Kaspersky ICS CERT

kaspersky

Краткий обзор основных инцидентов в области промышленной кибербезопасности за третий квартал 2025 года

18.12.2025

Версия 1.0

Оглавление

В третьем квартале 2025 года жертвами было публично подтверждено 129 инцидентов. Все эти инциденты включены в таблицу в конце обзора, а некоторые из них описаны подробно.

Общие сведения

Третий квартал 2025 года был ознаменован несколькими крупными инцидентами, некоторым из которых, возможно, суждено остаться в списке самых масштабных и значимых инцидентов за последние пару лет. Показательно, что все из них пришлись на один сектор — транспорта и логистики.

Атака вымогателей на Jaguar Land Rover (JLR) вызвала пятинедельный простой производства, ставший прямой причиной убытков, оцениваемых, по меньшей мере, в десятки миллионов долларов и вынудивший компанию взять дополнительных кредитов от государства и коммерческих банков на общую сумму в 4,69 млрд долларов. Инцидент стал фатальным для нескольких поставщиков JLR — им пришлось прибегнуть к процедуре банкротства. По оценке британского центра мониторинга инцидентов, атака на JLR сказалась на работе около 5000 британских организаций, нанеся суммарный ущерб британской экономике в 2,5 млрд долларов. Ущерб для глобального автомобильного сектора и суммарный ущерб для мировой экономики еще предстоит оценить.

Атака вымогателей, выведшая из строя платформу онлайн-регистрации ARINC cMUSE американского разработчика Collins Aerospace, привела к сбоям в работе нескольких крупнейших европейских аэропортов, в очередной раз демонстрируя, насколько авиатранспортный сектор уязвим к атакам на цепочку поставок.

Еще одной жертвой злоумышленников стал крупнейший российский авиаперевозчик «Аэрофлот». Атака хактивистов на системы авиакомпании вынудила отменить множество рейсов.

Еще четыре организации из сектора авиаперевозок — Air France, KLM, Air Serbia, Qantas, а также аэропорт Род-Айленда — заявили о киберинцидентах, результатом которых стала кража конфиденциальных данных.

На этом список жертв транспортного сектора не заканчивается. Об инцидентах сообщили два гиганта автомобильной промышленности — Stellantis и Bridgestone и несколько более мелких организаций.

Пакистанская нефтегазовая компания Pakistan Petroleum Limited подверглась атаке шифровальщика, повлиявшей на непрерывность ее

финансовых операций. Возможно, мы увидим больше подобных инцидентов в Азии в скором будущем.

В Польше, возможно, произошел киберинцидент, в ходе которого была якобы предотвращена опасность оставить некий «большой город» без воды — об этом сообщил вице-премьер-министр страны. Надеемся, какие-то подробности истории и технические детали появятся в ближайшее время в публичном инфополе.

Июль

- Rhode Island Airport Corporation
- JCI Jones Chemicals
- Qantas
- Hero España
- Farmer's Rice Cooperative
- Louis Vuitton
- Surmodics
- HEXPOL Compounding Americas
- HEIM & HAUS
- Control Module
- EIZO Rugged Solutions
- SEMCO Technologies
- AzureWave Technologies
- Artivion
- NPK Construction Equipment
- Wibaie
- American Welding
- Tri State Electric
- GMK Associates
- FLOE International
- Dosatron International
- Vero Foods
- Mesa Natural Gas Solutions
- Ergonomic Products
- Berridge Manufacturing Company
- American Cord & Webbing
- Versa Designed Surfaces
- Novabev Group
- Delfingen
- Air Serbia
- BARTEC
- Birdsong Peanuts
- Safe Fleet Holdings
- Top Hydraulic
- Keystone Shipping
- Massachusetts Municipal Wholesale Electric Company
- King Industries
- Sauers Lopez Construction
- Tower Manufacturing Corporation
- Serviço Autônomo de Água e Esgoto de Barretos
- Distinctive Surfaces of Florida
- Certis USA LLC (Certis Biologicals)
- Lithium Nevada / Lithium Americas Corp.
- Lollytogs (LT Apparel Group)
- Exel Composites
- Baillie Lumber
- Aeroflot
- Vest Tube
- TIMEC Oil & Gas
- Kibernetik AG

Август

- Vaquero Underground Services
- Chanel
- PAC Strapping Products
- Pandora
- Episciences (Epionce)
- Air France and KLM
- Pakistan Petroleum Limited
- Old Dutch Foods
- Shinn Fu Company of America
- LBX Company
- Cate Equipment Company
- ENGIE Power & Gas
- Rohtstein Corporation
- Polish water supply
- Lumitex
- Brookshire Grocery Company
- City of Wichita Falls Cypress Water Treatment Facility
- Peter Pauper Press
- The Seydel Companies
- BB Diversified Services
- Data I/O Corporation
- KNH Enterprise
- The Hiller Companies
- Sun Pacific Solar Electric
- Maryland Transit Administration
- Util-Assist
- NHB Holdings
- Lasership / OnTrac Final Mile
- Gorham Sand & Gravel
- MoboTrex
- Antonio Sofo & Sons Importing Co / Sofo Foods

Сентябрь

- Jaguar Land Rover
- Bridgestone Americas
- Sunsweet Growers
- The LoveSac Company
- Cornwell Quality Tools
- Talisman civil consultants
- Champagne Logistics
- Minaris Advanced Therapies
- Transart Graphics
- Farmer Brothers
- Phoenix Mechanical Contracting
- G&H Wire Company (G&H Orthodontics)
- Channel Fish
- Sellmark Corporation
- NPK International
- Phoenix Products
- Miller Construction
- Gale Associates
- ENCON Heating & Air Conditioning
- Boliden / Miljödata
- MGM Transformers
- Chroma ATE
- Monterey Mushrooms
- CSJB Holdings
- National Molding
- Havco Wood Products
- Minsait ACS
- Hello Cake
- PCE Constructors
- Morrisroe
- Collins Aerospace (Heathrow, Berlin, Brussels and Dublin airports)
- Stellantis
- Carus
- Thermofin
- All States Materials Group
- Tekni-Plex
- Volvo Group North America
- Braun Electric Company
- Dulany Industries
- Okuma Europe
- Refresco
- Georgetown Brewing Company
- T.R.A. Industries Inc. / Huntwood Industries
- Thai Diamond & Zebra Electric
- Belkorp Ag
- Karndean Designflooring
- LG Balakrishnan & Bros
- Kering S.A.

