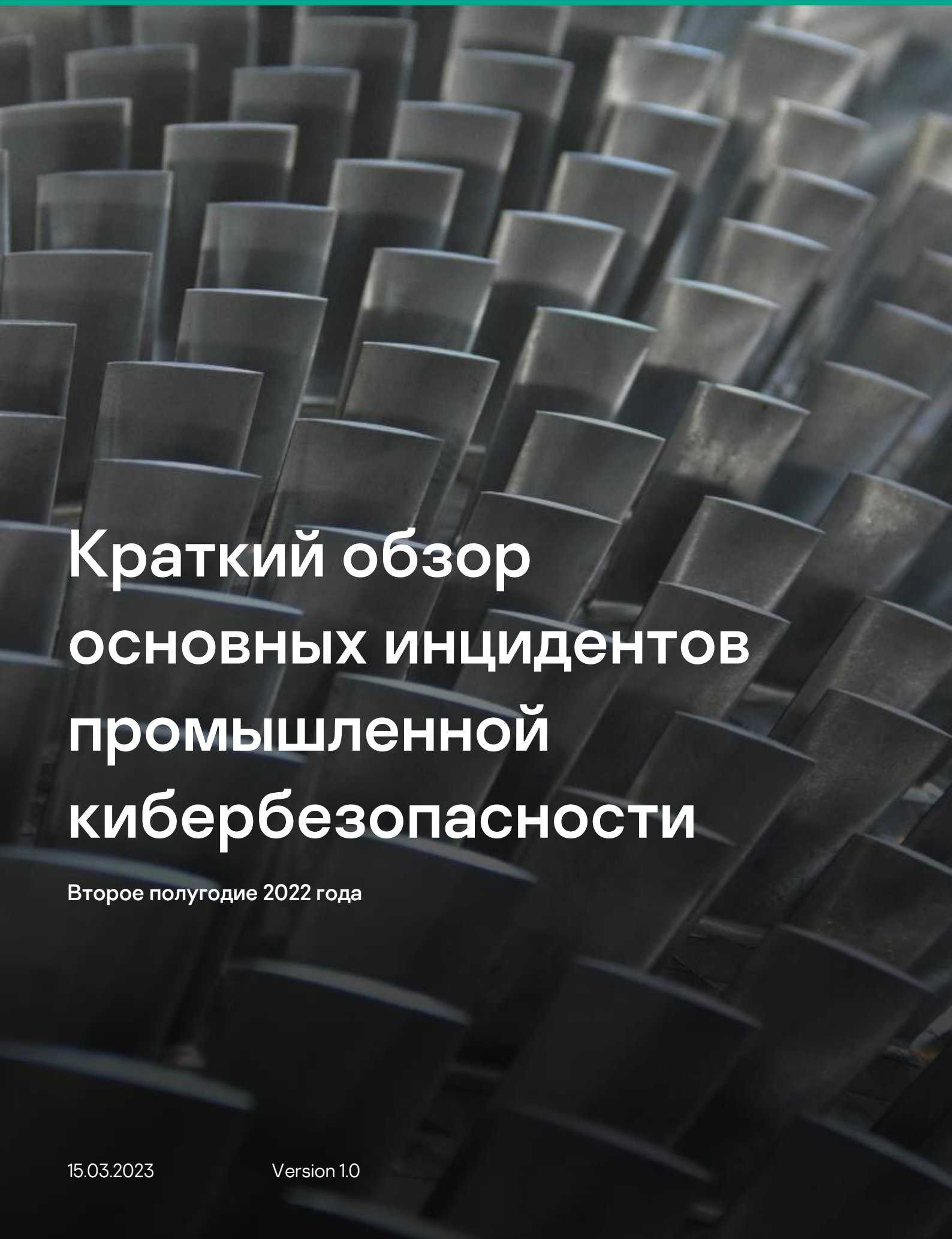
Kaspersky ICS CERT

kaspersky



Краткий обзор основных инцидентов промышленной кибербезопасности

Второе полугодие 2022 года

15.03.2023

Version 1.0

Атаки программ-вымогателей ... 3
Creos и Enovos ... 3
Cremo ... 3
Semikron ... 4
BRP ... 4
Cisco ... 5
South Staffordshire PLC ... 6
DESFA ... 6
Eni ... 7
Hensoldt ... 7
Elbit Systems ... 8
Läderach ... 8
Tata Power ... 9
Немецкое газетное издательство ... 9
U-blox ... 9
Richard Wolf ... 10
Uponor ... 10
Maple Leaf Foods ... 11
Sargent & Lundy ... 11
JAKKS Pacific ... 12
Fruttagel ... 12
EPM ... 13
Thyssenkrupp ... 13
CMMC ... 14
Лиссабонский порт ... 14
MOL ... 14
Sumitomo Bakelite North America ... 15
Бюллетени CISA ... 15
Атаки вымогателей Zeppelin ... 15
Атаки группы вымогателей Hive ... 16
Вымогатели Cuba ... 17

Другие кибератаки и случаи кражи данных 17
Weidmüller 17
Hettich Group 17
Sembcorp Marine 18
Continental 18
Eurocell 18
Enercity 19
Aurubis 19
Eesti Energia 19
Iochpe-Maxion 19
Meyer&Meyer 20
NIO Inc 20
Хактивисты 20
Атаки GhostSec на ПЛК Berghof 20

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

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

Атаки программ-вымогателей

В эту часть включены инциденты, в которых организация официально подтвердила компрометацию. Сообщения о компрометации организаций, заявленные только киберкриминальными группами, не рассматриваются.

