электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.732.056

Передача информации по каналу ПЭМИН на основе технологии soft tempest

***Рябинин А. М.**, аспирант*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Защита информации»

Научный руководитель: Бонч-Бруевич А.М., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Защита информации»
ryabinin@bmstu.ru

Принятые сокращения

АС - автоматизированные системы

ВТСС - вспомогательные технические средства и системы

НСД - несанкционированный доступ

ОТСС - основные технические средства и системы

ПЭМИН - побочные электромагнитные излучения и наводки

РД - руководящий документ

СВТ - средства вычислительной техники

СЗИ - система защиты информации

СПО – специальное программное обеспечение

TEMPEST (сокращение от Transient Electromagnetic Pulse Emanation Standard) представляет собой стандарт на переходные электромагнитные импульсные излучения работающей радиоэлектронной аппаратуры. Аббревиатура TEMPEST появилась в начале 70-х годов, как название секретной программы Министерства Обороны США по разработке методов предотвращения утечки информации через различного рода демаскирующие и побочные излучения электронного оборудования. В России этот канал утечки информации называется ПЭМИН (Побочные ЭлектроМагнитные Излучения и Наводки).

Технология Soft Tempest - технология скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств. Предложенная ученым из Кембриджа Маркусом Куном (Markus Kuhn) в 1998 году[1] технология Soft

Tempest по своей сути есть разновидность компьютерной стеганографии, т.е. метода скрытной передачи полезного сообщения в безобидных видео, аудио, графических и текстовых файлах. Основная опасность технологии Soft Tempest заключается в скрытности работы вредоносного СПО. Такое СПО, в отличие от большинства вирусов не портит данные, не нарушает работу ПК, не производит несанкционированную рассылку по сети, а значит, долгое время не обнаруживается как пользователем и администратором сети, так и антивирусным программным обеспечением. Поэтому, если вирусы, использующие сетевые коммуникации (Интернет) для передачи данных, проявляют себя практически мгновенно, то вирусы, использующие побочные излучения электронного оборудования для передачи данных, могут работать годами, не обнаруживая себя.

Канал ПЭМИН характеризуется размером «зоны 2» (R2) – расстоянием между ОТСС и условной границей, за пределами которой невозможен эффективный прием вследствие естественного снижения уровня излучаемого сигнала. Значение R2 рассчитывается по результатам специальных исследований и задаётся «в сфере», т.е. в трёх измерениях [2].

Канал случайных антенн характеризуется размерами их «зоны 1» (r1, r1’) для сосредоточенных случайных антенн (ССА) и распределенных случайных антенн (РСА). К сосредоточенным случайным антеннам относятся любые технические средства, имеющие выход за пределы контролируемой зоны. К распределенным случайным антеннам относят провода, кабели, элементы конструкций здания и т.п. Расстояние между ОТСС и СА, на котором невозможен эффективный перехват, определяет размер зоны 1 (так же «в сфере»).

ОТСС считается защищенным от утечки за счет ПЭМИН, если:

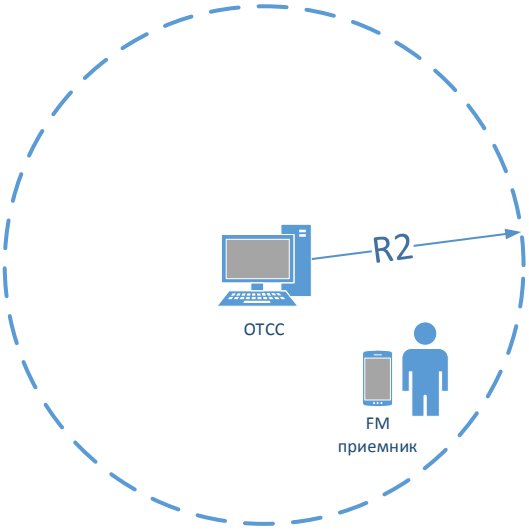
- радиус зоны 2 для любого устройства, входящего в его состав и в любом режиме функционирования, не превышает минимально допустимого расстояния от ОТСС до границы КЗ;
- радиус зоны 1 для любого устройства, входящего в его состав и в любом режиме функционирования, не превышает минимально допустимого расстояния от ОТСС до ССА и РСА либо отношение мощностей информативного сигнала нормированной помехи во всех СА не превышает на границе КЗ предельно допустимую величину;
- отсутствуют отходящие от ОТСС коммуникации (выходящие за пределы КЗ) либо отношение мощностей информативного сигнала к нормированной помехе в них на границе КЗ не превышает предельно допустимую величину.

