Безопасность личной информации в сети

Выполнил студент группы
ЭЛ-07
Некоркин Роман

Безопасность личной информации в сети

- Аккаунты являются "хранилищами" личной информации, на них можно найти начиная от личной информации и заканчивая данными паспорта и банковских карт. А так-же фотографии с аккаунтом могут использоваться с целью вымогания денег у родственников или для шантажа личными фотографиями

Способы кражи данных

Способов кражи данных очень много но мы разберём основные

Брутфорсинг

Фишинг

Вирусы и Кейлогеры

Сниффер

Брутфорсинг

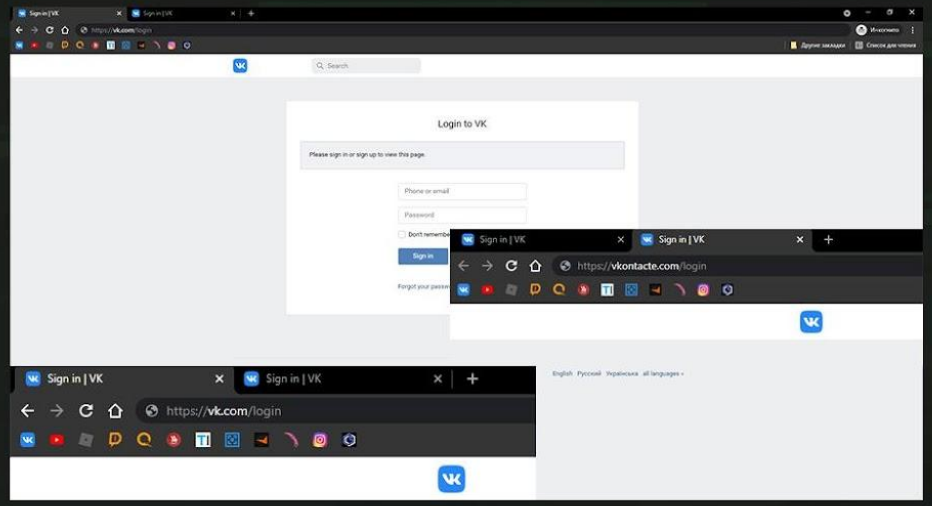
Брутфорсом называется метод взлома учетных записей путем подбора паролей к ним. Термин образован от англоязычного словосочетания «brute force», означающего в переводе «грубая сила». Суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью рано или поздно найти правильную. Брутфорс направлен на получение доступа к личным данным конкретного пользователя: аккаунтам социальных сетей, почте, сайту.

Во время общения через интернет, в том числе используя мошеннические схемы, злоумышленник старается узнать логин, персональные сведения и другую информацию, которая понадобится для подбора пароля. Далее взломщик прописывает в специальную программу адрес ресурса, к которому нужен доступ, логин учетной записи, подключает словарь и подбирает пароль.

BruteX – программа для брута

Фишинг

Фишинг (phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логины и пароли к банковским картам, учетным записям). Чаще всего фишинг представляет собой массовые рассылки писем и уведомлений от имени известных брендов, банков, платежных систем, почтовых сервисов, социальных сетей. Такие письма, как правило, содержат логотип, сообщение и прямую ссылку на сайт, внешне неотличимый от настоящего. По ссылке требуется перейти на сайт «сервиса» и под различными предлогами ввести конфиденциальные данные в соответствующие формы. В результате мошенники получают доступ к аккаунтам и банковским счетам пользователей.



Вирусы и кейлогеры

Компьютерный вирус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.

