2025

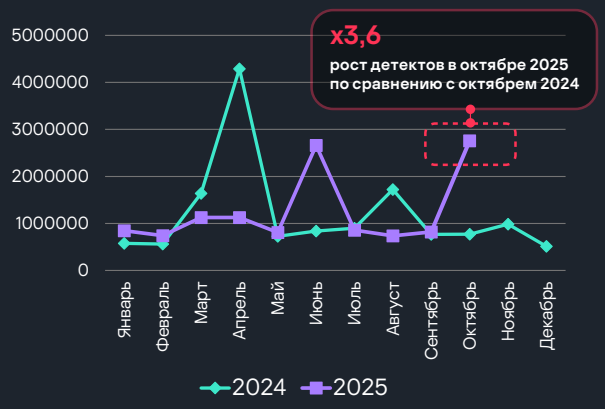
Почтовые киберугрозы для бизнеса

Россия

kaspersky

Ключевая статистика почтовых киберугроз для бизнеса в России

Динамика количества детектов писем с вредоносным ПО **в организациях** по месяцам, 10 мес. 2024 vs 10 мес. 2025*



81% российских организаций столкнулись с почтовыми киберугрозами в 2025 году

Отрасли российской экономики с наибольшим % компаний, которые подверглись почтовым кибератакам за 9 месяцев 2025 г. *

Телеком	86%	Государственные учреждения	78%
Промышленное производство	85%	Строительство	78%
Энергетика	84%	ИТ	75%
Ритейл	84%		
Финансы	83%		
Образование	81%		
Транспорт	81%		

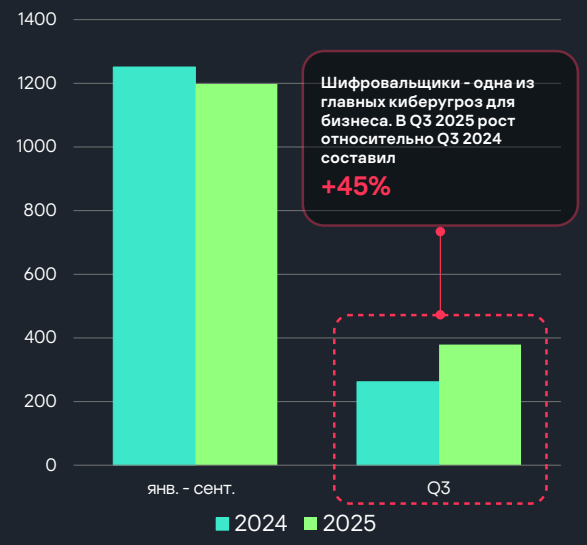
В последние несколько лет трендом стали беспрецедентные всплески атак на отели по всему миру в том числе, в России

Регионы РФ по количеству детектов писем с вредоносным ПО за первые 9 мес. 2025*

1. Москва и Московская область
2. Санкт-Петербург и Ленинградская область
3. Свердловская область
4. Краснодарский край
5. Челябинская область

+42% рост количества почтовых кибератак на бизнес в Вологодской области, по сравнению с 9 мес. 2024

Количество детектов программ-шифровальщиков (ransomeware) в почте российских организаций, 2024 vs 2025**



Наиболее частые типы вредоносного ПО в корпоративной почте российских организаций за 9 мес. 2025

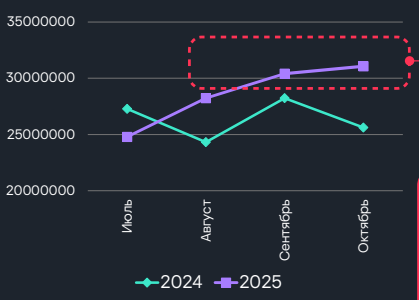
доля пользователей, столкнувшихся с данной угрозой, от общего числа пользователей, столкнувшихся с каким-либо вредоносным ПО в почте*

10 самых распространенных видов угроз в почте российских организаций

Trojan	96%	Virus	27%
Hoax	87%	Trojan-Ransom	19%
Trojan-Spy	76%		
Backdoor	72%		
Trojan-PSW	71%		
Trojan-Downloader	68%		
Exploit	62%		
Trojan-Dropper	50%		

Trojan-Spy — вредоносная программа, предназначенная для ведение электронного шпионажа за пользователем (вводимая с клавиатуры информация, снимки экрана, список активных приложений и т.д.). Для передачи данных злоумышленнику могут быть использованы электронная почта, FTP, HTTP и др.

