Как взломать изолированный компьютер

Пока что эти атаки – в основном страшилки, но за последние годы были обнаружены образцы вредоносного ПО, способного проникать за «воздушный зазор».

Как говорится в старом анекдоте о мерах профилактики СПИД, «и главное – никаких контактов» Особо чувствительные компьютерные системы – военные, финансовые, правительственные и т.д. – защищают от киберугроз физической изоляцией от Интернета и локальных сетей (air-gapping). Но хакеры проникают и туда, обычно при помощи съемных носителей, о чем время от времени сообщается в новостях. Для кражи информации есть и более экзотические методы, использующие скрытые радиоканалы, акустические колебания и даже изменения температуры.

«СиБ» решил выяснить, что собой являют атаки на изолированные системы и как от них можно защититься.

Роковой разъем

Наиболее очевидный способ проникнуть в изолированную сеть – использовать USB-носитель. Именно так произошла самая известная на данный момент атака ***Stuxnet***, когда «крот» пронес зараженную флешку на ядерный объект в иранском Натанзе. Если верить документам, опубликованным Wikileaks в 2017 году, доставка вредоносного ПО через USB – довольно распространенная тактика из арсенала ЦРУ. Тогда речь шла о пакете под названием ***Brutal Kangaroo***, включавшем в себя несколько программ, которые обеспечивали цепочку атаки. Она начиналась с заражения подключенного к Интернету компьютера («первичного хоста»). Затем, когда пользователь вставлял флешку в эту машину, носитель заражался отдельным ПО под названием Drifting Deadline / Emotional Simian, которое и переносилось через воздушный зазор посредством этой флешки. Схема именно такой атаки представлена на **рис. 1.**

Интересно, что спецслужба использовала уязвимость в Windows, которая позволяла заражать компьютер, если пользователь просто просматривал в Windows Explorer список файлов на флешке, даже не открывая их (позже Microsoft эту уязвимость закрыла).

Другой способ – заразить доверенную организацию (например, поставщика ПО), которая может доставить вирус в изолированную систему, сама при этом являясь более легкой целью

