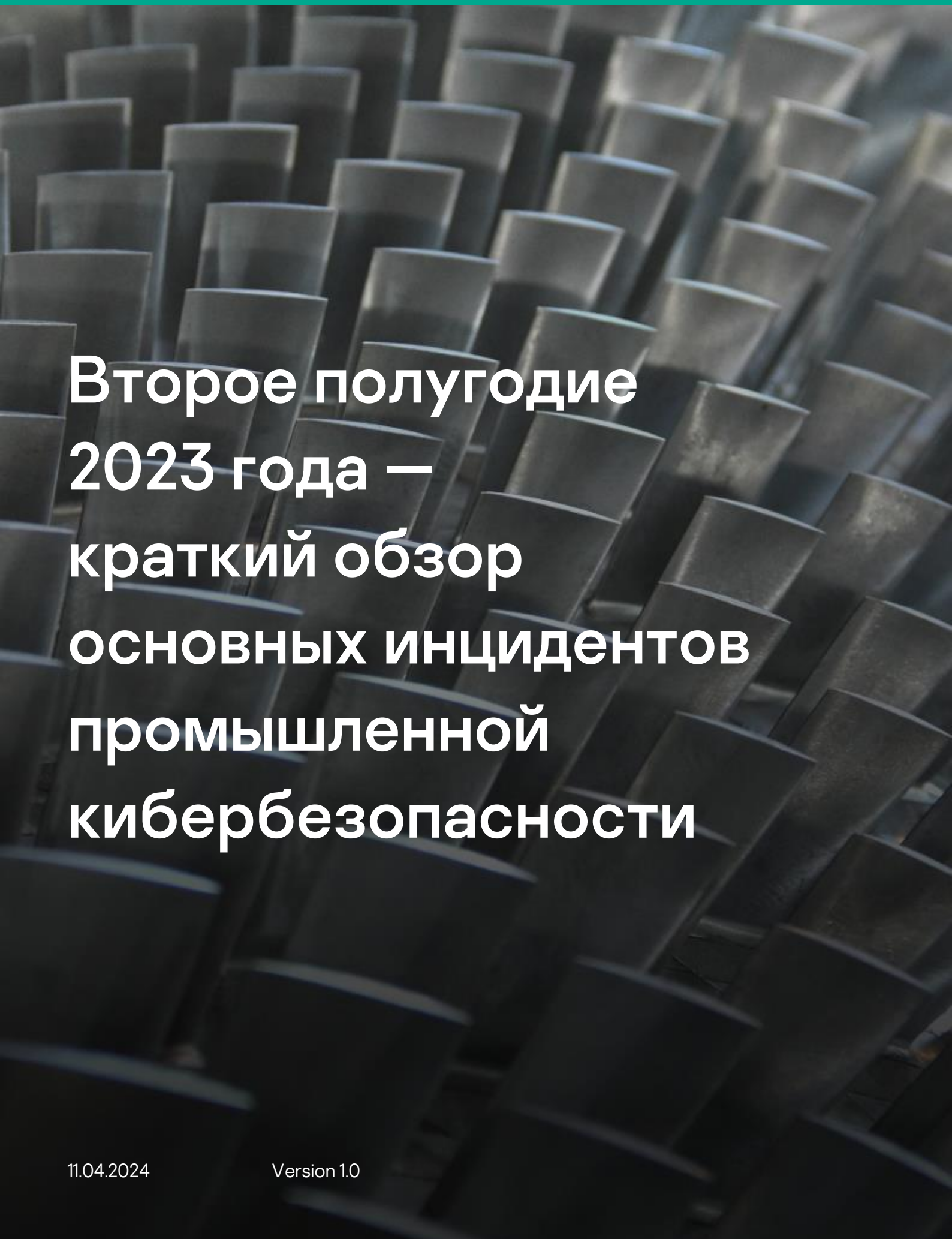
kaspersky



Второе полугодие 2023 года — краткий обзор основных инцидентов промышленной кибербезопасности

11.04.2024 Version 1.0

В этом обзоре мы расскажем об атаках киберпреступников и хактивистов на промышленные предприятия. APT-атакам посвящен отдельный отчет.

Многие ссылки на сайты компаний, где была опубликована информация об инцидентах, в настоящее время не работают — соответствующая информация уже удалена. Тем не менее мы решили оставить эти ссылки в тексте, потому 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 госслужащими. Неподтвержденные заявления киберпреступных групп о компрометации в отчете не рассматриваются.

Количество историй в этом обзоре почти совпало с предыдущим полугодием (64 против 67), однако в среднем последствия атак оказались более серьезными (либо пострадавшие организации почему-то оказались более честными).

О материальных последствиях атак, таких как остановка производства или поставок продукции, жертвы атак второго полугодия 2023 года сообщали в 2 раза чаще, чем жертвы атак первого полугодия (в 37,5% случаев против 18%).

Некоторые жертвы опубликовали информацию о понесенных в результате атаки убытках. Максимальную цифру — 356 миллионов долларов — назвала Clorox, американская компания — производитель чистящих, моющих и дезинфицирующих средств.

Атака на одного из старейших британских грузовых перевозчиков KNP Logistics стала причиной закрытия бизнеса (по крайней мере, так заявила администрация — «...<атака> лишила компанию возможности привлечь дополнительные инвестиции и финансирование»). Большинство сотрудников KNP Logistics в результате атаки были уволены фактически одним днем. 170 сотрудникам одной из дочерних компаний перевозчика повезло больше — компанию продали, и они избежали увольнения.

Некоторые из атак чуть было не вызвали лавинообразный эффект — серьезных инфраструктурных последствий едва удалось избежать. Так, например, в результате атаки на логистическую компанию DP World Australia в четырех австралийских портах застряло более 30 000 контейнеров. Атака на китайскую компанию Yanfeng, мирового лидера производства деталей интерьера автомобилей, привела к остановке сборочных конвейеров другого автомобильного супергиганта — компании Stellantis.

В трех известных случаях атакующим удалось получить доступ к системам автоматизированного управления — и с его помощью добиться физических последствий. Атака произраильской группировки парализовала до 70% иранских автозаправочных станций. Атака на ПЛК Unitronics израильского производства, применяемые в ЖКХ ряда стран мира, оставила временно без воды 160 домовладений в Ирландии. О третьем громком случае — атаке на украинское энергетическое предприятие — написано в нашем обзоре APT-атак на промышленные предприятия, результаты технического исследования которых были опубликованы и стали доступны для широкой общественности.

Из случаев, по разным причинам показавшихся нам интересными, хочется выделить атаку на ORBCOMM — американского производителя оборудования для промышленного интернета вещей и M2M-коммуникаций и провайдера сервиса сбора телеметрии. Атака остановила их платформу управления флотом FleetManager и блокировала работу линейки Blue Tree — оборудования для логирования работы водителей грузовиков, обязательного в соответствии

с локальным законодательством. Атака интересна тем, что может предвещать развитие нового вектора атак — на конечное оборудование и системы сбора телеметрии транспортных средств, а через них на сами транспортные средства. О возможности такого развития мы писали в наших недавних прогнозах на 2024 год.

Июль

- KNP Logistics Group
- Japan Aerospace Exploration Agency
- Port of Nagoya
- Wildeboer Bauteile
- TOMRA
- Estée Lauder
- Tempur Sealy
- Seiko Group
- Campbell Soup
- BAZAN Group
- Stader Land Drinking Water Association

Август

- Zaun Limited
- Freeport-McMoRan
- Clorox
- Kansai Nerolac
- Engie
- Stadtwerke Neumünster
- Kendrion Kuhnke

Сентябрь

- KIA Motors
- ORBCOMM
- Alps Alpine
- Auckland Transport
- Somagic
- Wacoal
- Johnson Controls
- Baccarat

Октябрь

- D-Link
- Estes Express
- Hochsauerlandwasser and HochsauerlandEnergie
- Volex
- Simpson Manufacturing
- BHI Energy
- Verhelst Groep
- Röhr + Stolberg GmbH
- SIAAP
- Yamaha Motor
- Boeing
- BAUER Group

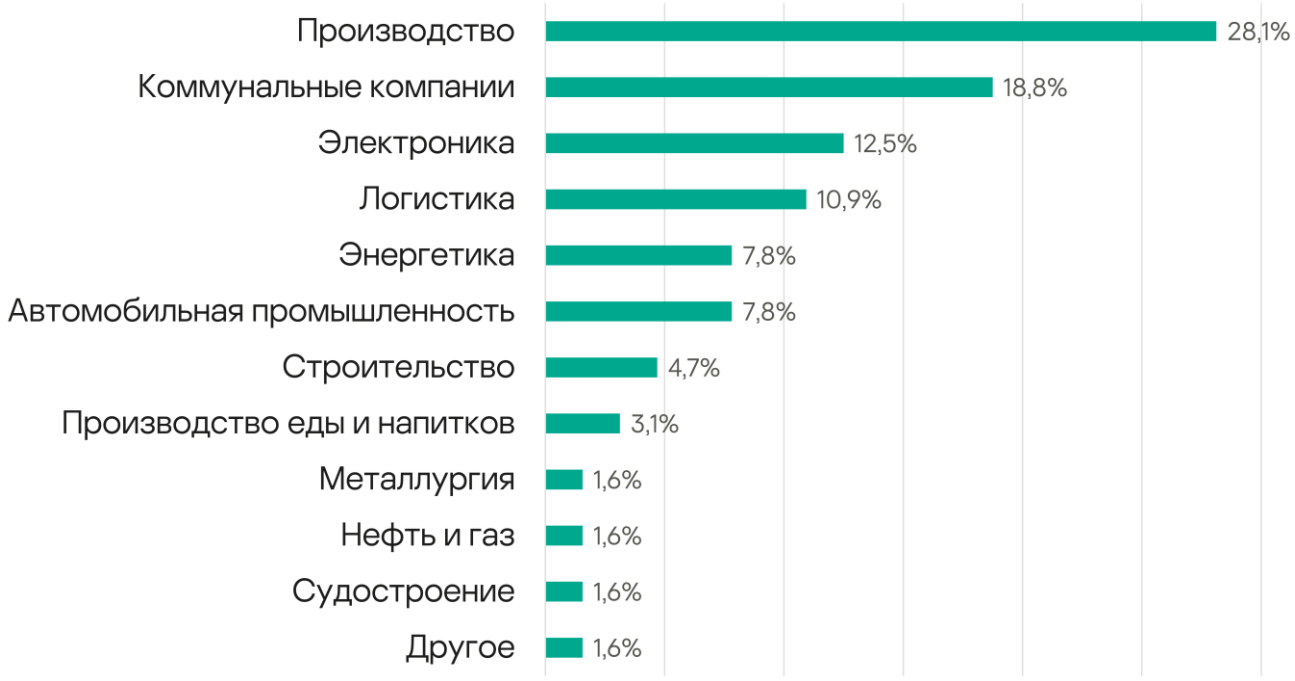
Ноябрь

- Japan Aviation Electronics
- Bartec
- DP World
- North Texas Municipal Water District
- Yanfeng
- Idaho National Laboratory
- HSE
- PFAFF
- Municipal Water Authority of Aliquippa
- AVU
- Grimme
- Guyamier
- Drum/Bingham stown Group Water Scheme

Декабрь

- Gräbener Maschinentechnik
- Koh Brothers Eco
- Aqualectra
- Austal USA
- Nissan Australia
- Allgaier
- Jysk Energi
- VF Corporation
- Yakult Australia
- Iran's gas stations
- Elektroprivreda Srbije
- Lower Valley Energy

2024



Производственный сектор

Атака с использованием программы-вымогателя на Wildeboer Bauteile

Производственный сектор

Отказ IT-сервисов, нарушение операционной деятельности

Программы-вымогатели

Немецкая компания Wildeboer Bauteile стала жертвой кибератаки 14 июля. На своем сайте компания сообщила, что инцидент привел к существенным нарушениям в работе ее информационных и коммуникационных систем. Узнав об атаке, компания сразу же отключила пострадавшие системы, что привело к ограничению возможностей взаимодействия с клиентами, поставщиками, органами власти и партнерами по бизнесу.

