УГРОЗЫ ДЛЯ БАНКОВСКИХ КЛИЕНТОВ. НЕЦЕЛЕВЫЕ АТАКИ

Часть 1

ROOT LEVEL RESOURCES

Root Level Resources продолжает следить за актуальными угрозами информационной безопасности. Киберпреступники не сдают позиций, быстро реагируют на известия о новых уязвимостях, адаптируются и продолжают совершенствовать методы своих атак.

Так, основной угрозой для клиентов банков остаются фишинг и социальная инженерия. При этом, наиболее динамично развивающейся угрозой является JS-сниффферы[1], которые позволяют атакующим зарабатывать больше, чем на банковских троянах.

Компрометация финансовых данных

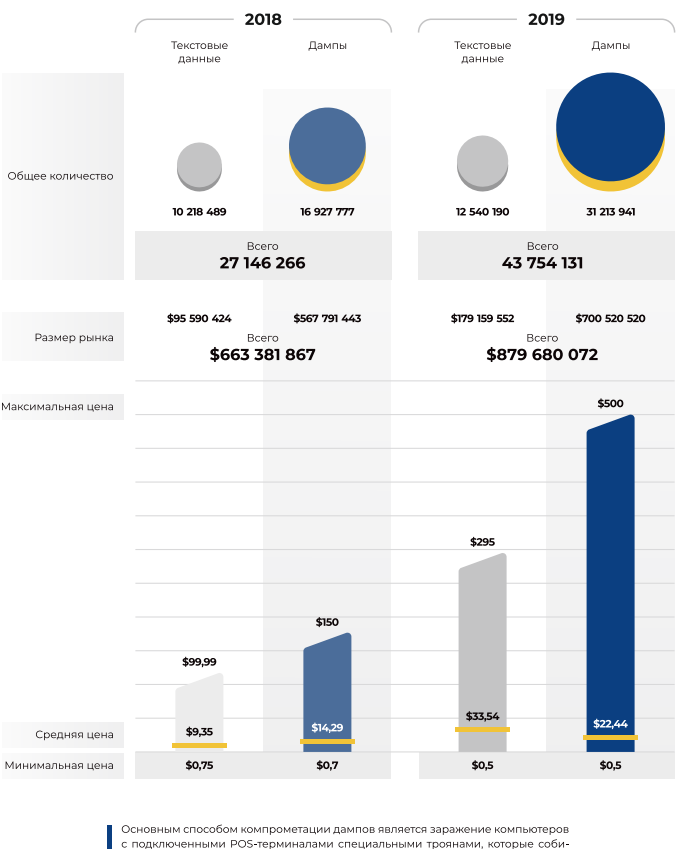
Рынок сбора данных банковских карт продолжает расти. Его можно условно разделить на два сегмента: **текстовые данные**[2] и **дампы**[3].

Для сбора текстовых данных используют фишинговые сайты, банковские трояны для ПК, Android и банкоматов, а также JS-сниффферы[4].

Дампы собираются с помощью скимминговых устройств и троянов для компьютеров с подключенными POS-терминалами.

Тенденции кардинга[5]

ROOT LEVEL RESOURCES



Основным способом компрометации дампов является заражение компьютеров с подключенными POS-терминалами специальными трояна, которые собирают информацию о банковских картах из оперативной памяти.

В 2019 году, специалистами сетевой безопасности, выявлено 4 новых POS-трояна, которые ранее оставались неизвестными и активно использовались в атаках.

Новые трояны

- DMSniff
- Glitch
- Badhatch
- RtPOS

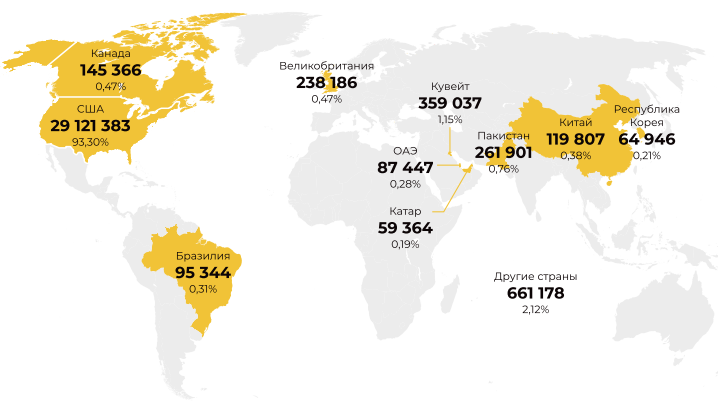
Старые но еще активные трояны

- FrameworkPOS
- MajikPos
- TinyPOS
- UdPOS
- Alina

Так, в 2018-2019 произошло 17 громких массовых утечек, 14 из которых были идентифицированы специалистами, и только 3 не удалось связать с конкретной компанией. Однако реальный объем скомпрометированных дампов может быть больше. Так, при обнаружении дампов практически отсутствуют технические детали, что усложняет процесс атрибуции и позволяет делать только предположения о том, кто был причастен к утечке.

География источников дампов

ROOT LEVEL RESOURCES



JS-сниферы - новый тренд компрометации банковских карт

Именно благодаря развитию JS-снифферов в 2019 году, картинг стал самым быстрорастущим сегментом в области угроз на клиентов банков.

В партнерстве с компанией Flashpoint аналитики RiskIQ были первыми, кто проанализировал деятельность злоумышленников, использующих сниффферы. Они выделили 12 групп под общим названием MageCart. Эксперты Group-IB изучили обнаруженные сниффферы и, применив собственные аналитические системы, уже к концу 2019 года выявили как минимум 38 разных семейств. Каждое семейство обладает уникальными признаками и, скорее всего, управляется разными людьми. Так как все сниффферы имеют схожий функционал, создание двух снифферов одной группой злоумышленников нецелесообразно.

