

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

Оглавление

Общие сведения 3

Инциденты в крупных организациях..... 5

 Tata Technologies 5

Две атаки на одну цель 5

 Troxler Electronic Laboratories 5

Неудачные переговоры 6

 National Presto Industries 6

Атаки, которые привели к нарушению операционной деятельности..... 7

 Marposs 7

 Crystal D 7

 Fabricaciones Militares..... 8

 Ålands Centralandelslag..... 8

 Imaflex..... 8

 Kuala Lumpur International Airport..... 9

 Unimicron Technology 9

 Astral Foods..... 10

 Ganong Bros. 10

Атака, продолжавшаяся почти год..... 11

 Littleton Electric Light and Water Departments..... 11

Приложение. Полный список подтвержденных инцидентов 11

В первом квартале 2025 года жертвами было публично подтверждено 118 инцидентов. Все эти инциденты включены в таблицу в конце обзора, а некоторые из них описаны подробно.

Общие сведения

В этом квартале довольно много организаций из различных отраслей и уголков мира сообщили о серьезных инцидентах вследствие кибератак. Атаки привели к утрате конфиденциальных данных, сбоям в работе ИТ-сервисов и ключевых операционных процессов, в том числе в производстве и поставке продукции. Несомненно, самой громкой историей стала атака на аэропорт Куала-Лумпура, в результате которой на 10 часов были выведены из строя многие информационные системы: табло вылета и прилета, терминалы регистрации и системы обработки багажа.





Инциденты в крупных организациях

Tata Technologies

Строительство
и инжиниринг

Отказ
ИТ-сервисов

Шифровальщики

Индийская международная технологическая компания Tata Technologies, входящая в состав концерна Tata Motors и специализирующаяся на автомобильном, аэрокосмическом и промышленном машиностроении, 31 января [уведомила](#) Национальную фондовую биржу Индии об инциденте кибербезопасности. В письме говорилось, что из-за атаки вымогателей компания была вынуждена приостановить работу некоторых своих ИТ-сервисов. Позже их работа была восстановлена. Инцидент не затронул службы доставки, и они продолжали функционировать в штатном режиме. Представители Tata Technologies [заявили](#), что компания незамедлительно начала расследование инцидента, а также подтвердили отсутствие сбоев в производстве и работе клиентских сервисов.

В марте группа вымогателей Hunters International [взяла на себя ответственность](#) за атаку на Tata Technologies, заявив, что она похитила у компании 1,4 Тб данных, включающих 730 000 файлов. Однако злоумышленники не опубликовали никаких образцов украденной информации и дополнительных подробностей не раскрыли.

Две атаки на одну цель

Troxler Electronic Laboratories

Производственный сектор,
строительство

Утечка
персональных
данных

Шифровальщики

Американская компания Troxler Electronic Laboratories, производящая измерительное оборудование для испытаний и контроля качества в автомобильной и строительной отраслях, а также [радиоизотопные влагоплотномеры грунтов](#) (промышленная радиография), [подверглась](#) двум кибератакам, в результате которых злоумышленники украли персональные данные. 10 ноября 2024 года Troxler Electronic Laboratories обнаружила подозрительную активность в своей сети и незамедлительно приняла необходимые меры. Кроме того, компания пригласила сторонних экспертов по кибербезопасности для расследования характера и масштабов инцидента. В результате расследования было установлено, что неавторизованные сторонние лица получили доступ к некоторым файлам и данным в сети компании. Troxler Electronic Laboratories начала долгую детальную реконструкцию атаки и анализ данных, хранившихся на серверах на момент инцидента, чтобы понять, какая именно информация могла быть

затронута. 4 декабря 2024 года были определены лица, чьи персональные данные могли быть скомпрометированы. А 11 декабря 2024 года компания заметила другие подозрительные действия, в результате которых злоумышленники могли получить доступ и скопировать информацию из систем, затронутых в ходе прежнего инцидента. Troxler Electronic Laboratories установила, что данные, которые, возможно, были похищены, содержали имя, номер социального страхования и номер водительского удостоверения. Ответственность за атаку на Troxler Electronic Laboratories в декабре 2024 года [взяла на себя](#) группа RansomHub.

Неудачные переговоры

National Presto Industries

Производственный сектор

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

Шифровальщики

Американский холдинг National Presto Industries, в который входят компания по производству потребительских товаров и оборонная компания, подвергся кибератаке, ставшей причиной нарушений его операционной деятельности. Это следует из [документа](#), поданного National Presto Industries 1 марта в Комиссию по ценным бумагам и биржам США. После обнаружения инцидента организация задействовала команду реагирования, в которую вошли штатные специалисты и внешние эксперты по кибербезопасности, привлеченные для оказания помощи в устранении последствий. National Presto Industries провела криминалистический анализ для определения характера, масштаба и последствий инцидента. Инцидент повлиял на работу организации, в частности были приостановлены отправка и получение заказов, нарушены некоторые производственные процессы и работа офиса. National Presto Industries приняла временные меры для поддержания критически важных функций на период восстановления систем. Согласно заявлению, инцидент может оказать существенное негативное влияние на финансовые показатели и результаты деятельности организации.