Злоумышленникам удалось взломать мощную систему защиты корпоративных IT-систем, но на начальном этапе было неясно, украли ли они данные компании. Чтобы ответить на этот вопрос, Wildeboer привлекла к расследованию внешних специалистов по криминалистическому анализу, а также уполномоченные органы власти, которые принимали участие во всех последующих этапах работы с инцидентом. Представитель Wildeboer подтвердил телерадиокомпании Norddeutscher Rundfunk, что в результате атаки корпоративные данные были зашифрованы. Преступники оставили файл-записку с требованием выкупа и виртуальным адресом для связи. Однако вместо ответа на это требование компания подала заявление в полицию.

11 августа компания выпустила обновление, в котором говорилось, что производство возобновилось. Это подтвердило, что производство было остановлено почти на месяц.

Кибератака на TOMRA

Производственный сектор

Отказ IT-сервисов, нарушение операционной деятельности, утечка данных

TOMRA, норвежский производитель сортировочного оборудования, пострадал от масштабной кибератаки, которая вывела из строя некоторые корпоративные системы хранения данных. Компания обнаружила атаку 16 июля и сразу же приняла меры к ее сдерживанию и нейтрализации: отключила некоторые службы и привлекла к устранению последствий инцидента штатных и внешних специалистов. Большинство цифровых сервисов некоторое время продолжали работать в автономном режиме, но функциональность некоторых служб была нарушена. Крупные офисы, в которых трудились удаленные сотрудники, остались без интернета, но подразделения TOMRA Recycling и TOMRA Food продолжали работать, несмотря на ограничения в работе цифровых сервисов.

Позже TOMRA уточнила детали инцидента. Компания заявила, что злоумышленник получил доступ к системам технической инфраструктуры, что позволило ему добраться и до других объектов. В ходе первоначального расследования выяснилось, что атака началась уже давно: преступники получили доступ к системам через скомпрометированные учетные записи сотрудников компании. Штатным специалистам TOMRA по ИБ удалось выяснить, какие методы и инструменты использовали злоумышленники. По заключению TOMRA, атака на компанию не представляла угрозы для ее клиентов и партнеров и не могла привести к компрометации их систем. Данные компании не были зашифрованы, а выкупа никто не требовал.

Кибератака привела к перестройке всей IT-инфраструктуры глобальной организации. Она включила восстановление основных центров обработки данных, проверку более пяти тысяч учетных записей пользователей, а также переработку и восстановление базовой IT- и сетевой инфраструктуры. TOMRA заявила, что внедрила архитектуру Zero Trust. Как показал инцидент, осведомленность сотрудников и их бдительность играет ключевую роль — очень важно обеспечить их всестороннее обучение. Создание определенной структуры и процедуры восстановления после инцидентов имеет важное значение, поскольку инциденты часто могут длиться дольше, чем первоначально ожидалось. Изучение соответствующего опыта других людей может оказаться неоценимым.

Кибератака на Estée Lauder

Производственный сектор

Отказ IT-сервисов, утечка данных

0-day, MOVEit MFT, программы-вымогатели

18 июля 2023 года американский производитель косметики Estée Lauder Companies Inc. сообщил о несанкционированном доступе третьих лиц к своим системам. Компания предусмотрительно отключила пострадавшие системы и приступила к расследованию с участием экспертов по кибербезопасности и представителей правоохранительных органов. Неавторизованному пользователю удалось получить некоторые данные, и компании предстояло оценить масштаб и характер инцидента. Estée Lauder предприняла меры для восстановления пострадавших систем и служб, а также защиты нарушенных бизнес-процессов.

В этот же день группы вымогателей Clop и BlackCat добавили группу компаний Estée Lauder в список жертв на своем сайте в даркнете — видимо, переговоры о выкупе не состоялись или зашли в тупик. Для доступа к корпоративным системам Clop, вероятно, использовала уязвимость платформы MOVEit Transfer, которая предназначена для безопасной передачи файлов. Вымогатели из BlackCat написали жертве сообщение, в котором высмеивали принятые компанией меры безопасности.

Злоумышленники утверждали, что они до сих пор присутствуют в сети, несмотря на то что Estée Lauder привлекла к расследованию инцидента экспертов Mandiant и специалистов Microsoft по обнаружению и реагированию (DART). Атакующие также заявили, что не шифровали корпоративные системы, но при этом угрожали распространить украденные данные, если Estée Lauder не пойдет на переговоры.

Кибератака на Tempur Sealy

Производственный сектор

Отказ IT-сервисов, нарушение операционной деятельности

Американскому производителю кроватей Tempur Sealy International пришлось отключить часть своих IT-систем в результате кибератаки, которая была обнаружена 23 июля. Это привело к временной остановке операционной деятельности компании. Tempur Sealy уведомила об инциденте Комиссию США по ценным бумагам и биржам по форме 8-K, указав, что уже принимает меры к восстановлению критически важных IT-систем и операций. Tempur Sealy обратилась в правоохранительные органы и привлекла к работе с инцидентом юриста, экспертов по цифровой криминалистике и других специалистов по реагированию. 2 августа группа вымогателей AlphV/BlackCat взяла на себя ответственность за атаку, заявив, что имеет в своем распоряжении конфиденциальные документы высшего руководства компании.

Атака с использованием программы-вымогателя на Zaun Limited

Производственный сектор

Утечка данных

Программы-вымогатели

Zaun Limited, британский производитель спортивных ограждений и высоконадежных систем для защиты периметра, подвергся изощренной атаке группы вымогателей LockBit 5 — 6 августа. Согласно заявлению компании, которое было опубликовано на ее сайте, шифрование сервера и простои в работе удалось предотвратить. Заявление было опубликовано уже после того, как 13 августа группа LockBit взяла на себя ответственность за атаку. Злоумышленники проникли в систему через незащищенный компьютер с ОС Windows 7, на котором работало ПО управления производственным оборудованием. После инцидента компания отключила это оборудование и закрыла уязвимость.

Изначально компания считала, что ей удалось предотвратить утечку информации, но позже подтвердила, что LockBit извлекла около 10 ГБ данных. Скорее всего, все они хранились на уязвимом компьютере, но не исключено, что к преступникам попали и некоторые данные с сервера (0,74% всех данных компании). В расследовании инцидента принимали участие Национальный центр кибербезопасности (NCSC) и Управление по вопросам информации (ICO) Великобритании.

Кибератака на Clorox

Производственный сектор

Отказ IT-сервисов

14 августа американская компания Clorox, которая занимается производством химической продукции, сообщила об обнаружении подозрительной активности в некоторых корпоративных IT-системах. Компания сразу же приняла меры к сдерживанию инцидента и устранению его последствий, в том числе отключила некоторые системы от интернета. Для устранения проблемы Clorox активно взаимодействовала со специалистами по реагированию и правоохранительными органами. Компания нашла эффективные временные решения, которые обеспечили непрерывность некоторых операций даже в отсутствие интернета, и продолжала обслуживать клиентов. Тем не менее инцидент негативно отразился на многих аспектах бизнес-процессов компании.

В следующем месяце Clorox подала еще один отчет SEC, в котором говорилось, что, по их мнению, взлома удалось избежать, но это привело к замедлению темпов производства и «повышению уровня проблем с доступностью потребительских товаров». Clorox заявила, что общий ущерб от инцидента составил 356 миллионов долларов за счет снижения чистых продаж.

Атака с использованием программы-вымогателя на Kansai Nerolac

Производственный сектор

Программы-вымогатели

Kansai Nerolac Ltd., расположенная в Индии дочерняя компания японского производителя красок Kansai Paint, сообщила об атаке вымогателей, которая произошла 20 августа. В обращении к акционерам Kansai заявила, что технические специалисты, отдел ИБ и руководство компании оперативно отреагировали на угрозу, приняли предусмотренные протоколами необходимые меры, чтобы устранить последствия атаки, и незамедлительно уведомили о ней соответствующие органы. К расследованию причин инцидента и оценке масштаба его последствий были привлечены специализированные агентства безопасности. Компания также отметила, что восстановила все бизнес-процессы и что системы в японских подразделениях не пострадали.

Атака с использованием программы-вымогателя на Somagic

Производственный сектор

Программы-вымогатели

По сообщениям местных СМИ, французский производитель оборудования для гриля и барбекю Somagic пострадал от кибератаки. 18 сентября доступ сотрудников к корпоративным данным оказался заблокирован, а ко всем файлам было добавлено расширение .medusa, что говорит о связи инцидента с хакерской группой Medusa. Medusa добавила компанию в список своих жертв.

Кибератака на Wacoal

Производственный сектор

Отказ IT-сервисов

Компания Wacoal Europe Co. Ltd., европейский филиал японского производителя нижнего белья, 19 сентября пострадала от кибератаки, которая вывела из строя ее системы обработки заказов, сайты и телефонные системы. Сайты брендов Wacoal, Fantasie, Freya и Elomi не работали, выдавая лишь сообщение о проведении технических работ. Следуя рекомендациям внешних экспертов, Wacoal Europe провела полноценное расследование и повысила безопасность систем. Компания приняла меры реагирования на инцидент и восстановила повседневные операции. Подробные сведения не разглашаются.

