DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.5
УДК 004.77:005.334
ББК 32.971.35

АНАЛИЗ УГРОЗ И УЯЗВИМОСТЕЙ КОНЦЕПЦИЙ IoT И IIoT

Вадим Юрьевич Шевцов

Ассистент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Никита Павлович Касимовский

Студент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. данная статья описывает концепции IoT и IIoT угрозы информационной безопасности для них. Рассмотрены концепции интернета вещей и промышленного интернета, виды возможных устройств, основные проблемы информационной безопасности. Также выделены рекомендации по защите данных технологий и приведены результаты исследований крупных компаний в данной области.

Ключевые слова: интернет вещей, промышленный интернет, ботнет, кибербезопасность, вредоносное ПО.

IoT (интернет вещей) – система взаимосвязанных компьютерных сетей и подключенных физических объектов (вещей) со встроенными сенсорами и программным обеспечением для манипуляции с данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия пользователя [2; 5].

IoT включает в себя несвязанные между собою разрозненных сетей, каждая из которых была построена для решения конкретных задач. Как пример можно привести работу современных автомобилей, в которых функционирует сразу несколько различных сетей: первая отвечает за функционирование двигателя, вторая управляет системами безопасности, третья поддерживает связь и т. д. В различных зданиях устанавливаются аналогичные сети для управления коммунальными системами, средствами безопасности и прочие. По мере развития Интернета вещей множественные сети будут объединяться и получать большие возможности в области безопасности, аналитики и управления. В итоге IoT предлагает человечеству более широкие перспективы для реализации его потенциала (см. рис. 1).

Технологии Интернета вещей:

– подключение:

– 2G/3G/4G, 5G Спутниковая (VSAT), LPWAN (LORA, LTE-M, NB IOT, NB FI и т. д.), сетевые подключения;

– оборудование:

– датчики;

– аппаратные модули защиты информации;

– серверы;

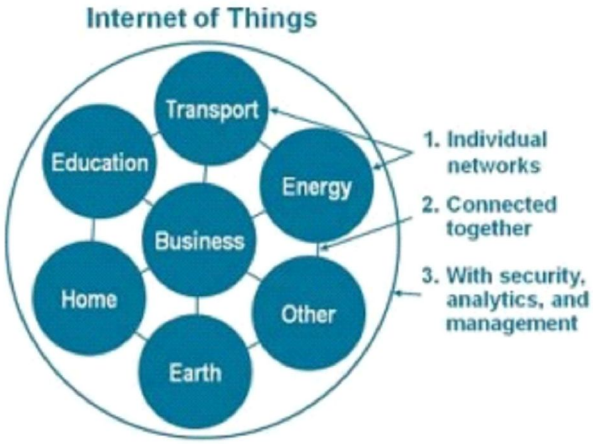

Рис. 1. Возможная схема взаимодействия различных сфер жизнедеятельности с использованием технологий интернета вещей

– СХД;
– иные устройства (специальное оборудование);
– услуги:
– системы по управлению компонентами ИВ;
– аутсорсинг инфраструктуры;
– хостинг и управление приложениями;
– информационные услуги (системная интеграция, разработка приложений) и ввод устройств;
– программное обеспечение:
– программы аналитики;
– прикладные приложения;
– кросс-индустриальные платформы;
– индустриальные платформы;
– программное обеспечение защиты информации;
– другое программное обеспечение.

Экспертное сообщество утверждает, что производители услуг и оборудования сферы IoT не выполняют принцип сквозной информационной безопасности, необходимый для информационных технологий. Исходя из этого информационная безопасность должна закладываться на исходном этапе проектирования устройства или услуги и поддерживаться вплоть до завершения их жизненного цикла.

К примеру, часть данных наблюдений компании HP (лето 2014 г.), целью которых являлось не обнаружить определенные уязвимые интернет-устройства и уличить их производителей, но актуализировать тему ИБ-рисков в сфере IoT в целом.