При проведении СИ, в том числе объектовых устанавливаются уровни ПЭМИН исследуемого объекта ОТСС, а также частоты информативных сигналов, определяется энергетика сигналов, вычисляются границы зоны R2. В соответствии с идеологией Soft Tempest даже после проведения подобных мероприятий вредоносное СПО может остаться необнаруженным и продолжать скрытное излучение информативного сигнала в пределах зоны R2. Это может произойти поскольку современные комплексы «Навигатор», «Легенда» и «Сигурд» в режиме автоматического сканирования определяют пиковые (квазипиковые) значения уровней электромагнитных излучений, при тестовых режимах работы ОТСС, что позволяет грамотно определить зону R2, но не позволяет сделать вывод о наличии программной закладки в ОТСС. Обнаружить вредоносное ПО так же не позволяет и специальный программный контроль в рамках специальных проверок, который не предполагает поиск ПЭМИН в соответствии с технологией Soft Tempest.

А субъект исследования довольно опасен с практической точки зрения, так одной из мер защиты от НСД является физическая изоляции локальной вычислительной сети организации от сетей общего пользования. В последние годы была продемонстрирована возможность проникать и в изолированные ЛВС, с этой задачей успешно справился Stuxnet[3]. ПЭМИН сформированный по технологии Soft Tempest является одним из вариантов обратной связи в изолированных ЛВС.

1. Модель атаки

Любая автоматизированная система излучает побочное электромагнитное излучение, которое может являться физической основой для передачи информационного сигнала. Управляя различной периферией АС можно добиться полного контроля над ПЭМИН. Задача Soft Tempest в сложных многокомпонентных вредоносных программах – сформировать ТКУ информации от объекта ОТСС, рассмотрим, как он формируется за счет пренебрежения организационными мерами безопасности.



Как показано на рисунке, источником ПЭМИН является ОТСС с установленным на нем вредоносным СПО. Далее электромагнитное излучение распространяется в пределах зоны R2 и принимается FM приемником мобильного телефона, внесенным зону R2.

Радиоприемники в мобильных телефонах, впервые появились примерно в 1998 году и стали популярны с появлением современных смартфонов. Сегодня большинство крупных производителей встраивают FM-приемники в свои продукты.

Компания Microsoft объявила о поддержке радиоприемников в обновлении Windows Phone 8. Из почти 700 млн смартфонов, проданных Nokia в 2012 и 2013 годах, две модели (Lumia 520 и Lumia 920) оснащены радиоприемниками с FM демодуляцией сигналов. Среди смартфонов на базе Android более 450 моделей поддерживают FM-радиоприемники. FM-радиоприемники также интегрированы во многие мобильные телефоны низкого ценового сегмента и различные медиа-плееры.

При нынешней популярности тенденции "Bring Your Own Device" (BYOD), сотрудники организаций, часто вносят и выносят мобильные телефоны в пределы контролируемой зоны. А поскольку зона R2 визуально не обозначена в её пределы смартфон попадет автоматически. Сотрудники организаций знают о правилах «не пользоваться телефонами на объектах ОТСС», но в понимании большинства это значит не звонить по телефону, чтобы не создавать канал утечки акустической информации. Про автономную регистрацию радиосигналов владельцы смартфонов в большинстве своём не задумываются.

Таким образом атака состоит из трех основных этапов:

1) Установка вредоносного код на объекте ОТСС;
2) Заражение вредоносным кодом смартфонов сотрудников организаций;

3) Обнаружение излученных электромагнитных сигналов и передачи их злоумышленникам.

Хоть данная модель и выглядит сложной, она является реализуемой при должном упорстве со стороны злоумышленников.

Установка вредоносного код на объекте ОТСС

Заражение изолированной системы это самый трудоемкий для злоумышленника этап. Как показывает практика, Stuxnet показал некоторые из возможных векторов атаки. К ним относятся варианты распространения вредоносного кода через неучтенные съемные носители (флешки), USB подключение тех же смартфонов к ОТСС (для зарядки), а также установка стороннего программного обеспечения или аппаратных компонентов с некачественно проведенной специальной проверкой или её отсутствием.

Разумно предположить, что информация о большинстве подобных случаев не опубликованы. После того, как враждебный код выполняется на одном узле ЛВС, составляющую ОТСС, но может распространяться дальше и инфицировать другие узлы.

2. Заражение вредоносным кодом смартфонов сотрудников организаций

Что касается мобильных телефонов, массив векторов атак значительно шире. Эти устройства подключены к внешнему миру через множество интерфейсов, таких как сотовые сети, Bluetooth, Wi-Fi, и физические соединения с другими девайсами.

Скорее всего, злоумышленник попытается найти и заразить мобильные телефоны тех сотрудников в целевой организации, кто, с наибольшей вероятностью, работает в непосредственной близости от объектов ОТСС.

