Kaspersky ICS CERT

kaspersky

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

19.02.2025

Версия 1.0

Общие сведения

В третьем квартале 2024 года спектр отраслей, пострадавших от кибератак, оказался особенно широк. С инцидентами кибербезопасности столкнулись промышленные предприятия, производящие текстиль, электронную аппаратуру, композитные и строительные материалы, машины и механизмы, автомобили и другие виды продукции. Чаще всего инциденты были связаны с активностью групп, распространяющих программы-вымогатели. Среди пострадавших оказалось много крупных компаний, в том числе с мировым именем. Несмотря на то что оценочный ущерб от подтвержденных инцидентов не был чрезвычайно высоким (максимальная сумма ущерба составила 21,4 млн долларов – о ней сообщила американская компания Microchip Technology), для немецкого производителя прецизионных стальных деталей Schumag AG инцидент кибербезопасности, возможно, стал последней каплей, подтолкнувшей фирму к банкротству. Другие отрасли, такие как пищевая промышленность, строительство, машиностроение, горнодобывающая промышленность и логистика, также не избежали атак. Необычно большое количество пострадавших компаний было зафиксировано в критически важных секторах, включая коммунальные услуги и энергетику. К счастью, ни одна из атак не привела к отказу ключевых систем, таких как водо- или электроснабжение, но многие пострадавшие компании столкнулись со сбоями в предоставлении цифровых сервисов.

Краткая статистика по кварталу

- В общей сложности 58 инцидентов, публично подтвержденных компаниями-жертвами.
- Большинство жертв (71%) сообщили, что **подверглись атакам программ-вымогателей**.
- Две трети всех пострадавших компаний (66%) относятся к производственному сектору; 68% из них (64% от общего числа жертв) сообщили об **утечке персональных данных** в результате инцидента.
- 31% всех пострадавших компаний сообщили о **сбоях в работе предприятий**, а 29% — об **отказе ИТ-систем** в результате инцидента.
- **Страны с наибольшим количеством подтвержденных инцидентов:**
  - США — 60% (35 инцидентов)
  - Германия — 7% (4)
  - Япония — 5% (3)
- В этом квартале зафиксированы инциденты в странах, откуда публичные подтверждения инцидентов поступают нечасто: **Британских Виргинских островах, Южной Африке, Сингапуре.**

Июль

- AKG
- Metalfrio
- Bassett Furniture
- Cadre Holdings Inc.
- K-FLEX USA
- TotalEnergies Clientes SAU
- BMW Hong Kong
- Hiap Seng Industries Ltd.
- Basement Systems
- Kulicke and Soffa Industries, Inc.
- Peco Foods
- Industrias Peñoles

Август

- Schlatter Industries
- Arntz Optibelt
- Direct Signalétique
- Nilörngruppen
- Lavelle Industries
- Noritsu America Corporation
- Congoleum Acquisition
- Hanwha Qcells
- Clark Material Handling Company
- M&R Printing Equipment
- Anderson Feazel
- Toyota Motor North America
- CRB Engineering
- Siegfried's Basement
- S&F Concrete Contractors Corp.
- Microchip Technology Incorporated
- Kernex Microsystems
- British Virgin Islands Electricity Corporation
- Blue Ridge Rural Water Company Inc.
- JAS Worldwide
- Port of Seattle
- Banham Poultry
- Innophos Holdings Inc.
- Evolution Mining

Сентябрь

- Zacros
- Smeg
- Kawasaki Motors Europe
- Schumag AG
- Oldenburg Group
- Noble Biomaterials
- Granit Design
- V H Blackinton & Company
- The Gill Corporation
- Elyria Foundry
- New England Wooden Ware
- Halliburton
- Netherland Sewell & Associates, Inc.
- Hanon Systems USA
- MEMC LLC
- Air-e
- Arkansas City Water Treatment Facility
- Kantsu
- Brown Integrated Logistics Inc.
- McIlhenny Company
- Ortec
- Sibanye Stillwater

2024

Производственный сектор

Кибератака на AKG

Производственный сектор

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

Немецкий производитель систем охлаждения и теплообменников AKG, имеющий более 10 подразделений по всему миру, стал жертвой кибератаки, которая нарушила производственные процессы и связь на нескольких объектах компании по всему миру. ИТ-системы компании были временно остановлены, чтобы предотвратить распространение вредоносного ПО, но, согласно интервью в немецкой прессе, компании удалось возобновить производство и избежать потери критически важных данных. Была начата проверка с участием Управления уголовных расследований земли Гессен и органов по защите данных. AKG также привлекла эксперта по цифровой криминалистике.

Позднее AKG North America, Inc. — американское подразделение компании — уведомило генерального прокурора штата Массачусетс о нарушении безопасности данных, в результате которого злоумышленники могли получить доступ к конфиденциальным персональным данным. В уведомлении о нарушении AKG указала, что утечка затронула различные сведения о разных людях; среди попавших в чужие руки данных потенциально могли быть имена и номера социального страхования.

15 августа 2024 года AKG North America, Inc. начала рассылать уведомления лицам, чьи данные могли быть похищены. Согласно письмам, направленным жителям штата Массачусетс, AKG предоставила получателям список конкретных типов конфиденциальной информации, которая могла быть раскрыта, а также бесплатный доступ к сервису мониторинга кредитной истории на 24 месяца.

Кибератака на Metalfrio

Производственный сектор

Отказ ИТ-систем, нарушение операционной деятельности

Шифровальщики

15 июля бразильский производитель коммерческих холодильников Metalfrio объявил, что стал жертвой кибератаки, которая вывела из строя часть его систем в Бразилии и Мексике. Компания оперативно активировала свои протоколы информационной безопасности для минимизации угрозы и изолировала свои системы, чтобы предотвратить дальнейший ущерб. Она также сообщила, что прибегла к услугам специализированной внешней консалтинговой фирмы. Metalfrio заявила, что утечки данных клиентов и поставщиков, а также персональных данных, обрабатываемых компанией, выявлено не было. В течение нескольких дней после инцидента компания приняла все необходимые меры для восстановления нормальной работы. 16 июля группа RansomHub взяла на себя ответственность за атаку, опубликовав сообщение на своем сайте, посвященном утечкам.

Кибератака на Bassett Furniture

Производственный сектор

Отказ ИТ-систем, отказ сервисов и нарушение операционной деятельности

Американский производитель и ретейлер мебели Bassett Furniture 10 июля обнаружил несанкционированную активность в части своих ИТ-систем, как указано в отчете по форме 8-K, поданном в Комиссию по ценным бумагам и биржам США. Злоумышленники нарушили работу компании, зашифровав некоторые файлы данных. После обнаружения несанкционированной активности компания немедленно предприняла меры для локализации инцидента, его оценки и разрешения, включая проведение расследования, активацию плана реагирования на инциденты и отключение некоторых систем. Магазины компании и ее платформа электронной коммерции продолжали работать, и клиенты могли оформлять заказы и покупать товары, которые были доступны, однако выполнение заказов было затруднено. Согласно комментарию, данному генеральным директором компании отраслевому изданию, заводы Bassett Furniture простаивали четыре с половиной дня. Компания признала, что атака существенно повлияла на ее операционную деятельность и, вероятно, будет продолжать оказывать негативное влияние до завершения восстановительных работ.

Позднее генеральный директор Bassett Furniture сообщил о финансовых потерях в третьем квартале 2024 года, отчасти связанных с последствиями кибератаки. В то время как полный ущерб от инцидента еще не был определен, компания указала, что он включает 600 000 долларов, выплаченные в качестве заработной платы сотрудникам в течение недельного простоя производства, вызванного атакой.

Атака на Schlatter Industries с применением шифровальщика

Производственный сектор

Отказ ИТ-систем

Шифровальщики

Компания Schlatter Industries, швейцарский производитель систем контактной сварки и ткацких станков, стала жертвой кибератаки 9 августа. Согласно официальному заявлению компании, в ходе атаки было развернуто вредоносное ПО, после чего хакеры пытались вымогать деньги у компании. Компания сразу же начала принимать необходимые меры безопасности, а также обратилась за поддержкой к соответствующим органам. Эксперты по безопасности работали над минимизацией ущерба и скорейшим восстановлением систем. Schlatter Industries провела расследование на предмет кражи данных и задействовала специалистов для полного восстановления работы систем. 20 августа компания сообщила агентству Reuters, что с 19 августа ее сеть, полностью восстановленная после кибератаки, работает в штатном режиме. В своем последнем заявлении Schlatter Industries не сообщила о последствиях кибератаки или о том, были ли украдены какие-либо данные.

Кибератака на Arntz Optibelt

Производственный сектор

Отказ ИТ-систем

Немецкий производитель ременных приводов Arntz Optibelt стал жертвой кибератаки. Компания зафиксировала сбой утром 25 августа и предприняла соответствующие меры, в том числе создала рабочую группу для расследования инцидента. Arntz Optibelt работала в тесном сотрудничестве с органами безопасности, чтобы определить источник и масштаб атаки. Согласно сообщениям немецких СМИ, электронные письма, отправленные в компанию, не были доставлены. Представитель Arntz Optibelt сообщил, что кибератака привела к определенным ограничениям, но компания при поддержке специалистов приложила все усилия для сохранения работоспособности всех своих объектов по всему миру.

