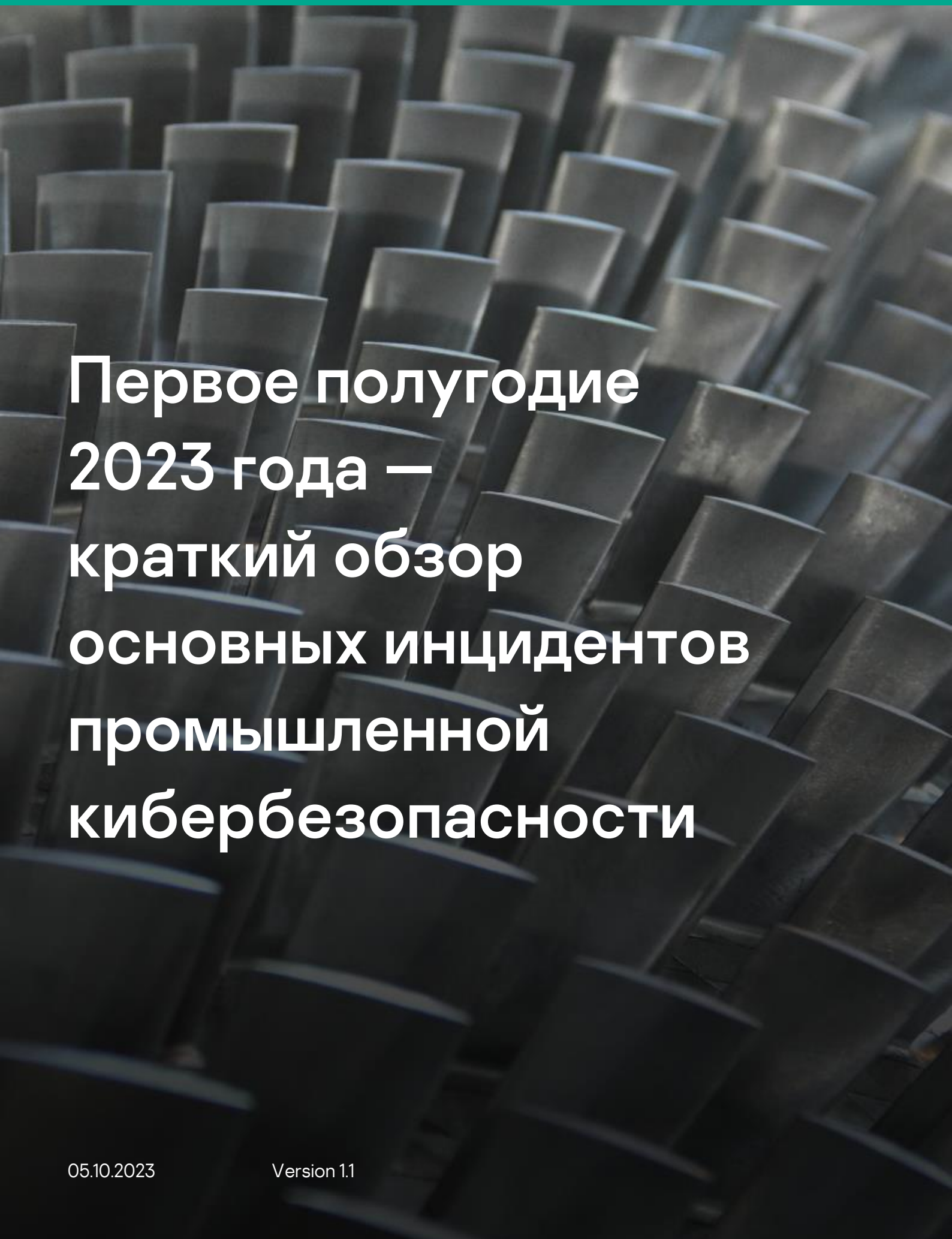
kaspersky



Первое полугодие 2023 года — краткий обзор основных инцидентов промышленной кибербезопасности

05.10.2023 Version 1.1

В этом обзоре мы рассказываем об атаках на промышленные компании киберкриминала и хактивистов. APT-атакам посвящен отдельный отчет.

Многие ссылки на сайты компаний, где была опубликована информация об инцидентах, в настоящее время не работают — соответствующая информация уже удалена. Несмотря на это, мы оставили такие ссылки в тексте, поскольку ориентировались на заявления пострадавших компаний.

В обзор включены инциденты, в которых организации официально подтвердили компрометацию. Сообщения о компрометации организаций, заявленные только киберкриминальными группами, не рассматриваются.

Вместо вступления

Атаки вымогателей и прочие криминально-мотивированные атаки становятся настоящим бичом промышленных организаций по всему миру. В отчёте за первую половину 2022 года включено 7 историй об атаках хактивистов и 10 историй о криминальных атаках вымогателей. В предыдущем, за второе полугодие 2022 года, было 40 историй, описывающих инциденты, связанные с действиями киберкриминала, и одна — об атаке хактивистов. В текущий отчёт мы включили 67 киберкриминальных историй. Как видим, прослеживается не самая радующая тенденция.

Стоит учитывать при этом, что в наших отчётах, как сказано выше, мы упоминаем традиционно только истории, публично обнародованные либо подтверждённые уполномоченными лицами — или со стороны пострадавшей организации или от соответствующего ей государства. Они показывают лишь вершину айсберга — подавляющее большинство организаций не афишируют факт компрометации и не подтверждают соответствующие сообщения в прессе, которые появляются, как правило, при добавлении организации в списки жертв киберзлодеев на их сайтах. При этом журналисты обычно реагируют на появление в этих списках только наиболее громких имён, общее же количество пострадавших организаций — многократно больше. По нашему мнению, для получения более объективного значения грубой оценки количества организаций, чьи данные были выставлены на публичную продажу, цифры, приводимые в отчётах, можно смело умножать на 10. При этом количество организаций, не знающих о том, что они скомпрометированы (потому, что злоумышленники не обращались к ним за выкупом и не выкладывали имя организации и примеры украденных данных в публичный доступ) — ещё, как минимум, в десяток раз больше. То есть, реальный объём айсберга оказывается больше «вершины» примерно на 2 порядка. Общая картина таким образом складывается весьма тревожная.

Если попытаться тем не менее судить об айсберге по его вершине, говоря только об официально (и публично!) подтверждённых данных за первое полугодие 2023, можно сделать несколько замечаний.

Первое и наиболее очевидное замечание. Среди атакованных организаций *подавляющее большинство относится к промышленному производству* чего-бы то ни было — это наиболее многочисленная и разнообразная категория потенциальных жертв из числа промышленных организаций. К тому же обладающая большим количеством секретов, интересных потенциальным покупателям, при этом в меньшей степени

зарегулированная (в смысле невозможности платить выкуп) и не столь ревностно оберегаемая государством, как, например, энергетика (что для злоумышленников значит меньший риск ответственности за преступление).

Внутри сектора промышленного производства оказалось особенно много атакованных организаций, имеющих отношение к автопроизводству (нерадостное наблюдение, с учётом общей непростой ситуации на рынке автомобилей), и, так или иначе, к транспортной отрасли — в частности пострадали организации, связанные с кораблестроением и логистикой.

Второй крупной частью сектора промышленного производства под атакой оказалось производство микроэлектроники — это одна из ключевых отраслей, которая влияет на большое количество рынков, включая, в том числе, и рынок автомобилей. Здесь в числе жертв мы видим множество хорошо известных названий компаний.

Вторым важным замечанием отметим *разнообразие пострадавших отраслей экономики* из числа «реальных» — затронуты и металлургия, и фармацевтика, и добыча полезных ископаемых, и производство продуктов питания, и энергетика и многие другие. Неожиданным кажется появление в списке известной организации-производителя сноубордического оборудования, одежды и экипировки и даже двух организаций-производителей оборудования для пожаротушения. Вероятно, в скором времени появление в подобных списках организаций, работающих в любых рынках и нишах, перестанет казаться экзотичным.

Из не относящихся напрямую к производству наиболее пострадавшими (по числу жертв) секторами стали коммунальное хозяйство, транспорт и логистика, нефть и газ и поставщики электроэнергии.

Если рассматривать электроэнергетику в целом, включая производителей комплексов специализированного оборудования и программного обеспечения и поставщиков соответствующих сервисов, то она в этом полугодии попала в список наиболее атакованных секторов экономики, следуя сразу за промышленным производством.

Третьим важным замечанием отметим *множество крупных, известных и узнаваемых имён в списке жертв*. К сожалению, даже их бюджетов, выделенных на задачи информационной безопасности, оказалось недостаточно. А поскольку такие организации стараются не разглашать деталей компрометации (вероятно, опасаясь дополнительных прямых убытков), судить о реальном масштабе бедствия по данным из публичных источников сложно. Стоит лишь держать в уме теоретическую возможность компрометации также их партнёров и клиентов.