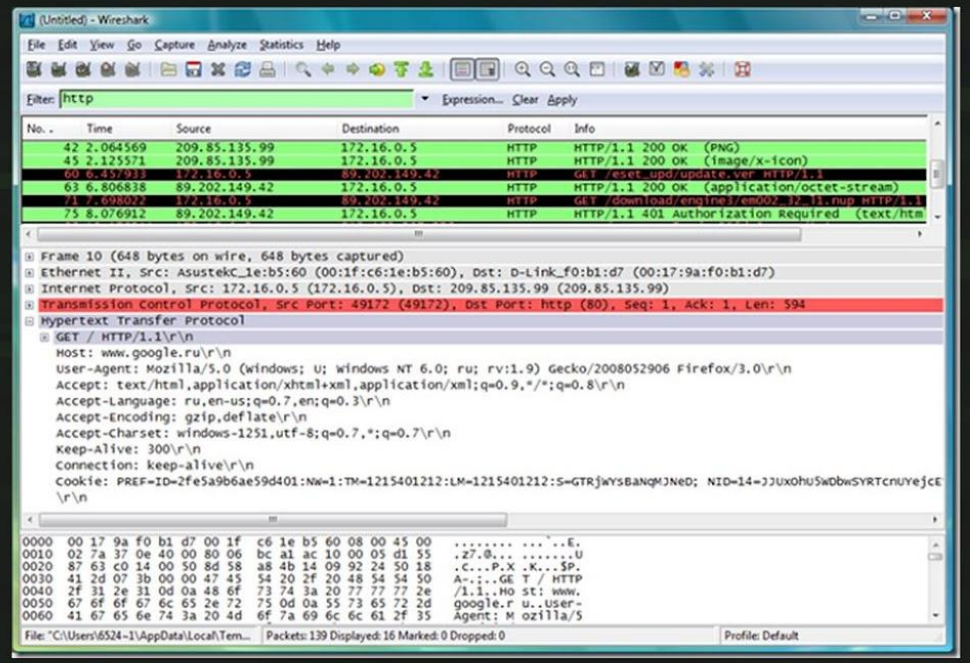
Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами.

Keylogger фиксирует все действия пользователя на клавиатуре, т.е. это некий «репитер» (повторитель), готовый в любой момент «слить» (куда следует) все то, что он за Вами нафиксировал. Перехват нажатий клавиш может использоваться обычными программами и часто применяется для вызова функций программы из другого приложения с помощью «горячих клавиш» или, например, для переключения неправильной раскладки клавиатуры (как Keyboard Ninja).

Снифер

Сниффер не всегда является вредоносным. В действительности, данный тип ПО часто используется для анализа сетевого трафика в целях обнаружения и устранения отклонений и обеспечения бесперебойной работы. Однако сниффер может быть использован с недобрым умыслом. Снифферы анализируют все, что через них проходит, включая незашифрованные пароли и учетные данные, поэтому хакеры, имеющие доступ к снифферу, могут завладеть личной информацией пользователей. Кроме того, сниффер может быть установлен на любом компьютере, подключенном к локальной сети, без необходимости его обязательной установки на самом устройстве - иными словами, его невозможно обнаружить на протяжении всего времени подключения.

Droidsheep – сниффер для Андроид телефонов



Как защитить личные данные в Интернете:

Не используйте открытые Wi-Fi-сети. Они могут выглядеть как вполне надежный источник Интернета, предоставленный местным кафе или даже библиотекой, но вам будет сложно отличить «добропорядочный» Wi-Fi от «зловредного».

Избегайте ненадежных паролей. Слабые комбинации практически ни от чего не защищают. На самом деле не так сложно запомнить надежный пароль.

Каждая соцсеть — это бесценный источник информации для злоумышленников, собирающих персональные данные, которые они затем используют для обмана и мошенничества. Поэтому так важно правильно настроить конфиденциальность вашего профиля Facebook, «ВКонтакте», «Одноклассников» и любой другой соцсети.

Относитесь осторожно к ссылкам и интернет-адресам, присланным в незапрашиваемыми вами электронных письмах или текстовых сообщениях. Не передавайте критически важную информацию в незашифрованном виде по электронной почте, будьте осмотрительны, нажимая на ссылки в электронных письмах.