Creos и Enovos

25 июля энергетическая компания Encevo из Люксембурга подтвердила, что её дочерние компании — оператор систем транспортировки природного газа и электрических сетей Creos и поставщик энергии Enovos — подверглись кибератаке.

По сообщению Encevo, результатом атаки стала кража злоумышленниками данных атакованных компаний, а также потеря доступа к данным. Атака также вывела из строя клиентские порталы обеих компаний. Была немедленно задействована команда реагирования на инциденты; клиентам было рекомендовано сменить учетные данные аккаунтов. Encevo подала жалобу в полицию Великого Герцогства и проинформировала об инциденте CNPD (Национальную комиссию по защите данных, National Commission for Data Protection), the ILR (Институт регулирования Люксембурга, Luxembourg Institute of Regulation) и соответствующие министерства.

Группа вымогателей ALPHV, известная также как BlackCat, взяла на себя ответственность за кибератаку на Creos и добавила информацию об этой атаке на свой сайт 30 июля, угрожая выложить в открытый доступ 180 000 украденных файлов суммарным размером 150 ГБ, в том числе контракты и договоры, паспортные данные, счета и электронные письма.

Cremo

В июле швейцарский гигант молочной промышленности Cremo пал жертвой кибератаки. Компания подала заявление в полицию, было начато расследование. По словам генерального секретаря Cremo, злоумышленники украли у компании данные и потребовали выкуп. Несмотря на атаку, компания сумела не прерывать производство и поставки продукции клиентам. Источник внутри компании подтвердил, что производство продукции не пострадало, однако вышли из строя электронные инструменты по крайней мере на части предприятий компании. В частности, не работали системы электронной почты, размещения заказов и выставления счетов.

Semikron

Немецкий производитель полупроводников Semikron сообщил 1 августа, что стал жертвой кибератаки, результатом которой стало «частичное шифрование ИТ-систем и файлов». Злоумышленники, атаковавшие Semikron, утверждают, что украли у жертвы данные. Компания немедленно приняла все необходимые меры для ограничения возможного ущерба, провела расследование инцидента и предприняла усилия для минимизации его последствий для своих сотрудников, клиентов и контрагентов.

Компания не назвала злоумышленников, однако издание BleepingComputer, сотрудник которого видел записку с требованием выкупа на одной из систем Semikron, сообщило, что за атакой, возможно, стоит группа вымогателей LV, и что, согласно записке, у жертвы украдено два терабайта данных.

BRP

Канадский производитель техники для активного отдыха BRP (Bombardier Recreational Products) сообщил 9 августа, что стал жертвой «вредоносной активности в области кибербезопасности» и принял «оперативные меры по сдерживанию ситуации». Эти меры предусматривали активацию «внутренней сети ИТ-профессионалов» и привлечение экспертов по кибербезопасности к обеспечению безопасности компьютерных систем компании и участию во внутреннем расследовании инцидента. Приостановленная в результате вторжения работа компании была возобновлена. Дочерняя компания BRP — австрийская компания по производству двигателей Rotax, также пострадала от кибератаки и приостановила свою работу.

15 августа BRP сообщила, что её работа по восстановлению своих систем и операционной деятельности продолжается, а производственные мощности в четырех странах наращивают производственную активность и могут полностью восстановить нормальную работу на следующий день. Планировалось поэтапное возвращение остальных производственных площадок к нормальной работе в течение недели. В том же сообщении BRP представила первые результаты своего внутреннего расследования, сообщив, что хакеры проникли в ее системы через стороннего поставщика услуг.

Группа вымогателей RansomEXX взяла на себя ответственность за «вредоносную киберактивность» и кражу файлов BRP общим объемом 29,9

ГБ, включая договоры о неразглашении конфиденциальных сведений, паспортные и личные данные, контракты и соглашения о поставке.

23 августа BRP опубликовала заявление, в котором подтвердила подлинность украденных документов, добавив, что компания активно работает с пострадавшими от атаки, чтобы минимизировать негативные последствия раскрытия конфиденциальной информации. В частности, BRP подтвердила, что уже связалась с очень немногочисленными сотрудниками, которые могли пострадать от инцидента.

Cisco

Транснациональный технологический конгломерат и производитель сетевого оборудования Cisco опубликовал уведомление об инциденте информационной безопасности и технический блогпост с подробностями взлома, который был обнаружен 24 мая. Компания опубликовала подробную информацию об атаке 10 августа, вскоре после публикации киберпреступниками списка файлов, якобы украденных с систем Cisco.

По сведениям Cisco, злоумышленники атаковали одного из сотрудников компании, и им удалось украсть только файлы, которые хранились в папке Box, относящейся к учетной записи атакованного сотрудника, а также данные аутентификации сотрудников из Active Directory. Компания утверждает, что информация, которая хранилась в папке Box, не была конфиденциальной.

Для получения первоначального доступа к системам компании был взломан личный аккаунт Google сотрудника. Хакеры получили учетные данные атакованного сотрудника в системах Cisco из браузера Google Chrome, в котором была включена синхронизация паролей. Для обхода многофакторной аутентификации (multi-factor authentication, MFA) злоумышленники использовали прием, известный как MFA fatigue (усталость от MFA), который основан на отправке большого количества push-запросов на мобильное устройство жертвы в надежде, что она примет запрос по ошибке или в попытке прекратить поток уведомлений.

