



# HI-TECH CRIME TRENDS 2016

GROUP-IB.RU



<b>КЛЮЧЕВЫЕ ВЫВОДЫ</b>	<b>3</b>
<b>ПРОГНОЗЫ</b>	<b>10</b>
<b>ХИЩЕНИЯ</b>	<b>13</b>
<b>ЦЕЛЕВЫЕ АТАКИ НА БАНКИ</b>	<b>14</b>
Ключевые русскоязычные преступные группы, атакующие банки	16
Атаки на систему SWIFT	18
Логические атаки на банкоматы	19
<b>АТАКИ НА КОМПАНИИ И ФИЗИЧЕСКИХ ЛИЦ</b>	<b>21</b>
Трояны для ПК	21
Мобильные трояны	24
5 самых популярных схем хищений с использованием Android-троянов	28
Автоматизированные фишинговые и вишинговые атаки	30
<b>ШПИОНАЖ</b>	<b>33</b>
На уровне сотовых операторов	34
На уровне интернет-провайдеров	36
На уровне корпоративной сети	37
<b>АТАКИ НА ПРОМЫШЛЕННЫЕ СИСТЕМЫ И КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ</b>	<b>39</b>
<b>ВЫМОГАТЕЛЬСТВО</b>	<b>46</b>
DDoS-атаки	47
Атаки с использованием программ-шифровальщиков	50
<b>МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БРЕНДА</b>	<b>54</b>

## ОЦЕНКА РОССИЙСКОГО РЫНКА ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ ПОСРЕДСТВОМ ВЫСОКОТЕХНОЛОГИЧНЫХ АТАК

Q2 2015 – Q1 2016, данные Group-IB

Тип преступления	Количество групп	Общее число успешных атак в день	Средняя сумма одного хищения	Средний объем хищений в день	Q2 2015- Q1 2016 (в рублях)	Q2 2015- Q1 2016 (средний курс 70 рублей за \$1)	% роста к прошлому периоду
Целевые атаки на банки	5	-	140 000 000 ₽		2 500 000 000 ₽	\$43 859 649	292%
Хищения в интернет-банкинге у юридических лиц	6	8	480 000 ₽	3 840 000 ₽	956 160 000 ₽	\$16 774 737	-50%
Хищения у физических лиц с использованием троянов для ПК	1	0,5	51 600 ₽	25 800 ₽	6 424 200 ₽	\$112 705	-83%
Хищения у физических лиц с Android-троянами	11	350	4 000 ₽	1 400 000 ₽	348 600 000 ₽	\$6 115 789	471%
Обналичивание похищаемых средств	-	-	-	2 369 610 ₽	1 715 032 890 ₽	\$30 088 296	44%
<b>ИТОГО</b>				<b>5 265 800 ₽</b>	<b>5 526 217 090 ₽</b>	<b>\$96 951 177</b>	<b>44%</b>

Как мы и прогнозировали в прошлом году, выросло и количество, и средний ущерб от целенаправленных атак на банки. Доход хакеров от них перекрыл суммарный заработок от всех остальных способов хищений, сделал банки самой привлекательной мишенью для атак.

В России уже несколько лет подряд наблюдается снижение объема хищений у физических и юридических лиц с использованием банковских троянов для персональных компьютеров. Их место занимают атаки с использованием Android-троянов, которые стремительно упрощаются и автоматизируются.



## КЛЮЧЕВЫЕ ВЫВОДЫ

### ЦЕЛЕВЫЕ АТАКИ НА БАНКИ

*Сами банки, а не их клиенты стали наиболее привлекательной мишенью для киберпреступников*

**Целевые атаки на банки, которые только начинают распространяться по миру, происходят в России с 2013 года.** Русскоговорящие преступные группы имеют опыт атак практически на все банковские системы, включая платежные шлюзы и банкоматы (Anupak), карточный процессинг и биржевые терминалы (Corkow).

**За отчетный период ущерб российских банков от целевых атак вырос почти на 300%** (более 2/3 хищений приходятся на группу Vuhtrap). Все преступные группы, стоящие за ними, ранее специализировались на хищениях денежных средств у юридических лиц (клиентов банков).

**Наиболее профессиональные преступные группы, атаковавшие компании, переориентируются на банки,** а преступные группы, получившие опыт целевых атак в России, выходят в другие страны.

**Атаки на банки Западной и Восточной Европы, СНГ, Азиатско-Тихоокеанского региона, Ближнего Востока выполнялись по схожему шаблону.** Для проникновения, повышения привилегий, захвата управления контроллером домена, получения удаленного доступа к интересующим системам и даже для удаления следов атаки использовались одинаковые или очень схожие инструменты, часть из которых является легальным и бесплатным программным обеспечением.

**Использование этого шаблона позволяет добраться до критических систем и атаковать их без разработки дорогостоящего программного обеспечения.** Некоторые преступные группы уже отказываются от частных троянов, а развитие индустрии нелегальных сервисов и инструментов для атак только поддерживает эту тенденцию.

**2,5 млрд ₺**

*Объем хищений в результате целевых атак на банки*

**+292%**

---

*По аналогичному шаблону группа Black Energy атаковала киевский аэропорт Борисполь и украинские энергосети.*

**956+ млн ₺**

*Объем хищений в интернет-банкинге у юридических лиц*

**-50%**

## ХИЩЕНИЯ У ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ

*Продолжается автоматизация заражений и хищений*

**В России объем хищений денежных средств у компаний с помощью троянов для ПК ежегодно снижается:** наиболее профессиональные преступные группы, на которые приходилась большая часть атак, переориентировалась на атаки напрямую на банки, другие, набравшись опыта, стали искать жертв за пределами РФ.

**Именно русскоязычные специалисты подогревают рынок троянов для ПК, использующихся для атак по всему миру.** Они причастны к таким новым банковским троянам, как Panda Banker, Shifu, Midas bot, GozNym, Sphinx, Corebot.

**Хакеры делают ставку на автоматизацию хищений:**

- Все новые трояны для хищений у юридических лиц, появившиеся в России за отчетный период, поддерживают веб-инъекты, позволяющие проводить автозалив. Этот метод начинают поддерживать и Android-трояны.
- С помощью легальных сервисов переводов с карты на карту хакерам удалось полностью автоматизировать фишинговые и вишинговые атаки на физических лиц, для завершения которых требуется SMS-код подтверждения транзакции с телефона жертвы. Такая атака укладывается в несколько минут и не требует от хакера никакого участия.

**Развитие функциональности троянов для Android и их доступность стимулируют взрывной рост числа успешных атак.** В России ежедневно жертвами становятся 350 пользователей устройств на этой платформе, а объем хищений вырос более чем на 450%. Хищения у физических лиц с помощью троянов для ПК при этом практически прекратились – ими занимается только одна преступная группа.

**Темпы роста объема хищений будут трехзначными по всему миру, поскольку заражения вредоносным ПО становятся незаметнее, а хищения автоматизируются:**

- Android-трояны начали распространяться с помощью эксплойтов, которые позволяют установить вредоносную программу при посещении взломанного сайта незаметно для пользователя.

---

*16 из 19 троянов для ПК, наиболее активно используемых для хищений по всему миру, связаны с русскоязычными преступниками.*

---

*Автозалив – метод хищений, позволяющий автоматически и незаметно для пользователя интернет-банка подменять реквизиты и сумму платежа.*

*Пассивный автозалив производится в момент формирования мошеннического платежа пользователем, а активный может осуществляться без участия жертвы.*

---

*Вишинг – разновидность фишинговых атак, при которой сбор данных (логинов, паролей, данных банковских карт) производится по телефону.*

- Появились веб-инъекты под мобильные браузеры. Этот функционал есть, например, в новой версии одного из наиболее активно используемых для хищений по всему миру Android-тroyанов Marcher. Веб-инъекты позволяют атаковать пользователей любых систем интернет-банкинга и реализовывать все схемы, которые раньше были доступны только на компьютерах, включая автозалов.
- Преступники начали защищать сетевое взаимодействие между C&C-сервером и устройством, что усложняет обнаружение тroyана, и проводить заражения в несколько этапов, устанавливая основной модуль только на устройства с подходящими параметрами: например, с доступом к интересующей системе мобильного банкинга.

**Растет число опасных мобильных приложений.** Вредоносные программы не только мимикрируют под приложения, стабильно держащиеся в региональных топах, но и отвечают на ситуативные всплески интереса пользователей: например, они распространялись под видом приложения Pokemon Go. **Для продвижения мобильных приложений активно используются инструменты интернет-маркетинга:** контекстная реклама по ключевым словам, накрутка установок и отзывов в GooglePlay, SEO-оптимизация сайтов с загрузчиками.

## ШПИОНАЖ

*Инструменты для прослушивания разговоров и перехвата трафика становятся доступнее*

**Отслеживание местоположения и прослушивание разговоров пользователей мобильных телефонов** с помощью атак на SS7-канал предлагают все больше легальных компаний. Растет и черный рынок услуг: соответствующие предложения все чаще можно увидеть на хакерских форумах.

**Техника перехвата трафика с помощью BGP Hijacking**, который является идеальным инструментом шпионажа, привлекает еще больше внимания со стороны атакующих.

**Android-тroyаны совмещают инструменты для шпионажа и хищений.** Так, практически все мобильные тroyаны для хищений, активные в России, имеют функционал для перехвата SMS. Это открывает доступ к системам с двухфакторной аутентификацией, например, облачным хранилищам, почте, корпоративным порталам, а через них ко всей персональной и конфиденциальной информации.

**6,2 млн ₹**

*Объем хищений денежных средств у физических лиц с использованием тroyанов для ПК*

**-83%**

**348+ млн ₹**

*Объем хищений денежных средств у физических лиц с использованием Android-тroyанов*

**+471%**

---

*Активное использование кибершпионажа для последующих информационных вбросов резко повысило уровень угроз для чиновников, бизнесменов, и журналистов.*

## АТАКИ НА ПРОМЫШЛЕННЫЕ КОМПАНИИ И ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

*Сложилась предпосылка для увеличения количества атак*

**Внимание к хакерским атакам со стороны медиа привлекает на рынок новых заказчиков.** Технологические аварии, утечки пользовательских данных, остановка бизнес-процессов становятся привлекательным инструментом для борьбы за рынки и покупателей.

**Появление эффективного шаблона целевой атаки,** позволяющего получить доступ к критической инфраструктуре без разработки дорогостоящих вирусов, упрощает атаку для исполнителя и снижает ее стоимость для заказчика.

**Владельцы бот-сетей для хищений начали продавать доступы к компьютерам, не представляющим для них интереса.** Так, мы наблюдали переговоры о продаже доступов к рабочим станциям, взаимодействующим со SWIFT, и пакетные предложения для последующих атак с помощью программ-шифровальщиков. Таким же образом атакующие могут получить доступ к компьютерам, входящим в сети промышленных и энергетических компаний. То есть, если раньше злоумышленники, получавшие доступ к критичной инфраструктуре без возможности его монетизации, ничего с ним не делали, то теперь они ищут покупателя, интересующегося этим доступом.

**Появляются новые схемы атак.** Например, атака может быть замаскирована под шифровальщик, а преступники могут попросить предоставить удаленный доступ к зараженной системе, чтобы провести расшифровку файлов вручную.

**Усиливается рекрутинговый потенциал террористических групп.** Европейский миграционный кризис, ухудшение социально-экономической ситуации, обострение этнических и религиозных конфликтов целом ряде регионов мира питают почву для восприятия пропаганды террористических и экстремистских группировок, которые открыто рекрутируют хакеров в теневом сегменте интернета.

---

*Иногда программы-вымогатели ставят средства удаленного управления автоматически.*



## ВЫМОГАТЕЛЬСТВО

*Растет количество и эффективность атак*

**Наметился тренд на возврат популярности бот-сетей для DDoS-атак**, но теперь для их создания используют не компьютеры с Windows, как было раньше, а Linux-серверы и простые IoT (Internet of Things)-устройства.

**Круглосуточно доступные и незащищенные антивирусами, IoT-устройства стали главным драйвером роста бот-сетей для DDoS-атак.**

**Растет число DDoS-вымогателей, не имеющих собственных бот-сетей.** Некоторые из них просто рассылают письма с угрозами, некоторые – заказывают на сервисах краткосрочные атаки, чтобы запугать жертву.

**Атаки с использованием программ-шифровальщиков становятся эффективнее.** Повышать вероятность выплаты хакерам помогает выкуп у владельцев бот-сетей доступа к компьютерам, имеющим выход на критичные для бизнеса системы. Кроме того, хакеры начали проверять серверы с подобранными паролями на предмет наличия информации, шифрование которой повысит вероятность выплаты выкупа.

**Развиваются сервисы, упрощающие атаки.** Появились новые партнерские программы для распространения программ-шифровальщиков, предоставляющие любому желающему возможность сгенерировать исполняемый файл вымогателя и среду для ведения переписки с жертвой за процент от выкупа.

**Растет количество атак на пользователей мобильных устройств.** Под угрозой не только пользователи гаджетов на Android. Не имея возможности заразить шифровальщиком iOS-устройства, преступники блокируют устройства посредством перехвата доступа к iCloud.





## МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БРЕНДА

*Спектр угроз для брендов расширяется*

**Преступники активнее используют инструменты интернет-маркетинга для продвижения сайтов и приложений** с использованием популярных брендов, что не только наносит ущерб репутации, но и приводит к снижению потока клиентов. Контекстная реклама в поисковых системах лишает официальные ресурсы части целевого трафика, а использование преступниками методов SEO-оптимизации приводит к понижению позиций в поисковой выдаче официальных сайтов.

**Использование поддельных SSL-сертификатов повышает эффективность фишинга.** Все вредоносные программы, которые занимаются перенаправлением пользователей на поддельные сайты, используют SSL-сертификаты, выпущенные на имена легальных компаний.

**Доверие к брендам позволяет успешно атаковать не только физических, но и юридических лиц.** Например, мы фиксировали создание и продвижение копий сайтов российских промышленных, машиностроительных предприятий, компаний нефтегазового сектора, производителей удобрений для последующего заключения мошеннических контрактов от их имени. Средний подтвержденный ущерб от такой атаки составил 1,5 млн Р.

## ПРОГНОЗЫ

### Целевые атаки на банки продолжают победное шествие по миру.

- Профессиональные преступные группы, занимавшиеся атаками на юридических лиц, будут переориентироваться на банки.
- Можно ожидать прироста инцидентов с участием русскоязычных хакеров, которые, получив успешный опыт в атаках на банки России и Украины, будут уходить в другие регионы мира.
- Команды, занимавшиеся логическими атаками на банкоматы, будут пробовать себя в атаках на SWIFT.
- Будут появляться новые инструменты и сервисы для целевых атак.
- Хакеры начнут уделять больше внимания поиску инсайдеров для предоставления нужной информации и первичного заражения.
- Средний размер ущерба одной успешной атаки увеличится.

### Хищения с помощью троянов для ПК в мире останутся на высоком уровне, но постепенно уступят свои позиции.

- Атакующие начнут использовать Android-трояны.
- С популяризацией целенаправленных атак их методы начнут использоваться для атак на расчетные центры крупного бизнеса.
- Владельцы бот-сетей будут монетизировать их за счет продажи доступа в сети интересующих компаний. В последствии они будут продавать бот-сети менее опытным хакерам, чтобы скрыть свою связь с хищениями.

