Kaspersky ICS CERT

kaspersky

Краткий обзор основных инцидентов в области промышленной кибербезопасности за четвертый квартал 2024 года

08.04.2025

Версия 1.0

В четвертом квартале 2024 года жертвами было публично подтверждено 107 инцидентов. Все эти инциденты включены в таблицу в конце обзора, а некоторые из них описаны подробно.

Краткая информация

- По меньшей мере половина жертв (50%) **столкнулась с атаками вымогателей**.
- В 12% случаев жертвы сообщили о **нарушении операционной деятельности**, а в 19% — об **отказе ИТ-систем** в результате инцидента.
- **Страны с наибольшим количеством зарегистрированных инцидентов:**
  - США: 81% (87 инцидентов)
  - Германия: 6% (7 инцидентов)
  - Япония: 4% (4 инцидента)
- В этом квартале зафиксированы инциденты в нескольких странах, где подобные случаи нечасто подтверждают публично: в **Коста-Рике, Люксембурге, Латвии, Буркина-Фасо** и **Пакистане**.
- Особое внимание хотелось бы обратить на следующее:
  - Мы знаем, что кибератаки наносят ущерб бизнесу. В сочетании с другими проблемами киберинцидент может подтолкнуть руководство компании к решению объявить о ее неплатежеспособности. В этом квартале было два таких объявления — оба были сделаны производственными компаниями (одна из Германии, другая из США).
  - Кибератаки на ключевых поставщиков технологий или материалов потенциально могут иметь разрушительные последствия для всего сектора. В одном из таких случаев команда по реагированию на инциденты заявила, что ей удалось минимизировать последствия атаки и предотвратить масштабную катастрофу.
  - Значительные ресурсы, выделенные на обеспечение кибербезопасности, не всегда означают, что можно спать спокойно. В этом квартале по меньшей мере три крупные международные компании подтвердили факт компрометации: никто не защищен на 100%.
  - По меньшей мере три организации, связанные с критической инфраструктурой, столкнулись с отказом внутренних и публичных сервисов в результате атаки. В одном из случаев коммунальная компания была вынуждена перейти на ручное управление.

  - Атака на поставщика продуктов и услуг в сфере управления автопарком привела к отказам в обслуживании, затронувшим его клиентов, один из которых — британское подразделение DHL.
  - Результатом атаки на компанию общественного транспорта в Питтсбурге стали задержки поездов и сбои в работе некоторых цифровых сервисов для пассажиров.
  - В двух случаях сразу две группы злоумышленников взяли на себя ответственность за одну и ту же атаку с применением программ-вымогателей.
- Полный список инцидентов, подтвержденных жертвами в четвертом квартале 2024 года, приведен в Приложении.

Октябрь

- Dynapar
- Foley Material Handling Company Inc.
- Sierra Construction Company, Inc.
- Saeilo Enterprises, Inc.
- Industrial Scientific Corporation
- Dover Motion
- Pacific Scientific Energetic Materials Company LLC
- Setra Systems, Inc.
- Advanced Sterilization Products, Inc.
- American Water Works Company, Inc.
- Fluke Corporation
- TDX Construction Corporation
- Casio
- Kulicke and Soffa Industries
- Aero Simulation Inc.
- The Plastic Bag Company
- Polar
- Hubergroup
- Nidec
- Karat Packaging Inc.
- Yorozu
- Eastern Shipbuilding Group
- Saneamento Básico do Estado de São Paulo (Sabesp)
- MMI Services Inc.
- Wise Construction Corporation
- Berry Bros. General Contractors, Inc.
- S. Lichtenberg & Co
- Van Wingerden International, Inc.
- Rogers Foam Corporation
- Stadtwerke Burg
- EPI Breads
- Wright Consulting Engineers, LLC
- Elastec, Inc.
- SelectBlinds
- Microlise Group PLC

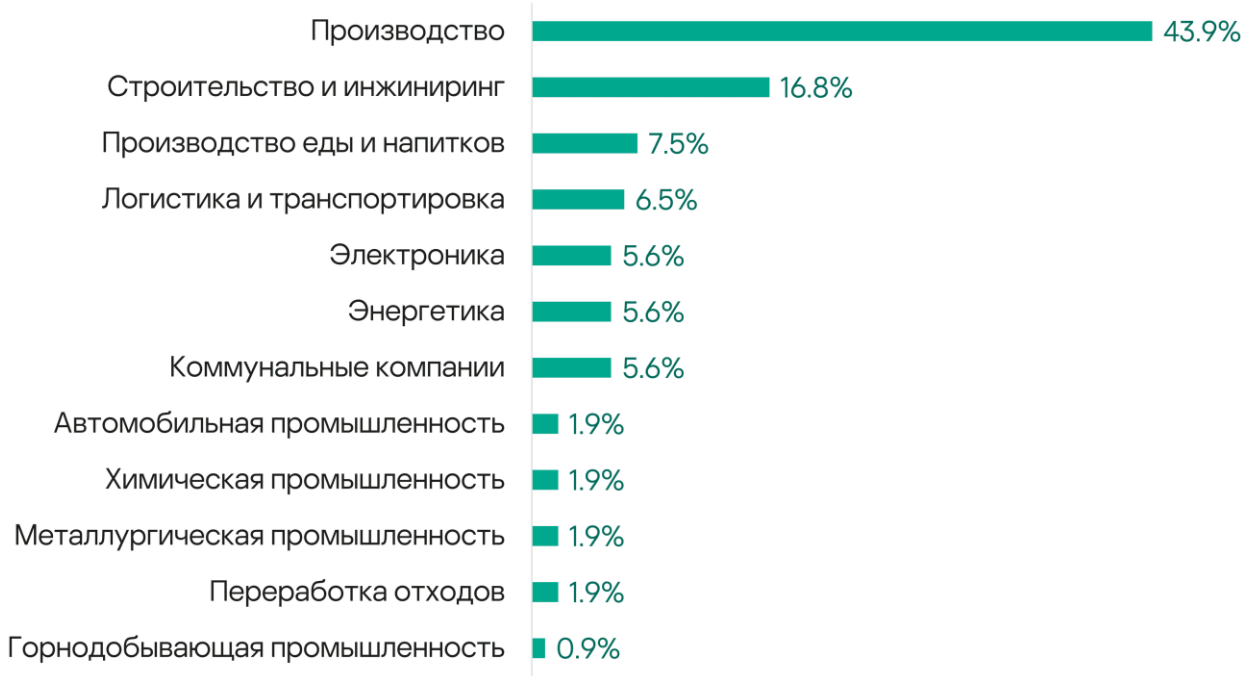
Ноябрь

- Kemlon Products & Development Group
- Mauser Packaging Solutions
- TetraSoft
- Great Star Tools USA Inc.
- The Manual Woodworkers and Weavers Inc.
- Schneider Electric
- Diligent Delivery Systems
- Fiskars Group
- Phoenix Footwear Group
- Denkai America Inc.
- Newpark Resources, Inc.
- English Construction Company
- J.S. McCarthy Co., Inc.
- American Construction Corp.
- Misionero Vegetables
- Pallet Logistics of America
- Tibber
- Harmac Medical Products Inc.
- SOFITEX
- Kreisel GmbH & Co.
- Mark Cerrone Inc.
- American Gypsum LLC
- VOSSKO
- Dome Construction Corporation
- ShoreMaster, LLC
- Tedder Industries LLC
- Dynamic Air Inc.
- Ariel Corporation
- Graphique De France LTD
- RECOPE
- Eichelberger Construction Inc.
- New River Electrical Corporation
- Universal Pegasus International LLC
- Medion AG
- Stoli Group USA/Kentucky Owl
- Dewan Farooque Motors Limited