Эксперты HPE делают акцент на проблемах, как со стороны пользователей устройств, так и на проблемы, уделить внимание которым должны производители. Изначально пользователю необходимо произвести настройку пароля, сменив пароль разработчика, используемый по умолчанию, на стойкий, так как пароли разработчика одни и те же на разных устройствах и имеют низкую надежность. Однако далеко не каждый следует этому правилу. Поскольку не каждое устройство содержит встроенный функционал ИБ, пользователям рекомендуется произвести установку дополнительной защиты, предназначенной для личного пользования, для того чтобы интернет-устройства не превратились в открытую дверь внутренней сети или непосредственной причиной нанесения ущерба.

В результате исследования HP обнаружено, что около 70 % выбранных устройств не использует шифрование в беспроводной передаче данных. Веб-интерфейс 60 % устройств исследователи HP признали уязвимым из-за небезопасной реализации доступа и большого риска межсайтового скриптинга. Во многих устройствах используются пароли невысокой надежности. Около 90 % устройств используют телеметрию, собранную о владельце без его согласия.

Также исследователи HP выявили около 25 всевозможных уязвимостей в каждом из выбранных устройств (телевизоров, дверных замков, бытовых весов, домашних охранных систем, электророзеток и т. п.) и в их веб-компонентах.

Вывод исследователей HP настораживает: безопасная система IoT на данный момент отсутствует. Основную опасность IoT представляют в предмете распространения целевых атак. Как только злоумышленники решат воздействовать на кого-либо, и наши верные помощники из мира IoT превращаются в предателей, нараспашку открывающих доступ в мир своих владельцев.

Уязвимые места интернета вещей:

– IPv6;

– питание сенсоров;

– стандартизация архитектуры и протоколов, сертификация устройств;

– обеспечение защиты информации;

– учетные записи по умолчанию, низкая надежность механизмов аутентификации;

– отсутствие сопровождения продуктов от производителя для решения проблем безопасности;

– невозможность обновить программно-аппаратной составляющей;

– использование открытых протоколов и лишних открытых портов;

– зависимость безопасности сети от конкретных устройств;

– использование слабозащищенных мобильных технологий

– использование незащищенной облачной инфраструктуры;

– использование уязвимого программного обеспечения

Как вариант, не исключается установка на устройства сети специальных уникальных чипов, которые обезопасят их от атак хакеров. Такие меры должны увеличить уровень доверия к IoT в обществе и помешать злоумышленникам реализовывать ботнеты из подключаемой техники (см. таблицу).

В первой половине 2019 г. специалисты из «Лаборатории Касперского» с помощью приманок для злоумышленников зафиксировали 105 млн атак на IoT-устройства, исходящих с 276 тыс. уникальных IP-адресов. Данный показатель в семь раз больше, чем в первой половине 2018 г., когда было обнаружено около 12 млн атак с 69 тыс. IP-адресов. Пользуясь практически отсутствующей защитой IoT-продуктов, злоумышленники прикладывают больше усилий для создания и монетизации IoT-ботнетов.

Количество атак на IoT-устройства постоянно растет, потому что пользователи и организации все чаще приобретают «умные» устройства, такие как роутеры или камеры видеонаблюдения, но при этом мало кто заботится об их защите и установке актуальных обновлений. Злоумышленники, в свою очередь, видят все больше финансовой выгоды в эксплуатировании таких устройств. Они используют сети зараженных «умных» устройств для проведения DDoS-атак или в качестве прокси-сервера для других типов вредоносных действий.

Согласно полученным данным, атаки на IoT-устройства не выделяются сложной реализацией, но являются достаточно незаметными для рядовых пользователей. Самым популярным типом вредоносных программ, который позволяет ботнетам компрометировать устройства с помощью старых уязвимостей и управлять ими, является Mirai. Данное семейство программного обеспечения применялось в 39 % от всех атак. Второе место занимает вредоносное ПО Nyadrop (38,57 %), которое использует брут-форс в своей реализации, а также часто использовался в качестве загрузчика Mirai. Третьим наиболее рас-

Статистика и прогноз расходов на сервисы безопасности [4]

	2016	2017	2018	2019	2020	2021
Endpoint Security	240	302	373	459	541	631
Gateway Security	102	138	186	251	327	415
Professional Services	570	734	946	1,221	1,589	2,071
Total	**912**	**1,174**	**1,506**	**1,931**	**2,457**	**3,118**

пространенным ботнетом стал Gafgyt (2,12 % от всех атак) (рис. 2) [3].