В-четвёртых, заметим, что много организаций, включая, как минимум, три организации-гиганта*, было скомпрометировано через незакрытую уязвимость в двух различных MFT (Managed File Transfer) продуктах*. Используемые крупными организациями, в том числе и для задачи обеспечения информационной безопасности — «безопасной» (как заявляют их разработчики) передачи файлов, — решения этого типа в очередной раз становятся источником проблемы безопасности для своих клиентов. Отдельно стоит отметить, что крупные промышленные организации часто оказываются не в состоянии быстро закрыть опасную уязвимость не только в технологических сетях своих предприятий, но и, по сути, находящихся на периметре офисной сети.

Пятое и последнее. Для многих промышленных организаций кибератака стала причиной не только утечки данных или перебоя в работе внутренних IT-систем, но и прямой причиной внеплановых остановок и простоев производства и отгрузки продукции, в некоторых случаях длившихся неделями и принёсших прямые убытки в сотни миллионов долларов. Таким образом, риск кибератаки, угрожающей бизнесу, переходит в новую категорию и уже никак не может быть исключен из внимания первых лиц промышленного предприятия любого сектора и любого типа.

Январь

- DNV
- Morgan Advanced Materials
- Qulliq Energy Corporation
- The Fritzmeier Group
- Exco Technologies
- Solar Industries

Февраль

- Super Bock Group
- Trodat
- Acea
- MKS Instruments
- Lumila
- Laremo
- Vesuvius
- Águas do Porto
- Ziegler
- Gates Corporation
- Burton
- Aker Solutions
- ACER
- Encino Energy
- Trèves Group
- Stiles Machinery
- Rosenbauer Group

Март

- STEICO
- FIEGE Logistics
- Groupe SEB
- Hahn Group
- Hitachi Energy
- Puerto Rico Aqueduct and Sewer Authority
- Ferrari
- Storopack
- Rio Tinto
- Western Digital
- SAF Holland

Апрель

- Bernina
- Anton Paar Group
- Micro-Star International
- Bobst
- Israeli irrigation systems
- Hyundai
- Lürssen
- Fincantieri Marine Group
- Rheinmetall
- Sociedad Eléctrica Del Sur Oeste
- Grupo Nutresa
- Badische Stahlwerke
- Vopak
- Coca-Cola FEMSA
- Alto Calore Servizi

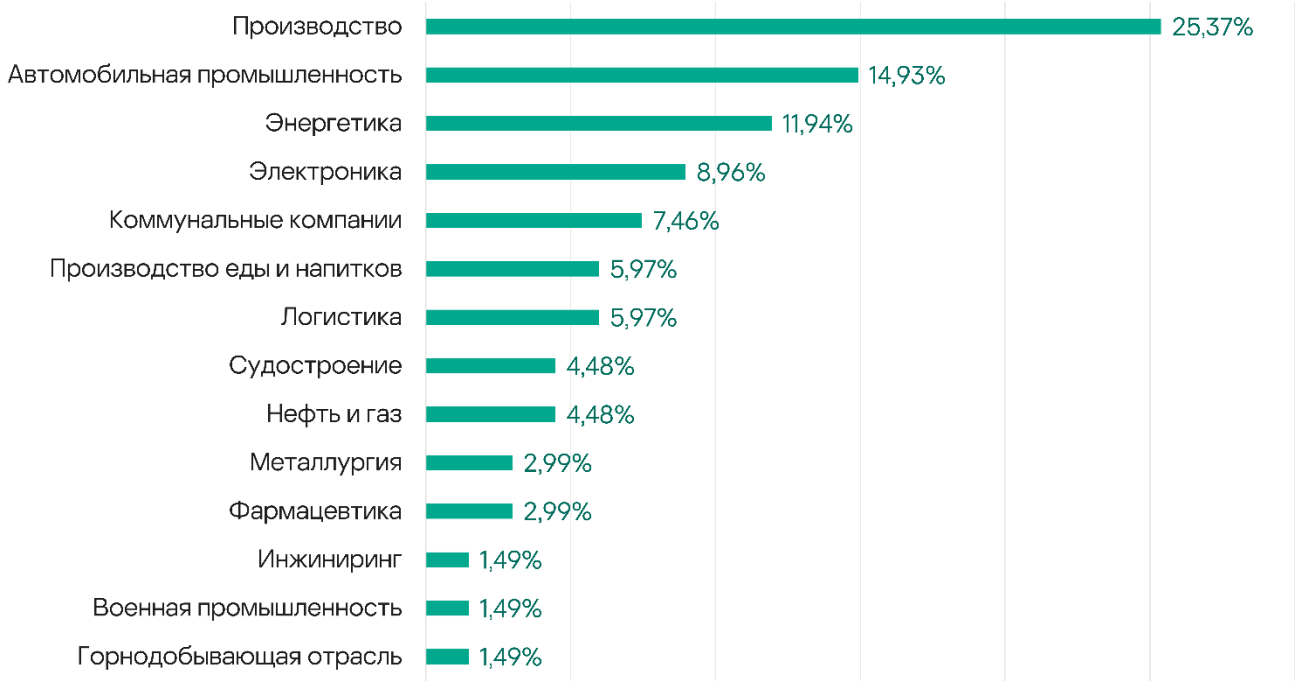
Май

- ABB
- Suzuki Motorcycle India
- Lacroix Group
- MPPMC

Июнь

- YKK
- Automatic Systems
- Hep Global
- Eisai
- Haynes International
- Brunswick Corporation
- Yamaha Corporation
- Shell
- Virbac
- Suncor Energy
- Siemens Energy
- TSMC
- Schwälbchen Molkerei

2023



Производство

Trodat подверглась атаке вымогателей

Производство

Отказ ИТ-сервисов

Ransomware

Компания Trodat, австрийский производитель штемпельной продукции, подверглась атаке вымогателей, в результате чего произошло шифрование некоторых серверов. Большая часть центральных ИТ-сервисов временно стала недоступной во многих местах по всему миру. Согласно заявлению представителей компании, благодаря немедленной реакции на чрезвычайную ситуацию была обеспечена непрерывная деятельность компании. После отключения систем и их детального анализа, была проведена «контролируемая реконструкция» (“controlled reconstruction”). В течение недели компания перешла от аварийного режима работы к нормальному.

Lumila подверглась атаке вымогателей

Производство, системы освещения, железные дороги

Ransomware

Французский производитель освещения Lumila, предоставляющий услуги для французских железных дорог, стал одной из жертв атаки вымогателей, нацеленной на несколько французских хостинг-компаний, таких как Scaleway и OVHCloud, 3 февраля. Компания подала жалобу в Центральное управление по борьбе с преступлениями в сфере информационных и коммуникационных технологий (OCLTIC). Масштаб кибератаки был определен, и компания тесно сотрудничала с соответствующими органами для проведения расследования. Все сервисы были восстановлены и находились в рабочем состоянии на момент официального объявления.

Bernina подверглась атаке вымогателей

Производство

Утечка данных, утечка персональных данных

Ransomware

Швейцарская компания Bernina International AG, ведущий производитель швейных и вышивальных машин, сообщила о том, что стала жертвой кибератаки после включения в список жертв группой вымогателей ALPHV. Компания немедленно приняла необходимые меры по обеспечению безопасности, пригласила внешних специалистов и привлекла ответственные органы к расследованию инцидента. BERNINA не согласилась с требованиями вымогателей. Злоумышленники опубликовали украденные файлы ночью 26 апреля 2023 года. Группа вымогателей заявила, что среди украденных данных находится чувствительная информация, такая как данные клиентов, данные сотрудников, соглашения о неразглашении и документы, чертежи и разработки, а также банковские данные и отчеты.

Группа Anton Paar подверглась атаке вымогателей

Производство

Отказ IT-систем, фишинг, утечка персональных данных

Ransomware

Австрийский производитель лабораторных приборов и систем измерения, Anton Paar, стал жертвой атаки вымогателей, начавшейся с получения фишинговых электронных писем 6 апреля. 19 апреля атакующие зашифровали примерно 10% ПК и серверов компании. Согласно заявлению на веб-сайте организации, компания немедленно отключила большую часть своих систем и сервсисов по всему миру и работала над восстановлением работоспособности ИТ-систем с высшим приоритетом. Компания оказывала поддержку правоохранительным органам в их расследовании. Киберинцидент привел к несанкционированному раскрытию персональных данных. Пострадавшие лица были незамедлительно проинформированы Anton Paar Group. Группа вымогателей Black Basta добавила Anton Paar в список своих жертв на своем сайте в сети Tor.

