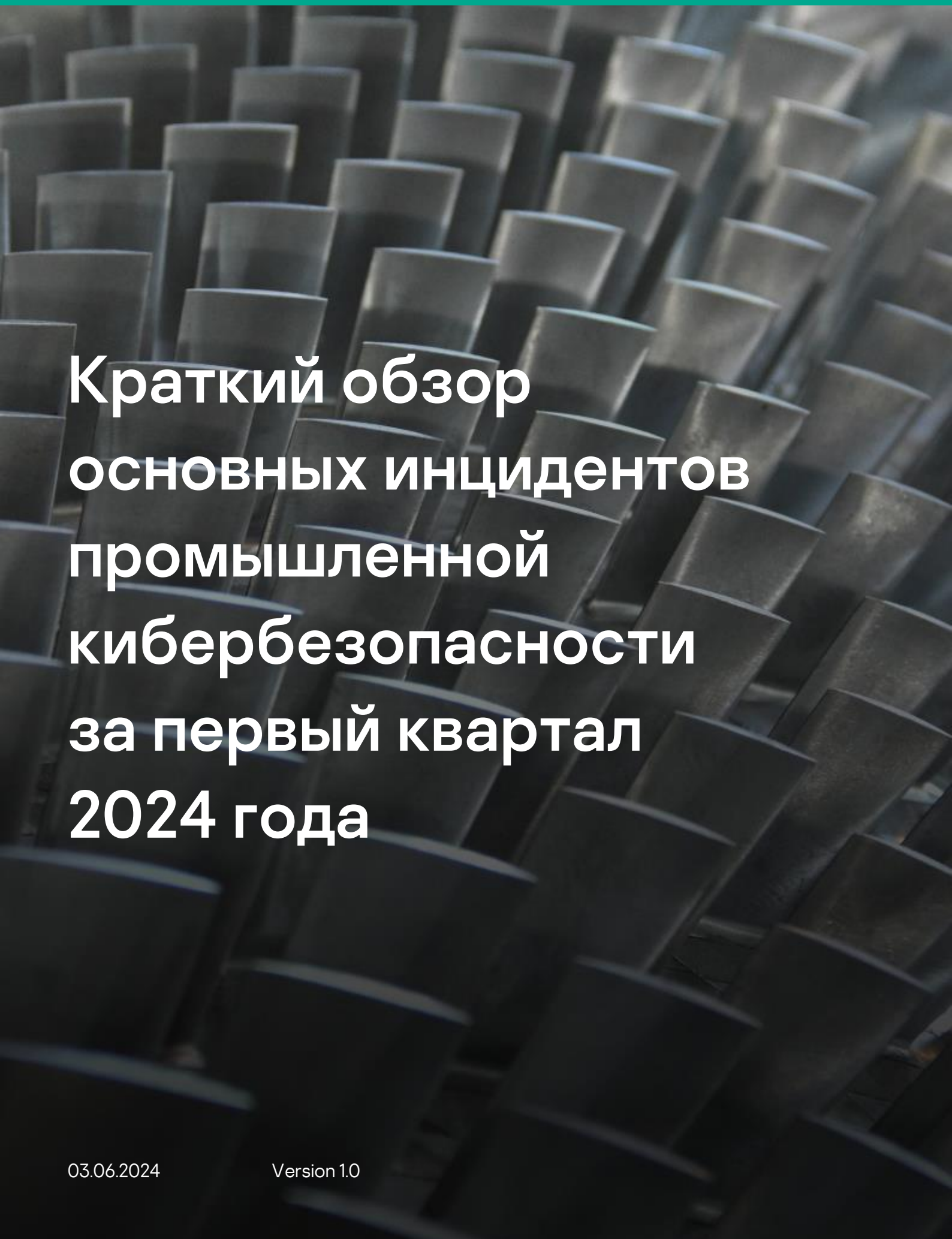


Краткий обзор основных инцидентов промышленной кибербезопасности за первый квартал 2024 года

03.06.2024 Version 1.0

В этом обзоре мы расскажем об инцидентах, связанных с атаками злоумышленников на промышленные предприятия. Обзору технических исследований атак, опубликованных в первом квартале 2024 г, посвящен отдельный отчет.

Некоторые ссылки на сайты компаний, где была опубликована информация об инцидентах, ко времени публикации отчёта могут не работать, если соответствующая информация была удалена. Тем не менее, все ссылки сохранены в тексте, чтобы подчеркнуть, что в основе нашего отчета лежат заявления пострадавших компаний.

Достоверность всей информации об инцидентах, с которой мы предлагаем вам ознакомиться, публично подтверждена пострадавшими организациями или ответственными госорганами. Официально неподтвержденные заявления злоумышленников о компрометации в отчете сознательно не рассматриваются.