В процессе атаки сотруднику также в течение нескольких дней поступали телефонные звонки, в ходе которых звонящий (представлявшийся сотрудником организации поддержки) пытался выманить у жертвы нужные сведения. В результате злоумышленникам удалось подключить новые устройства к MFA и пройти аутентификацию на VPN-сервере Cisco. Далее атакующим удалось повысить уровень привилегий в системе и получить права администратора, что дало им возможность авторизоваться на различных системах и установить на них средства удаленного доступа и

вредоносное ПО для следующих этапов атаки. Хакеры устанавливали бэкдоры для закрепления в системе и затем перемещались на соседние системы, включая серверы Citrix и контроллеры доменов.

По сведениям Cisco, эта атака — дело рук брокера первоначального доступа (initial access broker, IAB), связанного с группой UNC2447. Это группа злоумышленников, имеющая связи с Россией и известная использованием программ-вымогателей FiveHands и HelloKitty, а также Lapsus$. Группа отметилась в атаках на несколько крупных компаний, после чего её возможных членов вычислили правоохранительные органы. Данный брокер первоначального доступа связан также с группой вымогателей Yanluowang, которая взяла на себя ответственность за атаку на Cisco, заявив, что ей удалось украсть около 3 000 файлов общим объемом 2,8 ГБ. Судя по опубликованным хакерами именам файлов, они украли пароли для VPN-клиентов, исходный код, договоры о неразглашении конфиденциальных сведений и другие документы.

South Staffordshire PLC

South Staffordshire PLC — британская водоснабжающая компания, родительская компания South Staffs Water и Cambridge Water, — подтвердила 15 августа, что она пала жертвой кибератаки. Согласно официальному заявлению компании, было нарушено функционирование корпоративной сети, что не отразилось на её «способности поставлять безопасную воду» потребителям.

По словам предполагаемого виновника атаки — группы кибервымогателей Clop — атакована была другая, более крупная водоснабжающая компания Thames Water, которая в свою очередь назвала это заявление «киберфальшивкой». В своем заявлении группа Clop утверждала, что завладела более чем 5 ТБ данных организации-жертвы, а также получила доступ к некоторым из ее систем SCADA. Пару дней спустя группа Clop обновила информацию на своем сайте. По новым сведениям, атакована была South Staffordshire PLC, а не Thames Water.

DESFA

Крупнейшая газотранспортная компания Греции DESFA подтвердила 20 августа, что она стала жертвой кибератаки, которая негативно сказалась на доступности некоторых систем, а также привела к утечке данных. По сообщению DESFA, компания превентивно отключила многие из своих ИТ-сервисов, доступных через интернет, чтобы защитить клиентские данные. Затем она приступила к постепенному восстановлению их

работоспособности. DESFA заявила, что отправила сведения об инциденте в подразделение полиции по борьбе с киберпреступлениями, национальное управление по защите данных, министерство обороны и министерство энергетики и охраны окружающей среды. Компания сделала это, чтобы разрешить инцидент с минимальными потерями времени и последствиями.

Операторы программы-вымогателя Ragnar Locker взяли на себя ответственность за атаку, заявив при этом, что украли у компании-жертвы конфиденциальные данные. Злоумышленники опубликовали на своем вымогательском сайте список якобы украденных сведений, а также небольшой набор украденных документов, по-видимому, не содержащих конфиденциальных данных. Кроме того, группа вымогателей утверждает, что обнаружила несколько уязвимостей в системах DESFA и сообщила о них газотранспортной компании — вероятно, это тоже было частью вымогательской схемы злоумышленников. Организаторы атаки не получили от DESFA ответа.

Eni

Новостной ресурс Bloomberg 31 августа сообщил об атаке на итальянский нефтяной гигант Eni. По неподтвержденным данным издания, Eni стала жертвой атаки программ-вымогателей.

Eni подтвердила вторжение злоумышленников в её корпоративную сеть. По сообщению представителя компании, благодаря оперативному обнаружению вторжение имело незначительные последствия. Компания уведомила об инциденте итальянские власти, которые начали расследование, чтобы определить масштаб атаки.

Сама компания не обнародовала никаких технических данных, и остается неизвестным, как злоумышленникам удалось взломать защиту и какие цели они преследовали.

Hensoldt

ИТ-инфраструктура производителя электроники для оборонной промышленности — компании Hensoldt Nexeya France, французской «дочки» HENSOLDT AG, — пала жертвой кибератаки. По сведениям Hensoldt, злоумышленники, вероятно, получили доступ к значительным объемам данных. Часть систем была зашифрована. Hensoldt начала комплексное расследование инцидента в тесном сотрудничестве с властями. По сведениям компании, инцидент не затронул ИТ-инфраструктуру и данные других компаний, входящих в холдинг Hensoldt Group.

Elbit Systems

Elbit Systems of America, дочерняя компания израильского оборонного подрядчика Elbit Systems, подтвердила факт вторжения через несколько месяцев после того, как группа вымогателей заявила о взломе систем компании. В уведомлении о вторжении, поданном в управление генерального прокурора штата Мэн, компания заявила, что вторжение произошло 8 июня и было обнаружено в тот же день. В соответствии с тем же уведомлением, затронуты данные только 369 сотрудников компании, включая их имена, адреса, даты рождения, данные о прямом депозите, национальность и номера социального страхования (Social Security numbers). Компания раскрыла минимум информации об инциденте, сообщив лишь, что «кто-то пытался нарушить киберпроцессы Elbit America» и что расследование продолжается.