2025

Атаки, которые привели к нарушению операционной деятельности

Heim & Haus

Производственный сектор

Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов, утечка персональных данных

Шифровальщики

Немецкий производитель строительных комплектующих Heim & Haus стал жертвой кибератаки, в ходе которой часть его ИТ-систем была зашифрована. Компания незамедлительно приняла комплекс мер по локализации и расследованию инцидента, работая в тесном сотрудничестве с экспертами по цифровой криминалистике, чтобы полностью восстановить системы с соблюдением требований Федерального управления Германии по информационной безопасности (BSI). Согласно обновленной информации на сайте компании от 6 июля, производство было восстановлено в полном объеме и функционировало устойчиво. Прямые продажи, монтаж и обслуживание клиентов по всей стране также были полностью восстановлены. Согласно обновлению на сайте от 10 июля, была восстановлена связь с компанией по телефону и электронной почте. Работа клиентского портала Heim & Haus также была восстановлена, однако при обработке отдельных запросов и заказов могли наблюдаться ограничения или задержки. Расследование показало, что, помимо шифрования систем, злоумышленники скомпрометировали персональные данные. Ответственность за июльскую атаку на Heim & Haus взяла на себя группа злоумышленников, использующих программу-вымогатель Kawa4096.

Hero España

Производственный сектор

Нарушение операционной деятельности, отказ сервисов

Испанский производитель продуктов питания Hero España сообщил, что 30 июня его компьютерные системы подверглись кибератаке, что привело к временным сбоям в работе предприятия в городе Алькантарилья (регион Мурсия). Атака привела к временным ограничениям производственной деятельности и логистических операций компании в Испании. Источники в компании подтвердили, что инцидент затронул только локальную деятельность Hero и не повлиял на международные подразделения группы. По словам представителей компании, в качестве первоочередной меры был выполнен контролируемый останов скомпрометированных систем, чтобы предотвратить распространение атаки и защитить данные. Для расследования причин атаки и обеспечения безопасного восстановления систем была сформирована команда специалистов по кибербезопасности и цифровой криминалистике, в которую вошли как сотрудники компании, так и внешние эксперты.

Wibaie

Производственный сектор

Нарушение операционной деятельности

Шифровальщики

В ночь с 9 на 10 июля 2025 года французский производитель окон и дверей Wibaie подвергся кибератаке, в результате которой начиная с 10 июля предприятие было полностью остановлено. Менеджер компании по связям с общественностью подтвердил факт атаки местным СМИ. Wibaie привлекла экспертов для устранения последствий инцидента. Из-за атаки около 600 сотрудников потеряли возможность выполнять свои обязанности. Ответственность за атаку на Wibaie взяла на себя группа Qilin.

Novabev Group

Производственный сектор

Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов

Шифровальщики

Российский производитель алкогольной продукции Novabev Group 14 июля подвергся кибератаке, в результате которой, согласно официальному заявлению компании, была временно нарушена работоспособность части ее ИТ-инфраструктуры. Атака отразилась на доступности некоторых сервисов и инструментов, а также сетевой инфраструктуры дочерней группы «ВинЛаб». Злоумышленники потребовали выкуп, однако компания отказалась выполнять их требования. Атака отразилась на деятельности компании, включая работу сети «ВинЛаб», однако признаков компрометации персональных данных клиентов выявлено не было. На момент публикации заявления веб-сайт «ВинЛаб» оставался недоступен. Собственная ИТ-команда круглосуточно работала над устранением последствий инцидента. Для ускорения процесса к расследованию также были привлечены внешние эксперты.

Аэрофлот

Транспорт, логистика

Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов

Российская авиакомпания «Аэрофлот» 28 июля столкнулась со сбоем в работе своих информационных систем в результате кибератаки. Авиакомпания была вынуждена отменить рейсы и предупредила о возможных перебоях в работе сервисов. «Аэрофлот» сообщил, что команда специалистов работает над минимизацией рисков для выполнения производственного плана полетов и скорейшим восстановлением штатной работы сервисов. Генеральная прокуратура РФ подтвердила, что сбой в работе информационных систем «Аэрофлота» был вызван хакерской атакой, и возбудила уголовное дело по признакам несанкционированного доступа к информации. Хакерские группировки «Киберпартизаны» и Silent Crow опубликовали 28 июля заявления, в которых взяли на себя ответственность за атаку на «Аэрофлот». Злоумышленники сообщили, что кибератака стала результатом операции продолжительностью в год, в ходе которой им удалось глубоко проникнуть в сеть «Аэрофлота», вывести из строя 7000

серверов и получить контроль над персональными компьютерами сотрудников, включая высшее руководство.

Pakistan Petroleum Limited

Энергетика

Отказ ИТ-систем, нарушение операционной деятельности, утечка персональных данных

Шифровальщики

Пакистанская нефтегазовая компания Pakistan Petroleum Limited (PPL) стала жертвой крупномасштабной атаки с использованием программы-вымогателя. По сведениям газеты Pakistan Today, хакеры, действовавшие под псевдонимом Blue Locker, зашифровали серверы PPL, заблокировали доступ к резервным копиям и потребовали выкуп. Атака привела к приостановке операционной деятельности компании, так как была парализована вся ее финансовая система. По данным источников, среди зашифрованных систем были виртуальные машины и финансовые серверы. Злоумышленники заявили, что похитили критически важные данные, связанные с операционной деятельностью и контрактами, а также сведения о сотрудниках. В официальном заявлении PPL сообщила, что инцидент был обнаружен 6 августа. Команды собственных ИТ-специалистов и экспертов по кибербезопасности совместно с внешними экспертами оперативно приняли меры по локализации инцидента, включая временную приостановку работы отдельных некритичных ИТ-сервисов для минимизации потенциальных последствий инцидента и обеспечения целостности системы. Основные системы, обеспечивающие функционирование компании, не были затронуты атакой, а партнеры компании по совместным предприятиям и внешние контрагенты продолжили работу без перебоев. Признаков компрометации критически важных или конфиденциальных данных выявлено не было.