Automatic Systems подверглась атаке вымогателей

Производство

Утечка данных

Ransomware

3 июня бельгийский производитель средств контроля доступа для транспортных средств, Automatic Systems обнаружил атаку вымогателей, которую на себя взяла группа ALPHV. Согласно заявлению на главной странице веб-сайта компании, Automatic Systems немедленно приняла определенные меры для остановки распространения программы-вымогателя. Компания обратилась за помощью к внешним экспертам по кибербезопасности, которые круглосуточно поддерживали внутренние ИТ-команды. Проводились расследования для определения характера информации, которая могла стать доступной третьим лицам. Automatic Systems подала жалобу в Бельгии и во Франции. Согласно снимку экрана, опубликованному Falcon Feeds, хакеры опубликовали 121 вложение с данными, якобы украденными в результате взлома систем Automatic Systems. Группа ALPHV заявила, что украла данные о продажах и информацию о логистике, документы, связанные со страхованием, и утверждала, что располагает паролями от аккаунтов и доступом к нескольким ресурсам организации и её партнеров.

Yamaha Corporation подверглась атаке вымогателей

Производство

Ransomware

Японский производитель музыкальных инструментов и аудиооборудования объявил 15 июня, что произошел несанкционированный доступ к Yamaha Corporation of America (YCA), дочерней компании в США, что было вызвано атакой программ-вымогателей. Компания заявила в своем пресс-релизе, что немедленно отключила сетевое подключение к устройству, к которому был незаконно получен доступ. Кроме того, компания подтвердила,

что это не повлияло на системы в Японии. Вероятно информация, связанная с местными деловыми партнерами, могла быть скомпрометирована. Группа вымогателей BlackByte включила Yamaha Corporation в свой список жертв на своем сайте.

Morgan Advanced Materials подверглась кибератаке

Производство

Отказ IT-систем

Английская производственная компания Morgan Advanced Materials подверглась кибератаке. Точная природа атаки не была раскрыта, но она описывается как «инцидент с безопасностью данных». Компания сообщила, что некоторые из ее серверов были отключены для предотвращения атаки, что привело к ограничениям работы электронной почты и другим ограничениям сети. Сторонняя компания была привлечена для проведения анализа сети, чтобы лучше понять характер атаки и помочь предотвратить её дальнейшее развитие.

Fritzmeier Group подверглась кибератаке

Производство

Немецкий производитель пластиковых компонентов, металлообработки и экологических технологий, Fritzmeier Group, подвергся кибератаке, как сообщили несколько местных СМИ. Атака была обнаружена 17 января. Все соответствующие системы были выключены. Большая часть производства по-прежнему функционировала, но работала в аварийном режиме. Компанией были поданы заявления в правоохранительные органы, и были привлечены внешние эксперты для быстрого устранения проблем. По словам официального представителя, компания также консультировалась с Государственным уголовным полицейским управлением Нижней Саксонии, которое является центральной точкой контакта по киберпреступности.

Gates Corporation подверглась кибератаке

Производство

Отказ IT-систем, остановка производства и поставки

11 февраля Gates Industrial Corporation plc, производитель гидравлических систем и систем ременной передачи в США, сообщила, что стала целью атаки вредоносного программного обеспечения. Согласно выпущенному отчету, компания немедленно активировала свои планы реагирования на инциденты и обеспечения непрерывности бизнеса для ограничения, оценки и ликвидации инцидента. Компания также начала расследование, воспользовавшись услугами специалистов по кибербезопасности и внешних советников, и уведомила соответствующие правоохранительные органы. Атака затронула некоторые ИТ-системы компании, в процессе сдерживания развития инцидента компания приостановила затронутые системы

и некоторые дополнительные. Это привело к временной невозможности большей части предприятий производить и отправлять продукцию. Gates Industrial Corporation восстановила производство и отправку в некоторых из этих предприятий и занималась восстановлением оставшихся затронутых систем.

Stiles Machinery подверглась кибератаке

Производство, Поставщик оборудования

Отказ IT-систем

Американский поставщик промышленного оборудования Stiles Machinery Inc. объявил на своем веб-сайте, что обнаружил атаку и отключил свои системы для их защиты и для исследования ситуации. Уведомление было по-прежнему активным на сайте на 22 февраля. По словам представителей компании безопасность и данные клиентов и деловых партнеров «являются высшим приоритетом». Они также добавили, что «нет никаких свидетельств потери данных». По словам представителей компании, операционная деятельность и каналы коммуникации функционировали с ограничениями в период проведения восстановительных работ.

Burton подверглась кибератаке

Производство

Остановка поставки

Компания по производству сноубордов Burton Snowboards отменила все интернет-заказы после кибер-инцидента, произошедшего 11 февраля. В отдельном заявлении Burton сообщила, что начала расследование инцидента с помощью внешних экспертов, чтобы определить его последствия. Компания не предоставила подробностей о характере этого кибер-инцидента.

STEICO подверглась кибератаке

Производство

Остановка производства

Группа STEICO, немецкий производитель теплоизоляционных материалов для энергосбережения, стала целью кибератаки, обнаруженной 1 марта, информацию о которой компания затем опубликовала на своем веб-сайте. Атака затронула как производственные операции, так и административную часть. Была проведена оценка степени последствий атаки. Рабочая группа, сформированная сразу же, работала с поддержкой экспертов по кибербезопасности и специалистов по форензике, чтобы восстановить нормальную работу как можно быстрее. Дополнительных деталей компания не предоставила.

Groupe SEB подверглась кибератаке

Производство

Французский производитель бытового оборудования Groupe SEB объявил, что обнаружил попытку использовать уязвимость. После расследования было подтверждено вторжение в некую информационную систему. Компания сообщила, что «были предприняты необходимые меры для ограничения последствий этого вторжения». Groupe SEB написала, что находится в тесном контакте с клиентами и партнерами, а также с соответствующими органами, согласно общим правилам по защите данных (RGPD). Утечек данных или повреждения информационных систем «выявлено не было».

Hahn Group подверглась кибератаке

Производство, автоматизация и робототехника

Отказ IT-систем, остановка производства

Немецкая компания по промышленной автоматизации и робототехнике HAHN Group объявила, что стала жертвой кибератаки 17 марта. Согласно сообщению на ее веб-сайте, ИТ-специалисты «быстро заметили атаку и смогли ее остановить». «Все системы» были выключены. После обнаружения атаки внутренний ИТ-персонал и другие внешние эксперты по форензике работали над инцидентом, чтобы «шаг за шагом безопасно включить выключенные системы». Компания начала восстанавливать операционную деятельность с 27 марта. Восстановление потребовало переустановки инфраструктуры в чистой среде с использованием резервных систем.

Storopack подверглась кибератаке

Производство

Отказ ИТ-сервисов

Немецкий производитель упаковочных материалов и защитной упаковки Storopack обнаружил кибератаку 21 марта. Согласно новостям на официальном веб-сайте, компания стала недоступна по электронной почте, связаться с ней можно было только по телефону, официальный веб-сайт не пострадал, но интернет-магазин также стал недоступен. Storopack сразу же после обнаружения кибератаки «приняла необходимые меры» и уведомила полицию и другие ответственные органы. Могли возникнуть задержки в поставке, но Storopack сделала всё, чтобы продолжить обеспечивать возможность непрерывной поставки. Производство не прерывалось.

Bobst подверглась кибератаке

Производство

Деградация производства

По сообщению «Le Temps», швейцарский производитель промышленных машин и оборудования Bobst Group столкнулся с двумя атаками на пасхальные выходные, что вынудило компанию работать в ограниченном режиме. Компания считает, что «всё не так уж плохо», «так как данных Bobst Group не было найдено в даркнете». Были предприняты экстренные меры для защиты критических компьютерных систем путем их изоляции, чтобы ограничить риск возможного распространения атаки, что затронуло производство, исследование и разработку и поддержку клиентов компании. Различные предприятия компании по всему миру вернулись к нормальной работе в период с 12 по 18 апреля. Производитель уведомил своих клиентов и поставщиков о некоторой нестабильности, через пять дней после события. Директор Bobst заявил, что знает, кто атаковал компанию и откуда были произведены атаки, но не предоставил дополнительных деталей. Требования о выкупе не поступало.

