Kaspersky ICS CERT

kaspersky

Первое полугодие 2022 — краткий обзор основных событий из мира промышленной кибербезопасности

08.09.2022

Version 1.0

С первых месяцев 2022 года новости, появляющиеся в средствах массовой информации, буквально соревнуются друг с другом по накалу страстей и порой добавляют по нескольку седых волос своим читателям или слушателям. Новостные ленты, посвященные событиям из мира кибербезопасности (в том числе и промышленной), в первом полугодии 2022 также были весьма насыщенными.

- Геополитическая ситуация спровоцировала рост активности хактивистов, причем помимо государственных учреждений и СМИ досталось и некоторым промышленным компаниям.

- Ничто не останавливает злоумышленников, которых интересует исключительно нажива. Вымогатели активны и гребут широко, жертвами их атак стали представители разных отраслей в разных регионах мира — производители автомобилей; компании, которые относятся к сфере возобновляемой энергии; производители электроники и нефтедобывающая компания. Разумеется, в этом обзоре приведен далеко не полный список их жертв.

- APT по-прежнему шпионят, и интересует их не только политика, но и технологии.

- Техники, тактики и сценарии атак совершенствуются злоумышленниками. Появление нового вредоносного ПО, нацеленного на промышленные компании, — весьма опасная тенденция.

Калейдоскоп событий первого полугодия 2022 не давал скучать специалистам по промышленной кибербезопасности многих стран. Посмотрим на наиболее яркие «картинки» из этого калейдоскопа.

Хактивисты

Атака на Белорусскую ЖД

Активизации хактивистов в 2022 году невозможно не заметить — действуют они весьма активно. И один из первых примеров атак, совершенных таким типом злоумышленников, — январская атака на инфраструктуру Белорусской Железной Дороги. В результате атаки было зашифровано множество систем БЖД. За расшифровку данных атакующие требовали от правительства Беларуси перестать оказывать помощь российским военным. Ответственность за атаку взяла на себя группа под названием «Кибер Партизаны».

Атака на станции зарядки электроавтомобилей в России

Некоторые атаки хактивистов были вызваны геополитическими событиями, начавшимися 24 февраля. Один из примеров — атака на станции зарядки электроавтомобилей в России. На трассе М11 станции зарядки электроавтомобилей были деактивированы, а на экранах выводились политические лозунги. Как выяснилось, разработка этих станций была отдана на аутсорс в компанию, которая расположена в Харькове. Россети быстро отреагировали и заменили прошивку станций зарядки.

Атака на Rosneft Deutschland

В середине марта немецкая «дочка» Роснефти (Rosneft Deutschland GmbH) также подверглась кибератаке. В опубликованном заявлении Группа Anonymous сообщила, что стоит за этой атакой. Злоумышленники утверждали, что у Rosneft Deutschland было похищено 20 Тб данных. В результате атаки также предположительно были нарушены внутренние процессы компании, а именно работа с контрактами. Согласно официальным заявлениям, других серьезных последствий не было, в том числе и развития атаки на технологический сегмент сети.

Атаки на российские компании пищевой промышленности

Агрохаб Селятино

26 февраля в агрохабе Селятино в Московской области на складе с замороженной продукцией некий пользователь под ником Supervisor проник в сеть дистанционного мониторинга работы холодильных устройств и

изменил температурный режим с -24° С на +30 градусов. На складе хранилось 40 тонн замороженного мяса и рыбы.

Холдинг Мираторг

18 марта холдинг Мираторг, один из крупнейших производителей мясной продукции в России, был атакован шифровальщиком Bitlocker. Атаке подверглись складские и бухгалтерские информационные ресурсы. Также была нарушена система обработки электронных ветеринарных сопроводительных документов. Пострадали 18 компаний, входящих в холдинг.

Россельхознадзор сообщил о восстановлении работы холдинга 28 марта. В отличие от большинства атак с использованием шифровальщиков, в данном случае нет оснований говорить о коммерческом интересе атакующих — атакующие денег не требовали.

Холдинг «Тавр»

24 марта кибератаке подверглись структуры крупнейшего продуктового холдинга «Тавр» группы «Агроком» в Ростовской области. Согласно официальному заявлению, работа компании, в том числе производство, была временно парализована, нанесен значительный экономический ущерб. Представитель холдинга оценил произошедшее как «тщательно спланированную масштабную диверсию».