Декабрь

- BNBuilder
- Fermented Food Holdings Inc.
- ENGlobal
- Overseas Shipholding Group Inc.
- Delmar
- American Engineers Inc.
- Crowley Maritime Corporation
- Wheels Manufacturing, LLC
- Kurita America Inc.
- Artivion, Inc.
- Electrica Group
- Rumpke
- Ames Goldsmith Corporation
- Krispy Kreme Inc.
- Maggie Sottero Designs
- Hyperice Inc.
- OLA Consulting Engineers
- Keeco, LLC
- Pier Foundry & Pattern Shop Inc.
- Pirelli Tire LLC
- Fitzemeyer & Tocci Associates, Inc.
- PS Logistics
- Norwex USA, Inc.
- General Dynamics, Corp.
- R. Zoppo Corp.
- DBM Global, Inc.
- Pittsburgh Regional Transit
- Hubbard-Hall Inc.
- CR&R Inc.
- Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH
- Peikko
- Tycon Medical Systems, Inc.
- Troxler Electronic Laboratories Inc.
- Central Valley Meat Co, Inc.
- LBX Company LLC

2024



Атаки, приведшие к объявлению о неплатежеспособности

Kreisel

Производственный сектор

Нарушение операционной деятельности, неплатежеспособность

Шифровальщики

Немецкая компания Kreisel GmbH & Co., специализирующаяся на производстве оборудования для работы с сыпучими материалами, 19 ноября 2024 года подала заявление о несостоятельности. Текущие финансовые трудности компании в первую очередь связаны с ростом расходов и снижением доходов из-за последствий пандемии COVID-19, увеличением цен на сырье и энергоносители, а также с кибератакой, произошедшей в феврале 2024 года. Из-за атаки операционная деятельность компании была значительно ограничена в течение нескольких недель. По сведениям немецкой прессы, компания получила по факсу письмо от вымогателей, но отказалась платить выкуп. Никаких подробностей об атаке, включая имя взявшей ответственность за нее группы, не поступало.

Stoli Group

Производственный сектор, пищевая промышленность

Нарушение операционной деятельности, отказ ИТ-сервисов, утечка данных, банкротство

Шифровальщики

Американские дочерние компании люксембургского производителя водки Stoli Group — Stoli Group USA и Kentucky Owl — 29 ноября 2024 года подали заявление о несостоятельности в соответствии с Главой 11 Кодекса о банкротстве США. Это случилось спустя несколько месяцев после кибератаки вымогателей, которая привела к сбоям в работе компаний. В августе 2024 года произошли серьезные сбои в работе ИТ-инфраструктуры Stoli Group в результате утечки данных и атаки. Атака привела к значительным проблемам в работе всех подразделений Stoli Group, включая Stoli USA и Kentucky Owl, так как корпоративная система управления ресурсами предприятия была отключена, и большинство внутренних процессов компании, включая бухгалтерский учет, пришлось выполнять вручную. Согласно заявлению, полное восстановление этих систем ожидалось не ранее первого квартала 2025 года, а кибератака стала одной из нескольких причин, побудивших компании искать защиту от кредиторов. Кроме того, инцидент не позволил американским подразделениям Stoli Group предоставить финансовые отчеты кредиторам.

Наиболее серьезные последствия, предотвращенные командами по реагированию на инциденты

TetraSoft

Энергетика, горно-добывающая промышленность

Нарушение операционной деятельности, отказ сервисов, атака на цепочку поставок / доверенного партнера

В этом квартале была обнаружена и предотвращена целенаправленная кибератака на российскую компанию TetraSoft, занимающуюся удаленным мониторингом добычи углеводородов и бурения скважин. Специалисты экспертного центра безопасности Positive Technologies провели расследование инцидента и реагирование на него, не допустив его влияния на российскую добывающую отрасль. Инцидент был классифицирован как атака на цепочку поставок, направленная против добывающей отрасли. Если бы эта атака достигла своей цели, она могла бы привести к перебоям в поставках углеводородов по внутренним и международным контрактам. В ходе расследования было установлено, что первоначальное проникновение произошло в июле 2024 года, а первые действия атакующих в системах были зафиксированы в конце сентября — начале октября. Атака осуществлялась с использованием утилит удаленного доступа и управления серверами. Прямой ущерб от простоя TetraSoft оценивается более чем в 65 млн рублей, а затраты на восстановление внутренних сервисов уже превысили 25 млн рублей. При этом в компании не считают эту сумму окончательной.

Инциденты в крупных организациях

Schneider Electric

Энергетика, производственный сектор

Утечка персональных данных

Шифровальщики

Французский производитель энергетического оборудования и оборудования для промышленной автоматизации Schneider Electric 4 ноября подтвердил факт кибератаки, связанной с несанкционированным доступом к одной из внутренних платформ компании для управления проектами, размещенной в изолированной среде. Заявление было сделано после утверждения группы злоумышленников Grep (Hellcat) о краже 40 Гб данных и выдвижения ими требований о выкупе. Schneider Electric инициировала расследование инцидента и провела аудит своих внутренних платформ. Компания заявила, что ее продукция и услуги не пострадали. В разговоре с изданием BleepingComputer представители Grep сообщили, что получили доступ к серверу Jira компании Schneider Electric, использовав

скомпрометированные учетные данные. По их словам, после проникновения в систему они использовали MiniOrange REST API для сбора 400 000 строк пользовательских данных, среди которых 75 000 уникальных адресов электронной почты и полные имена сотрудников и клиентов Schneider Electric.