YKK подверглась кибератаке

Производство

Ransomware

Японский производитель молний YKK подтвердил кибератаку на свои системы в США после того, как компания была указана в качестве жертвы на сайте группы вымогателей LockBit 2 июня. Согласно словам представителя компании, как только была выявлена кибератака, команда кибербезопасности компании быстро отреагировала и «успешно сдержала ее», «прежде чем она смогла причинить значительный ущерб или привести к утечке конфиденциальной информации». Быстрый и эффективный ответ компании способствовал тому, что атака не повлияла на их операционную деятельность и качество обслуживания для клиентов. Точная природа кибератаки остается не разглашенной, и компания не комментировала, был ли потребован выкуп. Тем не менее, следует отметить, что группа вымогателей LockBit угрожала опубликовать украденные данные компании до 16 июня, но остается неясным, произошла ли в действительности утечка каких-либо конфиденциальных данных.

Автомобильная промышленность

Trèves Group подверглась атаке вымогателей

Производство, автомобильная промышленность

Ransomware, требование выкупа

Французский автомобильный производитель Trèves Group столкнулся с масштабной кибератакой в выходные 18 и 19 февраля 2023 года. Согласно пресс-релизу компании, чтобы ограничить воздействие атаки и защитить своих партнеров, Trèves Group сразу «задействовала протоколы изоляции». Группа тесно сотрудничала с властями и обещала предпринять «все необходимые меры по этому вопросу». Компания мобилизовалась, чтобы гарантировать непрерывную работу и возвращение к нормальной работе как можно скорее. Trèves Group упомянула группу вымогателей Lockbit 3.0 как источник атаки в пресс-релизе, которая, в свою очередь, добавила компанию в список своих жертв. Компания решила не платить выкуп.

Группа Rosenbauer подверглась атаке вымогателей

Производство, автомобильная промышленность, пожарно-спасательная техника

Отказ ИТ-систем

Ransomware

Группа Rosenbauer, австрийский производитель пожарных автомобилей и пожарной техники, стала целью кибератаки. Согласно краткому пресс-релизу, опубликованному 24 февраля, часть ИТ-инфраструктуры была отключена в качестве мер предосторожности. Принятые компанией меры затронули все локации Rosenbauer. Немедленно была создана оперативная группа, привлечены внешние эксперты по кибербезопасности и форензик эксперты, чтобы безопасно и быстро восстановить работу систем. По информации компании, «ни клиентские данные, ни данные компании не были украдены или зашифрованы». К расследованию были привлечены соответствующие органы. Несколько дней спустя после официального подтверждения атаки группа вымогателей LockBit 3.0 включила компанию в список своих жертв.

Ferrari подверглась атаке вымогателей

Производство, автомобильная промышленность

Утечка данных, требование выкупа, утечка персональных данных

Ransomware

Итальянский производитель автомобилей Ferrari сообщил о киберинциденте с программой-вымогателем. Атакующий потребовал, чтобы компания заплатила выкуп за данные клиентов. Компания уведомила своих клиентов о возможной утечке данных. Согласно заявлению компании, после получения требования о выкупе она немедленно начала расследование совместно с одной из ведущих мировых компаний по кибербезопасности и уведомила соответствующие органы. Она добавила, что в соответствии с политикой компании Ferrari не будет платить выкуп, так как такие платежи финансируют преступную деятельность. Компания уведомила своих клиентов и предупредила их о возможной утечке данных и характере инцидента. Компания заявила, что инцидент с программой-вымогателем никак не повлиял на ее операционную деятельность.

Exco Technologies подверглась кибератаке

Производство, автомобильная промышленность

Отказ ИТ-систем

Канадская международная компания, занимающаяся производством литейных инструментов и автозапчастей Exco Technologies, объявила 23 января, что три производственных предприятия в составе своей Группы по производству литых форм восстанавливаются после киберинцидента. Компания временно отключила некоторые компьютерные системы, чтобы провести расследование инцидента с привлечением независимых экспертов. По ожиданиям компании операционная деятельность должна была в значительной степени восстановиться в течение следующих двух недель. В заявление не было подробного описания вида атаки, а также не было указано, были ли украдены личные или корпоративные данные.

Ziegler подверглась кибератаке

Производство, автомобильная промышленность, пожарные автомобили

Отказ ИТ-систем, остановка поставки

Немецкий производитель пожарных автомобилей Albert Ziegler GmbH стал жертвой кибератаки, которая была обнаружена утром 9 февраля. Согласно новостям, все соответствующие системы были немедленно выключены. В результате, все системы были выведены в офлайн по всем локациям, что ограничило работу и доступность компании по электронной почте. 20 февраля компания выпустила заявление, что все системы были восстановлены, но компания всё ещё доступна по электронной почте с задержками. Система управления товарными запасами стала доступной снова лишь спустя несколько дней. Что позволило кампании возобновить поставки продукции в Гингене.

SAF-Holland подверглась кибератаке

Производство, автомобильная промышленность

Отказ ИТ-систем, остановка производства: 7-14 дней

Немецкий производитель шасси для прицепов и грузовиков SAF-Holland стал объектом кибератаки, о которой было объявлено 27 марта. В результате системы были отключены от Интернета выключены. По оценкам компании приостановка производства на некоторых ее объектах могла продлиться на семь-четырнадцать дней. Однако руководство ожидало, что удастся скомпенсировать отставание в производстве в течение следующих трех месяцев. Компания оценила, что на восстановление утерянного производства понадобится три месяца.

Rheinmetall подверглась кибератаке

Производство, автомобильная промышленность

Отказ ИТ-систем

Rheinmetall, немецкий производитель автомобилей и вооружения с головным офисом в Дюссельдорфе объявил, что столкнулся с кибератакой, произошедшей 14 апреля. Атака затронула бизнес-подразделение Rheinmetall, обслуживающее промышленных клиентов, в частности, в автомобильной отрасли. По словам представителя Rheinmetall в письме для Recorded Future News, подразделение компании, которое производит военные транспортные средства, оружие и боеприпасы, не пострадало и продолжает работать. Неясно, кто стоит за атакой. Известно, что хактивистская группа Killnet опубликовала сообщение на своем канале в Telegram в марте, призывая своих последователей к DoS (denial-of-service) атакам на Rheinmetall.

Кража данных в Hyundai

Производство, автомобильная промышленность

Утечка данных, утечка личных данных

Производитель автомобилей Hyundai Motor уведомил владельцев автомобилей во Франции и Италии о несанкционированном доступе к данным. Компания предупредила, что хакеры получили незаконный доступ к личной информации клиентов компании. Утечка данных содержит номера телефонов, адреса электронной почты, местоположения и номера шасси транспортных средств (VIN). В предупреждении подтверждается, что, хотя злоумышленники и получили доступ к базе данных Hyundai, они не получили доступа к финансовой информации о клиентах или к их паспортным данным. Hyundai сообщила, что перевела свои системы в офлайн-режим в ответ на атаку, пока не будут приняты дальнейшие меры защиты. Компания также уведомила французские и итальянские органы по защите данных. Hyundai рекомендует своим клиентам быть бдительными по отношению к подозрительным электронным письмам и нежелательным текстовым сообщениям, так как это может быть попыткой социальной инженерии.

Suzuki Motorcycle India подверглась кибератаке

Производство, автомобильная промышленность

Остановка производства

Suzuki Motorcycle India, дочернее предприятие Suzuki Motor Corporation, стало жертвой кибератаки. С 10 мая компания приостановила производство на заводе в Гургаоне, расположенном в северном индийском штате Харьяна. Представитель Suzuki Motorcycle India заявил, что они знают об инциденте и немедленно сообщили об этом. На момент сообщения об атаке технических деталей не предоставлено. Как сообщалось, кибератака заставила компанию отложить ежегодную конференцию для поставщиков, которая должна была состояться в мае.

Laremo подверглась атаке вымогателей

Стальные конструкции

Отказ в обслуживании, потеря данных, утечка данных

Ransomware

Немецкая компания — производитель спецоснащения грузовиков и строительной техники Laremo GmbH подверглась атаке с использованием программы-вымогателя 5 февраля, компания объявила об этом в публичном заявлении 22 февраля. Согласно заявлению серверные системы хранения данных были зашифрованы, так что данные были потеряны. Злоумышленники получили доступ к базе данных клиентов и финансовому учету. Компания обратилась к соответствующим следственным органам.

Ответственность за атаку взяла на себя группа LockBit, которая загрузила данные компании на свой веб-сайт в даркнете 19 февраля.

Энергетика

Aker Solutions подверглась кибератаке

Энергетика

Отказ ИТ-систем

Ransomware

Подразделение Aker Solutions, норвежского поставщика услуг для энергетической отрасли, CSE Mecanica e Instrumentação SA в Бразилии, стало жертвой кибератаки, которая повлияла на его ИТ-системы. На момент заявления Aker Solutions не обладали всей полнотой картины. Они установили диалог с властями Бразилии по поводу инцидента. К решению проблемы были привлечены эксперты извне. Aker Solutions меры по сдерживанию развития инцидента потребовали временного отключения большинства ИТ-систем, используемых в подразделении CSE. По утверждению злоумышленников, они получили доступ к ИТ-системам организации, и зашифровали данные. Позже Aker Solutions опубликовали обновление, подтвердив, что другие части ИТ-систем, не относящиеся к подразделению CSE, не пострадали.