Национальная группа реагирования на компьютерные инциденты Пакистана опубликовала предупреждение о высоком уровне угрозы, содержащее предостережение о серьезных рисках, связанных с программой-вымогателем Blue Locker, и сообщение о том, что с помощью этого шифровальщика были скомпрометированы объекты критической инфраструктуры, включая Pakistan Petroleum Limited. Компании Resecurity удалось получить образцы исполняемых файлов Blue Locker и проанализировать их с применением реверс-инжиниринга. Программа-вымогатель, связанная с вариантами семейства Proton, такими как Shinra, использует шифрование AES-RSA и повышает привилегии через внесение изменений в системный реестр, затрудняет обнаружения защитными решениями, обфускацией и подменой временных меток (timestomping). Компания Hackmanac сообщила, что группа злоумышленников yyy32111 заявила о взломе PPL и похищении 1 ТБ конфиденциальных данных в результате утечки, произошедшей 1 августа 2025 года.

KNH Enterprise

Производственный сектор

Отказ ИТ-систем, нарушение операционной деятельности

Согласно бюллетеню, опубликованному 24 августа на портале Тайваньской фондовой биржи (TWSE), тайваньский производитель нетканых материалов KNH Enterprise подвергся кибератаке. В бюллетене сообщалось, что хакерская атака затронула некоторые информационные системы группы и ее зарубежных дочерних компаний. Согласно различным оценкам, инцидент не оказал значительного влияния на операционную деятельность группы. Группа привлекла международно признанную компанию по обеспечению кибербезопасности для оказания помощи в разрешении инцидента. По завершении инцидента компания заявила, что продолжит усиливать меры безопасности сетевой и ИТ-инфраструктуры и осуществлять непрерывный мониторинг для обеспечения информационной безопасности.

Data I/O Corporation

Электроника, производственный сектор

Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов

Шифровальщики

Компания Data I/O Corporation — американский производитель ручных и автоматизированных систем безопасной инициализации и программирования устройств на основе флеш-памяти, микроконтроллеров и логических устройств — сообщила об имевшем место инциденте, направив 21 августа в Комиссию по ценным бумагам и биржам США уведомление по форме 8-K. 16 августа Data I/O Corporation столкнулась с инцидентом, связанным с заражением нескольких внутренних ИТ-систем программой-вымогателем. После обнаружения инцидента компания оперативно приняла меры по локализации инцидента, включая превентивный перевод отдельных платформ в автономный режим. Она также привлекла ведущих экспертов по кибербезопасности для восстановления ИТ-систем и проведения тщательного расследования. Инцидент оказал временное влияние на операционную деятельность Data I/O Corporation, включая внутренние и внешние коммуникации, отгрузку, приемку и производство продукции, а также различные вспомогательные функции. Несмотря на то, что сроки полного восстановления не были известны на момент подачи уведомления, по оценке компании, инцидент не оказал существенного влияния на ее коммерческую деятельность. При этом у компании отсутствовало полное представление о масштабе и последствиях инцидента, и она допускала, что он все же может оказать существенное влияние на финансовые показатели и результаты своей операционной деятельности — как минимум, будущие затраты, связанные с инцидентом, включая гонорары экспертов по кибербезопасности и других консультантов, а также расходы на восстановление затронутых атакой систем.

Chroma ATE

Электроника, производственный сектор

Отказ ИТ-систем, нарушение операционной деятельности

Шифровальщики

Согласно бюллетеню, опубликованному 17 сентября на портале Тайваньской фондовой биржи (TWSE), тайваньский производитель электронных контрольно-измерительных приборов Chroma ATE подвергся кибератаке. Атака затронула информационные системы компании. Подразделение по обеспечению безопасности работало над разрешением проблемы в тесном контакте с внешними ИТ-специалистами. Согласно бюллетеню, утечки персональной информации, конфиденциальных документов или важных данных не произошло. Атака не оказала существенного влияния на операционную деятельность Chroma ATE. Компания начала внедрять дополнительные меры по обеспечению информационной безопасности, такие как постоянный мониторинг и контроль безопасности своих сетевой и информационной инфраструктур. Ответственность за сентябрьскую атаку на Chroma ATE взяла на себя группа вымогателей Warlock.

Thermofin

Производственный сектор

Нарушение операционной деятельности, отказ сервисов, утечка персональных данных

Шифровальщики

Немецкий производитель теплообменников Thermofin стал жертвой кибератаки, согласно заявлению, опубликованному на сайте компании. Пострадали также дочерние компании Thermofin в Китае и Польше. Злоумышленники получили несанкционированный доступ к ИТ-системам компании и похитили, среди прочего, персональные данные. Похищенные данные предположительно включают имена, адреса, контактные данные и банковские реквизиты. В соответствии со статьей 34 Общего регламента по защите данных (GDPR), Thermofin проинформировала пострадавших от атаки лиц. Согласно сообщению в местной прессе, компания с трудом поддерживала производство из-за спровоцированных атакой ограничений операционной деятельности, связь с ней по горячей линии также была ограничена. Ответственность за атаку на Thermofin в сентябре взяла на себя группа вымогателей Sarcoma.

Refresco

Пищевая промышленность, производственный сектор

Нарушение операционной деятельности, отказ сервисов

Производитель напитков Refresco 22 сентября подвергся кибератаке, которая нарушила производственную деятельность компании в Германии, затронув производственные системы, а также прием и отгрузку продукции. В процессе восстановления нормальной работы компания продолжала принимать заказы клиентов по электронной почте. Другие подробности об инциденте, включая тип атаки и сведения о скомпрометированных данных, не сообщались в связи с продолжающимся расследованием.

Наиболее серьезные последствия, предотвращенные командами по реагированию на инциденты

Система водоснабжения в Польше

Коммунальные услуги, водоснабжение

Нарушение операционной деятельности

Вице-премьер и министр цифровизации Польши Кшиштоф Гавковский 14 августа подтвердил новостному порталу Onet.pl, что 13 августа была атакована инфраструктура водоснабжения и канализации неназванного крупного польского города. Гавковский заявил, что атака могла оставить один из крупных городов страны без воды, но была предотвращена. Соответствующие службы узнали об атаке в последний момент и успели отключить все системы.

Инциденты в крупных организациях

Jaguar Land Rover

Автомобиле-строение, производствен-ный сектор

Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов, банкротство

Шифровальщики

Британский международный производитель автомобилей Jaguar Land Rover (JLR), принадлежащий компании Tata Motors, подтвердил крупный инцидент информационной безопасности, затронувший его деятельность во всем мире. Компания впервые сообщила об инциденте 1 сентября в уведомлении, поданном на индийскую фондовую биржу, заявив, что ускоренными темпами работает над решением глобальных ИТ-проблем, влияющих на ее бизнес. 2 сентября JLR опубликовала на своем сайте заявление, в котором говорилось, что компания предприняла первоочередные меры по минимизации последствий инцидента, превентивно отключив системы. Согласно заявлению от 2 сентября, не было обнаружено признаков хищения клиентских данных, однако деятельность по продаже и производству продукции была серьезно нарушена.

