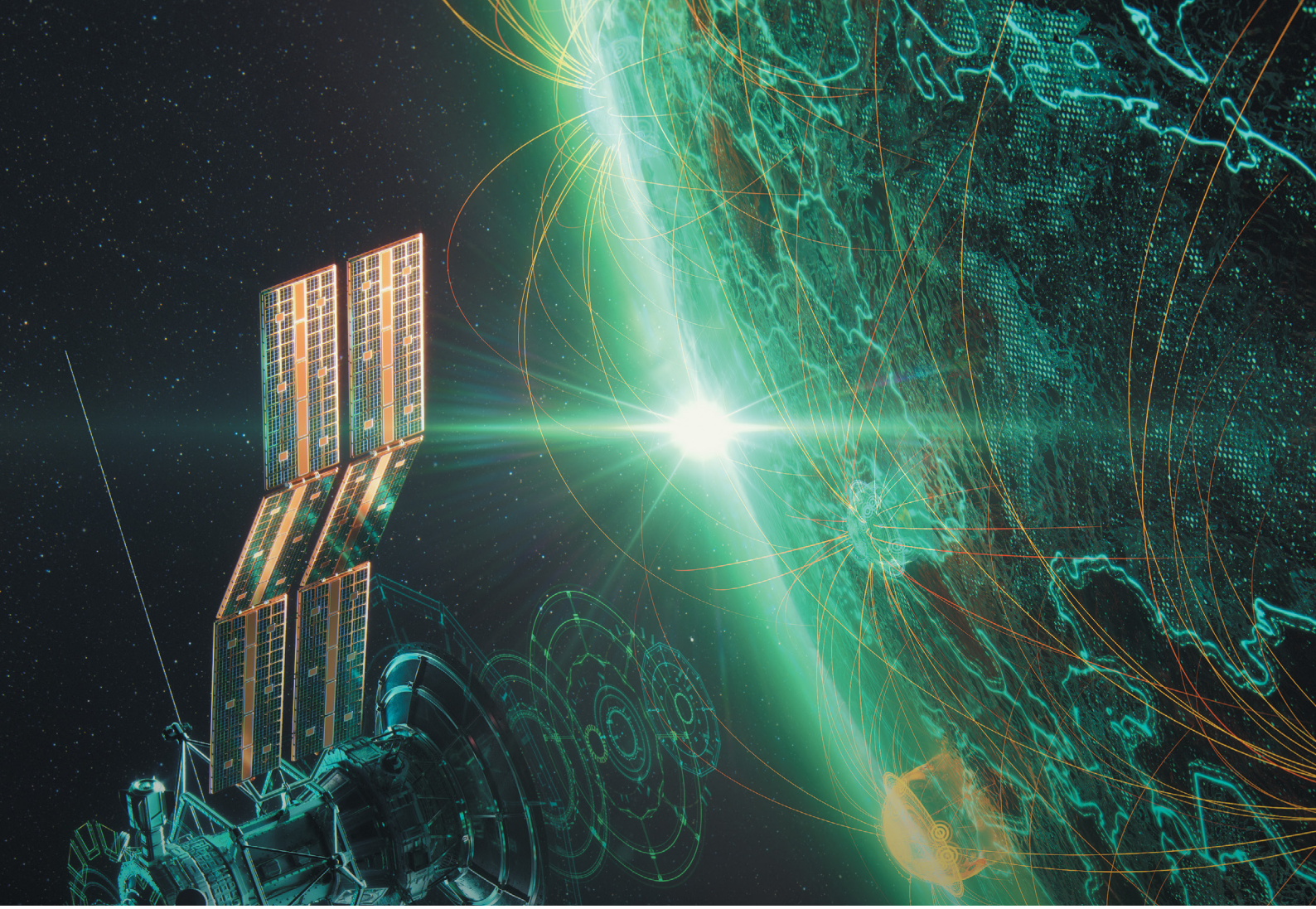


Безопасная ОС для телекоммуникационного оборудования

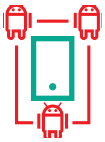
kaspersky АКТИВИРУЙ БУДУЩЕЕ

KasperskyOS®

KasperskyOS®

Топ-3 атак:

MIRAI Ботнет из устройств интернета вещей, источник ряда крупнейших DDoS-атак в истории