### Количество и объем успешных хищений с помощью Android-троянов продолжат динамично расти.

- Эксплойты для их распространения станут включаться в стандартные наборы эксплойтов, доступные на хакерском рынке.
- Распространение веб-инъектов под мобильные браузеры приведет к увеличению количества жертв и автоматизации хищений.
- Начнет более активно развиваться рынок продуктов и услуг для повышения эффективности проведения атак с помощью Android-троянов, например, сервисы по написанию веб-фейков и веб-инъектов.
- По мере освоения системами корпоративного дистанционного банковского обслуживания мобильных платформ Android-трояны начнут атаковать юридических лиц с целью хищений денежных средств.

---

*Наибольший потенциал для начала атак на банки в России – у групп Top1el и RTM.*

---

*Эксплойты позволяют установить вредоносную программу при посещении взломанного сайта незаметно для пользователя.*

**Фишинговые и вишинговые атаки на физических лиц будут автоматизироваться.**

**Появление новых фишинг-китов с автоматизированной системой выставления и подтверждения платежей** позволит значительно повысить эффективность атак в разных странах.

**Увеличится количество DDoS-атак с целью вымогательства**, однако, поскольку большая часть атакующих не имеет своих бот-сетей, их эффективность будет невысокой.

**Преступники будут наращивать бот-сети за счет IoT-устройств, в том числе для последующего использования в DDoS-атаках.** IoT-устройства будут использоваться в мошеннических схемах, например, для перенаправления на фишинговые сайты, демонстрации рекламы с предложением скачать вредоносные программы, замаскированные под легальные, и т.п.

**Инцидентов с программами-шифровальщиками станет больше.**

- Атаки на компании будут более качественно таргетированы, что приведет к повышению средней суммы выкупа.
- Программы-вымогатели усилят направленность на специфичные корпоративные сектора (например, колл-центры, аутсорсинговые бухгалтерские компании накануне сдачи отчетности и т.п.), где у атакующих будет больше шансов зашифровать критичную информацию и требовать выкупа.
- Увеличится количество инцидентов с шифрованием мобильных устройств.
- Продолжится развитие сервисов для автоматизации атак.
- Появятся трояны, которые реализуют возможность шифровать или блокировать доступ к данным на облачных сервисах.
- С появлением на рынке популярных производителей IoT-устройств начнется охота за информацией об их уязвимостях.

**Динамичный рост количества атак на компании и активный выход шифровальщиков на мобильные устройства стимулируют развитие сегмента страхования киберрисков.** Страхование приведет к увеличению случаев, когда жертва платит атакующему, что еще больше стимулирует атакующих, — а это, в свою очередь, еще активнее стимулирует рынок страхования.

---

*Фишинг-кит – набор инструментов для проведения фишинговой атаки.*

- Количество атак на промышленные объекты будет расти, высока вероятность атаки на объект критической инфраструктуры со значительным ущербом (вплоть до человеческих жертв).
- Растущее предложение решений для атак на SSL и перехвата трафика, а также расширение функционала для шпионажа у мобильных троянов неизбежно приведут к росту числа атак с целью шпионажа.

Киберармии разных стран продолжают атаковать объекты критической инфраструктуры как для шпионажа, так и для того, чтобы иметь контроль над ними и возможность воспользоваться им в нужный момент.

- Для сокрытия причастности государственных киберармий будут активно вербоваться хакеры с опытом проведения целенаправленных атак на корпоративный сегмент. Привлеченные хакеры будут использовать свои инструменты, в том числе легальные, для получения доступа к объектам с нужной информацией.
- Популяризация успешных атак в СМИ привлечёт внимание террористов к уязвимым объектам, атаки на которые смогут вызвать общественный резонанс, в том числе привести к человеческим жертвам. Террористы будут активнее рекрутировать хакеров, способных проводить целевые атаки.

**Преступники продолжают использовать политические разногласия, чтобы совершать хищения и атаки в других странах, не боясь экстрадиции** (примеры: Россия-Украина, Израиль-Ливан, Пакистан-Индия). Хакерские атаки на фоне взаимного недоверия спецслужб также могут быть использованы для оказания влияния на развитие конфликта извне или изнутри оппонирующих стран.

---

*Прежде всего атакующих будут интересовать энергетические компании, объекты транспортной инфраструктуры, аэропорты, химические производства, водоочистительные узлы. Тактика атак на все эти типы предприятий будет очень схожей.*



# ХИЩЕНИЯ

Под угрозой банки, платежные системы, платформы для биржевого трейдинга, а также все их клиенты. Чем удобнее дистанционный банкинг для клиентов, тем удобнее хищения для преступников.

Шаблон целевой атаки на банк может быть использован для проникновения в сети промышленных и энергетических предприятий, получения доступа к системам управления объектами критической инфраструктуры.



Прошло три года с момента начала действия группы Anupak и первых множественных целенаправленных атак на банки в России. Теперь эта тенденция набирает обороты по всему миру, как мы и прогнозировали в отчете за 2014 год.

Атака на банк приносит прибыль, эквивалентную доходу от нескольких десятков атак на юридических лиц. Возможность быстро обогатиться привлекает все больше киберпреступников.

## КЛЮЧЕВЫЕ ТЕНДЕНЦИИ

### ПЕРЕОРИЕНТАЦИЯ ГРУПП, АТАКОВАВШИХ ЮРИДИЧЕСКИХ ЛИЦ, НА БАНКИ

Все команды, которые атакуют банки, раньше занимались хищениями у компаний. Поэтому все действующие группы, специализирующиеся на юридических лицах, являются потенциальной угрозой и для самих банков.

### ИСПОЛЬЗОВАНИЕ ГОТОВЫХ ИНСТРУМЕНТОВ ДЛЯ ПРОВЕДЕНИЯ АТАК

Некоторые группы отказываются от специализированных троянов и используют общедоступные средства, которые все равно позволяют им успешно похищать деньги из банков. Появляются платные сервисы и инструменты для проведения атак.

### ШАБЛОНИЗАЦИЯ АТАК

Основная опасность групп не в используемых ими вредоносных программах, а в эффективном шаблоне их атак. Действия разных групп, атаковавших банки за последний год, очень похожи и разделены на несколько этапов, из которых реальную сложность представляет только финальный – обналичивание. Не все обналичивающие группы могут принять и успешно обналичить несколько сотен миллионов рублей.

**Важно понимать, что после получения привилегий администратора домена преступники могут атаковать любые системы** – сеть банкоматов, биржевые терминалы, системы электронных расчетов и межбанковских переводов. По такой же схеме могут быть атакованы промышленные системы управления.

---

*Для подготовки вредоносных документов часто используется инструмент под названием Microsoft Word Intruder (MWI), разработанный русскоязычными специалистами. Он постоянно обновляется и активно продается на популярных хакерских форумах. Стоимость в \$4000 за лицензию делает его доступным для широкого круга преступников.*

*Количество целевых атак на банки продолжит расти. Можно ожидать прироста инцидентов с участием русскоязычных хакеров, которые, получив успешный опыт в атаках на банки России и Украины, будут уходить в другие регионы мира. К этому их подталкивают в том числе задержания в России членов преступных групп, причастных к целевым атакам.*

*Хакеры начнут больше внимания уделять поиску инсайдеров для предоставления нужной информации и организации первичного заражения. Также возрастет качество и количество техник социальной инженерии.*

## ТАКТИКА ЦЕЛЕВОЙ АТАКИ С ПРОНИКНОВЕНИЕМ

*Мы описываем шаблон подобных атак с целью показать, что реализация каждого этапа, за исключением последнего, не требует особого опыта или труднодоступного программного обеспечения.*

### 1. ПРОНИКНОВЕНИЕ

Основным способом проникновения в банковскую сеть является отправка фишингового письма с вложением в виде документа с эксплойтом/макросом, исполняемого файла или запароленного архива с исполняемым файлом. Подготовить вложение с эксплойтом можно с помощью готовых инструментов (virus creation kits), а для отправки исполняемого файла не требуется никаких специальных средств.

### 2. УДАЛЕННЫЙ ДОСТУП

После успешного заражения все группы используют различные средства удаленного управления. Как правило, это или легитимные и бесплатные инструменты (TeamViewer, Ammy Admin, VNC, Light Manager), или средства удаленного управления, встроенные в популярный фреймворк Metasploit.

### 3. ПОЛУЧЕНИЕ ПРИВИЛЕГИЙ

Получив удаленный доступ в сеть банка, атакующие часто применяют бесплатный инструмент Mimikatz, который позволяет извлекать логины и пароли в открытом виде из оперативной памяти зараженного компьютера. Исходный код этой утилиты опубликован на Github и доступен всем желающим без ограничений.

### 4. ПОИСК ЦЕЛЕЙ

Имея привилегии администратора домена, они начинают исследовать внутреннюю сеть банка в поисках интересующих систем. Целями могут быть системы межбанковских переводов, системы мгновенных переводов для физических лиц, сети управления банкоматами, платежные шлюзы, карточный процессинг. Поиск осуществляется в ручном режиме и не требует специальных инструментов.

### 5. РАБОТА С ЦЕЛЕВЫМИ СИСТЕМАМИ

Обнаружив интересующие системы, злоумышленники с помощью тех же средств удаленного управления отслеживают действия легальных операторов, чтобы в последствии повторить их шаги и отправить деньги на подконтрольные счета. Более продвинутые группы используют готовые инструменты для модификации платежных документов – простые скрипты или исполняемые файлы, повторяющие работу скриптов, которые автоматизируют формирование мошеннических платежей.

### 6. ОБНАЛИЧИВАНИЕ

Если первые 5 этапов доступны многим хакерам и каждый из них можно реализовать с минимальными затратами, то для обналичивания больших объемов денежных средств нужны люди с опытом и ресурсами. Поэтому когда профессиональные группы, занимающиеся обналичиванием денег, распадаются или уходят на дно, хищения временно прекращаются.

## КЛЮЧЕВЫЕ РУССКОЯЗЫЧНЫЕ ПРЕСТУПНЫЕ ГРУППЫ, АТАКУЮЩИЕ БАНКИ

### ANUNAK

#### ЦЕЛИ

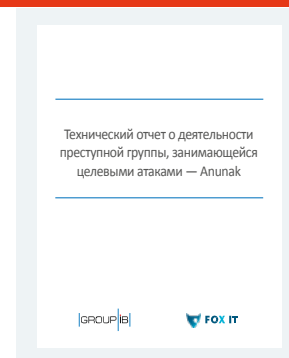
Системы межбанковских переводов, системы мгновенных переводов для физических лиц, сети управления банкоматами, платежные шлюзы, карточный процессинг, POS-терминалы, трейдинговые платформы, государственные структуры.

#### ПОЧЕМУ ВАЖНА

Группа, ответственная за первые успешные целевые атаки на банки в России. Самая опытная группа, в 2013–2014 году атаковавшая более 50 российских банков и 5 платежных систем, похитив в общей сложности более 1 млрд рублей (около \$25 млн). Также атаковала POS-терминалы американских и европейских ритейл-сетей. Активно вовлекала людей в атаки и делилась опытом. Имеет целый ряд последователей, копирующих их тактику.

#### СТАТУС

Не совершила ни одного успешного хищения на территории России начиная с начала 2015 года, троян еще используется для атак на компании за пределами СНГ. В России зафиксированы атаки с целью шпионажа, использующие ее вредоносную программу.



### CORKOW

#### ЦЕЛИ

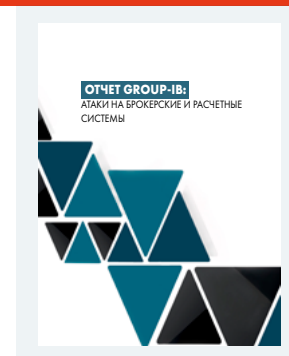
Карточный процессинг, банкоматы, биржевые терминалы.

#### ПОЧЕМУ ВАЖНА

В феврале 2015 совершила первую в мировой практике атаку на брокера, вызвавшую аномальную волатильность на валютном рынке. Заразив внутреннюю сеть банка, преступники получили доступ к биржевому терминалу и провели серию операций, повлекшую скачок курса доллара по отношению к рублю почти на 20%. Ущерб банка составил 224 млн рублей (\$4 млн).

#### СТАТУС

Приостановила активность.





## BUHTRAP

**ЦЕЛИ.** Системы межбанковских переводов.

**ПОЧЕМУ ВАЖНА.** Образец успешной переориентации группы, занимавшей лидирующие позиции по объему хищений у юридических лиц. С августа 2015 по февраль 2016 совершила 13 успешных атак на российские банки, 1,8 миллиарда рублей (\$25 млн). В двух случаях сумма хищений в 2,5 раза превзошла уставной капитал банка.

**СТАТУС.** Приостановила атаки на банки, продолжаются хищения у юридических лиц с помощью бот-сети, проданной другим атакующим.

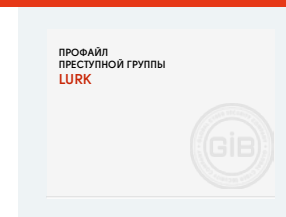


## LURK

**Цели.** Системы межбанковских переводов.

**Почему важна.** Разработала один из самых продвинутых троянов для хищений у юридических лиц, позволявший незаметно для пользователя подменять реквизиты и сумму платежа в системах интернет-банкинга, а также обходить SMS-подтверждение платежей. В феврале 2015 года похитила 150 млн рублей (\$2,3 млн) из российского банка, после этого совершила еще две неудачных попытки атак в России и Украине.

**Статус.** Участники преступной группы задержаны в мае 2016. Часть атакующих остается на свободе и в ближайшее время может вернуться к целенаправленным атакам на системы межбанковских переводов.



Узнайте больше о каждой преступной группе из отчетов Group-IB [group-ib.ru/reports](http://group-ib.ru/reports)

## АТАКИ НА СИСТЕМУ SWIFT

В феврале 2016 хакеры попытались похитить из Центрального банка Бангладеш \$951 млн через систему международных межбанковских переводов SWIFT, но из-за ошибки в платежном документе им удалось украсть только \$81 млн. Изначально вредоносную программу, использованную для атаки, связали с северокорейской группой Lazarus, позже появилась информация, что за атаками могут стоять российские хакеры. Последняя версия пока не подтвердилась.

Этот инцидент и последующая публикация данных об использованной вредоносной программе запустила волну проверок, в ходе которых стало известно об аналогичных инцидентах в других банках. Так, в 2015 году злоумышленники предприняли неудачную попытку вывода из вьетнамского Tien Phong Bank \$1,13 млн и успешно атаковали эквадорский Banco del Austro, похитив \$12 миллионов.

Сразу вслед за эквадорским банком от атаки на SWIFT пострадал украинский банк, лишившийся \$10 млн. Схема атак была идентичной. Проникнув в сеть банка, преступники тщательно изучали внутренние процессы: с помощью специальной программы они отслеживали движение денежных средств и собирали в папки файлы, содержащие в себе токены (идентификаторы) интересующих транзакций, а затем использовали их для формирования мошеннических платежных поручений.

**Подготовка к атаке на SWIFT длится от нескольких дней до нескольких недель, за которые банк может обнаружить активность преступников в сети.**

В мае 2016 на русскоязычном закрытом хакерском форуме нами были обнаружены сообщения о поиске специалистов по SWIFT и международным переводам. Один из участников форума подтвердил, что в его бот-сети есть компьютеры с доступом к SWIFT, входящие в сети европейских банков. В ходе дальнейшего исследования удалось установить, что речь идет о немецких банках.