Первые сообщения о серьезных сбоях в работе JLR поступили от дилеров в Великобритании, которые столкнулись с невозможностью регистрации новых автомобилей и поставки запчастей в сервисные центры. Отвечая на запросы СМИ, JLR заявила, что атака произошла в выходные 30—31 августа, что вынудило компанию отключить несколько систем, в том числе используемые на заводе в Солихалле. Издание Liverpool Echo сообщило, что утром 1 сентября работники завода компании в Хейлвуде (Мерсисайд) получили указание не выходить на работу по причине инцидента. Атака на

JLR затронула также поставщиков компании. По сообщению BBC, несколько мелких поставщиков Jaguar Land Rover столкнулись с угрозой банкротства из-за длительной остановки производства. Они были вынуждены приостановить собственную деятельность и отправить сотрудников в отпуск. После кибератаки немецкая компания Eberspächer Gruppe GmbH & Co., производящая выхлопные системы для JLR, была вынуждена приостановить производство на своем заводе в Нитре (Словакия). Генеральный директор словацкой компании Hollen, обеспечивающей контроль качества автозапчастей, сообщил, что она ввела ограничения из-за остановки работы JLR. На встрече с комитетом правительства по бизнесу и торговле 25 сентября 10 компаний из цепочки поставок выразили обеспокоенность своими перспективами, так как у некоторых из них средств оставалось всего на 7–10 дней работы.

10 сентября JLR опубликовала заявление, в котором говорилось, что часть данных была скомпрометирована, и компания проинформировала об этом соответствующие регулирующие органы. 27 сентября британское правительство пообещало предоставить гарантии по кредиту на сумму 2 миллиарда долларов для поддержки цепочки поставок JLR в связи с остановкой производства, вызванной атакой. Газета Financial Times 29 сентября сообщила, ссылаясь на осведомленные источники, что JLR также получила новую кредитную линию от коммерческих банков на сумму 2,69 миллиарда долларов в дополнение к кредитным средствам, гарантированным правительством.

Компания проинформировала 29 сентября коллег, розничные площадки и поставщиков о предстоящем в ближайшие дни возобновлении работы некоторых производственных участков. JLR продолжала работать в круглосуточном режиме в сотрудничестве со специалистами по кибербезопасности, Национальным центром кибербезопасности (NCSC) Великобритании и правоохранительными органами для обеспечения безопасного перезапуска производства.

Производство было поэтапно перезапущено к 8 октября. Судя по опубликованным JLR финансовым результатам, кибератака привела к значительному снижению прибыли компании. «Убыток до налогообложения и чрезвычайных статей составил 485 млн фунтов стерлингов за второй квартал (имеется в виду второй квартал финансового года, который в Англии завершился 30 сентября. — *Прим. ред.*) и 134 млн фунтов стерлингов за первое полугодие, при этом за те же периоды предыдущего года компания получила прибыль, соответственно, 398 млн и 1,1 млрд фунтов стерлингов», — заявила компания. JLR отметила, что кибератака стала одним из основных факторов снижения прибыли.

По оценке британского центра мониторинга инцидентов, атака на JLR сказалась на работе около 5000 британских организаций, нанеся суммарный ущерб британской экономике в 2,5 млрд долларов. Ущерб для глобального автомобильного сектора и суммарный ущерб для мировой экономики еще предстоит оценить.

В начале сентября группа, называющая себя Scattered Lapsus$ Hunters (неформальное объединение хакеров, связанных с тремя различными группами: Scattered Spider, Lapsus$ и ShinyHunters), взяла на себя ответственность за атаку на JLR в сообщениях в Telegram. Хакеры опубликовали изображения внутренних систем JLR и документации на автомобили, заявив, что получили доступ к системам, использовав уязвимость в технологической платформе SAP NetWeaver (CVE-2025-31324).

Bridgestone Americas

Производственный сектор

Нарушение операционной деятельности

Компания Bridgestone Americas (BSA) — североамериканское подразделение японского производителя шин Bridgestone Corporation — 2 сентября подтвердила инцидент, затронувший два производственных предприятия в округе Эйкен в штате Южная Каролина. На следующий день канадское СМИ сообщило о схожих перебоях на заводе BSA в Жольете в провинции Квебек. Мэр Жольета заявил, что лично общался с руководством Bridgestone, и сообщил канадскому изданию, что киберинцидент, по всей вероятности, затронул все заводы Bridgestone в Северной Америке. BSA отметила, что благодаря оперативному реагированию на инцидент удалось локализовать атаку на ранней стадии и тем самым предотвратить кражу данных клиентов и дальнейшее проникновение в сеть. Специалисты работали круглосуточно, чтобы минимизировать перебои в цепочке поставок, способные привести к дефициту продукции.

Stellantis

Автомобилестроение, производственный сектор

Утечка персональных данных

Вымогательство

Stellantis — международный автопроизводитель со штаб-квартирой в Нидерландах — 21 сентября сообщил об утечке данных. Компания обнаружила несанкционированный доступ к платформе стороннего поставщика услуг, который обеспечивает поддержку операций по обслуживанию клиентов в Северной Америке. Затронутые персональные данные были ограничены контактной информацией. После обнаружения взлома компания Stellantis немедленно активировала свои протоколы реагирования на инциденты, уведомила соответствующие органы власти и напрямую проинформировала пострадавших клиентов.

Интернет-ресурсу BleepingComputer стало известно, что атака была частью недавней волны связанных с группой вымогателей ShinyHunters атак на известные компании, приведших к утечке данных с платформы Salesforce. 22 сентября ShinyHunters взяла на себя ответственность за утечку данных Stellantis и сообщила BleepingComputer, что похитила более 18 млн записей Salesforce, включая имена и контактные данные, из экземпляра платформы, принадлежащего компании.