Группа вымогателей InterLock [взяла на себя ответственность](#) за кибератаку на Национальную оборонную корпорацию, дочернюю компанию National Presto Industries. На своем сайте утечек в даркнете злоумышленники заявили, что украли 4200 Гб данных, содержащих 2 900 205 файлов и 449 989 папок. В качестве доказательства они предоставили некоторые скриншоты. InterLock [сообщила](#) DataBreaches, что потребовала выкуп у Национальной оборонной корпорации, но переговоры ни к чему не привели. Представители корпорации якобы ответили, что не считают инцидент серьезным — украденная информация не представляет большой ценности для других, а

сам факт утечки данных скажется на финансовом состоянии организации минимально. Кроме того, они сообщили, что все системы в корпорации уже работают в штатном режиме. Вымогатели утверждали, что зашифровали информацию на системах по меньшей мере трех предприятий National Presto Industries, включая AMTEC, которое производит боеприпасы и взрывчатые вещества для военных и правоохранительных органов.

Атаки, которые привели к нарушению операционной деятельности

Marposs

Производственный сектор

Нарушение операционной деятельности, отказ сервисов

Шифровальщики

Итальянский производитель контрольно-измерительного оборудования для промышленных производств Marposs 26 января [подвергся кибератаке](#) вымогателей, которые зашифровали несколько его серверов. Инцидент в значительной степени затронул логистику и в меньшей — производство. Компания уведомила о случившемся соответствующие органы и начала работу по восстановлению систем. Она оперативно задействовала команду экспертов по кибербезопасности, чтобы минимизировать ущерб. Также в связи с кибератакой Marposs запросила поддержку в государственном резервном фонде сроком до 7 февраля для компенсации потерь. Данный механизм разработан специально для форс-мажорных ситуаций подобного рода и предполагает поддержку пострадавших организаций, которая постепенно сокращается по мере нормализации производственного процесса.

Crystal D

Производственный сектор

Нарушение операционной деятельности, отказ сервисов

Шифровальщики

Американский производитель хрустальных наград и подарков Crystal D [сообщил](#), что 7 марта подвергся кибератаке, которая нарушила его работу и привела в том числе к сбоям каналов связи с клиентами и логистических сервисов. Заказы со сроком отправки 7 марта были отложены. Компания заявила, что признаков получения злоумышленниками доступа к конфиденциальной информации о клиентах не обнаружила. Уже 12 марта она [сообщила](#), что снова может взаимодействовать с клиентами и обрабатывать заказы. Вице-президент по маркетингу и продажам объяснил, что кибератака вынудила Crystal D временно отключить часть своей сети. Компания не смогла пользоваться телефонами и электронной почтой, поэтому связь с клиентами была прервана. Отправка некоторых заказов

была перенесена на более поздний срок. Ответственность за кибератаку на Crystal D [взяла на себя](#) группа вымогателей Lock Bit.

Fabricaciones Militares

Производственный сектор

Нарушение операционной деятельности, отказ сервисов, утечка данных

Шифровальщики

Аргентинская государственная военная корпорация Fabricaciones Militares Sociedad del Estado подверглась кибератаке, которую Cyber Press [связала](#) с группой вымогателей [MONTI](#). Предположительно, злоумышленники [похитили](#) более 300 Гб конфиденциальных данных. В результате атаки было остановлено производство стрелкового оружия на заводе Domingo Matheu в Буэнос-Айресе и задержаны поставки по контрактам, финансируемым Фондом Министерства обороны. Аргентинское агентство по кибербезопасности подтвердило, что злоумышленники получили доступ к секретным документам. Группа MONTI на своем портале в даркнете высмеяла руководство Fabricaciones Militares за «неэффективное сотрудничество». Cyber Press полагает, что под этим подразумеваются неудачные переговоры о выкупе за восстановление украденной информации.

Ålands Centralandelslag

Пищевая промышленность, производственный сектор

Нарушение операционной деятельности

Компании по производству молочных продуктов и хлебобулочных изделий с Аландских островов — Ålandsmejeriet и Ålandsbagarn, входящие в кооператив Ålands Centralandelslag (ÅCA), 5 марта подверглись кибератаке. По [сообщениям](#) финской прессы, после нескольких часов интенсивной работы все системы снова заработали. Некоторые операции были отложены, поскольку часть процессов по соображениям безопасности выполнялись вручную. ÅCA предупредил своих клиентов о необходимости быть внимательными в отношении подозрительных сообщений, которые могли прийти от имени компании.