*Наблюдаемая активность на хакерских форумах показывает повышенную заинтересованность в организации хищений через SWIFT. Жертвой может стать любой банк, подключенный к этой системе.*

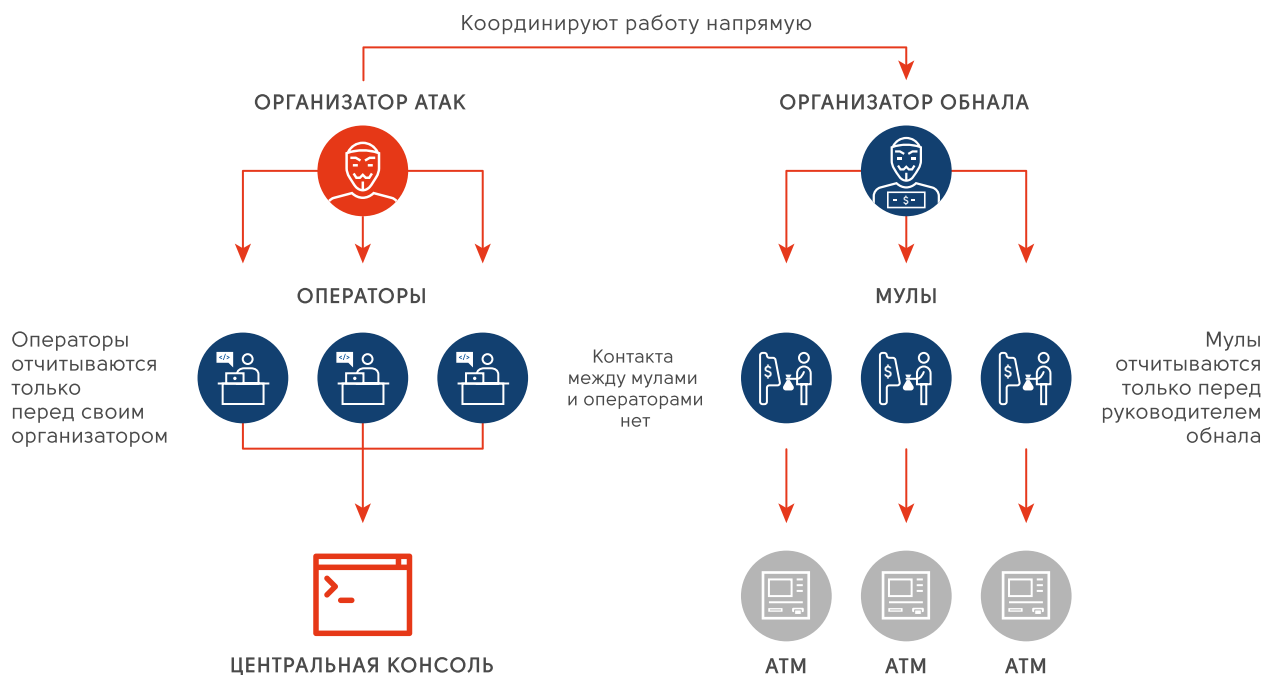
## ЛОГИЧЕСКИЕ АТАКИ НА БАНКОМАТЫ

В арсенале киберпреступников есть множество методов физических атак на банкоматы: скимминг, шимминг, захват карт (card trapping), кража и даже взрывы банкоматов стали привычным делом. Однако при физическом воздействии преступники получают возможность добраться до денег только из отдельного банкомата, оставляя при этом много следов. Самые сообразительные хакеры стараются увеличить объем хищений и снизить риски, переходя от физических атак к логическим.

**В ходе логической атаки злоумышленники получают доступ к локальной сети банка и уже из нее устанавливают полный контроль над банкоматами.** По удаленной команде машины начинают выдавать наличность, а заранее подготовленные люди просто собирают деньги в сумки.

По такой схеме в июле 2016 хакеры получили доступ к 41 банкомату First Bank в Тайване и успешно похитили \$2 миллиона долларов. По подозрению в совершении преступления были задержаны граждане Латвии, Молдовы и Румынии. Еще как минимум 13 подозреваемых, среди которых есть гражданин России, успели покинуть остров. Мулы зачастую въезжают в страну по туристическим визам специально для осуществления атаки и покидают ее как только операция окончена.

### ТИПОВАЯ ОРГАНИЗАЦИОННАЯ СХЕМА АТАКИ



## ТАКТИКА ЛОГИЧЕСКОЙ АТАКИ НА БАНКОМАТЫ

*На примере атаки на First Bank на Тайване*

- Хакеры получили доступ к сети филиала банка в Великобритании.
- В этом филиале они нашли систему, подключенную к сети центрального офиса.
- Используя канал связи между центральным офисом и офисом в Великобритании, они получили доступ к сети центрального офиса.
- В сети центрального офиса они нашли систему управления банкоматами.
- Используя систему управления банкоматами в центральном офисе банка, они загрузили на банкоматы вредоносные файлы: несколько исполняемых файлов и скрипт Visual Basic. Задача вредоносных файлов – начать выдачу денег по удаленной команде от злоумышленника.
- Запуск вредоносных файлов осуществлялся через стандартный планировщик задач Windows.
- К банкоматам отправили людей (мулов) для приема денег. В их задачу входило стоять возле банкомата и держать связь с организатором по телефону. Организатору они сообщали когда можно давать команду на выдачу наличных и все ли идет нормально.
- Организатор, получивший доступ к банкомату, удаленно давал команду на выдачу денег из банкомата.
- Когда мулы подтверждали, что банкомат пустой, организатор давал команду на удаление вредоносных программ с банкомата.

*Логические атаки набирают все большую популярность, и мы видим, что география атакуемых стран расширяется. Эта угроза стала глобальной и количество инцидентов будет только расти.*

*Каждая успешная атака предоставляет преступникам возможность расширить список будущих жертв за счет установления рабочих контактов сотрудников других банков и имен лиц, поддерживающих с ними связь. Это позволит повысить эффективность целевых рассылок фишинговых писем.*

*Инструментарий для атак на банкоматы может быть использован для хищений через систему SWIFT. Как только хакеры найдут способ отмывания полученных средств, они могут освоить и этот вектор атак, что приведет к еще большим ущербам.*

## ТРОЯНЫ ДЛЯ ПК

**В течение последних лет количество атак с помощью банковских троянов для ПК в России стабильно снижается.** За прошедший период с помощью банковских троянов у юридических лиц удалось похитить 956 160 000 ₽, что на 50% меньше, чем в прошлом периоде.

**В это же время за рубежом наблюдается бум троянов для ПК.** 16 из 19 троянов, наиболее активно использующихся для хищений у компаний, разработаны русскоязычными специалистами.

### РОССИЯ

Группы, которые раньше занимались атаками на компании, переориентировались на банки.

**Из старых преступных групп, специализирующихся на юридических лицах, осталась активной только Top1el.** После года паузы хищения возобновила группа, использовавшая троян Ranbyus (Triton).

Впрочем, некоторые группы после успешных атак на банки возвращаются к менее рискованным хищениям у юрлиц. Так, после ареста одного из членов Corkow, участники группы возобновили хищения у компаний, но уже с помощью другого трояна и в немного измененном составе. То же самое сделали и некоторые члены группы Buhtrap.

**Все новые трояны (RTM, Jupiter) для хищений у юридических лиц позволяют проводить атаки с помощью веб-инъектов.** С их помощью преступники получают возможность проводить атаки man-in-the-browser и использовать технологии автозалива. Модуль автозалива получил даже старый троян Ranbyus.

**Практически полностью прекратились хищения у физических лиц с помощью троянов для ПК.** Таким видом атак занимается только одна группа – Proxu, вернувшаяся на российский рынок после годовой паузы. Мы установили, что в этот период компания предпринимала попытки атак на банки Израиля и Австрии, однако, вероятно, используемый ими троян и тактика хищения не принесли ожидаемых результатов.

**Аресты участников русскоязычных преступных групп оказывают значительно влияние на мировой ландшафт банковских угроз.** Задержание участников группы Dure в ноябре 2015 устранило угрозу №1 для клиентов банков по всему миру. В мае 2016 в ходе масштабной операции российских правоохранительных органов были задержано около 50 участников группы Lurk, что тоже очень сильно повлияло на иностранный сегмент, поскольку группа имела отношение к популярной связке эксплойтов Angler, и сразу после задержания сильно просели некоторые ботнеты. После задержания участника группы Corkow с нашего радара пропала связка эксплойтов Niteris.

## ПРЕСТУПНЫЕ ГРУППЫ, ЗАНИМАЮЩИЕСЯ ХИЩЕНИЯМИ В РОССИИ

<b>ЦЕЛЕВЫЕ АТАКИ НА БАНКИ</b>	Buhtrap <b>new</b> Lurk <b>new</b> Cobalt <b>new</b> Corkow Andromeda	Lurk Corkow Andromeda
<b>ХИЩЕНИЯ У ЮРИДИЧЕСКИХ ЛИЦ С ПОМОЩЬЮ ТРОЯНОВ ДЛЯ ПК</b>	Buhtrap (новые владельцы бот-сети) Toplel Ranbyus RTM <b>new</b> Jupiter <b>new</b>	Lurk Corkow Yebot Kronos Chtonic
<b>ХИЩЕНИЯ У ФИЗИЧЕСКИХ ЛИЦ С ПОМОЩЬЮ ТРОЯНОВ ДЛЯ ПК</b>	Proхy	
<b>ХИЩЕНИЯ С ПОМОЩЬЮ ANDROID-ТРОЯНОВ</b>	Group 404 (приватный троян) ApiMaps Adabot Cron1 <b>new</b> (приватный троян) Cron2 <b>new</b> FlexNet <b>new</b> Agent.sx <b>new</b> (2 группы) Agent.BID <b>new</b> (4 группы) Honli <b>new</b> Asucub <b>new</b> FakeInst.ft <b>new</b> GM bot <b>new</b> Fake Marcher <b>new</b>	Greff (приватный троян) March Webmobil Mikorta MobiApps Xruss Tark Sizeprofit

### МИР

За прошедший период появились такие банковские трояны, как Panda Banker, Shifu, Midas bot, Gozi, GozNym, Sphinx, Corebot, Atmos. Все они были разработаны русскоязычными хакерами.

По-прежнему были активны Dridex, Qadars, Gootkit, Vawtrak, Tinba, KINS, Citadel, Zeus, к которым также причастны русскоговорящие специалисты, а также Quakbot, Retefe и Ramnit. Троян Ramnit ранее не был банковским, однако теперь он обзавелся веб-инжектными и с его помощью уже были атакованы клиенты нескольких банков.

Карта атакуемых троянами регионов показывает, какие страны больше всего интересуют владельцев бот-сетей, построенных с их помощью.



## МОБИЛЬНЫЕ ТРОЯНЫ

Россия традиционно была испытательным полигоном для мобильных троянов, а доказавшие эффективность технологии быстро распространялись по всем регионам мира. Описанные ниже тренды актуальны для глобального рынка вредоносных программ для Android.

В прошлом году мы уже писали о том, что рынок Android-троянов будет самым быстро растущим, поскольку они упрощают хищения у физических лиц. Так, в России после небольшого падения объема хищений с помощью Android-троянов в прошлом отчетном периоде, обусловленного введением банками жестких лимитов на размер переводов, этот метод вновь показал рекордную доходность. За последний год **с использованием Android-троянов было украдено 348 600 000 ₽, на 471% больше, чем в прошлом.**

*В будущем количество атак продолжит расти, а их жертвами начнут становиться юридические лица. Этому будет способствовать распространение веб-инъектов под мобильные браузеры, которые позволят совершать хищения с любого Android-устройства, имеющего доступ к корпоративному счету, а также популяризация банковских мобильных приложений для юридических лиц.*

## КЛЮЧЕВЫЕ ТЕНДЕНЦИИ

### ИСПОЛЬЗОВАНИЕ ЭКСПЛОЙТОВ ДЛЯ РАСПРОСТРАНЕНИЯ

Этот метод устанавливает трояна при посещении взломанного сайта незаметно для пользователя, не требуя от него никаких подтверждений или разрешений. Так, в феврале 2016 года компания Blue Coat зафиксировала распространения программы-вымогателя через набор эксплойтов. На вредоносном сервере был скрипт с эксплойтом под libxslt, который, в частности, использовался итальянской компанией Hacking Team, продававшей программы для шпионажа правительствам разных стран. В будущем **эксплойты для распространения мобильных троянов будут включаться в наборы, продающиеся на хакерском рынке.**

### СНИЖЕНИЕ РИСКА ОБНАРУЖЕНИЯ

**Преступники начали защищать сетевое взаимодействие** между С&С-сервером и зараженным устройством, чтобы было сложнее обнаруживать и исследовать трояны. Кроме того, трояны для Android стали **использовать несколько стадий заражения**. Сначала на систему устанавливается специальный загрузчик, который проверяет, что устройство представляет интерес, а потом тело основного трояна. Такой прицельный выбор жертв позволяет увеличивать эффективность заражения и не привлекать лишнего внимания пользователей.



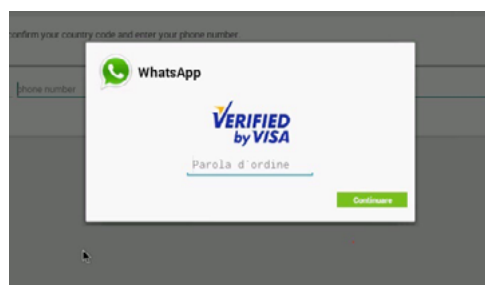
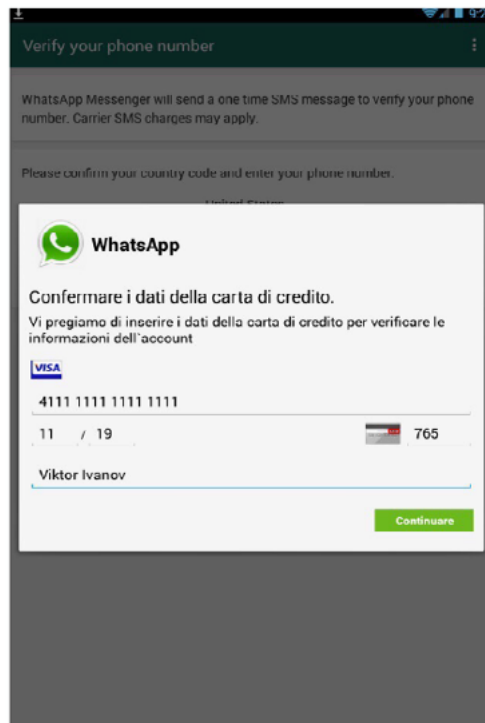
## ТАРГЕТИРОВАНИЕ ВЕБ-ФЕЙКОВ

Формы сбора для сбора логинов, карт и другой чувствительной информации загружаются по команде или на лету во время работы с интересующим преступников приложением.

## ИСПОЛЬЗОВАНИЕ ВЕБ-ИНЖЕКТОВ ДЛЯ МОБИЛЬНЫХ БРАУЗЕРОВ

Веб-инъекты – самый новый и перспективный способ сбора данных на мобильных устройствах. Он позволяет в том числе атаковать тех клиентов, которые не используют мобильный банкинг и не доверяют поддельным окнам, требующим указать данные банковских карт. На рынке уже **начали появляться сервисы по написанию инъектов именно для Android-тroyанов.** Опасность веб-инъектов в том, что они позволят реализовать на мобильных устройствах все технологии хищений, доказавшие эффективность на ПК.