Кибератака на Direct Signalétique

Производственный сектор

Отказ ИТ-систем

Французский производитель наглядно-информационных средств Direct Signalétique подвергся кибератаке 16 августа, по сообщениям местных СМИ, которые отметили, что «все перестало работать». 27 августа компания опубликовала сообщение в LinkedIn, в котором объяснила, что ее провайдер ИТ-сервисов подвергся кибератаке, и это привело к сбоям в работе сайта

Direct Signalétique и программного обеспечения для обработки данных. С компанией по-прежнему можно было связаться по телефону и электронной почте.

Атака шифровальщиков на компанию Nilörngruppen

Производственный сектор

Отказ ИТ-систем, отказ сервисов, нарушение операционной деятельности, нарушение отгрузки продукции

Шифровальщики

Шведский производитель одежды и тканей Nilörngruppen обнаружил 6 августа, что его ИТ-системы скомпрометированы в результате кибератаки. Это привело к нарушению операционной деятельности компании и временной приостановке работы сервисов. Атака вывела из строя системы, и Nilörngruppen предпринимала усилия для их скорейшего восстановления. Компания задействовала свои протоколы ИТ-безопасности и сотрудничала с экспертами в области кибербезопасности, чтобы определить масштабы инцидента и принять необходимые меры по защите своих систем. 13 августа она опубликовала обновленную информацию, сообщив об успешном возобновлении поставок со всех объектов и постепенном восстановлении операционной деятельности. Nilörngruppen прежде всего восстановила наиболее критичные для бизнеса системы, что позволило возобновить поставки клиентам. 9 августа группа кибервымогателей Play внесла Nilörngruppen в свой список жертв на сайте в даркнете. 25 октября компания указала в своем отчете за третий квартал 2024 года, что ущерб от кибератаки составил 4,4 млн шведских крон (примерно 400 000 долларов).

Атака на Lavelle Industries с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

В августе американский производитель резины и пластмасс Lavelle Industries выпустил уведомление о нарушении безопасности данных в результате кибератаки, произошедшей в марте 2024 года. Компания заявила, что обнаружила подозрительную несанкционированную активность в своих системах 17 марта. Она оперативно отреагировала, приняв меры для защиты своих систем и инициировав расследование, чтобы определить характер и масштаб инцидента. Расследование показало, что в период с 10 по 17 марта 2024 года неизвестные злоумышленники получили доступ к некоторым системам и, возможно, просмотрели или скопировали данные, хранившиеся на этих системах. Эти данные включали имена, номера социального страхования, номера водительских удостоверений и сведения о финансовых

счетах. Lavelle Industries отправила первоначальное уведомление потенциально пострадавшим лицам 4 апреля. Компания также сообщила, что, в соответствии с требованиями, уведомит регулирующие органы штата и федеральные правоохранительные органы. Кроме того, она заявила, что работает над внедрением дополнительных мер безопасности и обучением своих сотрудников. Компания подчеркнула, что не обнаружила признаков злоупотребления или мошенничества, связанных с инцидентом. Группа LockBit взяла на себя ответственность за мартовскую атаку на Lavelle Industries.

Атака на Zacros с применением шифровальщика

Производственный сектор

Отказ ИТ-сервисов, нарушение операционной деятельности, нарушение отгрузки продукции

Шифровальщики

Японский производитель гибкой упаковки Zacros подвергся кибератаке с применением программы-вымогателя, которая зашифровала часть серверов компании — об этом говорится в кратком сообщении, опубликованном на сайте компании 15 сентября. 27 сентября компания опубликовала более подробное заявление. В нем сообщается, что 14 сентября некоторые из серверов систем управления производством и информационных систем компании были атакованы программами-вымогателями, которые зашифровали часть информации на этих серверах. Это привело к задержкам в производстве и отгрузке некоторых продуктов компании, что, в свою очередь, сказалось на сроках поставок. Компания отключила атакованные системы от сети, приостановила их использование и инициировала криминалистическое расследование силами внешней специализированной фирмы, чтобы оценить масштаб ущерба и определить, какая информация была утрачена или подверглась утечке. Были приняты меры по предотвращению повторения инцидента, в том числе усилена безопасность перед перезапуском систем.

С момента публикации заявления Zacros использовала резервные системы и работала над восстановлением своей операционной деятельности, включая производство и отгрузку продукции. Компания сообщила о происшествии в полицию и Комиссию по защите персональных данных. Также она планировала уведомить тех, чьи персональные данные могли быть скомпрометированы, сразу же после выявления случаев компрометации.

Хакерская группа Argonauts заявила, что взломала системы Zacros и вывела с них данные объемом 140 ГБ. Компания получила требование о выкупе, но не стала его платить.

Кибератака на Smeg

Производственный сектор

Отказ ИТ-систем, нарушение операционной деятельности

Итальянский производитель бытовой техники Smeg стал жертвой кибератаки, которая была обнаружена 27 сентября. Атака привела к останову производства и отключению ИТ-систем, включая системы управления производством, логистикой, персоналом и бухгалтерским учетом. Из соображений безопасности системы были заблокированы для предотвращения потери конфиденциальных данных. В качестве меры предосторожности деятельность компании была приостановлена до восстановления полной работоспособности систем. По сообщениям местных СМИ, сотни сотрудников компании не могли продолжить работу и были отправлены домой. Хакерская группа Interlock взяла на себя ответственность за инцидент. Предположительно, группа украла с систем компании 820 ГБ данных.

Кибератака на Kawasaki Motors Europe

Производственный сектор

Нарушение операционной деятельности

Шифровальщики

Kawasaki Motors Europe, европейское подразделение японского производителя транспортных средств, подверглось кибератаке. Атака затронула штаб-квартиру компании в ЕС и привела к временному прекращению операционной деятельности из-за того, что серверы подразделения были временно изолированы для предотвращения дальнейшего ущерба. В качестве меры предосторожности было решено изолировать каждый сервер и провести процесс очистки, в ходе которого проверить все данные, обнаружить и обработать все подозрительные материалы. Компания также начала расследование с привлечением внешних экспертов по кибербезопасности. В итоге была возобновлена нормальная работа с дилерами, системами управления предприятием и взаимодействие с поставщиками, такими как логистические компании.

Группа RansomHub внесла Kawasaki Motors Europe в свой список жертв на сайте в даркнете 5 сентября, заявив о краже 487 ГБ данных. Позднее, 16 сентября, RansomHub опубликовала данные, якобы украденные у компании. Утечка включала бизнес-документы, финансовую информацию, банковские документы, сведения о дилерах и информацию о внутренних коммуникациях.

Кибератака на Schumag

Производственный сектор

Нарушение операционной деятельности, банкротство

Шифровальщики

Немецкий производитель прецизионных стальных деталей Schumag AG заявил 23 сентября, что стал жертвой кибератаки. В официальном заявлении компания сообщила о решении отменить ежегодное общее собрание акционеров, запланированное на 25 сентября. Несмотря на атаку, производство было частично восстановлено еще до проведения оценки последствий и ущерба. Компания планировала провести новое собрание акционеров в ближайшее время. Группа вымогателей 8Base добавила Schumag AG на свой сайт, посвященный утечке данных.

Позднее компания подала в районный суд Аахена заявление о признании банкротом (в рамках процедуры «реструктуризации в режиме самоуправления»). Эта особая процедура банкротства позволяет совету директоров сохранить контроль над управлением компанией под надзором внешнего администратора. Schumag AG продолжила свою операционную деятельность, а заработная плата 450 сотрудников была обеспечена за счет льгот при банкротстве. Генеральный директор компании отметил: «У нас был четкий план по исправлению ситуации, но мы были вынуждены признать, что после кибератаки предыдущие планы реструктуризации оказались недостаточными. Дополнительное бремя, вызванное хакерской атакой, внесло серьезные коррективы в наши расчеты».

Атака на Oldenburg Group с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

Американский поставщик тяжелого оборудования и архитектурных осветительных приборов Oldenburg Group и его подразделение Visa Lighting сообщили генеральным прокурорам штатов Мэн и Вермонт, что стали жертвами кибератаки, произошедшей 4–5 мая. В ходе этой атаки злоумышленники, предположительно связанные с группой вымогателей Play, установили программы-вымогатели на основные серверы компании и, возможно, получили доступ к находившимся на них персональным данным. Oldenburg Group начала расследование, чтобы определить характер инцидента. В ходе расследования было установлено, что могли быть скомпрометированы персональные данные, хранящиеся на системах компании. Компания приступила к анализу данных, чтобы определить, какие сведения затронуты атакой, и выявить пострадавших. Скомпрометированные данные варьировались в зависимости от пострадавшего, но могли включать: имя, номер социального страхования,

адрес, дату рождения, адрес электронной почты, номер водительских прав, информацию о финансовых счетах, а также налоговые и медицинские сведения и информацию о медицинском страховании. Компания привлекла сторонних экспертов по криминалистике и ИТ-сервисам, а также внешних консультантов для помощи в расследовании и приняла меры по усилению своих существующих протоколов безопасности. В сентябре группа Play взяла на себя ответственность за атаку на Oldenburg Group Inc./Visa Lighting.