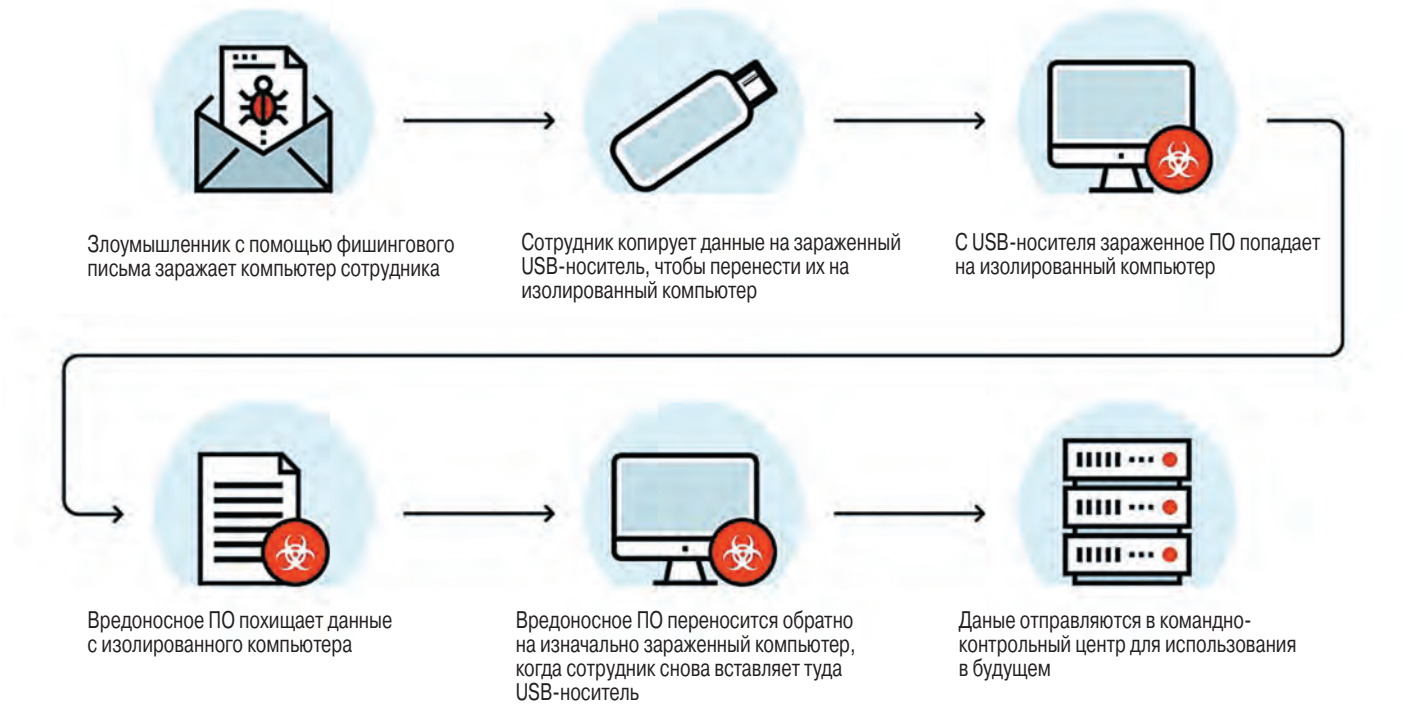

Рис. 1. Взлом изолированного компьютера с помощью USB-носителя (источник: Trend Micro)

для атаки. Этот метод использовался на втором этапе атаки Stuxnet, когда заражение происходило через пять иранских фирм-подрядчиков (упрощение механизма распространения привело к тому, что в конечном итоге Stuxnet вышел из-под контроля и был выявлен «в дикой природе»).

В 2016 году было обнаружено вредоносное ПО, получившее название ***Project Sauron*** (имя главного злодея «Властелина колец» встречалось в исходном коде), тогда как APT-группу, стоявшую за этой кампанией, назвали ***Strider***. ***«Лаборатория Касперского»*** нашла образцы Sauron в 30 организациях в России, Иране и Руанде, ***Symantec*** обнаружила его в других странах, в том числе в китайской авиакомпании и в неназванном посольстве в Бельгии.

Обе компании тогда высказывали предположение, что за атаками может стоять одна из ведущих мировых держав, причем Евгений Касперский в конце 2017-го прямо обвинил США, назвав расследование его компанией хакерских операций ЦРУ причиной неприязни американских властей. Сайт CyberScoop со ссылкой на двух бывших сотрудников американской разведки писал, что Sauron был делом рук не США, а одной из стран-союзниц. После огласки хакерская группа больше никак себя не проявляла – наоборот, все вредоносное ПО было с компьютеров жертв убрано.

Sauron использовался для шпионажа и умел воровать пароли, ключи шифрования, файлы конфигурации и т.п. Вирус не оставлял каких-либо характерных артефактов, атакуя каждую систему новым способом, пути вывода информации также могли отличаться. Из-за этого было сложно определить уникальные индикаторы компрометации и искать признаки заражения других систем. В контексте этой статьи важно, что Sauron, по-видимому, также умел проникать в изолированные системы. На специально подготовленном USB-носителе создавался скрытый раздел размером в несколько сотен мегабайт, где находилась виртуальная файловая система, которая содержала вредоносное ПО и куда затем перебрасывались данные.

В 2018 году американский Департамент внутренней безопасности обвинил власти России в атаках на критическую инфраструктуру США. Как сообщалось, хакерская группировка ***Dragonfly*** (она же ***Energetic Bear***) проникла в энергосистему страны, заразив поставщиков оборудования, для чего злоумышленники использовали направленные фишинговые атаки и «заминированные» веб-страницы. Воспользовавшись тем, что поставщики имеют удаленный доступ для техподдержки и установки патчей, хакеры собирали информацию об энергосистеме США и также могли влиять на работу оборудования («переключать тумблеры»). Кроме того, они могли проникать в изолированные системы, расположенные в диспетчерских комнатах.

Год назад наделала шороху атака на Кундакуламскую атомную электростанцию, что в индийском штате Тамил-Наду. В сентябре 2019-го исследователь Пухрадж Сингх проинформировал власти страны о выявленном вредоносном ПО под названием ***Dtrack***, которое успешно поразило «исключительно критичные цели» на электростанции. Сингх даже охарактеризовал случившееся как «casus belli в индийском киберпространстве». «Лаборатория Касперского», которая расследовала инцидент, сообщила, что Dtrack позволял загружать файлы на зараженный компьютер, выполнять злонамеренные команды, передавать информацию на сервер, контролируемый хакерами, и многое другое. За атакой предположительно стояла организация ***Lazarus Group***, которая, как считается, работает на правительство Северной Кореи.