Collins Aerospace

Транспорт, логистика, аэрокосмическая и оборонная промышленность

Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов

Цепочка поставок/ доверенные партнеры

Шифровальщики

Атака программы-вымогателя нарушила работу нескольких крупных европейских аэропортов, в частности в Лондоне (Хитроу), Берлине, Брюсселе и Дублине, вызвав задержки рейсов. Атака, обнаруженная 19 сентября, была нацелена на программное обеспечение для автоматической регистрации и посадки пассажиров на рейсы ARINC cMUSE, поставляемое американской компанией Collins Aerospace, принадлежащей крупному оборонному конгломерату RTX и специализирующейся на разработке программного обеспечения. Авиакомпании, использующие это ПО, были вынуждены осуществлять регистрацию и посадку пассажиров вручную, в результате чего несколько рейсов были задержаны или отменены. Агентство Европейского Союза по кибербезопасности (ENISA) подтвердило, что инцидент представлял собой атаку с применением программы-вымогателя.

Компания Collins Aerospace 20 сентября опубликовала заявление, в котором говорилось, что она находится на завершающей стадии внедрения необходимых обновлений программного обеспечения. Согласно служебной записке из аэропорта Хитроу, с которой ознакомилась BBC, после обнаружения атаки Collins Aerospace прежде всего пересобрала и перезапустила свои системы, но обнаружила, что хакеры сохранили доступ к ним. Согласно оценкам, приведенным в служебной записке, более 1000 компьютеров в аэропорту Хитроу придется восстанавливать вручную. По имеющимся данным, Collins Aerospace посоветовала авиакомпаниям не выключать компьютеры и не выходить из программного обеспечения Muse, если вход в систему уже выполнен.

Представитель Национального центра кибербезопасности (NCSC) 20 сентября заявил, что центр работает в сотрудничестве с Collins Aerospace, пострадавшими аэропортами Великобритании, министерством транспорта и правоохранительными органами, чтобы получить полное представление о масштабах инцидента. В Великобритании в рамках расследования инцидента был арестован один человек. 24 сентября корпорация RTX в уведомлении,

поданном в Комиссию по ценным бумагам и биржам (SEC), подтвердила, что в атаке на ее программное обеспечение для обработки пассажирских данных использовалась программа-вымогатель, а также заявила, что не ожидает значительного влияния атаки на финансовые результаты.

Приложение. Полный список подтвержденных инцидентов

Жертва	Отрасль / Профиль	Страна	Последствия и особенности инцидента	Дата уведомления Дата инцидента (если известна) Предполагаемые акторы
Rhode Island Airport Corporation	Логистика и транспорт / Аэропорт	США	Утечка персональных данных	1 июля 2025 года 14 мая 2025 года
HEXPOL Compounding Americas	Производство / Компаундирование и производство полимеров	США	Утечка персональных данных Шифровальщики	3 июля 2025 года 22 декабря 2024 года Qilin
JCI Jones Chemicals	Химическая промышленность, производство / Производитель химикатов для очистки воды	США	Утечка персональных данных	1 июля 2025 года 9 июня 2025 года
Dosatron International	Производство / Производитель оборудования для дозирования и смешивания с приводом от потока воды	США	Утечка персональных данных	14 июля 2025 года 4 марта 2025 года
Artivion	Производство / Производитель медицинских изделий	США	Утечка персональных данных	9 июля 2025 года 20 ноября 2024 года

Ergonomic Products	Производство / Производитель стоматологического оборудования	США	Утечка персональных данных	15 июля 2025 года 2 октября 2024 года
Vero Foods	Пищевая промышленность, производство / Производитель продуктов питания	США	Утечка персональных данных	14 июля 2025 года 2 декабря 2024 года
Keystone Shipping	Логистика и транспорт / Компания морских перевозок	США	Утечка персональных данных Шифровальщики	21 июля 2025 года 3 июня 2025 года Akira
Massachusetts Municipal Wholesale Electric Company	Коммунальное хозяйство / Поставщик электроэнергии	США	Утечка персональных данных Шифровальщики	21 июля 2025 года 25 января 2025 года BlackSuit
Birdsong Peanuts	Пищевая промышленность, производство / Переработка арахиса	США	Утечка персональных данных	18 июля 2025 года 23 июня 2025 года
Safe Fleet Holdings	Производство / Производитель решений в области безопасности	США	Утечка персональных данных	18 июля 2025 года 12 апреля 2024 года
Top Hydraulic	Производство / Производитель гидравлических компонентов	США	Утечка персональных данных	18 июля 2025 года 11 июля 2025 года
American Welding	Производство / Производитель и дистрибьютор промышленных газов	США	Утечка персональных данных	11 июля 2025 года
Tri State Electric	Строительство и инжиниринг / Монтаж электрической дорожной инфраструктуры, оптоволокна, систем микроволнового обнаружения транспортных средств	США	Утечка персональных данных Шифровальщики	11 июля 2025 года RansomHouse

NPK Construction Equipment	Производство / Производитель верхних монтажных кронштейнов, кронштейнов для гидромолотов, виброплит, сваебойных машин, систем манипуляторов, систем разгрузки твердых пород, систем для работы с твердыми материалами	США	Утечка персональных данных Шифровальщики	10 июля 2025 года Worldleaks
Berridge Manufacturing Company	Производство / Производитель архитектурных изделий из листового металла, окрашенной рулонной стали и плоских листов, переносных профилегибочных станков	США	Утечка персональных данных Шифровальщики	15 июля 2025 года Brain Cipher
Mesa Natural Gas Solutions	Энергетика, производство / Проектирование, производство и эксплуатация энергетических технологий, включая генераторные установки и микросети, работающие на природном газе и сжиженном пропане	США	Утечка персональных данных	14 июля 2025 года
GMK Associates	Строительство и инжиниринг / Поставщик услуг в области архитектуры, инжиниринга, строительства и проектирования	США	Утечка персональных данных	11 июля 2025 года
King Industries	Химическая промышленность, производство / Химическая производственная компания	США	Утечка персональных данных Шифровальщики	21 июля 2025 года Akira
Distinctive Surfaces of Florida	Производство / Производитель столешниц	США	Утечка персональных данных	23 июля 2025 года 1 апреля 2025 года