ABB подверглась кибератаке

Производство, электротехническое оборудование, энергетика

Утечка данных, отказ ИТ-систем

Ransomware

Шведско-швейцарский производитель электротехнического оборудования ABB подтвердил, что стал объектом атаки с использованием программ-вымогателей, и что хакеры похитили некоторые данные. Согласно пресс-релизу, все ключевые сервисы и системы ABB функционировали, все заводы работали, и компания продолжала обслуживать своих клиентов. На момент заявления компания продолжала восстанавливать пострадавшие сервисы и системы и занималась повышением безопасности своих систем. В частных уведомлениях, отправленных клиентам, ABB сообщила, что ее расследование показало, что системы клиентов не были напрямую затронуты, и нет признаков того, что подключение к системам ABB небезопасно. Ресурс Bleeping Computer первым сообщил о том, что ABB были атакованы группой вымогателей Black Basta 7 мая. Издание сообщило, что атака вымогателей затронула Windows Active Directory компании ABB, повлияв на сотни устройств. В ответ на атаку ABB разорвала VPN-соединения с клиентами, чтобы предотвратить распространение программ-вымогателей на другие сети. В сообщении от 26 мая исследователь в области кибербезопасности Кевин Боумонт заявил, что компания заплатила выкуп, что объясняет, почему ее не указали на сайте для утечки Black Basta.

MPPMC подверглась атаке вымогателей

Энергетика

Отказ ИТ-систем

Ransomware

Компания Madhya Pradesh Power Management Company Limited, базирующаяся в Джабалпуре, Индия, стала жертвой атаки вымогателей. Инцидент был обнаружен во внутренней ИТ-системе IABS компании 22 мая. Суперинтендант полиции Джабалпура заявил, что началось расследование по поступившему заявлению. Главный управляющий директор MPPMC сообщил, что злоумышленники, стоящие за атакой вымогателей, предоставили электронные адреса для связи с ними. MPPMC просканировали серверы в соответствии с рекомендациями правительства и попытались восстановить их. На момент объявления не было предоставлено дополнительных технических подробностей.

Qulliq Energy Corporation подверглась кибератаке

Энергетика, утилиты

Отказ ИТ-систем, отказ в обслуживании клиентов

Корпорация Qulliq Energy (QEC), обслуживающая территорию Нунавут в Канаде, сообщила, что ее сеть была скомпрометирована 15 января. Она раскрыла, что атака повлияла на системы в ее офисе обслуживания клиентов и административных офисах и не затронула операции электростанций, хотя клиенты не могут оплатить свои счета кредитной картой. Компания привлекла внешних экспертов по кибербезопасности вместе с ИТ-командами QEC и правительства Нунавута, чтобы исследовать объем атаки и определить, какие данные были скомпрометированы.

Кража данных в Hitachi Energy

Производство, энергетика

Утечка данных

Уязвимость нулевого дня, GoAnywhere MFT, Ransomware

Компания Hitachi Energy подтвердила кражу данных после того, как группа вымогателей Clop похитила данные, используя уязвимость 0-дня в GoAnyway, добавив компанию в число своих жертв.
Hitachi Energy — подразделение японского инжинирингового и технологического гиганта Hitachi, специализирующееся на энергетических решениях и электроэнергетических системах. Атака стала возможной благодаря эксплуатации уязвимости нулевого дня в Fortra GoAnywhere MFT (Managed File Transfer), раскрытой впервые 3 февраля 2023 года и теперь отслеживаемой как CVE-2023-0669. Эта уязвимость позволяет злоумышленникам выполнять удаленное выполнение кода на не обновлённых версиях GoAnywhere MFT, что особенно опасно, еслит административная консоль доступна из Интернет. Компания немедленно отреагировала на инцидент, отключив затронутую систему (GoAnywhere MFT) и начав внутреннее расследование для определения последствий компрометации. Все затронутые сотрудники, соответствующие органы по защите данных и правоохранительные органы были уведомлены об инциденте безопасности непосредственно компанией Hitachi. В заявлении компании говорится, что у нее нет информации о том, что работа сети компании или безопасность данных клиентов были нарушены. В заявлении не указано, стали ли какие-либо системы неоперабельными после атаки.
Группа вымогателей Clop заявила, что они взломали более 130 организаций, используя уязвимость инструмента безопасной передачи файлов GoAnywhere MFT. Атакующие также утверждают, что они могли перемещаться по сетям своих жертв и развертывать программы-вымогатели для шифрования их систем, но решили отказаться от этого и лишь скопировали документы, хранящиеся на скомпрометированных серверах GoAnywhere MFT.

Sociedad Eléctrica Del Sur Oeste подверглась кибератаке

Электроэнергетика, энергетика, утилиты

Отказ ИТ-систем

Электроснабжающая компания Sociedad Eléctrica del Sur Oeste (SEAL) в Перу подверглась кибератаке 17 апреля. Компания сообщила в пресс-релизе, отправленном местным новостным агентствам, что некоторые услуги и данные пользователей недоступны до дальнейшего уведомления. Сроки действия платежей за электроснабжение и некоторые услуги также были приостановлены. Согласно генеральному директору SEAL, злоумышленники пытались похитить информацию, однако система безопасности компании предотвратила это. Единственное, что им удалось сделать, — это получить доступ к коммерческой части. В официальном сообщении компании утверждалось, что специалисты решают проблему, чтобы восстановить систему клиентского обслуживания.

Siemens Energy подверглась кибератаке

Производство, энергетика, энергетические технологии

0-day уязвимость, MOVEit MFT, Ransomware

Компания Siemens Energy, специализирующаяся на энергетических технологиях и базирующаяся в Мюнхене, официально подтвердила несанкционированный доступ к данным через атаку на платформу безопасной передачи файлов MOVEit Transfer 27 июня после того, как группа вымогателей Clop добавила компанию на свой веб-сайт для утечек данных. Злоумышленники использовали уязвимость нулевого дня в платформе MOVEit Transfer, чтобы получить несанкционированный доступ к чувствительной информации. Однако согласно представителю компании Siemens Energy критические данные не были похищены, и бизнес-деятельность не пострадала. Компания предприняла немедленные меры, как только обнаружила инцидент. Компания Siemens Energy не ответила на последующие вопросы новостных агентств о том, какие системы или устройства были затронуты, и какие данные были похищены.

Hep Global подверглась кибератаке

Производство, возобновляемая энергия

Утечка данных

Ransomware

Немецкая компания по производству и эксплуатации солнечных электростанций по всему миру Hep Global подверглась кибератаке. Согласно заявлению на ее веб-сайте, все потенциально затронутые системы были отключены как немедленная мера, и чтобы избежать возможного ущерба клиентам. На момент публикации компания не могла сказать, были ли фактически похищены данные. Компания сотрудничала с органами власти и внешними экспертами и подала жалобу против неизвестных лиц. 19 июня Hep Global выпустили обновление, где сообщили, что немедленные меры и плотное сотрудничество с органами власти и внешними экспертами по информационной безопасности обеспечили

непрерывность бизнеса, и расследование кибератаки все еще продолжается. Группа вымогателей Darkrace заявила, что они несут ответственность за утечку данных в Hep Global и указали компанию в качестве своей жертвы.

Электроника

MKS Instruments подверглась атаке вымогателей

Производство, электроника, оборудование для чиповой индустрии

Отказ в обслуживании, приостановка производства и поставок, финансовые потери: 200 млн долларов

Ransomware

Производитель оборудования для чиповой индустрии MKS Instruments сообщил о том, что был подвергнут атаке вымогателей, произошедшей 3 февраля, которая затронула бизнес-системы, включая системы, связанные с производством. На момент объявления веб-сайт MKS оставался недоступным. Чтобы сдержать развитие инцидента компания временно приостановила операционную деятельность на некоторых своих объектах. Компания сообщила о случившемся в правоохранительные органы. Организация пыталась оценить объем ущерба и выяснить, какая его часть покрыта страхованием. Атакующие зашифровали бизнес- и производственные системы, а также могли украсть личные данные, согласно докладу, представленному в регулирующие органы Калифорнии. Атака повлияла на способность компании обрабатывать заказы, отправлять продукцию и предоставлять услуги клиентам в ее подразделениях Vacuum Solutions и Photonics Solutions. Компания объявила в конце февраля, что атака приведет к убыткам в размере не менее 200 миллионов долларов в первом квартале. До инцидента MKS Instruments ожидала объявить о доходах примерно на 1 миллиард долларов.