Группа вымогателей Black Basta объявила, что это она взломала системы Elbit Systems of America в конце июня. По сведениям с сайта в сети Tor, который группа использует для размещения информации об утечках, все украденные у Elbit файлы выложены в публичный доступ.

Läderach

Швейцарский производитель шоколада Läderach пострадал от кибератаки. Согласно заявлению компании, опубликованном 6 сентября, атака была обнаружена утром 5 сентября; она затронула производство, логистику и административные функции Läderach. Примерно за две недели компании удалось почти полностью возобновить работу.

Портал новостей из сферы информационных технологий Inside-IT обнаружил в дарквебе несколько пакетов данных из сети Läderach, загруженных группой вымогателей Bianlian. По словам киберпреступников, это файлы, относящиеся к бизнесу компании, такие как управленческая документация, сведения о развитии продуктов и перспективных проектах, бюджетном планировании и аналитике, а также технические документы. На момент публикации представитель Läderach не смог подтвердить валидность данных, загруженных на ресурс злоумышленников, и заявил, что компания «будет продолжать отслеживать ситуацию вместе с представителями соответствующих ведомств — и при необходимости снова информировать всех, кого затронул инцидент».

Tata Power

Крупнейшая энергетическая компания Индии Tata Power Company Limited 14 октября подтвердила, что подверглась кибератаке, которая затронула ее ИТ-инфраструктуру. Компания сообщила, что все необходимые меры по восстановлению систем уже приняты, и все критически важные системы функционируют. Кроме того, в качестве меры предосторожности для предотвращения несанкционированного доступа были реализованы ограничения доступа и профилактические проверки сотрудников и клиентов при работе с порталами компании.

Расположенная в Мумбае электроэнергетическая компания, входящая в состав конгломерата Tata Group, не опубликовала никаких сведений о характере или времени атаки.

Группа вымогателей Hive взяла на себя ответственность за атаку. Хакеры из группы Hive утверждают, что зашифровали системы Tata Power 3 октября. Сообщение об атаке появилось на сайте группы в дарквебе 24 октября. Хакеры загрузили на свой ресурс примеры украденных файлов, включая договоры о найме, договоры с поставщиками, личные дела сотрудников, документы о компенсационных пакетах руководства и другие сведения.

Немецкое газетное издательство

Атака программ-вымогателей привела к отключению систем, используемых для печати нескольких немецких газет. Атака нарушила работу медийного холдинга, выпускающего такие издания как Heilbronner Stimme, Pressedruck, Echo и RegioMail.

Главный редактор Heilbronner Stimme заявил, что атака — дело рук известной киберпреступной группы, которая зашифровала системы издательства вечером 14 октября, оставив записки с требованиями о выкупе. Была создана антикризисная команда, и эксперты по кибербезопасности приступили к расследованию инцидента. В расследовании также приняли участие представители полиции и министерства внутренних дел.

U-blox

U-blox — швейцарская компания, создающая беспроводные микросхемы и модули для потребительского рынка, автомобильной промышленности и других промышленных отраслей, –28 октября сообщила, что она подверглась атаке вредоносных программ-вымогателей, которая была обнаружена и заблокирована 24 октября.

Атака вызвала сбои в нескольких внутренних ИТ-системах. Компания заявила, что ни клиентские данные, ни интеллектуальная собственность не были скомпрометированы, производство не пострадало, и восстановление идет полным ходом. Кибератака сказалась на доступности системы ERP (планирования ресурсов предприятия), что могло послужить причиной задержки отгрузок.

Компания привлекла внешних экспертов по кибербезопасности для участия в проведении всестороннего криминалистического анализа инцидента. Чтобы обеспечить дальнейшее снижение уровня риска для клиентов, сотрудников и компании в целом, собственные и внешние эксперты подготовили планы обеспечения безопасности и минимизации риска. Кроме того, компания заручилась поддержкой местных властей, чтобы обеспечить дальнейшее расследование атаки и наказание виновных.

Richard Wolf

Производитель медицинского оборудования Richard Wolf подвергся кибератаке в начале ноября. Согласно пресс-релизу компании, ее данные были зашифрованы. Почти через три недели после инцидента компания заявила, что почти все ограничения на использование телефонных сервисов и почтовых аккаунтов сняты. Ожидалось, что к концу недели будет завершена работа по восстановлению работоспособности ИТ-систем компании.

Компания привлекла внешних экспертов по компьютерной криминалистике для обеспечения кибербезопасности своих систем. По заявлению Richard Wolf, компания в последние годы готовилась именно к такому сценарию: принимала технические и организационные меры, нанимала профильных специалистов, проводила тренинги для своего персонала и задействовала внешних консультантов. После атаки были немедленно проинформированы все компетентные органы, поставщики, крупные клиенты и персонал. Компания не ответила на требования о выкупе.

Uponor

Финский производитель сантехнического оборудования Uponor объявил в пресс-релизе, что стал жертвой атаки программ-вымогателей, обнаруженной 5 ноября. Расследование показало, что результатом атаки стала также кража данных, относящихся к сотрудникам, клиентам и партнерам Uponor. По сведениям Uponor, украденные данные не опубликованы на общедоступных ресурсах.