Certis USA LLC (Certis Biologicals)	Производство / Производитель биологических средств защиты растений	США	Утечка персональных данных	24 июля 2025 года
Tower Manufacturing Corporation	Производство / Производитель устройств электробезопасности	США	Утечка персональных данных	22 июля 2025 года 3 июня 2025 года
TIMEC Oil & Gas	Энергетика, строительство / Компания по техническому обслуживанию и монтажу технологического оборудования	США	Утечка персональных данных	30 июля 2025 года 7 апреля 2025 года
Vest Tube	Производство / Производитель электросварных труб из углеродистой стали	США	Утечка персональных данных, отказ ИТ-систем	29 июля 2025 года 14 февраля 2025 года
Baillie Lumber	Производство / Производитель пиломатериалов из лиственных пород	США	Утечка персональных данных Шифровальщики	28 июля 2025 года 7 февраля 2025 года Cactus
Sauers Lopez Construction	Строительство и инжиниринг / Генеральный подрядчик, специализирующийся на строительстве и реконструкции автосалонов	США	Утечка персональных данных, отказ ИТ-систем	21 июля 2025 года 22 мая 2024 года
Lollytogs (LT Apparel Group)	Производство / Производитель одежды	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	25 июля 2025 года 19 февраля 2024 года Clop
Control Module	Производство / Производитель систем учета времени, решений для автопарков, топливных систем и зарядных станций для электромобилей	США	Утечка персональных данных	7 июля 2025 года

FLOE International	Производство / Производитель причалов, лодочных подъемников, прицепов	США	Утечка персональных данных Шифровальщики	12 июля 2025 года Qilin Play
American Cord & Webbing	Производство / Производство текстильных лент, пластиковых изделий, ремней	США	Утечка персональных данных	15 июля 2025 года
Versa Designed Surfaces	Производство / Производитель коммерческих настенных покрытий и средств защиты стен	США	Утечка персональных данных	16 июля 2025 года 12 апреля 2025 года
EIZO Rugged Solutions	Производство / Производство графических и видео решений для обороны и разведки	США	Утечка персональных данных Шифровальщики	7 июля 2025 года 6 мая 2025 года Play
Heim & Haus	Производство / Производитель строительных комплектующих	Германия	Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов, утечка персональных данных Шифровальщики	4 июля 2025 года Kawa4096
Qantas	Логистика и транспорт / Авиакомпания	Австралия	Утечка персональных данных Шифровальщики	1 июля 2025 года 30 июня 2025 года Scattered Spider
Louis Vuitton	Производство / Производитель товаров класса люкс	Франция	Утечка персональных данных Вымогательство	2 июля 2025 года 7 июня 2025 года ShinyHunters
Surmodics	Производство / Производитель медицинского оборудования	США	Отказ ИТ-систем	2 июля 2025 года 5 июня 2025 года

Hero España	Пищевая промышленность, производство / Производитель продуктов питания	Испания	Нарушение операционной деятельности, отказ сервисов	1 июля 2025 года 30 июня 2025 года
AzureWave Technologies	Электроника, производство / Производитель модулей беспроводной связи и модулей обработки изображений	Тайвань	Отказ ИТ-систем Шифровальщики	8 июля 2025 года 7 июля 2025 года Qilin
Wibaie	Производство / Производитель окон и дверей	Франция	Нарушение операционной деятельности Шифровальщики	10 июля 2025 года 9 июля 2025 года Qilin
Novabev Group	Пищевая промышленность, производство / Производитель алкогольной продукции	Россия	Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов Шифровальщики	16 июля 2025 года 14 июля 2025 года
Delfingen	Автомобилестроение, производство / Производитель решений для защиты бортовых сетей и трубок для перекачки жидкостей	Франция	Утечка данных Шифровальщики	16 июля 2025 года PayoutsKing
Exel Composites	Производство / Производитель композитных профилей и промышленных труб	Финляндия	Утечка персональных данных Шифровальщики	25 июля 2025 года Июль 2025 года World Leaks
Serviço Autônomo de Água e Esgoto de Barretos	Коммунальное хозяйство / Водоснабжение, канализация	Бразилия	Отказ ИТ-систем и сервисов Шифровальщики	22 июля 2025 года
Air Serbia	Логистика и транспорт / Авиакомпания	Сербия	Отказ ИТ-систем и сервисов	17 июля 2025 года 4 июля 2025 года

Аэрофлот	Логистика и транспорт / Авиакомпания	Россия	Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов	28 июля 2025 года Киберпартизаны Silent Crow
SEMCO Technologies	Электроника, производство / Производитель электростатических патронов и ключевых компонентов для полупроводниковых приборов	Франция	Утечка персональных данных Шифровальщики	7 июля 2025 года Qilin
BARTEC	Производство / Производитель взрывозащищенного оборудования	Германия	Утечка персональных данных Шифровальщики	17 июля 2025 года Safepay
Kibernetik AG	Производство / Производитель холодильного оборудования и тепловых насосов	Швейцария	Отказ ИТ-систем и сервисов, утечка данных	31 июля 2025 года
PAC Strapping Products	Производство / Производитель обвязочных материалов	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	4 августа 2025 года 26 марта 2025 года Play
Episciences (Epionce)	Производство / Производитель средств личной гигиены	США	Утечка персональных данных	6 августа 2025 года 27 апреля 2025 года
Lumitex	Производство / Производитель систем светопередачи	США	Утечка персональных данных	15 августа 2025 года 30 июля 2025 года
Old Dutch Foods	Пищевая промышленность, производство / Производитель продуктов питания	США	Утечка персональных данных	11 августа 2025 года 16 октября 2024 года

Farmer's Rice Cooperative	Пищевая промышленность, производство / Производитель риса	США	Утечка персональных данных	1 июля 2025 года 30 августа 2024 года
The Seydel Companies	Химическая промышленность, производство / Производитель химикатов	США	Утечка персональных данных Шифровальщики	20 августа 2025 года 26 апреля 2025 года Play
Util-Assist	Коммунальное хозяйство / Управляющая компания в сфере коммунальных услуг	Канада	Утечка персональных данных	27 августа 2025 года 11 июля 2025 года
NHB Holdings (New Horizons Baking Company, Genesis Baking Company, Metraco Transportation Company, New Horizons Food Solutions)	Пищевая промышленность, производство / Производитель хлебобулочных изделий	США	Утечка персональных данных	27 августа 2025 года 6 января 2025 года
Lithium Nevada (Lithium Americas Corp.)	Горнодобывающая промышленность / Добыча лития	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	24 июля 2025 года 7 апреля 2025 года Medusa
The Hiller Companies	Строительство и инжиниринг / Проектирование и инжиниринг систем и оборудования противопожарной защиты	США	Утечка персональных данных	25 августа 2025 года 18 декабря 2024 года
Lasership / OnTrac Final Mile	Логистика и транспорт / Транспортно-логистические услуги	США	Утечка персональных данных	27 августа 2025 года 13 апреля 2025 года

