ПАНДОРИНО ГОРЕ И ЧЕРНЫЙ ЯЩИК

Одним из столпов защиты от кибершпионажа и сетевых угроз является адекватная оценка ландшафта угроз для конкретного банка или финансовой компании, поскольку атаки становятся персонализированными



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Как утверждают аналитики портала Antimalware.ru, за последние два года (на начало 2025-го) отечественный рынок кибербразведки, включая такие его компоненты, как Threat Intelligence (TI), OSINT и прочие, вырос примерно в два раза. С другой стороны, уже со стороны хакеров, в первом полугодии 2025 года почти 39% всех вредоносных действий в интернете были связаны с кибербразведкой, например сбором данных об уязвимостях веб-приложений. По сравнению с аналогичным периодом прошлого года доля таких атак выросла более чем в пять раз — с 6,8 до 38,7%.

Ожидается, что в мировом масштабе отрасль Threat Intelligence вырастет с 14,9 млрд долларов в 2024 году до 36,6 млрд к 2034 -му, увеличиваясь в среднем в год на 9,4%. Отечественный рынок Threat Intelligence можно считать уже сформировавшимся и практически импортонезависимым, однако его сегмент финансовой отрасли вследствие изменений законодательства в области КИИ вступает в стадию кардинальных перемен: очевидно, будут создаваться отраслевой центр кибербразведки, а также специализированные сценарии реагирования на целевые (персонализированные) атаки (APT) как в сфере классических финансов, так и в области цифровых активов.

Почему это так? Во-первых, технические средства ИБ-защиты не могут закрыть собою все 100% поверхности атаки. Во-вторых,

требуется непрерывный R&D в новинки, что порой неэффективно с экономической точки зрения. Гораздо проще с помощью киберразведки получить контекст атаки, проанализировать цели и методы работы кибергруппировок, подобрать адекватные средства защиты, а главное, заранее наработать алгоритмы и практики противодействия. В-третьих, в рядах нападающих и защищающихся появился ИИ, что «перевернуло доску» былых трендов в распределении доли различных решений внутри ИБ-рыка в пользу TI, а в хакерской среде — в сторону мощной эволюции разработки и проведения APT-атак. Все это привело к новому прочтению бизнесом известного тезиса: «Предупрежден — значит вооружен!».

Приключения итальянцев в России

Из аналитиков «Б.О» наиболее кратко и емко итоги 2025 года с точки зрения оценки актуальных ИБ-угроз подвел **Сергей Демидов,** ИБ-директор Мосбиржи, в своем декабрьском интервью изданию CNews. В частности, эксперт заявил: «Мы видим, что случаев сканирования и попыток атаковать IT-инфраструктуру стало на 30% меньше по сравнению с предыдущим годом. Однако атаки эволюционируют. В своих отчетах ИБ-аналитики пишут, что тактики продвинутых хакерских группировок сильно изменились. Скорее всего, они спонсируются недружественными по отношению к России государствами. Им дают цели и деньги. Поэтому после анализа каждого отчета мы проводим учения на своей инфраструктуре».

Схожей точки зрения придерживаются в компании «Информзащита». По данным ее специалистов, «в 2025 году число успешных атак на финансовый сектор составило 1,07 тыс., что на 12% меньше по сравнению с прошлым годом и более чем в три раза меньше, чем в 2022 году. Доля успешных атак снизилась до 7%, что стало минимумом за четыре года».

Эксперты компании отметили, что при этом сценарии атак усложнились, увеличилось количество точечных атак, требующих больше ресурсов и приводящих к серьезным последствиям. Злоумышленники применяют менее агрессивные, но более эффективные методы, включая фишинг и перебор учетных записей с использованием данных о клиентах. В 2026 году ожидается дальнейшее усложнение атак, включая использование ИИ.

О каком именно усложнении атак говорят ИБ-эксперты? В чем это выражается и где искать следы недружественных стран? Почему все чаще приходится иметь дело с кибершпионажем? За примерами эволюции кибератак далеко ходить не надо.

По данным специализированного портала Securelist by Kaspersky, в марте 2025 года «Лаборатория Касперского» (ЛК) выявила волну заражений, происходивших сразу после того, как жертва открывала персонализированную фишинговую ссылку, полученную по электронной почте. Единственным действием, которое требовалось от пользователя, было открытие ссылки. Все используемые ссылки были персональными и действовали крайне ограниченное время. Однако специалисты ЛК смогли выявить сложный эксплойт Dante, применявшийся для обхода защитных механизмов браузера Chrome и не только. Основной функциональностью этого вредоносного ПО является кибершпионаж. Саму же атаку с помощью фишинговых писем под видом приглашений на научно-экспертный форум «Примаковские чтения» аналитики ЛК навали «Форумный тролль».