Medion

Производственный сектор, электронная промышленность

Нарушение операционной деятельности, отказ ИТ-систем, утечка данных

Шифровальщики

Немецкий поставщик электроники Medion AG (дочерняя компания китайской технологической корпорации Lenovo) стал жертвой кибератаки. Группа вымогателей Black Basta взяла на себя ответственность за атаку на Medion AG 18 декабря. По заявлению злоумышленников, опубликованному на их сайте, посвященном утечке данных, им удалось похитить около 1,5 Тб информации, включая финансовую и бухгалтерскую документацию, файлы проектов, данные разработки, а также персональные данные сотрудников. Первоначально Medion AG подтвердила факт инцидента ИТ-безопасности, вызванного действиями неизвестных внешних злоумышленников, опубликовав 28 ноября заявление, однако позже удалила его. В заявлении говорилось, что от атаки частично пострадали внутренние системы и розничные операции. Компания привлекла внешних специалистов для устранения последствий инцидента и выяснения его причин. Она поддерживала тесный контакт с соответствующими органами, однако связь с ней была возможна только в ограниченном объеме по телефону, а обрабатывать письменные запросы компания не имела возможности. 20 декабря Medion AG направила заявление редакции Golem.de, в котором сообщила, что 26 ноября столкнулась со сбоями в ИТ-системах, вызванными атакой программы-вымогателя, из-за которой в течение нескольких дней наблюдались проблемы в работе части внутренних систем и розничных магазинов.

Федеральное управление уголовной полиции Германии (BKA) и прокуратура Кельна вели расследование инцидента. Было установлено, что группа киберпреступников проникла в часть ИТ-систем Medion AG и похитила данные компании. Часть украденной информации была опубликована в даркнете, однако, согласно заявлению компании, там не было персональных данных клиентов. 20 декабря Medion AG разместила на своем сайте заявление о том, что ее ИТ-системы полностью восстановлены после сбоя, она вновь доступна по телефону, а письменные запросы снова будут обрабатываться. В то же время компания предупредила о возможных задержках в доставке заказов.

Casio

Производственный сектор, электронная промышленность

Утечка данных, утечка персональных данных, отказ сервисов, отказ ИТ-систем

Шифровальщики

Японский производитель электронных устройств Casio Computer Co., Ltd. подтвердил атаку вымогателей, в результате которой злоумышленники получили доступ к сети компании, нарушили работу ее систем и некоторых клиентских сервисов. Инцидент произошел 5 октября, компания сразу же сообщила о нем в соответствующие органы и привлекла экспертов по кибербезопасности для проведения расследования. Casio Computer Co., Ltd. приняла меры по укреплению своей безопасности и защите клиентских данных, а также обязалась улучшить протоколы безопасности для предотвращения подобных инцидентов в будущем. Согласно заявлению компании, злоумышленники, вероятно, получили доступ к персональным данным сотрудников, подрядчиков, деловых партнеров и соискателей, проходивших собеседования, а также к некоторой технической и конфиденциальной информации, включающей счета-фактуры и кадровые документы. Об этом Casio Computer Co., Ltd. уведомила Комиссию по защите личной информации. В обновлении от 21 октября компания сообщила, что из-за атаки возникли значительные задержки в доставке запчастей, а выполнение многих заказов было и вовсе отложено. Casio Computer Co., Ltd. приостановила прием заявок на ремонт персональных устройств и планировала возобновить полноценную работу к концу ноября.

Атаки на объекты критической инфраструктуры

Brazil Saneamento Básico do Estado de São Paulo

Водоснабжение, коммунальные услуги

Отказ ИТ-систем и сервисов

Шифровальщики

Бразильская коммунальная компания Saneamento Básico do Estado de São Paulo (Sabesp), обеспечивающая водоснабжение и очистку сточных вод в штате Сан-Паулу, стала жертвой кибератаки, что было подтверждено в письме CISO Advisor Brazil от 22 октября. В заявлении компании отмечается, что она незамедлительно приняла необходимые меры по обеспечению безопасности и контролю, а также реализовала план восстановления затронутых систем. Компрометации персональных данных выявлено не было. Системы водоснабжения, сбора и очистки сточных вод также не пострадали. Sabesp приложила все усилия для восстановления целостности своей цифровой сети, при этом предупредила о возможных задержках в обслуживании из-за нестабильности системы.

Согласно информации, опубликованной на сайте профсоюза работников санитарных служб Сан-Паулу (Sintaema), 17 октября у Sabesp возникли проблемы с доступом в интернет. В руководстве Sintaema пояснили, что с тех пор работала только система управления резервуарами, а доступ сотрудников к другим системам был возможен только через мобильные устройства или внешние сети. Даже государственный сервис Poupatempo, предоставляющий более 400 различных услуг, связанных с оформлением официальных документов, был недоступен в течение пяти дней из-за сбоя, который затронул все подразделения Sabesp по всей стране. Группа вымогателей RansomHouse взяла на себя ответственность за атаку.

Refinadora Costarricense de Petróleo

Энергетика, коммунальные услуги

Нарушение операционной деятельности, отказ сервисов

Шифровальщики

Коста-риканская энергетическая компания Refinadora Costarricense de Petróleo (RECOPE) 27 ноября подтвердила, что стала жертвой атаки вымогателей, из-за которой ей пришлось перейти на ручное управление своими системами, но заверила общественность, что инцидент не скажется на поставках топлива. Компания сообщила, что из-за атаки были отключены все цифровые системы, используемые для проведения платежей, поэтому осуществлять продажу топлива пришлось в ручном режиме. 27 ноября работа нефтеналивных терминалов была продлена до поздней ночи, а на следующий день она осуществлялась в расширенном режиме. RECOPE заявила, что работает совместно с Министерством науки, инноваций, технологий и телекоммуникаций (MICITT) Коста-Рики для устранения последствий атаки. 29 ноября президент RECOPE сообщила, что в День благодарения (28 ноября) в компанию прибыли специалисты по кибербезопасности из США, которые помогли постепенно восстановить некоторые системы. Однако руководство подчеркнуло, что компания продолжит использовать ручное управление до тех пор, пока не будет полностью гарантирована безопасность технологических процессов. Компания столкнулась с резким ростом спроса на топливо из-за опасений по поводу возможного дефицита газа и нефти. В течение выходных RECOPE расширила часы работы, чтобы обеспечить бесперебойную продажу топлива. 30 ноября компания объявила о стабилизации работы терминалов и гарантированном наличии топлива. Совместная работа RECOPE, MICITT, международных экспертов и Управления разведки и безопасности продолжалась для окончательного устранения последствий атаки. Группировка RansomHub взяла на себя ответственность за кибератаку на RECOPE.

Electrica Group

Энергетика, коммунальные услуги

Отказ сервисов

Шифровальщики

Румынская электрораспределительная компания Electrica Group 9 декабря объявила, что подверглась кибератаке, и заявила, что работает в тесном сотрудничестве с национальными органами по кибербезопасности для управления инцидентом и его разрешения. Компания подчеркнула, что ее критически важные системы не пострадали, а возможные сбои в обслуживании клиентов связаны с мерами по защите внутренней инфраструктуры. В соответствии с внутренними процедурами и действующими нормативными требованиями были активированы все необходимые протоколы реагирования. Министр энергетики Румынии сообщил в интервью местному новостному ресурсу, что компания подверглась атаке вымогателей, однако ее автоматизированные системы управления (SCADA) не пострадали. 11 декабря Национальное управление кибербезопасности Румынии (DNSC) заявило, что за атакой стоит группа вымогателей Lynx. По данным DNSC, критически важные системы энергоснабжения работали в штатном режиме. Чтобы помочь службам безопасности других компаний обнаружить возможные признаки компрометации в своих сетях, DNSC опубликовало правила YARA и индикаторы компрометации.