- **Автоподмена.** Непосредственно перед подписанием платежного поручения, вредоносная программа заменяет реквизиты платежа и сумму на мошеннические, при этом на экране и в истории операций отображаются данные, внесенные владельцем счета.
- **Модификация избранного в интернет-банкинге.** С помощью инъектов программа добавляет в «избранное» мошеннические реквизиты, что позволяет делать переводы без дополнительных подтверждений или с повышенными лимитами.
- **Автоматическая смена номера телефона для SMS-информирования.**
- **Соккрытие мошеннических транзакций в истории платежей** в интернет-банкинге, а не только в SMS-уведомлениях.
- **Хищение денег с корпоративных счетов** при наличии доступа к ним с зараженных устройств.
- **Сбор любых данных, доступных в интернет-банкинге.** Внедряя дополнительные формы в отображаемые страницы банка, преступники могут собирать и другую информацию, которая может пригодиться атакующим.



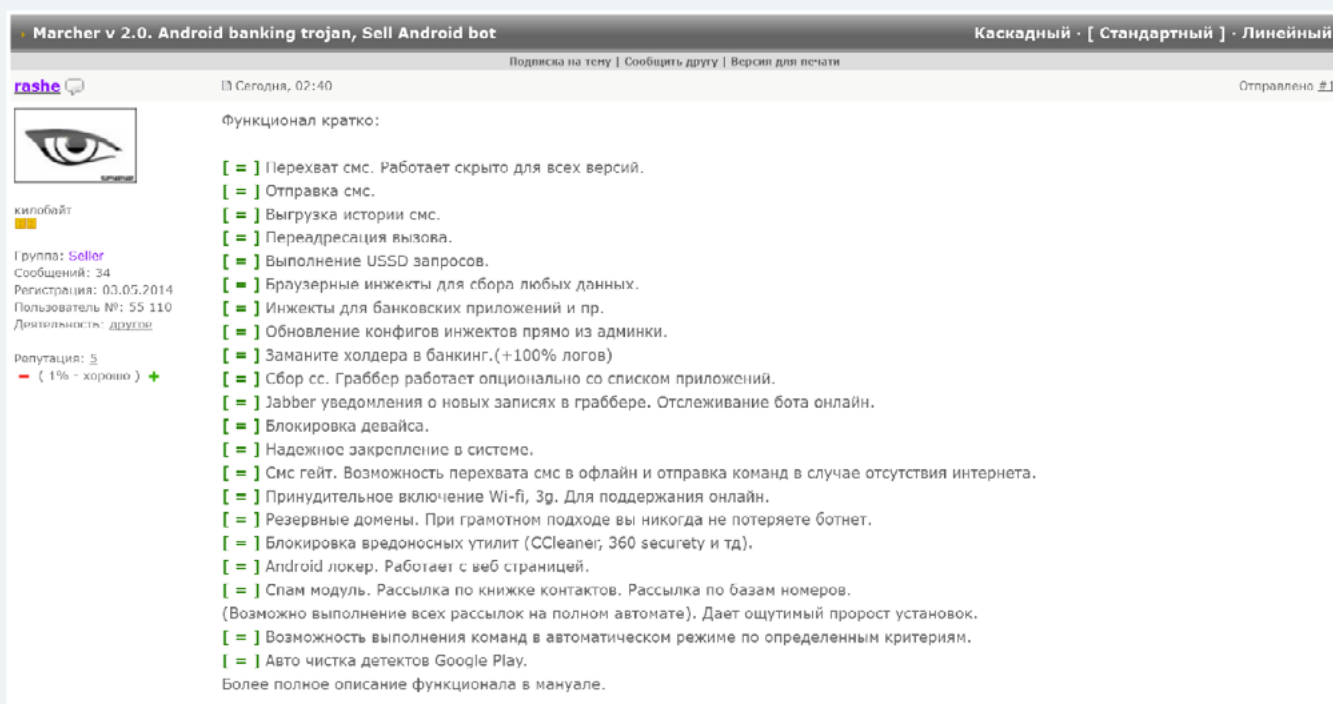
Пример работы веб-фейка на устройстве с Android-тroyаном: мошенническая форма для сбора данных о банковских картах загружается автоматически при открытии приложения

## КЕЙС: MARCHER

Одним из наиболее активно используемых Android-троянов по всему миру является Marcher (также известный как Rahunok). Разработанный русскоязычными специалистами, изначально он использовался одной группой для атак на российских пользователей интернет-банка. Позднее хакеры стали продавать его на закрытых площадках под названием Android-KNL.

В апреле 2016 года вышла его обновленная версия Marcher 2.0, которая поддерживает три метода компрометации банковской информации:

- **Габбер для сбора банковских карт.** Габбер реализован в виде диалога, использующего дизайн официального приложения из магазина Google Play. Злоумышленник заранее прописывает в административной панели список ID приложений, при запуске которых будет появляться диалог с запросом данных банковской карты.
- **Использование заранее написанный HTML-инъектов (веб-фейков).** Инъекты представляют собой фишинговые диалоги, которые показываются жертве при запуске определенного приложения. Пока жертва не введет запрошенные данные, она не сможет продолжить использовать приложение, так как инъект запускается поверх его окна.
- **Использование веб-инъектов для мобильных браузеров.** Marcher одним из первых стал поддерживать веб-инъекты.



Marcher v 2.0. Android banking trojan, Sell Android bot

Каскадный · [ Стандартный ] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

rashe

13 Сегодня, 02:40

Отправлено #1

килобайт

Группа: **Seller**  
Сообщений: 34  
Регистрация: 03.05.2014  
Пользователь №: 55 110  
Дейтельность: [другие](#)

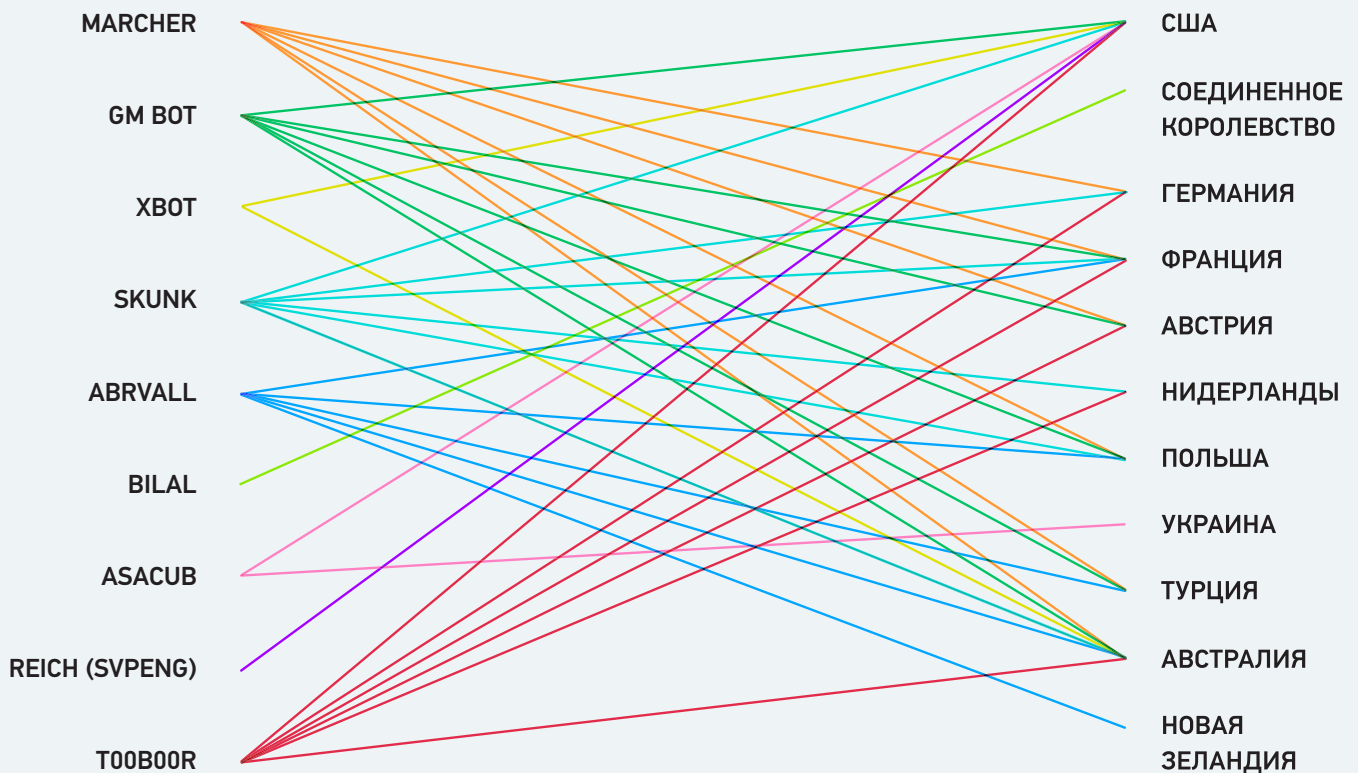
Репутация: 5  
- ( 1% - хорошо ) +

Функционал кратко:

- [ = ] Перехват смс. Работает скрыто для всех версий.
- [ = ] Отправка смс.
- [ = ] Выгрузка истории смс.
- [ = ] Переадресация вызова.
- [ = ] Выполнение USSD запросов.
- [ = ] Браузерные инъекты для сбора любых данных.
- [ = ] Инъекты для банковских приложений и пр.
- [ = ] Обновление конфигов инъектов прямо из админки.
- [ = ] Заманите холдера в банкинг. (+100% логов)
- [ = ] Сбор сс. Габбер работает опционально со списком приложений.
- [ = ] Jabber уведомления о новых записях в габбере. Отслеживание бота онлайн.
- [ = ] Блокировка девайса.
- [ = ] Надежное закрепление в системе.
- [ = ] Смс гейт. Возможность перехвата смс в офлайн и отправка команд в случае отсутствия интернета.
- [ = ] Принудительное включение Wi-fi, 3g. Для поддержания онлайн.
- [ = ] Резервные домены. При грамотном подходе вы никогда не потеряете ботнет.
- [ = ] Блокировка вредоносных утилит (CCleaner, 360 security и тд).
- [ = ] Android локер. Работает с веб страницей.
- [ = ] Спам модуль. Рассылка по книжке контактов. Рассылка по базам номеров. (Возможно выполнение всех рассылок на полном автомате). Дает ощутимый пророст установок.
- [ = ] Возможность выполнения команд в автоматическом режиме по определенным критериям.
- [ = ] Авто чистка детектов Google Play.

Более полное описание функционала в мануале.

## БОТНЕТЫ, ПОСТРОЕННЫЕ С ПОМОЩЬЮ ТРОЯНА MARCHER



### РАСПРОСТРАНЕНИЕ ПОД ВИДОМ ОФИЦИАЛЬНЫХ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Мы все чаще фиксируем распространение Android-троянов под видом мобильных приложений, **как через сайты, так и через Google Play**. Чаще всего преступники используют бренды банков и платежных систем, а также социальных сетей, мессенджеров, облачных хостингов и других популярных сервисов с высоким количеством загрузок. При этом они реагируют и на ситуативные всплески интереса пользователей, например, Android-трояны распространялись под видом приложения Pokemon Go.

### ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ ИНТЕРНЕТ-МАРКЕТИНГА

Для целевого распространения поддельных мобильных приложений через email рассылки и контекстную рекламу в поисковых системах.

## 5 САМЫХ ПОПУЛЯРНЫХ СХЕМ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ANDROID-ТРОЯНОВ

### ХИЩЕНИЯ ЧЕРЕЗ SMS-БАНКИНГ

Некоторые банки позволяют совершать переводы денег по SMS-команде, отправленной на специальный номер банка. Для завершения операции банк отправляет SMS с кодом подтверждения транзакции, который надо отправить обратно в банк. Такие операции можно совершать только с номера телефона владельца счета и на них действуют очень жесткие лимиты.

Android-трояны сами отправляют команды на перевод, перехватывают SMS с кодом подтверждения и автоматически пересылают их в банк. Для хищения атакующим не надо знать ни номер карты, ни логины, ни пароли, только баланс, который они всегда могут получить, отправив SMS -запрос в банк.

SMS-банкинг особенно распространен в России и СНГ, где мы фиксируем максимальное количество таких атак. Мы наблюдаем бот-сети, которые ежедневно автоматически совершают от 50 до 200 мошеннических транзакций. Средняя сумма транзакции составляет 3 000 рублей (\$50).

**ОГРАНИЧЕНИЯ:** жесткие лимиты на размер перевода; не все банки предоставляют услугу SMS-банкинга.

**ПРЕИМУЩЕСТВА:** для хищения не нужны логины, пароли, данные счетов или карт; не требует взаимодействия с пользователем; легко автоматизировать процесс хищения; подходят очень простые трояны, в том числе находящиеся в открытом доступе.

### ПЕРЕВОДЫ С КАРТЫ НА КАРТУ

Чтобы обойти лимиты и иметь возможность атаковать даже клиентов банков, которые не предоставляют услуги SMS-банкинга, преступники начали собирать на Android-устройствах данные банковских карт (номер, CVV, срок действия) через фальшивые диалоговые окна от имени популярных брендов (Whatsapp, Facebook, Google, банка и т.п.). Зная их, злоумышленники используют различные сервисы по переводу денег с карты на карту. Для завершения операции банк отправляет SMS с кодом подтверждения транзакции, которое перехватывается тем же трояном и немедленно отправляется атакующему.

**ОГРАНИЧЕНИЯ:** требуется, чтобы пользователь сам ввел данные банковской карты в поддельное окно; есть лимиты на переводы.

**ПРЕИМУЩЕСТВА:** подходит для атаки на клиентов любого банка в любой стране, лимиты на суммы перевода в большинстве случаев позволяют вывести с банковского счета все деньги.

## ■ ПЕРЕВОДЫ ЧЕРЕЗ ОНЛАЙН-БАНКИНГ

Метод идентичен схеме с переводом с карты на карту, только троян просит ввести логин и пароль от интернет-банкинга, а не данные карты. При этом фальшивое диалоговое окно показывается только если пользователь является клиентом банка, под который у атакующих есть шаблон окна.

**ОГРАНИЧЕНИЯ:** работает только на пользователей онлайн-банкинга, фальшивые диалоговые окна требуют доработки под конкретный банк; требуется, чтобы пользователь ввел логин и пароль в поддельное окно.

**ПРЕИМУЩЕСТВА:** нет лимитов; атакующий получает доступ ко всем счетам; есть возможность открыть кредитный счет и похитить больше денег, чем было у клиента изначально.

## ■ ПЕРЕХВАТ ДОСТУПА К МОБИЛЬНОМУ БАНКУ

Получив номер карты с помощью поддельного диалогового окна, преступник может установить и активировать на своем устройстве официальное мобильное приложение банка. SMS с кодом подтверждения активации будет направлено на зараженный мобильный телефон, где его перехватит троян. Коды для подтверждения последующих транзакций так же будут направляться злоумышленнику.

**ОГРАНИЧЕНИЯ:** схема работает с ограниченным списком банков; требуется, чтобы пользователь сам ввел данные банковской карты в поддельное окно.

**ПРЕИМУЩЕСТВА:** нет лимитов; атакующий получает доступ ко всем счетам; есть возможность открыть кредитный счет и похитить больше денег, чем было у клиента изначально.