Дальше — больше! Анализ активности шпионского ПО с 2022 года выявил другие атаки той же группы на банки, организации и частных лиц в России и Беларуси. Выяснилось, что использовалось коммерческое шпионское ПО Dante, разработанное итальянской компанией Memento Labs, ранее известной как Hacking Team.

Hacking Team — один из старейших и самых известных поставщиков шпионского ПО. Компания была основана в 2003 году и стала известна благодаря софту Remote Control Systems (RCS), которым пользовались государственные органы по всему миру. Известна компания и крупной утечкой внутренних документов в 2015 году, что привело к тому, что в 2019-м компания InTheCyber Group приобрела ее и переименовала в Memento Labs.

Спустя четыре года на конференции правоохранительных органов и служб разведки ISS World MEA 2023 компания раскрыла название своего флагманского шпионского продукта — Dante, отодвинув в тень свой предыдущий «хит», печально известный в узком кругу пострадавших, — Da Vinci. При этом до сих пор мало что было известно о возможностях этого ПО, и никто не встречал его в реальных атаках, но последние три года банки России и Беларуси находятся под прицелом итальянского Dante.

Все детали этого исследования, в также информация о хакерской группе ForumTroll и шпионском ПО Dante доступны на сервисе по предоставлению актуальных данных об APT-угрозах Securelist на Threat Intelligence Portal.

Совпадение это или нет, но 24 декабря 2025 года МТС Банк сообщил в пресс-релизе о том, что усилил киберзащиту своей IT-инфраструктуры благодаря внедрению российского решения Threat Intelligence от компании BI.ZONE, которое позволяет банку оперативно получать киберразведданные и актуальную информацию о динамике ландшафта киберугроз в банковском секторе. В этом пресс-релизе приведена довольно любопытная оценка **Олега Скулкина,** руководителя BI.ZONE Threat Intelligence, раскрывающая масштаб проблемы APT-атак и кибершпионажа: «По нашим данным, сейчас на российскую финансовую отрасль нацелены более 60 хакерских группировок, и у каждой из них — свой уникальный почерк».

Почерк «профессионалов»

О чем могут поведать своим владельцам системы Threat Intelligence из того, что необходимо знать любому банкиру? Например, о том, что в текущей геополитической обстановке время андеграунд-одиночек давно прошло. На «том конце интернет-кабеля» находятся такие силы, последствия действий которых могут значительно превысить ущерб от экономии на инвестициях в кибербезопасность. Какие же это силы?

В конце октября 2025 года бизнес-консультант по ИБ компании Positive Technologies **Алексей Лукацкий** написал у себя в теле-

грам-канале: «**Питер Вильямс**, бывший руководитель подразделения кибербезопасности Trenchant компании L3Harris Technologies, специализировавшейся на инструментах хакерского и разведывательного профиля, обвинен правительством США в краже коммерческих и технологических секретов».

Как мы знаем из лекций не менее известного отечественного специалиста в области OSINT и «мастера искусства слежки в даркнете» **Андрея Масаловича** (известного в интернете под ником КиберДед и находящегося с 2023 года под санкциями правительства США за «продажу инструмента для слежки на основе больших данных Avalanche спецслужбам»), нет ничего более информативного для исследователей, нежели детали судебных разбирательств.

Неудивительно, что Алексею Лукацкому не составило особого труда изучить обвинительный документ и выяснить, что примерно с апреля 2022 года по июнь-август 2025-го Питер Вильямс похитил 15 секретных технологических продуктов либо решений у двух компаний, которые занимались разработкой уязвимостей класса Zero Day и продажей их спецслужбам альянса «Пяти глаз», которые в 2018 году были куплены L3Harris. Целью похищения, как утверждают американские прокуроры и Алексей Лукацкий, было дальнейшее их предоставление покупателю, расположенному в Российской Федерации. Сумма, которую он якобы получил от сделки, составляет около 1,3 млн долларов США.

В телеграм-канале Russian OSINT появился еще один показательный пост: «В начале ноября 2025 года произошла масштабная утечка данных из китайской компании Knownsec, крупного игрока на рынке кибербезопасности. Содержимое утечки включает в себя техническую документацию на кибероружие, исходные коды внутренних хакерских инструментов и списки глобальных целей, охватывающие более двадцати стран». Арсенал Knownsec, как известно, содержит сложный набор троянов для удаленного доступа, предназначенных для компрометации различных операционных систем. Особого внимания заслуживает вредоносное ПО для Android, способное извлекать историю переписки из защищенных мессенджеров.

Но если доля кибератак на банки снижается, то на какие сектора переориентируются хакеры? Свою версию ответа дали специалисты отечественной ИБ-компании F6, которые раскрыли детали атак с 2014 года в России и Беларуси группировки Cloud Atlas — прогосударственной APT-группы, специализирующейся на кибершпионаже и краже конфиденциальных данных. Изощренные высокие технологии, используемые хакерами, не оставляют сомнений в обильном ее финансировании, однако принадлежность группировки к какой-то конкретной стране в F6 не указывают.