Кибератака на Baccarat

Производственный сектор

Отказ IT-сервисов, нарушение операционной деятельности и поставок

27 сентября компания Baccarat S.A., французский производитель хрусталя, сообщила, что стала жертвой кибератаки. Атака привела к нарушению операционной деятельности компании, обработка онлайн-заказов и поставки были временно приостановлены. Согласно заявлению Baccarat, не было обнаружено признаков компрометации персональных или других конфиденциальных данных клиентов. Компания наняла сторонних специалистов для оценки причиненного ущерба, поиска пострадавших систем и подготовки плана постепенного восстановления. Группа вымогателей Black Basta добавила компанию в список своих жертв 17 октября. 21 октября Baccarat сообщила о том, что публикацию злоумышленников анализируют эксперты. Компания принимала многочисленные и решительные меры по обеспечению безопасности своих систем с самого начала кибератаки.

Атака с использованием программы-вымогателя на Johnson Controls

Производственный сектор

Отказ IT-сервисов

Программы-вымогатели

Johnson Controls International (JCI), крупная американская компания, которая занимается производством автозапчастей, оборудования для систем вентиляции, кондиционирования и обогрева воздуха, а также систем безопасности и автоматизации для зданий и сооружений, 27 сентября уведомила Комиссию США по ценным бумагам и биржам о кибератаке, в результате которой пострадала ее внутренняя IT-инфраструктура. Компания немедленно привлекла внешних экспертов по кибербезопасности к расследованию, ход которого согласовывался со страховщиками.

В результате инцидента некоторые бизнес-процессы компании были нарушены. По данным BleepingComputer, несколько филиалов JCI, которые занимаются производством противопожарного оборудования, оборудования для систем вентиляции, кондиционирования и обогрева воздуха и средств обеспечения безопасности зданий и сооружений, не могли пользоваться IT-системами, поскольку по указанию официальных лиц те были отключены от интернета в ответ на атаку.

Специалист Nextron Systems опубликовал в Twitter записку с требованием выкупа, которую киберпреступная группа Dark Angels создала с помощью своего шифровальщика, атакующего гипервизоры VMware ESXi. В записке говорилось о компрометации Johnson Controls International, шифровании их систем и утечке критически важных данных. По информации CNN, в служебной записке Министерства национальной безопасности США был поднят вопрос о том, что атака на Johnson Controls могла привести к компрометации конфиденциальных сведений, например о поэтажных планах здания министерства, и таким образом поставить под угрозу физическую безопасность этого ведомства.

Группа вымогателей Dark Angels заявила, что украла более 27 ТБ конфиденциальных данных у Johnson Controls. Затем злоумышленники потребовали выкуп в размере 51 миллиона долларов за удаление данных и предоставление расшифровщика файлов.

По мнению SEC, «влияние на чистую прибыль за три месяца, закончившихся 31 декабря 2023 года, упущенных и отложенных доходов, за вычетом доходов, отложенных в конце 2023 финансового года и признанных в первом квартале 2024 финансового года, и расходов в течение квартала составила около 27 миллионов долларов».

Кибератака на Volex

Производственный сектор

Volex, британский производитель кабелей для передачи электроэнергии и данных, 9 октября подтвердил, что злоумышленники проникли в его техническую инфраструктуру и получили доступ к его данным. В обращении к инвесторам компания сообщила, что она активировала протоколы безопасности и приняла меры для блокирования несанкционированного доступа к своим системам и данным сразу же после обнаружения атаки. Инцидент не привел к остановке производства ни на одном из объектов и минимально повлиял на глобальный уровень производства. Торговля с клиентами и партнерами не прерывалась. Финансовый ущерб, по оценкам компании, будет несущественным.

Кибератака на Simpson Manufacturing

Производственный сектор

Отказ IT-сервисов

Simpson Manufacturing, один из ведущих производителей строительных и конструкционных материалов в Северной Америке, пострадал от инцидента, который вызвал сбои в работе приложений и IT-инфраструктуры. В результате атаки компании пришлось отключить инфраструктуру, о чем она уведомила Комиссию США по ценным бумагам и биржам по форме 8-K 10 октября 2023 года. Компания заявила, что вследствие инцидента возникли нарушения в некоторых бизнес-процессах. Simpson Manufacturing привлекла ведущих сторонних экспертов для помощи в расследовании и восстановлении.

Атака с использованием программы-вымогателя на Yamaha Motor

Производственный сектор

Утечка персональных данных

Программы-вымогатели

Компания Yamaha Motor Co., Ltd., японский производитель мототехники, сообщила об атаке с использованием программы-вымогателя на один из серверов ее дочернего предприятия Yamaha Motor Philippines (YMPH), Inc., которое расположено на Филиппинах и занимается производством и продажей мотоциклов. Инцидент был подтвержден 25 октября, а 16 ноября компания подтвердила утечку персональных данных некоторых сотрудников. 27 октября YMPH уведомила об инциденте уполномоченные органы Филиппин.

Компания сообщила, что, узнав об атаке, IT-центр головного офиса Yamaha Motor в Японии и YMPH незамедлительно собрали группу реагирования, приняли меры для предотвращения дальнейшего ущерба и приступили к оценке масштаба последствий. Согласно заявлению компании, к работе по восстановлению была привлечена внешняя организация, специализирующаяся на кибербезопасности.

Атака затронула только один сервер YMPH. Компания подтвердила, что системы головного офиса и других подразделений Yamaha Motor не пострадали.

Группа вымогателей INC Ransomware взяла на себя ответственность за атаку и кражу данных. 15 ноября злоумышленники добавили компанию в список своих жертв в даркнете и опубликовали около 37 ГБ данных, в том числе персональных данных сотрудников, резервных копий файлов, корпоративных данных и сведений о продажах.

Атака с использованием программы-вымогателя на Boeing

Производственный сектор

Отказ IT-сервисов, нарушение операционной деятельности

Программы-вымогатели

Американская компания Boeing, производитель авиационной, космической и военной техники, подтвердила факт кибератаки на ее подразделение глобального обслуживания через пять дней после того, как группа вымогателей LockBit заявила 28 октября об атаке на компанию. Согласно официальному комментарию компании, от кибератаки пострадало подразделение по обеспечению комплектующими, однако инцидент не представляет угрозы для безопасности полетов. Boeing подтвердила, что проводит расследование при участии правоохранительных и надзорных органов. После атаки сайт подразделения глобального обслуживания был недоступен — посетители видели лишь сообщение о «технических проблемах».

Впоследствии злоумышленники удалили упоминание Boeing со своего сайта, заявив компании VX-Underground, которая занимается исследованием и анализом киберугроз, что 1 ноября начались переговоры. Однако 7 ноября, после того как переговоры провалились, они вновь добавили компанию в список своих жертв. 10 ноября преступники опубликовали данные, предположительно украденные у Boeing. Большая часть этих данных представляет собой резервные копии различных систем от 22 октября и старше. Исследовательская группа MalwareHunterTeam отметила, что многие файлы связаны с принадлежащей Boeing компанией Aviall, которая занимается производством авиационно-космических компонентов.

21 ноября Агентство США по кибербезопасности и защите инфраструктуры (CISA) информировало, что злоумышленники, вооруженные шифровальщиком LockBit 3.0, использовали уязвимость CVE-2023-4966 в системах Boeing для получения первоначального доступа к отдельной среде Boeing Distribution Inc. — подразделения по обеспечению комплектующими. Об этом сообщила сама компания Boeing.

Кибератака на PFAFF

Производственный сектор

Нарушение операционной деятельности, отказ IT-сервисов

Немецкая компания PFAFF Werkzeug- und Formenbau с головным офисом в Рётенбахе, производящая оборудование для автомобилестроения, стала жертвой кибератаки, которая парализовала ее системы. Об этом сообщила местная пресса 23 ноября. В письме управляющего директора клиентам говорилось, что в результате инцидента, который произошел 20 ноября, пострадали заводы в Рётенбахе и Шарлотте (США). Атака привела к частичной остановке производственного цикла, а часть сотрудников пришлось отправить по домам.

Кибератака на Grimme

Производственный сектор

Нарушение операционной деятельности и поставок

28 ноября Grimme, немецкий производитель сельскохозяйственного оборудования, подвергся кибератаке, которая привела к остановке производства и заставила отправить сотрудников по домам. IT-специалистам компании удалось обнаружить инцидент на ранней стадии. Они оперативно создали кризисную группу, отключили системы и тщательно проверили их. Однако последствия атаки остались не вполне ясными. На своем сайте компания опубликовала предупреждение, что из-за атаки хакеров поставки запчастей и оборудования могут быть ограничены, равно как и доступ к сайтам и порталу для поставщиков, партнеров и соискателей myGRIMME. Компания выразила надежду, что инцидент не затронул много систем и производство скоро восстановится.

Атака с использованием программы-вымогателя на VF Corporation

Производственный сектор

Отказ IT-сервисов, утечка данных, нарушение операционной деятельности

Программы-вымогатели

Компания VF Corporation, американский производитель одежды и обуви, обнаружила инцидент безопасности 13 декабря и уведомила о нем уполномоченный орган по форме 8-K. Злоумышленники зашифровали несколько корпоративных IT-систем и украли данные. VF привлекла к расследованию инцидента экспертов по кибербезопасности.

Компания отметила, что приняла меры реагирования, но тем не менее возможности обработки заказов оказались ограничены, и ей не удалось найти оперативного решения этой проблемы. В ответ на кибератаку VF отключила некоторые системы. Пытаясь обеспечить непрерывность процессов, компания перевела некоторые из них в автономный режим до тех пор, пока пострадавшие системы не были восстановлены.

В уведомлении, направленном уполномоченному органу, компания указала, что атака привела к серьезным нарушениям ее бизнес-процессов. VF сделала публичное заявление об инциденте 15 декабря — в день вступления в силу новых требований Комиссии по ценным бумагам и биржам США к отчетности о киберинцидентах. Согласно этому документу, компания должна сообщать инвесторам о существенных инцидентах кибербезопасности в течение четырех дней с того момента, когда она определила, что инцидент повлияет на ее деятельность.

Как следует из более позднего обновления, после отключения систем для сдерживания атаки компания не смогла пополнить запасы розничных магазинов, а выполнение заказов было отложено, что привело к отмене заказов, снижению спроса на некоторые интернет-магазины и задержке некоторых оптовых поставок.

Компания также сообщила, что хакеры украли личную информацию примерно 35,5 миллионов индивидуальных потребителей.

Автомобилестроение

Атака с использованием программы-вымогателя на KIA Motors

Производственный сектор, автомобилестроение

Нарушение операционной деятельности

Программы-вымогатели

6 сентября издание LaGrange Daily News получило в социальной сети сообщение о том, что неизвестный взломал компьютерные системы автопроизводителя KIA Motors Manufacturing Georgia, в результате чего компании пришлось остановить производство во время первой рабочей смены и отменить вторую смену. Представитель компании подтвердил, что один из поставщиков предупредил Kia Georgia о киберинциденте, который привел к нарушению графика производства. Kia Georgia тесно сотрудничала с поставщиком для минимизации последствий атаки и ожидала быстрого восстановления нормальной работы, однако на момент публикации новости более подробной информации об инциденте от компании не поступало. По данным еще одного источника, KIA Motors и другие поставщики автопрома, использовавшие те же программные системы, подверглись атакам вымогателей, которые требовали выкуп за восстановление данных и сервисов.