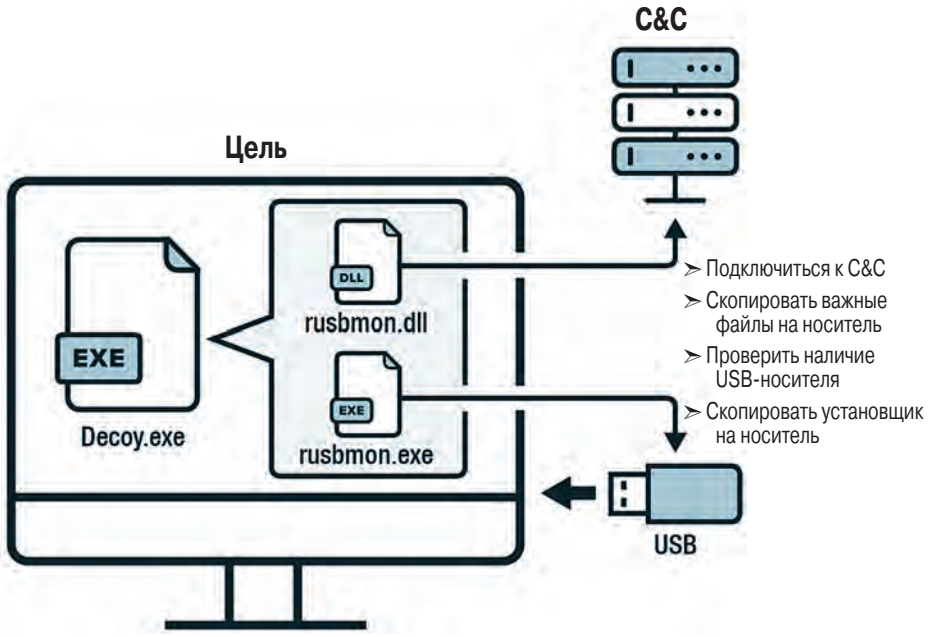

Рис. 2. Первый этап атаки USBferry (схема Trend Micro)

Корпорация ядерной энергетики Индии опубликовала пресс-релиз, в котором говорилось, что системы управления индийских АЭС не подключены к внешним компьютерным сетям и Интернету, соответственно никакие атаки на них не возможны. Когда эта попытка тотального отрицания дала обратный результат, корпорация все же признала, что кибератака имела место, но заражен был подключенный к Интернету компьютер, используемый для административных целей, а критические системы не пострадали. Однако сайт The Hacker News считает, что Dtrack мог быть лишь первым этапом более обширной атаки, и его целью мог быть сбор информации об используемом на объекте оборудовании. Располагая этими сведениями, преступники могли бы затем определить возможные пути проникновения в изолированную часть, но атака была вовремя раскрыта. Впрочем, индийские власти так и не сообщили, какие данные хакерам удалось украсть.

В мае нынешнего года компания ***Trend Micro*** сообщила о возобновлении активности группы ***Tropic Trooper***, которая атаковала изолированные компьютерные сети тайваньских и филиппинских военных, целями также стали правительственные организации и даже национальный банк одной из стран. Преступники использовали «троян» под названием ***USBferry***, который скрытно ворует информацию с помощью USB-накопителя.

Зная, что в военных и государственных организациях действует жесткая дисциплина доступа к изолированным сетям (например, использование биометрической аутентификации или проверка USB-носителей в карантинных машинах), преступники атаковали связанные с ними и потенциально незащищенные учреждения, которые могли послужить отправной точкой. Например, в одном из случаев таковой послужил военный госпиталь, откуда вирус был занесен в изолированную среду армейской структуры.

Исследователи обнаружили, что цепочка атаки USBferry начиналась с файла-установщика, который передавался по электронной почте, связывался с командно-контрольным центром (C&C) и скачивал свои компоненты, зашифрованные в графическом файле методом стеганографии, то есть с сокрытием самого факта шифрованной передачи (**рис. 2**). USBferry пытался определить, подключен ли к компьютеру USB-носитель, и записать туда свой установщик. С помощью команд ping и tracert программа выясняла, имеет ли машина доступ к локальной сети, и определяла топологию последней. Если оказывалось, что сеть недоступна, она записывала собранную информацию на флешку.

Также в мае компания ***ESET*** опубликовала результаты исследования еще одного вредоносного ПО под названием ***Ramsay***, которое предназначено для кражи ценных документов и может работать в изолированных сетях. Образец ПО был впервые загружен из Японии. Малое количество обнаруженных жертв свидетельствует о том, что ПО все еще находится в разработке, но также может быть связано с тем, что ПО предназначено для поражения изолированной инфраструктуры. Отдельные признаки указывают на группу ***Darkhotel***, которая давно известна своими атаками против государственных органов Японии и Китая, однако метки времени показали, что данная конкретная программа разрабатывается или разрабатывалась с конца 2019 года.

