

kaspersky



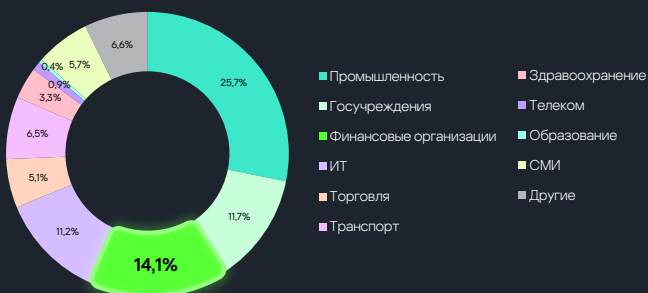
Осень 2025

Киберпульс. Финансы.

Россия.

Ключевая статистика киберугроз для финансовой отрасли в России

Распределение инцидентов по отраслям*



Количество кибератак на финансовые организации в России, H1 2025 vs H1 2024**



+13%

Данные по основным типам угроз для финансового сектора в России, H1 2025 vs H1 2024

+81%

рост количества атак с **различных онлайн-ресурсов** на финансовые организации**

-63%

снижение количества атак с помощью **бэкдоров** на финансовые организации**

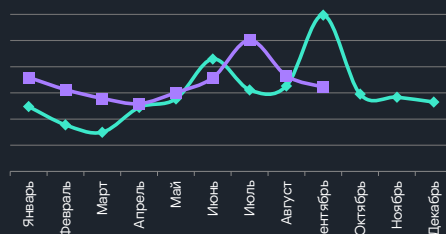
x 2,4

рост количества атак с помощью **банкеров** (ВПО для кражи денежных средств через онлайн доступ к банковским счетам)**

+6%

рост количества атак на финансовые организации с помощью **программ-вымогателей** (ransomware)**

Сезонность атак с использованием шифровальщиков на финансовые организации в России***



Традиционный всплеск атак на стыке Q3-Q4

Наиболее распространённые программы-вымогатели у группировок, атакующих финансовый сектор России в 2025 году***



Proton



Babuk

Группировки, атакующие российский финансовый сектор в 2025 году



Angry Likho



GOFEE



Lazarus



Horned Ghouls



TWELVE



Crypt Ghouls



Hive0117



BlueNoroff



OldGremlin



Carbanak

Наиболее активно атакуют российские организации группировки, позиционирующие себя как проукраинские. Подробнее прочитать про их тактики, техники и процедуры можно в отчете «[Записки цифрового ревизора: три кластера угроз в киберпространстве](#)», сентябрь 2025 г.

* По данным отчета Kaspersky Managed Detection and Response
** По данным Kaspersky Global Research and Analysis Team (GReAT)
*** По данным Kaspersky Cyber Threat Intelligence Team

Главные сигналы для кибербезопасности финансовой отрасли



Активность шифровальщиков

Программы-вымогатели и их разновидности – главная угроза. Более 40% атак на отрасль связаны с их использованием.



Тёмная сторона ИИ

Начало масштабного использования технологий ИИ в подготовке и организации атак: от написания кода до инструментов распространения и внедрения в инфраструктуру.



Усложнение тактик и техник

Смещение угроз в финансовом секторе России в сторону целевых атак с использованием изощрённых инструментов и схем. Например, компрометация цепочек поставок (ИТ-поставщиков) – один из самых частых способов получения первоначального доступа к финансовым организациям страны.

Актуальные угрозы для финансовой сферы в III квартале 2025 года



GodRAT – троянец удалённого доступа

Троянец распространяется через вредоносные файлы с расширением .scr, замаскированные под финансовые документы. После заражения троянец собирает сведения об инфраструктуре и учётные записи пользователей. Атакующие пытаются скрыть активность и обойти защитные решения: зашивают во вредоносный архив инструмент для быстрой сборки GodRAT, который позволяет выбрать, в какой легитимный файл внедрить вредоносную нагрузку, и используют стеганографию, чтобы спрятать шелл-код в файле изображения с якобы финансовыми данными.

[Подробнее](#)

Шифровальщик на ИИ

Эксперты Kaspersky GReAT изучили активность кибергруппы FunkSec. Их вредоносное ПО отличается сложная техническая архитектура и использование ИИ. Разработчики зловреда включили возможность полномасштабного шифрования и кражи данных в один исполняемый файл, написанный на Rust. Он способен отключать более 50 процессов на устройствах жертв и оснащён функциями самоочистки. Вместе с шифровальщиком идут и другие инструменты – генератор паролей и инструмент для DDoS-атак. Во всех случаях есть явные признаки синтеза кода с использованием больших языковых моделей (LLM). Кроме того, похоже, что многие фрагменты кода написаны автоматически.

