Аннотация – в документе представлен анализ Fuxnet, приписываемого хакерской группе Blackjack, которое, как сообщается, нацелено на инфраструктуру отдельных стран. Анализ включает в себя различные аспекты вредоносного ПО, включая его технические характеристики, влияние на системы, механизмы защиты, методы распространения, цели и мотивы, стоящие за его внедрением. Изучив эти аспекты, цель документа-обеспечить подробный обзор Fuxnet по возможности и её значение для кибербезопасности.

Документ предлагает качественное описание Fuxnet, основанное на информации, которой публично доступной от экспертов по кибербезопасности. Этот анализ полезен для специалистов в области ИБ, ИТ-специалистов и заинтересованных сторон в различных отраслях, поскольку он не только проливает свет на технические тонкости сложной киберугрозы, но и подчёркивает важность надёжных мер кибербезопасности для защиты критически важной инфраструктуры от возникающих угроз. Документ способствует более широкому пониманию тактики ведения кибервойны и повышает готовность организаций к защите от подобных атак в будущем.

I. Введение

Хакерская группа Blackjack, предположительно связанная с украинскими спецслужбами, взяла на себя ответственность за кибератаку, которая якобы поставила под угрозу возможности обнаружения чрезвычайных ситуаций и реагирования на них в прилегающих районах РФ. Эта группа была связана с предыдущими кибератаками, направленными против интернет-провайдеров и военной инфраструктуры. Их последнее заявление касается нападения на компанию, отвечающую за строительство и мониторинг инфраструктуры подземных вод, канализации и коммуникаций.

Группа распространила подробную информацию об атаке на веб-сайте ruexfil[.]com, включая использование Fuxnet, включая скриншоты систем мониторинга, серверов и баз данных, которые, по их утверждению, были удалены и выведены из строя, а также дампы паролей.

Основные выводы из анализа Fuxnet, в т.ч. из материалов Team82 и Claroty:

- **Неподтверждённые заявления**: Team82 и Claroty не смогли подтвердить заявления относительно влияния кибератаки на возможности правительства по реагированию на чрезвычайные ситуации или степени ущерба, причинённого Fuxnet.
- **Несоответствие в сообщениях о воздействии**: первоначальное утверждение о 2659 сенсорных шлюзов не совпали с информацией об атаке 1700. А проведённый Team82 анализ показывает, что только немногим более 500 были фактически затронуты Fuxnet. На это последовали заявление Blackjack об выведено из строя 87000 датчиков также было разъяснено, заявив, что они отключили датчики, «уничтожив шлюзы путём фаззинга», а не физическое уничтожение датчиков.
- **Фаззинг M-Bus**: метод был направлен на отключение датчиков, но точное количество датчиков оказалось невозможно установить ввиду их недоступности извне.
- **Отсутствие прямых доказательств**: отсутствуют прямые доказательства, подтверждающие масштабы ущерба или влияние на возможности обнаружения чрезвычайных ситуаций и реагирования на них в т.ч. о Москоллектор.
- **Разъяснение от Blackjack**: после публикации первоначального анализа Team82 Blackjack обратилась с просьбой предоставить разъяснения, в частности, оспорив утверждение о том, что было затронуто только около 500 сенсорных шлюзов и обнародованные файлы JSON были лишь примером полного объёма их деятельности.

II. Отрасли и последствия

A. *Возможные отрасли:*

- **Коммунальные службы**: Основной целью Fuxnet был сектор коммунальных услуг, в частности сенсорные шлюзы, управляющие системами водоснабжения и канализации. Это может иметь последствия для предоставления этих основных услуг и мониторинга за ними.
- **Службы экстренной помощи**: Группа утверждала, о получении доступ к службе экстренной помощи 112, что могло повлиять на способность эффективно реагировать на чрезвычайные ситуации.
- **Транспорт**: Группа также утверждала, что вывела из строя датчики и контроллеры в критически важных объектах инфраструктуры, включая аэропорты и метро, что могло нарушить транспортное обслуживание и безопасность.
- **Энергетика**: В качестве ещё одной цели были упомянуты газопроводы, что указывает на

потенциальный риск для систем распределения энергии и мониторинга.