Вирус распространяется через зараженные документы и также может маскироваться под установщик 7zip. В отличие от традиционного вредоносного ПО, Ramsay не делает попыток связаться с командно-контрольным центром, а ищет файлы управления в файловых хранилищах и на съемных носителях. Корреляция между тем, какие носители Ramsay сканирует для последующего распространения самого себя и для вывода похищенных документов, свидетельствует о том, что программа рассчитана на работу в изолированных сетях.

Вывоз награбленного

Одно дело доставить вредоносный код по назначению. Если целью атаки является не разрушение, как у Stuxnet, а шпионаж, остается задача переправки похищенной информации к конечным бенефициарам. Лучше всего, когда есть инсайдер, который может просто скачать и вынести файлы с объекта. Если же его нет, вывод информации через USB может быть проблематичным.

С другой стороны, передачу информации между двумя компьютерами можно осуществить и прямым путем, используя различные физические явления. Исследованиями в этом направлении занимается группа под руководством Мордехая Гури из Университета Бен-Гуриона, которая регулярно публикует результаты испытаний различных скрытых каналов передачи. В большинстве экспериментов в качестве приемного устройства используется другой ПК или смартфон, который лежит на небольшом расстоянии от

Рис. 3. Fansmitter: зараженный компьютер без динамиков и с отключенными аудиовыходами (A) передает данные на мобильный телефон (B) посредством акустических сигналов (рисунок из статьи Мордехая Гури и др.)

изолированного компьютера. Группа Гури исходит из того, что и компьютер, и приемник уже заражены шпионским ПО. Инфицирование мобильного телефона, отмечают ученые, намного более простая задача, которая может быть реализована с помощью разных векторов атаки (почта, SMS, вредоносные приложения и т.д.). Предполагается, что полученные данные телефон затем передает хозяевам через Wi-Fi или сеть мобильной связи.

Особенно много работ посвящено использованию аудиоканала. Как отмечается в работах группы Гури, типичная политика безопасности предусматривает запрет использования динамиков и микрофонов на изолированном компьютере для создания «звукового зазора» (audio-gap). Это обеспечивается как физическим отсоединением соответствующего оборудования, так и закрытием его поддержки в BIOS во избежание случайного подключения динамиков через линейные разъемы. Однако израильские ученые придумали несколько инструментов, которые позволяют это обойти.

Например, передачу данных с помощью звука без динамиков обеспечивает программа ***Fansmitter***. Это достигается путем управления скоростью вращения вентилятора центрального процессора и других кулеров внутри ПК, что позволяет генерировать модулированный акустический сигнал. В качестве приемника используется мобильный телефон, расположенный на расстоянии до 8 м (**рис. 3**), скорость передачи данных может достигать 900 бит/ч. Поскольку шум вентиляторов различим человеческим ухом, для обеспечения скрытности можно использовать нижнюю часть диапазона или близкие по частоте несущие, а также передавать в то время, когда за компьютером никто не работает.

Также передачу данных с помощью акустических сигналов обеспечивает свежая разработка под названием ***POWER-SUPPLaY***. Эта программа манипулирует загрузкой центрального процессора и частотой переключения блока питания, тем самым генерируя модулированный сигнал в диапазоне 0–24 кГц. В ходе экспериментов информация передавалась в формате WAV с максимальной скоростью 50 бит/с, приемником служил смартфон, расположенный в 2,5 м от ПК. При этом вредоносный код сам по себе не требует доступа к аппаратной части или прав администратора.

Работа под названием ***MOSQUITO*** посвящена передаче данных между двумя ПК с использованием динамика в роли микрофона. В современных материнских платах есть возможность программного переключения аудиовыхода для работы на прием, а конструкция динамика позволяет преобразовывать как электрические сигналы в звуковые, так и наоборот, хотя в последнем случае качество звука будет невысоким. В работе рассматривались разные сценарии передачи данных. При обмене между двумя встроенными динамиками теоретическая емкость канала на расстоянии от 1 до 8 м составляла 1200–1800 бит/с на частотах до 18 кГц, но деградировала до 300–600 бит/с при переходе на суб-басы (до 60 Гц) и ближний ультразвук (свыше 18 кГц), поскольку громкоговорители пользовательских ПК оптимизированы под человеческое ухо. Если передача осуществлялась с динамика на пассивное устройство (наушники, головные телефоны и ушные вкладыши), скорость в большинстве случаев также составляла 300–600 бит/с. Рассматривался и вариант передачи между двумя парами наушников, но в этом случае дальность оказалась ограничена тремя метрами, а скорость – 250 бит/с.