Атака на иранские металлургические предприятия

В июне стало известно об атаке на иранские металлургические предприятия: Hormozgan, Khouzestan и Mobarakeh. Атака, по заявлениям атакующих и нескольких внешних экспертов, привела к нарушению производственного процесса на заводе Khouzestan. Однако сами компании отрицают, что произошел сбой или останов производства. Ответственность на себя взяла группа хактивистов Gonjeshk'e Darandeh (также известны как Indra). Эти же злоумышленники в июле 2021 года атаковали иранскую железную дорогу, что привело к огромным задержкам и нарушениям в логистике.

Вымогатели

Атаки на автомобилестроительные компании

Атака на производителя шин Bridgestone Americas

27 февраля Bridgestone Americas сообщила о начале расследования возможной компрометации IT-систем компании. Во избежание распространения вредоносного ПО были отключены компьютерные сети и остановлено производство на многих предприятиях в Латинской и Северной Америке. 11 марта стало известно, что это была атака вымогателя LockBit — злоумышленники внесли Bridgestone в список своих жертв и потребовали выкуп, угрожая в противном случае опубликовать похищенные данные.

Атака на поставщика Toyota Kojima Industries, Toyota пострадала

28 февраля компания Toyota сообщила об остановке на 24 часа 14 своих заводов в Японии из-за атаки на одного из своих поставщиков — Kojima Industries. Атакованная компания производит важнейшие детали для автомобилей, без которых все производство невозможно. Что именно произошло в Kojima Industries, не сообщалось. Один из самых вероятных сценариев — атака программы-вымогателя.

В любом случае атака на цепочку поставщиков в очередной раз вывела из строя крупную компанию и остановила производство.

Атака Pandora на производителя автомобильных комплектующих Denso

Через две недели, 13 марта, стало известно еще об одной атаке – на корпорацию Denso, второго по величине в мире производителя автомобильных комплектующих, которая считается основным поставщиком Toyota. Группа злоумышленников Pandora заявила о краже 1,4 Тб данных Denso Automotive Deutschland, Denso подтвердила «несанкционированный доступ с использованием программы вымогателя». В этот раз обошлось без влияния на производство, но объем украденных данных и наличие в них «секретных документов» вряд ли позволили Denso утешиться.

Атаки на компании, обслуживающие ветряные турбины

Атака Conti на производителя ветряных турбин Nordex

В начале апреля о кибератаке сообщила компания Nordex, один из крупнейших производителей ветряных турбин. Когда атака была

обнаружена, компания отключила IT-системы и удаленный доступ к управляемым турбинам, предотвратив дальнейшее распространение вредоносного ПО. В результате пострадала только внутренняя IT-система компании. О своей причастности к атаке заявили злоумышленники из группы Conti.

Атака Black Basta на Deutsche Windtechnik

11 апреля была атакована компания Deutsche Windtechnik, которая специализируется на техническом обслуживании ветряных турбин. Из соображений безопасности были отключены все системы и удаленные подключения для мониторинга турбин. На полное восстановление нормального режима работы потребовалось два дня. О том, что это была атака вымогателей, стало известно после того, как злоумышленники из группы Black Basta внесли компанию в список своих жертв, опубликованный на сайте в Tor.

Enercon

Хотя производитель ветряных турбин Enercon пострадал не от атаки вымогателей (см. ниже часть про APT) и был задет «рикошетом», упомянем и его в этом списке. В феврале в результате атаки на Viasat, Enercon лишился возможности удаленного контроля и мониторинга 5800 ветряных турбин общей мощностью 11 гигаватт, доступ к которым осуществлялся по спутниковой связи. По заявлениям представителя компании, угрозы безопасности систем не было: турбины работают в автоматическом режиме и в случае возникновения проблем выключаются. Однако в результате инцидента пострадало используемое IT-оборудование, которое компании пришлось менять.

Атака Conti на производителя закусок KP Snacks

В начале февраля стало известно, что группа Conti атаковала крупного британского производителя закусок KP Snacks. Как уже стало привычным для атак вымогателей, данные жертвы не только были зашифрованы, но и похищены. Часть данных была опубликована, чтобы подтвердить кражу и, таким образом, повысить шансы на выплаты со стороны атакованной компании.