Micro-Star International подверглась атаке вымогателей

Производство, компьютеры и электроника

Утечка данных

Ransomware

Тайванская компания по производству компьютеров и электроники MSI (Micro-Star International) подтвердила 7 апреля, что ее сеть была скомпрометирована в ходе кибератаки после того, как группа вымогателей Money Message заявила, что они взломали некоторые системы MSI и украли файлы. В заявлении MSI призвал пользователей «получать обновления прошивки/BIOS только с официального веб-сайта», а также избегать использования файлов из других источников. MSI не уточнили масштаб ущерба и не раскрыла, что было украдено. Компания только сообщила, что обнаружила аномалии в сети, и ее IT-отдел «активировал соответствующие защитные механизмы и провел восстановительные меры». Компания сообщила о вторжении правоохранительным органам и подразделениям кибербезопасности. Она также отметила, что вернулась к нормальной работе без значительных финансовых потерь.

Кража данных в ACER

Производство, компьютеры и электроника

Утечка данных

Тайваньский производитель электроники я ACER подтвердил утечку данных на одном из своих серверов д после того, как хакеры заявили, что украли 160 Гб данных у компании. ACER сообщили SecurityWeek, что обнаружили инцидент несанкционированного доступа к одному из своих серверов, хранящих документацию, предназначенную для специалистов по ремонту. В процессе расследования инцидента, не было обнаружено признаков того, что какие-либо клиентские данные хранились на этом сервере. Киберпреступники утверждали, что данные, украденные в середине февраля, включают конфиденциальные слайды, инструкции для сотрудников, конфиденциальная документация о продукции, бинарные файлы, информация о бэкенд инфраструктуре, образы дисков, цифровые ключи для замены продуктов и информация, имеющая отношение к BIOS.

Western Digital подверглась кибератаке

Производство, компьютеры и электроника, устройства хранения данных

Утечка данных, утечка персональных данных, отказ в обслуживании клиентов

5 мая американский производитель устройств хранения данных Western Digital выпустил заявление, в котором признал, что мартовская кибератака на его компьютерные системы привела к краже данных. Согласно заявлению, скомпрометированные данные включают имена, адреса, телефонные номера, хеши паролей и часть номеров платежных карт. Western Digital временно приостановил доступ к своему интернет-магазину. Компания знала о том, что их информация предположительно стала общедоступной, но не подтвердила достоверность сведений об утечке. TechCrunch сообщил, что «неизвестная» хакерская группа взломала Western Digital и заявила, что украла десять терабайт данных. Несмотря на то, что злоумышленники утверждали, что они не являются частью ALPHV, они использовали сайт утечки данных этой группы. Злоумышленники опубликовали скриншоты украденных писем, документов и приложений, которые показывали, что они имели доступ к сети компании, даже после обнаружения. Хакеры также утверждали, что украли базу данных SAP Backoffice, содержащую информацию о клиентах, и опубликовали скриншот того, что, по всей видимости, является счетами клиентов.

Lacroix Group подверглась кибератаке

Производство, электроника

Отказ ИТ-систем, остановка производства

Lacroix Group, многонациональный производитель электронного оборудования для автомобильной отрасли, домашней автоматизации, авиационной, промышленной и отрасли здравоохранения, сектора умных дорог, а также управления системами водоснабжения и энергоснабжения, объявила, что ночью с пятницы 12 мая на субботу 13 мая стала жертвой целенаправленной кибератаки. Кибератака затронула французские, немецкие и тунисские площадки. Немедленно были предприняты меры для обеспечения безопасности всех остальных объектов компании. Некоторые локальные инфраструктуры были зашифрованы. 31 мая компания выпустила обновление, в котором сообщила, что частично возобновила производство на своих площадках по производству электроники в Тунисе, Франции и Германии с 17 мая.

Кража данных в TSMC

Производство, электроника, полупровод-ники

Утечка данных

Тайваньская компания по производству полупроводников Taiwan Semiconductor Manufacturing Company (TSMC) подтвердила нескольким информационным агентствам 30 июня, что стала жертвой утечки данных после того, как была включена в список жертв группы LockBit на ее сайте. Группа угрожала опубликовать украденные у компании данные, но так и не предоставила никаких доказательств. В заявлении, предоставленном информационным агентствам, представитель TSMC подтвердил, что утечка данных произошла из-за инцидента у одного из поставщиков аппаратного обеспечения компании, Kinmax Technology, что привело к утечке информации, относящейся к начальной настройке и конфигурации сервера. Согласно заявлению, это происшествие не повлияло на бизнес-операции TSMC и не скомпрометировало информацию клиентов TSMC. После инцидента TSMC немедленно прекратила обмен данных с этим поставщиком в соответствии с протоколами безопасности и стандартными процедурами компании.

Коммунальные компании

Acea подверглась кибератаке

Энергетика, коммунальные услуги

Ransomware

Acea, итальянская публичная холдинговая компания, предоставляющая энергию и другие услуги в Риме, подтвердила кибератаку в начале февраля, предположительно осуществленную группой вымогателей Black Basta. Согласно заметке компании, атака не повлияла на основные услуги, предоставляемые пользователям (распределение воды и электроэнергии), благодаря оперативному решению проблемы в сотрудничестве с соответствующими учреждениями, Национальным агентством кибербезопасности (Acn) и CNAIPIC.

Águas do Porto подверглась кибератаке

Водоснаб-жение, коммунальные услуги

Отказ веб-сервисов

Ransomware

Águas e Energia do Porto, водоснабжающая компания в Португалии, объявила 8 февраля, что она подверглась кибератаке, и ее служба безопасности смогла ограничить ущерб. Общественное водоснабжение и санитария не пострадали от атаки. В результате инцидента некоторые услуги предоставлялись с ограничениями. Офисы обслуживания клиентов продолжали работать и для избежания очередей компания просила клиентов использовать виртуальные талоны на обслуживание.
Águas e Energia do Porto обратиласть к Португальскому национальному центру кибербезопасности и Судебной полиции за помощью в решении ситуации. Ответственность за атаку взяла на себя группа вымогателей LockBit.

Puerto Rico Aqueduct and Sewer Authority подверглась кибератаке

Водоснаб-жение, коммунальные услуги

Утечка данных, утечка персональных данных

Ransomware

Государственная водопроводно-канализационная компания Puerto Rico Aqueduct and Sewer Authority (PRASA) привлекла к расследованию кибератаки, о которой было объявлено 19 марта, американские агентства ФБР и CISA. Злоумышленники получили доступ к информации о клиентах и сотрудниках. Официальные лица отметили, что критическая инфраструктура ведомства не пострадала от инцидента благодаря сегментации сети. PRASA собиралаась уведомить пострадавших клиентов и сотрудников с помощью уведомительных писем о нарушении.
Группа вымогателей Vice Society добавила организацию в список жертв на своем утечка данных на Tor. Группа вымогателей опубликовала паспорта, водительские удостоверения и другие документы пострадавших лиц.

Израильские системы орошения подверглись кибератаке

Ирригация, системы очистки сточных вод, коммунальные услуги

Отказ в работе OT-систем, остановка операционной деятельности

Хактивизм

Jerusalem Post сообщила, что кибератака заблокировала несколько контроллеров, которые мониторят системы орошения и системы очистки сточных вод в Долине Иордана, управляемые компанией Galil Sewage Corporation. Эксперты компании потратили весь день на восстановление работы, на момент инцидента источник атаки оставался неясным. Местные власти были осведомлены о риске кибератаки и сообщили о нём фермерам в регионе. Некоторые фермеры отключили свои системы орошения от Интернета и перевели их на ручное управление. По сообщению Jerusalem Post, Национальный Директорат кибербезопасности предупреждала о риске кибератак, которые антиизраильские хакеры могут провести против национальной инфраструктуры во время месяца Рамадан, сообщая об увеличившемся количестве фишинга, попыток авторизации в CMS и попытках эксплуатаций уязвимостей веб-сайтов, таких как SQL Injection. В апреле частные и государственные организации в Израиле подверглись массовым кибератакам, которые были частью кампании #OPIsrael, запущенной хактивистами против израильской критической инфраструктуры.

Alto Calore Servizi подверглась кибератаке

Водоснаб-жение, канализация и очистка, коммунальные услуги

Утечка данных

Ransomware

Итальянская водоснабжающая, канализационная и очистительная компания Alto Calore Servizi SpA подтвердила кибератаку 28 апреля. Атака не повлияла на водоснабжение, но база данных компании была скомпрометирована, согласно сообщению на веб-сайте компании. 2 мая Medusa Locker заявили о кибератаке на своем собственном сайте, опубликовав некоторые файлы, принадлежащие компании ACS. Группа заявила, что получила данные клиентов, контракты, протоколы заседаний правления, отчеты, информацию о распределении труб, документы о расширении и многое другое.