Кибератака на Gräbener Maschinentechnik

Производственный сектор, автомобилестроение

Злоумышленники атаковали немецкого производителя машинного оборудования Gräbener Maschinentechnik GmbH & Co. KG в период с 1 по 3 декабря 2023 года. Согласно официальному заявлению компании, опубликованному на ее сайте, преступники получили доступ к некоторым корпоративным базам данных, но атака не повлияла на производственные процессы и операционная деятельность была успешно восстановлена. Компания отметила, что не исключает возможности публикации ее данных. Расследование инцидента и реагирование на него осуществлялось в тесном взаимодействии с правоохранительными органами.

Кибератака на Yanfeng

Производственный сектор, автомобилестроение

Отказ IT-сервисов, отказ в обслуживании, атака на цепи поставок / доверенных партнеров

В ноябре компания Yanfeng (Yanfeng Automotive Interiors, YFAI), крупный китайский производитель автомобильных комплектующих и крупнейший мировой OEM-производитель деталей салона автомобиля для ведущих автосборочных корпораций, стала жертвой кибератаки, от которой пострадала Stellantis. Stellantis — транснациональная компания по производству автомобилей, образованная в результате слияния итальяно-американского автопроизводителя Fiat Chrysler Automobiles с французской компанией Groupe PSA и владеющая брендами FIAT, Citroen, Peugeot, Opel, Jeep, Chrysler, Dodge и многими другими.

Представитель Stellantis заявил изданию The Detroit News, что из-за атаки на внешнего поставщика пришлось приостановить производство на нескольких заводах Stellantis в Северной Америке. Stellantis поставила ситуацию на контроль и вместе с поставщиком принимала меры к восстановлению бизнес-процессов. Сайт Yanfeng 13 ноября не работал. Китайская компания отказалась комментировать ситуацию.

Группа вымогателей Qilin, также известная как Agenda, взяла на себя ответственность за кибератаку на Yanfeng Automotive Interiors и добавила компанию в список своих жертв в сети Tor 27 ноября, опубликовав финансовые документы, соглашения о неразглашении информации, коммерческие предложения, технические данные и внутренние отчеты.

Кибератака на Nissan Australia

Производственный сектор, автомобилестроение

Утечка данных, нарушение операционной деятельности

Японский автопроизводитель Nissan сообщил, что в начале декабря его подразделения в Австралии и Новой Зеландии пострадали от серьезного киберинцидента, который привел к нарушениям штатных рабочих процессов. Кроме того, злоумышленники могли получить доступ к персональным данным. Компания проинформировала клиентов Nissan Oceania о возможной утечке данных, предупредив, что в ближайшее время им следует остерегаться мошенничества.

Nissan привлекла свою международную группу реагирования к оценке последствий инцидента и приняла меры к восстановлению пострадавших систем. Компания отметила, что дилерская сеть не пострадала.

Nissan уведомила об инциденте Австралийский центр кибербезопасности и Национальный центр кибербезопасности Новой Зеландии. Компания не сообщила подробных данных о кибератаке или ее масштабах.

В своем обновлении, опубликованном 13 марта 2024 года, компания Nissan заявила, что уведомит около 100 000 человек о кибернарушении. Тип украденной у пользователей информации отличается. По текущим оценкам, у 10% пострадавших были скомпрометированы в той или иной форме правительственные документы. Набор данных включает около 4000 карточек Medicare, 7500 водительских прав, 220 паспортов и 1300 номеров налоговых деклараций. У остальных 90% пострадала другая личная информация, в том числе копии отчетов об операциях по кредитным счетам, информация о занятости или зарплате или общая информация, такая как даты рождения. В список затронутых пользователей входят некоторые клиенты Nissan (в том числе клиенты финансовых предприятий под брендами Mitsubishi, Renault, Skyline, Infiniti, LDV и RAMS), дилеры, а также некоторые нынешние и бывшие сотрудники.

Кибератака на Allgaier

Производственный сектор, автомобилестроение

По информации местных СМИ, 8 декабря Allgaier Werke GmbH, немецкий поставщик систем для автомобильной промышленности, стал жертвой кибератаки. Инцидент произошел в разгар производства по делу о финансовой несостоятельности компании. Allgaier не пришлось останавливать производство в результате атаки, однако и компания, и конкурсный управляющий воздержались от дальнейших комментариев по поводу последствий инцидента. В первоначальном сообщении также не было прямых указаний на характер и масштаб инцидента.

Энергетика

Атака с использованием программы-вымогателя на BHI Energy

Энергетика

Утечка данных, утечка персональных данных, атака на цепи поставок / доверенных партнеров

Программы-вымогатели

18 октября в уведомлении об утечке данных американская энергетическая компания BHI Energy сообщила о том, что группа вымогателей Akira проникла в ее сети и украла данные.

Злоумышленники внедрились в корпоративную сеть 30 мая 2023 года и взломали внутреннюю сеть BHI через учетную запись стороннего подрядчика, используя VPN-подключение. В течение недели после получения первоначального доступа преступники, воспользовавшись той же скомпрометированной учетной записью, провели исследование внутренней сети. 16 июня 2023 года операторы Akira вернулись в сеть компании, чтобы определить, какие данные следует извлечь. В период с 20 по 29 июня злоумышленники украли 767 тысяч файлов общим объемом 690 ГБ, включая базу данных Windows Active Directory. И, наконец, 29 июня 2023 года, после извлечения всех данных, до которых добрались злоумышленники, на все устройства BHI Energy был установлен шифровальщик Akira.

Компания сразу же сообщила об инциденте в правоохранительные органы и привлекла сторонних экспертов для восстановления систем. 7 июля 2023 года вредоносное ПО было удалено из сети BHI. Компания сообщила, что ей удалось восстановить данные из сохраненной в облаке резервной копии, которая не пострадала от атаки. Таким образом, выкуп платить не пришлось.

Некоторые из украденных файлов содержали персональные данные, в частности фамилии и имена, адреса, даты рождения, номера социального страхования и, возможно, медицинскую информацию. 18 октября 2023 года BHI уведомила об атаке 896 затронутых пользователей.

После инцидента компания усилила защиту: ввела многофакторную аутентификацию для VPN-подключений, сбросила все пароли, расширила применение EDR-решений и антивируса на все компоненты информационной среды и вывела из эксплуатации устаревшие системы.

Кибератака на Национальную лабораторию Айдахо

Энергетика

Утечка персональных данных, утечка данных

Хактивизм

Группа хактивистов SiegedSec взломала системы Национальной лаборатории Айдахо — центра ядерных исследований, входящего в структуру Министерства энергетики США. Об этом стало известно 20 ноября, после того как SiegedSec опубликовала образцы украденных данных в даркнете.

На территории лаборатории, которая специализируется на ядерной энергетике и национальной безопасности, расположено 50 экспериментальных ядерных реакторов. В настоящее время лаборатория занимается разработкой ядерных энергетических установок нового поколения, легководных реакторов и решений для защиты систем управления от киберугроз, тестированием перспективных транспортных средств, биоэнергетикой, роботизацией и переработкой радиоактивных отходов.

На хакерских форумах и в Telegram-каналах злоумышленники опубликовали подробные данные о 45 047 бывших и нынешних сотрудников, их супругов и иждивенцев, в том числе адреса электронной почты и номера телефонов, номера социального страхования, домашние адреса, кадровую информацию, включая банковскую информацию и информацию о зарплате. SiegedSec также выложила скриншоты интерфейсов системы Oracle HCM, которую использовала лаборатория, и опубликовала сообщение о взломе в корпоративной сети. Представитель лаборатории подтвердил факт взлома, отметив, что службы киберразведки и правоохранительные органы, привлеченные к расследованию, уже занимаются оценкой масштаба инцидента и поиском утечек научных данных.

Атака с использованием программы-вымогателя на HSE

Энергетика

Отказ IT-сервисов

Программы-вымогатели

По сообщениям местного издания, словенская энергетическая компания Holding Slovenske Elektrarne (HSE) столкнулась с атакой шифровальщика 22 ноября. Остановить злоумышленников, которые уже зашифровали системы и файлы компании, удалось 24 ноября. Руководитель отдела информационной безопасности заявил СМИ, что инцидент не нарушил процессы производства электроэнергии, несмотря на блокировку IT-систем и файлов.

Компания незамедлительно уведомила об инциденте Национальный офис по киберинцидентам Si-CERT и полицию Любляны и наняла внешних экспертов для устранения последствий атаки и предотвращения дальнейшего распространения вируса по информационным системам

Словении. Атаку связывают с группой вымогателей Rhysida, которая оставляет жертвам адрес электронной почты для связи без прямого требования выкупа.

По сообщению словенского новостного агентства 24ur, инцидент произошел из-за плохой кибергигиены (т. е. из-за хранения паролей в облаке).

Кибератака на Jysk Energi

Энергетика

Отказ в обслуживании

Злоумышленникам удалось проникнуть в системы Jysk Energi, крупного датского поставщика электроэнергии, однако доказательств того, что они украли или зашифровали какие-либо данные, нет. Пострадавшая компания сообщила, что после кибератаки, которая была обнаружена 9 декабря, она отключила физический доступ к интернету и некоторые системы, которыми сотрудники пользовались для работы с клиентами. Она уведомила об инциденте уполномоченные органы, ожидая, что нормальная работа будет восстановлена через неделю после публикации сообщения об атаке.

Атаки на заправочные станции в Иране

Энергетика

Отказ в обслуживании

Хактивизм

В Иране около 70% заправочных станций перестали работать в результате кибератаки. Атака ограничила возможности подачи топлива, что спровоцировало огромные очереди на заправках и пробки. Группа хактивистов Gonjeshke Darande («Хищный воробей») взяла на себя ответственность за атаку, написав об этом в своем Telegram-канале 18 декабря. Эта группировка уже проводила атаки на иранскую железнодорожную инфраструктуру и металлургический завод, и власти Ирана заявили о ее возможной связи с Израилем. Член Комитета Иранского парламента по энергетике заявил, что атака на иранскую систему топливоснабжения является внутренней и что злоумышленники проникли в систему с помощью USB-устройства или программы, запущенной внутри системы.

Электронная промышленность

Кибератака на Seiko Group

Производственный сектор, электронная промышленность

Утечка данных

10 августа японская компания Seiko Group Corporation, занимающаяся производством электроники, подтвердила утечку данных. Она заподозрила взлом 28 июля, а 2 августа наняла экспертов по кибербезопасности для оценки ситуации. Эксперты нашли следы несанкционированного доступа по крайней мере к одному из серверов компании. У Seiko были все основания полагать, что ее системы взломали, а часть данных, которая хранилась в системах компании и (или) группы компаний, была скомпрометирована.