Подготовкой к этому этапу может служить интеллектуальный анализ данных о сотрудниках и организации, данные из социальных сетей, фишинг и другие методы социальной инженерии. Мобильный телефон может быть заражен через Интернет, после посещения зараженных сайтов, сообщением по электронной почте с вредоносными вложениями, или непосредственно путем установки вредоносных приложений.

Другие способы инфицирования заключаются в физическом доступе к смартфону и поиску различных уязвимостей (SMSит.д.).

Так же, стоит заметить, что программная составляющая смартфона не просто круглосуточно регистрирует электромагнитное излучение, а может наделяться более интеллектуальными функциями. Среди которых отложенная передача накопленной информации, только с использованием Wi-Fi соединений, для экономии сетевого трафика

и энергоэффективности. Интеллектуальная функция мониторинга ПЭМИ от ОТСС: мониторинг по расписанию (только в рабочие часы), мониторинг на основе анализа окружающих сигналов (вышки сотовой связи, ID беспроводных точек доступа) или с использованием геолокации (по результатам GPS/ГЛОНАС). Команда на запись обнаруженного сигнала может поступить по каналу управления на смартфон через интернет. ПО на смартфоне так же может анализировать записанные данные и получать другие команды управления от злоумышленников.

3. Процесс формирования ПЭМИН ОТСС

Генерация радиосигналов от видеокарт обсуждалась в ряде работ и технических статей [4] [5] [6].

Основным исходным параметром для расчета несущей частоты излучаемого радиосигнала является частота тактового сигнала пикселей, передающихся на экран. Частота пикселей представляет собой частоту, с которой пиксели передаются на экран, так что бы полный кадр пикселей соответствовал одному циклу обновления.

Она может быть рассчитана с помощью простого умножения:

$$(\text{H пикселей} + \text{H Sync})\ (\text{V пикселей} + \text{V Sync})\ (\text{Rr}) = \text{PC},$$

где $\text{H}_{\text{пикселей}}$ и $\text{V}_{\text{пикселя}}$ разрешение по вертикали и горизонтали (например, 1024 и 768), $\text{V}_{\text{синхронизации}}$, $\text{H}_{\text{синхронизации}}$ являются длинами вертикальной и горизонтальной синхронизации (в пикселях), Rr частота обновления (например, 60 Гц) и PCчастота тактового сигнала пикселей. Эти параметры определяются в соответствии с параметрами дисплея.

Как правило, и в аналоговых и цифровых стандартах, пиксельное временя определяется главным образом разрешением экрана и частотой обновления. С учетом стандартов графических карт, можно сконструировать шаблон изображения, который, будучи отправленным на дисплей будет генерировать несущую, модулированную информационным сигналом.

В случае аналогово интерфейса изменение изображения происходит непосредственным изменением напряжение сигнала необходимым для изменения цвета пикселей. Амплитудная модуляция (АМ) является очевидным выбором для передачи данных ко каналу ПЭМИН в этом случае.

Для цифровых интерфейсов постепенное изменение оттенков пикселей в течение фиксированного времени обеспечит формирование несущего сигнала.

Проведенные исследования показали возможность преднамеренной генераций радиосигналов, промодулированных информационным сигналом, по средствам использованием мониторов и видеоадаптеров.

Целью исследования является передача FM радиосигналов, которые будут получены и обработаны FM-приемником мобильного телефона. FM радиосигналы генерируются построением изображения из чередующихся последовательностей черных и белых пикселей, которые отражают требуемую несущую частоту модуляции. FM модуляция, может использоваться для создания максимальной, фиксированной амплитуды ПЭМИН необходимой для стабильной генерации информационного сигнала.

Дальнейшие исследования направлены на выявления количественных показателей сформированного ТКУ, таких как пропускная способность, длина и информативность.

Список литературы

1. Markus G. Kuhn. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, 1998. Available at: http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf, accessed 20.03.2015.
2. Пятачков А.Г. Защита информации, обрабатываемой вычислительной техникой, от утечки по техническим каналам. Воронеж: НП РЦИБ «Факел», 2007. 190 с.
3. ISBN 1553-572X. Stuxnet Worm Impact on Industrial Cyber-Physical System Security. Stamatis Karnouskos. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6120048, accessed 20.03.2015.
4. ISBN 978-1-4799-7328-6 Mordechai Guri. AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6999418, accessed 20.03.2015.
5. B. Kania. VGASIG: FM radio transmitter using VGA graphics card. Available at: http://bk.gnarf.org/creativity/vgasig/vgasig.pdf, accessed 20.03.2015.
6. Хорев А.А. Оценка возможности по перехвату побочных электромагнитных излучений видеосистемы компьютера. Ч. 2 // Специальная техника. 2011. № 4. С. 51–62.