## ■ ПОДДЕЛЬНЫЙ МОБИЛЬНЫЙ БАНК

Хакеры распространяют поддельное приложение под видом легального мобильного банка, размещая его на сайтах с доменами, созвучными официальным доменам банка, и в магазинах приложений. Ссылка на программу распространяется с использованием целевых email-рассылок и контекстной рекламы в поисковых системах. Контекстная реклама зачастую показывается первой в поисковых запросах типа «мобильный название\_банка». Специальный скрипт на странице проверяет тип устройства и провайдера, и, если вы зашли с мобильного устройства или из сети мобильного провайдера, вам покажут фишинговую страницу с предложением скачать поддельное приложение. Если вы зашли с компьютера или из сети проводного провайдера, вас перенаправят на страницу с официальным приложением. Таким образом злоумышленники таргетируют установки и защищают себя от обнаружения.

**ОГРАНИЧЕНИЯ:** требует разработки мобильного приложения, прохождения процедур одобрения в магазинах; работает только на пользователей мобильного банкинга; дополнительные расходы на рекламу.

**ПРЕИМУЩЕСТВА:** нет лимитов; атакующий получает доступ ко всем счетам; есть возможность открыть кредитный счет и похитить больше денег, чем было у клиента изначально.

## АВТОМАТИЗИРОВАННЫЕ ФИШИНГОВЫЕ И ВИШИНГОВЫЕ АТАКИ

Мечта любого хакера – полная автоматизация хищений: нажал кнопку «запустить атаку» – и уже через несколько минут на счет начинают поступать деньги, не обязательно даже следить за этим процессом. Именно так совершаются самые современные фишинговые и вишинговые атаки.

### ФИШИНГОВЫЕ АТАКИ

Многие банки защищают денежные средства своих клиентов, требуя подтверждения транзакций с помощью SMS-кодов, скретч-карт, кодов, генерируемых специальными токенами, или секретными вопросами. Это означает, что даже если хакеры получили данные банковской карты, они не смогут перевести деньги без кодов подтверждения или другой проверочной информации. Чтобы успешно похитить деньги у клиентов таких банков, необходимо **получить код подтверждения платежа и воспользоваться им немедленно**, поскольку он имеет ограниченный срок действия.

В середине 2015 года в России нами была зафиксирована серия фишинговых атак на клиентов банков с обходом SMS-подтверждения транзакций. **Этот метод использует только одна русскоязычная хакерская группа, однако именно за ним – будущее фишинговых атак.**

### ТАКТИКА АВТОМАТИЗИРОВАННОЙ ФИШИНГОВОЙ АТАКИ

- Преступная группа имеет большой список «поломанных» сайтов.
- На этих сайтах они размещают специальный Javascript код, проверяющий источник перехода. Если пользователь перешел на «поломанный» сайт из поисковой системы, его перенаправят на фишинговый сайт. Если он зашел по прямой ссылке или на главную страницу взломанного ресурса, перенаправление не производится. Это затрудняет отслеживание и подтверждение взлома.
- Фишинговый сайт, замаскированный под сайт с промо-акцией, информирует жертву о том, что она выиграла денежный приз и может получить деньги немедленно. Для этого ее просят указать данные банковской карты.
- Если жертва указывает данные, на следующем шаге ее просят указать текущий баланс карты.
- В этот момент на сервере атакующего специальный модуль пытается осуществить вывести деньги с карты жертвы, используя онлайн-сервисы для переводов с карты на карту.
- Для завершения перевода необходим SMS-код, который отправляется на телефон жертвы. Как только мошеннический модуль инициирует перевод с карты на карту, на фишинговом сайте появляется окно, запрашивающее SMS-код для получения выигрыша. Если жертва вводит код, операция перевода автоматически подтверждается и деньги мгновенно списываются.

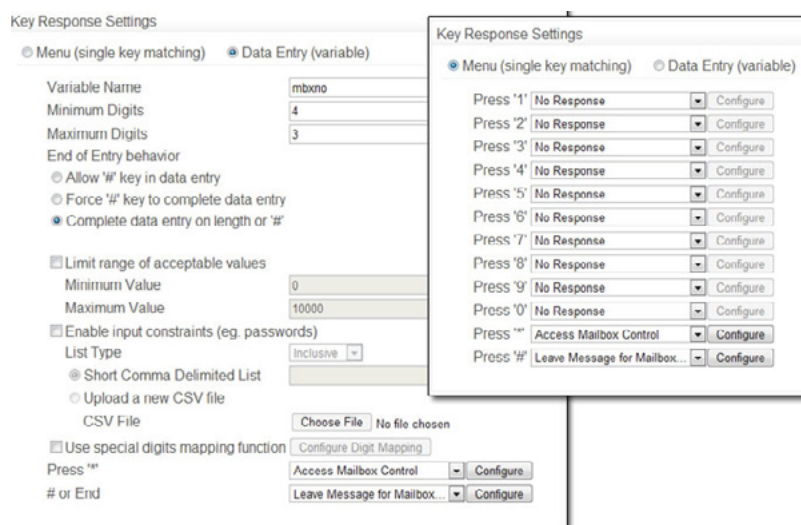
Схема требует, чтобы пользователь указывал все данные сам, но, как показывают наблюдения, на фишинговые страницы попадают тысячи пользователей ежедневно и среди этих тысяч всегда находятся доверчивые люди, которые и становятся жертвой мошенников.

## ВИШИНГОВЫЕ АТАКИ

Вишинг – это разновидность фишинговых атак, но вместо использования поддельных сайтов атакующие собирают информацию (логины, пароли, данные банковских карт) **по телефону**.

## ТАКТИКА АВТОМАТИЗИРОВАННОЙ ВИШИНГОВОЙ АТАКИ

- Используя различные сервисы для отправки SMS, преступники массово рассылают уведомления о блокировке карты пользователя, просроченной оплате кредита или с другим сообщением от банка, которое призвано спровоцировать пользователя на контакт. В тексте SMS указывается мошеннический номер телефона для обратной связи банком.
- На отдельном сервере устанавливается программное обеспечение IVR (Interactive voice response), общение с жертвой осуществляет робот по определенному сценарию.
- В этом сценарии жертву просят пройти стандартную процедуру идентификации клиента: в тоновом режиме ввести данные банковской карты, продиктовать кодовое слово и любую другую необходимую преступникам информацию.



Скриншот системы, автоматизирующей вишинговые атаки



- На сервере с IVR при нажатии клавиш в тоновом режиме пишется специальный журнал, в котором сохраняются данные банковских карт. Кроме нажатия клавиш пишется и голос, и именно из аудиозаписи атакующие извлекают секретное слово. После того как преступники получили эту информацию, уже ни что не препятствует списанию денег.
- Если для подтверждения мошеннической транзакции требуется SMS-код, атакующим, как и в описанном выше сценарии фишинга, будет достаточно начать автоматическую процедуру перевода денег и запрашивать приходящие на телефон жертвы SMS-коды в момент разговора.

**Вишинг хорошо автоматизирован для атак на клиентов банков США и Канады,** в то время как в России и СНГ он еще не получил популярности из-за распространения SMS-подтверждений платежей. Но это неизбежно случится, поскольку такие атаки могут принести ощутимый финансовый результат.

*Мы прогнозируем увеличение количества автоматизированных атак. Появление новых фишинг-китов с автоматизированной системой выставления и подтверждения платежей позволит сильно повысить эффективность хищений в разных странах.*





# КИБЕРШПИОНАЖ

Использование уязвимостей мобильных сетей угрожает не только пользователям телефонов, но и растущей экосистеме промышленных и IoT-устройств, от банкоматов до GSM-систем контроля за работой газовых станций.

Жертвой шпионажа на уровне интернет-провайдера может стать любая организация или компания, владеющая собственной подсетью внешних IP-адресов.



## ШПИОНАЖ НА УРОВНЕ СОТОВЫХ ОПЕРАТОРОВ

Основные проблемы с безопасностью в мобильных сетях связаны со стандартом сигнализации **Signaling System 7 (SS7)** – набором сетевых протоколов, обеспечивающих обмен служебными сообщениями между мобильными устройствами и станциями, а также между самими станциями. Ранее SS7-канал был физически отделен от голосового, но с 2000 года операторы начали передавать сообщения SS7 по IP-сетям, что дало возможность получать доступ к ним извне.

Уязвимости сигнальных сетей позволяют осуществлять самые разнообразные атаки. **Имея доступ к SS7 и зная номер телефона жертвы, можно прослушать разговор, определить местоположение человека, перехватить SMS**, отправить USSD-команду и осуществить другие атаки. Выполнить все эти действия можно, находясь за тысячи километров от атакуемого устройства, а для проведения таких атак не требуется специальное дорогостоящее оборудование.



*В феврале 2014 года посол США в Украине Джеффри Пайат стал жертвой утечки секретного разговора с помощником государственного секретаря США по делам Европы и Евразии Викторией Нуланд. Некоторые считают, что это произошло благодаря использованию уязвимостей в сети мобильных данных SS7, что частично подтверждается отчетом украинского правительства, выпущенным через несколько месяцев после происшествия.*

Для того чтобы получить возможность проводить атаки на SS7, необходимо иметь доступ к SS7-хабу. Этот хаб может быть подключен в любой стране, а через него можно отправлять команды в сеть любого оператора в любой точке мира. Не во всех странах легко получить доступ к таким хабам, но для преступников это не проблема. **Законодательство некоторых стран позволяет легко получить лицензию оператора и установить хаб. В интернете достаточно предложений по подключению к таким хабам.**

**О том, насколько популярным становится слежение за пользователями в сотовых сетях, говорит количество легальных компаний, предоставляющих такие услуги.** По данным Bloomberg, услуги по отслеживанию абонентов с помощью SS7 предлагают американские Defentek и Verint Systems. Об аналогичных предложениях со стороны израильской CleverSig и болгарской Circles говорилось и в утекшей переписке Hacking Team. По сведениям Брюса Шнайера (Bruce Schneier), британская компания Cobham продает систему, позволяющую определить местоположение любого сотового телефона с точностью до метра. Среди ее клиентов госструктуры более 10 стран, включая США, Саудовскую Аравию, Сингапур и Пакистан.

Вот как выглядит описание возможностей одной из таких компаний:

- Комплексное решение с возможностью слежения за абонентом по всему миру. Включает модули, предоставляющие оператору различные аналитические возможности.
- Обеспечивает определение местоположение GSM/UMTS абонента с точностью до соты.
- Независимое решение, основанное на SS7-хабах распределенных в разных точках мира и не требующих взаимодействия с локальными операторами связи.
- Скрытое и безопасное решение, которое сводит к минимуму риск отслеживанию источника.
- Все запросы выполняются с использованием интеллектуальной маршрутизации, маскирующих запросы, что делает практически невозможным мониторинг или отслеживание команд SS7.

**Растет и черный рынок услуг по слежке через SS7:** соответствующие предложения все чаще можно увидеть на хакерских форумах.

**Обнаружить такие атаки на уровне телефона невозможно, они заметны только на уровне оператора связи.**

- **Pointer** - Enables the user to detect if past target locations are nearby, and if so - This module can be used, for example, to protect a VIP figure from approaching targets, or to track a meeting between several targets in real time.

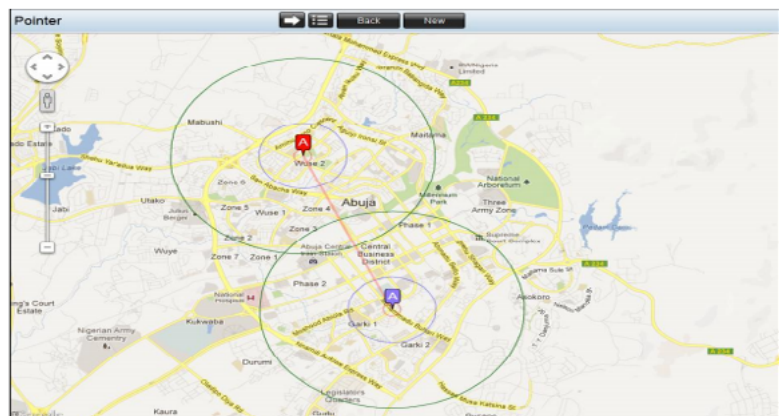


Figure 8 – Pointer module screen

Иллюстрация из буклета о возможностях системы SkyLock компании Verint: корреляция местоположения разных мобильных устройств для отслеживания контактов между несколькими объектами

## ШПИОНАЖ НА УРОВНЕ ИНТЕРНЕТ-ПРОВАЙДЕРОВ

В 2014 году мы уже писали о том, что атаки на протокол BGP будут проводиться чаще, в основном с целью шпионажа. Суть BGP hijacking или перехвата маршрута заключается в перенаправлении сетевого трафика отдельных префиксов автономной системы (пулов IP-адресов) через свое оборудование.

**В умелых руках BGP Hijacking становится прекрасным инструментом для проведения целенаправленных атак и шпионажа.** Если раньше для перехвата трафика нужно было договариваться с провайдером, что в ряде случаев делало атаку невозможной, то, используя BGP hijacking, можно, находясь в одной стране, перехватить весь трафик подсети в другой.

В комбинации с инструментами для целевых атак, манипулирование перехваченным трафиком позволяет получить доступ ко всем данным, включая те, которые шифруются, в том числе, к системам управления серверами, почтой, порталами и т.п.

**Обнаружить перехват трафика так же можно только на уровне интернет-провайдера.** Однако изменение BGP-маршрута в результате ошибок при настройке сетевого оборудования встречается часто, и выявить, какие именно случаи относятся к целенаправленным атакам, очень сложно, что играет на руку преступникам.

---

*В 2015 году в публичном доступе оказался архив с 400ГБ конфиденциальной информации, относящейся к Hacking Team – итальянской компании, специализирующейся на разработке и продаже шпионского программного обеспечения для правоохранительных органов и спецслужб различных государств. В сеть утекла переписка с клиентами, заключенные договоры и другая информация, связанная с деятельностью компании.*

*Анализ переписки показал, что Hacking Team использовала BGP hijacking для перехвата трафика подсети в 256 IP-адресов, принадлежавших хостингу Santrex, активно используемому хакерами.*

## ШПИОНАЖ В КОРПОРАТИВНОЙ СЕТИ

Внедрение шпионского программного обеспечения в сеть компании – одна из старейших и хорошо изученных угроз. Наблюдение за активностью пользователя является одним из этапов атак с самым широким спектром целей: например, функционал для шпионажа есть у многих троянов для хищений.

---

*Троян русскоязычной преступной группы Lurk, еще в 2014 году лидировавшей по числу хищений у юридических лиц, отслеживал работу с окнами, в заголовках которых встречались слова «УГМК» (Уральская горно-металлургическая компания – один из крупнейших производителей меди в России), «медь», «мрамор», «гранит».*

**Злоумышленники все чаще используют для шпионажа не только специальные программы, но и возможности самой корпоративной сети.**

В крупных компаниях есть централизованные системы управления политиками безопасности, установки программного обеспечения на корпоративные компьютеры и мобильные устройства, предотвращения утечек и множество других систем, облегчающих работу администраторам сети. Они же облегчают задачу злоумышленникам.

Например, с помощью систем инвентаризации и установки программного обеспечения атакующие с легкостью находят рабочие станции с нужными доступами, устанавливают на компьютеры и мобильные устройства топ-менеджеров программы слежения.