Imaflex

Производственный сектор

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

Канадский производитель гибкой упаковки, полиэтиленовой пленки и пакетов Imaflex 21 февраля [сообщил](#) об инциденте кибербезопасности, который привел к сбоям в работе систем и операционных процессах. Компания незамедлительно приняла меры для снижения риска компрометации данных и воздействия на операционную деятельность. Для определения источника и масштабов инцидента Imaflex, в соответствии с лучшими отраслевыми практиками, начала всестороннее расследование, к которому привлекла внешних экспертов по кибербезопасности. Несмотря на сложности, компания продолжала производство продукции, отправку

готовой продукции и поддерживала внутренние рабочие процессы, местами используя временные решения. 27 марта Imaflex [объявила](#), что полностью восстановила свои системы и возобновила работу в штатном режиме. Вместе с тем она [уведомила](#) генерального прокурора штата Массачусетс о компрометации конфиденциальной личной информации, находящейся в ее ведении.

Kuala Lumpur International Airport

Транспорт,
логистика

Нарушение
операционной
деятельности,
отказ сервисов

Шифровальщики

Сбои в работе компьютеров в международном аэропорту Куала-Лумпура были результатом кибератаки — об этом говорится в совместном [заявлении](#) Национального агентства кибербезопасности Малайзии и Malaysia Airports Holdings Berhad. Атака началась 23 марта и привела к сбоям в работе критически важных систем аэропорта. Премьер-министр Малайзии [заявил](#), что он категорически отказался платить злоумышленникам выкуп в размере 10 млн долларов. Дополнительные технические подробности не разглашались.

Представители Malaysia Airports Holdings Berhad сообщили, что атака практически не повлияла на ключевые процессы в работе аэропорта Куала-Лумпура. Однако, судя по [сообщениям в интернете](#), несколько терминалов самостоятельной регистрации на рейсы, табло вылета и прилета, а также система обработки багажа не работали более 10 часов. Это вынудило персонал аэропорта вернуться к ручному управлению — сотрудники писали расписание рейсов на большой маркерной доске. На продолжительный сбой в работе аэропорта [обратил внимание](#) бывший член парламента Малайзии. Ответственность за атаку [взяла на себя](#) группа вымогателей Qilin. По словам злоумышленников, они украли 2 Тб данных.

Unimicron Technology

Производственный сектор,
электронная
промышленность

Нарушение
операционной
деятельности

Шифровальщики

Дочерняя компания тайваньского производителя печатных плат и интегральных схем Unimicron Technology в Китае подверглась атаке вымогателей. Согласно [бюллетеню](#), опубликованному на портале Тайваньской фондовой биржи, инцидент произошел 30 января и повлиял на работу Unimicron Technology (Shenzhen). Компания заявила, что последствия атаки на операционную деятельность были незначительными, тем не менее для анализа инцидента и оказания помощи в реализации защитных мер она привлекла внешнюю команду киберкриминалистов. Факт утечки данных она не подтвердила.

Ответственность за атаку на Unimicron Technology [взяла на себя](#) группа вымогателей Sarcoma. Злоумышленники заявили, что украли 377 Гб документов и файлов баз данных, и опубликовали якобы образцы похищенной информации. Издание BleepingComputer [обратилось](#) в Unimicron Technology с просьбой прокомментировать заявления вымогателей, но ответа не получило.

Astral Foods

Производственный сектор,
пищевая
промышленность

Нарушение
операционной
деятельности,
отказ сервисов,
финансовые
потери

Южноафриканский производитель мяса птицы Astral Foods [подтвердил](#) инцидент кибербезопасности случившийся 16 марта. Атака привела к простоям в подразделении по переработке мяса, что сказалось на поставках клиентам и нарушило производственный цикл. Хотя компания оперативно внедрила протоколы аварийного восстановления, временная остановка производства привела к финансовым потерям (снижение выручки и затраты на ликвидацию отставания в производстве). Ни конфиденциальная информация компании, ни персональные данные клиентов, поставщиков и отдельных стейхолдеров не были скомпрометированы в результате кибератаки.

Ganong Bros.

Производственный сектор,
пищевая
промышленность

Нарушение
операционной
деятельности

Шифровальщики

Канадский производитель сладостей Ganong Bros. стал жертвой атаки вымогателей. Местные СМИ [сообщили](#) со ссылкой на представителя компании, что инцидент был обнаружен 22 февраля, а работа предприятия временно остановлена. Ganong Bros. немедленно предприняла меры по укреплению защиты сети и данных, а также привлекла сторонних экспертов по кибербезопасности для помощи в локализации атаки, устранении последствий и определения масштабов инцидента, а также юриста — для проведения судебного расследования. В ходе этих работ предстояло определить, в какой степени какие-либо данные, в том числе персональная информация, могли быть скомпрометированы. Компания не сообщила, требовали ли злоумышленники выкуп. Ответственность за атаку на Ganong Bros. [взяла на себя](#) группа вымогателей PLAY.