[Подробнее](#)



Cobalt Strike Beacon – удаленное управление устройствами и кража денег

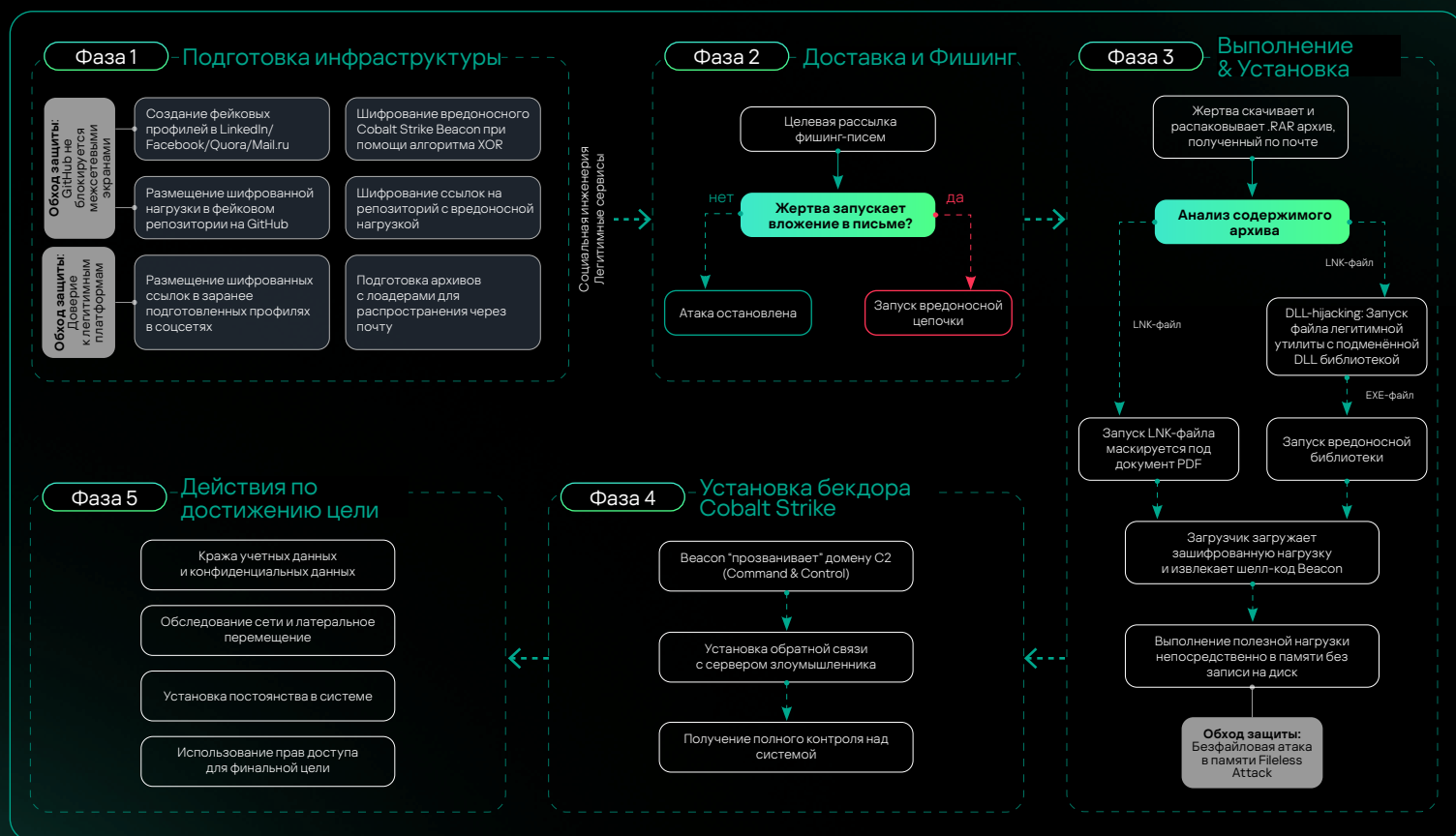
Обнаружены новые случаи кибератак на российские организации с использованием **Cobalt Strike Beacon**. Сначала злоумышленники рассылают таргетированные фишинговые письма с вредоносным вложением. Чтобы запустить зловред, атакующие используют метод подмены DLL (Dynamic Link Library) и также легитимную утилиту для отправки отчетов о сбоях. В результате манипуляций она открывает вредоносный файл вместо легитимного.

Для дальнейшего функционирования вредоносное ПО извлекает и загружает код, который хранится в зашифрованном виде в публичных профилях на популярных легитимных платформах. После выполнения вредоносного кода на устройствах жертв запускается Cobalt Strike Beacon – и системы оказываются скомпрометированы.



Подробнее

Подробнее об атаках с использованием DLL Hijacking и защите от них



Недозакрытая уязвимость в Microsoft SharePoint

Эксплойт **ToolShell**, использованный в массовых атаках на серверы Microsoft SharePoint, оказался очень похож на эксплойт для другой уязвимости, обнаруженной ещё в 2020 году. Это позволяет предположить, что уязвимость пятилетней давности, вероятно, была не до конца закрыта ещё тогда. Попытки эксплуатации свежей уязвимости в SharePoint фиксировались в самых разных сферах, включая финансовый и госсектор, промышленность, а также лесное и сельское хозяйство. Защитные решения «Лаборатории Касперского» – Kaspersky NGFW и Kaspersky Symphony XDR – детектировали и блокировали попытки эксплуатации уязвимостей в SharePoint ещё до публикаций Microsoft.