21 августа группа вымогателей AlphV/BlackCat взяла на себя ответственность за кибератаку, опубликовав скриншоты с украденными данными, в том числе снимки электронных таблиц и презентаций.

Позже Seico заявила, что завершила всестороннюю проверку взлома с привлечением внешних экспертов по кибербезопасности. Утекшие данные хранились в бизнес-подразделениях, известных как Seiko Group Corporation, Seiko Watch Corporation и Seiko Instruments Inc. Утекло около 60 000 единиц персональных данных клиентов, сотрудников, деловых партнеров и соискателей работы.

Кибератака на Kendrion Kuhnke

Производственный сектор, электронная промышленность

Нарушение операционной деятельности

В августе Kendrion, производитель систем управления со штаб-квартирой в Амстердаме, подвергся кибератаке, в результате которой третьи лица получили несанкционированный доступ к корпоративным системам.

Для сдерживания угрозы компания отключила от сети все системы и активировала протокол реагирования, следуя плану действий в чрезвычайной ситуации для обеспечения непрерывности операций. Для расследования инцидента Kendrion наняла ведущих экспертов по кибербезопасности.

В результате атаки филиал Kendrion в Маленте (Германия) был вынужден остановить разработку и продажу продукции. При этом производство на пострадавшем участке не прерывалось. Большинство из 300 сотрудников филиала в Маленте пришлось отправить по домам. До завершения расследования компания не исключает, что преступники могли получить доступ к корпоративным данным.

5 сентября компания сообщила, что полностью возобновила работу.

Атака с использованием программы-вымогателя на Alps Alpine

Производственный сектор, электронная промышленность

Нарушение операционной деятельности и поставок

Утечка данных, утечка персональных данных

Программы-вымогатели

Японская компания Alps Alpine Co Ltd, производитель и поставщик электронных компонентов, информационно-коммуникационного и аудиооборудования, подверглась атаке с использованием программы-вымогателя. Согласно официальному заявлению, атака была обнаружена 10 сентября.

Для минимизации ущерба компания незамедлительно отключила пострадавшие серверы от сети и приступила к тщательному расследованию с участием консультанта по безопасности, чтобы определить масштаб последствий. Атака не сказалась на работоспособности компании, хотя и вызвала сбои в некоторых процессах, включая производство и поставки. Постепенно восстанавливая серверы, Alps Alpine продолжала отключать от сети те из них, которые могли пострадать от атаки.

Группа вымогателей BlackByte добавила компанию в список своих жертв в даркнете 12 сентября.

28 ноября 2023 г. компания Alps Alpine North America, Inc. подала уведомление об утечке данных Генеральному прокурору штата Техас после того, как обнаружила, что несанкционированная сторона могла получить доступ к конфиденциальной информации сотрудников, включая их имена, номера социального страхования, адреса, номера водительских прав и другие идентификационные номера, выданные правительством.

Кибератака на D-Link

Производственный сектор, электронная промышленность, сетевое оборудование

Утечка данных

D-Link, тайваньский производитель сетевого оборудования, подтвердил факт взлома и утечки данных после публикации информации об инциденте на хакерском форуме 1 октября. По предварительным данным, украденная информация не носила строго конфиденциального характера и была доступна ограниченному кругу лиц. Скорее всего, она связана со старой системой D-View 6, которая использовалась для регистрации и не поддерживается с 2015 года.

Атака была обнаружена, когда неизвестные заявили о краже персональных данных должностных лиц Тайваня и исходного кода программы для управления сетями D-View, разработанной D-Link. В расследовании принимали участие специалисты Trend Micro. Оно показало, что в результате взлома было скомпрометировано около 700 устаревших, разрозненных записей, что противоречит утверждениям преступников о краже данных

миллионов пользователей. Утечка произошла в результате фишинговой атаки, проведенной одним из сотрудников компании. Дальнейшие подробности атаки не разглашаются. D-Link подчеркнула, что ее клиенты, вероятнее всего, не пострадают от этой атаки.

Кибератака на Kyocera AVX Corporation

Производственный сектор, электронная промышленность

Нарушение операционной деятельности, утечка данных, утечка персональных данных

Компания Kyocera AVX Components Corporation (KAVX), американский производитель инновационных электронных компонентов и филиал крупнейшего японского производителя полупроводников Kyocera, 30 октября сообщила о том, что 30 марта она подверглась кибератаке на серверы ее подразделений в Гринвилле и Мертл-Бич (Южная Каролина), которая привела к прерыванию операций и утечке данных.

Узнав об инциденте, компания наняла внешнего специалиста по кибербезопасности и приступила к расследованию, уведомив правоохранительные органы. В ходе детального расследования компания выяснила, что с 16 февраля по 30 марта 2023 года неавторизованный пользователь подключался к отдельным корпоративным системам и извлекал данные.

Позже компания KAVX обнаружила, что данные, содержащиеся на затронутых серверах, включали личную информацию отдельных лиц по всему миру. Могли быть затронуты: имя и фамилия, адрес, дата рождения, личные контактные данные, такие как номер телефона и адрес электронной почты, данные, связанные с трудоустройством, такие как удостоверение личности сотрудника, информация о компенсации и заработной плате, показатели занятости, торговая деятельность, профсоюзные данные, информация о состоянии здоровья и медицинская информация, гендерная идентичность, расовая и этническая принадлежность, подписи, некоторые государственные идентификаторы, такие как номер социального страхования, номер водительских прав, номер паспорта, другие идентификационные номера, налоговая информация и номер финансового счета.

26 мая 2023 года группа вымогателей LockBit взяла на себя ответственность за атаку на KAVX, внеся ее в список жертв на своем сайте.

Атака с использованием программы-вымогателя на Japan Aviation Electronics

Производственный сектор, электронная промышленность

Отказ IT-систем, утечка данных

Программы-вымогатели

Japan Aviation Electronics, производитель электроники и аэрокосмической продукции, подтвердил кибератаку на свои системы 2 ноября, в результате которой компании пришлось отключить свой сайт. Компания сообщила, что оценила масштаб ущерба и восстановила процессы, однако ей пришлось временно отключить некоторые системы. Кроме того, наблюдались задержки в отправке и получении электронной почты.

Изначально компания сообщила только о сбоях в функционировании IT-систем, отрицая утечку данных. Однако 6 ноября группа вымогателей ALPHV/BlackCat добавила Japan Aviation Electronics в список жертв на своем сайте. Впоследствии компания подтвердила атаку вымогателей, в результате которой файлы на серверах оказались зашифрованы, а информация, хранящаяся на сервере зарубежного филиала JAE Oregon, Inc. (Орегон, США), в результате несанкционированного доступа попала в руки злоумышленников.

Japan Aviation Electronics создала рабочую группу и приступила к оценке ущерба и восстановлению систем при содействии внешних экспертов. Она проконсультировалась с уполномоченными органами и сообщила, что уведомит об инциденте клиентов и партнеров, чьи данные могли быть украдены, а также усилила защиту и приняла меры для предотвращения повторной атаки.

Кибератака на Bartec

Производственный сектор, электронная промышленность, инжиниринг

Bartec TOP HOLDING Gmbh, немецкая инжиниринговая компания — производитель электронного оборудования, сообщила на своем сайте о киберинциденте, произошедшем 10 ноября. В заявлении компании говорится о попытке несанкционированного доступа к данным на нескольких участках IT-инфраструктуры BARTEC. На большинстве участков атаку заблокировали корпоративные системы безопасности. Bartec немедленно проверила всю IT-инфраструктуру, но других попыток несанкционированного доступа к данным не обнаружила. Тем не менее компания не исключает утечки некоторых данных.

Кибератака на NXP

Производственный сектор, электронная промышленность

Утечка данных

APT

24 ноября 2023 года нидерландская пресса сообщила подробности масштабного инцидента кибербезопасности в компании NXP, которая является крупнейшим в Нидерландах производителем микроэлектроники. Chimera, китайскоязычная APT-группа, проникла в корпоративную сеть в октябре 2017 года и до начала 2020 года шпионила за компанией, оставаясь незамеченной.

О взломе стало известно в январе 2021 года, после того как Fox-IT опубликовала информацию о двух продвинутых кибератаках, нацеленных на некие авиакомпании и производителя полупроводников, название которого также не уточнялось. Позже выяснилось, что это NXP.

Злоумышленники получили доступ к системам NXP через учетные записи пользователей: для их взлома они использовали классический метод перебора паролей, а для обхода двухфакторной аутентификации — подмену телефонных номеров. Первичную информацию об учетных записях преступники нашли среди скомпрометированных данных LinkedIn и Facebook. После проникновения в инфраструктуру злоумышленники постепенно расширяли права доступа, заметали следы и перемещались в защищенные участки сети. Преступники каждую неделю возвращались в инфраструктуру жертвы в поисках ценных данных. Перед извлечением они объединяли конфиденциальные данные в зашифрованные архивы, которые затем загружали в облачные хранилища Google Drive, Microsoft OneDrive и Dropbox.

О присутствии в сети кибершпионов стало известно только после атаки на нидерландскую авиакомпанию Transavia в 2019 году, когда преступники пытались взломать систему бронирования этой дочерней компании KLM. Специалисты Microsoft и Fox-IT подключились к расследованию и локализации инцидента в апреле 2020 года — им предстояло оценить объем утечки и выяснить все подробности об атаке. Расследование показало, что APT-группа украла часть интеллектуальной собственности NXP, однако какая именно информация попала в их руки, не уточняется. Согласно годовым отчетам NXP за 2020 и 2021 годы, компания не понесла прямого материального ущерба в результате атаки.

Кроме того, журналисты NRC выяснили, что в 2018–2019 годах злоумышленники атаковали не только Transavia, но и семь тайваньских производителей микросхем. В апреле 2020 года тайваньская компания CyCraft опубликовала подробности этих инцидентов: это была крупномасштабная, хорошо скоординированная атака на Научный парк Синьчжу на Тайване, где находится головной офис TSMC — крупнейшего производителя микросхем.

Коммунальные службы

Атака с использованием программы-вымогателя на Ассоциацию производителей питьевой воды Stader Land

Водоснабжение, коммунальные службы

Отказ IT-систем, утечка данных

Программы-вымогатели

Ассоциация производителей питьевой воды Stader Land опубликовала на своем сайте сообщение об атаке вымогателей, которая произошла в конце июля. Злоумышленникам не удалось зашифровать целевые системы.

В IT-инфраструктуре Ассоциации как раз завершались работы по реконструкции с внедрением систем безопасности, которые выполнялись при поддержке внешних экспертов и в тесном сотрудничестве с правоохранительными органами и органами по надзору за соблюдением законодательства о защите персональных данных.

Атака не вызвала перебоев в поставках питьевой воды и не повлияла на качество работы Ассоциации. Однако не исключено, что преступникам удалось получить доступ к конфиденциальным данным, например адресам и сведениям об учетных записях, хотя подтверждений этому обнаружено не было.