Центр интернет-безопасности опубликовал отчет о растущей угрозе подобных атак на организации, работающие в сфере коммунальных услуг, причем особое внимание в документе было уделено деятельности группы вымогателей Lynx (отслеживаемой Microsoft как Storm-2113), а также приведены индикаторы компрометации, связанные с ее атаками.

Другие крупные инциденты, представляющие интерес

Microlise

Транспорт, логистика

Отказ ИТ-систем, отказ сервисов

Шифровальщики

Британская компания Microlise, поставщик решений в области телематики и управления автопарком, пострадала от кибератаки, которая привела к сбоям в доставке службой DHL товаров для ритейлера NISA. По сообщению NISA, в результате атаки были полностью удалены данные с серверов, обслуживающих систему отслеживания поставок DHL. Представитель логистической компании подтвердил факт инцидента, но уточнил, что собственные системы DHL не пострадали. NISA пояснила, что из-за кибератаки у DHL не было возможности отслеживать статус своих доставок.

Издание Motor Transport сообщило, что атака затронула и другие компании, но ни одна из них, включая организации, использующие программное обеспечение Microlise, не дала комментариев. По данным Financial Times, транспортная компания Serco, обеспечивающая перевозку заключенных для Министерства юстиции Великобритании, также пострадала от атаки: были отключены системы отслеживания транспортных средств, тревожные сигналы, навигация и уведомления о предполагаемом времени прибытия. В заявлении, поданном на Лондонскую фондовую биржу 31 октября, Microlise сообщила, что обнаружила несанкционированную активность в своих сетях, которая привела к сбоям в работе и отключению значительной части ее сервисов. В обновленном заявлении от 18 ноября компания подтвердила, что уведомила международные органы о факте хищения корпоративных данных из головного офиса и продолжает сотрудничество с правоохранительными органами в связи с инцидентом. При этом компания подчеркнула, что никакие данные клиентских систем не были скомпрометированы. Ответственность за атаку на Microlise взяла на себя группа вымогателей SafePay.

Pittsburgh Regional Transit

Транспорт

Нарушение операционной деятельности, отказ сервисов, утечка персональных данных

Шифровальщики

Компания Pittsburgh Regional Transit (PRT) организовала расследование атаки вымогателей, которая была обнаружена 19 декабря и вызвала сбои в работе общественного транспорта. Временные перебои затронули рельсовый транспорт, но в целом транспортные службы работали в штатном режиме. Атака негативно повлияла на пассажирские сервисы, в том числе работу Центра обслуживания клиентов PRT, который временно не мог принимать и обрабатывать проездные пенсионеров и детей. По данным местных СМИ, из-за атаки поезда задерживались более чем на 20 минут. В ходе расследования инцидента выяснилось, что злоумышленники могли получить доступ к персональным данным, включая номера социального страхования и водительских удостоверений как соискателей, так и бывших и действующих сотрудников компании. К расследованию инцидента и реагированию на него были привлечены правоохранительные органы и специалисты по кибербезопасности.

Инциденты, в которых ответственность за атаку взяли на себя сразу две группы

Nidec

Производственный сектор

Утечка данных, утечка персональных данных

Шифровальщики

Японский производитель электродвигателей Nidec подтвердил, что в результате атаки вымогателей в августе 2024 года были похищены различные коммерческие и внутренние документы. Согласно заявлениям компании, опубликованным на ее веб-сайте, инцидент затронул ее вьетнамское подразделение Nidec Precision (NPCV) и был обнаружен после того, как злоумышленники связались с Nidec и потребовали выкуп. Атака была ограничена сетью NPCV и не привела к компрометации других подразделений организации. По данным компании, злоумышленники похитили у NPCV в общей сложности 50 694 файла, включая внутреннюю документацию, связанную с «зелеными» закупками, охраной труда, политиками компании, ее коммерческими операциями, а также переписку с деловыми партнерами. В Nidec отметили, что проникновение скорее всего произошло после того, как атакующие скомпрометировали учетные данные общего доменного аккаунта NPCV, используя их, вошли на сервер и получили доступ к файлам, разрешенным для данного аккаунта. В ответ на атаку Nidec и ее дочерние компании провели тщательное расследование, пересмотрели права доступа к серверам и сменили пароли. Кроме того, NPCV приостановила использование VPN-приложения, которое, предположительно, использовали злоумышленники. В сентябре 2024 года NPCV подала уведомление об инциденте в Департамент кибербезопасности и предотвращения преступлений в сфере высоких технологий Министерства общественной безопасности Вьетнама в соответствии с Законом о защите персональных данных.

Сразу две группы вымогателей включили компанию в свои списки жертв на сайтах, посвященных утечке данных: 8base — в июне, а Everest — в августе. В уведомлении Nidec об инциденте содержится предположение, что за атакой стоит группа Everest, так как эта группа в начале августа выложила в сеть якобы похищенные у компании данные.

CR&R

Производственный сектор, переработка отходов

Отказ ИТ-систем, утечка персональных данных

Шифровальщики

Американская компания CR&R Inc., занимающаяся сбором и переработкой отходов, уведомила генеральных прокуроров штатов Мэн и Вермонт о том, что столкнулась с нарушением безопасности данных, в результате чего в руки злоумышленников могли попасть конфиденциальные персональные данные, хранившиеся в системах компании. Согласно уведомлению, примерно 13 декабря 2022 года компания столкнулась с сетевым сбоем, затронувшим некоторые системы. CR&R Inc. начала расследование, которое было завершено 30 октября 2024 года. Компания подтвердила, что неавторизованные сторонние лица могли получить несанкционированный доступ к конфиденциальной информации в ее системах в ходе инцидента, произошедшего 19 октября 2022 года. В связи с этим CR&R Inc. приступила к анализу данных, чтобы определить масштабы утечки и выявить пострадавших от нее лиц. Компания не раскрыла конкретный характер скомпрометированных персональных данных. 26 декабря 2024 года она разослала уведомления о нарушении безопасности данных пострадавшим. Группа вымогателей Vice Society взяла на себя ответственность за атаку на CR&R Inc. 6 ноября 2022 года. Спустя месяц, в декабре 2022 года группа вымогателей BlackCat/ALPHV также включила компанию в список своих жертв.