WIREX Ботнет из взломанных устройств Android для запуска DDoS-атак

REAPER (IoTroop) недавно обнаруженный ботнет, по объему превосходящий Mirai

Два основных типа устройств интернета вещей, которые подвергаются атакам:

33,6% Роутер
23,2% DVR (цифровая видеокамера)

Общая информация

Сегодня интернет стал неотъемлемой частью повседневной жизни, и многие предприятия трансформируются в ИТ- и технологические компании. Однако новые возможности порождают новые риски. Мы часто не осознаем, как сильно наша работа, жизнь и досуг связаны с использованием Сети. В отношении интернета риски в первую очередь связаны с киберугрозами, которые могут повлиять на стабильность его инфраструктуры. Стабильность работы интернета зависит от поставщиков телекоммуникационных услуг и телекоммуникационного оборудования.

Цели

Среди киберугроз для телекоммуникационного оборудования наиболее значимыми являются:

1. Угрозы, связанные с неумышленными действиями:

- Действия сотрудника, ставшие причиной полного или частичного отказа оборудования, отключения или изменения режима работы.
- Неавторизованная установка и использование неучтённых программ.

2. Угрозы, связанные с умышленными действиями:

- Удалённые атаки на аппаратное обеспечение с целью изменения его настроек или подмены встраиваемого ПО (прошивки).
- Использование встроенных бэкдоров, эксплуатация известных программных и аппаратных уязвимостей для перехвата трафика или получения контроля над оборудованием или над автоматизированной системой.
- Неавторизованная установка и использование неучтенных программ.

Некоторые из этих угроз можно нейтрализовать с помощью специального защитного ПО, в то время как надёжной защиты от других угроз можно добиться только с помощью доверенных программно-аппаратных комплексов, обеспечивающих гарантированную защиту от установки неавторизированного ПО и выполнения несанкционированных действий.

Это означает, что производители оборудования сталкиваются с трудной дилеммой. С одной стороны, оборудование, которое они производят, должно предоставлять широкие функциональные возможности; с другой стороны, его прошивка должна быть достаточно компактной, чтобы сделать возможной её проверку на уязвимости и бэкдоры. Оборудование также должно обеспечивать безупречную работу, быть надёжным и иметь отличные характеристики кибербезопасности.

Следует также иметь в виду, что защита телекоммуникационного оборудования от киберугроз дополнительно осложняется рядом факторов, среди которых:

- необходимость автономного функционирования оборудования – без обслуживания и обновления программного обеспечения в течение длительных периодов времени;
- узкая специализация оборудования;
- проприетарность встроенного программного обеспечения;
- необходимость постоянного прямого подключения к интернету;
- невозможность установки дополнительной защиты, разработанной для систем общего назначения.

Устройства интернета вещей легко взломать, поскольку они:

- Не используют безопасное ПО
- Не спроектированы безопасно
- Не получают регулярно патчи

Единственный способ решения перечисленных проблем – создание интегрированного программного пакета для обеспечения кибербезопасности, включающего операционную систему, а также системное и прикладное программное обеспечение.

Чтобы решить вопросы кибербезопасности телекоммуникационного оборудования и при этом минимизировать время, необходимое для разработки защитных средств, мы предлагаем KasperskyOS – операционную систему, позволяющую обеспечить безопасную эксплуатацию ПО, в том числе небезопасных приложений. KasperskyOS также обеспечивает защиту при случайных ошибках ПО и неправомерных действиях пользователей.

Особенности

Существуют дополнительные функции безопасности телекоммуникационного оборудования, которые могут быть предоставлены наряду с KasperskyOS:

Единственный способ решения проблем – создание интегрированного программного пакета для обеспечения кибербезопасности, включающего операционную систему, а также системное и прикладное программное обеспечение.

Доверенный канал

Это набор компонентов, которые могут использоваться для организации безопасного канала коммуникации между устройством и удаленной стороной. Технология основана на протоколе TLS – зрелом стандартном протоколе для организации безопасных взаимодействий. Возможны разные реализации (включая открытые источники) с поддержкой протоколов различных вендоров. Однако зачастую решения на базе TLS объединяют в одном домене различные функции (в т.ч. процессы Linux), такие как:

- Реализация TLS
- Контроль соединений
- Исполнение специализированных протоколов (например, HTTP)
- Более высокоуровневая логика

Все эти функции должны быть доверенными – компрометация одной из них грозит компрометацией всей системы.