Кибератака на Noble Biomaterials

Производственный сектор

Утечка персональных данных

Американская биотехнологическая компания Noble Biomaterials обнаружила подозрительную активность в своей компьютерной сети, как указано в уведомлении о нарушении безопасности данных, поданном генеральному прокурору штата Мэн в сентябре. Компания провела расследование и установила, что ее сеть была заражена вредоносным ПО, которое заблокировало доступ к некоторым файлам на системах. В ходе расследования было установлено, что с 25 июля по 3 августа неавторизованные лица, возможно, получили доступ к некоторым системам, содержащим информацию о существующих и бывших сотрудниках. Хотя не было обнаружено свидетельств кражи личных данных или мошенничества, Noble Biomaterials уведомила лиц, чьи личные данные хранились на потенциально скомпрометированных системах. Информация, к которой мог быть осуществлен несанкционированный доступ, включала имена и номера социального страхования. После обнаружения подозрительно активности компания оперативно приступила к расследованию и реагированию на инцидент, оценке безопасности своих систем и выявлению лиц, чьи данные могли быть скомпрометированы. Noble Biomaterials также уведомила федеральные правоохранительные органы и оказала им содействие в проведении расследования. Кроме того, компания реализовала дополнительные меры безопасности и провела обучение своих сотрудников.

Атака на Granit Design с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

Granit Design, канадский производитель поверхностей из природного камня, кварца и ультракомпактных искусственных материалов, сообщил в сентябре генеральным прокурорам штатов Мэн и Вермонт, что стал жертвой кибератаки, которая затронула конфиденциальные данные сотрудников компании. Сразу же после обнаружения инцидента компания приняла меры по защите своей сетевой инфраструктуры и начала расследование с привлечением внешних экспертов по кибербезопасности и криминалистике. Расследование показало, что с 20 июля по 2 августа неавторизованные лица получили доступ к серверу и скачали с него часть файлов. Компания заявила, что на момент подачи уведомления не было обнаружено свидетельств кражи личных данных, но на атакованных системах хранился определенный объем персональной информации. На скомпрометированных системах хранились следующие типы личных данных: полное имена и фамилии, даты рождения, номера водительских прав, номера социального страхования, банковские реквизиты, а также другие личные данные сотрудников, включая медицинские анкеты. Группа вымогателей Play взяла на себя ответственность за августовскую атаку на Granit Design.

Кибератака на V.H. Blackinton & Company

Производственный сектор

Утечка персональных данных

Американский производитель нагрудных знаков и знаков отличия для сотрудников служб общественной безопасности V.H. Blackinton & Company, Inc. 30 августа обнаружил необычную активность в своей цифровой инфраструктуре, как указано в отчете, направленном в сентябре генеральным прокурорам штатов Мэн и Вермонт. Сразу же после обнаружения подозрительной активности компания приняла меры по защите своей сети и начала расследование с участием независимых экспертов по кибербезопасности. В результате расследования компания установила, что неавторизованные лица получили доступ к некоторым файлам и данным, хранящимся на ее системах. После завершения тщательного анализа всех данных, потенциально затронутых атакой, V.H. Blackinton & Company 4 сентября подтвердила, что персональные данные некоторых лиц, возможно, были скомпрометированы. Среди потенциально скомпрометированных данных были имена и номера социального страхования. С этого момента V.H. Blackinton & Company работала над сбором контактной информации пострадавших лиц и готовилась уведомить их о случившемся. Компания внедрила дополнительные меры безопасности для предотвращения повторения подобных инцидентов.

Атака на The Gill Corporation с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

Американский производитель композитных материалов The Gill Corporation (TGC) подвергся в конце июня кибератаке, в ходе которой злоумышленники зашифровали данные компании. В сентябре она подала уведомление о нарушении безопасности данных генеральным прокурорам штатов Мэн и Вермонт. В ходе атаки неавторизованные лица получили доступ к системам TGC и зашифровали большое количество файлов, а также системы, на которых хранились резервные копии. Впоследствии компания провела расследование, чтобы определить, могла ли атака привести к компрометации персональных данных бывших сотрудников TGC и краже этих данных. Было установлено, что персональная информация, затронутая этим инцидентом, могла включать имена, номера социального страхования и некоторое количество номеров водительских удостоверений и/или номеров банковских счетов, а также форм W-2 (отчет о заработной плате и налогах в США. — **Прим. ред.**). Компания выявила уязвимость, использованную злоумышленниками, и устранила ее из своих систем. Также она внедрила дополнительные меры защиты для обеспечения безопасности своих систем и приняла к рассмотрению дополнительные меры для предотвращения подобных инцидентов в будущем. В июле группа вымогателей Hunters International взяла на себя ответственность за атаку на TGC, сообщив о ней на своем сайте в даркнете, посвященном утечке данных.

Атака на Noritsu America Corporation с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

Американский производитель высококлассного профессионального оборудования для цифровой обработки изображений Noritsu America Corporation, являющийся дочерней компанией японского холдинга Noritsu, стал жертвой кибератаки, в результате которой произошла утечка персональных данных, согласно уведомлению о нарушении безопасности данных, поданному в августе. Noritsu North America обнаружила необычную активность в своей сети, начавшуюся 29 апреля. 31 июля компания узнала, что в ходе инцидента могли быть скомпрометированы персональные данные клиентов. Noritsu America Corporation немедленно приняла меры по локализации вредоносной активности и привлекла сторонних экспертов по кибербезопасности, которым поручила провести расследование и определить, какая информация могла быть просмотрена или получена без авторизации. Потенциально затронутая инцидентом информация включала

имена и номера социального страхования. Компания внедрила дополнительные меры безопасности, чтобы уменьшить риск повторения подобных инцидентов в будущем, уведомила Федеральное бюро расследований и заявила о готовности поддержать будущее расследование. В мае группа вымогателей Hunters International взяла на себя ответственность за атаку на Noritsu America Corporation, сообщив о ней на своем сайте в даркнете, посвященном утечке данных.

Атака на Congoleum Acquisition с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

Американский производитель напольных покрытий Congoleum Acquisition LLC уведомил генерального прокурора штата Мэн о том, что стал жертвой утечки данных, в результате которой злоумышленники похитили конфиденциальную личную информацию. Согласно уведомлению, компания обнаружила несанкционированную активность в своей цифровой инфраструктуре 30 июня. После обнаружения этой активности Congoleum Acquisition немедленно приняла меры для защиты сети и начала расследование с привлечением независимых экспертов по кибербезопасности, чтобы выяснить, что произошло и могла ли быть затронута конфиденциальная информация. В результате расследования компания выяснила, что неавторизованные лица завладели некоторыми файлами и данными, хранящимся в ее системах. После завершения анализа всех потенциально затронутых инцидентом данных Congoleum 11 июля подтвердила, что персональные данные некоторых лиц могли быть скомпрометированы. Среди украденных данных, в зависимости от конкретного человека, могли быть имена и номера социального страхования. В июле группа вымогателей Play взяла на себя ответственность за атаку на Congoleum Acquisition.

Кибератака на Cadre Holdings

Производственный сектор

Нарушение операционной деятельности

Американский поставщик защитной экипировки и средств выживания Cadre Holdings Inc. установил 15 июля, что стал жертвой кибератаки, в результате которой неавторизованные лица получили доступ к некоторым из технологических систем компании, согласно отчету по форме 8-K, поданному в Комиссию по ценным бумагам и биржам США. В рамках реагирования на инцидент были отключены некоторые системы компании,

что повлияло на ее операционную деятельность. После обнаружения атаки компания немедленно активировала свои стандартные протоколы реагирования на инциденты, чтобы локализовать, оценить и устранить ее последствия. В частности она начала расследование с привлечением внешних экспертов, активировала план реагирования на инциденты, уведомила федеральные правоохранительные органы и отключила некоторые системы в качестве меры предосторожности. Хотя инцидент отразился на некоторых аспектах деятельности Cadre Holdings, на момент подачи отчета было неизвестно, оказала ли атака существенное влияние на финансовое состояние компании или ее результаты и насколько вероятно такое влияние в будущем.

Позднее стало известно, что влияние атаки на результаты в третьем квартале 2024 года составило около 5% валовой прибыли.

Атака на Hanwha Qcells с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

The Немецкий филиал производителя фотоэлектрических элементов Hanwha Qcells подвергся кибератаке. Согласно письму клиентам, оказавшемуся в распоряжении портала heise online, атака на ИТ-системы компании произошла 14 июля. Позднее Hanwha Qcells подтвердила порталу факт инцидента. Согласно письму, неизвестные третьи лица, по-видимому, получили доступ к части базы данных клиентов и бизнес-партнеров, в результате чего произошла утечка персональных данных. Компания приняла меры для восстановления своих систем. В расследовании инцидента были задействованы Управление уголовных расследований и Уполномоченный по защите данных федеральной земли Саксония-Анхальт.

В августе группа вымогателей Abyss взяла на себя ответственность за атаку на Hanwha Qcells и утверждала, что завладела 5,4 ТБ данных компании.