Сразу же после атаки компания приняла меры по расследованию и исправлению ситуации. В частности, в качестве меры предосторожности были отключены все системы и производственные мощности компании. Через неделю после отключения систем началось их возвращение к нормальному функционированию, и в течение недели поставки были возобновлены всеми подразделениями компании. После этого Uponor поставила перед собой задачу вернуть производительность к уровням, предшествующим атаке, обеспечив при этом защиту систем компании.

Maple Leaf Foods

Канадский производитель продуктов питания Maple Leaf Foods 6 ноября опубликовал заявление о том, что у него произошел сбой в работе систем в связи с инцидентом кибербезопасности. Компания сообщила, что ввела в действие планы по обеспечению бесперебойной работы и работает над восстановлением затронутых инцидентом систем. Ожидалось, что полное восстановление работоспособности систем потребует времени и будет сопровождаться некоторыми сбоями в функционировании систем и сервисов. После публикации этого заявления группа вымогателей Black Basta взяла на себя ответственность за атаку и упомянула Maple Leaf Foods как одну из своих жертв. Группа опубликовала несколько скриншотов технических документов, финансовых сведений и других корпоративных файлов, чтобы показать, что она действительно получила доступ к системам Maple Leaf Foods.

Sargent & Lundy

Sargent & Lundy — чикагская строительная и инжиниринговая фирма, спроектировавшая сотни электростанций в США, подверглась кибератаке. В результате вторжения, произошедшего 15 октября, злоумышленники украли из систем компании персональные данные. По сведениям Turke & Strauss — юридической фирмы, которая опубликовала 8 декабря от имени компании уведомление о вторжении, — утечке, возможно, подверглись имена и номера социального страхования более чем 6 900 физических лиц. Согласно документу с описанием взлома, который есть в распоряжении CNN, участники расследования внимательно отслеживали форумы в даркнете на предмет украденных в ходе атаки данных и атрибутировали атаку группе вымогателей Black Basta.

JAKKS Pacific

Американский производитель игрушек JAKKS Pacific 8 декабря был атакован программами-вымогателями, которые зашифровали его серверы. Компания наняла экспертов по кибербезопасности для реагирования на инцидент и восстановления серверов. Также компания в середине декабря подала документы, подтверждающие факт инцидента, в Комиссию США по ценным бумагам и биржам. Согласно заявлению компании, среди данных, к которым злоумышленники незаконно получили доступ, может присутствовать личная информация (включая имена, электронные адреса, почтовые адреса, индивидуальные номера налогоплательщиков, а также банковские реквизиты физических и юридических лиц).

Две разных группы вымогателей — Hive и BlackCat — взяли на себя ответственность за атаку и опубликовали данные, украденные у JAKKS Pacific. Hive была первой — она опубликовала краденные сведения 19 декабря. BlackCat последовала ее примеру 28 декабря, опубликовав скриншоты с информацией на своем сайте для украденных данных. Представитель группы вымогателей Hive сообщил DataBreaches, что обе группы купили доступ к сети компании у брокера первоначального доступа и договорились поделить выкуп в размере 5 миллионов долларов, однако компания отказалась платить выкуп и не пошла на переговоры.

Fruttagel

Итальянский производитель продуктов питания и напитков Fruttagel подвергся кибератаке 11 декабря. В результате атаки были частично скомпрометированы информационные системы компании.

Согласно заявлению компании, опубликованному местной газетой, Fruttagel немедленно задействовала все предусмотренные чрезвычайные меры, используя экспертные знания как собственных сотрудников, так и внешних специалистов по кибербезопасности. Однако компании не удалось избежать серьезных сбоев в производственном процессе и, как следствие, временной невозможности отгружать продукцию потребителям.

После публикации заявления компании группа вымогателей BlackCat/ALPHV добавила Fruttagel к своему списку жертв, утверждая при этом, что имеет доступ к 720 ГБ корпоративных данных, включая финансовую информацию, контракты и значительные объемы других данных.

EPM

В декабре колумбийская коммунальная компания Empresas Públicas de Medellín (EPM) подверглась атаке программ-вымогателей, которая нарушила работу компании и привела к отключению ее онлайн-сервисов. Сотрудники получили указание работать дома, поскольку ИТ-системы компании потеряли работоспособность.

Группа вымогателей BlackCat, известная также под именем ALPHV, взяла на себя ответственность за эту атаку. После обнаружения чилийским исследователем безопасности нового образца созданного BlackCat инструмента кражи данных ExMatter, который был загружен из Колумбии на сайт для анализа вредоносных образцов, были найдены новые свидетельства того, что хакеры, вероятно, украли во время атаки на EPM достаточно большой объем данных.

Вариант ExMatter, загруженный на сервер из Колумбии, отправлял данные на незащищенный удаленный сервер, на котором файлы хранились в папках с различными именами, начинающимися с «EPM-». Это имена компьютеров, соответствующие схеме именования компьютеров, используемой Empresas Públicas de Medellín.

Thyssenkrupp

Немецкий производитель промышленных систем и стали Thyssenkrupp пострадал от кибератаки. Служба безопасности компании обнаружила инцидент на раннем этапе, и злоумышленникам не удалось нанести значительный урон. Атака затронула лишь некоторые сегменты ИТ-инфраструктуры ThyssenKrupp, включая подразделение Materials Services и штаб-квартиру компании. Компания не нашла никаких улик, указывающих на то, что ее данные были украдены или изменены. Возможность того, что другие сегменты и подразделения затронуты атакой, также исключена.