Атаки, которые привели к нарушению операционной деятельности

Hubergroup

Производственный сектор

Нарушение операционной деятельности, отказ ИТ-систем и сервисов

Немецкий производитель красок для печати Hubergroup стал жертвой кибератаки. По сообщениям местных СМИ, операционная деятельность и производство, а также доступ в интернет в компании были ограничены почти на две недели. Hubergroup подтвердила факт инцидента в СМИ, хотя конкретные последствия остались неизвестными. Представитель компании заявил, что атака затронула отдельные региональные ИТ-системы, подчеркнув, что системы безопасности компании незамедлительно отреагировали на угрозу. Благодаря этим мерам атака не коснулась значительной части подразделений Hubergroup в других странах. Пострадавшие системы были временно изолированы, чтобы предотвратить дальнейшее распространение атаки. ИТ-команда компании тесно взаимодействовала с внешними экспертами по кибербезопасности, чтобы как можно быстрее восстановить региональные системы. Сразу после атаки

клиенты и сотрудники были проинформированы о возможных временных ограничениях в работе и кратковременных задержках в производстве и доставке.

Artivion

Производственный сектор

Нарушение операционной деятельности, отказ сервисов, утечка данных

Американский производитель медицинского оборудования Artivion, Inc. 9 декабря сообщил об инциденте с безопасностью данных, подав отчет по форме 8-K в Комиссию по ценным бумагам и биржам США. Инцидент произошел 21 ноября и касался получения несанкционированного доступа и шифрования файлов. В ходе реагирования компания перевела часть систем в автономный режим, инициировала расследование и привлекла внешних консультантов, в том числе юристов, специалистов по кибербезопасности и криминалистике для локализации, оценки и устранения последствий инцидента. Artivion, Inc. восстановила свои системы в кратчайшие сроки и подготовила все необходимые уведомления. Компания продолжила предоставлять продукцию и услуги клиентам, несмотря на сбои в процессах, связанных с оформлением заказов и доставки, а также в некоторых внутренних операциях, которые в основном были устранены. В отчете отмечено, для Artivion, Inc. сохранились риски, в том числе связанные с последствиями задержек с восстановлением, поэтому компания не может гарантировать отсутствие материального ущерба вследствие атаки в будущем.

Peikko

Производственный сектор

Нарушение операционной деятельности, отказ сервисов, отказ ИТ-систем, утечка персональных данных

Шифровальщики

Финский производитель строительных материалов Peikko столкнулся с кибератакой в конце декабря. В заявлении компании от 30 декабря указывалось, ее сайты, электронная почта и телефоны работали в штатном режиме, равно как программы для дизайна, однако некоторыми инструментами и системами сотрудники пользоваться не могли. На следующий день Peikko проинформировала, что процесс восстановления идет успешно: снова стали доступны инструменты для 3D-моделирования Tekla и совместного проектирования в облаке Tekla Model Sharing. Несмотря на это компания была вынуждена ограничить производство и поставку продукции на нескольких из своих 12 заводов. Кроме того, она признала, что злоумышленникам, вероятно, удалось получить доступ к некоторым данным клиентов и украсть их. 2 января Peikko сообщила, что использует решение для управления процессами предприятия Microsoft Dynamics 365, как и ее зарубежные подразделения в 21 стране. Хотя некоторые функции платформы были недоступны, в целом она везде функционировала корректно. Peikko

продолжала производить и отгружать продукцию. Интересно, что некоторые иностранные подразделения компании, использующие более старую ERP-систему, избежали проблем, тогда как другим пришлось временно перейти на ручное управление операциями. 9 января Peikko проинформировала, что ее подразделения возобновили работу в обычном режиме. Компания заявила об инциденте в полицию и другие компетентные органы, включая Национальный центр кибербезопасности Финляндии. На следующий день группировка Akira добавила Peikko в список жертв на сайте утечек данных, утверждая, что было похищено 30 Гб информации.

Newpark

Энергетика, строительство

Нарушение операционной деятельности, отказ ИТ-систем

Шифровальщики

Американский поставщик решений и оборудования для нефтегазовой отрасти Newpark Resources, Inc. 29 октября обнаружил кибератаку вымогателей, в результате которой третьи лица получили доступ к некоторым ИТ-системам. Последствиями атаки стали сбои в работе и ограничение доступа к отдельным компонентам информационных систем и бизнес-приложений, касающихся в частности финансовой и операционной отчетности. Тем не менее, производство и полевые работы продолжались практически в обычном режиме, с соблюдением установленных процедур простоя. Newpark Resources, Inc. сообщила об инциденте в отчете по форме 8-K, поданном в Комиссию по ценным бумагам и биржам США.

VOSSKO

Производственный сектор, пищевая промышленность

Нарушение операционной деятельности, отказ ИТ-систем

Шифровальщики

Немецкий производитель мясных полуфабрикатов VOSSKO стал жертвой целевой кибератаки вымогателей, которая зашифровала информацию во внутренних системах и базах данных. Вредоносное ПО нарушило операционную деятельность, но впоследствии системы и производство были восстановлены. ИТ-отдел компании при активной поддержке внешних специалистов справился с проблемой. В первые дни к расследованию были привлечены полиция, в том числе уголовная, специалисты по информационной безопасности и криминалистике. Ответственность за атаку на VOSSKO взяла на себя группа вымогателей Black Basta. Предполагается, что было зашифровано 800 Гб данных, включая финансовые сведения, личные данные сотрудников и документы, а также проектную документацию.

Ingenieurbüro Fritz Spieth

Строительство и инжиниринг

Нарушение операционной деятельности, отказ ИТ-систем

Шифровальщики

Немецкая инжиниринговая компания Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH стала жертвой целевой кибератаки. Сразу после ее выявления руководство проинформировало власти и подало жалобу. Одновременно все ИТ-системы были отключены или изолированы для обеспечения безопасности клиентов, поставщиков и сотрудников. Благодаря последовательному выполнению протокола безопасности и плана действий в подобных ситуациях компания вернулась к нормальной работе. Независимые ИТ-эксперты не нашли доказательств заражения сайтов компании и электронной почты. 19 ноября группа вымогателей Safepay включила Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH в список своих жертв.

Атаки, которые привели к отказу ИТ-систем

Stadtwerke Burg

Энергетика, коммунальные службы

Отказ ИТ-систем, отказ ИТ-сервисов

Немецкая энергосбытовая компания Stadtwerke Burg 29 октября разместила на своем сайте сообщение о том, что с ней снова можно связаться по электронной почте и через онлайн-центр. В рамках мер противодействия кибератаке 22 августа компания отключила доступ ко всем своим ИТ-сервисам и изолировала атакованные системы. Они были тщательно проверены и восстановлены совместными усилиями компании, поставщиков ИТ-услуг и приглашенных экспертов по цифровой криминалистике. В октябре было объявлено, что большинство систем уже возвращены в рабочее состояние, персональные данные защищены, а электроэнергия поставлялась клиентам без перебоев. По итогам инцидента Stadtwerke Burg заявила о планах дальнейшего усиления защиты своих ИТ-систем путем введения более строгих требований к паролям и повышения уровня осведомленности сотрудников относительно рисков, связанных с загрузкой вложений из электронных писем. Согласно заявлению Stadtwerke Burg, сделанному в сентябре, инцидент затронул и остальных участников рынка, например, невозможно было переключиться с другого поставщика энергии на Stadtwerke Burg.