Исследователи также определили страны, которые чаще других оказывались источниками атак в первом полугодии 2019 года. 30 % от общего числа атак исходило из Китая, из Бразилии – 19 %, далее Египет с долей в 12 %. В первом полугодии 2018 г. положение оказалось другим – Бразилия являлась первой с долей 28 %, Китай был источником 14 % атак, а третьей оказалась Япония с 11 % [3].

Внутри IoT-систем накопление информации происходит в режиме реального времени. К примеру, информация о занятости индустриальных систем, информация необходимая для управления дорожным трафиком, информация о текущем состоянии человека, видео, текстовая информация и т. д. Устройства, отправляющие такую информацию, могут оказаться уязвимыми, из-за чего возможна утечка важных данных. К тому же небезопасными могут оказаться протоколы взаимодействия составных частей интернета вещей. Это обстоятельство имеет высокую актуальность. Если в прошлом устройства зачастую использовали клиент-серверную модель и представляли собой частные сети, то сейчас многие устройства подключаются друг к другу напрямую, при этом в этом случае облачная платформа используется для управления и сбора статистики. Это размывает границы информационной безопасности и заставляет организации пересматривать подходы к организации защиты на сетевом уровне.

Рассматривая прикладные протоколы с позиции производителей, получается огромный арсенал механизмов взаимодействия, стандарты не регулируются. Есть только несколько стандартных прикладных протоколов, например MQTT, CoAP и AMQP. Но большинство производителей IoT-устройств изначально производили электрооборудование, и когда они реализуют собственные протоколы и стандарты, то нечасто задумываются о безопасности.

Иная угроза – это возможность взлома локальных устройств в целях проведения вредоносного воздействия на инфраструктуру предприятия или путем использования IoT. Например одна из версий вредоносной сети Mirai внедрилась в более 5 миллионов устройств, считая и IoT в 164 странах мира. В результате у интернет-провайдера в Германии была заражена большая часть роутеров, что привело к серьезным репутационным и материальным потерям.

Другая угроза – это несанкционирование завладение правами администратора в устройствах IoT и изменение исходящих пакетов. К примеру, если IoT применяется в здравоохранении, то доктор получит некорректную информацию о самочувствии больного (от сенсора) и пропишет неправильное лечение.

Реализация безопасности конечных устройств при установке IoT содержит следующие этапы:

– анализ патча программно-аппаратной системы с последующей сертификацией на

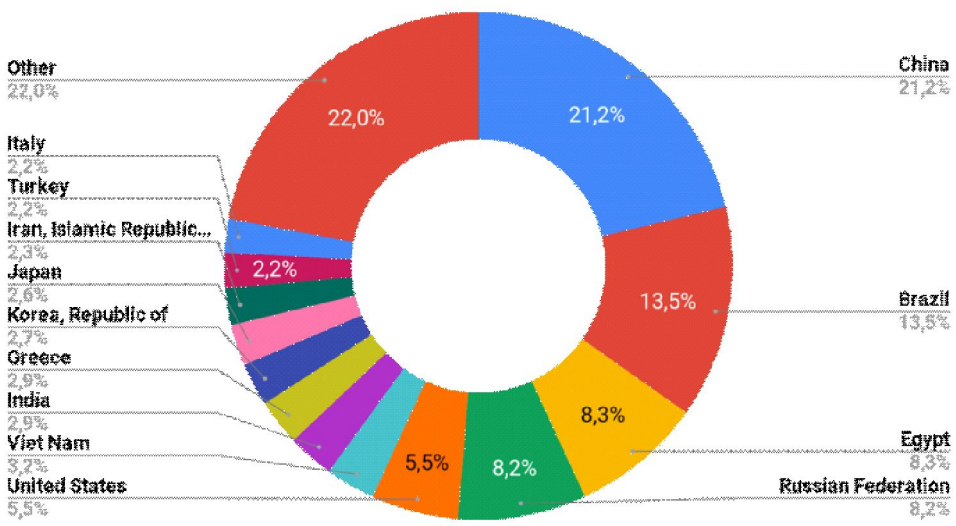

Рис. 2. Страны – источники атак на ханипоты за 2018 г.