Краткая статистика по кварталу

- В общей сложности жертвами подтверждено **30 инцидентов**. Это хорошо согласуется с предыдущими периодами (более 60 публично подтвержденных случаев за полгода).
- **37%** жертв сообщили о **нарушении операционной деятельности или задержках в отгрузке продукции** в результате инцидента — эта доля почти такая же, как и в предыдущем периоде (37,5% во второй половине 2023 года).
- Почти половина (**47%**) всех инцидентов привела к тому, что жертвам пришлось **остановить работу своих публичных цифровых сервисов**.
- Пострадали представители таких сфер, как промышленное производство (включая автомобильную, аэрокосмическую, фармацевтическую, текстильную, косметическую, пищевую промышленности и некоторые другие производственные секторы), **коммунальное хозяйство, энергетика, транспорт и логистика, машиностроение** и **горнодобывающая промышленность**.
- **2/3** жертв относятся к сфере **производства. 50%** всех жертв из сферы производства сообщили о нарушении операционной деятельности, что составляет **100%** от общего числа жертв, подтвердивших останов операционной деятельности в результате атаки. Организации из этой сферы либо менее устойчивы к атакам, либо просто более честно сообщают общественности о произошедшем.
- Ни одна из жертв, работающих с критически важными инфраструктурами, например из сфер энергетики и коммунального хозяйства, не сообщала о каком-либо значительном ущербе — к этому уже все привыкли.
- **Наиболее пострадавшие страны:**
  - **США — 1/6 всех жертв;**
  - **Германия — 1/6 всех жертв;**
  - **Франция, Бельгия и Нидерланды — по 1/10 части.**
- В числе пострадавших также есть страны, в которых мы редко видим публичное подтверждение инцидентов: **Северная Македония, Южная Африка и Сингапур.**

Январь

- Lush
- Foxsemicon
- Schneider Electric
- Benetton
- Veolia
- Hewlett Packard
- Southern Water
- Muscatine Power and Water

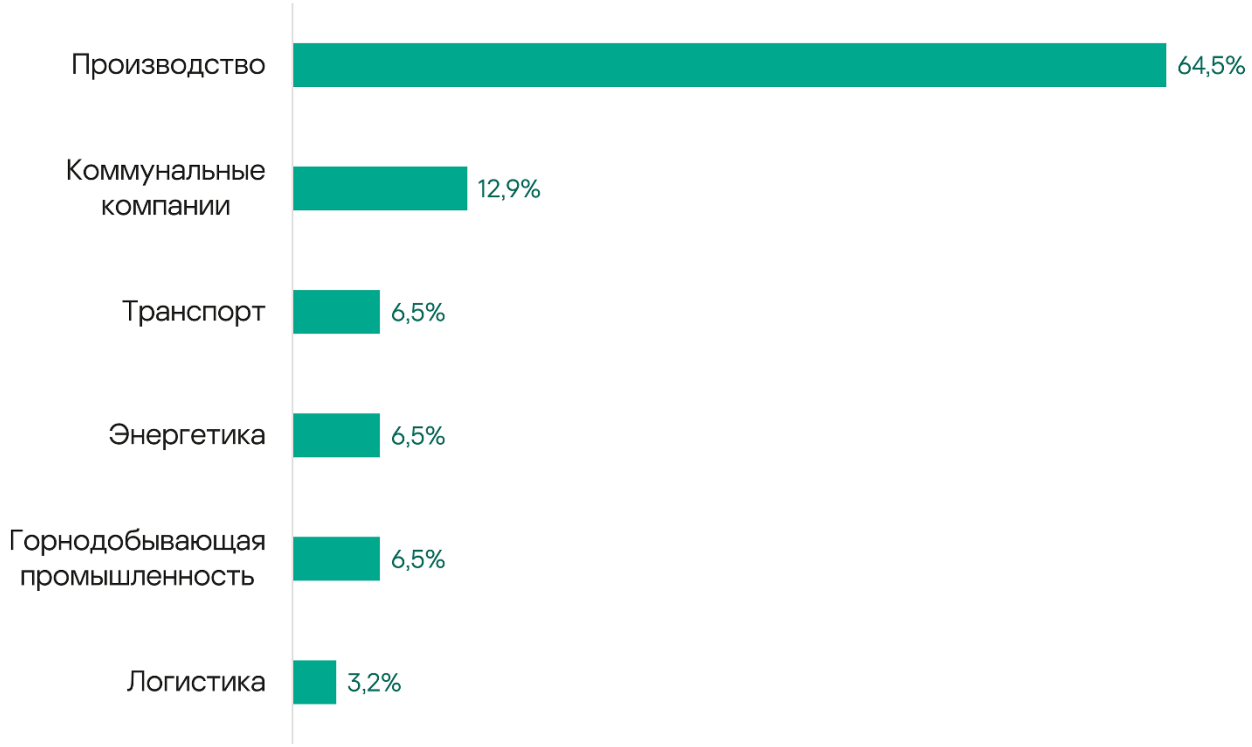
Февраль

- Etesia
- Kind
- Varta
- Aztech Global
- ThyssenKrupp
- AB Texel
- GCA
- HAL Allergy
- Continental Aerospace
- International Paper
- Kampf
- EAS