Атака, продолжавшаяся почти год

Littleton Electric Light and Water Departments

Водоснабжение,
энергетика,
коммунальные
услуги

Утечка данных

АРТ

Исследователи из Dragos выпустили [отчет](#), в котором описали свою работу по оказанию помощи государственному энергетическому предприятию Littleton Electric Light & Water Department (LELWD) в борьбе с группой VOLTZITE, у которой был постоянный доступ к сети организации. По мнению исследователей, активность VOLTZITE пересекается с деятельностью другой группы — [Volt Typhoon](#), которая широко известна атаками на промышленные организации критической инфраструктуры с начала 2023 года. Исследователи Dragos нашли доказательства несанкционированного доступа и утечки данных, однако расследование показало, что скомпрометированная информация не включала никаких конфиденциальных данных клиентов, поэтому оказалось достаточным изменить архитектуру сети LELWD, чтобы пресечь возможные дальнейшие действия злоумышленников.

Исследователи Dragos [рассказали](#) SecurityWeek, что взлом LELWD был обнаружен в ноябре 2023 года, а расследование показало, что хакеры находились в сети организации с февраля 2023 года, то есть более 300 дней. Злоумышленники собирали информацию об операционных системах компании. По мнению исследователей, Volt Typhoon является одной из нескольких активных групп, у которой есть возможности для разработки и тестирования «специфических и разрушительных атак на АСУ». А еще во многих случаях, в том числе и в этом, злоумышленники осуществляли эксфильтрацию данных географической информационной системы (ГИС), в частности важную информацию о местоположении энергосистем.

Приложение. Полный список подтвержденных инцидентов

Пострадавшая компания	Отрасль / Профиль	Страна	Последствия инцидента	Дата уведомления Дата инцидента (если известна) Предполагаемый актор
Garden of Life	Производство / Производитель пищевых добавок	США	Утечка персональных данных	17 января 2025 года 18 декабря 2024 года

Avery Products	Производство / Производитель этикеток и наклеек	США	Утечка персональных данных Шифровальщики	13 января 2025 года 18 июля 2024 года
Prodinger	Производство / Производитель упаковочных материалов	Германия	Утечка данных, отказ ИТ- сервисов, нарушение доставки Шифровальщики	21 января 2025 года 6 декабря 2024 года
All American Poly	Производство / Производитель выдувной пленки и изделий из полиэтилена	США	Утечка персональных данных Шифровальщики	27 января 2025 года 26 августа 2024 года RansomHub
Mizuno USA	Производство / Производитель спортивного инвентаря и спортивной одежды	США Япония	Утечка персональных данных Шифровальщики	30 января 2025 года 21 августа 2024 года BianLian
Flashforge	Производство / Производитель оборудования для 3D-печати	Китай	Утечка данных	20 января 2025 года
Mayer Steel Pipe Corporation	Производство / Производитель стальных труб	Тайвань	Отказ ИТ- сервисов	2 февраля 2025 года
Fashion Box/Replay	Производство / Производитель текстиля и одежды	Италия	Утечка данных, Утечка персональных данных	Февраль 2025 года 29 января 2025 года
Natures Organics	Производство / Производитель экологически чистых чистящих средств и средств личной гигиены	Австралия	Утечка данных Шифровальщики	12 февраля 2025 года 30 января 2025 года Medusa
Raymond Limited	Производство / Компания по производству тканей и одежды, девелопер	Индия	Отказ ИТ-систем Шифровальщики	19 февраля 2025 года RansomHub
GIGAFLIGHT Connectivity, Inc.	Производство / Производитель кабелей и разъемов для аэрокосмичес-	США	Утечка персональных данных	29 января 2025 года 20 мая 2024 года

	кой и других отраслей			
Textiles Coated	Производство / Производитель текстиля	США	Отказ ИТ-систем, Утечка персональных данных	4 февраля 2025 года 1 ноября 2024 года
Mid-State Industrial	Производство / Поставщик оборудования для проектирования, производства, обслуживания и транспортировки специальной механизированной техники	США	Утечка персональных данных Шифровальщики	11 февраля 2025 года 23 января 2025 года Play
SMC Corporation of America	Производство / Производитель пневматических устройств управления	США Япония	Утечка персональных данных Шифровальщики	3 февраля 2025 года 3 декабря 2024 года Qilin
Nuna Baby Essentials	Производство / Производитель детских товаров	США Нидерланды	Утечка персональных данных	21 февраля 2025 года 8 сентября 2024 года
Daedong-USA	Производство / Производитель сельскохозяйственной техники	США	Утечка персональных данных	20 февраля 2025 года 12 января 2024 года
Racal Acoustics	Производство / Производитель гарнитур и средств защиты слуха для военных	Великобритания	Отказ ИТ-систем, утечка персональных данных Шифровальщики	24 февраля 2025 года 2 мая 2024 года RansomHub
Hartson-Kennedy	Производство / Производитель столешниц	США	Утечка персональных данных Шифровальщики	20 февраля 2025 года 24 июня 2024 года Clope
Stiiizy	Производство / Компания по производству товаров из каннабиса	США	Утечка персональных данных	8 января 2025 года 10 октября 2024 года Everest
McMillan Electric Company	Производство / Производитель электродвигателей	США	Утечка персональных данных	13 февраля 2025 года 29 октября 2024 года Medusa