отсутствие возможностей не указанных в документации;

– повышение безопасности встроенной операционной системы;

– обнаружение уязвимостей в непосредственной работе;

– правильное конфигурирование брандмауэра по умолчанию, предотвращение вторжений на прикладном уровне и на уровне протоколов передачи данных;

– использование технологий виртуальных частных сетей;

– проверка неизменности прошивки

– реализация общего механизма сертификации либо децентрализованной доверенной системы аутентификации для обеспечения связи между различными устройствами.

К тому же необходимо защитить облачные вычислительные мощности, осуществляющую управление и мониторинг, агрегацию и анализ информации, получаемой от устройств интернета вещей. Затем следует выборать брандмауэр, WAF, систему обнаружения и предотвращения атак, VPN, реализовать систему противодействия DDoS и отслеживанию действий клиентов, SIEM. Для всех систем необходимо выработать специальные требования в целях обеспечения безопасности устройств интернета вещей.

IIoT – многоуровневая система, имеющая в своем составе контроллеры и датчики, размещенные на узлах и агрегатах индустриальной системы, система передачи получаемой информации и ее отображения, инструменты аналитики и интерпретации получаемых данных и другие компоненты (рис. 3) [2].

Технология имеет следующую особенность: сначала вводятся сенсоры, механизмы исполнения, контроллеры и HMI в базовых элементах оборудования, затем производится получение данных, в дальнейшем позволяющих предприятию получить реальную информацию о текущем положении систем. Обработанные данные поступают в каждый департамент организации, в результате чего совместная работа сотрудников разных отделов становится быстрее и выносятся обоснованные решения.

Также организациям становится доступна замена традиционного документооборота.

Собираемые данные возможно применить в целях недопущения приостановки работ, неисправностей оборудования, снижения риска проведения экстренного техобслуживания и проблем проведении цепочек поставок, что дает возможность предприятию значительно повысить производительность труда.

В процессе структурирования необработанных больших массивов данных и фильтрации, объективная интерпретация является основной задачей для организаций. Здесь первостепенным значением становится корректное представление информации в понятном пользователю виде, для этого сегодня на рынке представлены прогрессивные аналитические платформы, предназначенные для сбора, хранения и анализа данных о технологических процессах и событиях в реальном времени.

Рис. 3. Сферы применения технологий IIoT [1]

Благодаря этим решениям производственные данные преобразуются в полезную информацию, необходимую для безопасного и рационального управления предприятием.

Внедрение таких технологий дает возможность предприятиям из разных отраслей экономики получить определенные преимущества:

– увеличить эффективность использования производственных активов на 10 % за счет сокращения количества незапланированных простоев;

– снизить затраты на техническое обслуживание на 10 %, усовершенствовав процедуры прогнозирования и предотвращения катастрофических отказов оборудования и выявляя неэффективные операции;

– повысить производительность на 10 %, увеличить уровень энергоэффективности и сократить эксплуатационные расходы на 10 % за счет более эффективного использования энергии.

Таким образом, передовые технологии позволяют предприятиям из различных отраслей промышленности добиться существенных конкурентных преимуществ.

11 февраля 2019 г. появилась информация о том, что Международная организация по стандартизации (ИСО/ISO) разработала стандарт ISO/TR 22100-4:2018 «Безопасность производственного оборудования – Связь с ISO 12100 – Часть 4: Руководство для производителей оборудования по рассмотрению соответствующих аспектов информационной безопасности (ISO/TR 22100-4:2018 Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects). Документ был опубликован в декабре 2018 года [6].

Глубокое проникновение промышленного интернета вещей в критически важную инфраструктуру и производственный сектор приводит к увеличению числа атак на информационные структуры предприятий. Об этом свидетельствуют данные исследования, проведенного аналитиками компании Frost & Sullivan, о чем стало известно 13 декабря 2018 года.