Март

- Koffie Beyers
- Stadtwerke Bruck
- Sprimoglass
- Duvel Moortgat
- MEPSO
- Radiant Logistics
- BerlinerLuft
- Polycab
- Nampak

2024



Производственный сектор

Атака на компанию Lush

Производственный сектор

Утечка данных, отказ ИТ-сервисов

Программы-вымогатели

Британский производитель косметики Lush подвергся кибератаке. Как стало известно 11 января, компания приняла срочные меры по защите и изоляции всех своих систем, чтобы локализовать инцидент и минимизировать его воздействие на бизнес. Компания пригласила сторонних специалистов по ИТ-криминалистике для проведения тщательного расследования. Также компания Lush проинформировала соответствующие органы об инциденте. О характере инцидента изначально ничего не сообщалось. 25 января имя компании Lush появилось на сайте с похищенными данными, принадлежащем вымогательской группе Akira. Группа заявила, что похитила у Lush 110 ГБ данных, в том числе большое количество информации, содержащей персональных данные, такой как сканы паспортов, а также корпоративных документов, относящихся к бухгалтерскому учету, финансам, налогам, проектам и клиентам. 29 января представитель Lush в новом заявлении сообщил, что в компании произошел инцидент с заражением шифровальщиком, повлекший за собой временный несанкционированный доступ к части ее британской ИТ-инфраструктуры. Компания незамедлительно приняла меры по противодействию, и после короткого периода, когда организация испытывала незначительные проблемы, компания вернулась к обычному режиму работы. Чтобы проверить заявления злоумышленников о похищенных данных, компания Lush обратилась к партнерам-специалистам.

Кибератака на Benetton

Производственный сектор

Отказ ИТ-систем, отказ сервисов и нарушение операционной деятельности

Итальянский производитель одежды Benetton стал жертвой кибератаки в ночь с 18 на 19 января, говорится в сообщении компании. Пострадали серверы электронной торговли и системы логистического центра компании в Кастретте-ди-Виллорба. Логистические операции были нарушены, и сотрудников отпустили домой. Как сообщается, в течение нескольких дней наблюдались неполадки из-за вынужденных перебоев в работе серверов. Они были оперативно отключены, чтобы защитить всю ИТ-инфраструктуру и изолировать ее от внешних атак. Штатная команда по противодействию вмешательству в ИТ-системы быстро среагировала и приняла все необходимые контрмеры, чтобы устранить последствия атаки и обеспечить нормальную работу практически всей глобальной коммерческой сети. С понедельника, 23 января, компания планирует возобновить значительную часть рабочих процессов во всех регионах.

Кибератака на Varta

Производственный сектор, автомобилестроение

Отказ ИТ-систем, нарушение операционной деятельности

Немецкая компания Varta, производящая аккумуляторы для автомобильного, промышленного и потребительского секторов, сообщила, что 12 февраля ее системы подверглись кибератаке. В результате инцидента были нарушены производственные и административные процессы на пяти заводах компании. Varta отключила свои ИТ-системы и соединение с интернетом на время расследования инцидента. Компания заявила, что реализовала меры, предусмотренные планом действий в чрезвычайных ситуациях, и сформировала рабочую группу, состоящую из экспертов по кибербезопасности и специалистов по ИТ-криминалистике, которые будут помогать в восстановлении системы. 22 февраля компания Varta выпустила новое сообщение, уточнив, что доступность ее систем все еще ограничена. В сообщении не было сказано, сколько потребуется времени на устранение последствий атаки и когда будет полностью восстановлено производство на всех пяти фабриках в разных странах. Ожидалось, что заводы частично заработают в течение следующей недели после выпуска сообщения. Были возобновлены процессы, не связанные с ИТ, — в частности, на все заводы были направлены сотрудники для проведения технического обслуживания, ремонта и подготовительных работ. Власти были проинформированы о ситуации, а полиция официально начала расследование.

