Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Аудит IoT-парка офиса: реверс ESP8266-розеток и VLAN

Как мы инвентаризуем 47 умных устройств, снимаем дампы прошивок и режем сеть на изолированные...

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

IoT-парк офиса растёт стихийно: розетки с маркетплейса, термостаты, камеры и NAS попадают в одну плоскую /24 с бухгалтерскими ПК и 1С. Дефолтные пароли, открытый telnet, устаревшие прошивки и «фонящие» наружу устройства превращают каждую умную розетку в точку входа. Мы находим теневые устройства сканом и обходом, снимаем дамп подозрительной прошивки, вычищаем C2-каналы и загон…

Почему это важно бизнесу

- Скомпрометированная камера или розетка в сети бухгалтера — прямой путь к 1С-базе и утечке
- Теневые устройства на корпоративном Wi-Fi невидимы для админа и обходят весь периметр
- Дефолтные admin/12345 и SNMP public вскрываются автоматом за минуты после нахождения
- Простой при инциденте и восстановление обходятся кратно дороже планового аудита
- Без регламента закупок парк снова обрастает «зоопарком» за считанные месяцы

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

802.1Q

Аппаратная VLAN-сегментация на bridge с vlan-filtering=yes и режимом IVL

по докам RouterOS 7

0x400000

Полный дамп флеша ESP8266 (4 МБ) командой read-flash 0x0 0x400000

по докам esptool

12.1.3

Ghidra для статики: ядро Xtensa в дистрибутиве с 11.0, плагин не нужен

Ghidra 12.1.3

3.1.0

binwalk (переписан на Rust) для сигнатурного разбора и извлечения SPIFFS

binwalk v3

DENY

Дефолтное правило forward для IoT-VLAN: всё, кроме белого списка облаков

наш стандарт

0x8100

EtherType внешнего тега, по которому bridge разделяет tagged/untagged

по докам RouterOS 7

РЕАЛИЗАЦИЯ 1 ИЗ 3

Инвентаризация: скан + физобход, поиск теневых устройств

Что настраиваем

Вся LAN /24 клиента с ноутбука инженера в trunk-порту, плюс Wi-Fi-сегмент

Как мы это делаем

1. masscan по /24 -p1-65535 --rate=10000 -oG для быстрого списка живых хостов
2. nmap -A -p- по найденным IP (включает -sV/-O) — баннеры, ОС, открытые порты
3. Сверка MAC-префиксов (OUI Espressif, Hikvision, Tuya) со списком админа
4. Личный обход офиса и склада: находим то, что скан не покажет по OUI
5. Сводим в реестр: MAC, IP, прошивка, ответственный — «известные» против «теневых»

РЕЗУЛЬТАТ

Реальное число устройств почти всегда выше заявленного админом. Мы отделяем санкционированную оргтехнику от личных гаджетов сотрудников и явно подсвечиваем теневые устройства, сидящие на пароле сотрудника в одной сети с 1С.

КЛЮЧЕВОЙ НЮАНС

Скан по OUI и баннерам не заменяет физобход: устройства за NAT, в спящем режиме или с чужим MAC видны только глазами. Оба метода запускаем параллельно.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Реверс прошивки ESP8266: дамп, SPIFFS, статика в Ghidra

Что настраиваем

Одна изъятая розетка на ESP-12F (ESP8266) на стенде инженера, вне сети клиента

Как мы это делаем

1. GPIO0 на землю → режим загрузки, USB-UART CP2102 на TX/RX, питание 3.3В
2. esptool read-flash 0x0 0x400000 dump.bin, затем verify-flash 0x0 dump.bin — сверка образа с флешем
3. binwalk -e: разбор разделов, извлечение файловой системы SPIFFS
4. Строки из SPIFFS: конфиги, автозапуск — проверяем на прошитый Wi-Fi-пароль
5. main-app в Ghidra (Xtensa): grep по строкам heartbeat/http/post/eval в .rodata

РЕЗУЛЬТАТ

Статический анализ показывает реальное поведение прошивки без облака вендора: адрес и интервал heartbeat, формат JSON-пейлоада, наличие парсера входящих команд. Это документируется как основание для замены устройств.

КЛЮЧЕВОЙ НЮАНС

Прошитый в открытом виде Wi-Fi-пароль в SPIFFS — типовая находка. После любого реверса, где всплыл пароль сети, планируем ротацию PSK, а не только изъятие устройства.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Сегментация на MikroTik: bridge VLAN filtering + default-drop

Что настраиваем

MikroTik CCR2004 как маршрутизатор + управляемые CRS328 как access/trunk уровня

Как мы это делаем

1. Один bridge с vlan-filtering=yes, IVL; порты — tagged (trunk) и untagged (access)
2. Bridge VLAN Table: членство портов по VLAN 10/20/30/40, PVID на access-портах
3. Отдельные /ip address и DNS на каждый VLAN-интерфейс, изоляция шлюзов
4. Firewall forward: CCTV → только NVR, NAS/VoIP → backup+SIP, IoT → белый список
5. Замыкающий drop в конце цепочки forward для IoT-сегмента (default-deny)

РЕЗУЛЬТАТ

Даже устройство с C2-каналом физически не дотянется наружу и не сходит латерально к бухгалтерии: трафик мимо белого списка облаков рубится на шлюзе мгновенно. Камеры видит только NVR, телефоны — только SIP-провайдер.