Количество спама в корпоративной почте российских организаций и % от общего количества писем



44% средний показатель спама в почте российских организаций за 10 мес. 2025

* Данные Kaspersky Global Research and Analysis Team (GReAT)
** Данные команды Kaspersky Cyberthreat Intelligence (CTI)

Главные сигналы для кибербезопасности корпоративной почты

Активное применение искусственного интеллекта

Злоумышленники применяют технологии ИИ на всех этапах атак: в частности, языковые модели помогают в короткое время генерировать большое количество текстов под разные аудитории для вредоносных рассылок

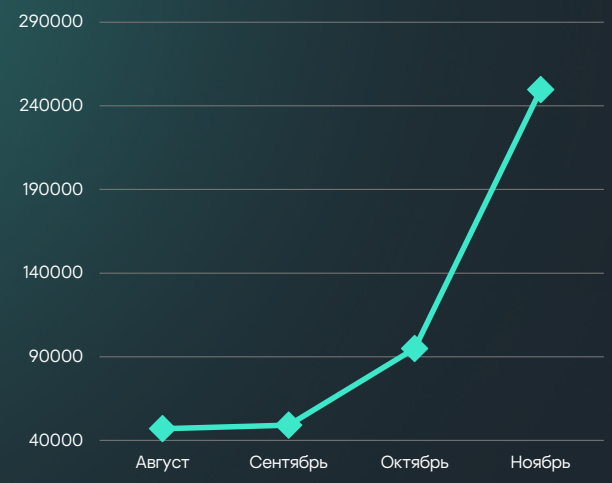
Рост таргетированности

Степень таргетированности атак растет: в рассылках прорабатываются мельчайшие детали — от схожести почтовых доменов и логики составления адресов до синхронизации с реальными корпоративными событиями и процессами

Увеличение охвата таргетированных атак

С ростом доступности продвинутых технологий злоумышленникам становится все легче организовывать таргетированные атаки, затрагивающие не только конкретные предприятия, но и целые технологические секторы

Обзор актуальных техник и тактик в почтовых атаках на бизнес



Глобальный тренд, характерный и для России: бурный рост детектов почтовых атак на российские организации с использованием QR-кодов в октябре и ноябре*

Новые грани PDF-вложений

Рассылки с PDF-вложениями все чаще встречаются как в массовом фишинге, так и в целевом. Тренд 2025 – использование вместо фишинговых ссылок внутри файла QR-кодов. Такой метод одновременно упрощает маскировку фишинговой ссылки и мотивирует пользователя открыть ее на телефоне, который можеть быть менее защищен, чем рабочий ПК.

Рассылки с фишинговыми ссылками в PDF-вложениях остаются актуальными, но все чаще сопровождаются дополнительными приемами обхода обнаружения. Некоторые PDF-файлы зашифрованы — чтобы их открыть, требуется пароль. Пароль может содержаться во вложении с PDF или отправляться отдельным сообщением. Это, с одной стороны, затрудняет быстрое сканирование файла, с другой — добавляет злоумышленникам «солидности» и может восприниматься как соответствие высоким стандартам безопасности.