Логистика

Wabtec подверглась атаке вымогателей

Транспорт, логистика, железные дороги

Утечка персональных данных

Ransomware

Американская Wabtec Corporation, один из крупнейших в мире поставщиков высокотехнологичных продуктов и услуг с добавленной стоимостью для мировой железнодорожной отрасли, сообщила об утечке конфиденциальных и персональных данных после того, как группа LockBit сначала опубликовала образцы похищенных данных, а 20 августа 2022 года слила все украденные у Wabtec данные.

В объявлении Wabtec говорится, что хакеры взломали их сеть и установили вредоносное ПО на определенные системы уже 15 марта 2022 года. 26 июня Wabtec обнаружила необычную активность в своей сети и начала расследование атаки.

30 декабря 2022 года, согласно соответствующим нормативам, Wabtec начала рассылать официальные письма пострадавшим лицам с уведомлением о том, что их данные были скомпрометированы. Среди украденной информации: имя и фамилия, дата рождения, национальный идентификационный номер, номер социального страхования или налоговый код, номер паспорта, IP-адрес, номер работодателя (EIN) и другие данные. Wabtec в соответствии с требованиями уведомила все применимые регулирующие органы и органы по защите данных.

DNV подверглась атаке вымогателей

Транспорт, логистика, мореплавание

Отказ в обслуживании, цепи поставок

Ransomware

Норвежское общество по классификации судов DNV сообщило, что стало жертвой атаки вымогателей, произошедшей 7 января.

В результате атаки компания отключила от сети свои серверы для управления флотом ShipManager, программное решение для управления флотами, которое поддерживает управление судами в различных технических и операционных аспектах, включая соответствия требованиям регуляторов. По оценке DNV инцидент мог затронуть до 1000 судов и повлиял на 70 клиентов. Согласно сообщениям от организации, функциональность программного обеспечения на борту судов не пострадала.

Поставщик морского программного обеспечения начал расследование инцидента с привлечением партнеров по информационной безопасности. Компания также сообщила о случившемся норвежским властям.

FIEGE Logistics подверглась атаке вымогателей

Логистика

Утечка данных, отказ в обслуживании

Ransomware

Немецкая компания FIEGE Logistics подтвердила, что стала жертвой атаки вымогателей после того, как группа вымогателей Lockbit 3.0 опубликовала украденные данные в даркнете. Киберпреступники заявили, что украли 259 ГБ данных компании.

Согласно комментариям пострадавшей компании для местных СМИ, атака коснулась трех локаций в Италии, пострадало примерно 15 процентов бизнеса в этой стране. Затронутые ИТ-системы были незамедлительно изолированы. ИТ-специалисты интенсивно работали, чтобы восстановить нормальную производительность. Команда киберзащиты тесно сотрудничала со своими ИТ-партнерами, а также с правоохранительными органами и органами по защите данных.

Vopak подверглась атаке вымогателей

Логистика, хранение топлива

Утечка данных

Ransomware

Нидерландская компания по хранению топлива в резервуарах Royal Vopak N.V. стала жертвой атаки вымогателей. Компания подтвердила, что произошел ИТ-инцидент на терминалах Pengerang Independent Terminals (PTSB) в Малайзии, следствием которого стал несанкционированный доступу к некоторым данным.

По словам генерального директора компании, кибератака не повлияла на её повседневную деятельность ни в данной локации ни в других местах в мире.

Vopak практически наверняка подверглась атаке группы вымогателей ALPHV/BlackCat, так как компания была включена злоумышленниками в список жертв на их сайте в даркнете. Предположительно, была украдена критическая информация компании, в том числе об инфраструктуре хранения топлива.

Производство еды и напитков

Группа Nutresa подверглась атаке вымогателей

Производство продуктов питания

Утечка данных, задержка отправки продукции

Ransomware

Grupo Nutresa, одна из ведущих компаний по производству переработанных продуктов в Колумбии, объявила о том, что стала жертвой атаки вымогателей 20 апреля. Атака повлияла на ее бизнес-процессы и отправку продукции.

Согласно информации от компании, сразу после выявления инцидента был активирован протокол, принятый для такого рода инцидентов, чтобы смягчить его потенциальное воздействие.

24 апреля группа Lockbit взяла на себя ответственность за эту кибератаку и несколько дней спустя опубликовала внутренние документы Nutresa.

Super Bock Group подвергся кибератаке

Производство, продукты питания и напитки

Отказ ИТ-систем, отказ отправки продукции

Португальская пивоваренная компания Super Bock Group стала объектом кибератаки, которая нарушила нормальную работу компьютерных служб, что повлияло на производственную деятельность. В выпущенном на LinkedIn заявлении компания добавила, что ситуация вызвала серьезные ограничения в операции поставок на рынок некоторой части её продукции. Компания активировала необходимые протоколы безопасности. Она также уведомила соответствующие органы по защите данных в Португалии и следовала экстренному плану для пополнения запасов на рынке.

Coca-Cola FEMSA подверглась кибератаке

Производство, напитки

Производитель напитков Coca-Cola FEMSA México объявил о том, что стал жертвой кибератаки. Компания провела расследование и одновременно приняла меры по защите и реагированию на киберугрозы, чтобы определить масштаб инцидента. Корпорация не уточнила, что именно произошло — кража данных или паролей или нарушение работы ее систем. В заявлении для Мексиканской фондовой биржи (BMV) было сказано, что «компания сотрудничает с экспертами для принятия мер предотвращения негативного воздействия на ее IT-приложения».

Schwälbchen Molkerei подверглась кибератаке

Производство, еда и напитки

Согласно заявлению, полученному местными новостными агентствами, немецкий производитель молочных продуктов Schwälbchen Molkerei Jakob Berz AG стал жертвой кибератаки. В результате атаки пострадала часть ИТ-инфраструктуры компании и была нарушена ее доступность. Текущее производство и логистика не пострадали. Была проведена работа по полному восстановлению систем. Неясно, получили ли злоумышленники доступ к данным компании, и если да, то какой объем информации был им доступен. Компания тесно сотрудничает с органами безопасности и внешним поставщиком услуг по ИТ-безопасности. Дополнительные детали предоставлены не были, тип атаки компания не уточнила.

Нефть и газ

Encino Energy подверглась кибератаке

Нефть и газ

Утечка данных

Ransomware

Encino Energy, американская компания-производитель природного газа и нефти, признала факт кибератаки после того, как группа BlackCat/ALPHV добавила компанию в список жертв на своем сайте в дарквебе.

Представитель Encino Energy не сообщил, была ли кибератака случаем вымогательства, заплатила ли компания выкуп, изучила ли 400 ГБ данных, опубликованных на сайте BlackCat/ALPHV. Он заявил, что инцидент не повлиял на деятельность компании и она продолжает работать в нормальном режиме.

Компания Encino Energy своевременно обнаружила несанкционированную деятельность, провела расследование и устранила проблему.

Suncor Energy подверглась кибератаке

Нефть и газ

Отказ в обслуживании клиентов

Канадская нефтяная компания Suncor подтвердила, что причиной широкомасштабных сбоев, приведших к остановке обслуживания 23 июня, стала кибератака. Клиенты сообщали о проблемах со входом в приложение и на веб-сайт сети заправочных станций Petro-Canada, принадлежащей Suncor. На некоторых заправочных станциях клиенты могли платить только наличными.

Согласно заявлению компании, были предприняты меры для смягчения последствий атаки, а власти были проинформированы о ситуации. Suncor предупредила клиентов и поставщиками о возможности перебоев в транзакциях до разрешения инцидента. Компания не предоставила подробностей о типе кибератаки и о том, была ли это атака вымогателей.

Shell подверглась кибератаке

Нефть и газ

0-day, MOVEit MFT

Ransomware

Британская международная нефтегазовая компания Shell 15 июня подтвердила, что ее системы пострадали от взлома группой вымогателей Cl0p. Злоумышленники эксплуатировали ранее неизвестную уязвимость в инструменте передачи файлов MOVEit. Сообщение об атаке появилось после того, как группа Cl0p добавила компанию в список жертв на своем сайте.

В пресс-релизе компания подчеркнула, что нет доказательств воздействия на её основные ИТ-системы и заявила, что ИТ-команды Shell продолжают расследование инцидента. Компания уточнила, что в данном случае «инцидент не был атакой вымогателей» (вероятно, злоумышленники придерживались стратегии похожей на ту, что и в атаке на Hitachi Energy). Представитель компании также заявил, что они не общаются с хакерами.