Атака на Aztech Global

Производственный сектор

Отказ ИТ-систем

Программы-вымогатели

12 февраля компания Aztech Global, сингапурский поставщик производственных услуг, объявила о том, что стала жертвой шифровальщика, в результате чего злоумышленникам удалось получить несанкционированный доступ к компьютерной сети компании. Компания приняла срочные меры, в частности отключила свои серверы на время каникул в период китайского Нового года и защитила остальные данные специализированным ПО. Aztech Global также привлекла сторонних- экспертов по ИТ-криминалистике для расследования инцидента, проинформировала о нем соответствующие органы власти, а также запросила рекомендации по повышению ИТ-безопасности.

Кибератака на Continental Aerospace

Производственный сектор

Нарушение операционной деятельности

Компания Continental Aerospace, американский производитель авиационных двигателей, стала жертвой кибератаки, которая нарушила ее операционную деятельность. 20 февраля на баннере своего сайта компания сообщила, что совместно со специалистами работает над решением проблемы и надеется скоро возобновить нормальную работу. Никаких дополнительных сведений о том, чем закончилась атака и каковы масштабы нарушений в работе компании, а также о возможной утечке данных предоставлено не было. Continental Aerospace активно взаимодействовала с командой специалистов, которые приложили все усилия для скорейшего решения проблемы.

Кибератака на Etesia

Производственный сектор

Отказ ИТ-систем, отказ сервисов, нарушение операционной деятельности

По сообщению местной прессы, 2 февраля французская компания Etesia, производящая косильное оборудование, стала жертвой кибератаки, в результате чего 160 сотрудников компании перешли на неполный рабочий день. Атака нарушила телефонную связь, систему электронной почты и внутренние процессы производства. С 20 февраля деятельность компании начала постепенно возобновляться после полной блокировки.

Кибератака на Kind

Производственный сектор

Отказ ИТ-систем, отказ сервисов

Немецкая компания Kind, производящая слуховые аппараты, 6 февраля подверглась кибератаке. По словам представителя компании, возникли нарушения в работе ИТ-системы. Собственный ИТ-отдел компании начал принимать меры реагирования. Компания уведомила об инциденте полицию и инспектора по защите персональных данных. Была нарушена связь с более чем 600 специализированными магазинами. После сбоя в работе ИТ-системы связь была возможна только по телефону. Заказы нельзя было оформить электронно, поэтому иногда приходилось записывать их от руки на бумаге. Свидетельства кражи данных клиентов не были обнаружены. Системы были немедленно остановлены, проверены внешними специалистами и постепенно снова введены в эксплуатацию.

Кибератака на International Paper

Производственный сектор
Отказ ИТ-систем
Атака на цепочку поставок / доверенного партнера

Американская компания International Paper по производству бумаги и упаковки подверглась кибератаке, согласно ее заявлению. Компания приступила к реализации планов по сдерживанию атаки и реагированию на инцидент, а также уведомила соответствующие органы власти. На всякий случай International Paper организовала плановое закрытие фабрики и в настоящее время приступила к ее запуску. Представитель компании сообщил, что злоумышленники получили доступ к системе International Paper через стороннего производителя и что их компания или фабрика не являлись непосредственной целью атаки. Атака затронула лишь часть производственных систем на фабрике Riegelwood Mill. Другие фабрики, производственные объекты или системы не пострадали. Компания не располагает сведениями об утечке каких-либо конфиденциальных, служебных, личных или бизнес-данных.

Атака на Polycab

Производственный сектор
Программы-вымогатели

Индийская компания Polycab, производитель кабелей, проводов и сопутствующих товаров, 17 марта подверглась атаке на свою ИТ-инфраструктуру с применением шифровальщика. Согласно отчету, поданному в регулирующие органы, инцидент не повлиял на основные системы и операции компании. Системы компании и все ее заводы продолжили работу в штатном режиме. Техническая команда компании вместе со специальной группой внешних экспертов по кибербезопасности активно работала над анализом инцидента. 26 марта оператор шифровальщика LockBit добавил Polycab в список жертв на своем сайте в даркнете.

Атака на Nampak

Производственный сектор
Утечка данных, утечка персональных данных, отказ ИТ-систем
Программы-вымогатели

Южноафриканская компания по производству упаковочной продукции Nampak обнаружила 20 марта несанкционированную активность в своих ИТ-системах. Nampak разместила заявление на своем сайте, где сообщила, что неизвестная третья сторона получила доступ к ее ИТ-системам, несмотря на «надежные протоколы безопасности». Компания немедленно приступила к локализации, оценке и устранению последствий инцидента. Nampak приняла все необходимые меры, чтобы определить масштаб компрометации, восстановить целостность своих информационных систем и исключить возможные дальнейшие риски. Компания заявила, что инцидент не повлиял на производственные объекты и технологические процессы,

которые функционируют в обычном режиме, за исключением перевода некоторых систем на ручное управление. Nampak направила первичное уведомление в регулирующий орган по информационной безопасности. 26 марта оператор шифровальщика LockBit добавил Nampak в список жертв на своем сайте в даркнете. 4 апреля Nampak выпустила новое заявление, где говорилось, что затронутые атакой данные могли включать файлы, относящиеся к юридическим, финансовым и кадровым подразделениям Nampak. В этих файлах могла быть определенная персональная информация, касающаяся физических и юридических лиц.