Атака на Elyria Foundry Holdings LLC с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

Американский производитель чугунных отливок Elyria Foundry Holdings LLC, обслуживающий автомобильную, машиностроительную и другие отрасли, 25 июня обнаружил подозрительную активность в своей компьютерной сети и в сентябре подал уведомление о нарушении безопасности данных генеральному прокурору штата Мэн. Сразу же после обнаружения инцидента компания приняла меры по защите своих систем и начала расследование характера и масштаба инцидента с привлечением сторонних экспертов по криминалистике. Расследование показало, что в течение нескольких часов с 24 по 25 июня 2024 года неизвестные лица получили доступ к некоторым системам в сети компании и, возможно, просмотрели или скопировали оттуда файлы. Компания провела тщательный анализ затронутых инцидентом файлов, чтобы определить, какую информацию они содержали. 1 августа Elyria Foundry Holdings завершила проверку и начала уведомлять лиц, потенциально пострадавших в результате инцидента. Скомпрометированные данные включали имена и номера социального страхования. Впоследствии компания внедрила дополнительные технические меры обеспечения безопасности для защиты своей информационной инфраструктуры. В июле группа вымогателей Play взяла на себя ответственность за атаку на Elyria Foundry Holdings.

Атака на New England Wooden Ware Corporation с применением шифровальщика

Производственный сектор

Утечка персональных данных

Шифровальщики

Американский производитель упаковки New England Wooden Ware Corporation (NEWW) в сентябре сообщил генеральному прокурору штата Мэн, что в районе 5 апреля в компьютерных системах компании была зафиксирована подозрительная активность. Сразу же после обнаружения этой активности NEWW приняла меры по защите своей сети и оперативно привлекла стороннюю группу расследователей-криминалистов для определения характера и масштаба инцидента. 2 августа, по результатам тщательного расследования, компания установила, что неавторизованные лица могли получить доступ к ограниченному количеству персональных данных. Информация, к которой неавторизованные лица, возможно, получили доступ, включала имена и фамилии, а также другие данные, которые не были указаны в публичных документах. NEWW приняла меры для устранения последствий инцидента и заявила о своей приверженности защите персональной информации, находящейся в ее распоряжении. После

обнаружения инцидента компания оперативно предприняла шаги по защите своих систем и усилению безопасности сети, чтобы предотвратить подобные инциденты в будущем. В апреле группа вымогателей Play взяла на себя ответственность за атаку на New England Wooden Ware.

Атака на Clark Material Handling Company с применением шифровальщика

Производственный сектор

Отказ ИТ-систем, утечка персональных данных

Шифровальщики

Американский производитель вилочных погрузчиков Clark Material Handling Company 3 марта 2024 года обнаружил инцидент безопасности, затронувший внутренние системы компании, а в августе уведомил об этом генерального прокурора штата Мэн. Компания немедленно начала расследование, приняла меры по локализации и ликвидации последствий инцидента с привлечением внешних экспертов по кибербезопасности. Расследование показало, что примерно с 14 февраля по 3 марта неавторизованные лица получили доступ и скопировали файлы, размещенные в некоторых сегментах сети компании. Установлено, что причиной инцидента стал взлом систем внешнего веб-разработчика, через аккаунт которого злоумышленники получили доступ к инфраструктуре компании. В рамках расследования Clark Material Handling Company организовала детальную проверку файлов, затронутых атакой. Проверка, которая была завершена 9 июля, показала, что некоторые файлы содержали персональные данные, включая имена и фамилии, номера социального страхования, а также, возможно, номера паспортов, номера водительских удостоверений, идентификационные номера налогоплательщиков, номера финансовых счетов, номера платежных карт, сведения о состоянии здоровья и/или страховую информацию. После обнаружения инцидента компания оперативно приняла меры реагирования в тесном контакте с консультантами по криминалистике, включая расследование, локализацию и устранения последствий атаки, а также анализ безопасности сетевой инфраструктуры. Clark Material Handling Company уведомила об инциденте федеральные правоохранительные органы, сбросила все пароли и внедрила дополнительные меры безопасности для усиления защиты конфиденциальной информации, размещенной на системах компании.
В марте группа вымогателей Hunters International взяла на себя ответственность за атаку на Clark Material Handling Company.

Атака на M&R Printing Equipment Inc. с применением шифровальщика

Производственный сектор

Отказ ИТ-систем, утечка персональных данных

Шифровальщики

Американский производитель оборудования для цифровой и трафаретной печати M&R Printing Equipment Inc. 6 июня обнаружил, что стал жертвой сложной атаки с применения программы-вымогателя, согласно уведомлению о нарушении безопасности данных, поданному в августе. Сразу же после обнаружения атаки компания задействовала свою команду ИТ-специалистов и сторонних экспертов-криминалистов, чтобы обеспечить безопасность сети, восстановить работоспособность систем и провести всестороннее расследование характера и масштаба инцидента. M&R Printing Equipment также уведомила об инциденте федеральные правоохранительные органы. Расследование показало, что атака могла затронуть данные существующих и бывших сотрудников компании. Полный анализ инцидента был завершен 8 июля. M&R Printing Equipment не раскрыла публично, к каким именно персональным данным могли получить доступ злоумышленники.

Кибератака на K-FLEX USA

Производственный сектор

Утечка персональных данных

В июле американский производитель изоляционных материалов K-FLEX USA LLC уведомил генерального прокурора штата Мэн о том, что стал жертвой нарушения безопасности данных, в результате которого конфиденциальные персональные данные могли быть просмотрены и присвоены злоумышленниками. Согласно уведомлению, примерно 14 ноября 2023 года компания обнаружила, что стала жертвой кибератаки. K-FLEX начала расследование, чтобы определить характер инцидента. В ходе расследования она определила, что конфиденциальные персональные данные могли быть просмотрены или скачаны злоумышленниками. Компания начала работу по анализу данных, чтобы определить, какая информация была затронута инцидентом, и выявить конкретных лиц, пострадавших от атаки. 12 июля K-FLEX завершила анализ данных. Скомпрометированные данные, которые могли быть разными для разных людей, могли включать имя, номер социального страхования и/или номер водительского удостоверения или номер идентификационной карты штата. Компания внедрила дополнительные меры безопасности для минимизации риска повторения подобных инцидентов в будущем.

Энергетика

Кибератака на TotalEnergies Clientes SAU

Энергетика

Утечка персональных данных

TotalEnergies Clientes SAU, глобальная энергетическая компания со штаб-квартирой во Франции, сообщила о серьезной кибератаке, в результате которой были скомпрометированы персональные данные 210 715 клиентов. Компания зафиксировала несанкционированный доступ к одной из своих компьютерных систем управления продажами, что привело к утечке конфиденциальной информации о клиентах. Совместно с полицией и Испанским агентством по защите данных TotalEnergies Clientes SAU предприняла все необходимые юридические действия в отношении виновных в инциденте.

Атака на Halliburton с применением шифровальщика

Энергетика

Нарушение операционной деятельности, утечка данных

Шифроваль-щики

Американская нефтяная сервисная компания Halliburton подтвердила, что стала жертвой кибератаки. В уведомлении, направленном в Комиссию по ценным бумагам и биржам США, Halliburton сообщила, что 21 августа обнаружила инцидент и отключила некоторые системы, чтобы минимизировать последствия и предотвратить дальнейшее распространение атаки. После выявления проблемы компания активировала план реагирования на инциденты кибербезопасности и начала внутреннее расследование с привлечением внешних консультантов для оценки и устранения последствий несанкционированной активности. По сообщению агентства Reuters, атака затронула операционную деятельность на площадке Halliburton в северном Хьюстоне, а также некоторые глобальные сети связи. Некоторым сотрудникам было рекомендовано не подключаться к внутренним сетям компании. 30 августа Halliburton подала еще одно уведомление, подтвердив факт кражи данных. В уведомлении сообщалось, что инцидент вызвал сбои и ограничения доступа к части бизнес-приложений, которые поддерживают некоторые аспекты операционной деятельности и корпоративные функции компании. Halliburton понесла расходы, связанные с реагированием на инцидент, и предположительно, эти расходы могут еще увеличиться.

После получения от компании Halliburton электронного письма со списком индикаторов компрометации с именами файлов и IP-адресами, связанными с атакой, портал BleepingComputer установил, что за атакой стояла группа

вымогателей RansomHub. Среди индикаторов компрометации был файл с именем maintenance.exe, который был идентифицирован порталом Bleeping Computer как средство шифрования, используемое программой-вымогателем RansomHub. В распоряжение издания TechCrunch попала копия записки с требованием выкупа, якобы связанной с атакой на Halliburton, в которой утверждалось, что файлы компании были зашифрованы и украдены. Согласно записке, ответственность за кибератаку взяла на себя группа вымогателей RansomHub.

Позднее Halliburton сообщила о расходах в размере 35 млн долларов, непосредственно связанных с атакой.

Кибератака на Anderson Feazel Management

Энергетика

Утечка персональных данных

Американская энергетическая компания Anderson Feazel Management, Inc., специализирующаяся на добыче нефти и газа, подверглась атаке на свои компьютерные системы, которая произошла примерно 31 июля. В сентябре компания начала рассылать жертвам нарушения безопасности данных письма с уведомлениями, о чем сообщила прокурорам штатов Мэн и Нью-Гэмпшир. Злоумышленники просмотрели и присвоили незашифрованные финансовые документы, содержащие сведения о сотрудниках, коммерческую информацию, договоры на право добычи полезных ископаемых, данные о заработной плате и другую частную и личную информацию. После обнаружения вторжения 1 августа Anderson Feazel Management, Inc. немедленно уведомила ФБР и правоохранительные органы штатов. Компания сообщила, что украденные данные варьировались в зависимости от отношений пострадавшего с компанией и могли включать имя, дату рождения, номер социального страхования, адрес, информацию о заработной плате, формы W-2 и налоговые ведомости. Anderson Feazel Management, Inc. приняла меры для безопасного восстановления систем и операционной деятельности, включая сброс паролей и усиленный мониторинг безопасности. Компания также наняла независимого эксперта-криминалиста для проведения полного криминалистического расследования, определения вектора атаки, характера и масштаба инцидента, а также помощи в устранении последствий атаки.