Подробнее

\$500k долларов – стоимость установки заражённого пакета с открытым исходным кодом

Злоумышленники похитили у российского блокчейн-разработчика криптовалюту на сумму около 500 тысяч долларов. Пользователь установил на свой ПК заражённый пакет с открытым исходным кодом, который мимикрировал под расширение для Cursor AI (среды разработки с поддержкой ИИ). Вместо желаемой функциональности на компьютер проникла вредоносная сборка ПО ScreenConnect, что позволило получить удалённый доступ к устройству. Затем она заразила устройство бэкдором Quasar и стилером, который собирает данные из браузеров, почтовых клиентов и криптокошельков. Таким образом атакующие получили доступ к криптокошелькам и вывели с них криптовалюту.



[Подробнее](#)

Новый уровень таргетированного корпоративного фишинга

Злоумышленники рассылают сотрудникам организаций персонализированные письма под видом инструкций от отдела кадров. Особенность кампании в том, что индивидуализируют в ней не только тексты писем, но и вложения. В обнаруженных рассылках к получателю обращаются по имени как в самом письме, так и во вложенном файле. Документ во вложении якобы содержит информацию о протоколах удалённой работы, стандартах безопасности и доступных льготах. В реальности во вложенном файле находится QR-код якобы для перехода на полную версию инструкции. На самом деле ссылка в QR ведёт на поддельную страницу, имитирующую форму авторизации в сервисах Microsoft, где пользователя просят ввести логин и пароль от корпоративной почты.

[Подробнее](#)

«Эфемерный» троянец

Летом 2025 года зафиксирован всплеск атак с использованием троянца **Efimer**, в том числе на корпоративных пользователей. Зловред распространяется через взломанные WordPress-сайты, вредоносные торренты и электронную почту. Он может подбирать пароли к сайтам и собирать базы электронных адресов для дальнейшей рассылки вредоносных писем. В фишинговых письмах говорится, что юристы некой корпорации заметили, что в названии домена, принадлежащего адресату, есть слова или фразы, якобы уже зарегистрированные этой организацией. По их словам, они не будут подавать в суд, если получатель письма сменит название домена, и даже готовы выкупить его. Детали претензии якобы можно посмотреть во вложении — к письму прикреплен запароленный архив с вредоносным файлом.



[Подробнее](#)

Рекомендации ИБ-командам финансовых организаций



Дмитрий Галов

Руководитель Kaspersky GReAT в России



О Kaspersky GReAT

Глобальный центр исследования и анализа угроз Kaspersky GReAT основан в 2008 году. В его задачи входит поиск и исследование наиболее сложных атак, кампаний кибершпионажа, новых методов заражения, эксплойтов, использующих уязвимости нулевого дня. Сегодня в команде центра более 30 экспертов, работающих по всему миру в Европе, России, Южной Америке, Азии, на Ближнем Востоке. Они известны своими достижениями в расследовании наиболее сложных атак, включая кампании кибершпионажа и киберсаботажа.



Контроль приложений и загрузчиков: запретить использование нестандартизированных установщиков, особенно open-source без цифровой подписи, внедрить Application Whitelisting



Мониторинг и защита реестра и автозагрузки: настроить SIEM и политики безопасности для обнаружения подозрительных изменений в реестре автозагрузки, блокировать несанкционированные скрипты входа в систему, отслеживать активности в планировщике задач



Обнаружение и реагирование на фишинг и поведение C2: использовать TLS/SSL инспекцию в пределах корпоративной сети для выявления подозрительных C2-коммуникаций с взаимной аутентификацией, настроить IDS/IPS и DNS-фильтрацию для выявления и блокировки фишинговых страниц и доменов командных серверов



Провести **актуальный тренинг по фишингу** для офисных сотрудников



Пересмотреть контракты с ИТ-поставщиками — ввести требования по ИБ



Обеспечить постоянный **мониторинг активности DLL Sideloadng**, запусков из пользовательских директорий и необычных скриптов NodeJS



Усиление защиты конечных точек (Endpoint Protection) с помощью продвинутых технологий EDR/XDR-решений с поведенческим анализом



В рамках стратегии защиты сосредоточиться на **обнаружении горизонтального перемещения**, а также утечек данных. Уделить внимание исходящему трафику, чтобы своевременно выявить подключение злоумышленников ко внутренней сети



Предоставлять SOC-командам **доступ к информации о новейших тактиках, техниках и процедурах злоумышленников**

Взгляд вперёд: на что обратить внимание уже сейчас



Рост атак на цепочку поставок в проектах с открытым исходным кодом



«Нормативный» шантаж в атаках шифровальщиков



Новые угрозы на основе блокчейна



Рост числа финансовых кибератак через смартфоны



Больше искусственного интеллекта и машинного обучения в системах безопасности