Атака на Sprimoglass

Производственный сектор

Отказ сервисов, нарушение операционной деятельности, задержки поставок продукции

Программы-вымогатели

Как стало известно в начале марта, бельгийская стекольная компания Sprimoglass подверглась кибератаке, повлекшей за собой остановку производства. По данным видеосюжета местного СМИ, компания узнала о кибератаке 23 февраля и не работала около 10 дней. Около шестисот-семисот компьютеров пришлось полностью переформатировать. На момент съемки видеорепортажа несколько производственных линий уже работали в течение трех дней с участием 20–30% штата сотрудников. Остальные работники простаивали по техническим причинам. Это серьезно сказалось на персонале компании и на поставках клиентам, которые пришлось отложить. Представители компании заявили, что производство будет восстановлено должным образом, постепенно, без выплаты выкупа.

Кибератака на BerlinerLuft

Производственный сектор, машиностроение

Отказ ИТ-систем, нарушение операционной деятельности

Немецкая компания BerlinerLuft, занимающаяся разработкой и производством заводского оборудования, 16 марта стала жертвой кибератаки. Согласно сообщению на сайте компании, она стала недоступна для связи по телефону и электронной почте. Команда компании приложила все усилия, чтобы как можно быстрее восстановить доступность. Компания предупредила, что в связи с экстренной ситуацией в ее ИТ-инфраструктуре возможны кратковременные ограничения при проведении деловых операций, а также сбои в технологических процессах и задержки поставок. Компания уведомила об инциденте правоохранительные органы и государственные органы по защите персональных данных. 27 марта компания выпустила новое сообщение, где говорилось, что производство компонентов воздуховодов, клапанов жалюзи и звукоизоляционных перегородок на немецком и польском заводах возобновлено, а также восстановлена работа электронной почты и телефонной связи.

Атака на EAS

Производственный сектор, Машиностроение

Утечка данных, нарушение операционной деятельности

Программы-вымогатели

Голландская производственная компания EAS Europe, по информации с ее сайта, 26 февраля стала жертвой атаки с применением шифровальщика. Злоумышленники зашифровали серверы EAS Europe и, возможно, похитили конфиденциальные данные с серверов EAS. Возможно, были похищены данные клиентов и поставщиков. EAS привлекла компанию по кибербезопасности, чтобы оценить масштаб инцидента и повысить уровень кибербезопасности и защиты данных. Инцидент привел к остановке операционной деятельности компании в Нидерландах на период восстановления данных из резервных копий. 6 апреля вымогательская группа Qilin добавила в список своих жертв компанию EAS change systems.

Атака на Kampf

Производственный сектор, Машиностроение

Отказ ИТ-систем

Программы-вымогатели

24 февраля немецкая машиностроительная компания Kampf GmbH стала жертвой кибератаки. Злоумышленники применили специализированное ПО, частично зашифровав ИТ-системы компании. Согласно сообщению на сайте компании, она немедленно отключила все внешние каналы связи и остановила работу всех ИТ-систем. Компания Kampf расследовала масштабы атаки при поддержке внешних экспертов по кибербезопасности и специалистов по криминалистике. Компания проинформировала об инциденте соответствующие органы и сотрудничала с ними по всем вопросам. Компания не исключила возможность того, что данные были похищены. В новом сообщении от 4 марта компания заявила, что все предприятия группы Kampf, которые были отключены от Сети в качестве меры предосторожности, вернулись к нормальной работе, за исключением Kampf GmbH и Atlas Converting Equipment Ltd. Все остальные предприятия группы Jagenberg работали без ограничений.

Электронная промышленность

Атака на Foxsemicon

Производственный сектор, электронная промышленность

Отказ ИТ-сервисов

Программы-вымогатели

15 января жертвой кибератаки стала компания Foxsemicon Integrated Technology, производящая полупроводниковое оборудование и являющаяся дочерним предприятием крупнейшей тайваньской компании по производству электроники Foxconn. Сайт компании был взломан, и на нем появилось сообщение о том, что данные компании похищены и зашифрованы. Если верить сообщению, было похищено 5 ТБ корпоративных данных. Злоумышленники утверждали, что получили персональные данные клиентов и сотрудников, и угрожали обнародовать их на своем сайте с утекшими данными, если не будет заплачен выкуп. Вымогательская группа не раскрыла своего имени на взломанном сайте Foxsemicon, но предоставленные ею ссылки вели на Tor-сайт LockBit, где публиковались утекшие данные. Вскоре после инцидента компания уведомила Тайваньскую фондовую биржу, что сайт был восстановлен сразу после обнаружения атаки шифровальщика и что проблемой занимаются эксперты по безопасности. Однако различные разделы сайта, включая английскую и китайскую версии, а также его корпоративный и финансовый разделы, оставались недоступными. Компания Foxsemicon также добавила, что инцидент не должен существенно повлиять на ее операционную деятельность.

