HIGH-TECH CRIME TRENDS 2016
ТЕНДЕНЦИИ РАЗВИТИЯ ВЫСОКОТЕХНОЛОГИЧНЫХ ПРЕСТУПЛЕНИЙ 2016

2015 Q2 – 2016 Q1

КЛЮЧЕВЫЕ ВЫВОДЫ

Хищения

Оценка российского рынка хищений денежных средств посредством высокотехнологичных атак

2015 Q2 – 2016 Q1, данные Group-IB

	Кол-во групп	Успешных атак в день	Средняя сумма хищения	Средний объем хищений в день, ₽	Объем хищений, ₽	Объем хищений, $ (средний курс – 70 руб. за доллар)	% 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 помощью троянов для ПК	1	0,5	51 600 ₽	25 800 ₽	6 424 200 ₽	$112,705	-83%
Хищения у физических лиц с помощью Android-троянов	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%
ИТОГО				**5 265 800 ₽**	**5 526 217 090 ₽**	**$96,951,177**	**44%**

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 (Anunak), 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 Buhtrap). 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.

—

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

—

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

Хищения денежных средств 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. 16 из 19 троянов для ПК, наиболее активно использующихся для хищений по всему миру, связаны с русскоязычными преступниками.

Объем хищений у юридических лиц с использованием троянов для ПК (Россия)
956 160 000 ₽
-50%

Хакеры делают ставку на автоматизацию хищений:

- Все новые трояны для хищений у юридических лиц, появившиеся в России за отчетный период, поддерживают веб-инжекты, 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.

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.

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.

Объем хищений денежных средств у физических лиц с использованием Android-троянов (Россия)
348 600 000 ₽
+471%

Объем хищений у физических лиц с использованием троянов для ПК (Россия)
6 424 200 ₽
-83%

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.
- **Появились веб-инжекты под мобильные браузеры.** Этот функционал есть, например, в новой версии одного из наиболее активно используемых для хищений по всему миру Android-троянов Marcher. Веб-инжекты позволят атаковать пользователей любых систем интернет-банкинга и реализовывать все схемы, которые раньше были доступны только на компьютерах, включая автозалив.
- **Преступники начали защищать сетевое взаимодействие между C&C-сервером и устройством**, что усложняет обнаружение трояна, и проводить заражения в несколько этапов, устанавливая основной модуль только на устройства с

подходящими параметрами: например, с доступом к интересующей системе мобильного банкинга.

Веб-инжекты дают возможность манипулировать отображением страниц в браузере, например, добавлять новые пункты в форме авторизации интернет-банкинга или скрывать мошеннические операции в истории платежей.

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-трояны совмещают инструменты для шпионажа и хищений. Так, практически все мобильные трояны 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.

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

Атаки на промышленные компании и объекты критической инфраструктуры

Сложились предпосылки 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. Иногда программы-вымогатели ставят средства удаленного управления автоматически.

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.

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 бренда, 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 ₽ ($23 тыс).

ПРОГНОЗЫ

Успешные целевые атаки на банки продолжат победное шествие по миру.

- Профессиональные преступные группы, занимавшиеся атаками на юридических лиц, будут переориентироваться на банки. Наибольший потенциал для начала атак на банки в России – у групп Toplel и RTM.
- 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 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.
- Некоторые бот-сети будут коммерциализироваться за счет продажи доступа в сети интересующих компаний. В последствии эти бот-сети будут проданы менее опытным хакерам.

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

- Эксплойты для их распространения станут включаться в стандартные наборы эксплойтов, доступных на хакерском рынке.
- Распространение веб-инжектов 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-инжектов.
- По мере освоения системами корпоративного дистанционного банковского обслуживания мобильных платформ Android-трояны начнут атаковать юридических лиц с целью хищений денежных средств.

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 и в мошеннических схемах, например, для перенаправления на фишинговые сайты, демонстрации рекламы с предложением скачать трояны, серверами эксплойтов и др.

Инцидентов с программами-шифровальщиками станет больше.

- Атаки на компании будут более качественно таргетированы, что приведет к повышению средней суммы выкупа.
- Программы-вымогатели станут более направленными на специфичные корпоративные секторы (например, колл-центры, аутсорсинговые бухгалтерские компании в день 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 активного выхода шифровальщиков на мобильные устройства стимулирует развитие сегмента страхования киберрисков. Страхование приведет к увеличению случаев, когда жертва будет платить атакующему, что будет еще больше будет стимулировать атакующих, а это в свою очередь еще больше стимулировать рынок страхования.

Количество атак на промышленные объекты будет расти, высока вероятность атаки на объект критической инфраструктуры со значительным ущербом (вплоть до человеческих жертв).

- Киберармии разных стран продолжат атаковать объекты критической инфраструктуры как для шпионажа, так и для того, чтобы иметь контроль над ними и иметь возможность воспользоваться им в нужный момент.
- Для сокрытия причастности государственных киберармий будут активно вербоваться хакеры с опытом проведения целенаправленных атак на корпоративный сегмент. Эти 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 активно рекрутировать хакеров, способных проводить целевые атаки.
- Прежде всего атакующих будут интересовать энергетические компании, аэропорты, химические производства, водоочистительные узлы, органы управления транспортом, магистральные сети и т.п. Тактика атак на все эти типы предприятий будет очень схожей.

Растущее предложение решений для атак на SSL и перехвата трафика, а также расширение функционала для шпионажа у мобильных троянов неизбежно приведет к росту числа атак с целью шпионажа.

Преступники продолжат 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.