Получив доступ к системе предотвращения утечек, они смогут осуществлять поиск по типу, по имени файла или его содержимому, вести запись с помощью микрофона и видеокамеры, копировать файлы с внешних носителей и мобильных устройств, подключаемых к зараженному компьютеру, перехватывать переписку в почте и мессенджерах.

**По своей сути эти системы позволяют делать все то же самое, что и шпионское программное обеспечение, только в локальной сети они являются легальными.**

Начальное проникновение, закрепление в сети, получение привилегий происходит по схеме, описанной в разделе «Целенаправленные атаки на банки».

Стоит отметить, что **чем крупнее компания, тем легче ее атаковать**, и связано это прежде всего с большим количеством сотрудников, каждый из которых может стать точкой проникновения в сеть.

Чтобы гарантировать успешное проникновение, преступники используют таргетированные фишинговые схемы, например, звонят сотруднику компании от имени потенциального клиента, предваряя отправку фишингового письма, или используют для рассылки взломанную почту текущих клиентов.

## СОВМЕЩЕНИЕ ФУНКЦИОНАЛА ДЛЯ ХИЩЕНИЙ И ШПИОНАЖА В ANDROID-ТРОЯНАХ

Для автоматизации хищений с помощью Android-тroyанов хакеры используют поиск в SMS по ключевым словам и маскам, выбирая из них те, которые нужны для подтверждения платежа. **То же самое они делают, когда надо найти жертву, потенциально интересную для сбора критичной информации.**

Даже если на зараженном устройстве нет нужных файлов, но атакующим понятно, что жертва представляет особый интерес, они могут получить доступ к облачному хранилищу, привязанному к телефону. В таких хранилищах можно найти документы, резервные копии других устройств, привязанных к AppleID или учетной записи Google, удаленные с телефона фотографии и заметки.

Облачные хранилища часто защищены двухфакторной авторизацией: для доступа к ним кроме пароля необходимо знать и одноразовые коды, которые приходят по SMS. **Но когда у атакующего есть доступ к зараженному телефону, он автоматически получает и пароль от хранилища, и все коды подтверждений.**

**Практически все мобильные трояны для хищений, активные в России, уже сейчас имеют функционал для перехвата SMS.** Со временем этот функционал станет стандартом и для мобильных троянов во всем мире, открывая доступ не только к банковскому счету, но и ко всей конфиденциальной информации, доступной пользователю.

---

*Еще более ухудшает ситуацию то, что зачастую руководители имеют удаленный доступ к ряду критичных для предприятия систем и, атакуя один мобильный телефон, преступники могут получить доступ к данным всей компании.*

*Об атаках с целью шпионажа редко становятся известно широкой публике, поэтому достоверно отследить их динамику невозможно. Однако растущее предложение решений для атак на SSL и перехвата трафика, а также расширение функционала для шпионажа у мобильных троянов неизбежно приведет к росту их числа.*



# АТАКИ НА ПРОМЫШЛЕННЫЕ СИСТЕМЫ И КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ

В фокусе интереса правительственных киберармий и кибертеррористов энергетические компании, химические производства, водоочистительные узлы, аэропорты и транспортные объекты, магистральные сети и другие объекты критической инфраструктуры. Тактика атак на все эти типы предприятий будет очень схожей.





Количество атак на промышленные IT-системы растет на 20% ежегодно. Динамика прироста остается относительно стабильной, но меняется их характер. С обострением взаимного недоверия на международной арене, атаки правительственных киберармий, которые раньше рассматривались как способ расширения каналов сбора разведданных, начинают восприниматься как метод установления контроля над ресурсами политических оппонентов. **Это значит, что целью кампаний все чаще будет не шпионаж, а получение доступа к критическим системам.**

«Гонка кибервооружений» между крупными акторами международной политики стимулирует рост и технологическое усовершенствование инструментов атак, а ее отголоски в медиа привлекают интерес новых заказчиков.

---

*Хакеры, взломавшие Equation Group, связанную с Агентством национальной безопасности США, утверждают, что в предлагаемом к продаже массиве данных АРТ-группы содержатся сведения о «кибероружии», превосходящем по возможностям червя Stuxnet, с помощью которого американские спецслужбы пытались сорвать ядерную программу Ирана.*

**Вхождение в широкую практику использования хакерских атак и их результатов для манипуляции общественным мнением делает их привлекательным инструментом в борьбе за рынки и контракты:** например, остановка производственных линий, технологические аварии могут использоваться конкурентами для подрыва доверия клиентов или снижения стоимости активов, а вброс компрометирующих топ-менеджеров сведений, полученных посредством кибершпионажа, может привести к смене руководства.

Успеху атакующих способствует убежденность многих специалистов по информационной безопасности в том, что если критичная инфраструктура изолирована от глобального интернета, получить к ней удаленный доступ практически невозможно. **Но банки тоже имеют изолированные сегменты сети, и, при огромных инвестициях в обеспечение информационной безопасности, они становятся жертвами атак постоянно.**





## КЛЮЧЕВЫЕ ТЕНДЕНЦИИ

### ДОСТУП К ИНТЕРЕСУЮЩЕЙ СИСТЕМЕ МОЖНО КУПИТЬ

Владельцы бот-сетей для хищений уже сейчас продают доступы к компьютерам, не имеющим выхода на интересующие их финансовые системы (подробнее об этом в разделе «Вымогательство»). Учитывая широкий круг инструментов для кибершпионажа, используемых в банковских трояках, **найти точку входа в интересующую сеть можно через ботнеты.**

### ПОЯВИЛИСЬ ЭФФЕКТИВНЫЕ ШАБЛОНЫ АТАК И КОМБИНАЦИИ БЕСПЛАТНЫХ ИНСТРУМЕНТОВ

Тактика проникновения и получения привилегий, описанная в разделе «Целевые атаки на банки», доказала свою эффективность и может быть использована для получения доступа и удаленного управления критическими системам предприятий. Для написания программы, которая позволит атакующим достичь непосредственных целей, можно привлечь сторонних разработчиков.



*Летом 2016 года на одном из русскоязычных хакерских форумов мы наблюдали обсуждение доклада американской неправительственной организации The Cyber Security Forum Initiative (CSFI) о безопасности систем контроля воздушного пространства и управления самолетами. Использование описанных в нем уязвимостей – посильная задача для хакеров, среди которых есть и выпускники авиационных институтов.*

В главе «Шпионаж» мы описали технологии, которые используются для хищения конфиденциальной информации и слежки за топ-менеджментом. В комбинации с инструментами для целевых атак, они также позволяют получить доступ к критическим системам.

### ФИШИНГ СТАНОВИТСЯ ЭФФЕКТИВНЕЕ, УРОВЕНЬ ПОДГОТОВКИ ПЕРСОНАЛА ПО-ПРЕЖНЕМУ НИЗКИЙ

По данным отчета Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT), американского государственного центра реагирования на инциденты компьютерной безопасности в промышленности, из 295 инцидентов, зафиксированных на объектах критической инфраструктуры за 2015 год, 37% стали результатом фишинговых атак.

**Значительная часть успешных целевых атак, которые мы наблюдали в отчетном периоде, начиналась именно с таргетированной фишинговой рассылки.** Фишинг используют и хактивисты, например, группа Desert Falcons, взламывающая сети промышленных компаний, энергетических объектов, военных и государственных структур в ближневосточном регионе.

## КЕЙС: BLACK ENERGY

### Атаки на энергетический сектор

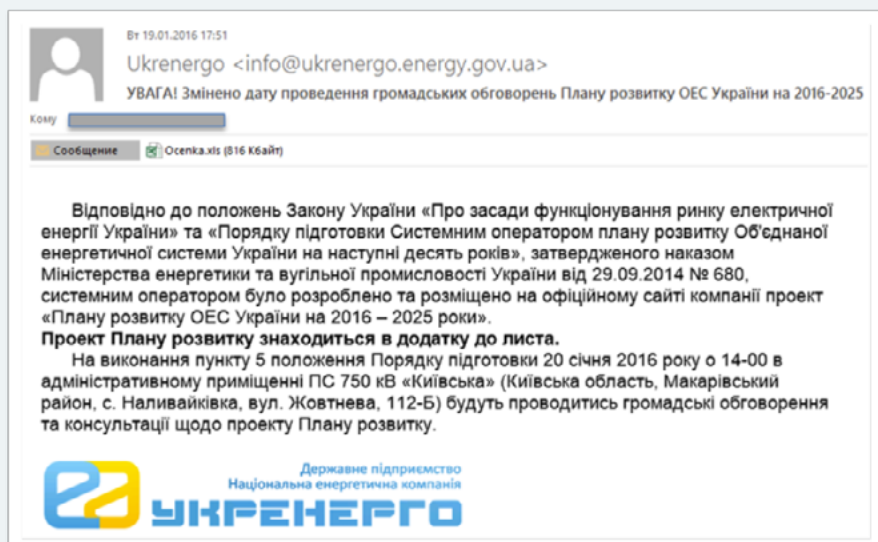
В 2014 году Industrial Control Systems Computer Emergency Response Team (ICS-CERT) сообщил об обнаружении в промышленных системах управления американских энергетических компаний вредоносной программы Black Energy. Целью атак, которые начались еще в 2011 году, были компоненты систем SCADA – человеко-машинные интерфейсы (HMI) разных производителей. Видимых последствий присутствия программы в системах обнаружить не удалось.

23 декабря 2015 года была проведена успешная атака на украинские энергосети, в результате которой без электричества остались более 700 тысяч жителей. В ней использовалась та же BlackEnergy с плагином Win32/KillDisk, предназначенным для уничтожения более 4000 типов файлов (документы, изображения, файлы баз данных и конфигурации и др.) и повреждения операционной системы до такой степени, чтобы она перестала загружаться.

Полный список атакованных украинских компаний не разглашается, известно, что в их число входят «Прикарпатьеоблэнерго» и «Киевоблэнерго». Активность программы в их сетях привела к перебоям в электроснабжении западной части Украины.

В январе 2016 с помощью Black Energy преступникам удалось получить доступ к системе управления воздушным движением аэропорта Борисполь (г. Киев, Украина).

В том же месяце была зафиксирована еще одна атака, которую также связывают с BlackEnergy. От имени ОАО «Укрэнерго» на электронные адреса энергетических предприятий были разсланы фишинговые письма с вредоносным файлом Microsoft Excel. Однако в данной атаке использовалась другая программа – модифицированная версия бэкдора Gcat. Он находится в свободном доступе и предназначен для загрузки дополнительного вредоносного программного обеспечения на зараженные компьютеры и исполнения их с помощью shell-команд.



Еще 6% инцидентов, выявленных ICS-CERT на объектах критической инфраструктуры, были связаны со слабыми паролями. Таким образом, можно сказать, что **безопасность критических объектов как минимум на 40% зависит от персонала**. При этом доля расходов на решения, минимизирующие киберриски, связанные с «человеческим фактором», в общем объеме инвестиций в обеспечение безопасности промышленных, энергетических и инфраструктурных объектов непропорционально мала.

---

*Опыт банков, которые находятся в авангарде борьбы с фишинговыми атаками, показывает, что их предотвращение требует комплексного подхода:*

- *обучение персонала, проведение соцтестов,*
- *использование киберразведки (threat intelligence) для оперативного получения данных о новых рассылках,*
- *контроль сетевого трафика с использованием систем обнаружения целевых атак,*
- *запуск вложений и исследование их поведения в изолированной среде для выявления неизвестного вредоносного кода.*

## **УСИЛИВАЕТСЯ РЕКРУТИНГОВЫЙ ПОТЕНЦИАЛ КИБЕРТЕРРОРИСТИЧЕСКИХ ГРУПП**

Европейский миграционный кризис, ухудшение социально-экономической ситуации, обострение этнических и религиозных конфликтов в целом ряде регионов мира питают почву для восприятия пропаганды террористических и экстремистских группировок, которые **открыто рекрутируют хакеров в теневом сегменте интернета**. Как показывает наш опыт расследований, чтобы организовать изобретательную и разрушительную атаку, зачастую нужен всего один человек с острым умом. Рано или поздно такой человек окажется на стороне террористов.

Атаки киберхалифата (Cyber Caliphate, киберподразделения ИГИЛ), которые мы фиксируем в разных регионах мира, по-прежнему носят хаотичный характер и в большинстве своем ограничиваются DDoS-, дефейс-атаками и взломами некритичных баз данных. Такой же уровень подготовки демонстрируют хакеры, участвующие в операциях Anonymous. Но за мелкими инцидентами, количество которых будет только расти, важно не пропустить одну организованную целевую атаку, ущерб от которой перекроет все предыдущие достижения кибертеррористов.

---

*В марте 2016 в Нью-Йорке были предъявлены обвинения семи иранским хакерам, которые, по версии следствия, в интересах Revolutionary Guards Corps, подразделения вооруженных сил Ирана, совершили не менее 46 DDoS-атак на американские банки, а в 2013 проникли в системы управления дамбы Bowman Avenue (США). Доступ к компьютеру диспетчера плотины давал им возможность контролировать уровень и температуру воды, а также регулировать положение ворот дамбы.*



*Мы прогнозируем сохранение темпов прироста количества атак и увеличение числа резонансных взломов. Некоторые специалисты по информационной безопасности считают, что хакеры (например, опытные вирусписатели или проправительственные группировки), которые могут совершить атаки на критические инфраструктуры, не заинтересованы в них, а те, кто заинтересован (например, террористические организации), пока не обладают нужной квалификацией. Разделяя это мнение по существу, мы оцениваем вероятность атаки на объект критической инфраструктуры со значительным ущербом, вплоть до человеческих жертв как высокую.*

*Уже сегодня киберпреступники используют политические разногласия, чтобы совершать хищения в других странах, не боясь экстрадиции (примеры: Россия-Украина, Израиль-Ливан, Пакистан-Индия). На фоне взаимного недоверия спецслужб атаки на промышленные объекты позволяют строить и более сложные схемы, подогревая конфликт изнутри или влияя на его развитие извне.*

## ХАКЕРСКИЕ АТАКИ В ПОЛИТИЧЕСКОМ КОНТЕКСТЕ

Обострение политических конфликтов и взаимное недоверие игроков на международной арене привело к резкой политизации темы хакерских атак, которые теперь воспринимаются через призму отношений между странами. Мы недалеко от ситуации, когда подозрение проправительственных хакеров одной страны в атаке на критические объекты другой может привести к кризису дипломатических отношений, их разрыву, а в последствии и полномасштабным военным действиям.

Расследуя киберпреступления более 10 лет, мы привыкли к тому, что хакеры имитируют действия других преступных групп и расставляют приманки, наводящие на ложный след, чтобы отвести от себя подозрения. При установлении источника атаки, имеющей политическое значение, цена ошибки может быть очень велика.

Для связывания атак с конкретной страной исследователи обращают внимание на такие факторы, как:

- наличие в коде строк на определенном языке,
- время сборки вредоносных файлов,
- язык операционной системы, на которой происходила компиляция файла или создания документа,
- регистрационные данные доменов,
- местонахождение серверов для управления вредоносными программами,

и целый ряд других параметров.

Важно понимать, что о них известно как профессионалам, исследующим атаки, так и атакующим. В распоряжении которых целый арсенал инструментов, позволяющих провести атаку, следы которой будут вести в другую страну.

Перед киберкриминалистами, проводящими исследование подобных инцидентов, стоит сложнейший профессиональный вызов, с которым сложно справиться в одиночку.