Кибератака на Hewlett Packard

Производственный сектор, электронная промышленность

Утечка данных

APT-угрозы

19 января компания Hewlett Packard Enterprise подала заявление по форме 8-K в Комиссию по ценным бумагам и фондовому рынку США (SEC), сообщив о несанкционированном доступе к облачной системе электронной почты компании со стороны APT-группы — предположительно Midnight Blizzard (также известной как Dukes, CozyBear и NOBELIUM/APT29/BlueBravo). HPE была уведомлена о кибератаке 12 декабря 2023 года неизвестным субъектом. Предполагается, что злоумышленники получили доступ к данным и занимались их эксфильтрацией с мая 2023 года. Были получены и похищены корпоративные данные из «небольшого процента» почтовых ящиков HPE и «ограниченного числа» файлов SharePoint, принадлежащих сотрудникам службы кибербезопасности и других подразделений. При содействии внешних экспертов по кибербезопасности компания немедленно запустила процесс реагирования, чтобы расследовать, локализовать и устранить инцидент, ликвидировав вредоносную активность.

Автомобильная отрасль

Кибератака на ThyssenKrupp

Производственный сектор, автомобилестроение

Нарушение операционной деятельности

Немецкая компания ThyssenKrupp, производитель стали и автомобильных компонентов, заявила, что подверглась кибератаке, затронувшей подразделение компании по производству автомобильных кузовов — ThyssenKrupp Automotive Body Solutions. В Automotive Body Solutions смогли обнаружить инцидент на раннем этапе и с того момента прилагали усилия, чтобы локализовать и устранить угрозу и ее последствия. При этом ThyssenKrupp уточнила, что другие подразделения или сегменты производства не пострадали. Был принят ряд различных мер безопасности, а некоторые приложения и системы были временно отключены. Немецкое новостное издание первым обнародовало информацию об этой атаке, сообщив, что она непосредственно затронула завод ThyssenKrupp в Саарланде с более чем тысячей сотрудников. Компания подтвердила изданию BleepingComputer остановку производства, но отметила, что это никак не повлияло на поставки клиентам.

Фармацевтическая отрасль

Атака на HAL Allergy

Производственный сектор, фармацевтика

Утечка данных, отказ сервисов, задержка в поставке продукции

Программы-вымогатели

19 февраля голландская фармацевтическая компания HAL Allergy Group, по информации с ее сайта, стала жертвой атаки с применением шифровальщика. Компания могла столкнуться с задержками в обработке заказов или доставке продукции. HAL Allergy немедленно привлекла внешних экспертов по кибербезопасности для помощи в восстановлении затронутой атакой сети, после чего было начато криминалистическое расследование. Компания не исключает, что были скомпрометированы персональные данные физических лиц. Среди мер, принятых компанией, — отключение сети от интернета, восстановление данных, уведомление Голландской службы по защите данных, обращение в полицию Нидерландов. 28 февраля вымогательская группа RansomHouse добавила HAL Allergy в список жертв на своем даркнет-сайте.

Пищевая промышленность

Атака на Duvel Moortgat с применением шифровальщика

Производственный сектор, пищевая промышленность

Нарушение операционной деятельности

Программы-вымогатели

Бельгийская пивоваренная компания Duvel Moortgat подтвердила местной прессе, что стала жертвой шифровальщика. Производство практически остановилось. Кибератака была обнаружена 6 марта на пивоваренном заводе в провинции Антверпен. По всей видимости, серверы были заражены вредоносным ПО и выведены из строя. Как пояснила представительница компании, от инцидента пострадали объекты компании в Бельгии и один объект в США. ИТ-отдел немедленно приступил к работе, пытаясь выяснить суть произошедшего. Производство в Антверпене возобновилось 7 марта. Вымогательская группа Stormous взяла на себя ответственность за произошедшую 7 марта кибератаку на пивоваренную компанию Duvel Moortgat и заявила, что было похищено 88 ГБ данных. 12 марта группа Black Basta на своем даркнет-сайте также добавила в список жертв компанию Duvel Moortgat и принадлежащую Duvel пивоварню Boulevard Brewing в США.