Согласно мнению экспертов, атаки только на энергетические и коммунальные отрасли обходятся предприятиям в среднем в $13,2 млн ежегодно. Специалисты Frost & Sullivan выделяют, что увеличение рисков является одной из причин разработки общих подходов к обеспечению информационной безопасности.

В отчете Frost & Sullivan указано несколько рекомендаций для развития компаний на рынке услуг обеспечения кибербезопасности. Одной из таких рекомендаций является создание интегрированных платформ, реализующих требуемый показатель защищенности конечных пользователей, одновременное внедрение лучших практик обеспечения ИБ, использование автоматизированных сервисов управления и расширенной аналитики для разработки комплексного портфеля услуг, который может быть адаптирован для всех типов конечных пользователей. Кроме того, аналитики считают перспективными гибкие модели ценообразования и подход CSaaS (Cybersecurity-as-a-Service – «кибербезопасность как услуга»).

Согласно результатам исследования «Лаборатории Касперского», инциденты с устройствами интернета вещей входят в тройку угроз с наибольшим финансовым ущербом для компаний. Это относится к компаниям любого размера: от малого бизнеса до больших корпораций.

По информации «Лаборатории Касперского», одной из главных проблем в сфере кибербезопасности индустриальных IoT-устройств является отсутствие единых стандартов. Рекомендации ENISA, как ожидается, станут важным шагом в сторону единообразия практик и политик безопасности, причем они касаются как создателей и пользователей промышленных IoT-устройств, так и разнообразных агентств Евросоюза, разрабатывающих политики безопасности.

Среди основных рекомендаций, разработанных для регуляторов:

– фокус на конкретных рекомендациях вместо общих для каждого сектора;

– стандартизировать рекомендации внутри ЕС, установить единую терминологию и классификацию;

– сотрудничать с представителями индустрии и вовлекать частный сектор в разработку законов, используя действующие ассоциации и объединения, например, AIOTI.

Главные рекомендации для производителей устройств и разработчиков ПО:

– убедиться, что с сотрудниками проведены беседы в области кибербезопасности, и

они обучены навыкам в области защиты информации;

– обеспечить совместимость данных с доверенной автоматизированной системой установки обновлений;

– провести проверку кода во время процесса установки – это уменьшит количество ошибок в конечной версии продукта, а также выявит любые попытки злоумышленника внедрить вредоносное программное обеспечение или обойти аутентификацию.

Популярность промышленного интернета вещей планомерно растет вместе с развитием интернета вещей. Оба этих подхода предполагают обмен данными через интернет, используют общие аппаратные платформы и управляются при помощи специализированного программного обеспечения, и это приводит к тому, что увеличивается количество общих уязвимостей и возможных атак на объекты промышленного сектора. Из отчета Frost & Sullivan следует, что промышленная и IT-инфраструктуры становятся прозрачнее. В первую очередь это связано с развитием стандарта Industrial 4.0 и отказ от изолирования промышленных объектов, что влечет за собой общие уязвимости, использование сервисов безопасности по модели SaaS для объектов промышленности, а также использование аппаратных устройств, доступ к которым потенциальный злоумышленник может получить довольно легко.

Если говорить про подход к защите IoT-систем в целом, то это нужно делать параллельно с определением требований информационной безопасности, то есть проводить подробный анализ рисков, которые появляются с внедрением различных технологий интернета вещей, и выстраивать систему с учетом максимально возможного уменьшения этих рисков. В текущей ситуации рекомендуется применять интернет вещей только для тех бизнес-процессов, для которых нарушение работоспособности не приводит к плачевным последствиям для бизнеса и здоровья людей.

СПИСОК ЛИТЕРАТУРЫ

1. Будущее за промышленным интернетом: телеком-компании нашли ниши для роста. – Электрон. текстовые дан. – Режим доступа: https://yamobi.ru/posts/iiot-2016.

2. Зачем вам нужен Splunk? Интернет вещей и промышленные данные. – Электрон. текстовые дан. – Режим доступа: https://www.securitylab.ru/blog/company/ts-solution/344595.php.