Еще несколько исследований посвящены оптическим каналам. Например, ***LED-it-GO*** – механизм передачи сигналов через индикатор работы жесткого диска. Скорость передачи данных при этом может достигать довольно приличных 4000 бит/с. Модуляция происходит посредством команд чтения и записи. В качестве приемника может использоваться, например, скрытая камера, сенсор или просто мобильный телефон, если в деле участвует инсайдер. В ином случае можно снимать через камеру высокого разрешения за пределами здания (**рис. 4**), взломанную камеру видеонаблюдения либо с беспилотника (впрочем, авторы предупреждают, что этот вариант годится лишь для съема небольших объемов информации наподобие ключей шифрования).

Этот способ сам по себе является скрытным, поскольку на мигание индикатора HDD обычно никто не обращает внимания; более того, используемая частота мерцания 5800 раз в секунду далеко превышает предел восприимчивости глаза.

Одна из самых перспективных разработок – ***USBee*** – обеспечивает передачу данных с помощью электромагнитного излучения подключенного USB-устройства. Исследователи приметили, что запись на флешку последовательности двоичных нулей генерирует заметное электромагнитное

Рис. 4. LED-it-GO: скрытая камера, расположенная на расстоянии 8 м, смотрит на индикатор HDD в центре картинки (рисунок из статьи Мордехая Гури и др.)

излучение в диапазоне 240–480 МГц, что обусловлено резкими перепадами напряжения в соответствии с используемым в USB кодом NRZI (без возвращения к нулю с инверсией).

Соответственно передача данных осуществляется путем отправки двоичных последовательностей на флешку или вообще любое подключенное USB-устройство, в результате чего порождается модулированное электромагнитное излучение. Процесс передачи не требует никаких особых привилегий – достаточно разрешения на создание файлов в системе съемного носителя. В ходе эксперимента двоичный код записывался в такой временный файл, при этом использовалась двоичная частотная манипуляция B-FSK. На приемной стороне использовался демодулятор на базе открытой платформы обработки сигналов GNU Radio. Сообщается, что данные могут передаваться со скоростью от 20 до 80 бит/с.

Для нейтрализации утечки через электромагнитное излучение используют клетку Фарадея – металлическую оболочку, в которую может быть заключено важное оборудование или целое помещение. Поэтому израильские ученые разработали механизм под названием ***ODINI***, основанный, по их утверждению, на использовании магнитного поля, которое образуется вокруг центрального процессора. Магнитное поле быстро ослабевает с удалением, но все же в 2004 году была предложена технология связи на малых расстояниях с помощью магнитной индукции (near-field magnetic induction communication). В частности, анализ показал, что колебания магнитного поля частотой до 50 Гц легко проникают сквозь металлические корпуса компьютеров и клетки Фарадея. Управляя загрузкой CPU и соответственно протекающими в нем токами, можно модулировать магнитное поле, которое этими токами порождается. Авторы предлагают несколько способов генерации сигнала: загрузка незадействованных ядер процессора обеспечивает желанную скрытность, варьирование количества «передающих» ядер позволяет использовать амплитудную манипуляцию, а управление загрузкой каждого ядра индивидуально – использовать более эффективные виды модуляции, такие как OFDM.

Для приема данных использовался магнитный датчик ***Honeywell*** – цифровой магнетометр, умеющий измерять силу и направление магнитного поля в пространстве. В ходе эксперимента удалось передать информацию с ноутбука на максимальное расстояние 50 см, со стационарного компьютера – на 100 см, с сервера – на 150 см. Теоретическая пропускная способность канала передачи с ПК и сервера, в зависимости от расстояния, составляет от 30 до 300 бит/с (для ноутбука она оказалась еще меньше по причине слабости генерируемого им поля). С другой стороны, тесты показали, что на расстоянии 100 см реальная скорость будет всего 1 бит/с, тогда как показатели 10 и 40 бит/с достигались, лишь когда приемник и передатчик находились на расстоянии 5–20 см.