Атака на Netherland, Sewell & Associates с применением шифровальщика

Энергетика

Отказ ИТ-систем, утечка персональных данных

Шифровальщики

Американская инжиниринговая компания Netherland, Sewell & Associates, Inc., работающая в нефтегазовом секторе, подверглась в июле атаке с применением программы-вымогателя и в сентябре подала заявление о нарушении безопасности генеральному прокурору штата Мэн. Netherland, Sewell & Associates немедленно начала расследование и привлекла к нему внешних экспертов-криминалистов и юридическую фирму. Был проведен тщательный анализ информационных систем, затронутых атакой. Примерно 16 августа было установлено, что в результате инцидента могли быть скомпрометированы персональные данные клиентов, включая номера социального страхования.

Автомобильная отрасль

Нарушение безопасности данных BMW Hong Kong

Производственный сектор, автомобильная отрасль

Утечка персональных данных

BMW Hong Kong стала жертвой утечки данных, затронувшей около 14 000 клиентов. О случившемся стало известно 15 июля после публикации на сайте в даркнете сообщения от злоумышленника под псевдонимом 888. Утечка включала конфиденциальные персональные данные, такие как титулы, фамилии, имена, номера мобильных телефонов и настройки отказа от получения SMS-сообщений. 25 июля BMW Concessionaires, эксклюзивный дистрибьютор автомобилей BMW в Гонконге, подтвердил факт утечки конфиденциальной информации. Компания сообщила, что данные находились под управлением стороннего подрядчика Sanuker, который уведомил об утечке полицию и орган по защите конфиденциальных данных. Управление Уполномоченного по защите конфиденциальности персональных данных провело расследование инцидента.

Нарушение безопасности данных Toyota Motor North America

Производственный сектор, автомобильная отрасль

Утечка данных, утечка персональных данных

Американское подразделение Toyota подтвердило порталу BleepingComputer факт утечки данных после того, как группа злоумышленников ZeroSevenGroup разместила архив объемом 240 ГБ с украденной информацией на форуме киберпреступников. Первоначально компания утверждала, что инцидент имел локальный характер и не затронул всю систему. Toyota Motor North America также заявила что взаимодействует со всеми пострадавшими от атаки и предоставит необходимую помощь. День спустя в новом заявлении представитель компании уточнил, что ее системы не подверглись взлому или компрометации, а данные были украдены у стороннего лица, ошибочно представляемого как Toyota, однако отказался назвать это стороннее лицо. Предположительно, сведения, подвергшиеся утечке через хакерский форум, включали личные и рабочие контактные данные сотрудников, финансовую документацию, профили клиентов, бизнес-планы, информацию о сотрудниках и многое другое. Хакеры утверждали, что получили доступ к внутренним системам Toyota Motor North America, а украденные данные якобы включают также фотографии, базы данных, сведения о сетевой инфраструктуре и электронные письма. Злоумышленники также опубликовали инструмент AD-Recon, предназначенный для детального исследования целевой сети, включая пароли и другую конфиденциальную информацию о сети.

Атака на Hanon Systems USA с применением шифровальщика

Производственный сектор, автомобильная отрасль

Утечка персональных данных

Шифровальщики

Американский производитель автомобильных систем охлаждения Hanon Systems USA, LLC 21 июля стал жертвой атаки с применением программы-вымогателя, в ходе которой злоумышленники получили доступ к определенной информации и требовали за нее выкуп, как указано в уведомлении о нарушении безопасности данных, поданном генеральному прокурору штата Мэн в сентябре. Компания подтвердила, что инцидент затронул определенный объем персональных данных. Потенциально скомпрометированные данные включают имена, контактную информацию и номера социального страхования. Сразу же после обнаружения инцидента Hanon Systems USA приняла меры для предотвращения повторения подобных атак в будущем, включая внедрение усиленных мер безопасности. Группа вымогателей Hunters International заявила о своей причастности

к атаке на Hanon Systems USA в августе. Хакеры заявили, что изъяли 2,3 ТБ данных (1 632 581 файл).

Строительство

Атака на Hiap Seng Industries с применением шифровальщика

Строительство, инжиниринг

Утечка персональных данных

Шифроваль-щики

Сингапурская инженерно-строительная компания Hiap Seng Industries Ltd. сообщила в июле, что стала жертвой инцидента с использованием программы-вымогателя, в ходе которого неизвестные злоумышленники получили несанкционированный доступ к серверам компании. Сразу же после обнаружения инцидента компания приняла меры к его локализации, изолировав серверы от сети, и начала восстановительные работы, чтобы обеспечить непрерывность бизнеса и операций. По состоянию на 2 июля инцидент не оказал существенного влияния на операционную деятельность компании, и Hiap Seng Industries привлекла сторонних экспертов для проведения криминалистического расследования и консультирования по вопросам усиления мер кибербезопасности. Компания также проинформировала об инциденте кибербезопасности соответствующие органы.

В октябре Комиссия по защите персональных данных Сингапура сообщила подробности об атаке на Hiap Seng Engineering. Расследование показало, что 11 июня злоумышленники получили доступ к сети компании через VPN-устройство, являющееся частью сетевого экрана, используя учетные данные локального администратора, полученные с использованием уязвимости в VPN-устройстве. Пароли хранились в конфигурационном файле VPN-устройства и были зашифрованы с использованием устаревших методов, что, вероятно, позволило злоумышленникам расшифровать данные. Инцидент затронул персональные данные 10 000 человек (сотрудников, бывших сотрудников и подрядчиков компании), большая часть которых хранилась компанией локально в зашифрованном виде в ПО для расчета зарплат. Среди скомпрометированных данных были имена, адреса, номера NRIC/FIN (номер национальной регистрационной идентификационной карты и иностранный идентификационный номер. — **Прим. ред.**), даты рождения, фотографии, номера разрешений на работу, банковские реквизиты, телефонные номера и номера паспортов.

Атака на CRB Engineering с применением шифровальщика

Строительство, инжиниринг

Отказ ИТ-систем, утечка персональных данных

Шифроваль-щики

Американская инжиниринговая, строительная и консалтинговая компания CRB Engineering уведомила генерального прокурора штата Нью-Гэмпшир о нарушении безопасности данных, в результате которого могли быть скомпрометированы конфиденциальные персональные данные. Согласно уведомлению, 3 января 2024 года компания столкнулась с сетевым сбоем, который затронул некоторые компьютерные системы. CRB Engineering начала расследование, чтобы определить природу инцидента. Расследование показало, что между 25 декабря 2023 года и 3 января 2024 года неавторизованные лица могли получить доступ к конфиденциальным личным данным и присвоить их. CRB Engineering приступила к анализу данных, чтобы определить, какая информация затронута инцидентом и выявить людей, пострадавших в результате атаки. 21 августа CRB Engineering направила уведомления о нарушении безопасности данных пострадавшим лицам. В феврале группа вымогателей LockBit взяла на себя ответственность за атаку.

Атака на Basement Systems с применением шифровальщика

Строительство, инжиниринг

Отказ ИТ-систем, утечка персональных данных

Шифроваль-щики

Американская строительная компания Basement Systems уведомила генеральных прокуроров штатов Мэн и Вермонт о нарушении безопасности данных, в результате которого могли быть скомпрометированы конфиденциальные персональные данные, размещенные на ее системах. Согласно уведомлению о нарушении, 13 мая Basement Systems обнаружила инцидент, временно нарушивший работу ее компьютерной сети. Компания начала расследование, чтобы определить природу инцидента. В результате расследования выяснилось, что в период с 12 апреля по 14 мая неавторизованные сторонние лица могли получить доступ к конфиденциальной информации. Basement Systems провела анализ затронутых инцидентом данных, чтобы определить, какая информация была скомпрометирована, и идентифицировать пострадавших лиц. Потенциально скомпрометированные данные включали имена и номера социального страхования. Компания приняла энергичные меры по усилению безопасности сети и предотвращения повторения подобных инцидентов. Basement Systems уведомила Федеральное бюро расследований и выразила готовность оказать максимальное содействие в привлечении виновных к ответственности. В июне группа вымогателей Cicada3301 взяла на себя ответственность за атаку, заявив, что украла 739 ГБ данных.

Атака на Siegfried's Basement с применением шифровальщика

Строительство, инжиниринг

Утечка персональных данных

Шифроваль-щики

Американская строительная компания Siegfried's Basement уведомила генерального прокурора штата Вермонт о нарушении безопасности данных, в результате которого могли быть скомпрометированы конфиденциальные персональные данные. Они включали имена, контактные данные, номера социального страхования, даты рождения, а также финансовую и банковскую информацию, включая данные кредитных карт. Компания разослала пострадавшим лицам уведомления о нарушении безопасности данных и предложила услуги по мониторингу кредитной истории. Группа вымогателей BlackSuit взяла на себя ответственность за атаку на компанию Siegfried's Basement.