Вынести взвешенное решение, особенно в условиях политического давления, поможет обмен данными киберразведки (threat intelligence) внутри профессионального сообщества (CERT, регистраторами доменных имен и хостинг-провайдерами, киберкриминалистами и т.п.). Такой обмен позволяет строить эффективные связи между разными инцидентами и получать более полную картину по отдельной атаке.

Именно полная картина дает возможность снизить вероятность ошибок в выводах об источнике реальной угрозы и опасных политических последствий, следующих за ними.



# ВЫМОГАТЕЛЬСТВО

За последние годы не осталось ни одного сектора, компании которого не были бы атакованы с помощью вирусов-шифровальщиков. Чем критичнее для вас доступ к информации, тем больший выкуп могут потребовать злоумышленники.

Краткосрочные DDoS-атаки также опасны для всех секторов, однако наиболее перспективны для преступников атаки на компании, чья лишь операционная деятельность зависима от портала, например, на интернет-магазины, веб-сервисы, банки и СМИ.



## DDOS-АТАКИ

Буквально 4-5 лет назад наиболее опасными DDoS-атаками были те, которые проводились с использованием бот-сетей, поскольку это позволяло даже небольшим числом ботов вызвать большую нагрузку на атакуемый ресурс. Со временем атакующие начали находить более эффективные методы DDoS-атак, вызывая максимальную нагрузку не на сервер, а на канал.

Для эффективной атаки на канал активно начали использовать усилители (DNS, NTP, SSDP, CharGen и др.) и этот тренд держался несколько лет, в результате чего в 2016 году максимальная мощность атак выросла до 602 Gbps (с 450 Gbps в 2015).

Все это время мы наблюдали активное использование для этих целей роутеров и контроллеров, которые идеально подходят для DDoS-атак: они доступны круглосуточно, не защищены антивирусами, подключены к хорошим каналам и позволяют проводить сложные атаки без подмены IP-адресов.

## ИОТ – ДРАЙВЕР РОСТА БОТ-СЕТЕЙ ДЛЯ DDOS-АТАК

Количество неправильно настроенных серверов, которые можно использовать в качестве усилителей, постоянно снижается. Отчасти это связано с действиями компаний, занимающихся защитой от DDoS-атак, которые оповещают как владельцев серверов, так и провайдеров, предоставляющих этим серверам доступ в интернет.

**В этом году наметился тренд на возврат популярности бот-сетей для DDoS-атак, но теперь для их создания используют не компьютеры с Windows, как было раньше, а Linux-серверы и простые IoT (Internet of Things)-устройства.**

Такие ботнеты становятся достаточно большими, а время жизни каждого бота значительно дольше, чем у Windows-трояна. Например, последняя описанная бот-сеть из камер видеонаблюдения (CCTV) считывала 25 тысяч устройств, есть аналогичные бот-сети из домашних маршрутизаторов или даже из аппаратных контроллеров для удаленного управления серверами.

Основным способом получения доступа и к серверам, и к IoT устройствам остается перебор паролей, либо эксплуатация известных уязвимостей.

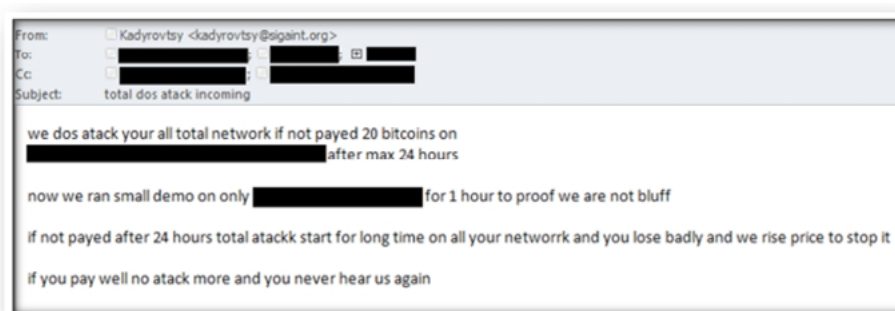
### IoT-устройства прекрасно подходят на роль ботов:

- они имеют динамические IP-адреса и их сложно фильтровать;
- не имеют антивирусов, и удалить с них вредоносный код будет проблематично;
- они имеют круглосуточный доступ в сеть и, как правило, без каких-либо ограничений;
- их сложно обновлять и устранять известные уязвимости, поэтому их время жизни очень продолжительно;
- часть таких устройств имеют пароли, установленные по умолчанию, что облегчает процесс заражения.

Хакеры постоянно сканируют интернет на наличие открытых портов SSH, Telnet или уязвимых сервисов. В случае успешного подбора пароля или эксплуатации уязвимости на устройство загружаются боты разных типов. Преимущественно это IRC-боты на основе выложенного в 2015 году исходного кода LizardStresser, а также отдельные утилиты для проведения атак типа HTTP flood.

## АКТИВИЗАЦИЯ DDoS-ВЫМОГАТЕЛЕЙ

В январе 2016 года в рамках операции Европола была задержаны члены группы DD4BC, вымогавшей деньги за прекращение DDoS-атак. После этого приостановили активность Armada Collective и Kadyrovtsy. **Группы исчезли, но стали появляться клоны, которые копируют тактику их действий.**



Письмо с требованием выкупа за прекращение DDoS-атак от группы Kadyrovtsy

Как правило, у клонов нет собственной инфраструктуры для проведения атак. Некоторые из них просто занимаются рассылкой писем. **Если перед тем как отправить письмо с угрозой вымогатели не провели атаку, значит, у них нет своих ресурсов для ее осуществления и их требования можно игнорировать.**

Некоторые устраивают показательные атаки, используя публичные платные сервисы, где можно заказать DDoS-атаку на любой сайт. Такие атаки длятся в среднем 15 минут, прекращаясь сразу по достижению пика.



Короткая продолжительность обусловлена следующими причинами:

- пиковые значения, которые производят самый большой эффект на жертву, достигаются примерно за 15 минут;
- обычно после пиковых значений начинают эффективно работать системы противодействия DDoS и эффективность атаки автоматически снижается.

Поскольку преступники оплачивают каждую атаку из собственного кармана, они не хотят инвестировать в одну жертву больше стоимости минимальной по времени атаки (обычно как раз 15 минут), поэтому **если после первой атаки компании отказываются платить, то они переключатся на следующую жертву**. Повторная атака может быть запущена, но продлится она недолго, особенно если компания использует защиту от DDoS-атак.

*С учетом широкого и бесплатного распространения эффективных вредоносных программ для IoT-устройств, вымогатели начнут создавать собственные бот-сети, сокращая расходы на аренду внешних сервисов для DDoS. Это в свою очередь, приведет к тому, что вымогатели начнут вести себя более активно и первоочередной их целью будут компании из финансового сектора, но без постоянно включенной защиты от DDoS-атак.*

## АТАКИ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ

Основной задачей таких программ является шифрование файлов таким образом, чтобы расшифровать их можно было только при наличии специального секретного ключа, находящегося у атакующего.

Изначально программы-вымогатели были нацелены только на обычных граждан, использующих компьютеры под управлением Windows, но сейчас ситуация сильно поменялась: **появились новые программы, увеличилось количество атакующих, изменились схемы распространения.**

### КЛЮЧЕВЫЕ ТЕНДЕНЦИИ

#### ОБМЕН ДАННЫМИ О ПОТЕНЦИАЛЬНЫХ ЖЕРТВАХ

Рост количества атак на компании связан в том числе с тем, что владельцы бот-сетей начали продавать доступы к компьютерам с критичными финансовыми системами, из которых нельзя похитить деньги, но потеря данных из которых критична для бизнеса.

Некоторые хакеры, управляющие банковскими троянями, в первую очередь интересуются компьютерами с системами дистанционного банковского обслуживания, и часто обнаруживают компьютеры бухгалтеров, которые привыкли работать удаленно в 1С. Поэтому они начали продавать информацию о таких компьютерах своим «партнерам», чтобы те шифровали данные и извлекали из этого прибыль. **По аналогичной схеме доступы к системам могут быть проданы кибертеррористам или игрокам, заинтересованным в кибершпионаже.**

19	ACCI	13B6	77	186°	UA	0.250	80k Отр
20	ACCI	3A8	210	12.83°	—	4.243	Фуфен
21	ACCI	A15	190	75.19°	UA	0.703	укрсиб 40k
22	ACEI	69	46	02°	UA	21.014	укрсиб - 50k
23	ACEI	0343	62	212°	UA	0.900	1c
24	ADM	530	95	00°	UA	1.210	privat online
25	ADM	176A	77	1.180°	UA	2.000	bot
26	ADM	AED	37	87°	UA	0.453	aval 11k
27	ADM	522DF69	94	134°	UA	2.059	40k F&C
28	ADM	3611E8A	176	88°	UA	1.217	ukrsots
29	ADM	13D58F2	82	2.16°	UA	0.735	1c
30	AID-I	576	176	70.111°	UA	0.422	exim MENS
31	ANV	3F0C	3.2	0°	—	198.900	1c
32	ANV	0	62	51°	RU	19.070	200k rub
33	ALEI	3F1A	93	222°	UA	13.320	25k ukrgazbank
34	ALEI	7D4	190	5.90°	UA	0.531	ukrsib 73k
35	ALEI	22DF69	82	109°	UA	10.826	386k Aval
36	ALEI	23	190	14°	UA	0.500	2x asans
37	ALEI	00	94	22°	RU	0.702	1c
38	ALEI	72DF4	78	1.100°	UA	2.449	privat online
39	ALLF	A2	91	230°	UA	40.370	aval 1k
40	ALLF	58	37	62°	UA	3.187	ukrsots - 23k
41	ALTE	34D	194	1.175°	UA	1.888	VShank 15k
42	AME	1AA	91	3.72°	UA	0.749	1c
43	ANA	1F98A6F1	91	2.18°	UA	0.734	bux
44	ANGI	2DF69	180	76.115°	UA	0.577	-300k Kredobank

Пример системы управления зараженными компьютерами, на которых была установлена система 1С (рисунок предоставлен компанией CyS Centrum).

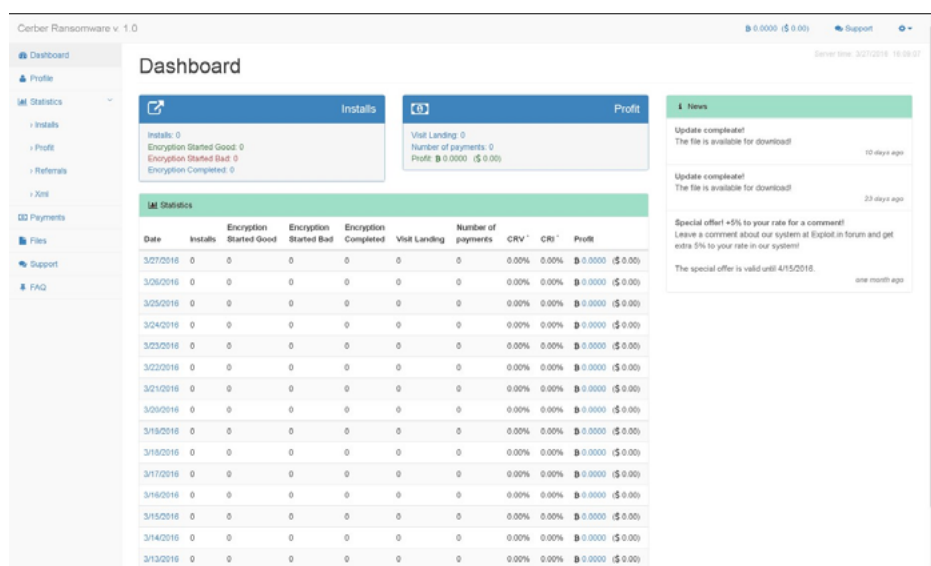
## ПОВЫШЕНИЕ ВЕРОЯТНОСТИ ВЫПЛАТЫ

Кроме того, хакеры начали проверять серверы с подобранными паролями на наличие систем с данными, потеря доступа к которым с высокой степенью вероятности приведет к выплате суммы, требуемой вымогателями.

Наиболее важная информация хранится на серверах, а самой популярной операционной системой для серверов является Linux. Поэтому атакующие создали вымогателей, которые шифруют данные на Linux-серверах.

## РАЗВИТИЕ СЕРВИСОВ, УПРОЩАЮЩИХ АТАКИ

Появились новые партнерские программы по распространению программ вымогателей, предоставляющие любому желающему возможность сгенерировать исполняемый файл вымогателя, который может быть использован для заражения устройств жертв, и среду для переписки с требованиями выкупа. 20% от выкупа перечисляются создателю сервиса.



**Dashboard**

Installs: 0  
Encryption Started Good: 0  
Encryption Started Bad: 0  
Encryption Completed: 0

Profit: \$ 0.0000 (\$ 0.00)

Visit Landing: 0  
Number of payments: 0  
Profit: \$ 0.0000 (\$ 0.00)

Date	Installs	Encryption Started Good	Encryption Started Bad	Encryption Completed	Visit Landing	Number of payments	CRV *	CRS *	Profit
3/27/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/26/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/25/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/24/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/23/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/22/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/21/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/20/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/19/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/18/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/17/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/16/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/15/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/14/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)
3/13/2016	0	0	0	0	0	0	0.00%	0.00%	\$ 0.0000 (\$ 0.00)

Скриншот системы управления программы-вымогателя Cerber, которая не только шифрует файлы, но и позволяет использовать компьютер для проведения DDoS-атак и рассылки спама

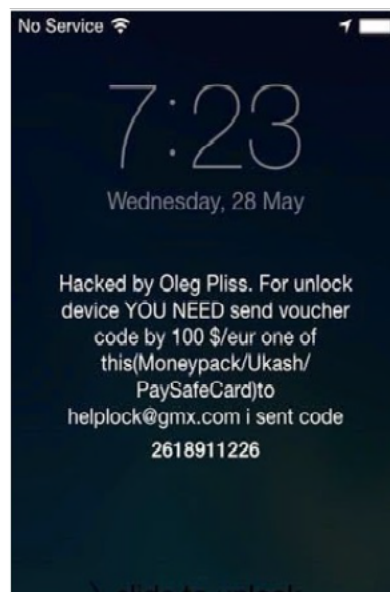
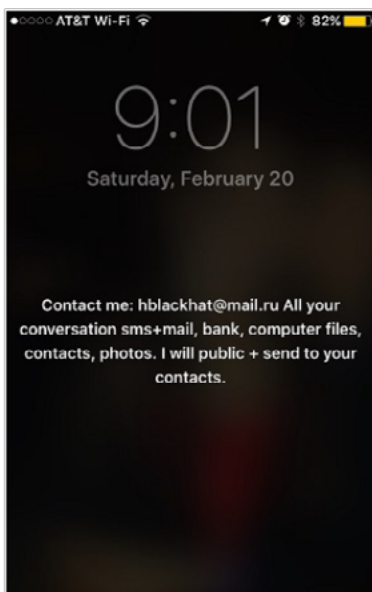
## УВЕЛИЧЕНИЕ КОЛИЧЕСТВА АТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА

### — На Android-устройства

Вымогатели для Android после шифрования выводят на экран устройства страницу, написанную на HTML/JS коде, с требованием перевести деньги на счет злоумышленника. В феврале 2016 года компания Blue Coat зафиксировала распространение программы-вымогателя под Android через набор эксплойтов. На вредоносном сервере был скрипт с эксплойтом под libxslt, который был в утечке Hacking Team.