B. Возможные последствия:

- **Нарушение работы служб**: Разрушение или неисправность сенсорных шлюзов может привести к нарушению работы систем мониторинга и управления коммунальными службами, что потенциально может привести к перебоям в обслуживании.
- **Нарушение безопасности**: В транспортном и энергетическом секторах потеря функциональности датчиков может представлять угрозу безопасности, поскольку эти датчики часто имеют решающее значение для обнаружения опасных условий.
- **Экономический эффект**: Потенциальные простои и затраты на ремонт, связанные с заменой или перепрошивкой повреждённых шлюзов датчиков, могут иметь значительные экономические последствия для затронутых отраслей.
- **Задержки с реагированием на чрезвычайные ситуаци**и: может привести к задержкам в реагировании на чрезвычайные ситуации, что повлияет на общественную безопасность.
- **Утечка данных**: возможная компрометация сетевые системы потенциально может привести к утечке данных и утечке конфиденциальной информации.
- **Потеря общественного доверия**: может привести к потере общественного доверия к сервисам и организациям, ответственным за их безопасность.

III. MOSCOLLECTOR-АТАКА

Недавно группа обнародовала свою деятельность и украденную информацию на веб-сайте ruexfil, подробно описав масштабы и последствия своего кибератаки. Выход из строя этой системы потенциально может привести к нарушению возможностей реагирования на чрезвычайные ситуации, что скажется на безопасности населения.

A. Установка датчиков и контроллеров критически важной инфраструктуры

Группа утверждает о взломе датчиков и контроллеров в критически важных секторах инфраструктуры, включая аэропорты, метро и газопроводы. Это действие, если оно было реальным, могло привести к отключению основных систем мониторинга и контроля, что привело бы к значительным сбоям в работе общественных служб и обеспечении безопасности.

B. Сбой в работе сетевого устройства

Группа утверждает, что они отключили сетевые устройства, такие как маршрутизаторы и брандмауэры. Это оказало бы каскадное воздействие на целостность сети, потенциально изолировав различные сегменты и затруднив коммуникацию в инфраструктуре.

C. Удаление серверов и баз данных

Злоумышленники утверждают, что удалили серверы, рабочие станции и базы данных, уничтожив около 30 ТБ данных, включая диски резервных копий. Такого рода уничтожение данных может привести к потере исторических данных, нарушению текущих операций и усложнению усилий по восстановлению.

D. Аннулирование доступа в офисное здание

Все карточки-ключи от офисного здания, как сообщается, признаны недействительными. Это действие может помешать сотрудникам получить доступ к своему рабочему месту, что ещё больше затруднит любые попытки оценить ущерб или запустить протоколы восстановления.

E. Сброс пароля

Также было заявлено о сбросе паролей из нескольких внутренних служб, что могло быть повлечь несанкционированный доступ к различным системам и данным, усугубляя последствия взлома и потенциально приводя к дальнейшей эксплуатации.

IV. НАБОР ЮНОГО АТАКУЮЩЕГО

Основное внимание было уделено коммуникационным шлюзам, которые служат критическими узлами для передачи данных от датчиков к глобальным системам мониторинга. Эти датчики являются неотъемлемой частью различных систем мониторинга окружающей среды, в том числе используемых в пожарной сигнализации, газовом мониторинге и системах управления освещением.

Датчики предназначены для сбора физических данных, таких как температура, и передачи этой информации по последовательному соединению или шине, в частности по шине RS485/Meter-Bus, на шлюз. Эти шлюзы действуют как узлы передачи, позволяя передавать телеметрические данные через Интернет в централизованную систему мониторинга, которая обеспечивает операторам видимость и контроль над системами.

Стандарт связи RS485, как упоминалось в деталях атаки, является широко распространённым протоколом для промышленных систем управления благодаря своей надёжности и возможностям связи на большие расстояния. Это позволяет нескольким устройствам взаимодействовать по единой системе шин, что важно для централизованного мониторинга различных датчиков и контроллеров.

Шина M-Bus — это протокол связи, используемый для сбора и передачи данных о потреблении, обычно для коммунальных услуг, таких как электричество, газ, вода или тепло. В сочетании с RS485 он образует надёжную сеть, позволяющую промышленным датчикам передавать информацию в центральные системы.

Компрометируя шлюзы, можно потенциально нарушить передачу телеметрии и управление датчиками, что приведёт к потере оперативной видимости и потенциально вызовет хаос в системах, которые полагаются на эти данные.

A. Утечка информации

Информация из файлов JSON была подтверждена двумя видеороликами на YouTube, демонстрирующими развёртывание Fuxnet. Устройства, перечисленные в видеороликах, соответствовали шлюзам из файла JSON,

подтверждая, что шлюзы TMSB / MPSB были основными целями Fuxnet.