			Шифровальщики	
McLanahan Corporation	Производство / Поставщик инженерного и производственного оборудования	США	Утечка персональных данных	28 февраля 2025 года 23 февраля 2024 года
Mity, Inc.	Производство / Производитель мебели	США	Утечка персональных данных Шифровальщики	27 января 2025 года 6 марта 2024 года
JSP International Group	Производство / Производитель синтетических смол и пластмасс	США Япония	Утечка персональных данных Шифровальщики	7 февраля 2025 года RansomHub
Commercial Specialty Truck Holdings	Производство / Производитель кузовов и запчастей для грузовиков	США	Утечка персональных данных	13 февраля 2025 года
Big Green Egg	Производство / Производитель грилей и сопутствующих товаров	США	Утечка персональных данных Шифровальщики	4 февраля 2025 года 26 июля 2024 года RansomHub
Oceanside Glasstile Company	Производство / Производитель стекла и плитки	США	Утечка персональных данных Шифровальщики	12 февраля 2025 года 15 августа 2024 года RansomHub
Finn Corporation	Производство / Производитель оборудования для ландшафтного дизайна	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	12 февраля 2025 года 12 ноября 2024 года DragonForce
Fortis Solutions Group	Производство / Производитель упаковки	США	Утечка персональных данных	18 февраля 2025 года 5 января 2024 года
Title 9 Sports	Производство / Производитель спортивной одежды	США	Утечка персональных данных	21 февраля 2025 года 2 ноября 2024 года
Standard Calibrations	Производство / Производитель измерительных приборов и систем	США	Утечка персональных данных Шифровальщики	20 февраля 2025 года 30 ноября 2024 года Play

QualiTech	Пищевая промышленность, производство / Производитель пищевых добавок для людей, а также добавок для подкормки растений и животных	США	Утечка персональных данных Шифровальщики	21 февраля 2025 года 19 ноября 2024 года Lynx
Ålands Centralandelslag (Ålandsmejeriet и Ålandsbagarn)	Пищевая промышленность, производство / Производство молочных продуктов и хлебобулочных изделий	Финляндия	Нарушение операционной деятельности	6 марта 2025 года 5 марта 2025 года
Advanced Foam Recycling / Amalgamate Processing	Производство / Поставщик полиуретановой пены	США	Утечка персональных данных	24 февраля 2025 года 25 июня 2024 года
Suit-Kote Corporation	Производство / Производитель асфальто-бетонных изделий	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	26 февраля 2025 года 16 октября 2024 года Black Basta
Mark Dunning Industries	Коммунальные услуги / Компания по сбору и утилизации твердых отходов	США	Утечка персональных данных	7 февраля 2025 года 7 ноября 2023 года
Adval Tech Group	Производство / Производитель инновационных пластиковых и металлических компонентов	Швейцария	Отказ ИТ-систем Шифровальщики	3 марта 2025 года 2 марта 2025 года Lynx
Numotion	Производство / Производитель медицинского оборудования	США	Утечка персональных данных	7 марта 2025 года 2 сентября 2024 года
Keding Enterprises Co.	Производство / Компания по производству изделий из дерева	Тайвань	Отказ ИТ-систем	17 марта 2025 года
Johnson Health Tech	Производство / Производитель товаров для фитнеса	Тайвань	Шифровальщики	25 марта 2025 года CrazyHunter

	и здорового образа жизни			
Sheng Yu Steel	Производство / Производитель изделий из стали	Тайвань	Отказ ИТ-систем Шифровальщики	30 марта 2025 года Underground
Brucha	Производство / Производитель изоляционных панелей	Австрия	Отказ ИТ-систем Шифровальщики	7 марта 2025 года 3 марта 2025 года
Troxler Electronic Laboratories	Производство / Производитель измерительного оборудования для испытаний и контроля качества в строительной отрасли	США	Утечка персональных данных Шифровальщики	30 декабря 2024 года 29 октября 2024 года RansomHub
National Presto Industries	Производство / Производитель потребительских товаров и оборонная компания	США	Нарушение операционной деятельности, отказ сервисов и ИТ-систем, утечка данных Шифровальщики	1 марта 2025 года InterLock
Marposs	Производство / Производитель прецизионного оборудования для измерения и управления технологическим и процессами	Италия	Нарушение операционной деятельности, отказ систем Шифровальщики	28 января 2025 года 26 января 2025 года
Crystal D	Производство / Производитель наград и сувениров из хрусталя	США	Нарушение операционной деятельности, отказ сервисов Шифровальщики	7 марта 2025 года LockBit
Fabricaciones Militares Sociedad del Estado	Производство / Производитель оружия	Аргентина	Нарушение операционной деятельности, отказ сервисов, утечка данных Шифровальщики	3 марта 2025 года Monti
Imaflex	Производство / Производитель гибкой упаковки, полиэтиленовой пленки и пакетов	Канада	Нарушение операционной деятельности, отказ ИТ-систем, утечка	21 февраля 2025 года 17 февраля 2025 года