Компания оперативно создала антикризисную команду для расследования инцидента и ликвидации его последствий. Представители Thyssenkrupp сообщили журналистам, что за атакой стоит организованная преступность, но не уточнили, была ли это атака вредоносных программ-вымогателей. Тем не менее, все указывает именно на такой тип атаки, поскольку за последние несколько лет Thyssenkrupp несколько раз подвергалась атакам групп вымогателей, включая Netwalker.

CMMC

Компания Canadian Copper Mountain Mining Corporation (CMMC) объявила, что подверглась атаке программ-вымогателей, которая произошла вечером 27 декабря. ИТ-команда компании оперативно отреагировала на инцидент, введя в действие заранее определенные системы управления рисками и протоколы. Чтобы локализовать инцидент, CMMC изолировала зараженные системы, чтобы внимательно изучить их и определить ущерб от атаки вымогателей. Инженеры CMMC были вынуждены в качестве превентивной меры остановить завод, чтобы оценить состояние его системы управления, а другие процессы были переведены на ручное управление.

Согласно заявлению, в процессе расследования инцидента CMMC стремилась найти источник атаки, работая в контакте с компетентными органами. В заявлении уточняется, что инцидент кибербезопасности не поставил под удар меры обеспечения функциональной безопасности и не вызвал никакого ущерба для окружающей среды. Компания рассматривала в качестве главных приоритетов скорейшее возвращение к нормальной работе и минимизацию финансового ущерба от инцидента.

Лиссабонский порт

Лиссабонский порт стал мишенью кибератаки 25 декабря. В соответствии с заявлением, опубликованным в местной газете, атака не повлияла на операционную деятельность порта. Все протоколы безопасности и меры реагирования, запланированные на случай подобных ситуаций, были оперативно введены в действие; при этом ситуацию отслеживали Национальный центр кибербезопасности и уголовная полиция. Сайт компании на момент публикации заявления был недоступен.

29 декабря группа вымогателей LockBit подтвердила, что осуществила атаку на порт, подтвердив кражу финансовых и аудиторских отчетов, бюджетных сведений, договоров, судовых журналов и других сведений о грузах и судовых командах судов. Группа пообещала опубликовать все украденные в ходе атаки файлы, если их требования о выплате выкупа в размере полутора миллионов долларов не будут выполнены.

MOL

Бельгийский автопроизводитель и поставщик запчастей MOL Cy подвергся кибератаке. Согласно короткому сообщению на сайте компании, она сразу же сообщила об инциденте компетентным органам. Было также решено немедленно прибегнуть к помощи специализированной внешней компании. В

сообщении говорится, что «масштабы атаки теперь известны, и команда делает все возможное для скорейшего возврата к нормальной работе» и «с компанией снова можно связаться по телефону, а электронная почта тоже заработает в ближайшее время». Группа вымогателей Royal разместила информацию о компании и украденные у нее файлы на своем сайте для краденных данных в сети Tor.

Sumitomo Bakelite North America

Sumitomo Bakelite North America — американская «дочка» японского производителя пластика — сообщила в официальном заявлении, что стала жертвой кибератаки. Компания оперативно сообщила об инциденте американским компетентным органам и организовала расследование с целью выяснить подробности атаки и масштабы ее последствий.

Дочерняя компания в США в полной мере сотрудничает с компетентными органами страны в связи с данным инцидентом. Компанией уже были приняты меры безопасности, однако по следам данного инцидента она пересмотрит и усилит свои существующие политики, связанные с защитой и обеспечением безопасности.

Ответственность за атаку взяла на себя группа вымогателей BlackCat/ALPHV.

Бюллетени CISA

Атаки вымогателей Zeppelin

Федеральное бюро расследований (ФБР) и Агентство по кибербезопасности и безопасности инфраструктуры США (Cybersecurity and Infrastructure Security Agency, CISA) выпустили совместный Бюллетень кибербезопасности для распространения известных индикаторов компрометации и сведений о тактиках, техниках и процедурах группы вымогателей Zeppelin, связанных с вариантами вредоносных программ-вымогателей, обнаруженных в процессе проведения расследований ФБР, последнее из которых датируется 21 июня 2022 года.

Вредоносная программа-вымогатель Zeppelin «выросла» из написанного на Delphi семейства вредоносного ПО Vega и работает по схеме «вымогатели как сервис» (Ransomware as a Service, RaaS). С 2019 года по как минимум июнь 2022 года злоумышленники использовали это вредоносное ПО для атак на широкий круг компаний и организаций критической информационной инфраструктуры, включая оборонных подрядчиков, образовательные

учреждения, производственные и технологические компании и, в особенности, организации здравоохранения и медицины.

Операторы Zeppelin получают доступ к сетям жертв, используя уязвимости в RDP, уязвимости в сетевых экранах SonicWall и фишинговые рассылки. До развертывания программ-вымогателей Zeppelin злоумышленники тратят одну-две недели на построение карты или схемы сети жертвы, выявляя места хранения данных, включая облачные хранилища и сетевые резервные копии. Прежде чем приступить к шифрованию, злоумышленники, использующие Zeppelin, сливают файлы с конфиденциальными данными компании, чтобы иметь возможность продать или опубликовать данные в случае если жертва откажется платить выкуп.