Sun Pacific Solar Electric	Энергетика, строительство / Монтаж и обслуживание систем солнечной энергетики	США	Утечка персональных данных	25 августа 2025 года
LBX Company	Производство / Производитель тяжелой техники	США	Утечка персональных данных	14 августа 2025 года 18 июня 2025 года
Gorham Sand & Gravel	Строительство и инжиниринг / Строительные материалы и земляные работы	США	Утечка персональных данных Шифровальщики	28 августа 2025 года 23 апреля 2025 года Play
BB Diversified Services	Производство / Производство механически обработанных и собранных компонентов	США	Утечка персональных данных	20 августа 2025 года 24 февраля 2025 года
Shinn Fu Company of America	Производство / Производитель гидравлического подъемного оборудования	США	Утечка персональных данных Шифровальщики	11 августа 2025 года Play
Cate Equipment Company	Производство / Тяжелое оборудование и техника	США	Утечка персональных данных	14 августа 2025 года 2 августа 2024 года
ENGIE Power & Gas	Коммунальное хозяйство, энергетика / Производство и распределение электроэнергии, природный газ, атомная энергетика, возобновляемая энергетика, централизованное теплоснабжение, нефтяная промышленность	Франция	Утечка персональных данных	14 августа 2025 года
Rohtstein Corporation	Пищевая промышленность, производство /	США	Утечка персональных данных	14 августа 2025 года

	Производитель продуктов питания			
Peter Pauper Press	Производство / Полиграфия и издательское дело	США	Утечка персональных данных	18 августа 2025 года Teamxxx
MoboTrex	Производство / Производитель средств регулирования дорожного движения	США	Утечка персональных данных	28 августа 2025 года
Vaquero Underground Services	Строительство и инжиниринг / Прокладка подземных коммуникаций	США	Утечка персональных данных	1 августа 2025 года
Brookshire Grocery Company	Пищевая промышленность, производство / Производитель выпечки, молочной продукции, мороженого, йогуртов, готовых продуктов, льда, воды и напитков	США	Утечка персональных данных	15 августа 2025 года
City of Wichita Falls Cypress Water Treatment Facility	Коммунальное хозяйство / Очистка и подготовка воды	США	Утечка персональных данных	15 августа 2025 года
Antonio Sofo & Sons Importing (Sofo Foods)	Логистика и транспорт / Дистрибуция продуктов питания	США	Утечка персональных данных Шифровальщики	28 августа 2025 года Payouts King
Air France и KLM	Логистика и транспорт / Авиакомпания	Франция Нидерланды	Утечка персональных данных Вымогательство	6 августа 2025 года ShinyHunters
Pakistan Petroleum Limited	Энергетика / Производитель нефти и газа	Пакистан	Отказ ИТ-систем, нарушение операционной деятельности, утечка персональных данных	7 августа 2025 года 6 августа 2025 года Blue Locker yyy32111

			Шифровальщики	
KNH Enterprise	Производство / Производитель нетканых материалов	Тайвань	Отказ ИТ-систем, нарушение операционной деятельности	24 августа 2025 года
Pandora	Производство / Производитель ювелирных изделий	Дания	Утечка персональных данных Вымогательство	5 августа 2025 года ShinyHunters
Chanel	Производство / Производитель товаров класса люкс	Франция	Утечка персональных данных Вымогательство	1 августа 2025 года 25 июля 2025 года ShinyHunters
Data I/O Corporation	Электроника, производство / Производитель ручных и автоматизированных систем безопасной инициализации и программирования устройств	США	Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов	21 августа 2025 года 16 августа 2025 года
Система водоснабже-ния в Польше	Коммунальное хозяйство / Водоканал	Польша	Нарушение операционной деятельности	14 августа 2025 года 13 августа 2025 года
The LoveSac Company	Производство / Производитель мебели	США	Утечка персональных данных Шифровальщики	4 сентября 2025 года 12 февраля 2025 года RansomHub
Cornwell Quality Tools	Автомобилестроение, производство / Производитель автомобильного ручного инструмента	США	Утечка персональных данных Шифровальщики	4 сентября 2025 года 12 декабря 2024 года Cactus

Sellmark Corporation	Производство / Производитель товаров для активного отдыха и тактического снаряжения	США	Утечка персональных данных	11 сентября 2025 года 10 марта 2025 года
NPK International	Производство / Производитель экологичных композитных настилов	США	Утечка персональных данных	11 сентября 2025 года
Farmer Brothers	Пищевая промышленность, производство / Производитель кофе, чая и кулинарной продукции	США	Утечка персональных данных Шифровальщики	9 сентября 2025 года 6 марта 2025 года Chaos
Carus	Химическая промышленность, производство / Химические продукты для очистки воды, воздуха, рекультивации почвы	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	22 сентября 2025 года 7 августа 2025 года Akira
Havco Wood Products	Производство / Компания по производству настилов для прицепов	США	Утечка персональных данных	19 сентября 2025 года 30 марта 2025 года
Minsait ACS	Коммунальное хозяйство / Программные решения для управления энергосетями и передовые технологии автоматизации для коммунальных предприятий	США	Утечка персональных данных	19 сентября 2025 года 26 марта 2025 года
Monterey Mushrooms	Пищевая промышленность, производство / Производитель грибов	США	Утечка персональных данных Шифровальщики	18 сентября 2025 года 2 августа 2025 года Payouts King
Georgetown Brewing Company	Пищевая промышленность, производство / Крафтовая пивоварня	США	Утечка персональных данных Шифровальщики	26 сентября 2025 года 22 августа 2025 года INC

T.R.A. Industries Inc. / Huntwood Industries	Производство / Производитель деревянных шкафов	США	Утечка персональных данных Шифровальщики	26 сентября 2025 года 9 августа 2025 года Interlock
Tekni-Plex	Производство / Производитель в области материаловедения и упаковки	США	Утечка персональных данных Шифровальщики	24 сентября 2025 года 18 ноября 2024 года RansomHub
All States Materials Group	Производство / Производитель дорожных материалов	США	Утечка персональных данных Шифровальщики	23 сентября 2025 года 22 августа 2025 года Play
Champagne Logistics	Логистика и транспорт / Логистическая, транспортная компания, цепочки поставок	США	Утечка персональных данных	8 сентября 2025 года
Phoenix Products	Производство / Производитель осветительного оборудования	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	11 сентября 2025 года 31 июля 2025 года
Phoenix Mechanical Contracting	Строительство и инжиниринг / Монтажные и строительные услуги в сфере сантехники, электрики, отопления, природного газа, кондиционирования воздуха	США	Утечка персональных данных	9 сентября 2025 года
Gale Associates	Строительство и инжиниринг / Консалтинговая инжиниринговая компания	США	Утечка персональных данных	12 сентября 2025 года 4 июня 2025 года
ENCON Heating & Air Conditioning	Строительство и инжиниринг / Проектирование, монтаж	США	Утечка персональных данных	12 сентября 2025 года