			персональных данных	
Prime Technological Services	Электроника, производство / Производитель электронных плат и комплектующих	США	Утечка персональных данных	Январь 2025 года
Nan Ya Printed Circuit Board Corporation	Электроника, производство / Производитель печатных плат	Тайвань	Отказ ИТ-систем	2 февраля 2025 года
Unimicron Technology	Электроника, производство / Производитель печатных плат	Тайвань	Шифровальщики	30 января 2025 года Sarcoma
Transcend Information	Электроника, производство / Производитель модулей оперативной памяти и устройств хранения данных	Тайвань	Отказ ИТ-систем Шифровальщики	7 февраля 2025 года RansomHub
Fortune Electric	Энергетика, производство / Производитель силовых трансформаторов и распределительных устройств	Тайвань	Отказ ИТ-систем Шифровальщики	8 февраля 2025 года Lynx
Unikorn Semiconductor Corporation	Электроника, производство / Компания по литью полупроводниковых соединений	Тайвань	Неизвестно	4 марта 2025 года
Smiths Group	Строительство и инжиниринг / Поставщик технологичных решений для производства, энергетики и авиации	Великобритания	Отказ ИТ-систем	28 января 2025 года
Tata Technologies	Строительство и инжиниринг / Производитель автомобильной и аэрокосмической техники	Индия	Отказ ИТ-сервисов Шифровальщики	31 января 2025 года

Edw. C. Levy	Строительство и инжиниринг / Производитель бетона и асфальта	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	16 января 2025 года 29 октября 2023 года
InterCon Construction	Энергетика, строительство / Компания по предоставлению услуг в сфере энергетики и связи: электро-снабжение, телекоммуникации, инженерные работы	США	Утечка персональных данных Шифровальщики	30 января 2025 года 9 ноября 2024 года Hunters International
Argenio Bros.	Строительство и инжиниринг / Компания по строительству дорог и благоустройству территорий	США	Утечка персональных данных	23 января 2025 года 28 октября 2024 года
KMB Design Group	Строительство и инжиниринг / Компания по проведению инженерных и проектировочных работ, оказанию телекоммуникационных услуг	США	Утечка персональных данных Шифровальщики	28 января 2025 года 30 декабря 2024 года BlackBasta
O'Connor Corporation	Строительство и инжиниринг / Компания по техническому обслуживанию и строительству электростанций, турбин и генераторов, систем муниципального водоснабжения, промышленных объектов	США	Отказ ИТ-систем, утечка персональных данных	31 января 2025 года 23 ноября 2024 года
James H. Maloy	Строительство и инжиниринг / Подрядчик по строительству крупных магистралей	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	30 января 2025 года 5 ноября 2024 года Akira

IMI	Строительство и инжиниринг / Компания по проектированию и производству инженерных решений для перемещения жидкостей	Велико-британия	Неизвестно	6 февраля 2025 года
Lighthouse Electric Company	Строительство и инжиниринг / Компания по проектированию и строительству, а также техническому обслуживанию электро-оборудования	США	Утечка персональных данных Шифровальщики	4 февраля 2025 года 21 октября 2024 года RansomHub
Canyon State Electric	Строительство и инжиниринг / Компания по проектированию электротехнических решений, низковольтных систем	США	Утечка персональных данных	7 февраля 2025 года 8 января 2025 года
Nijhuis Bouw BV	Строительство и инжиниринг / Застройщик жилых комплексов, промышленных зданий, торговых центров, складов	Нидерланды	Утечка персональных данных Шифровальщики	28 февраля 2025 года
Trident Maritime Systems	Строительство и инжиниринг / Разработчик инженерных и электромеханических решений для морского транспорта	США	Утечка персональных данных	17 февраля 2025 года 1 февраля 2023 года
American Plumbing & Heating Corporation	Производство / Производитель сантехники	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	4 февраля 2025 года 17 декабря 2024 года RansomHub
Yazoo Valley Electric Power Association	Коммунальные услуги / Поставщик услуг по электро-	США	Утечка персональных данных	30 января 2025 года 23 августа 2024 года Akira