Атака на S&F Concrete Contractors с применением шифровальщика

Строительство, инжиниринг

Утечка персональных данных

Шифроваль-щики

Американская строительная компания S&F Concrete Contractors Corp. уведомила генеральных прокуроров штатов Вермонт и Мэн о нарушении безопасности данных, в результате которого могли быть скомпрометированы размещенные на системах компании конфиденциальные персональные данные и защищенные медицинские сведения. Согласно уведомлению, S&F Concrete Contractors Corp. обнаружила подозрительную активность в своих компьютерных системах ранее в 2024 году. Компания начала расследование, чтобы определить природу инцидента. Она провела анализ данных, чтобы определить, какая информация была затронута инцидентом и выявить конкретных лиц, пострадавших от него. В результате расследования выяснилось, что в период между 5 и 20 мая 2024 года могли быть скомпрометированы конфиденциальные персональные данные на системах компании, и неавторизованные лица могли получить доступ к ним. Потенциально скомпрометированные данные варьировались в зависимости от конкретного человека и могли включать имя, номер социального страхования, номер водительского удостоверения, номер удостоверения личности федерального уровня или уровня штата, сведения о финансовых счетах и информацию о медицинском страховании. Компания сообщила об инциденте правоохранительным органам, реализовала дополнительные меры безопасности и пересмотрела политику и процедуры, связанные с обеспечением конфиденциальности данных и безопасности. В мае группа

вымогателей Danon взяла на себя ответственность за атаку, заявив, что украла 1 ТБ данных.

Электронная промышленность

Атака на Microchip Technology с применением шифровальщика

Производственный сектор, электронная промышленность

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

Шифровальщики

Американский производитель микросхем Microchip Technology Incorporated зафиксировал 17 августа подозрительную активность в своих информационных системах, о чем сообщил в отчете по форме 8-K, поданном в Комиссию по ценным бумагам и биржам США. Атака привела к нарушению операционной деятельности компании и некоторых ее заводов, а также негативно повлияла на способность выполнять заказы. Microchip Technology начала расследование инцидента и реализовала меры по восстановлению систем и операционной деятельности в штатном режиме. После обнаружения проблемы компания приступила к оценке, локализации и ликвидации последствий потенциально несанкционированной активности, изолировала пострадавшие системы, отключила некоторые из них и привлекла внешних экспертов по кибербезопасности для проведения расследования. На момент подачи отчета финансовые последствия атаки еще не были определены.

Группа вымогателей Play 29 августа добавила Microchip Technology на свой сайт, посвященный утечке данных. Хакеры заявили о краже разнообразных конфиденциальных данных, включая частные и персональные конфиденциальные данные, клиентскую документацию, а также сведения о бюджете, заработной плате, бухгалтерском учете, контрактах, налогах, удостоверениях личности и финансах.

В документе, поданном в Комиссию по ценным бумагам и биржам США 4 сентября, Microchip Technology заявила, что ее критически важные ИТ-системы снова функционируют, операционная деятельность в основном восстановлена, а обработка заказов клиентов и отгрузка продукции возобновлены более недели назад. Компания продолжала усердно работать над восстановлением работоспособности оставшихся пострадавших систем, придерживаясь при этом протоколов обеспечения кибербезопасности. Microchip Technology считает, что неавторизованные лица завладели информацией, размещенных на некоторых ИТ-системах, включая контактные данные сотрудников и хеши некоторых зашифрованных паролей. Компания не обнаружила данных клиентов или поставщиков,

попавших в руки неавторизованных лиц. Microchip Technology сообщила в своем квартальном отчете о связанных с атакой расходах в размере 21,4 млн долларов.

Атака на Kernex Microsystems с применением шифровальщика

Производственный сектор, электронная промышленность

Шифровальщики

Индийский производитель электронных систем и программных решений для железнодорожной отрасли Kernex Microsystems сообщил в соответствии с Регламентом 30 Совета по ценным бумагам и биржам Индии о кибератаке на свою ИТ-инфраструктуру с применением вредоносной программы-вымогателя, произошедшей 28 августа. Команда технических специалистов компании совместно с внешними экспертами по кибербезопасности активно расследовала инцидент. Существенного влияния на операционную деятельность компании выявлено не было.

Атака на MEMC LLC с применением шифровальщика

Производственный сектор, электронная промышленность

Утечка персональных данных

Шифровальщики

Американский производитель передовых полупроводниковых материалов для электронной промышленности MEMC LLC столкнулся с несанкционированным проникновением в свою сеть в июне, а в сентябре подал уведомление о нарушении безопасности данных генеральным прокурорам штатов Мэн и Массачусетс. Сразу же после обнаружения проблемы MEMC LLC начала всестороннее расследование, изолировала сеть, реализовала меры по ее защите, ликвидировала угрозу и уведомила об этом правоохранительные органы. В результате криминалистического расследования и ручного анализа документов 18 сентября было установлено, что неавторизованное лицо или лица могли удалить из сети компании некоторые файлы, содержащие персональные данные. Компания сообщила, что файлы, удаленные злоумышленниками, содержали имена клиентов и другую информацию, которую она не стала раскрывать.

Группа вымогателей BlackBasta взяла на себя ответственность за атаку на MEMC LLC, опубликовав в июле информацию о ней на своем сайте в дарквебе, посвященном утечке данных. По утверждениям группы, ей удалось получить доступ к 1 ТБ данных, включая корпоративные документы, финансовую информацию, договоры о конфиденциальности, конфиденциальные сведения, данные кадровой службы, информацию

о найме сотрудников, данные разработок компании, инженерные данные, личные документы сотрудников и данные клиентов.

Атака на Kulicke and Soffa Industries с применением шифровальщика

Производственный сектор, электронная промышленность

Нарушение операционной деятельности, утечка персональных данных

Шифровальщики

Американский производитель полупроводников и решений для монтажа электронных компонентов Kulicke and Soffa Industries, Inc. (K&S) уведомил генерального прокурора штата Мэн и подал отчет по форме 8-K об инциденте, связанном с нарушением безопасности данных, в результате которого злоумышленники могли получить доступ и присвоить конфиденциальные персональные данные, размещенные на системах компании. Согласно отчету, 12 мая компания впервые узнала об атаке с использованием программы-вымогателя, когда с ней связались злоумышленники. Они утверждали, что получили доступ к некоторым файлам K&S и зашифровали их, а в доказательство предоставили снимки экрана. Нарушение операционной деятельности компании было сведено к минимуму благодаря эффективным действиям по изоляции, резервному копированию и восстановлению систем. Примененная стратегия обеспечения бесперебойной работы позволила компании продолжить операционную деятельность и обслуживание клиентов с минимальными нарушениями. 12 июля, по результатам всестороннего расследования, K&S подтвердила, что неавторизованные сторонние лица могли получить доступ к конфиденциальным персональным данным, размещенным на системах компании, и присвоить эти данные. Она провела анализ данных, чтобы определить, какая информация была затронута инцидентом, и выявить конкретных пострадавших лиц. 16 сентября компания завершила анализ, который показал, что потенциально скомпрометированные данные включали имена, идентификационные номера, номера банковских счетов и/или коды банков, относящиеся к существующим и бывшим сотрудникам, их иждивенцам и другим связанным с компанией лицам. После обнаружения инцидента K&S сбросила пароли для всех учетных записей сотрудников, приостановила доступ сотрудников к корпоративной электронной почте с мобильных устройств, обнаружила и удалила вредоносные файлы и значительно усилила возможности мониторинга, журналирования и обнаружения угроз. K&S также привлекла международных специалистов по безопасности для проведения независимого расследования и помощи в восстановлении систем.

В июне группа вымогателей LockBit взяла на себя ответственность за атаку, заявив, что изъяла 20 ТБ конфиденциальных данных (свыше 12 млн файлов) более чем с 2000 различных устройств.

Коммунальные службы

Атака на BVI Electricity Corporation с применением шифровальщика

Энергетика, коммунальные службы

Отказ ИТ-систем, нарушение операционной деятельности, отказ сервисов

Шифровальщики

Электроэнергетическая корпорация Британских Виргинских островов (BVIEC) объявила 19 августа, что стала жертвой кибератаки, которая повлияла на ее внутреннюю и внешнюю операционную деятельность. Совместно с экспертами и правоохранительными органами Британских Виргинских островов и Великобритании компания приняла меры для решения проблемы и возобновления нормальной работы. Несмотря на инцидент, BVIEC продолжала усилия по восстановлению электроснабжения на Британских Виргинских островах после тропического урагана Эрнесто. Генеральный директор BVIEC сообщил местным СМИ, что атака преодолела защиту компании, и инцидент был квалифицирован как атака с использованием программы-вымогателя. Инцидент серьезно ограничил способность BVIEC управлять своей работой в цифровом формате. Было отмечено, что для предотвращения дальнейшего ущерба компания была вынуждена отключить все системы. Финансовый контролер BVIEC сообщил, что инцидент повлиял на несколько систем компании, включая систему выставления счетов, базу данных по работе с клиентами, систему автоматизированного считывания данных счетчиков, а также возможности компании по расчету и печати счетов и чеков.

Система приема платежей от клиентов была восстановлена только в ноябре. До этого клиентам приходилось оплачивать счета лично и предоставлять чеки о прошлых оплатах для проведения взаиморасчетов.