КЛЮЧЕВОЙ НЮАНС

Bridge VLAN filtering с hardware offload работает на Prestera-чипах CRS3xx и ряде чипов вроде MT7621/RTL8367. Проверяем, что модель тянет offload, иначе фильтрация ляжет на CPU и просадит throughput.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Доверять списку устройств от админа**
  Заявленное число почти всегда занижено: теневые гаджеты и личные устройства не попадают в учёт. Сверяем скан, OUI и физобход между собой.

- ✕ **Плоская /24 на весь офис**
  Камеры, IoT и бухгалтерия в одной сети = один взлом до 1С. Режем на VLAN с межсегментным default-drop, а не полагаемся на пароли.

- ✕ **Считать закрытый веб безопасным**
  У розеток на ESP8266 telnet/8443 и heartbeat наружу живут мимо UI. Смотрим реальные исходящие соединения на шлюзе, а не только порты.

- ✕ **Дамп без верификации**
  Обрыв UART даёт битый образ и ложный анализ. Снимаем полный 0x400000 и сверяем образ с флешем через esptool verify-flash до разбора в binwalk.

- ✕ **Забыть про прошитый Wi-Fi-пароль**
  PSK в SPIFFS в открытом виде компрометирует всю сеть. После реверса с находкой пароля планируем ротацию ключа, а не только изъятие.

- ✕ **VLAN filtering без offload**
  На чипе без аппаратной поддержки фильтрация уходит на CPU и роняет пропускную способность. Сверяем модель свитча с матрицей поддержки RouterOS 7.

- ✕ **Открытый веб NAS через NAT**
  DSM-интерфейс наружу — приглашение к брутфорсу и эксплойтам CVE. Закрываем проброс, доступ только через VPN, DSM обновляем.

- ✕ **Аудит без регламента закупок**
  Через полгода парк снова обрастает умными лампочками из маркетплейса. Внедряем обязательную проверку каждого IoT до подключения.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Инвентаризация всех устройств: MAC, IP, прошивка, ответственный
- Смена всех дефолтных паролей и SNMP-community на камерах и принтерах
- Отключение telnet/UART-сервисов и закрытие внешних пробросов к NAS
- Обновление прошивок камер, NAS и точек доступа до актуальных

НОРМАЛЬНО

- Разделение на VLAN: офис, CCTV, NAS/VoIP, IoT-untrust
- Firewall с явным deny инета для CCTV и default-drop для IoT
- Белый список облаков (dst-address-list) для доверенных IoT-вендоров
- Изъятие и реверс любого устройства с неопознанным C2-трафиком

ХОРОШО

- Мониторинг топ исходящих хостов со шлюза с алертом на новое
- Регламент закупок IoT: проверка каждого устройства до подключения
- Ротация Wi-Fi PSK и вынос IoT на отдельный SSID в untrust-VLAN
- Стендовый реверс подозрительных прошивок как штатная процедура

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли актуальный реестр всех сетевых устройств с MAC, IP и версией прошивки?
- [ ] Совпадает ли число устройств в скане с заявленным админом и с физобходом?
- [ ] Выделены ли камеры, IoT и бухгалтерия в разные VLAN, а не в одну /24?
- [ ] Стоит ли на IoT-сегменте замыкающий default-drop в цепочке forward?
- [ ] Запрещён ли камерам выход в интернет всюду, кроме NVR-сервера?
- [ ] Сменены ли все дефолтные пароли и SNMP-community public на оргтехнике?
- [ ] Закрыт ли внешний доступ к веб-интерфейсам NAS, доступ только через VPN?
- [ ] Настроен ли белый список облаков для доверенных IoT-вендоров?
- [ ] Мониторится ли топ исходящих соединений со шлюза с алертом на новое?
- [ ] Действует ли регламент: любое новое IoT-устройство проходит проверку до подключения?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Полная инвентаризация IoT-парка: скан masscan/nmap, OUI-сверка и физобход
- Реверс подозрительной прошивки на стенде: дамп esptool, binwalk, статика в Ghidra
- Проект и внедрение VLAN-сегментации на MikroTik с bridge VLAN filtering и default-drop
- Настройка мониторинга исходящих соединений со шлюза с Telegram-алертами
- Регламент закупок IoT и обучение админа работе с инцидентами и логами

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 esptool: Basic Commands (read-flash, verify-flash) (docs.espressif.com — v5)

02 Ghidra: поддержка Xtensa в ядре с 11.0 (github.com — 12.1.3)

03 binwalk: сигнатурный разбор и извлечение FS (github.com — 3.1.0)

04 RouterOS: Bridging and Switching, vlan-filtering и IVL (help.mikrotik.com — 7.x)

05 RouterOS: Bridge VLAN Table, tagged/untagged членство (help.mikrotik.com — 7.x)

06 Наш шаблон firewall forward: default-drop + address-list (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.