ENGlobal

Энергетика, строительство и инжиниринг

Отказ ИТ-систем

Американская специализированная инжиниринговая компания ENGlobal Corporation, занимающаяся разработкой автоматизированных систем управления для энергетической отрасли, 25 ноября обнаружила инцидент безопасности, а 2 декабря подала соответствующий отчет по форме 8-K в Комиссию по ценным бумагам и биржам США. В ходе предварительного расследования выяснилось, что злоумышленники получили доступ к ИТ-системе компании и зашифровали некоторые файлы. После обнаружения несанкционированного доступа компания незамедлительно приняла меры по локализации, оценке и устранению последствий инцидента, начав внутреннее расследование, пригласив внешних специалистов по кибербезопасности и ограничив доступ к ИТ-системе. Работа системы была ограничена основными бизнес-операциями, а точные сроки полного восстановления на момент подачи отчета оставались неопределенными.

Dewan Farooque Motors Limited

Автомобиле-строение, производствен-ный сектор

Отказ ИТ-систем, отмена заседания совета директоров

Пакистанский производитель автомобилей Dewan Farooque Motors Limited подвергся кибератаке, в результате которой были повреждены данные и выведены из строя серверы. Инцидент привел к отмене заседания совета директоров, о чем компания уведомила Пакистанскую фондовую биржу 29 ноября. В сообщении говорится, что заседание отложено до тех пор, пока не будут восстановлены информационная система и финансовые данные за первый квартал, завершившийся 30 сентября 2024 года, а это потребует значительного времени.