Группа вымогателей LockBit взяла на себя ответственность за атаку и включила организацию в список своих жертв.

Кибератака на Stadtwerke Neumünster

Энергетика, коммунальные службы

Отказ IT-сервисов

В августе Stadtwerke Neumünster (SWN), региональная сервисная энергоснабжающая организация, расположенная в г. Ноймюнстер (Германия), стала жертвой кибератаки и отключила все свои системы для предотвращения ее дальнейшего распространения. Об этом компания сообщила на своем сайте.

Атака не повлияла на электро-, газо- и теплоснабжение клиентов и поставку интернет-услуг, однако привела к серьезным нарушениям рабочих процессов и сбоям в функционировании сервисов. IT-специалисты SWN обнаружили попытку шпионажа и незамедлительно отключили затронутые системы для ее пресечения. Согласно заявлению представителя компании, такие меры реагирования были необходимы для предотвращения дальнейшего ущерба и, несмотря на отключение систем, оказание социально значимых услуг осуществлялось в обычном режиме.

Тем не менее атака существенно ограничила возможности исполнения сотрудниками своих трудовых обязанностей: у них не было доступа

к электронной почте, телефонии и необходимому программному обеспечению. Дежурные службы также были недоступны, и компании пришлось записать сообщения для автоответчика с объяснением случившегося. Центр клиентского обслуживания продолжал работать с населением, однако из-за отключения систем данные клиентов были недоступны и внесение изменений в договоры оказалось невозможным.

Расследование проводило Государственное управление криминальной полиции. Представитель компании отметила, что на проведение тщательного анализа, запуск и восстановление всех систем потребуется несколько дней или даже недель.

Кибератака на Engie

Энергетика, коммунальные службы

Утечка персональных данных

23 августа пользователь хакерского форума с ником HommedeLombre опубликовал базу клиентов французской энергетической компании Engie, содержащую персональные данные 110 000 клиентов организации. Злоумышленник заявил, что использовал уязвимость в системе субподрядчика, который оказывал услуги по управлению сайтом программы субсидий на энергосбережение Engie (monespaceprime.engie.fr).

30 августа Engie подтвердила факт кибератаки, затронувшей ее сайт. Компания подала заявление и обратилась в уполномоченные органы за помощью в решении проблемы, а также сообщила о ситуации клиентам, чьи данные были похищены. Эти данные включали фамилии, имена, адреса электронной почты, телефонные и идентификационные номера клиентов.

Атака с использованием программы-вымогателя на Hochsauerlandwasser и HochsauerlandEnergie

Энергетика, водоснабжение, коммунальные службы

Отказ IT-сервисов

Программы-вымогатели

Немецкие компании Hochsauerlandwasser GmbH (HSW) и HochsauerlandEnergie GmbH (HE), осуществляющие поставки воды и электроэнергии населению, стали жертвами кибератаки, о чем стало известно 5 октября. Предоставление некоторых коммунальных услуг пришлось ограничить.

В IT-инфраструктурах компаний были обнаружены следы вредоносного ПО. Большую часть инфраструктуры удалось оперативно восстановить, однако часть рабочего ПО не использовали еще несколько дней по соображениям безопасности.

HSW и HE пригласили специалистов для проведения криминалистического аудита систем. К специалистам обеих муниципальных организаций можно

было обратиться в центрах клиентского обслуживания, по телефону, электронной или обычной почте. В результате атаки такие операции, как изменение суммы платежа, передача показаний и внесение изменений в договор, оказались недоступными.

HSW и HE подали заявление о возбуждении уголовного дела против исполнителей этой атаки. Управляющий директор подчеркнул, что вопрос выплаты выкупа не рассматривается.

Кибератака на SIAAP

Водоснабжение, коммунальные службы

Компрометация IT-сервисов

Французская организация Syndicat Interdépartemental pour l'Assainissement de l'Agglomération Parisienne (SIAAP), которая занимается очисткой сточных вод, подверглась кибератаке 24 октября. Согласно сообщению на ее веб-сайте, в результате атаки почтовый сервер SIAAP начал рассылать мошеннические сообщения «другим французским ведомствам».

IT-команды работали над защитой промышленных систем и закрыли все внешние соединения, чтобы предотвратить распространение атаки. Компания оперативно заблокировала атаку, и ее инфраструктура не пострадала. Однако с почтового сервера SIAAP было разослано несколько сотен мошеннических сообщений. SIAAP дала получателям подобных писем рекомендацию проявлять осторожность, проверять подлинность всех сообщений, которые поступают из SIAAP даже от известных отправителей, и не переходить по сомнительным ссылкам.

Компания провела тщательный анализ этого события и развернула дополнительные средства безопасности. SIAAP подала заявление в Национальное агентство безопасности информационных систем.

Кибератака на муниципальную водохозяйственную организацию г. Аликиппа

Водоснабжение, коммунальные службы

Нарушение операционной деятельности

Unitronics

Хактивизм

Муниципальная водохозяйственная организация г. Аликиппа (Пенсильвания), которая оказывает услуги водоснабжения и водоотведения, подтвердила местному телеканалу KDKA-TV, что злоумышленники получили контроль над системой, к которой подключена насосная станция.

Председатель совета директоров компании сообщил, что 25 ноября на станции, расположенной на окраине города, сработала сигнализация, после чего компания вызвала полицию. Местное издание Beaver Countian пишет, ссылаясь на комментарии компании, что злоумышленникам не удалось добраться непосредственно до водоочистных сооружений

и других компонентов системы, из строя был выведен только насос подкачки. Насос подключен к автономной компьютерной сети, которая не связана с основной сетью и физически находится в нескольких километрах от нее. Для поддержания давления воды компания воспользовалась резервным оборудованием, предварительно отключив от сети основное. Она заявила об отсутствии риска загрязнения питьевой воды или нарушения водоснабжения.

Для управления пострадавшим оборудованием использовалась система Unitronics Vision — программируемый логический контроллер с интегрированной панелью оператора. Продукты Unitronics Vision разрабатываются израильской технологической компанией, и в них уже не раз обнаруживались критические уязвимости, которые ставят под угрозу безопасность оборудования.

Группа иранских хактивистов Cyber Av3ngers вывела на дисплей скомпрометированной системы Unitronics Vision сообщение о взломе, взяв на себя ответственность за атаку. На своей странице в социальной сети группа опубликовала многочисленные ссылки на иранских лидеров и пообещала атаковать любую компанию, которая будет пользоваться израильскими продуктами или иметь иные связи с Израилем. Злоумышленники записали на свой счет уже 10 атак на водоочистные сооружения Израиля.

28 ноября Агентство США по кибербезопасности и защите инфраструктуры (CISA) сообщило, что злоумышленники проникли в инфраструктуру американской водохозяйственной компании, взломав программируемые логические контроллеры (ПЛК) Unitronics через интернет. CISA рекомендовало компаниям коммунального сектора изменить установленные по умолчанию пароли, включить многофакторную аутентификацию для всех удаленных подключений к промышленной сети, закрыть доступ к ПЛК из интернета либо установить сетевые экраны или VPN-решения, если без удаленного доступа не обойтись.

Кибератака на частный водохозяйственный комплекс Drum/Binghamstown Group Water Scheme

Водоснабжение, коммунальные службы

Нарушение операционной деятельности

Unitronics

Хактивизм

Электронные системы частного водохозяйственного комплекса в районе деревень Драм и Бингемстаун (баронство Эррис, Ирландия) подверглись кибератаке. В результате инцидента жители территории, обслуживаемой водохозяйственным комплексом Drum/Binghamstown Group Water Scheme, 30 ноября остались без воды. Как сообщалось, пострадали 180 человек (160 домохозяйств). По словам местного депутата, специалисты предпринимали все возможное для восстановления поврежденного оборудования.

Представители организации сообщили, что хакеры могли проникнуть в систему из-за того, что корпоративный сетевой экран оказался «недостаточно надежным».

Целью злоумышленников были ПЛК Unitronics израильского производства. По информации ирландских СМИ, спустившись в насосное помещение, дежурный увидел на экране оборудования сообщения «Вас взломали» и «Долой Израиль», а также название группировки, которая атаковала организацию. Хотя название этой группировки не раскрывается, вполне вероятно, что она связана с Cyber Av3ngers, взломавшей системы муниципальной водохозяйственной организации г. Аликиппа (Пенсильвания).

Кибератака на North Texas Municipal Water District

Водоснабжение, коммунальные службы

Отказ IT-сервисов

Утечка данных

Программы-вымогатели

Компания North Texas Municipal Water District (NTMWD), которая оказывает услуги водоснабжения, водоотведения и управления ликвидацией твердых отходов в 13 городах Техаса, включая Плано и Фриско, пострадала от кибератаки. Восстановив системы, компания заявила, что инцидент не повлиял на производственные процессы. NTMWD уведомила об инциденте правоохранительные органы, однако не ответила на вопрос, стоит ли за атакой группа вымогателей. По официальным данным, 12 ноября телефонные линии компании не работали.

Ответственность за атаку взяла на себя группа вымогателей Daixin Team, которая 28 ноября включила NTMWD в список своих жертв, заявив о краже более 33 000 файлов с информацией о клиентах.

Кибератака на AVU

Энергетика, коммунальные службы

Отказ IT-сервисов

В ноябре немецкая энергоснабжающая компания AVU, обслуживающая Хаттинген и Шпрокхёфель, сообщила, что пострадала от кибератаки. Для предотвращения ущерба AVU вывела системы из эксплуатации, предварительно отключив их от интернета, в результате чего онлайн-сервис компании оказался недоступным. Компания приняла превентивные меры и привлекла экспертов по безопасности к решению проблемы, благодаря чему удалось избежать компрометации клиентских данных и систем энергоснабжения.

Атака с использованием программы-вымогателя на Aqualectra

Энергетика, водоснабжение, коммунальные службы

Отказ IT-сервисов

Программы-вымогатели

Компания Aqualectra, оказывающая услуги водо- и энергоснабжения в Кюрасао, подверглась кибератаке, в результате которой ей пришлось временно отключить все системы от сети, что привело к неработоспособности внутренних систем и прекращению обслуживания клиентов.

Компания сообщила об инциденте после того, как 6 декабря группа вымогателей Akira взяла на себя ответственность за эту атаку, заявив, что она похитила рабочие файлы, платежные и другие документы компании.

Aqualectra приняла оперативные меры к нейтрализации атаки и выполнила расширенный анализ для предотвращения непоправимого ущерба. Обслуживание было полностью восстановлено, а последующие отключения электроэнергии на острове, по словам компании, не связаны с кибератакой.