	и обслуживание систем отопления, вентиляции и кондиционирования (HVAC)		Шифровальщики	21 февраля 2025 года RansomHub
MGM Transformers	Производство / Производитель трансформаторов	США	Утечка персональных данных Шифровальщики	17 сентября 2025 года Akira
CSJB Holdings	Производство / Производитель литейной продукции	США	Утечка персональных данных	18 сентября 2025 года
Minaris Advanced Therapies	Фармацевтика, производство / Производство по стандарту GMP, производство клеточной и генной терапии	США	Утечка персональных данных	8 сентября 2025 года 3 октября 2024 года
Hello Cake	Производство / Производитель товаров для сексуального здоровья	США	Утечка персональных данных	19 сентября 2025 года 25 июля 2025 года
PCE Constructors	Строительство и инжиниринг / Компания в сфере промышленного строительства	США	Утечка персональных данных	19 сентября 2025 года
National Molding	Производство / Производитель пластмасс	США	Утечка персональных данных	18 сентября 2025 года
Volvo Group North America	Автомобилестроение, производство / Производитель автотранспортных средств	США	Утечка персональных данных Шифровальщики	24 сентября 2025 года DataCarry
Braun Electric Company	Энергетика, производство / Электромонтажные и КИПиА-подрядные работы для нефтегазовой отрасли	США	Утечка персональных данных Шифровальщики	24 сентября 2025 года 26 июля 2025 года Qilin

Dulany Industries	Химическая промышленность, производство / Производитель удобрений	США	Утечка персональных данных	25 сентября 2025 года
G&H Wire Company (G&H Orthodontics)	Производство / Производитель ортодонтической продукции	США	Утечка персональных данных	10 сентября 2025 года
Belkorp	Логистика и транспорт / Логистика, транспорт, цепочки поставок, розничная торговля	США	Утечка персональных данных Шифровальщики	29 сентября 2025 года 18 апреля 2025 года Teamxxx
Channel Fish	Пищевая промышленность, производство / Производитель рыбы	США	Утечка персональных данных	10 сентября 2025 года
Sunsweet Growers	Пищевая промышленность, производство / Производитель чернослива	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	3 сентября 2025 года 11 декабря 2024 года RansomHub
Karndean Designflooring	Производство / Производитель виниловой плитки для пола	США	Утечка персональных данных	30 сентября 2025 года 5 июля 2025 года CRYPTO24
Talisman civil consultants	Строительство и инжиниринг / Компания гражданского строительства	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	5 сентября 2025 года 6 мая 2025 года Qilin
Miller Construction	Строительство и инжиниринг / Строительная компания	США	Утечка персональных данных Шифровальщики	11 сентября 2025 года 3 июля 2025 года
Jaguar Land Rover	Автомобилестроение, производство /	Велико-британия	Отказ ИТ-систем, нарушение операционной	1 сентября 2025 года

	Производитель автомобилей		деятельности, отказ сервисов, Шифровальщики	30 августа 2025 года Scattered Lapsus$ Hunters
Bridgestone Americas	Производство / Производитель шин	США	Нарушение операционной деятельности	2 сентября 2025 года
Maryland Transit Administration	Логистика и транспорт / Управление работой общественного транспорта	США	Отказ сервисов, утечка данных Шифровальщики	25 августа 2025 года Rhysida
Collins Aerospace (аэропорты Лондона (Хитроу), Берлина, Брюсселя и Дублина)	Логистика и транспорт, аэрокосмическая промышленность, оборонная промышленность / Компания в области авиационных и оборонных технологий	США Велико-британия Германия Бельгия Ирландия	Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов, цепочки поставок/ доверенные партнеры Шифровальщики	20 сентября 2025 года 19 сентября 2025 года
Stellantis	Автомобилестроение, производство / Производитель автомобилей	Нидерланды США	Утечка персональных данных Вымогательство	21 сентября 2025 года ShinyHunters
Chroma ATE	Электроника, производство / Производитель электронных контрольно-измерительных приборов	Тайвань	Отказ ИТ-систем, нарушение операционной деятельности Шифровальщики	17 сентября 2025 года Warlock
Transart Graphics	Производство / Компания трафаретной печати	Тайвань	Отказ ИТ-систем	8 сентября 2025 года
Morrisroe	Строительство и инжиниринг / Строительная компания	Велико-британия	Утечка персональных данных	19 сентября 2025 года 14 сентября 2025 года

Thermofin	Производство / Производитель теплообменников	Германия Китай Польша	Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов, утечка персональных данных Шифровальщики	22 сентября 2025 года Sarcoma
Okuma Europe	Производство / Станки с ЧПУ и оптимизация процессов	Германия Япония	Утечка персональных данных Отказ ИТ-систем Шифровальщики	25 сентября 2025 года
Thai Diamond & Zebra Electric	Электроника, производство / Производитель электронных компонентов	Таиланд Япония	Отказ ИТ-систем Шифровальщики	26 сентября 2025 года 8 сентября 2025 года
Refresco	Пищевая промышленность, производство / Производитель напитков	Германия	Нарушение операционной деятельности, отказ сервисов	25 сентября 2025 года
Boliden / Miljödata	Горнодобывающая промышленность, производство / Компания в области металлургии, горнодобычи и выплавки	Швеция	Утечка персональных данных, цепочки поставок/ доверенные партнеры Шифровальщики	15 сентября 2025 года 23 августа 2025 года DataCarry
LG Balakrishnan & Bros	Производство / Производитель трансмиссионных изделий	Индия	Отказ ИТ-систем Шифровальщики	30 сентября 2025 года Medusa
Kering S.A.	Производство / Производитель одежды класса люкс	Франция	Утечка персональных данных	15 сентября 2025 года ShinyHunters

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

Kaspersky ICS CERT ics-cert@kaspersky.com