3. Интернет вещей (IoT): история зловредов. – Электрон. текстовые дан. – Режим доступа: https://securelist.ru/iot-a-malware-story/94900/

4. Информационная безопасность интернета вещей (Internet of Things). – Электрон. текстовые дан. – Режим доступа: https://www.tadviser.ru/index.php/%D1%F2%E0%F2%FC%FF:%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF_%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC_%E8%ED%F2%E5%F0%ED%E5%F2%E0_%E2%E5%F9%E5%E9_%28Internet_of_Things%29

5. Технологическая платформа интернета вещей: стандарты, возможности, перспективы. – Электрон. текстовые дан. – Режим доступа: https://www.tssonline.ru/articles/tekhnologicheskaya-platforma-interneta-veshchej-standarty-vozmozhnosti-perspektivy.

6. ISO/TR 22100-4:2018 Safety of machinery – Relationship with ISO 12100. – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects.

REFERENCES

1. *Budushchee za promyshlennym internetom: telekom-kompanii nashli nishi dlya rosta* [The Future of the Industrial Internet: Telecom Companies Have Found Niches for Growth]. URL: https://yamobi.ru/posts/iiot-2016.

2. *Zachem vam nuzhen Splunk? Internet veshchej i promyshlennye dannye* [Why do you Need to Splunk? Internet of Things and Industrial Data]. URL: https://www.securitylab.ru/blog/company/ts-solution/344595.php.

3. *Internet veshchej (IoT): istoriya zlovredov* [Internet of Things (IoT): A History of Malware]. URL: https://securelist.ru/iot-a-malware-story/94900.

4. *Informacionnaya bezopasnost' interneta veshchej (Internet of Things)* [Information Security of the Internet of Things (Internet of Things)]. URL: https://www.tadviser.ru/index.php/%D1%F2%E0%F2%FC%FF:%C8%ED%F4%EE%F0%EC%E0%F6%E8%EE%ED%ED%E0%FF_%E1%E5%E7%EE%EF%E0%F1%ED%EE%F1%F2%FC_%E8%ED%F2%E5%F0%ED%E5%F2%E0_%E2%E5%F9%E5%E9_%28Inter net_of_Things%29.

5. *Tekhnologicheskaya platforma interneta veshchej: standarty, vozmozhnosti, perspektivy* [The Technological Platform of the Internet of Things:

Standards, Opportunities, Prospects]. URL: https://www.tssonline.ru/articles/tekhnologicheskaya-platforma-interneta-veshchej-standarty-vozmozhnosti-perspektivy.

6. *ISO/TR 22100-4:2018 Safety of machinery – Relationship with ISO 12100. Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*.

THREAT AND VULNERABILITY ANALYSIS OF IoT AND IIoT CONCEPTS

Vadim Yu. Shevtsov

Assistant Lecturer, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Nikita P. Kasimovsky

Student, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. IoT and IIoT are new information technologies. They are very efficient solutions for home, industry and infrastructure. A lot of complex processes can be implemented using this systems. The popularity of the industrial Internet of things is steadily growing along with the development of the Internet of things. Both of these approaches involve the exchange of data over the Internet, use of common hardware platforms and are managed by using specialized software, and this leads to an increase in the number of common vulnerabilities and possible attacks on industrial facilities. The Frost & Sullivan report shows that industrial and IT infrastructures are becoming more transparent. First of all, this is due to the development of the Industrial 4.0 standard and the refusal to isolate industrial facilities, which entails common vulnerabilities, the use of security services based on the SaaS model for industrial facilities, as well as the use of hardware devices that a potential attacker can access quite easily. But very actual problems of IoT and IIoT are information security. Many of this systems are critical and little error can stop the entire system. This is not hard for hackers because that complex system has sensitive components usually. For example simple router can have a lot of vulnerabilities. There an attacker takes a root easily in every system. To solve the problem successfully it is recommended to use complex security actions. These are secure configurations of network devices, using safe devices and protocols, regular audit, using backups, using actual politics of information security.

Key words: IoT, IIoT, botnet, cybersecurity, malicious software.