Атака с использованием программы-вымогателя на Elektroprivreda Srbije

Энергетика, коммунальные службы

Отказ IT-систем

Программы-вымогатели

Сербская энергетическая компания Elektroprivreda Srbije (EPS) подверглась атаке шифровальщика, но, благодаря своевременному принятию мер безопасности, смогла избежать остановки бизнес-операций, в том числе производства и поставок электроэнергии. IT-системы были отключены по соображениям безопасности. Была нарушена работа портала Account Insight. Компания уведомила уполномоченные органы об атаке и приняла необходимые меры безопасности.

Ответственность за атаку на сербскую электроснабжающую организацию в конце декабря взяла на себя группа вымогателей Qilin, которая предложила

пользователям даркнета скачать сотни тысяч документов, предположительно украденных у компании. Qilin предлагала более 34 ГБ данных Elektroprivreda Srbije сразу и обещала пополнить базу 27 января.

Кибератака на Lower Valley Energy

Энергетика, коммунальные службы

Американская энергетическая компания Lower Valley Energy Inc сообщила о кибератаке 28 декабря. Сразу же после обнаружения инцидента Lower Valley Energy привлекла к дальнейшему расследованию юридическую компанию, специализирующуюся на кибербезопасности и защите данных, а также сторонних специалистов по криминалистическому анализу. На момент заявления о кибератаке признаки компрометации персональных данных обнаружены не были.

Логистика и транспорт

Атака с использованием программы-вымогателя на KNP Logistics

Логистика

Отказ в обслуживании, нарушение операционной деятельности

Программы-вымогатели

Британская группа компаний KNP Logistics Group объявила о своей финансовой несостоятельности после масштабной июньской атаки шифровальщика, которая вывела из строя практически все ключевые системы, остановив бизнес-процессы, уничтожив финансовую информацию и причинив группе серьезный материальный ущерб.

В июне группа вымогателей Akira включила KNP Logistics Group в список своих жертв. В сентябре стало известно, что совладельцы- бизнеса не смогли привлечь дополнительные инвестиции и финансирование и были вынуждены пойти на крайние административные меры. BBC сообщает, что в результате атаки 730 сотрудников KNP Logistics были уволены, а компанию Nelson Distribution Limited, входившую в состав конгломерата, пришлось продать, сохранив 170 рабочих мест.

Представитель компании не сообщил, обращалась ли KLP в правоохранительные органы или стороннюю организацию, специализирующуюся на реагировании на инциденты. Неясно, как именно нападение повлияло на решение владельцев компании остановить бизнес. По словам администраторов, «крупная атака с использованием программы-вымогателя … затронула ключевые системы, процессы и финансовую информацию». Это отрицательно повлияло на финансовое положение KNP Logistics и, в конечном итоге, на ее способность обеспечить дополнительные инвестиции и финансирование».

KNP Logistics Group, которая торговала под несколькими именами, включая Knights of Old, была добавлена в список жертв банды вымогателей Akira в июне. В июле компания Avast, занимающаяся кибербезопасностью, опубликовала дешифратор программы-вымогателя Akira.

Атака с использованием программы-вымогателя на порт Нагоя

Транспорт, логистика, портовая инфраструктура

Нарушение операционной деятельности

Программы-вымогатели

5 июля административный орган порта Нагоя уведомил о прекращении грузовых операций в результате атаки шифровальщика на компьютерную систему NUTS (Nagoya United Terminal System), под управлением которой находилось пять контейнерных терминалов порта. Ежегодно порт обрабатывает более двух миллионов контейнеров и 165 миллионов тоннажа грузов, включая операции Toyota Motor Corporation по экспорту автомобилей. В Toyota заявили, что не могут загружать или выгружать автозапчасти из-за сбоя. Но в компании добавили, что не было никаких сбоев в ее производстве, а логистика готовых автомобилей остается неизменной, поскольку ею управляет другая компьютерная система.

По состоянию на 4 июля все грузовые операции, в том числе по погрузке и разгрузке контейнеров, были остановлены. Это привело к временному скоплению контейнеровозов в порту. Грузовые операции возобновились 6 июля.

Издательство Japan Times сообщает, что, по данным администрации порта, за атакой стоит группа вымогателей LockBit 3.0.

Атака с использованием программы-вымогателя на ORBCOMM

Транспорт, мореплавание, коммунальные службы, нефтегазовая отрасль

Отказ IT-систем

Цепочка поставок

Программы-вымогатели

Американская компания ORBCOMM, поставщик интернет-услуг для промышленных предприятий, а также оборудования, ПО и сервисов для межмашинного взаимодействия, предназначенных для отслеживания, мониторинга и контроля стационарных и мобильных активов в транспортной, нефтегазовой и тяжелой промышленности, морехозяйственной деятельности, коммунальном хозяйстве и государственном секторе, стала жертвой шифровальщика 6 сентября.

Компания сообщила изданию BleepingComputer, что атака на некоторое время вывела из строя платформу FleetManager и продукты линейки Blue Tree (устройства электронной регистрации, или ELD, которые дальнобойщики используют для регистрации своего рабочего времени в целях соблюдения федеральных правил безопасности). Инцидент

не сказался на функционировании других систем и сервисов — клиенты пользовались ими в привычном режиме.

Компания поддерживала связь со всеми пострадавшими клиентами, информируя их о ходе расследования и восстановления. Федеральная администрация США по пассажирским перевозкам опубликовала документ, разрешающий грузоперевозчикам использовать бумажные журналы до тех пор, пока работа сервисов не будет восстановлена, но не позднее 29 сентября.

BleepingComputer стало известно, что отключение сервисов вызвало сбои в работе нескольких крупнейших в стране грузоперевозчиков — они не могли отслеживать транспортные средства и другие активы.

Атака с использованием программы-вымогателя на Auckland Transport

Транспорт

Отказ в обслуживании

Программы-вымогатели

Auckland Transport (AT), транспортное управление Окленда (Новая Зеландия), ответственное за организацию общественных пассажирских перевозок паромами, автобусами и метро, а также за проектирование и строительство дорог и других объектов инфраструктуры, подверглось кибератаке, которая вывела из строя многочисленные клиентские сервисы.

Компания сообщила, что 13 сентября 2023 года она столкнулась с атакой программы-вымогателя на некоторые участки сети, которая вызвала сбои в работе сервиса AT HOP — интегрированной системы оплаты и учета проезда. По словам представителя AT, у компании были основания полагать, что она имеет дело с программой-вымогателем, но расследование еще не было завершено. Компания незамедлительно активировала протоколы безопасности и привлекла к решению проблемы экспертов.

Ответственность за атаку на систему транспортных карт AT HOP взяла на себя группа вымогателей Medusa 18 сентября.

Исполнительный директор AT Дин Кимптон подтвердил, что это была атака с использованием программы-вымогателя под названием Medusa, и заверил пассажиров, что никакие личные или финансовые данные в результате инцидента не были скомпрометированы. По словам Дина Кимптона, злоумышленники проникли в базу данных транзакций компании, хранящую информацию о картах HOP. Ни информация о клиентах, ни банковские или личные данные, ни какие-либо другие системы не были взломаны.

Кибератака на Estes Express

Логистика

Отказ в обслуживании, отказ IT-систем

Утечка персональных данных

Американская логистическая компания Estes Express стала жертвой кибератаки, которая привела к отключению ее ключевой инфраструктуры и вызвала сбои в работе некоторых систем. Об этом она сообщила 3 октября на своем сайте и в социальной сети X. На момент объявления компания не могла раскрыть подробности происшествия, однако известно, что, пока она занималась инцидентом, терминалы работали, а водители беспрепятственно забирали и доставляли грузы. На запрос одного из клиентов компания ответила, что из-за отключения онлайн-системы отслеживать перемещение грузов было невозможно.

24 октября Estes сообщила, что восстановила свою деятельность. Корпоративные API были доступны для интеграции сервисов доставки с клиентскими бизнес-приложениями и сайтами. Президент Estes Express отметил, что компания восстановила API для работы с документами в графическом формате и теперь занималась добавлением отсканированных изображений в систему, чтобы как можно скорее продолжить выставление счетов с использованием этих API. Сайт компании и телефонная связь также были восстановлены.

Судебное расследование инцидента было завершено 7 ноября. Согласно уведомлению об утечке данных, направленному компанией в Генеральную прокуратуру, нарушение произошло 26 сентября и было обнаружено 1 октября. Личная информация 21 884 человек была украдена. Письма-уведомления пострадавшим начали отправлять только в декабре, после того как правоохранительные органы завершили собственное расследование инцидента.

Ответственность за атаку в начале ноября взяла на себя банда вымогателей LockBit. 13 ноября группа опубликовала данные, предположительно украденные у Estes, на своем сайте утечки данных в Tor.

Кибератака на DP World

Транспорт, логистика, портовая инфраструк-тура

Потеря данных, отказ в обслуживании, нарушение операционной деятельности, утечка персональных данных

DP World, международный оператор контейнерных терминалов и цепей поставок со штаб-квартирой в Дубае, под управлением которого находятся 82 терминала в 40 странах, обслуживающих около 70 миллионов контейнеров ежегодно, подвергся кибератаке, которая привела к серьезным нарушениям в работе австралийских международных портов. Атака была обнаружена 10 ноября и привела к закрытию терминалов в портах Мельбурна, Сиднея, Брисбена и Фримантла. Сообщается, что в результате инцидента около 30 000 контейнеров с разными типами товаров были задержаны в портах.

Согласно официальному заявлению компании, опубликованному на ее сайте, третьи лица получили доступ к некоторым корпоративным системам, в том числе учетным записям пользователей. Криминалистическая экспертиза показала, что данные компании были похищены из сети.

Для сдерживания инцидента техническая группа отключила локальную сеть от глобального интернета, что привело к прекращению всех внешних коммуникаций, в том числе необходимых для выполнения береговых операций. В разрешении инцидента компании содействовали Австралийское управление по связи/Австралийский центр кибербезопасности, Уполномоченный по вопросам национальной кибербезопасности, Министерство внутренних дел и кибербезопасности, Министерство инфраструктурного, транспортного и регионального развития и Австралийская федеральная полиция.

Работа терминалов была полностью восстановлена к 13 ноября. К 20 ноября, примерно через семь дней после возобновления работы порта и через 10 дней после первого обнаружения инцидента, DP World Australia обслужила 100% накопившихся грузов, включающих около 30 137 контейнеров. Представитель компании сообщил изданию Financial Review, что они не получали сообщений с требованием выкупа и считают, что платить не придется.

Расследование DP World Australia подтвердило, что инцидент ограничился австралийскими операциями и не затронул другие рынки, на которых работает DP World. Оно также подтвердило, что в сети DP World Australia не было обнаружено и не было развернуто никаких программ-вымогателей (никаких исполняемых файлов программ-вымогателей, никаких зашифрованных файлов и никаких требований о выкупе). К некоторым файлам компании получила доступ неавторизованная третья сторона, а небольшой объем данных был украден из сети DP World Australia. Затронутые данные включают личную информацию нынешних и предыдущих сотрудников DP World Australia. DP World Australia уведомила затронутых лиц.