Приложение. Полный список подтвержденных инцидентов

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Производство	Nidec	Производитель электро-двигателей	Япония	Утечка данных, утечка персональных данных Шифровальщики	17 октября 12 августа	8base Everest
Производство	Polar	Производитель смарт-часов	Финляндия	Утечка данных, утечка персональных данных, отказ ИТ-сервисов	11 октября	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Производство	Karat Packaging Inc.	Производитель упаковки для напитков и продуктов питания	США		18 октября	
Производство	Hubergroup	Производитель полиграфических красок	Германия	Нарушение операционной деятельности, отказ ИТ-систем и сервисов	11 октября	
Производство	Eastern Shipbuilding Group	Судостроительная компания	США	Утечка персональных данных Шифровальщики	21 октября 1 февраля	LockBit
Производство	Saeilo Enterprises, Inc.	Подрядчик по производству на станках с ЧПУ и производитель огнестрельного оружия	США	Утечка персональных данных Шифровальщики	3 октября 8 августа	Metaencryptor
Производство	Rogers Foam Corporation	Производитель пеноматериалов по спецификации заказчика	США	Утечка персональных данных	28 октября 23 сентября	
Производство	Elastec, Inc.	Производитель оборудования для ликвидации разливов нефтепродуктов и загрязнений поверхностных вод	США	Утечка персональных данных	31 октября 4 июня	
Производство	S. Lichtenberg & Co	Производитель штор, драпировок и домашнего декора	США	Утечка персональных данных	24 октября 30 августа	
Производство	SelectBlinds	Производитель жалюзи и оконных штор	США	Утечка персональных данных	31 октября 7 января 2024 г.	
Производство	Industrial Scientific Corporation	Производитель газоанализато-ров	США	Утечка персональных данных	3 октября 25 января 2023 г.	
Производство	Dover Motion	Производитель промышленных систем для обеспечения точного перемещения	США	Утечка персональных данных	3 октября 25 января 2023 г.	
Производство	Aero Simulation Inc.	Производитель авиасимуляторов для государственных и военных структур	США	Утечка персональных данных	10 октября 1 февраля 2023 г.	
Производство	Fiskars Group	Глобальный разработчик и производитель товаров для дома	Финляндия США	Утечка персональных данных Шифровальщики	6 ноября 31 марта	Akira
Производство	Phoenix Footwear Group	Производитель обуви	США	Утечка персональных данных	6 ноября	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Производство	The Manual Woodworkers and Weavers Inc.	Производитель текстильных изделий	США	Утечка персональных данных	4 ноября 4 июля	
Производство	Dynapar	Производитель энкодеров, резольверов и систем мониторинга состояния	США	Утечка персональных данных	Октябрь	
Производство	Pacific Scientific Energetic Materials Company LLC	Производитель пиротехнических компонентов для критических систем	США	Утечка персональных данных	3 октября 25 января 2023 г.	
Производство	SOFITEX	Производитель хлопчатобумажной текстильной продукции	Буркина-Фасо	Отказ ИТ-систем	19 ноября 16 ноября	
Производство	The Plastic Bag Company	Производитель упаковочной продукции	Австралия	Утечка данных Шифровальщики	10 октября	Sarcoma
Производство	Harmac Medical Products Inc.	Производитель одноразовых медицинских изделий	США	Утечка персональных данных	15 ноября 13 сентября	
Производство	American Gypsum LLC	Производитель строительных материалов	США	Утечка персональных данных	22 ноября 24 мая	
Производство	ShoreMaster, LLC	Производитель причального оборудования	США	Утечка персональных данных Шифровальщики	26 ноября 4 августа	Akira
Производство	Kemlon Products & Development Group	Производитель электрических разъемов, датчиков, зондов и сопутствующих компонентов для агрессивных сред	США	Утечка персональных данных Шифровальщики	1 ноября	Space Bears
Производство	Foley Material Handling Company Inc.	Производитель промышленного оборудования и поставщик услуг	США	Утечка персональных данных	Октябрь 14 мая	
Производство	Mauser Packaging Solutions	Производитель упаковочных решений	США	Утечка персональных данных	Ноябрь	
Производство	Great Star Tools USA Inc.	Производитель инструментов	США	Утечка персональных данных	Ноябрь 2 августа 2023 г.	
Производство	Dynamic Air Inc.	Производитель решений для транспортировки материалов	США	Утечка персональных данных	27 ноября 29 августа	
Производство	Tedder Industries LLC	Производитель кобур для скрытого ношения оружия и аксессуаров	США	Утечка персональных данных	26 ноября 7 августа	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Производство	Ariel Corporation	Производитель газовых компрессоров	США	Утечка персональных данных	27 ноября 20 июня	
Производство	Artivion, Inc.	Производитель медицинских устройств	США	Нарушение операционной деятельности, отказ сервисов, утечка данных Шифровальщики	9 декабря 21 ноября	
Переработка отходов, производство	Rumpke	Компания по утилизации и переработке отходов	США	Утечка персональных данных Шифровальщики	10 декабря 20 июля	Hunters International
Производство	Peikko	Производитель строительных материалов	Финляндия	Нарушение операционной деятельности, отказ сервисов, отказ ИТ-систем, утечка персональных данных Шифровальщики	30 декабря	Akira
Производство	Kreisel GmbH & Co.	Производитель систем для работы с сыпучими материалами	Германия	Нарушение операционной деятельности, Неплатеже-способность Шифровальщики	19 ноября Февраль	
Производство	Keeco, LLC	Производитель текстильных изделий для дома	США	Утечка персональных данных	17 декабря 28 марта 2024	
Производство	Maggie Sottero Designs	Дизайнер свадебных платьев	США	Утечка персональных данных	12 декабря 3 июня	
Производство	Norwex USA, Inc.	Производитель чистящих средств	США	Утечка персональных данных	23 декабря 11 декабря	
Переработка отходов, производство	CR&R Inc.	Компания по сбору и переработке отходов	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	26 декабря 19 октября 2022 г.	Vice Society BlackCat/ALPHV
Производство	Tycon Medical Systems, Inc.	Производитель медицинского оборудования	США	Утечка персональных данных	30 декабря 15 октября	
Производство	Hyperice Inc.	Производитель товаров для реабилитации и улучшения подвижности	США	Утечка персональных данных Шифровальщики	12 декабря 25 июня	Play
Производство	Wheels Manufactu-ring, LLC	Производитель велосипедных компонентов	США	Утечка персональных данных	6 декабря 4 ноября	
Производство	Pirelli Tire LLC	Производитель шин	USA Italy	Утечка персональных данных	19 декабря 18 сентября	
Производство	General Dynamics, Corp.	Аэрокосмичес-кая, оборонная и судостроительна я компания	США	Утечка персональных данных	23 декабря 1 октября	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Производство	J.S. McCarthy Co., Inc.	Производитель печатной и упаковочной продукции	США	Утечка персональных данных Шифровальщики	8 ноября 19 октября	Play
Производство	Graphique De France LTD	Производитель декоративной бумаги и подарочной упаковки	США	Утечка персональных данных, отказ ИТ-систем	27 ноября 20 сентября	
Производство	Setra Systems, Inc.	Производитель промышленных датчиков и измерительных систем	США	Утечка персональных данных	3 октября 25 января 2023 г.	
Производство	Advanced Sterilization Products, Inc.	Производитель медицинского оборудования	США	Утечка персональных данных	3 октября 25 января 2023 г.	
Коммунальные услуги	American Water Works Company, Inc.	Водоснабжающая компания	США	Отказ сервисов, отказ ИТ-сервисов	3 октября	
Коммунальные услуги	Saneamento Básico do Estado de São Paulo (Sabesp)	Компания по водоснабжению и очистке сточных вод	Бразилия	Отказ ИТ-систем и сервисов Шифровальщики	21 октября	RansomHouse
Коммунальные услуги	Stadtwerke Burg	Энергоснабжающая компания	Германия	Отказ ИТ-систем и ИТ-сервисов	29 октября 22 августа	
Коммунальные услуги	Tibber	Энергоснабжающая компания	Германия	Утечка персональных данных Шифровальщики	13 ноября	888
Коммунальные услуги	RECOPE	Энергоснабжающая компания	Коста-Рика	Нарушение операционной деятельности, отказ сервисов Шифровальщики	27 ноября	RansomHub
Коммунальные услуги	Electrica Group	Энергоснабжающая компания	Румыния	Отказ сервисов Шифровальщики	9 декабря	Lynx
Электроника, производство	Casio Computer Co., Ltd.	Группа компаний по производству электроники	Япония	Утечка данных, утечка персональных данных, отказ сервисов, отказ ИТ-систем Шифровальщики	8 октября 5 октября	
Электроника, производство	Denkai America Inc.	Производитель электронных компонентов	США	Утечка персональных данных Шифровальщики	7 ноября	Cactus
Электроника, производство	Medion AG	Поставщик электронных товаров	Германия	Нарушение операционной деятельности, отказ ИТ-систем, утечка данных Шифровальщики	28 ноября 26 ноября	Black Basta
Электроника, производство	Fluke Corporation	Производитель промышленного испытательного, измерительного и	США	Утечка персональных данных	3 октября 25 января 2023 г.	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
		диагностического оборудования				
Электроника, производство	Troxler Electronic Laboratories Inc.	Производитель измерительного оборудования для тестирования и контроля качества в строительной отрасли	США	Утечка персональных данных	30 декабря 29 октября	
Электроника, производство	Kulicke and Soffa Industries	Производитель решений для сборки полупроводнико-вых и электронных систем	США	Утечка персональных данных Шифровальщики	8 октября 12 мая	LockBit
Энергетика, строительство и инжиниринг, логистика и транспортировка	MMI Services Inc.	Подрядчик по обслуживанию скважин	США	Утечка персональных данных, отказ ИТ-систем	23 октября 20 мая	
Энергетика, строительство и инжиниринг	Newpark Resources, Inc.	Производитель буровых растворов и композитных настилов для нефтедобычи	США	Нарушение операционной деятельности, отказ ИТ-систем Шифровальщики	7 ноября 29 октября	
Горно-добывающая промышленность, энергетика	TetraSoft	Дистанционный мониторинг добычи углеводородов и бурения	Россия	Нарушение операционной деятельности, отказ сервисов, атака на цепочку поставок / доверенного партнера	November 1 July 1 ноября Июль	
Энергетика, производство	Schneider Electric	Производитель систем для управления энерго-потреблением и автоматизации	Франция	Утечка персональных данных Шифровальщики	4 ноября	Grep (Hellcat)
Пищевая промышленность, производство	EPI Breads	Производитель продуктов питания	США	Утечка персональных данных Шифровальщики	30 октября 17 сентября	Play
Пищевая промышленность, производство	VOSSKO	Птицеводческая компания	Германия	Нарушение операционной деятельности, отказ ИТ-систем Шифровальщики	22 ноября 14 ноября	Black Basta
Пищевая промышленность, производство	Stoli Group USA/Kentucky Owl	Производитель водки	США Люксем-бург	Нарушение операционной деятельности, отказ ИТ-сервисов, утечка данных, банкротство Шифровальщики	29 ноября Август	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Пищевая промышленность, производство	Amber Beverage Group	Производитель алкогольных напитков	Люксем-бург Латвия	Шифровальщики	20 сентября	RansomHub
Пищевая промышленность, производство	Misionero Vegetables	Производитель продуктов питания и овощей	США	Утечка персональных данных Шифровальщики	11 ноября 26 сентября	Play
Пищевая промышленность, производство	Krispy Kreme Inc.	Производитель пончиков	США	Нарушение операционной деятельности, отказ сервисов, утечка данных Шифровальщики	11 декабря 29 ноября	Play
Пищевая промышленность, производство	Fermented Food Holdings Inc.	Производитель продуктов питания	США	Утечка персональных данных	Декабрь	
Пищевая промышленность, производство	Central Valley Meat Co, Inc.	Компания по переработке мяса	США	Утечка персональных данных	30 декабря 23 мая	
Строительство и инжиниринг	Wise Construction Corporation	Поставщик строительных и инжиниринговых услуг	США	Утечка персональных данных Шифровальщики	23 октября 7 мая	Qilin
Строительство и инжиниринг	Dome Construction Corporation	Строительная компания	США	Утечка персональных данных Шифровальщики	22 ноября 19 октября	Play
Строительство и инжиниринг	Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH	Инжиниринговая компания	Германия	Нарушение операционной деятельности, отказ ИТ-систем Шифровальщики	27 декабря	Safepay
Строительство и инжиниринг	English Construction Company	Строительная компания	США	Утечка персональных данных Шифровальщики	7 ноября 27 сентября	LYNX
Строительство и инжиниринг	Sierra Construction Company, Inc.	Строительство промышленных, многоквартирных, коммерческих зданий и помещений под аренду	США	Утечка персональных данных Шифровальщики	Октябрь 14 августа	LockBit
Строительство и инжиниринг	BNBuilder	Строительная компания	США	Утечка персональных данных Шифровальщики	Декабрь 17 июля	Hunters International
Строительство и инжиниринг	Wright Consulting Engineers, LLC	Строительная компания и подрядчик в области строительного проектирования	США	Утечка персональных данных Шифровальщики	30 октября 17 июня	Akira
Строительство и инжиниринг	Mark Cerrone Inc.	Компания по гражданскому строительству	США	Утечка персональных данных	20 ноября 7 сентября	
Строительство и инжиниринг	Eichelberger Construction Inc.	Строительная компания	США	Утечка персональных данных	27 ноября	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Строительство и инжиниринг, коммунальные услуги, энергетика	New River Electrical Corporation	Компания по электро-техническому строительству	США	Утечка персональных данных Шифровальщики	27 ноября 30 апреля 2024 г.	ElDorado
Строительство и инжиниринг	American Engineers Inc.	Компания в области гражданского строительства	США	Утечка персональных данных Шифровальщики	4 декабря 22 октября 2023 г.	LockBit
Строительство и инжиниринг	R. Zoppo Corp.	Компания в области инфраструктур-ного и гражданского строительства, а также строительства подземных коммуникаций	США	Утечка персональных данных Шифровальщики	23 декабря 19 июня	Abyss
Строительство и инжиниринг	American Construction Corp.	Строительная компания	США	Утечка персональных данных	8 ноября 4 сентября	
Энергетика, строительство и инжиниринг	ENGlobal	Разработчик автоматизирован ных систем управления	США	Отказ ИТ-систем Шифровальщики	2 декабря 25 ноября	
Энергетика, строительство и инжиниринг	Universal Pegasus International LLC	Подрядчик по проектированию и управлению строительством в энергетической отрасли	США	Утечка персональных данных	27 ноября 13 июня	
Строительство и инжиниринг	Fitzemeyer & Tocci Associates, Inc.	Подрядчик в области строительных и инженерных услуг	США	Утечка персональных данных Шифровальщики	19 декабря 14 сентўбря	Abyss
Строительство и инжиниринг	DBM Global, Inc.	Строительная компания	США	Утечка персональных данных	23 декабря 12 ноября	
Строительство и инжиниринг	OLA Consulting Engineers	Инжиниринговая компания	США	Утечка персональных данных Шифровальщики	13 декабря 16 ноября 2023 г.	Play
Строительство и инжиниринг	TDX Construction Corporation	Подрядчик в области проектирования, строительства и общестроитель-ных работ	США	Утечка персональных данных	3 октября 5 мая	
Производство, строительство и инжиниринг	LBX Company LLC	Производитель строительной техники	США	Утечка персональных данных	31 декабря 09 сентября	
Строительство и инжиниринг, производство	Berry Bros. General Contractors, Inc.	Подрядчик в области строительства промышленных объектов, трубопроводов и морских сооружений с собственной	США	Утечка персональных данных, отказ ИТ-систем	23 октября 13 августа	