Данные включали типы и названия устройств, IP-адреса, порты связи и данные о местоположении. В файле JSON были перечислены следующие типы устройств:

- MPSB (шлюз датчиков): 424 устройства
- TMSB (сенсорный шлюз+модем): 93 устройства
- IBZ (3g-маршрутизатор): 93 устройства
- Windows 10 (рабочая станция): 9 устройств
- Windows 7 (рабочая станция): 1 устройство
- Windows XP (рабочая станция): 1 устройство

Этот список указывает на то, что атака была сосредоточена на сенсорных шлюзах, а не на самих конечных датчиках. Шлюзы служат узлами связи для потенциально многочисленных датчиков, подключённых по последовательной шине, такой как RS485/Meter-Bus.

Утечка данных, включая скриншоты и экспорт в формате JSON, выявила два конкретных типа шлюзов, скомпрометированных во время атаки:

- **Шлюз MPSB**: Этот шлюз разработан для обмена информацией с внешними устройствами через несколько интерфейсов. Он поддерживает Ethernet и протоколы последовательной связи, включая CAN, RS-232 и RS-485. Шлюз MPSB является важнейшим компонентом для интеграции различных входных данных датчиков в единую систему мониторинга.
- **Шлюз TMSB**: Аналогичный по функциям MPSB, шлюз TMSB включает встроенный модем 3G / 4G, который позволяет передавать данные непосредственно через Интернет в удалённую систему без необходимости в дополнительном маршрутизирующем оборудовании.

Кибератака была нацелена на критически важную часть экосистемы датчиков: устройств оркестраторов / шлюзов, в частности шлюзы MPSB и TMSB. Эти устройства необходимы для считывания показаний основных датчиков ввода-вывода и управления ими, а также для передачи данных в глобальную систему мониторинга для централизованного надзора.

В ходе атаки использовались каналы связи между датчиками и глобальной системой мониторинга:

- **Для шлюза MPSB**: **Датчик —--- MBus/RS485 → MPSB + IoT роутер —---Интернет→ Система мониторинга.** данные датчика передаются через MBus/ RS485 на шлюз MPSB, который затем передает данные через маршрутизатор Интернета вещей в Интернет и, наконец, в систему мониторинга.
- **Для шлюза TMSB**: **Датчик —------ MBus/RS485 → TMSB (3g/4g модем) ----Интернет → Система мониторинга.** данные датчика передаются через MBus/ RS485 непосредственно на шлюз TMSB, который использует встроенный модем для передачи данных через Интернет в систему мониторинга.

B. Ошибки в системе безопасности и методология атак

Значительный недостаток в системе безопасности: использованием учётных данных по умолчанию (имя пользователя: sbk, пароль: temppwd) для доступа к шлюзам через SSH. Эта уязвимость позволила злоумышленникам легко скомпрометировать устройства.

Злоумышленники также опубликовали скриншоты из пользовательского интерфейса управления датчиками, демонстрирующие топологию сети.

Помимо модуля TMSB со встроенными возможностями 3/4G, злоумышленники упомянули использование роутеров iRZ RL22w. Эти маршрутизаторы, использующие OpenWRT использовались в качестве интернет-шлюзов для подключения датчиков к Интернету через 3G.

Сообщается, что злоумышленники использовали SSH для подключения к этим устройствам Интернета вещей и туннелирования к внутренним устройствам, вероятно, после получения паролей root. Поисковые запросы Shodan и Censys показали, что тысячи маршрутизаторов iRZ доступны в Интернете, при этом около 4100 устройств напрямую предоставляют свои услуги и около 500 подключены к Telnet.

C. Программное обеспечение для управления датчиками и ввода их в эксплуатацию:

ПО подключается к устройствам с использованием проприетарного протокола, который работает через порт TCP 4321. Интерфейс позволяет получать доступ к настройкам датчиков и изменять их, включая конфигурации ввода / вывода, узлы и показания. Эта возможность необходима для надлежащей настройки и обслуживания сенсорных сетей, гарантируя их эффективную и точную работу в назначенных условиях.

Особенности программного обеспечения:

- **Подключение устройства**: используется проприетарный протокол поверх TCP/4321 для установления безопасного соединения с датчиками.
- **Возможности настройки**: параметры датчиков, включая корректировку их рабочих параметров и управление данными, которые они собирают.
- **Пользовательский интерфейс**: интерфейс предоставляет средства взаимодействия с подключёнными датчиками

D. Техническое воздействие

Система мониторинга датчиков является важным компонентом инфраструктуры, предназначенной для. Эта система предназначена для объединения и отображения телеметрии и отчётов о состоянии, поступающих от сети датчиков, позволяя системным операторам получать оповещения в режиме реального времени, регистрировать данные и удалённо управлять датчиками.