Особенность недавних атак Cloud Atlas (теперь на предприятия агропромышленного сектора, а ранее — на госструктуры, ВПК и финансы) заключается в изменении тактики и экспериментировании с инфраструктурой, а также с методами доставки ПО. Группировка начала использовать нетипичные доменные зоны и изменила схему их применения.

Не остался без внимания хакеров и сектор Web 3.0, на технологиях которого основаны многие DeFi-сервисы. В конце октября 2025 года «Лаборатория Касперского» выпустила объемный отчет в отношении двух кампаний северокорейской APT BlueNoroff, которые получили названия GhostCall и GhostHire. Хакеры нацелились на разработчиков, которых обманным путем побуждают загрузить и запустить репозиторий GitHub, содержащий вредоносное ПО, под видом оценки навыков в процессе найма в сегменте Web 3.0.

Аналитики ЛК сделали следующий вывод: «Стратегия весьма качественного таргетинга злоумышленников вышла за рамки простой кражи учетных данных для доступа к криптовалюте и браузеру ее владельцев. Получив доступ, они собирают данные о различных активах, включая инфраструктуру, инструменты для совместной работы, приложения для ведения заметок, среды разработки и коммуникационные платформы (мессенджеры). Собранные данные используются не только для первоначальной цели, но и для последующих атак, что позволяет злоумышленникам проводить атаки на цепочки поставок».

Кто «льет трафик на дрейнеров»?

В начале данного обзора было приведено мнение Сергея Демидова из Московской биржи о том, что «атаки непрерывно эволюционируют». К сожалению, это действительно так, причем данный процесс идет параллельно с эволюций банковского мира, например с интеграцией классических финансовых инструментов в цифровые финансовые активы на базе блокчейна, к примеру криптовалюты.

Долгое время считалось, что «крипта» и ее производные неуязвимы по отношению к попыткам взлома блокчейна как IT-системы. Все иллюзии в ходе 3-й Практической конференции «ЦФА: инвестиции нового поколения», которую медиапроект «Банковское обозрение» провел 27 июня 2024 года в Москве, развеял тот же Андрей Масалович. Он красочно и живописно рассказал в своей презентации, «как именно будут ломать» операторов информационных систем (ОИС) и их клиентов» с помощью HUMINT, разновидности OSINT. По его словам, близко́ то время, когда хакеры начнут «взламывать» людей, эксплуатируя при этом, по сути, исключительно «гордыню» как ключ к уязвимостям мозга. В частности, был приведен пример неудачной «фотосессии» **Джеймса Чжуна**, хакера, который около десяти лет назад похитил 50 тыс. биткоинов. Полиция конфисковала эту сумму, которая стала второй по величине в истории такого рода хищений. Еще один пример связан с использованием ИИ для кражи 35 млн долларов из одного известного банка.

Коллеги «КиберДеда» из «Лаборатории Касперского» с прискорбием расширили список проблем с криптовалютами, однако, в отличие криминала, использующего OSINT, они применили технологию Kaspersky Digital Footprint Intelligence, что называется, «в мирных целях», изучая Darknet. И открылся ящик Пандоры…

Одно из значений термина «дрейнер» (drainer) — это тип вредоносного ПО, появившийся в начале 2020-х годов и предназначенный для обмана владельцев крипотокошельков в целях получения их

добровольного согласия на мошеннические транзакции и в итоге на кражу их крипотовалюты. Наиболее частыми в 2024 году методами распространения этого ПО, по данным аналитиков ЛК, были фальшивые аирдропы (airdrops) для раздачи фейковых токенов, фишинговые сайты, вредоносные расширения для браузера, демонстрировавшие людям такую же фейковую рекламу, поддельные торговые NFT-площадки, а также вредоносные смарт-контракты.

Специалисты по Footprint Intelligence зафиксировали взрывной рост интереса криптоандеграунда к этой теме: количество активных тематических сообществ в «теневом интернете» выросло с 55 до 129 (+135%) за период с 2022 по 2024 год.

Косвенным показателем роста интереса к данной теме стало «затоваривание» криминального рынка персональных данных (ПДн), о котором в рамках форума PHDays 2025 в докладе «Теневая экономика данных» доложил аудитории Алексей Лукацкий. С практической точки зрения это означает ликвидацию хакерами неликвида и массовый бесплатный слив на рынок баз данных ПДн. Возможно, свою роль сыграло ужесточение законодательства, а может быть, у криминала нашлось занятие поприбыльнее и менее рискованное.