Атаки группы вымогателей Hive

CISA (Агентство по кибербезопасности и безопасности инфраструктуры США) совместно с ФБР (Федеральным бюро расследований) и министерством здравоохранения США (Department of Health and Human Services, HHS) опубликовали совместный бюллетень безопасности об атаках группы вымогателей Hive на организации из широкого круга инфраструктурных секторов, включая государственные предприятия, телекоммуникации, сектор критически важного производства, информационные технологии и, в особенности, здравоохранение.

В бюллетене представлены известные индикаторы компрометации и тактики, техники и процедуры группы Hive, выявленные в результате расследований ФБР в период до ноября 2022 года. Сообщается, что группа вымогателей Hive получила более 100 миллионов долларов США в качестве выкупа от атакованных организаций.

Используемые группой методы первоначального вторжения включают однофакторный вход в систему через RDP, VPN и другие протоколы удаленного подключения. В некоторых случаях злоумышленникам из группы Hive удавалось обойти многофакторную аутентификацию и получить доступ к серверам FortiOS благодаря использованию уязвимости CVE-2020-12812. Эта уязвимость позволяет злоумышленнику войти в систему, не получая запроса на второй фактор аутентификации (FortiToken) при изменении регистра написания имени пользователя. Кроме того, злоумышленники из группы Hive получали первоначальный доступ к сетям жертв с помощью фишинговых рассылок с вредоносными вложениями и с использованием трех уязвимостей в серверах Microsoft Exchange.

Вымогатели Cuba

CISA (Агентство по кибербезопасности и безопасности инфраструктуры США) опубликовало совместно с ФБР (Федеральным бюро расследований) бюллетень безопасности, содержащий известные индикаторы компрометации вредоносных программ-вымогателей, а также тактики, техники и процедуры группы вымогателей Cuba, выявленные в ходе расследований ФБР, представленные в сторонних отчетах и отчетах из открытых источников. Основными целями атак вымогателей Cuba являются следующие секторы: финансовые сервисы, государственные органы, здравоохранение, критически важное производство и информационные технологии.

Злоумышленники использовали для получения доступа известные уязвимости (CVE-2022-24521, CVE-2020-1472), фишинговые рассылки, скрипты PowerShell, инструмент KerberCache, скомпрометированные учетные данные и RDP, а затем применяли загрузчик Hancitor для развертывания вредоносных программ-вымогателей.

Другие кибератаки и случаи кражи данных

Weidmüller

Немецкий производитель электроники Weidmüller стал жертвой кибератаки, которая была обнаружена 18 июля. Согласно пресс-релизу компании, Weidmüller, используя свои технические возможности, изолировала все системы, чтобы провести детальный анализ, а также защитить своих клиентов, партнеров и сотрудников. Важнейшие каналы внутренней и внешней коммуникации, а также системы SAP не были затронуты атакой; производство почти не пострадало. Работоспособность практически всех систем удалось восстановить.

Hettich Group

Китайская производственная компания, входящая в состав холдинга по производству мебельной фурнитуры Hettich, пала жертвой кибератаки. ИТ-специалисты группы компаний Hettich при поддержке внешних экспертов приняли меры для отражения атаки и реализации дополнительных мер безопасности для защиты систем компании. В опубликованном 15 августа пресс-релизе компания затруднилась сообщить, когда ее китайская дочерняя компания снова сможет использовать свои ИТ-системы в полном объеме, но заявила, что производство на китайском заводе не будет остановлено. По информации холдинга, атака не затронула другие компании группы Hettich.

Sembcorp Marine

Кораблестроительная и инжиниринговая компания Sembcorp Marine обнаружила инцидент кибербезопасности: неавторизованные злоумышленники получили доступ к части ИТ-сети компании с помощью стороннего программного обеспечения. Компании удалось установить, что были скомпрометированы персональные данные её новых, существующих и бывших сотрудников, а также не являющаяся критически важной информация об операционной деятельности компании. Sembcorp Marine привлекла экспертов по кибербезопасности для проведения детального анализа инцидента с целью ликвидировать все последствия компрометации, а также ее причины, оценить последствия атаки, пересмотреть и усилить меры безопасности. Компания подтвердила, что уведомила компетентные органы Сингапура об инциденте и тесно взаимодействует с ними в этой связи.

Continental

Производитель автомобильных запчастей и шин Continental подвергся кибератаке, которая была обнаружена в начале августа. В опубликованном 24 августа заявлении Continental утверждает, что его деловая активность не была затронута ни на каком этапе, что компания сохраняет полный контроль над своими ИТ-системами, и что ИТ-системы сторонних организаций также не затронуты атакой. Компания провела расследование инцидента при поддержке сторонних экспертов по кибербезопасности.

Eurocell

Eurocell, британский производитель НПВХ, стал жертвой кибератаки, которая привела к утечке конфиденциальных личных данных сотрудников компании, включая банковские реквизиты, даты рождения, сведения о родственниках, номера социального страхования и сведения о налогообложении, информацию о состоянии здоровье, дисциплинарных взысканиях, если они были, жалобы на сотрудников и т.п. Компания разослала сотрудникам письмо, в котором объясняется, что неавторизованные третьи лица получили доступ к системам компании в результате инцидента ИТ-безопасности. Eurocell утверждала, что «нет оснований» считать, что эти данные используются не по назначению, однако нет никаких гарантий, что это так и останется в дальнейшем. Компания отметила, что уведомила об инциденте Управление комиссара по информации и полицию.