* Данные Kaspersky Global Research and Analysis Team (GReAT)

«Вы уволены»: уведомления от имени HR

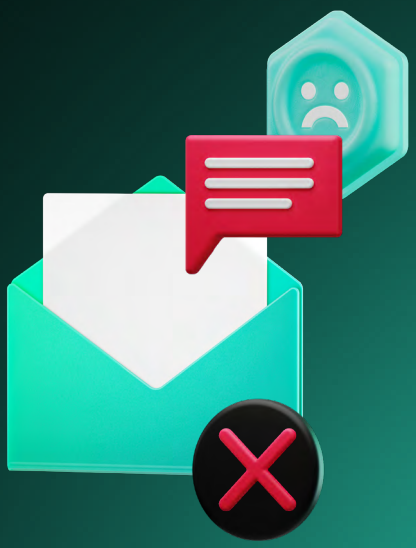
Тренд с использованием QR-кодов в PDF является частью более общего тренда. Сотрудника просят заполнить или подписать документ, например «график отпусков», доступный по ссылке из письма. Иногда злоумышленники предлагают найти себя в списке «уволенных сотрудников».

При переходе по ссылке вместо окна входа в рабочий кабинет сотрудник попадает на фишинговую форму ввода логина и пароля. Чаще всего злоумышленников интересуют учетные записи Microsoft, однако также встречаются страницы, имитирующие внутренние корпоративные порталы.

Переосмысление классики: календарные уведомления

Размещение фишинговых ссылок в текстовых полях календарного уведомления – старая схема массового спама, популярная в начале 2010-х годов. В 2025 году фишеры внезапно стали активно использовать эту технику в атаках именно на офисных сотрудников. Если пользователь, не разобравшись, примет встречу, в дальнейшем он получит напоминание о ней уже от приложения календаря. Таким образом увеличивается вероятность, что жертва перейдет на фишинговый сайт.

Получите, распишитесь: фальшивые уведомления от сервисов документооборота

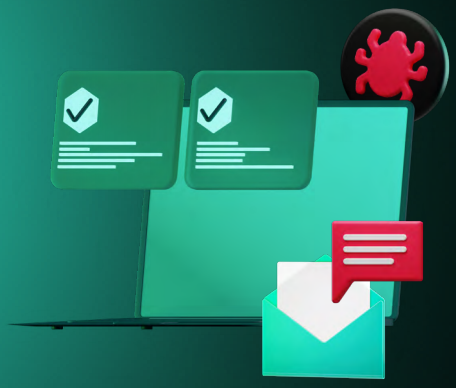


Сообщения, в которых под предлогом подписи документа принуждают перейти по фишинговой ссылке или открыть вредоносное вложение, в 2025 году попадались довольно часто. Наиболее популярной схемой являются фальшивые уведомления от сервисов для электронного подписания документов.

Особенно интересным оказался образец, который был своеобразной «матрешкой». В письме якобы от известной платформы для обмена документами получателя уведомляли о приглашении к совместному просмотру PDF-файла. На самом деле файл с таким форматом существовал только в тексте письма, а во вложении к нему находилось другое письмо с таким же названием. Приложенное письмо было очень похоже на исходное, но во вложении к нему, в свою очередь, был файл с двойным расширением: вредоносный SVG-файл с трояном маскировался под PDF-файл. Вероятно, мошенники таким образом пытались спрятать свой вредоносный файл и избежать блокировки антивирусом.

Письма от промышленников

Летом 2025 года встречались рассылки якобы от имени различных промышленных предприятий, во вложении которых был файл .docx с трояном внутри. Злоумышленники побуждали открыть вредоносное вложение под разными предлогами: утверждали, что это договор, который необходимо подписать; заключение, которое необходимо согласовать с руководством; или документ с информацией, на основе которой необходимо подготовить и предоставить отчет. Самым неприятным в этой кампании явилось использование настоящих доменов компаний промышленного сектора.



Усложнение BEC-атак

В 2025 году была зафиксирована изобретательная атака, в ходе которой злоумышленники выдавали себя за подрядчиков и ссылались на фальшивую переписку якобы с генеральным директором атакуемой организации, чтобы убедить бухгалтерию оплатить поддельный счёт. В ней обсуждались условия оплаты, а затем директор просил отправить письмо в его финансовый отдел. Конечно, вся приложенная переписка являлась подделкой.