Кибератака на Koffie Beyers

Производственный сектор, пищевая промышленность

По данным полиции, бельгийская компания — производитель кофе Koffie Beyers подверглась кибератаке. Расследование продолжается, и пока неясно, каковы последствия атаки. Полиция также выясняет, нет ли здесь связи с кибератакой на Duvel Moortgat, — компании пострадали примерно в одно и то же время и расположены менее чем в полутора километрах друг от друга в муниципалитете Пюр-Сент-Аманд. Проводится отдельное расследование, но полиция сравнит эти инциденты, чтобы выяснить, есть ли между ними сходство.

Коммунальные службы

Кибератака на Southern Water

Водоснабжение, коммунальные службы

Утечка персональных данных

Британская частная коммунальная компания Southern Water признала факт кражи данных из некоторых ее ИТ-систем. В заявлении компании от 23 января говорится, что ранее она обнаружила подозрительную активность и начала расследование под руководством независимых специалистов по кибербезопасности. По словам компании, нет никаких признаков того, что атака повлияла на системы взаимодействия с клиентами или финансовые системы. Сервисы компании не пострадали и работали в нормальном режиме. Компания Southern Water проинформировала об инциденте правительство, регулирующие органы и Управление комиссара по информации. Операторы шифровальщика Black Basta заявили о причастности к атаке, опубликовав фрагмент предположительно похищенных ею данных: сканы различных удостоверений, таких как паспорта и водительские права; документы из отдела кадров с персональными данными клиентов, включающие домашний адрес, адрес офиса, дату рождения, гражданство и адреса электронной почты; а также корпоративные документы об аренде автомобилей, содержащие личные данные.

Атака на Veolia

Водоснабжение, коммунальные службы

Отказ ИТ-систем, отказ сервисов, утечка персональных данных

Программы-вымогатели

Североамериканское водоснабжающее подразделение французской транснациональной коммунальной компании Veolia столкнулось с инцидентом, в ходе которого шифровальщик проник в некоторые ее приложения и системы. ИТ-специалисты и группа реагирования на инциденты безопасности компании оперативно включились в работу и совместно с правоохранительными органами и другими внешними организациями расследовали инцидент и устранили его последствия. В заявлении, опубликованном 19 января, говорится, что компания приняла защитные меры, в частности отключила от интернета затронутые системы и серверы до тех пор, пока их работа не будет восстановлена. Атака шифровальщика не нарушила работу систем водоснабжения и водоотведения. Некоторые клиенты столкнулись с задержками при использовании онлайн-систем оплаты счетов. В ходе расследования компания обнаружила некоторое количество людей, чьи личные данные, возможно, пострадали.

Атака на Muscatine Power and Water

Водоснабжение, энергетика, коммунальные службы

Отказ ИТ-систем, утечка персональных данных

Программы-вымогатели

Американская коммунальная компания Muscatine Power and Water (MPW) столкнулась с инцидентом кибербезопасности, затронувшим ее корпоративную сетевую среду. После кратковременного сбоя в работе корпоративных систем компании был проведен тщательный внутренний и внешний анализ инцидента, и все системы MPW вернулись в рабочее состояние. Согласно пресс-релизу, опубликованному на сайте компании 29 января, вся офисные, полевые и генерирующие объекты компании продолжили работу в обычном режиме. Компания сотрудничала с группой экспертов-криминалистов, чтобы полностью понять масштабы и последствия этого инцидента и восстановить работу в исправленной и безопасной сетевой среде. Позже MPW выпустила новое сообщение, где подтвердила инцидент с применением шифровальщика, выявленный 26 января. В сообщении говорится, что команда MPW быстро включилась в работу и развернула новое оборудование, чтобы восстановить работу интернет-служб в течение 8 часов. В те же выходные были восстановлены затронутые инцидентом бизнес-системы MPW, что позволило компании начать нормальную работу к 8 утра понедельника. MPW также уведомила об инциденте правоохранительные и регулирующие органы штата и федеральные власти. В ходе криминалистического расследования выяснилось, что некоторые данные настоящих и бывших клиентов (адрес, номер социального страхования, водительские права и т. д.) потенциально могли быть раскрыты в ходе этого инцидента.

Кибератака на Stadtwerke Bruck

Энергетика, коммунальные службы

Отказ ИТ-систем

4 марта австрийская коммунальная компания Stadtwerke Bruck столкнулась с инцидентом безопасности в ИТ-системах городского управления коммунального хозяйства. Согласно сообщению на сайте компании, затронутые инцидентом сервисы были быстро восстановлены, и ее системы снова стали доступна с 11 марта. Бизнес-данные удалось восстановить из резервных копий. Чтобы получить представление о характере и ходе этого инцидента и выработать потенциальные контрмеры, было проведено криминалистическое расследование. На момент публикации сообщения не было никаких признаков того, что из систем компании были эксфильтрованы какие-либо данные. В целях обеспечения прозрачности ответственным органам был представлен предварительный отчет.

