 [Источник фотографии]. URL – https://www.ebay.com/itm/Magnetic-Stripe-Card-Reader-Writer-Encoder-MSR206–606-/310325315390

3. Информация о понятии «Кардинг» [Ссылка на ресурс]. URL – https://xakep.ru/2002/07/02/15687/

4. Словарь кардера [Ссылка на ресурс]. URL – https://rabotadropom.work/chto-takoe-karding/

Ключевые слова: Кардинг, кардер, ридер, взлом, мошенничество.
Ключові слова: Кардинг, кардер, рідер, злом, шахрайство
Key words: Carding, carder, reader, hacking, fraud

***Науковий керівник**: к.т.н., доцент Задерейко О. В.*

Орел Анастасія Олександрівна
Національний університет «Одеська юридична академія»,
студентка 2-го курсу факультету кібербезпеки
та інформаційних технологій

АНАЛІЗ МЕТОДУ ВІОЛИ-ДЖОНСА ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧ

Спроби навчити комп'ютер розпізнавати образи розпочалися ще в 60-тих роках, але тільки 2001 року американські дослідники Поло Віола та Майкл Джонс розробили алгоритм пошуку облич на зображеннях, який згодом став революційним у сфері розпізнавання образів [1; 2]. Нині ця технологія розпізнавання використовується повсюдно. Її застосовують для ідентифікації пішоходів чи автомобілістів на дорозі, людей в аеропортах, у системах безпеки і контролю доступу, при створенні систем комп'ютерного зору в робототехніці, у сенсорних телефонах для ідентифікації власника і розблокування системи захисту, в усіх сучасних фотоапаратах для налаштування автофокусу, у камерах для розпізнавання емоцій та міміки лиця та навіть у дзеркалах з доповненою реальністю, які допомагають у віртуальному виборі окулярів, доборі вдалих відтінків макіяжу тощо.

Розповсюдженість алгоритму Віоли-Джонса з-посеред інших методів розпізнавання облич зумовлена прийнятною швидкістю оброблення і точністю визначення даних, що дало змогу застосовувати цей алгоритм не лише у роботі із зображеннями, а й у відео потоках.