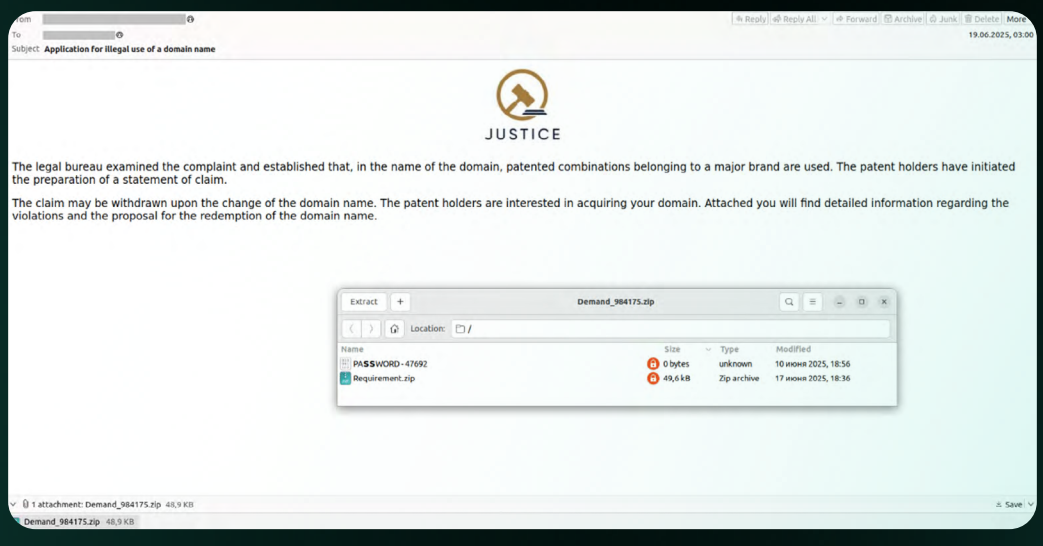
Архив в архиве, архивом погоняет (запароленным)

Сообщения с запароленным архивом с вредоносным содержимым остаются популярным способом распространения вредоносного ПО. В отдельных рассылках зараженные файлы могут находиться не во вложении, а скачиваться по ссылке из письма после ввода пароля. Вероятно, таким образом злоумышленники пытаются обойти защитные решения. Обычно пароль от зашифрованного архива указывается в тексте сообщения, реже — в самом названии вложения. Вредоносные архивы или ссылки зачастую маскируются под файлы с другими расширениями, например PDF, XLS или DOC.

В Рунете фиксировалось множество случаев отправки таких сообщений жертвам со взломанных ящиков их контрагентов. Некоторые письма содержали реальную переписку жертвы, ответом на которую злоумышленники отправляли письмо, содержащее вредоносный зашифрованный архив с двойным расширением. Все изученные сообщения в рамках этой кампании были уникальными и таргетированными на конкретные компании; содержимое писем отличалось высокой правдоподобностью.

Яркий пример попытки «спрятать» вредоносный файл — рассылки от имени юридических фирм. В них авторы писем угрожали получателям судебным разбирательством в связи с тем, что доменное имя получателя якобы перекликается с названием известного бренда. Далее получателю письма предлагали ознакомиться в приложенном документе с возможными способами урегулировать «спор».

Во вложении письма был незапароленный архив, внутри которого, в свою очередь, находились зашифрованный архив и отдельный файл с паролем от него. Если бы пользователь открыл архив и ввел указанный код, внутри он бы обнаружил вредоносный wsf-файл под видом юридического документа, после нажатия на который происходит заражение трояном через автозагрузку. Затем на экране открывается сообщение якобы о неработоспособности документа, в то же самое время на устройство скрытно скачивается и устанавливается Tor, который впоследствии регулярно отправляет снимки экрана пользователя на свой C2 в сети Tor. То есть конечной целью злоумышленников была слежка за пользователем.



Пример письма с запароленным архивом, содержащим вредоносное ПО

Рекомендации ИБ-командам

Игорь Кузнецов

Директор Kaspersky Global Research & Analysis Team (GReAT)

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.