Энергетика

Кибератака на MEPSO

Энергетика
Отказ ИТ-систем

Оператор системы ЛЭП Республики Северная Македония (MEPSO) подтвердил, что подвергся кибератаке. В пресс-релизе от 7 марта компания подчеркнула, что киберинцидент не был направлен на ее критически важную энергетическую инфраструктуру, которая остается защищенной и полностью работоспособной. MEPSO заверила, что целостность электросети и процесс электроснабжения не были нарушены. В соответствии с требованиями регулятора компания сообщила о кибератаке в соответствующие органы. Команда MEPSO совместно с экспертами по кибербезопасности приложила все усилия для смягчения последствий кибератаки и нормализации текущей деятельности компании. 11 марта MEPSO объявила о том, что ее веб-сайт функционирует должным образом. MEPSO утверждает, что за разблокировку частей взломанной информационной системы выкуп не требовался.

Атака на Schneider Electric

Энергетика
Утечка данных, отказ ИТ-сервисов
Программы-вымогатели

Как стало известно изданию BleepingComputer, 17 января произошла атака с применением шифровальщика на подразделение «устойчивости бизнеса» французской транснациональной энергетической компании Schneider Electric. Компания Schneider Electric была атакована шифровальщиком Cactus, в результате чего были похищены корпоративные данные. Атака привела к частичному нарушению работы облачной платформы Resource Advisor компании Schneider Electric. В комментарии редакции BleepingComputer компания Schneider Electric заявила, что атака была направлена лишь на одно это подразделение и не затронула остальные части компании. Сотрудники подразделения связались с клиентами, пострадавшими от атаки. Детальный анализ инцидента продолжился с привлечением ведущих компаний в области кибербезопасности. Компания приложила усилия для восстановления работы подразделения в течение двух дней после подтверждения инцидента. Позже компания опубликовала на своем сайте то же самое заявление, добавив к нему, что доступ к бизнес-платформам был возобновлен 31 января.

Логистика и транспорт

Кибератака на GCA

Транспорт, логистика

Отказ ИТ-сервисов

Французская транспортно-логистическая компания GCA (Groupe Charles André) подверглась кибератаке в ночь с 17 на 18 февраля. Как сообщается в письме, разосланном компанией ее клиентам, инцидент привел к отключению доступа в интернет и стандартных средств коммуникации. На данный момент сообщений об утечке данных не поступало. Компания провела расследование с привлечением внешних специалистов и при содействии агентства ANSSI. Не функционировали стандартные адреса электронной почты, стационарные телефоны, каналы электронного обмена данными и API-интерфейсы. GCA не уточнила, были ли ее системы зашифрованы.

Атака на AB Texel

Логистика

Программы-вымогатели

15 февраля голландская логистическая компания AB Texel, по информации с ее сайта, стала жертвой группы, использующей шифровальщик Cactus. Операция по восстановлению данных была начата немедленно. Атака не повлияла на работу сервисов компании. Компания продолжала операционную деятельность, обслуживая клиентов и информируя их и своих сотрудников о ситуации. Об инциденте немедленно доложили в Голландскую службу по защите данных. AB Texel также планирует подать заявление в полицию. 28 февраля группа — оператор программы Cactus добавила в список своих жертв компанию AB Texel.

Кибератака на Radiant Logistics

Транспорт, логистика

Отказ сервисов

Международная компания Radiant Logistics, занимающаяся грузоперевозками, изолировала свою инфраструктуру в Канаде после инцидента кибербезопасности. В заявлении, поданном в Комиссию по ценным бумагам и фондовому рынку США (SEC), компания Radiant указала, что обнаружила инцидент 14 марта. Канадские клиенты столкнулись с задержками в обслуживании — в других странах проблемы не наблюдались. После обнаружения инцидента компания сразу включила свои протоколы реагирования и обеспечения непрерывности работы и начала принимать меры против несанкционированной деятельности.

Другое

Кибератака на Alamos Gold

Горнодобывающая промышленность

Утечка данных, утечка персональных данных

Канадская горнодобывающая компания Alamos Gold стала жертвой кибератаки, которая произошла примерно в апреле 2023 года. По данным местных СМИ, в результате атаки конфиденциальные корпоративные данные стали доступны публично в прошлом году. Как сообщается, среди опубликованных злоумышленниками данных были номера социального страхования, платежные ведомости, финансовая информация, домашние адреса и номера мобильных телефонов высшего руководства. За атакой стоит, по всей видимости, вымогательская группа Black Basta. По заявлению Alamos, их деятельность никак не пострадала, и компания остается бдительной в защите своих систем, предпринимая меры для предотвращения кражи персональных данных.

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