Атака Lapsus$ на производителя чипов и видеокарт Nvidia

В начале марта производитель чипов и видеокарт Nvidia подвергся кибератаке, в результате которой, вероятно, было похищено до 1 Тб данных.

Изначально сама компания признала факт компрометации систем, но заявила, что ничего не было зашифровано. Впоследствии группа Lapsus$ взяла на себя ответственность за эту атаку. Кроме того, эта группа опубликовала в открытом доступе учетные данные сотрудников Nvidia. Такие публикации обычно ведут к волне фишинга, таргетированного фишинга, всплеску брутфорс атак и других попыток совершить проникновение в инфраструктуру пострадавшей компании другими группами злоумышленников.

Атака REvil на Oil India

В апреле индийская компания Oil India подверглась атаке шифровальщиком, предположительно REvil. Пострадали IT-системы, компьютеры в головном офисе компании были отключены. На системы, связанные с добычей и бурением, атака не повлияла. Злоумышленники затребовали выкуп — $7,5 миллионов. По результатам расследования высокопоставленный сотрудник индийской полиции заявил, что компания была атакована «русским вредоносным ПО», попавшим в системы компании с сервера в Нигерии.

Об атаке стало известно 14 апреля. 20 апреля на bleepingcomputer появилась информация о том, что «ожил» REvil — на RUTor предлагается новая, улучшенная, версия вредоносной программы, а список жертв REvil на их сайте пополнился двумя новыми компаниями. Одна из них — Oil India.

Атака LockBit на производителя электроники Foxconn

В конце мая 2022 года компания Foxconn, крупный производитель электроники, была атакована вымогательским зловредом. В 2020 году Foxconn уже заявляла об атаке вымогателем DoppelPaymer, тогда атакующие заявили, что украли до 100 Гб данных, удалили 20-30 Тб данных резервных копий и зашифровали около 1200 серверов.

На этот раз пострадал один из заводов Foxconn в Мексике, в результате были нарушены бизнес-процессы компании. Foxconn не сообщала, какой именно вымогатель атаковал компанию. Однако злоумышленники из группы LockBit внесли ясность в этот вопрос — они пригрозили опубликовать похищенную у Foxconn информацию, если компания не заплатит выкуп.

APT

Атаки на объекты возобновляемой энергии

В январе была опубликована информация о кампании кибершпионажа, которая началась как минимум в 2019 году. Среди атакованных — такие известные компании как Schneider Electric и Honeywell, а также китайский телекоммуникационный гигант Huawei, производитель полупроводников HiSilicon, Telekom Romania. Однако исследователи полагают, что атакующих особенно интересуют различные компании и организации, работающие в областях, связанных с возобновляемой энергией.

Интересный факт — атакующие пользовались услугами хостинга Zetta Hosting Solutions (AS44476), услугами которого пользовались две APT группы –- Fancy Bears и Konni (предположительно из Северной Кореи).

Атака на системы Viasat и нарушение работы ветрогенераторов

Первые новости об атаке на телекоммуникационные спутники связи высокой пропускной способности KA-SAT стали появляться 28 февраля. Как стало известно позже, эта атака произошла 24 февраля и была направлена против систем Viasat — одного из крупнейших операторов коммерческих спутников. В заявлении компании говорилось, что произошел частичный сбой сети, который повлиял на доступ в интернет в Украине и других странах в европейской сети KA-SAT.

Атака имела и неожиданный результат — из-за сбоя работы в сетях KA-SAT около 5800 ветрогенераторов общей мощностью 11 гигаватт остались без удаленного мониторинга и контроля со стороны немецкой компании Enercon. М ы упоминали этот инцидент выше, рассказывая о пострадавших компаниях, которые производят и/или обсуживают ветряные турбины.

Растущая угроза атак Turla и Curious Gorge

В мае команда аналитиков из Google Threat Analysis Group выпустила отчет о растущих угрозах в восточной Европе, исходящих от Turla в связи с февральскими событиями. Turla — предположительно русскоязычная группа, действующая примерно с 2008 года. Целью Turla является кража данных у государственных и правительственных организаций, организаций, входящих в ВПК, и организаций, связанных с кибербезопасностью.