Внедряйте многофакторную аутентификацию (MFA) для всех корпоративных ресурсов.

Настройте ресурсные записи DNS своих доменов для аутентификации почты (SPF, DKIM, DMARC). Эти сетевые проверки помогают проверять письма на наличие подмены отправителя (email spoofing) и таким образом защищают других пользователей от фишинговых или вредоносных рассылок от имени вашей компании.

Используйте шифрование данных, чтобы не допустить перехвата конфиденциальной информации третьими лицами. Применяйте последнюю версию протокола TLS для защиты данных в транзите и программу надёжные средства шифрования, например, S/MIME или PGP в сочетании с аппаратными ключевыми носителями.

Используйте сетевую песочницу для выявления и блокировки сложных угроз на рабочих станциях и серверах вашей компании. Изолированная среда позволяет безопасно проверять подозрительные файлы и ссылки, включая те, что содержатся в электронных письмах, на наличие вредоносного ПО. Благодаря своим принципам работы песочницы способны защищать от вредоносных программ, которые еще не известны антивирусу, и бороться с уязвимостями «нулевого дня».

Применяйте комплексное решение для защиты, которое объединяет возможности централизованного мониторинга и анализа информации, продвинутого обнаружения киберугроз и реагирования на них, а также инструменты исследования событий безопасности.

Следите за актуальностью ПО. Важно вовремя обновлять серверное ПО, включая почтовые серверы, клиентские приложения и антивирусное ПО, чтобы устранять известные уязвимости.

Необходимо регулярно проводить обучающие тренинги по информационной безопасности для сотрудников. В частности, им важно научиться безопасной работе с электронной почтой, чтобы уметь распознавать письма, содержащие почтовые угрозы, оценивать риски, сообщать об инцидентах и устранять их последствия. Регулярные тренинги и повышение осведомленности сотрудников об актуальных угрозах снижают вероятность успешных атак с использованием фишинга и других методов социальной инженерии.

Объясните сотрудникам важность проверки адресов отправителей сообщений, а также настоящих адресов гиперссылок, которые можно просмотреть при наведении курсора мыши. Также важно рассказать работникам о возможной опасности подозрительных вложений писем, особенно защищенных паролем архивов, документов с макросами, HTML-файлов, SVG-файлов и исполняемых файлов.

Используйте надежное специализированное решение для защиты корпоративной электронной почты.

Определите правила доступа к корпоративным ресурсам: учетные записи эл. почты, общие папки и онлайн-документы. Контролируйте и ограничивайте число лиц с доступом к важным данным компании. Поддерживайте списки доступа в актуальном состоянии и своевременно отзывайте доступ, когда сотрудники покидают компанию. Пользуйтесь брокерами безопасного доступа к облаку, чтобы отслеживать и контролировать действия сотрудников в облачных сервисах и обеспечивать принудительное соблюдение политик безопасности

Взгляд вперёд: на что обратить внимание уже сейчас

«Размытие» BEC и других таргетированных атак, мультиканальность

В распоряжении злоумышленников уже есть множество инструментов и данных для осуществления комплексных последовательных атак. Например, «точкой входа» может быть корпоративная почта, а дальнейшее общение будет развиваться в мессенджерах, чатах, телефонных звонках, причем со стороны злоумышленника разговор может поддерживать ИИ

Усиление тренда на маскировку фишингового url в фишинговых письмах

Например, с помощью QR, технологии link-protection, использования ESP-сервисов

Доминирование ИИ не только в создании текста, но и в поиске уязвимостей почтовой инфраструктуры, появление большего количества уязвимостей нулевого дня в почте

Возможности Kaspersky Security для почтовых серверов

Kaspersky Security для почтовых серверов

Обновленное решение Kaspersky Security для почтовых серверов (KSMS) обеспечивает безопасность корпоративной переписки, защищает от спама, атак по электронной почте, всех форм фишинга, компрометации корпоративной почты, атак с применением QR-кодов и других угроз.