	снабжению жилого и коммерческого секторов		Шифровальщики	
Stadtwerke Schwerte	Коммунальные услуги / Поставщик газа, воды и электричества	Германия	Отказ ИТ-систем, отказ ИТ-сервисов	5 марта 2025 года
Edesur Dominicana	Коммунальные услуги / Поставщик электроэнергии	Доминиканская Республика	Шифровальщики	13 марта 2025 года 11 марта 2025 года Hunters International
Water and Sewerage Corporation	Коммунальные услуги / Компания по водоснабжению и очистке воды	Багамские острова	Шифровальщики	21 марта 2025 года
AMA S.p.A. (Azienda Municipale Ambiente)	Коммунальные услуги / Компания по сбору и утилизации твердых городских отходов	Италия	Отказ ИТ-сервисов	24 марта 2025 года
Littleton Electric Light & Water Department	Коммунальные услуги / Поставщик воды и электричества	США	Утечка данных	12 марта 2025 года
Clutch Industries	Автомобилестроение, производство / Производитель механизмов сцепления для автомобилей	Австралия	Утечка данных Шифровальщики	21 января 2025 года Lynx
Port of Ostend	Логистика и транспортировка	Бельгия	Отказ ИТ-систем и сервисов	11 февраля 2025 года 10 февраля 2025 года
Biagi Bros.	Логистика и транспортировка / Поставщик услуг по складированию и грузоперевозке	США	Утечка персональных данных Шифровальщики	25 февраля 2025 года 31 декабря 2024 года Cactus
Anellotech	Химическая промышленность, производство / Производитель химикатов на 100-процентной	США	Утечка персональных данных Шифровальщики	26 февраля 2025 года 24 декабря 2024 года

	биологической основе			
NioCorp Developments	Горно-добывающая промышленность, производство / Компания по добыче важнейших полезных ископаемых	США	Ошибочно направленные платежи поставщикам	14 февраля 2025 года
Galliker's Dairy Company	Пищевая промышленность, производство / Производитель молочных продуктов	США	Утечка персональных данных	Февраль 2025 года 23 июня 2024 года
Boart Longyear Group	Горно-добывающая промышленность, производство / Поставщик бурового оборудования и оснастки для горнодобывающих компаний	США	Утечка персональных данных Шифровальщики	6 марта 2025 года 29 июня 2024 года Dark Angels
Bavaria Sausage	Пищевая промышленность, производство / Производитель колбасных и мясных изделий	США	Утечка персональных данных	3 марта 2025 года 6 апреля 2024 года
Purecoat North / Purecoat International	Производство / Поставщик услуг по финишной обработке металлов для аэрокосмической, автомобильной, электронной и транспортной отраслей	США	Утечка персональных данных	4 марта 2025 года 19 ноября 2024 года
Pocket Nurse	Производство / Производитель и дистрибьютор медицинских принадлежностей и оборудования для медицинского образования	США	Утечка персональных данных	3 марта 2025 года

Jonti-Craft	Производство / Производитель фурнитуры	США	Утечка персональных данных Шифровальщики	5 марта 2025 года 18 октября 2024 года BlackBasta
Engine Power Source	Производство / Производитель и дистрибьютор двигателей и генераторов	США	Утечка персональных данных Шифровальщики	6 марта 2025 года 1 января 2025 года Lynx
TERREPOWER	Автомобиле- строение, производство / Производитель автозапчастей	США	Утечка персональных данных	7 марта 2025 года 12 декабря 2024 года
Erickson Companies	Производство, строительство / Компания по строительству каркасных зданий	США	Утечка персональных данных	12 марта 2025 года 16 ноября 2024 года
Trinity Petroleum Management	Энергетика, строительство / Подрядчик по строительству и управлению объектами в нефтегазовой отрасли	США	Утечка персональных данных Шифровальщики	13 февраля 2025 года 10 октября 2024 года BianLian
IKAV Energy	Энергетика / Компания по строительству и обслуживанию объектов возобновляемой энергетики	США	Утечка персональных данных Шифровальщики	13 марта 2025 года DragonForce
OBI	Пищевая промышленность, производство / Производитель свежих, замороженных и консервиро- ванных морепродуктов	США	Утечка персональных данных	11 марта 2025 года 12 августа 2024 года
F.tech R&D North America	Производство / Производитель шасси для автомобилей	США	Утечка персональных данных Шифровальщики	7 марта 2025 года Qilin