Основная цель Доверенного канала – минимизировать объём доверенного кода путём разделения процессов безопасного соединения, авторизации и обработки удалённых запросов. В KasperskyOS безопасное соединение осуществляется посредством TLS в отдельном домене (сущности), равно как и авторизация соединения. Ни TLS, ни авторизация не выполняют обработку сообщений, специфичных для приложений.

В такой архитектуре сетевые модули, контроль соединений и обработка данных, специфичных для приложений (например, парсинг HTTP), не являются доверенными. Единственные доверенные компоненты – это TLS и авторизация.

84%

экспертов по ИТ-безопасности сообщили, что Mirai изменил их взгляд на угрозы для интернета вещей

90%

ИТ-специалистов считают, что подключённые устройства станут крупной проблемой безопасности в этом году

Оборудование также должно обеспечивать безупречную работу, быть надёжным и иметь отличные характеристики кибербезопасности.

Безопасное хранилище

Безопасное хранилище – это база данных «ключ-значение» с простым интерфейсом, подходящим для хранения важных конфигурационных параметров. Каждый параметр в базе данных соотносится со своими атрибутами безопасности.

Политика безопасности может быть применена для установки/получения определенного параметра на основе его атрибутов безопасности. Также можно установить политику безопасности для всех настроек обновлений, которые отвечают за то, чтобы обновления индивидуальных параметров были согласованы друг с другом.

KSS использует безопасное хранилище для хранения параметров политик безопасности. Хранилище также может использоваться любым приложением в системе. Политика безопасности определяет, к каким параметрам имеет доступ каждое приложение.

Прогноз: > 30 млрд устройств интернета вещей к 2020 г.

Количество атак на устройства интернета вещей в 2017 г. выросло на **600%** и достигло **50 000**

Сервисы безопасности

«Лаборатория Касперского» предлагает ряд проактивных сервисов для защиты телекоммуникационного оборудования от угроз, в том числе тестирование на проникновение и оценку защищённости. В рамках этих сервисов наши эксперты пытаются обнаружить уязвимости и обойти процедуры аутентификации и авторизации – так же, как это делают злоумышленники при попытке получить контроль над оборудованием.

Преимущества

Исходная безопасность. KasperskyOS – это безопасно спроектированная операционная система, и мы намерены и дальше поддерживать её безопасность, используя лучшие практики разработки программного обеспечения.

Универсальная модульная архитектура. Создание системы на основе слабосвязанных модулей помогает свести к минимуму объём доверенного кода и адаптировать каждое решение к индивидуальным потребностям клиента.

Грамотно спроектированные приложения. Компонентный подход к созданию безопасных приложений делает их разработку более простой и удобной, что помогает сократить время, необходимое для вывода новых продуктов на рынок.

Гибкая конфигурация безопасности. Продуманные инструменты настройки упрощают создание декларативных правил и их комбинаций для управления взаимодействиями в системе.

Отделение функций приложений от функций безопасности. Архитектура системы спроектирована таким образом, чтобы отделить функции безопасности от бизнес-логики приложений. Это упрощает настройку политик безопасности и разработку приложений.

Полноценная защита для подключенных устройств. KasperskyOS – это надёжная платформа для встроенных систем, которые имеют особые требования к кибербезопасности.

Технические требования

- Требования к CPU: Memory Management Unit (MMU); IOMMU (SDMA для ARM) настоятельно рекомендуется для надежной изоляции аппаратных ресурсов;
- Поддерживаемая архитектура: x86, x86_64, ARMv5, ARMv7, ARMv8 и MIPS32;
- Протестированные аппаратные платформы: Intel Generic и Atom CPUs, NXP i.MX6 (Solo, Duo и Quad), NXP i.MX27, TI Sitara AM335x, TI Sitara AM43xx, HiSilicon Kirin620, MIPS24k.
- Минимальный объём RAM зависит от решения. Рекомендуемый объём RAM 128 Мб.

Патенты

Технологии, составляющие основу KasperskyOS и Kaspersky Security System, имеют ряд патентов:

US 7386885 B1, US 7730535 B1,
US 8370918 B1, EP 2575318 A1,
US 8522008 B2, US 20130333018 A1,
US 8381282 B1, EP 2575317 A1,
US 8370922 B1, EP 2575319 A1,
US 9015797 B1, DE 202014104595 U1.

KasperskyOS®

Подробнее на os.kaspersky.ru

www.kaspersky.ru