Новая версия решения KSMS Plus с расширенными функциями защиты:

Content Disarm and Reconstruction (CDR)

Функция CDR позволяет «обезоружить» письмо с подозрительным вложением: извлекаются подозрительно активные элементы (потенциально вредоносные объекты) из вложений форматов .txt, .html, .docx, .xslx и тела письма, затем удаляется потенциальная угроза и воссоздается безопасная версия письма. При этом сохраняется полезное содержимое, а само письмо без задержек доставляется получателю. Пользователь может продолжать работу с документом без риска заражения. CDR создает дополнительный уровень защиты от целевых атак и других угроз, а также дополняет другие технологии в Kaspersky Security для почтовых серверов.

Проверка запароленных архивов

KSMS позволяет проверить содержимое запароленных архивов внутри электронных писем. Пользователь вводит пароль от архива на выделенном защищенном портале, после чего вложение отправляется на анализ с помощью технологий Kaspersky Security для почтовых серверов, а также KATA Sandbox. После проверки пользователь получает исходное письмо с проверенным вложением – быстро, безопасно и без необходимости привлечения IT-администратора.

Также рекомендуем

Kaspersky Security для бизнеса

Гибкая линейка продуктов для защиты рабочих мест с широкими возможностями для управления безопасностью компаний любого масштаба.

Kaspersky Security Awareness

Набор решений для создания культуры кибербезопасности, включающий образовательную платформу и тренинги для специалистов разного уровня.

Kaspersky Unified Monitoring and Analysis Platform

SIEM-платформа, которая обеспечивает централизованный сбор, ускоренный анализ и корреляцию событий безопасности из различных источников данных.

Kaspersky Threat Intelligence

Комплекс сервисов информирования об угрозах. Тактические, операционные и стратегические данные о динамично меняющемся ландшафте угроз для обогащения защитных решений и повышения экспертизы ИБ-команд.

Узнать больше о Kaspersky Security для почтовых серверов

Полезные ресурсы

Securelist.ru

Подробный анализ угроза информационной безопасности, реверс-инжиниринг вирусов и глобальная статистика.

Киберпульс

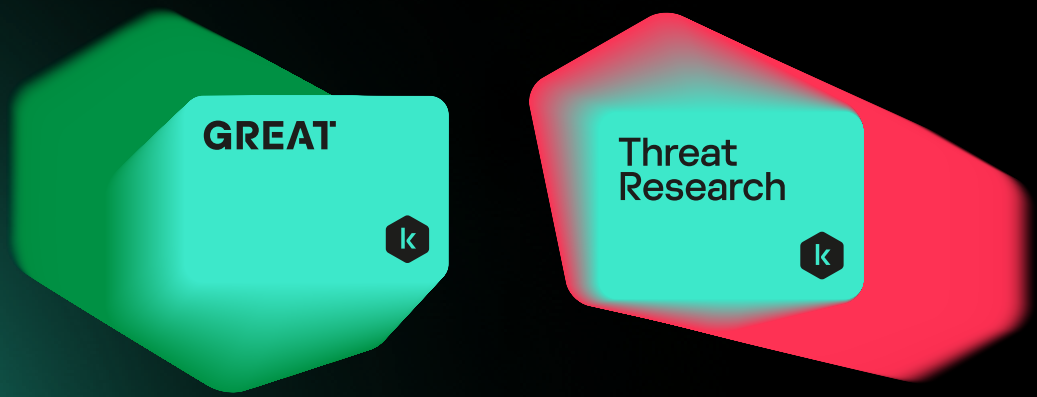
Статистика по киберугрозам в России

Записки цифрового ревизора: три кластера угроз в киберпространстве

Аналитическое исследование по актуальным для России киберугрозам. Техническое описание наиболее характерных тактик, техник и процедур, а также инструментария этих группировок — для использования этих данных специалистами SOC, DFIR, CTI и Threat Hunting на практике.

Rutube-канал Kaspersky Tech

Записи и онлайн-трансляции вебинаров, митапов, встреч сообществ, выступлений наших спикеров на технических конференциях



www.kaspersky.ru

#kaspersky
#активируйбудущее