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
		производственной базой				
Производство, строительство и инжиниринг	Van Wingerden International, Inc.	Компания по строительству теплиц и производству тепличного оборудования	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	25 октября 22 января 2024 г.	Abyss
Логистика и транспортировка	Microlise Group PLC	Поставщик решений в области телематики и управления автопарком	Великобритания	Отказ ИТ-систем, отказ сервисов Шифровальщики	31 октября	SafePay
Логистика и транспортировка	Pallet Logistics of America	Общенациональный поставщик решений для цепочек поставки	США	Утечка персональных данных	12 ноября 25 июля	
Логистика и транспортировка	Diligent Delivery Systems	Поставщик транспортных, логистических и курьерских услуг	США	Утечка персональных данных Шифровальщики	5 ноября 8 июля	Embargo
Энергетика, логистика и транспортировка	Overseas Shipholding Group Inc.	Поставщик услуг по транспортировке нефти и нефтепродуктов	США	Утечка персональных данных Шифровальщики	2 декабря 31 июля	RansomHub
Логистика и транспортировка	Pittsburgh Regional Transit	Поставщик транспортных услуг	США	Нарушение операционной деятельности, отказ сервисов, утечка персональных данных Шифровальщики	23 декабря 19 декабря	
Логистика и транспортировка	Delmar	Компания по логистике и управлению цепочками поставок	Канада	Утечка персональных данных Шифровальщики	3 декабря 14 ноября	Rhysida
Логистика и транспортировка	PS Logistics	Поставщик транспортно-логистических решений	США	Утечка персональных данных	19 декабря 20 февраля	
Логистика и транспортировка	Crowley Maritime Corporation	Поставщик услуг в областях морских грузоперевозок, управления цепочками поставок и логистики	США	Утечка персональных данных	4 декабря 24 сентября	
Автомобилестроение, производство	Dewan Farooque Motors Limited	Производитель автомобилей	Пакистан	Отказ ИТ-систем, отмена заседания совета директоров	29 ноября	
Автомобилестроение, производство	Yorozu	Производитель автомобильных запчастей	Япония	Отказ ИТ-систем, утечка персональных данных Шифровальщики	18 октября 14 октября	RansomHub

Отрасль	Жертва	Профиль	Страна	Последствия особенности инцидента	Дата уведомления / Дата инцидента (если известна)	Предполагаемые акторы
Металлургия, производство	Ames Goldsmith Corporation	Производитель серебра и поставщик услуг по его переработке	США	Утечка персональных данных	10 декабря 3 октября	
Металлургия, производство	Pier Foundry & Pattern Shop Inc.	Литейное производство	США	Утечка персональных данных Шифровальщики	17 декабря 16 апреля	BlackSuit
Химическая промышленность, производство	Kurita America Inc.	Производитель химических реагентов для водоочистки	США Япония	Отказ ИТ-систем, утечка персональных данных Шифровальщики	7 декабря 29 ноября	3AM (ThreeAM)
Химическая промышленность, производство	Hubbard-Hall Inc.	Производитель специализированной химической продукции и технологических решений	США	Утечка персональных данных, отказ ИТ-систем Шифровальщики	24 декабря 23 августа	Clop

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com