### — На iOS-устройства

Установить вредоносное программное обеспечение на устройство Apple непросто, поэтому мошенники придумали особый подход. Специальное вредоносное ПО, используя базу перехваченных логинов и паролей от iCloud, автоматически заходит в iCloud, сбрасывает пароль, меняет привязанный адрес электронной почты, блокирует все устройства, привязанные к AppleID и настраивает окно блокировки таким образом, чтобы оно отображало требование атакующего перевести деньги за разблокировку.



Поскольку данные на атакованном iOS-устройстве не шифруются, снять блокировку можно самостоятельно: для этого нужно войти в свой iCloud через веб-интерфейс, открыть приложение «Найти iPhone» (Find My iPhone), выбрать нужное устройство, а затем опцию «Стереть» («Erase»). Данные, не сохраненные в облаке, при этом потеряются, но выкуп платить не придется.

## ШИФРОВАНИЕ IOT-УСТРОЙСТВ

Специалисты компании Symantec провели исследование, в ходе которого успешно заразили Smart TV на платформе Android программой-вымогателем. Компании Pen Test Partners удалось зашифровать данные на термостате и вывести требование выкупа на экране устройства.

В реальности таких инцидентов еще не было, однако потенциал монетизации атак с помощью шифровальщиков, **увеличение числа IoT-устройств в бот-сетях будет стимулировать преступников искать способы их заражения.**

С появлением популярных производителей IoT-устройств возникнет и рынок информации об их уязвимостях. IoT-устройства будут использоваться и в мошеннических схемах, например, для перенаправления на фишинговые сайты, демонстрации рекламы с предложением скачать вредоносные программы, замаскированные под легальные, и т.п.

*Частота и результативность атак с использованием программ шифровальщиков продолжит расти за счет автоматизации и целевого таргетирования атак.*

*Динамичный рост количества атак на компании и активный выход шифровальщиков на мобильные устройства стимулируют развитие сегмента страхования киберрисков. Страхование приведет к увеличению случаев, когда жертва платит атакующему, что еще больше стимулирует атакующих, — а это, в свою очередь, еще активнее стимулирует рынок страхования.*



# МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БРЕНДА

Угрозы, связанные с брендом, актуальны не только для производителей товаров и поставщиков услуг для конечных потребителей, но и для компаний, работающих в B2B-сегменте.

Мошенники все чаще привлекают жертв с помощью инструментов интернет-маркетинга: контекстная реклама лишает официальные ресурсы части целевого трафика, а использование преступниками методов SEO-оптимизации приводит к понижению позиций в поисковой выдаче официальных сайтов.



Когда речь заходит о мошенничествах с использованием бренда, большинство думает о контрафакте и фишинге. Но спектр угроз для бренда значительно шире, и мы видим, что он активно увеличивается, распространяясь и на сектор B2B.

## 8 РАСПРОСТРАНЕННЫХ СХЕМ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ БРЕНДА

### МОШЕННИЧЕСКИЕ КОНТРАКТЫ

Один из методов, набирающих популярность, – создание копий официальных сайтов компании с измененными контактными данными. Для автоматизации этого процесса уже есть готовые инструменты, которые позволяют атакующим создавать множество клонов сайта в течение нескольких минут. В других вариациях этого мошенничества в разделе «Партнеры» на копии официального сайта вписывают ссылку на подставную компанию, которая в дальнейшем представляется клиентам официальным дистрибьютером.

Для привлечения посетителей используется продвижение в социальных сетях, email-рассылки по специальным базам, SEO-продвижение для повышения позиций сайта в выдаче по нужным поисковым запросам.

На сайте анонсируются распродажи, специальные предложения и другие скидки на продукцию. Если жертва связывается с владельцами мошеннического сайта, ей предлагают подписать контракт с предоплатой.

**ДЛЯ КОГО ОПАСНО.** Мы фиксировали создание мошеннических площадок с использованием брендов промышленных, машиностроительных предприятий, компаний нефтегазового сектора, производителей удобрений. Потенциально жертвой может стать любой известный бренд в сегменте B2B, в том числе в узкоспециализированных нишах.

---

*Мы фиксировали создание и продвижение копий сайтов российских промышленных, машиностроительных предприятий, компаний нефтегазового сектора, производителей удобрений для последующего заключения мошеннических контрактов от их имени. Средний подтвержденный ущерб от такой атаки составил 1,5 млн ₽.*

### ПОДДЕЛЬНАЯ ФИНАНСОВАЯ ОТЧЕТНОСТЬ

Мошеннические сайты помогают преступникам манипулировать стоимостью акций. На таком сайте публикуется недостоверная финансовая отчетность компании, ссылка на которую может быть вброшена, например, через форумы для биржевых аналитиков. Такие случаи обычно являются элементом более комплексной операции и могут сопровождаться дополнительными информационными атаками.

**ДЛЯ КОГО ОПАСНО.** Жертвой может стать любая публично торгуемая компания. Особенно уязвимы компании, для которых резкое колебание цен на акцию критично, например, при подготовке к допэмиссии или в процессе переговоров о слиянии.

## ПОДСТАВНЫЕ СОТРУДНИКИ КОМПАНИИ В СОЦИАЛЬНЫХ СЕТЯХ

Злоумышленники представляются сотрудниками компании в социальных сетях и предлагают услуги их клиентам. Например, такой сотрудник может ответить на пост с жалобой на сервис банка и предложить решить проблему, если автор назовет данные банковской карты или логин и пароль к личному кабинету. Для большей убедительности на аватаре такого пользователя (чаще всего – женского пола) может стоять фотография сотрудника банка в униформе.

Для этих целей используются как свежие зарегистрированные пользователи, так и поломанные учетные записи с хорошей историей, чтобы вызывать меньше подозрений недавно зарегистрированной учетной записью.

Нами были зафиксированы и более изощренные схемы, когда через социальные сети сотрудникам отправлялись указания и распоряжения от имени руководителя.

**ДЛЯ КОГО ОПАСНО.** Чаще всего преступники используют бренды банков, мобильных операторов и интернет-провайдеров, поскольку они позволяют запросить доступ к критичным идентификаторам пользователя, не вызывая подозрений.

## ЛОЖНАЯ РЕКЛАМА В СЕТИ

Контекстная реклама по релевантным поисковым словам, связанным с брендом, является одним из самых эффективных методов привлечения жертв на фишинговые сайты. Реклама показывается на первом месте в поисковой выдаче, поэтому пользователь может просто не дойти до строки со ссылкой на официальный ресурс.

Куда попадет пользователь после нажатия на рекламу, зависит от желания мошенников. Специальный скрипт на сайте позволяет определить географическое расположение пользователя, используемое им устройство и сеть. Зная эти параметры, преступники могут таргетировать атаки в зависимости от своих целей. Например, распространители мобильных троянов могут оставлять на мошенническом сайте только пользователей устройств на Android, а всех остальных перенаправлять на официальный сайт компании. Это позволяет им не привлекать лишнего внимания к своей активности.

---

*Отловить мошеннические объявления «руками» практически невозможно – они показываются в разное время, в разных регионах, и ориентированы на десятки разных ключевых запросов. Бороться с ними можно только используя решения для threat intelligence, позволяющие отслеживать контекстную рекламу.*



**ДЛЯ КОГО ОПАСНО.** Потенциально жертвой может стать любая компания, работающая в сегменте B2B, а также компании из B2C с популярным брендом или предоставляющие услуги широкому слою населения, например, государственные порталы, популярные игры, банки и другие.

## ПОДДЕЛЬНЫЕ МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ

О растущем количестве вредоносных мобильных приложений мы рассказывали в разделе о мобильных трояках. Такие приложения не только наносят ущерб жертвам атак, но и подрывают доверие в сети к компаниям, которые не уделяют должного внимания защите своих брендов.

**ДЛЯ КОГО ОПАСНО.** В первую очередь, владельцы приложений с большим количеством загрузок и компании с известным брендом. На небольших рынках и в отдельных нишах мобильные приложения могут использоваться для подрыва доверия к бренду и перехвата клиентской базы.

## ФИШИНГ ЧЕРЕЗ МЕССЕНДЖЕРЫ

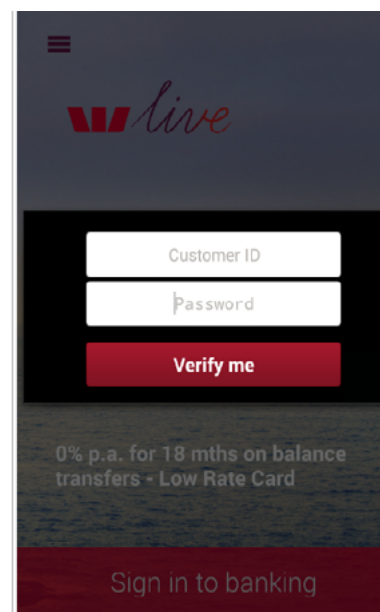
Через популярные мессенджеры рассылается картинка с предложением поучаствовать в опросе от имени бренда и получить небольшой, вполне реалистичный бонус, вроде символического подарка, скидки или денежного поощрения. Ответив на 3-5 простых вопросов на мобильном сайте, пользователь попадает на страницу с фишинговой формой для сбора данных о карте или других идентификаторов пользователя.

**ДЛЯ КОГО ОПАСНО.** Массовые, популярные бренды – от производителей продуктов питания до агрегаторов такси.

## ПОДДЕЛЬНЫЕ SSL-СЕРТИФИКАТЫ

Все вредоносные программы, которые занимаются перенаправлением пользователей на поддельные сайты, используют сертификаты, выпущенные на имена легальных компаний. Таким образом, пользователь попадает на поддельный сервер, но в адресе страницы остается легальный домен и сертификат не выдает никаких предупреждений. Поскольку сертификат мошеннический, атакующие имеют возможность прослушивать весь зашифрованный трафик.

**ДЛЯ КОГО ОПАСНО.** Прежде всего для компаний, пользователи которых обращают внимание на защищенность соединения, – банки, платежные системы, государственные порталы, облачные сервисы.



Поддельные мобильные приложения точно копируют дизайн официальных и практически неотличимы от настоящих

## ПИРАМИДЫ

В сети всегда находятся люди, которые хотят быстро заработать, и этим также активно пользуются мошенники. Для таких любителей «бесплатного сыра» создаются различные хайп-проекты (от англ. HYIP - High Yield Investment Program), а по сути – те же финансовые пирамиды. Для того, чтобы привлекать в них больше людей, необходимо развеять сомнения в их надежности. В этом очень помогает использование имен известных людей, логотипов хорошо узнаваемых компаний в числе партнеров или участников проекта.

**ДЛЯ КОГО ОПАСНО.** Прежде всего это актуально для банков и платежных систем: используя их бренды, преступники как бы подтверждают свою финансовую грамотность и демонстрируют наличие связей в финансовых кругах. Кроме этого, жертвой могут быть брокерские компании и международные финансовые корпорации, в зависимости от легенды используемой мошенниками.

*Чем больше точек контакта потребителя с брендом, тем больше возможностей для мошенничества, а чем популярнее бренд, тем более он интересен для злоумышленников. Для оперативного выявления преступной активности необходимо следить сразу за множеством объектов: доменными именами, SSL-сертификатами, контекстной рекламой, социальными сетями и мобильными приложениями близко к режиму реального времени. Делать это вручную, ресурсами компании практически невозможно, однако на это способны системы киберразведки (threat intelligence).*

Group-IB – одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий.

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

- Крупнейшая и самая опытная Лаборатория компьютерной криминалистики в Восточной Европе
- Круглосуточный Центр реагирования на инциденты информационной безопасности CERT-GIB
- Система раннего предупреждения киберугроз – линейка продуктов для проактивной защиты



Официальный партнер Europol, полицейской службы Евросоюза



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



Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider UK



Первый российский поставщик данных киберразведки (threat intelligence), вошедший в отчеты Gartner

## УНИКАЛЬНАЯ РЕСУРСНАЯ БАЗА, НАКОПЛЕННАЯ ЗА 13 ЛЕТ РАБОТЫ

Высокотехнологичная инфраструктура сбора данных об угрозах в ключевых регионах происхождения: Россия и Восточная Европа, Юго-Восточная Азия, Ближний Восток



### ИНФРАСТРУКТУРА МОНИТОРИНГА

- Распределенная сеть мониторинга и HoneyNet-ловушек
- Аналитика бот-сетей
- Трееры сетевых атак
- Мониторинг хакерских форумов и закрытых сетевых сообществ
- Данные сенсоров TDS
- Система поведенческого анализа



### ОПЫТ ЭКСПЕРТОВ

- Результаты криминалистических экспертиз Лаборатории Group-IB
- Материалы расследований
- Мониторинг и анализ вредоносных программ
- База обращений и практика реагирования на инциденты CERT-GIB
- Целевая аналитика Group-IB на 7 языках



### ОБМЕН ДАННЫМИ

- Команды реагирования CERT
- Регистраторы и хостинг-провайдеры
- Производители средств защиты
- Организации и объединения по противодействию киберугрозам
- Europol, Interpol и правоохранительные органы

## ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ПОД УПРАВЛЕНИЕМ ОПЫТНЫХ СПЕЦИАЛИСТОВ

Собственные решения для извлечения данных из закрытых источников, поиска по хакерским площадкам, проведения криминалистических исследований, анализа и моделирования угроз, в том числе:

Выявление неизвестных угроз с помощью алгоритмов поведенческого анализа и технологий машинного обучения

Система детектирования фишинга, извлечения phishing kits и оперативное блокирование опасных ресурсов с помощью глобально признанного CERT

Масштабная база преступных групп и индивидов с автоматическим построением связей между преступниками и анализом социальных графов

## СИСТЕМА РАННЕГО ПРЕДУПРЕЖДЕНИЯ КИБЕРУГРОЗ

### Threat Intelligence

Мониторинг, анализ и прогнозирование киберугроз

### TDS / TDS Polygon

Обнаружение целевых атак и выявление ранее неизвестного вредоносного кода

### Secure Bank / Secure Portal

Выявление хищений и мошенничеств на этапе подготовки

Настоящим Group-IB информирует о том, что:

- Настоящий отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
- Оценка рынка высокотехнологичных преступлений проводилась на основании собственной методики Group-IB.
- Описание технических деталей угроз в настоящем 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 настоящем отчете технические детали угроз ни в коем случае не являются пропагандой мошенничеств и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
- Все упоминания компаний и торговых марок в настоящем отчете сделаны на основании полученных от таких компаний разрешений и/или на основании уже опубликованных в средствах массовой информации сведениях.
- Сведения, опубликованные в настоящем отчете, могут быть использованы заинтересованными лицами по своему усмотрению при условии указания ссылки на Group-IB.



---

**УЗНАЙТЕ БОЛЬШЕ О GROUP-IB**

[Group-IB.ru](http://Group-IB.ru)

---

**СВЯЖИТЕСЬ С НАМИ**

+7 495 984-33-64

[info@group-ib.ru](mailto:info@group-ib.ru)

---

**БУДЬТЕ В КУРСЕ НОВОСТЕЙ**

[facebook.com/GroupIB](https://facebook.com/GroupIB)

[youtube.com/GroupIB](https://youtube.com/GroupIB)

[twitter.com/GroupIB](https://twitter.com/GroupIB)

[instagram.com/Group\\_IB](https://instagram.com/Group_IB)