Также аналитики Google Threat Analysis Group отмечают рост угроз со стороны группы Curious Gorge. Это предположительно китайско-говорящая

группа, которая относится к Силам Стратегического Обеспечения КНР. Целями группы являются правительственные, военные, логистические и производственные организации в России, Украине и центральной Азии.

Атака на немецких производителей автомобилей

Команда Check Point опубликовала отчет о вредоносной кампании, которая длится уже год и направлена против немецких компаний, связанных с производством автомобилей. Примечательно, что атаки проводились с использованием популярных вредоносных продуктов, работающих по принципу Malware-as-a-Service, таких как AZORult, BitRat и Racoon Stealer.

Атака на энергосети Индии с использованием бэкдора ShadowPad

Энергосети Индии были атакованы с использованием бэкдора ShadowPad. Целью атаки является либо сбор информации, либо подготовка к дальнейшему заражению и распространению внутри сетей жертвы. Изначально атаку приписывали группе RedEcho, но не было никаких технических доказательств, которые бы это доказывали. Пока нет таких доказательств, атакующим присвоили временное название TAG-38.

Атаки на системы АСУ с помощью ShadowPad

Еще одну волну атак с использованием ShadowPad исследовала команда Kaspersky ICS CERT. Вредоносные артефакты были найдены в организациях, работающих в секторах промышленного производства и телекоммуникаций в Пакистане и Афганистане. Кроме того, атака с применением более раннего, но очень похожего набора тактик, методов и процедур (TTP), проводилась на логистическую и транспортную организацию (порт) в Малайзии. Обнаруженная волна атак началась, по-видимому, в марте 2021 года, результаты исследования опубликованы в июне.

Среди систем, атакованных в рамках этой кампании, обнаружились системы автоматизации зданий, которые могут быть ценным источником строго конфиденциальной информации. Не исключено, что атакующие могут использовать их для доступа к другой, более тщательно охраняемой инфраструктуре.

TTP — тактики, методы и процедуры атак

Предупреждение ФБР об атаках с использованием рассылаемых по почте зараженных USB-носителей

Предупреждение об атаках с использованием USB носителей ФБР опубликовало в январе. Зараженные USB носители, отправляемые от имени Министерства Здравоохранения США и в подарочных посылках якобы от Amazon, были нацелены на компании, связанные с логистикой, страхованием и компании, имеющие отношение к ВПК. Предположительно за атаками стоит небезызвестная группа FIN7. Как правило, ее активность направлена на получение финансовой выгоды.

Распространение зараженных USB-носителей — довольно необычный вектор атаки на фоне классических методов проникновения (фишинг, спам, взлом инфраструктуры периметра и т.д.). Подключение к компьютеру жертвы зараженного съемного носителя позволяет атакующим получить первичный доступ и далее продолжить атаку внутри сети.

Вредоносное ПО, предназначенное для атак на системы промышленной автоматизации

Industroyer 2.0

Зловред, обнаруженный специалистами Eset в апреле, предназначен для атак по 104 протоколу (IEC 60870-5-104). Industroyer 2.0, также как и его первый вариант, нацелен на энергосистемы Украины. Однако на момент публикации (12 апреля 2022) исследователи так и не выяснили, как именно Industroyer 2.0 проникал в атакуемые системы.

Утилиты для атак на промышленное оборудование

Также в апреле 2022 вышел совместный отчет целого ряда государственных организаций США (CISA, FBI, DOE, NSA) об обнаружении набора утилит, предназначенных для атак на системы промышленной автоматизации, которые используют ПЛК Schneider Electric MODICON и MODICON Nano, ПЛК OMRON Sysmac версий NJ и NX, серверы OPC UA. Отчет не содержал никаких деталей касательно жертв и географии применения этих утилит.

Для понимая общей картины тенденций в мире информационной безопасности необходимо быть в курсе текущих событий. Kaspersky ICS CERT ежемесячно выпускает отчеты о произошедших событиях с подборкой индикаторов компрометации и собственной аналитикой там, где это возможно.

Для получения доступа ко всем отчетам вам необходимо подписаться на сервис Информирование об угрозах АСУ ТП.

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