Connecticut Container Corporation / Unicorr Packaging Group	Производство / Производитель нестандартных гофрированных контейнеров и защитной упаковки	США	Утечка персональных данных Шифровальщики	11 марта 2025 года 26 января 2025 года Akira
Grede Holdings	Производство / Производитель изделий из ковкого, серого и специального чугуна для промышленного сектора и автомобилестроения	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	5 марта 2025 года 27 января 2025 года Cactus
Topy America	Автомобилестроение, производство / Производитель стальных колесных дисков для различных автомобильных компаний	США	Утечка персональных данных	Март 2025 года 8 декабря 2024 года
Mark Thomas	Строительство и инжиниринг / Компания, осуществляющая планирование, проектирование и строительство объектов муниципальной инфраструктуры	США	Утечка персональных данных	17 марта 2025 года 11 октября 2024 года
Leisure Time Products / Backyard Discovery	Производство / Производитель уличных игровых комплексов из дерева	США	Утечка персональных данных Шифровальщики	17 марта 2025 года 31 октября 2024 года Clop/ EMBARGO
Geokon	Производство / Производитель геотехнического и строительного оборудования	США	Утечка персональных данных Шифровальщики	19 марта 2025 года 30 января 2025 года Lynx
Great Western Drilling Company	Энергетика / Компания, занимающаяся разведкой месторождений и добычей нефти	США	Утечка персональных данных	20 марта 2025 года

	и природного газа			
Fireproof Contractors	Строительство и инжиниринг / Поставщик услуг по противопожарной защите, тепло-, звуко- и гидроизоляции	США	Утечка персональных данных Шифровальщики	24 марта 2025 года Nitrogen
Strauss Brands	Пищевая промышленность, производство / Производитель говядины травяного откорма	США	Утечка персональных данных Шифровальщики	19 марта 2025 года Medusa
Astral Foods	Пищевая промышленность, производство / Производитель мяса птицы	ЮАР	Нарушение операционной деятельности отказ сервисов, финансовые потери	24 марта 2025 года 16 марта 2025 года
Ganong Bros.	Пищевая промышленность, производство / Кондитерская компания	Канада	Нарушение операционной деятельности Шифровальщики	14 марта 2025 года 22 февраля 2025 года Play
CSG Consultants	Строительство и инжиниринг / Консалтинговая компания по строительным нормам и правилам	США	Утечка персональных данных Шифровальщики	20 марта 2025 года Август 2024 года Akira
Sunnking Electronics Recycling	Электроника / Поставщик услуг по утилизации электроники	США	Утечка персональных данных	28 марта 2025 года 5 февраля 2025 года
Plaisted Companies	Производство, строительство / Производитель строительных и ландшафтных материалов	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	26 марта 2025 года Сентябрь 2024 года Play
Smiths Interconnect and Smiths Interconnect Americas	Электроника, производство / Производитель электронных компонентов, микроволнового, оптического и	США Велико-британия	Утечка персональных данных	27 марта 2025 года 23 января 2025 года

	радиочастотного оборудования			
Mission Bell Mfg	Производство, строительство / Изготовитель столярных изделий и архитектурных элементов из дерева	США	Утечка персональных данных	20 марта 2025 года 31 января 2025 года
Power Test Industries	Производство / Производитель динамометров и испытательных систем	США	Отказ ИТ-систем, утечка персональных данных Шифровальщики	3 марта 2025 года 29 апреля 2024 года LockBit
Continental Aerospace Technologies	Производство / Производитель авиационных двигателей	США	Отказ ИТ-систем, утечка персональных данных	13 марта 2025 года 12 февраля 2024 года
Champion Home Builders	Строительство и инжиниринг / Компания по строительству модульных домов	США	Утечка персональных данных Шифровальщики	31 марта 2025 года 16 января 2025 года Clop
Cardo Systems	Электроника, производство / Производитель гарнитур для мотоциклистов	Израиль	Утечка персональных данных	14 марта 2025 года 28 января 2025 года
Lane Automotive	Автомобилестроение, производство / Производитель стальных колесных дисков для различных автомобильных компаний	США	Утечка персональных данных	12 марта 2025 года 23 марта 2023 года
Eckert & Ziegler Isotope Products	Производство / Поставщик изотопных технологий для медицинских, научных и промышленных целей	США	Утечка персональных данных	6 марта 2025 года 2 февраля 2025 года
Eckert & Ziegler SE	Производство / Поставщик изотопных технологий для медицинских,	Германия	Отказ ИТ-систем	13 февраля 2025 года

	научных и промышленных целей			
OEC Freight Companies	Логистика и транспортировка / Поставщик транспортно-экспедиционных и логистических услуг	США	Утечка персональных данных	14 марта 2025 года 13 мая 2024 года
Vorwerk	Производство / Производитель бытовой техники и товаров для дома	Германия	Утечка персональных данных	7 февраля 2025 года
Hofmann Fördertechnik	Логистика и транспортировка / Поставщик интралогистических услуг	Германия	Отказ ИТ-систем и сервисов	31 марта 2025 года Hunters International
Kuala Lumpur International Airport	Логистика и транспортировка	Малайзия	Нарушение операционной деятельности, отказ сервисов Шифровальщики	25 марта 2025 года 23 марта 2025 года

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