Архитектура сниффера

Клиентская часть сниффера

Осуществляемый разными способами:

- По жестко записанному списку имен полей платежных форм;
- По списку регулярных выражений, определяющему интересные снифферу поля;
- По списку базовых HTML-элементов, используемых в платежной форме.

Серверная часть сниффера — приложение, с которым работает оператор сниффера

Выполняемые серверной частью функции зависят от того, насколько точно клиентская часть сниффера определяет тип украденных данных.

Как работают сниффферы

Шаг 1: Получение доступа к сайту

Вариант 1
Получение доступа к административной панели с использованием вредоносных программ, крадущих пароли

Вариант 2
Поиск уязвимых сайтов (эксплоиты популярных CMS, известные уязвимости поставщиков услуг). Используя эксплоиты, злоумышленник загружает веб-шелл и получает доступ к изменению файлов сайта

Вариант 3
Покупка доступа к сайту у другой группы злоумышленников

Шаг 2: Получение сниффера

Вариант 1
Собственная разработка

Вариант 2
Покупка/аренда готового варианта на андеграундном форуме.

Шаг 3: Установка сниффера

Установленный через панель управления или веб-шелл сниффер собирает информацию и отправляет ее на хост, управляемый злоумышленником. Некоторые сниффферы используют техники, позволяющие оставаться незамеченными при ручной проверке.

Шаг 4: Монетизация

Вариант 1
Продажа данных кардерам и получение от $1 до $5 с каждой карты. Этот способ самый простой — для его реализации достаточно иметь контакты проверенных скупщиков

Вариант 2
Оплата чужими банковскими картами товаров, которые легко перепродать: гаджетов, электроники, бытовой техники, предметов интерьера, одежды и обуви

Собранные платежные данные и персональная информация жертвы отправляется на сервер злоумышленников — гейт *(для усложнения обнаружения конечного сервера злоумышленников в цепочке передачи данных со сниффера может быть использовано несколько уровней гейтов, расположенных на разных серверах или взломанных сайтах)*. Конечный сервер злоумышленников, предназначенный для отслеживания активности снифферов и экспорта украденных данных, может представлять собой как полноценную административную панель, так и сервер для размещения инструментов администрирования баз данных.

Способы заражения

Злоумышленники могут заражать сайты и внедрять вредоносный код разными способами.

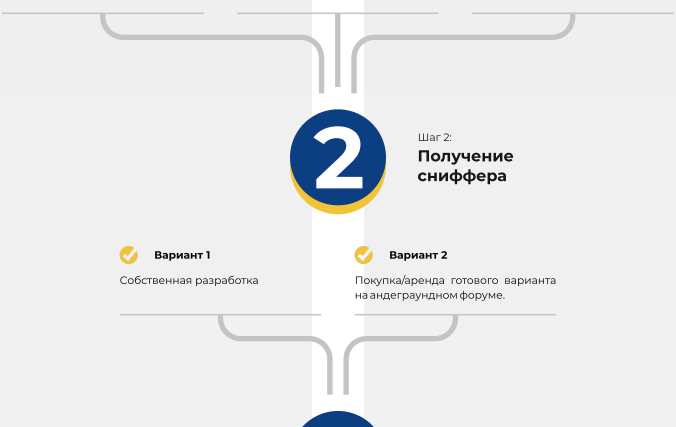
Эксплуатация уязвимостей CMS для внедрения вредоносного кода

Взлом административной панели сайта для установки сниффера

Атаки через поставщиков (взлом систем веб-аналитиков)

Масштабы заражений и жертвы

Обнаруженные семейства снифферов были использованы для заражения как минимум 2 440 онлайн-магазинов, принимающих к оплате банковские карты. Суммарное суточное количество посетителей всех зараженных сайтов — более полутора миллионов человек.



Количество человек – Сниффер

Исходя из анализа списка TLD (top-level domain) зараженных онлайн-магазинов, можно сделать вывод, что атакующие в целом заинтересованы в заражении сайтов, относящихся к крупным развитым странам:

ROOT LEVEL RESOURCES

Нужно понимать, что злоумышленник не сможет достичь своей цели, если атака будет вовремя выявлена и остановлена, а это возможно на любом ее этапе, если принимаются соответствующие меры защиты. Для эффективности обработки событий информационной безопасности необходим постоянный мониторинг событий безопасности. Чтобы эффективно противостоять активно развивающейся киберпреступности, важно не скрывать произошедшие инциденты, а участвовать в обмене информацией об атаках внутри отрасли, чтобы вовремя узнавать об индикаторах компрометации и сообщать о них другим.

1 – Сниффер - тип вредоносного кода, внедряемого злоумышленниками в сайт жертвы для перехвата вводимых пользователем данных: номеров банковских карт, имен, адресов, логинов, паролей и т.д. Полученные платежные данные злоумышленники перепродают или используют сами для покупки ценных товаров. Стоимость снифферов составляет от $250 до $5000

2 – Номер, дата истечения, имя держателя, адрес, CVV

3 – Содержимое магнитных полос банковских карт. Дампы занимают около 80% рынка кардинга

4 – Вредоносный код, внедренный на сайты онлайн-магазинов или других порталов, где пользователи вводят данные своих карт. Стали главным открытием 2019 года, и эксперты отмечают заметный тренд в их популяризации

5 – Вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтверждённая её держателем