Кибератака на Blue Ridge Rural Water Company

Водоснабжение, энергетика, коммунальные службы

Утечка персональных данных

Американская компания Blue Ridge Rural Water Company Inc., предоставляющая услуги водоснабжения, подверглась кибератаке на свою корпоративную сеть, которая была физически отделена от системы управления водоснабжением. По сообщению компании, после атаки, которая произошла 23 июля, она оперативно перешла в защитный режим, активировав свою систему безопасности. Система управления водоснабжением осталась незатронутой. Компания сразу же задействовала свои протоколы реагирования, приняла меры по локализации активности и начала расследование инцидента. Для помощи в расследовании была привлечена компания по кибербезопасности, имеющая опыт помощи другим компаниям, находящимся в аналогичных условиях. Blue Ridge Rural Water Company Inc. также уведомила правоохранительные органы и оказала содействие их расследованию. В результате анализа было установлено, что 23 июля 2024 года неавторизованные злоумышленники получили доступ и присвоили файлы, размещенные на нескольких серверах в сети компании. После тщательного анализа файлов она определила, что один или несколько скомпрометированных файлов содержат имена и номера социального страхования жителей штата Мэн.

Атака на Air-e с применением шифровальщика

Энергетика, коммунальные службы

Отказ сервисов

Шифровальщики

Колумбийская электрическая компания Air-e опубликовала 5 сентября заявление, сообщив, что она стала жертвой кибератаки с применением программы-вымогателя. Заявление последовало после жалоб в социальных сетях на недоступность некоторых сервисов со 2 сентября и получения анонимных снимков экрана с сообщениями, якобы оставленными злоумышленниками. Согласно заявлению компании, 2 сентября была обнаружена кибератака, которая привела к компрометации нескольких внутренних систем компании. Злоумышленники преодолели существующие меры защиты, включая службу мониторинга Clara и продвинутый защитный инструмент. Air-e заявила, что была применена ранее неизвестная программа-вымогатель, что свидетельствует о ее высоком уровне сложности. В ответ на инцидент компания уведомила генеральную прокуратуру Колумбии об атаке 2 сентября. Air-e активировала подготовленный заранее план действий в случае кибератаки, отдавая приоритет восстановлению пораженных систем из резервных копий. Совместно с экспертами по кибербезопасности компания провела всестороннюю оценку ситуации с целью минимизировать дальнейший

ущерб и повысить уровень безопасности. Компания подчеркнула, что инцидент не привел к перебоям с поставкой электроэнергии, которая продолжалась в обычном режиме. Также она сообщила своим пользователям, что для оплаты услуг необходимо лично посетить офисы. 13 сентября Air-e заявила о полном восстановлении системы печати и рассылки счетов. Выставление некоторых счетов было задержано в связи с инцидентом примерно на четыре дня.

Кибератака на станцию очистки воды в городе Арканзас-Сити

Водоснабжение, энергетика, коммунальные службы

Нарушение операционной деятельности

Станция очистки воды в городе Арканзас-Сити (США) подверглась кибератаке 22 сентября. Сообщение об инциденте было опубликовано 24 сентября. В качестве меры предосторожности станция перешла в ручной режим работы до разрешения ситуации. Городской управляющий заверил общественность, что водоснабжение в городе остается полностью безопасным и бесперебойным. Эксперты в области кибербезопасности и государственные учреждения работали над устранением последствий инцидента и восстановлением нормальной работы станции. Были введены дополнительные меры безопасности для защиты системы водоснабжения, и никаких изменений в качестве воды или обслуживании населения не ожидалось. Городские власти уведомили об инциденте соответствующие органы, и, по сообщениям местных СМИ, Департамент национальной безопасности и ФБР приступили к расследованию.

Расследование подтвердило, что конфиденциальные данные не были скомпрометированы или украдены. Атака потребовала временной перестройки работы объекта и привела к затратам в размере 105 201 доллара на замену серверов, новое программное обеспечение, лицензии и техническую помощь. Еще 58 550 долларов было потрачено на криминалистический анализ, юридические консультации и переговоры со злоумышленниками. Город заявил, что страховка покроет большую часть затрат, за исключением франшизы в 10 000 долларов.

Логистика и транспорт

Атака на JAS Worldwide с применением шифровальщика

Транспорт, логистика

Отказ ИТ-сервисов, нарушение операционной деятельности

Шифровальщики

JAS Worldwide, международная транспортная компания со штаб-квартирой в США, подтвердила 27 августа, что стала жертвой атаки с использованием программы-вымогателя, которая привела к нарушению операционной деятельности и сбоям в обслуживании клиентов. Компания оперативно обеспечила защиту своих систем и начала расследование с привлечением экспертов по кибербезопасности. Были приняты меры по восстановлению работы сервисов. 31 августа JAS Worldwide сообщила, что ей удалось восстановить некоторые аспекты своей операционной деятельности, включая работу электронной почты и веб-сайта. Спустя неделю после атаки JAS Worldwide подтвердила, что большинство систем восстановлено, и компания активно обрабатывает отложенные заявки. Она провела глобальный сброс паролей и внедрила дополнительные меры по повышению своей кибербезопасности. На тот момент работа платформы JAS SmartHub была полностью восстановлена, и клиенты могли отслеживать свои грузы в режиме реального времени. Работа с подавляющим большинством клиентов и партнеров компании велась в обычном режиме, а отложенные запросы обрабатывались выделенной командой.

Атака на Port of Seattle с применением шифровальщика

Транспорт, логистика

Отказ ИТ-систем, отказ сервисов, утечка данных

Шифровальщики

Компания Port of Seattle (США), управляющая портом и международным аэропортом Сиэтл-Такома, сообщила 24 августа через социальные сети о сбоях в системе, которые, возможно, были вызваны кибератакой. Сбои в доступе в интернет и веб-ресурсах компании затронули некоторые системы аэропорта. Телефонные системы в морских объектах порта также перестали работать. Порт изолировал критически важные системы и приступил к восстановлению полноценной работы инфраструктуры. Управление транспортной безопасности работало совместно со своими партнерами в порту. Его представитель сообщил изданию GeekWire, что инцидент не повлиял на работу системы безопасности. По сообщениям в социальных сетях, некоторые элементы морской инфраструктуры порта также работали в режиме восстановления.

Порт опубликовал 13 сентября заявление с дополнительными подробностями августовской кибератаке. Расследование показало, что

неавторизованные злоумышленники получили доступ к определенным частям компьютерных систем и зашифровали там некоторые данные. Согласно заявлению, атака была осуществлена группой Rhysida. По словам представителей порта, группа заявила, что украла данные и готова опубликовать их на своем сайте в дарквебе, если порт откажется заплатить выкуп. Порт предпринял меры по предотвращению дальнейшей активности злоумышленников, включая отключение своих систем от интернета, но шифрование файлов злоумышленниками и ответные меры повлияли на работу некоторых сервисов, включая обработку багажа, терминалы самостоятельной регистрации, продажу билетов, подключения Wi-Fi, информационные табло для пассажиров, веб-сайт порта, приложение flySEA и бронирование парковки. Команде порта удалось восстановить большую часть систем в течение недели, но работа по восстановлению некоторых сервисов, включая внешний сайт компании и внутренние порталы, продолжалась. 16 сентября группа Rhysida опубликовала требование выкупа в размере 100 биткоинов, а также изображения якобы украденных у организации документов.

Атака на Kantsu с применением шифровальщика

Транспорт, логистика

Отказ сервисов, нарушение операционной деятельности, утечка персональных данных

Шифроваль-щики

Японская транспортно-логистическая компания Kantsu 12 сентября стала жертвой атаки с применением программы-вымогателя, в результате чего было зафиксировано заражение нескольких серверов компании, и она отключила свои сети, чтобы предотвратить дальнейшие атаки. Была создана специализированная команда для расследования инцидента, ликвидации его последствий и предотвращения новых атак. Kantsu уведомила соответствующие государственные органы и полицию и провела с ними консультации, а также привлекла внешних экспертов по безопасности для расследования инцидента. 28 сентября компания сообщила, что нарушение безопасности, осуществленное с использованием внешнего сетевого подключения, привело к шифрованию нескольких серверов и сбоям в работе систем хранения и выдачи товаров. Атака затронула как Kantsu, так и ее партнеров, вызвав задержки в работе. Некоторые из атакованных серверов содержали персональные данные, что потребовало подачи отчета в Комиссию по защите персональной информации. Для восстановления нормальной работы компания построила новую инфраструктуру, полностью изолированную от пострадавшей среды.

Атака на Brown Integrated Logistics с применением шифровальщика

Транспорт, логистика

Утечка персональных данных

Шифроваль-щики

Американская логистическая компания Brown Integrated Logistics Inc. (BIL) уведомила генеральных прокуроров штатов Массачусетс, Мэн и Монтана о нарушении безопасности данных, в результате которого могли быть скомпрометированы конфиденциальные персональные данные. 15 ноября 2023 года BIL обнаружила подозрительную активность в своей компьютерной сети и немедленно начала расследование с привлечением сторонних специалистов по кибербезопасности. Расследование показало, что начиная примерно с 13 ноября 2023 года неавторизованные злоумышленники получили доступ к некоторым системам и потенциально могли получить доступ к определенной информации, размещенной на этих системах. Компания провела всесторонний — как программный, так и ручной — анализ, чтобы определить, какая информация была доступна и к кому эта информация относится. 27 августа 2024 года этот процесс был завершен. Потенциально скомпрометированные данные включали имена и номера социального страхования. Примерно 23 сентября 2024 года BIL начала рассылать уведомления о нарушении безопасности данных пострадавшим лицам. Группа вымогателей LockBit взяла на себя ответственность за атаку на Brown Integrated Logistics Inc., осуществленную в ноябре 2023 года.