Судостроение

Lürssen подверглась кибератаке вымогателей

Производство, судостроение

Остановка операционной деятельности

Ransomware

Немецкий производитель судов Lürssen подтвердил 12 апреля, что стал жертвой кибератаки с использованием программы-вымогателя, произошедшей во время праздничных дней на Пасху. В сотрудничестве с внутренними и внешними экспертами компания немедленно приняла все необходимые меры по защите и уведомила соответствующие органы власти. Согласно местным новостям, инцидент привел к полной остановке большой части деятельности верфи Lürssen.

Fincantieri Marine Group подверглась кибератаке

Производство, судостроение

Отказ ИТ-систем, остановка производства

Ransomware

Американская судостроительная компания Fincantieri Marinette Marine подтвердила случай атаки с использованием программы-вымогателя в заявлении для USNI News и Green Bay Press-Gazette. Атака произошла 12 апреля и затронула сервер электронной почты и некоторые сетевые операции, вызвав задержку в производстве.

В заявлении указано, что специалисты по сетевой безопасности компании немедленно изолировали системы и сообщили об инциденте соответствующим органам и партнерам. Fincantieri Marine Group привлекла дополнительные ресурсы для расследования и скорейшего восстановления полной функциональности затронутых систем. Компания добавила, что нет доказательств компрометации персональной информации сотрудников.

Brunswick Corporation подверглась кибератаке

Производство, мореплавание, судостроение

Остановка производства и поставок: 9 дней

Американский производитель лодок и двигателей Brunswick Corporation 13 июня столкнулся с инцидентом информационной безопасности, который повлиял на некоторые из его систем и производственные объекты, расположенные по миру. Компания сообщила, что активировала свои протоколы реагирования, включая приостановку деятельности на некоторых объектах, привлечение ведущих экспертов по безопасности и сотрудничество с соответствующими правоохранительными органами.

Brunswick сообщила, что работает над устранением инцидента, чтобы восстановить полную функциональность затронутых систем и минимизировать влияние на бизнес, сотрудников и клиентов. В пресс-релизе, опубликованном 22 июня, компания заявила, что добилась значительных успехов в восстановлении функциональности своих систем и возобновлении операционной деятельности на объектах, где было приостановлено производство или поставки. Все основные производственные и большинство распределительных объектов Brunswick были вновь запущены, возобновление работы остальных производственных и распределительные объекты ожидались к в течение нескольких рабочих дней.

Фармацевтика

Eisai подверглась атаке вымогателей

Производство, фармацевтика

Отказ в IT-сервисах, отказ логистических систем

Ransomware

Японская фармацевтическая компания Eisai объявила о том, что стала жертвой атаки вымогателей. Компания имеет производственные объекты в Азии, Европе и Северной Америке, а также филиалы на обоих американских континентах, в регионе Азиатско-Тихоокеанского бассейна, в Африке и Европе.

Атака вымогателей была обнаружена 3 июня и привела к шифрованию нескольких серверов как в Японии, так и за рубежом, в том числе логистических систем. Корпоративные веб-сайты и электронные системы компании остались работоспособными.

Eisai сообщила, что немедленно активировала свой план реагирования на инцидент, который предполагал отключение от сети пострадавших систем для локализации атаки, и начала расследование. Eisai Group немедленно создала рабочую группу и начала работу по восстановлению с учетом рекомендаций внешних экспертов и принимая меры для понимания масштабов инцидента. Кроме того, Eisai Group проконсультировалась с правоохранительными органами. Eisai заявила, что должна выяснить, были ли скомпрометированы или украдены какие-либо данные в ходе атаки.

Virbac подверглась кибератаке

Производство, фармацевтика

Отказ в IT-сервисах

Французский производитель ветеринарных медикаментов компания Virbac, согласно сообщению на ее веб-сайте, стала объектом кибератаки на нескольких своих объектах по всему миру ночью 19-20 июня. Как только компания узнала об атаке, она немедленно предприняла меры для ее локализации и создала кризисный центр, включая специалистов по кибербезопасности, чтобы оценить влияние на системы и организовать мероприятия по устранению последствий. В результате этой атаки компания столкнулась с замедлением или временным прерыванием работы некоторых своих сервисов. Virbac не уточнила тип атаки и не предоставила дополнительных подробностей.

Металлургия

Badische Stahlwerke подверглась кибератаке

Производство, сталь

Отказ IT-систем

Немецкий производитель стали Badische Stahlwerke GmbH в Кельне сообщил на своем веб-сайте о несанкционированном доступе к сети компании 20 апреля. Компания интенсивно работала для тщательного и быстрого выяснения обстоятельств инцидента. Из-за отключения и проверки затронутых систем сотрудники временно были недоступны по электронной почте и стационарному телефону. Согласно сообщению регионального новостного портала, полиция в Оффенбурге подтвердила атаку, начато расследование.

Haynes International подверглась кибератаке

Производство, металлургия, сплавы

Отказ IT-систем, задержка поставки

Производитель сплавов Haynes International со штаб-квартирой в США сообщил в пресс-релизе о выявлении 10 июня сбоя в сети, свидетельствующего об инциденте кибербезопасности. По обнаружении инцидента компания привлекла специалистов сторонних компаний для помощи в расследовании источника сбоя, определения его потенциального влияния на системы компании и безопасного восстановления полной функциональности систем компании.

Несмотря на то, что различные сервисы Haynes International были недоступны во время устранения инцидента, все производственные функции компании работали, пусть и с некоторыми ограничениями. Кроме того, на момент заявления, компания в значительной степени восстановила административные, коммерческие, финансовые и обслуживающие клиентов функции.

Компания не предоставила информацию о причинах инцидента, но заявила, что расследование и усилия по восстановлению все еще продолжаются. Компания сообщила, что задержка в поставках продукции возникла в ходе работ по реагированию на инцидент.

Другое

Военная промышленность. Solar Industries подверглась кибератаке

Производство, военно-оборонная промышленность

Утечка данных

Ransomware

Материнская компания частного поставщика министерства обороны и производителя военной техники Solar Industries Limited India, предположительно, подверглась атаке с использованием программы-вымогателя Windows Alphv (также известной как BlackCat). Группа, стоящая за атаками этим вредоносным ПО, опубликовала ряд документов в даркнете и утверждает, что украла у компании 2 ТБ данных.

Официально компания этого не подтвердила и отказалась от комментариев, однако информацию подтвердил не названный представитель правительства. Как заявили полицейские, соответствующий случай также был зарегистрирован в полицейском участке киберполиции Нагпура 25 января.

Сайт компании был недоступен 29 января. Согласно местным новостным источникам, хакерская группа проникла в Solar Group 21 января и потребовала выкуп. Компания не ответила на требования и сразу же сообщила об инциденте Компьютерной службе реагирования на чрезвычайные ситуации Индии (CERT-In).

Инжиниринг. Vesuvius подверглась атаке вымогателей

Инжиниринг, металл, керамика

Отказ в обслуживании

Ransomware

Британская инжиниринговая компания Vesuvius, известная на рынке металла и керамики, объявила о киберинциденте, который привел к отключению систем. Компания сотрудничала с ведущими экспертами по кибербезопасности для поддержки расследований и определения масштаба ущерба, включая влияние на производство и выполнение контрактов. Компания предприняла шаги для соблюдения всех соответствующих регулирующих обязательств. Группа хакеров Vice Society заявила о своей ответственности за кибератаку на Vesuvius и опубликовала в даркнете файлы, которые она похитила у компании.

Горнодобывающая отрасль. Утечка данных Rio Tinto

Горнодобывающая промышленность

Утечка данных, утечка персональных данных

Уязвимость GoAnywhere MFT

Ransomware

5 апреля англо-австралийская горнодобывающая корпорация Rio Tinto Group подтвердила местным новостным агентствам, что украденные в марте через сторонний сервис безопасной передачи файлов GoAnywhere MFT данные сотрудников были размещены в даркнете.

Ещё 23 марта Rio Tinto сообщила сотрудникам, что «сторонняя кибератака на одного из её поставщиков» могла подвергнуть риску персональные данные её нынешних и бывших сотрудников в Австралии. Хотя со стороны киберпреступной группы и были угрозы опубликовать данные в даркнете, у компании не было уверенности, что злоумышленники действительно этими данными обладают.

Однако группа хакеров Cl0p, заявившая об ответственности за взлом данных Rio Tinto, выложила много данных компании на своей странице в даркнете.

По заявлению представителя Rio Tinto, компания связалась со всеми пострадавшими, чтобы предоставить им информацию об украденных данных и предложить полную поддержку.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com