Одной из первых атак дрейнеров стала кража 14 Bored Ape NFT общей стоимостью более 1 млн долларов, произошедшая 17 декабря 2022 года, центральным элементом которой была вовремя подсунутая жертве на подписание транзакция, передававшая криптоактивы в собственность мошенников. За 2023 год от дрейнеров пострадало более 320 тыс. пользователей, а суммарный ущерб составил около 300 млн долларов. Среди зарегистрированных Footprint Intelligence сервисами мошеннических транзакций более десятка превышали 1 млн долларов.

В 2024 году суммарный ущерб только от drainer-фишинга составил около 494 млн долларов и 332 тыс. пострадавших адресов (+ 67% год к году). Крупнейшая разовая кража превысила 55 млн, а рынок «drainer-as-a-service» пережил смену «лидеров» (с Pink на Inferno и Angel) и эволюцию техник. В 2025-м появился новый дрейнер-вектор — подмена результатов симуляции транзакции в кошельках.

Кроме того, к началу 2025 года сформировался тренд миграции значительной части дрейнеров в TON, где быстро росла розничная аудитория из-за мини-игр и ботов в Telegram. Новички часто «подписывают, не считая», а фишинговые шорт-линки и боты подменяют домены и запросы. Тогда же у ИБ-специалистов появился термин «лить трафик на дрейнеров», чем занялись воротилы теневого арбитража интернет-трафика.

А вот по итогам 2025 года, как утверждают киберразведчики платформы безопасности Web3 Scam Sniffer, потери от криптофишинговых атак, связанных с утечкой средств из кошельков, снизились на 83% по сравнению с 2024 годом — до 83,85 млн долларов. Количество жертв также сократилось — до 106 тыс., что на 68% меньше, чем в предыдущем году. Это значит, что помимо симуляции транзакций авторы дрейнеров нашли новую «вкусную» нишу — объединение нескольких зловредный действий в одну «легитимную» подпись пользователя. Обычно это делалось с использованием обновления EIP-7702, которое может временно превратить обычные криптокошельки в смарт-контракты, после чего «всего одна подпись может снести весь баланс». Проще говоря, найдена возможность делегирования пользователем своего EOA-адреса смарт-контракту. А вот настоящий он или фейковый? Подписав транзакцию — узнаете!

Завершая блок Threat Intelligence в цифровых активах, нельзя не упомянуть о кейсе от 10 июля 2025 года, когда в ЛК обратился российский блокчейн-разработчик, у которого злоумышленникам удалось похитить криптовалюту на сумму около 500 тыс. долларов с использованием вредоносных программ и скомпрометированных open-source-пакетов для кражи криптоактивов. Обо всем остальном, как мы надеемся, эксперты из «Глобального центра исследования и анализа угроз Kaspersky GReAT» расскажут в свое время сами!

Что в итоге?

Использование TI в банковской системе регулируется соответствующими документами Банка России, например ГОСТ Р 57580.3-2022 — стандартом, определяющим требования к составу и содержанию мер по управлению риском реализации информационных угроз для финансовых организаций.

Стандарт определяет TI как процесс сбора, обработки и анализа информации о потенциальных ИБ-угрозах финансовым организациям. Это включает в себя идентификацию уязвимых мест, мониторинг активности злоумышленников и создание рекомендаций по снижению рисков.

Есть и целый спектр отечественный решений. Но, по данным специалистов компании «Ангара», сейчас в качестве базовых TI-платформ организаций довольно широко распространены open-source-решения типа MISP и OpenCTI, однако на практике есть ограничения. К примеру, MISP в типовой конфигурации начинает «задыхаться», когда поток индикаторов в сутки превышает 50–100 тыс. штук, а OpenCTI достаточно ресурсоемка. Кроме того, ни MISP, ни OpenCTI не являются отечественными продуктами, не сертифицированы в России и не входят в реестр ПО Минцифры, что для субъектов КИИ критически важно. Далее эксперты подробно приводят все плюсы и минусы девяти отечественных TI-решений. Идеала среди них, увы, пока нет.

Для чего все это сделано? С 1 марта 2026 года вступают в силу положения № 325-ФЗ от 31 июля 2025 года, которые уточняют порядок использования отечественного ПО для КИИ и госструктур. Теперь недостаточно включения продукта в реестр ПО Минцифры: для ряда задач обязательным станет наличие в специальных перечнях доверенного или отраслевого ПО, формируемых правительством.

Очевидно, что Банк России самым активным образом участвует в данных работах, возможно, будет добавлено нечто и в его ГОСТ 57580* и что-то в области интеграции с будущей доверенной платформой для обмена данными. А некоторые эксперты замахиваются даже на создание межведомственной интеллектуальной платформы киберразведки для защиты объектов КИИ. В любом случае, работы в данной сфере будет немало! Б.О