Пищевая промышленность

Атака на Banham Poultry с применением шифровальщика

Производ-ственный сектор, пищевая промышлен-ность

Утечка персональных данных

Шифроваль-щики

Британский производитель куриного мяса Banham Poultry сообщил, что злоумышленники получили удаленный доступ к его системе ранним утром 18 августа. В электронном письме, направленном сотрудникам и попавшем в руки BBC, компания сообщила, что злоумышленники получили доступ к информации, включая номера в системе национального страхования, копии паспортов и банковские реквизиты. Сразу же после кибератаки Banham Poultry отключила свои системы и привлекла сторонних экспертов-криминалистов. В письме департамента компании по работе с персоналом сообщалось, что на момент отправки письма не было известно о каких-либо случаях злоупотребления чьей-либо информацией или о том, что кто-то пострадал в результате инцидента. Banham Poultry заявила, что уведомила об инциденте Управление комиссара по информации, и внедрила дополнительные меры безопасности. Группа вымогателей RansomHub внесла Banham Poultry в список своих жертв 21 августа.

Нарушение безопасности данных McIlhenny Company

Производственный сектор, пищевая промышленность

Утечка персональных данных

Шифровальщики

Примерно 22 июля Американский производитель продуктов питания McIlhenny Company обнаружил нарушение безопасности данных, которое стало следствием уязвимости в стороннем программном коде, согласно уведомлению о нарушении безопасности данных, направленному генеральному прокурору штата Мэн в сентябре. Проблема была оперативно решена выпуском и установкой исправления, что позволило минимизировать риск, связанный с инцидентом. Компания начала расследование, которое показало, что уязвимость позволяет неавторизованным лицам получить доступ к определенной платежной информации. Потенциально скомпрометированные данные включали имена клиентов, почтовые адреса, адреса электронной почты, номера кредитных карт, даты истечения срока действия карт и коды безопасности. McIlhenny Company сообщила, что не получала сообщений о случаях кражи личных данных с момента инцидента.

Атака на Peco Foods с применением шифровальщика

Производственный сектор, пищевая промышленность

Утечка персональных данных

Шифровальщики

Американский производитель куриной продукции Peco Foods уведомил генерального прокурора штата Мэн в июле о нарушении безопасности данных, в результате которого могли быть скомпрометированы конфиденциальные персональные данные, размещенные на системах компании. Согласно уведомлению, после обнаружения несанкционированного доступа к своим системам компания начала расследование, чтобы определить природу инцидента. В ходе расследования выяснилось, что примерно 4 декабря 2023 года неавторизованные злоумышленники получили доступ к конфиденциальной информации. Peco Foods приступила к анализу данных, чтобы определить, какие данные были скомпрометированы в ходе инцидента и выявить конкретных пострадавших лиц. 23 мая 2024 года компания завершила анализ данных, однако не опубликовала точный перечень персональных данных, которые могли быть скомпрометированы. Группа вымогателей BlackBasta добавила Peco Foods на свой портал в даркнете в декабре 2023 года.

Химическая промышленность

Кибератака на Innophos Holdings

Производственный сектор, химическая промышленность

Нарушение операционной деятельности, утечка персональных данных

Innophos Holdings Inc., американский производитель минералов и специальных фосфатов, используемых в производстве продуктов питания, а также здравоохранении, нутрициологии и промышленности, уведомил генерального прокурора штата Мэн в августе о нарушении безопасности данных, в результате которого могли быть скомпрометированы конфиденциальные персональные данные, размещенные на его системах. Согласно уведомлению, 4 июня компания зафиксировала подозрительную активность в своей компьютерной сети. Innophos Holdings Inc. начала расследование, которое выявило, что примерно 4 июня неавторизованные лица могли получить доступ к конфиденциальным личным данным. Компания провела проверку данных, чтобы определить, какая информация была затронута инцидентом, и выявить пострадавших лиц, однако не уточнила, какие именно типы личных данных, возможно, были скомпрометированы. Компания оперативно приняла меры к блокированию своих систем, уведомила федеральные правоохранительные органы, привлекла группу ведущих экспертов-криминалистов к расследованию инцидента и внедрила передовые технологии мониторинга. В результате этих мер Innophos Holdings Inc. удалось восстановиться после инцидента и возобновить работу в обычном режиме. Компания продолжает работать с экспертами для устранения последствий атаки и внедрения дополнительных мер защиты.

Кибератака на Ortec

Производственный сектор, химическая промышленность

Отказ ИТ-систем, утечка персональных данных

Американский производитель специализированных химических продуктов Ortec столкнулся с нарушением работы сети 28 мая и уведомил генерального прокурора штата Мэн в сентябре. Компания немедленно приняла меры для защиты сетевой инфраструктуры и привлекла экспертов по кибербезопасности для проведения расследования, которое показало, что примерно 28 мая 2024 года неавторизованные лица могли несанкционированно изъять некоторые файлы. Ortec провела тщательный анализ данных, затронутых инцидентом, чтобы выяснить, содержалась ли в них персональная информация, и 5 сентября определила, что в состав этих данных входила определенная персональная информация. Такая информация могла включать имена клиентов и номера социального страхования. Компания реализовала дополнительные меры безопасности, чтобы

предотвратить повторение подобных инцидентов. Она также уведомила Федеральное бюро расследований, выразив готовность оказать максимальное содействие в привлечении виновных к ответственности.

Горнодобывающая промышленность

Атака на Sibanye-Stillwater с применением шифровальщика

Горнодобывающая промышленность

Отказ ИТ-систем, нарушение операционной деятельности

Шифровальщики

Южноафриканская горнодобывающая компания Sibanye-Stillwater стала жертвой кибератаки с применением программы-вымогателя, в результате чего была частично нарушена ее операционная деятельность. Компьютерные системы были отключены, после чего началось их постепенное восстановление. Sibanye-Stillwater заявила, что после обнаружения инцидента она незамедлительно приняла меры для превентивной изоляции ИТ-систем и защиты данных. В пресс-релизе от 11 июля компания указала, что атака затронула только систему начисления заработной платы. Однако представители подразделения в американском штате Монтана сообщили, что работа плавильного оборудования в Коламбусе, штат Огайо, была нарушена из-за выхода из строя всех автоматизированных систем, но при этом сотрудники оставались на местах. Компания не смогла установить, кто стоял за атакой, и не получала требований о каких-либо выплатах.

Sibanye-Stillwater уведомила 9 сентября генеральных прокуроров штатов Массачусетс и Мэн о нарушении безопасности данных, которое могло привести к компрометации конфиденциальных персональных данных и охраняемой медицинской информации, размещенной на ее системах. В августе компания узнала, что персональные данные, хранящиеся на ее системах в США, могли быть скомпрометированы. Она приступила к анализу данных, чтобы определить, какая информация могла быть затронута инцидентом, и выявить пострадавших. Затронутая информация различалась для разных людей, но типы данных, которые могли подвергнуться утечке, включали имена, номера социального страхования, даты рождения, контактные данные, номера удостоверений личности и/или паспортов, финансовую информацию и медицинские сведения. Общее число пострадавших было оценено в 7258 человек. Группа вымогателей RansomHouse включила Sibanye-Stillwater в свой список жертв.

Кибератака на Industrias Peñoles

Горнодобывающая промышленность

Шифровальщики

Мексиканская горнодобывающая компания Industrias Peñoles сообщила о том, что стала жертвой кибератаки, в заявлении, поданном на Лондонскую фондовую биржу 30 июля. Атака также затронула ее дочернюю компанию Fresnillo. Industrias Peñoles заявила, что атака привела к несанкционированному доступу к некоторым ИТ-системам и данным. После обнаружения инцидента Fresnillo задействовала меры реагирования для локализации инцидента; ИТ-специалисты совместно с внешними экспертами-криминалистами провели расследование инцидента и оценили последствия. Компания уточнила, что кибератака не повлияла на ее операционную деятельность и она не ожидает какого-либо финансового или материального ущерба. Группа вымогателей Akira взяла на себя ответственность за атаку.

Атака на Evolution Mining с применением шифровальщика

Горнодобывающая промышленность

Отказ ИТ-систем

Шифровальщики

Австралийская горнодобывающая компания Evolution Mining 8 августа столкнулась с атакой с применением программы-вымогателя, в результате чего были затронуты ИТ-системы. Это следует из заявления компании от 12 августа. Evolution Mining оперативно привлекла внешних экспертов по кибербезопасности и криминалистике для расследования и локализации инцидента, который, по утверждению компании, был успешно ликвидирован. Также она сообщила об атаке в Австралийский центр кибербезопасности, указав, что не ожидает значительного влияния инцидента на операционную деятельность. Австралийский центр кибербезопасности сообщил агентству Reuters, что Evolution Mining не предоставила ему существенной информации об атаке.

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