Enercity

Компания Enercity — один из крупнейших муниципальных поставщиков энергии Германии — подтвердила, что подверглась кибератаке 26 октября. По заявлению Enercity, системы безопасности сработали мгновенно и предотвратили нанесение компании более значительного ущерба. Компания подтвердила, что продолжает поставлять энергию клиентам, объяснив, что технологические системы и критическая информационная инфраструктура не затронуты атакой. При этом от атаки пострадали клиентские сервисы, которые не были доступны в полном объеме.

Aurubis

Aurubis, крупнейший в Европе производитель и переработчик меди, опубликовал заявление, в котором сообщил о кибератаке, произошедшей 28 октября. Инцидент не привел к останову производства, но послужил причиной временного отключения многих систем на площадках компании. В качестве превентивной меры Aurubis полностью отключил свои ИТ-системы, однако плавильные печи по всей Европе и другие производственные системы продолжали работать. Специалисты компании организовали расследование атаки совместно с властями. По заявлению компании, этот инцидент, по-видимому, был частью более широкой атаки на предприятия металлообрабатывающей и горнодобывающей промышленности.

Eesti Energia

В ноябре веб-сайт и онлайн-каналы эстонской государственной электрогенерирующей компании Eesti Energia и некоторых связанных с ней компаний оказались недоступны вследствие масштабной DoS-атаки. Результатом атаки стала неработоспособность сайта и мобильного приложения Eesti Energia, сайта компании Enefit Green, а также сайта компании Elektrilevi, отвечающей за содержание электрических сетей, и ее мобильного приложения MARU. Бизнес- и ИТ-директор Eesti Energia заявил, что клиентские данные и ИТ-системы группы компаний полностью защищены, и атака была успешно отражена.

Iochpe-Maxion

Бразильский производитель автомобильных компонентов Iochpe-Maxion сообщил, что его ИТ-системы подверглись кибератаке 5 декабря. Атака привела к недоступности части систем компании в некоторых подразделениях компании как в Бразилии, так и за рубежом. Компания

заявила в письме, отправленном в Комиссию по ценным бумагам Бразилии, что немедленно привела в действие свои протоколы безопасности, чтобы заблокировать кибератаку, а также превентивно изолировала часть своих систем с целью защиты окружающей среды. По заявлению компании, она и привлеченные ею консультанты прилагают все усилия для определения причин и масштабов инцидента и минимизации его последствий.

Meyer&Meyer

Немецкая логистическая и транспортная компания Meyer&Meyer пала жертвой кибератаки 6 декабря. Согласно заявлению компании, преступный акт отразился на деловой активности компании, которая, несмотря на отключение систем, сумела частично продолжить операционную деятельность после кибератаки, перейдя на ручное управление процессами. Компания отреагировала на целенаправленную атаку быстро и решительно, изолировав свои ИТ-системы. Она немедленно проинформировала своих сотрудников и бизнес-партнеров об инциденте и работала в тесном сотрудничестве с правоохранительными органами и органами, ответственными за защиту информации.

NIO Inc

Китайский производитель электромобилей Nio Inc объявил 20 декабря, что хакеры взломали его компьютерные системы и получили доступ к данным по клиентам и продажам автомобилей. По сообщениям в прессе, хакеры отправили производителю электрокаров электронное письмо с требованием выкупа в биткоинах на сумму 2,25 миллиона долларов и угрозой опубликовать конфиденциальные данные в случае отказа от оплаты. Компания заявила, что расследует утечку данных совместно с правоохранительными органами.

Хактивисты

Атаки GhostSec на ПЛК Berghof

Исследователи компании OTORIO опубликовали отчет, содержащий сведения об атаке на промышленные системы управления. 4 сентября 2022 года группа хактивистов GhostSec, ранее замеченная в атаках на израильские организации и платформы, объявила в социальных сетях и в своем Telegram-канале, что ей удалось взломать 55 устройств ПЛК Berghof в Израиле. В опубликованном сообщении группа GhostSec представила

видеоролик, демонстрирующий успешный вход в панель управления ПЛК, а также снимок экрана HMI, показывающий текущий статус управления ПЛК и еще одно изображение, на котором видно, что ПЛК остановлен.

Исследователи решили изучить детали этого инцидента, чтобы понять, каким образом GhostSec удалось перехватить управление ПЛК, и оценить соответствующие риски. Во время исследования IP-адреса ПЛК были по-прежнему доступны через интернет, и доступ к панели администрирования был защищен паролем. Однако при попытке использовать установленные по умолчанию и часто используемые учетные данные исследователям удалось войти в систему. Несмотря на то, что доступ к панели управления дает полный контроль над некоторыми функциями ПЛК, он не позволяет напрямую управлять технологическим процессом. Исследователи также выяснили, что Berghof использует в системах человеко-машинного интерфейса (HMI) технологию CODESYS, причем доступ к HMI возможен по определенному адресу через браузер. Исследователи не смогли выяснить, удалось ли GhostSec получить доступ к HMI, но они подтвердили, что экран HMI доступен через интернет.

Тот факт, что GhostSec, судя по всему, не получили доступ к интерфейсу HMI и не пытались в нем ничего изменить, а также не вмешивались в работу интерфейса Modbus, показывает, что они не знакомы с устройством технологических систем. Нет оснований полагать, что представители GhostSec нанесли какой-либо значительный ущерб системам, к которым они получили доступ. По всей видимости, они лишь пытались привлечь внимание к группе хактивистов и ее деятельности.

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