Согласно заявлениям, группа успешно взломала эту систему мониторинга и получили доступ к полному списку управляемых датчиков и смогли географически сопоставить эти датчики на карте. Это раскрыло конфиденциальные оперативные данные, позволило манипулировать выходными данными датчиков для нарушения их работы:

- **Функции геолокации**: Система мониторинга имеет геолокационные метки, которые помогают визуализировать физическое расположение датчиков по всей сети. Эта функция особенно полезна при крупномасштабных операциях, когда датчики разбросаны по обширным площадям.
- **Мониторинг конкретного объекта**: скриншоты из системы показывают, что она способна фокусироваться на конкретных объектах, таких как больницы, что указывает на её использование в критически важных инфраструктурных объектах, где точный мониторинг необходим для обеспечения безопасности и работоспособности.

V. Анализ Fuxnet

Логические процессы, выявленные в поведении Fuxnet, включают несколько шагов, направленных на нанесение необратимого ущерба целевым устройствам.

- Fuxnet была специально разработана для атаки на сенсорные шлюзы и их выведения из строя, а не на конечные датчики.
- Действия вредоносного ПО включали блокировку устройств, «уничтожение» файловых систем, чипов NAND и томов UBI, а также флуд в каналах связи.
- Атаке, вероятно, способствовало использование учётных данных по умолчанию и уязвимостей в протоколах удалённого доступа.
- Несмотря на заявления о компрометации 87 000 устройств, фактическое воздействие, по-видимому, ограничено сенсорными шлюзами, а конечные датчики, вероятно, остались нетронутыми.

A. Сценарий развёртывания

Злоумышленники составили полный список IP-адресов сенсорных шлюзов, на которые они намеревались напасть, наряду с подробными описаниями физического местоположения каждого датчика. Затем вредоносная программа была распространена среди каждой цели, вероятно, с использованием протоколов удалённого доступа, таких как SSH или проприетарный протокол SBK sensor protocol, через TCP-порт 4321.

B. Блокировка устройств и «уничтожение» файловой системы

После запуска на целевом устройстве Fuxnet инициировала процесс его блокировки. Повторное монтирование файловой системы с доступом на запись приводилось к удалению критически важных файлов и каталогов. Fuxnet также отключал службы удалённого доступа, включая SSH, HTTP, telnet и SNMP, эффективно предотвращая любые попытки удалённого восстановления. Кроме того, Fuxnet удалила таблицу маршрутизации устройства, что привело к нарушению его коммуникационных возможностей.

C. «Уничтожение» чипов NAND

Вывод из строя достигался путём выполнения операции изменения битов на участках чипа SSD NAND, многократно записывая и перезаписывая память до полного отказа чипа, так как память NAND имеет ограниченное количество циклов записи.

D. Разрушающий томов UBI

Чтобы предотвратить перезагрузку датчика, Fuxnet переписывает том UBI используя интерфейс IOCTL UBI_IOCVOLUP, чтобы заставить ядро ожидать, что будет записано большее количество байт, чем фактически отправлено было на запись, в результате чего устройство зависало на неопределённый срок. Затем вредоносная программа перезаписала том UBI ненужными данными, дестабилизируя файловую систему.

E. Отказ в обслуживании при мониторинге

Последним шагом в процессе работы вредоносного ПО было нарушение связи между шлюзами датчиков и самими датчиками. Fuxnet замусорила каналы RS485 / Meter-Bus случайными данными, перегружая шину и датчики, что предотвратило передачу и приём данных датчиками и шлюзами, сделав процесс сбора данных бесполезным.

F. Стратегия фаззинга M-Bus

Стратегия включала постоянную отправку данных M-Bus по последовательному каналу RS485 с целью перегрузки и потенциального повреждения датчиков, подключённых к этой сети.

- **Случайный фаззинг**: формирование случайных байт и отправку их по M-Bus с добавлением простого CRC, чтобы гарантировать, что данные не будут проигнорированы. Цель состояла в том, чтобы охватить весь диапазон возможных полезных нагрузок M-Bus, действительных или нет, в надежде вызвать неисправности датчиков или уязвимости.
- **Структурированный фаззинг**: формирование допустимых данных с изменением определённых полей в протоколе. Более точно придерживаясь структуры M-Bus, была увеличена вероятность того, что датчик сочтёт пакет действительным и полностью проанализирует его, тем самым увеличив шансы срабатывания уязвимости.