Атака с использованием программы-вымогателя на Guyamier

Транспорт, логистика

Потеря данных, отказ в обслуживании

Программы-вымогатели

Французское транспортное и логистическое предприятие Groupe Guyamier, объединившее несколько транспортных компаний, 29 ноября пострадало от кибератаки, в результате которой доступ сотрудников к клиентской базе, электронной почте и сохраненным на компьютерах файлам оказался заблокирован. Для сдерживания атаки была создана кризисная группа, однако вымогатели вывели из строя сервер и потребовали у компании выкуп, не указав при этом его точной суммы. В телефонном разговоре представитель компании сообщил местным СМИ, что сотрудники не могли связаться с клиентами из-за отсутствия доступа к заказам и службе сообщений. Компания изолировала атакованные системы, чтобы предотвратить дальнейшее распространение программы-вымогателя, и перешла на ручные операции, чтобы не прерывать обслуживание клиентов.

Пищевая промышленность

Кибератака на Campbell Soup

Производственный сектор, пищевая промышленность

Отказ IT-систем, нарушение операционной деятельности

Американская компания Campbell Soup Co., занимающаяся производством пищевых продуктов, обнаружила кибератаку на участок своей IT-сети в конце четвертого финансового квартала. (Четвертый финансовый квартал закончился в июле, информация об атаке появилась 3 августа.) Об этом она уведомила Комиссию США по ценным бумагам и биржам в ежегодном отчете. По данным Комиссии, атака не оказала существенного влияния на деятельность компании и не привела к материальному ущербу.

Компания приняла оперативные меры к расследованию, сдерживанию и устранению угрозы, наняла сторонних экспертов по кибербезопасности и уведомила о происшествии федеральные правоохранительные органы. Согласно отчету WTOL, Campbell Soup сообщила о «сложностях с IT-системами» на заводе в г. Наполеон, штат Огайо. Компания восстановила рабочую станцию, атака на которую негативно сказалась на функционировании систем. Издание Toledo Blade сообщило, что на заводе три дня не было интернета и работников пришлось временно отправить по домам, при этом некоторые производственные линии были остановлены.

Кибератака на Yakult Australia

Производственный сектор, пищевая промышленность

Отказ IT-систем, утечка данных

23 декабря Yakult Australia, производитель пробиотических напитков, подтвердил киберинцидент в беседе с изданием BleepingComputer и на своем сайте. Атака привела к отказу IT-систем в подразделениях, расположенных в Австралии и Новой Зеландии.

По словам представителя компании, об инциденте стало известно 15 декабря. Для оценки масштаба инцидента компания наняла экспертов по кибербезопасности. Yakult Australia уведомила о случившемся Австралийский центр кибербезопасности, Национальный центр кибербезопасности Новой Зеландии, Управление по вопросам информации в Австралии и Управление по защите конфиденциальности в Новой Зеландии.

Ответственность за атаку взяла на себя группа DragonForce (также известная как DragonLeaks). 20 декабря она включила Yakult Australia в список жертв на своем onion-сайте и впоследствии опубликовала 95,19 ГБ данных. Проанализировав образец украденных данных, компания ABC обнаружила документы пострадавшей компании, самые старые из которых датировались 2001 годом. Они включали конфиденциальные сведения о сотрудниках, в том числе копии паспортов и водительских удостоверений, результаты медицинских осмотров, размер заработной платы и сведения об аттестации.

Нефтегазовая отрасль

DDoS-атака на BAZAN Group

Нефтегазовая отрасль

Отказ в обслуживании

Хактивизм

30 июля BAZAN Group, крупнейшая в Израиле группа нефтеперерабатывающих компаний, пострадала от DDoS-атаки, в результате которой сайт группы в большинстве стран оказался недоступен.

Группа иранских хактивистов Cyber Avengers (также известная как CyberAv3ngers) взяла на себя ответственность за атаку и опубликовала скриншоты корпоративной системы SCADA. BAZAN отрицает утечку данных, заявляя, что скриншоты «полностью сфабрикованы». BAZAN Group заявила, что атака не привела к повреждению серверов или других активов и что она принимает надежные меры безопасности в тесном сотрудничестве с Национальным директоратом кибербезопасности Израиля.

Хактивисты дали понять, что проникли в системы завода через сетевой экран Check Point, но производитель защитного решения отрицает наличие уязвимости. Cyber Avengers также взяла на себя ответственность за пожары и атаки, которым подверглась железнодорожная инфраструктура Израиля в 2021 году.

Судостроение

Атака с использованием программы-вымогателя на Austal USA

Производственный сектор, судостроение

В начале декабря Austal USA, австралийское отделение американского подрядчика ВМС США, которое производит инновационные суда, подтвердило кибератаку после того, как группа вымогателей Hunters International включила его в список своих жертв и опубликовала образцы украденных данных. Компания быстро обнаружила инцидент и локализовала последствия атаки, которая, по официальным данным, не повлияла на ее операционную деятельность. Злоумышленникам не удалось получить доступ к персональным и другим конфиденциальным данным. Участие в расследовании инцидента и в оценке объема скомпрометированной информации принимали ФБР и Следственное управление ВМС США. Hunters International угрожала опубликовать украденные данные, включая сведения о сертификации и сотрудниках, финансовую и техническую документацию.

Металлургия

Атака с использованием программы-вымогателя на Röhr + Stolberg GmbH

Производственный сектор, металлургия

Нарушение операционной деятельности

Программы-вымогатели

20 октября немецкая металлообрабатывающая компания Röhr + Stolberg GmbH подверглась атаке вымогателей. Штатным IT-специалистам совместно с группой внешних экспертов удалось перезапустить серверы в течение недели и восстановить большую часть рабочих процессов, в том числе производственных. На момент заявления о кибератаке системы были отключены от интернета. Взаимодействие с клиентами и поставщиками осуществлялось через защищенные компьютеры, расположенные за пределами среды, которую потенциально могла затронуть атака.

Компания уведомила об инциденте полицию и органы по надзору за соблюдением законодательства о защите персональных данных. Röhr + Stolberg не исключает того, что преступники могли украсть корпоративные данные.

Группа вымогателей LockBit включила Röhr+ Stolberg в список жертв на своем сайте.

Строительство

Кибератака на Verhelst Groep

Строительство

Отказ в обслуживании и нарушение операционной деятельности

Программы-вымогатели

Бельгийская строительная компания Verhelst Groep стала жертвой кибератаки, о чем она сообщила на своем сайте 18 октября. Атака нарушила повседневные операции: компания не могла взаимодействовать с клиентами и отслеживать движение запасов и транспортных средств. Некоторые сотрудники были вынуждены остаться дома. На место происшествия прибыли группа специалистов по государственной безопасности и представители профессиональных организаций. Совместно с IT-службой компании они в несколько этапов запустили новое программное обеспечение и восстановили данные из облачного хранилища.

Группа вымогателей Falcon разместила информацию о компании на своем веб-сайте.

Кибератака на BAUER Group

Строительство

Отказ IT-систем, отказ в обслуживании

Немецкая строительная компания Bauer AG подверглась кибератаке, о чем стало известно 31 октября. Несмотря на многочисленные меры безопасности, 30 октября 2023 года неизвестным лицам удалось получить доступ к серверам компании, что привело к отключению различных корпоративных систем (некоторые из них были дополнительно отключены в качестве меры предосторожности). Кроме того, атака повлияла на работу сайтов компании. Bauer наняла экспертов, которые содействовали штатным IT-специалистам в анализе ситуации.

В результате атаки деятельность партнеров BAUER Group по всему миру оказалась ограничена. Bauer уведомила об инциденте уполномоченные органы. Компания приняла оперативные меры к восстановлению систем и принесла извинения партнерам по бизнесу. 13 декабря компания опубликовала сообщение о том, что все операции возобновлены.

Атака с использованием программы-вымогателя на Koh Brothers Eco

Строительство

Отказ IT-систем

Программы-вымогатели

Сингапурская строительная компания и разработчик экологичных технических решений Koh Brothers Eco Engineering стала жертвой кибератаки, вследствие которой злоумышленники получили несанкционированный доступ к серверам некоторых филиалов компании и зашифровали данные. Расследование показало, что атака была управляемой, а 4 декабря компания сообщила, что не может оценить, как инцидент повлияет на группу компаний и ее деятельность. Тем не менее атака не привела к остановке работы. Компания объявила, что незамедлительно приняла меры к сдерживанию инцидента, в том числе отключила пострадавшие серверы от сети и заблокировала несанкционированный доступ к информационным ресурсам. Для оценки, реагирования и управления инцидентом она привлекла экспертов по реагированию и внешнего юриста.

Другое

Кибератака на Freeport-McMoRan

Горнодобывающая промышленность

Нарушение операционной деятельности

Freeport-McMoRan (FCX), международная горнодобывающая компания со штаб-квартирой в США, стала жертвой кибератаки. Об этом стало известно 11 августа 2023 г.

Компания провела оценку последствий и приняла проактивные меры к разрешению ситуации. Было проведено расследование инцидента. Реагирование на инцидент осуществлялось в тесном сотрудничестве с экспертами по кибербезопасности и правоохранительными органами. Кроме того, FCX развернула временные решения для защиты информационных систем. Безопасность и ответственное производство остаются главным приоритетом FCX, однако компания признала, что если ей не удастся в ближайшее время восстановить системы, это может привести к нарушению ее деятельности в будущем. На момент публикации подробные сведения о характере и масштабе кибератаки не сообщались.

Кибератака на Японское агентство аэрокосмических исследований

Аэрокосмическая отрасль

Отказ IT-сервисов

По информации издания The Japan News, атака на Японское агентство аэрокосмических исследований (JAXA) продолжалась все лето. Осенью правоохранительные органы сообщили JAXA о компрометации его систем, однако данных о том, когда атака началась, не было.

Генеральный секретарь Кабинета министров Японии подтвердил инцидент, отметив во время пресс-конференции, что злоумышленники получили доступ к серверу, на котором развернута служба Active Directory, — критический компонент управления сетевыми операциями в JAXA.

Для оценки масштаба инцидента агентство привлекло государственных экспертов по кибербезопасности и правоохранительные органы. Несмотря на отсутствие подтвержденных утечек данных JAXA, преступники могли получить доступ к ним в результате взлома сервера Active Directory.

Местное СМИ Nippon сообщило, что хакеры предположительно воспользовались уязвимостью, обнаруженной производителем сетевого оборудования в июне 2023 года, со ссылкой на источники в агентстве. Имя производителя не упоминалось.

На время расследования агентство временно отключило часть своей сети, чтобы оценить масштабы инцидента. Представитель агентства заявил, что утечки данных пока не подтверждены. JAXA не ответило на запрос о комментариях.

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