Достоинством метода является его незаметность, поскольку он не требует исполнения каких-то особых инструкций процессора или специальных вызовов API, поэтому антивирусу трудно обнаружить злонамеренное поведение. Кроме того, канал передачи работает и в виртуализированной среде, которая нередко используется как дополнительное средство изоляции: тесты показали корреляцию сигналов, генерируемых из виртуальной машины и напрямую из ПК.

Разновидность этого метода под названием ***MAGNETO*** предполагает использование для приема сигналов не «жучка», а магнитного датчика мобильного телефона, который, как отмечают авторы, вообще не считается интерфейсом связи, а используется лишь для ориентации и позиционирования и поэтому остается включенным даже в режиме полета (airplane mode). Принятые данные затем декодируются и передаются на компьютер инициатора атаки по Wi-Fi или мобильной связи. Впрочем, результаты не слишком «обнадеживающие»: исследователям удалось достичь скорости передачи 5 бит/с с нулевым коэффициентом ошибок, лишь когда телефон находился в непосредственной близи от передающего компьютера (0–3 см), тогда как на 12,5 см скорость 1 бит/с сопровождалась 20% ошибок. Авторы «полагаются» на то,

что пользователи зачастую кладут мобильный рядом со своим рабочим ПК, что и обеспечит утечку данных.

И это далеко не все способы атак изолированных систем, которые придумали израильские ученые. Другие, не менее причудливые разработки включают использование проводки электропитания, выделяемого компьютерами тепла (причем возможен как прием информации, так и передача команд с одного ПК на другой), вибрации вентиляторов и многое другое.

Защита воздуха

Как защититься от всех этих напастей? Прежде всего, компьютер никогда и ни при каких условиях не должен подключаться к Интернету. Во-вторых, специалисты рекомендуют крайне осторожно относиться к USB-носителям, а также к периферийным устройствам (принтеры, сканеры). Один из ведущих экспертов организации SANS Institute Эд Скудис как-то отметил, что «воздушный зазор» – это всего лишь медленный сетевой канал, имея в виду, что USB-устройства могут играть роль моста через этот зазор. Поэтому флешки необходимо тщательно проверять, например, с помощью аппаратного сканера (USB kiosk). Рекомендуется проверять поставщиков ПО, поскольку через них тоже возможно заражение. Отдельное направление – работа с персоналом: его необходимо обучать основам кибербезопасности, уделяя особое внимание приемам социальной инженерии, которые используются в фишинговых атаках. Кроме того, стоит вести учет действий сотрудников для отслеживания подозрительной активности.

Другая очевидная мера – вообще запретить пронос мобильных телефонов в помещения, где находятся изолированные компьютеры. Пространство лучше разделить на зоны, где можно/нельзя использовать мобильные телефоны, микрофоны и другое электронное оборудование, причем опасность представляют не только смартфоны, но и обычные кнопочные трубки (feature phones), а также устройства IoT, которые могут быть легко взломаны.

Если зонирование непрактично или невозможно из-за ограниченного пространства или по другим причинам, можно применять другие ограничительные меры. Команда Гури описала основные пути противодействия рассмотренным ею же приемам атак. Например, чтобы исключить передачу сигналов через блок питания, помогут аппаратные детекторы и глушители сигналов. Против модуляции звука вентиляторов можно задать регулирование скорости оборотов драйверами устройств. Также можно установить аппаратные детекторы шума, которые отслеживают звуковые частоты в определенных диапазонах, хотя такие устройства могут выдавать ложные оповещения из-за фоновых звуков. Более радикальные меры, такие как изоляция ПК в шумопоглощающем корпусе или замена вентиляторов на жидкостное охлаждение, обойдутся дороже.

Для противодействия попыткам передачи по оптическим каналам рекомендуется размещать оборудование внутри контролируемого периметра. Для отпугивания пригодятся камеры видеонаблюдения, хотя, как говорилось, они сами могут быть взломаны. Также можно просто заклеить окна непроницаемой пленкой. Чтобы уберечься от утечки через LED-индикаторы, можно залепить сами индикаторы, более высокотехнологичное решение – запустить фоновый процесс, который случайным образом инициирует операции чтения-записи для генерации шума.

Обнаружение передачи через излучение USB-устройства – задача похитрее. Для этого нужно отслеживать операции ввода-вывода с целью выявления характерного поведения (например, частого создания временных файлов и записи в них), однако это тоже может генерировать большое количество ложных срабатываний, поскольку такие файлы создаются постоянно добропорядочными программами.

Выявление скрытой передачи путем управления загрузкой процессора и модуляции магнитных волн затруднительно, поскольку для этого требуется отслеживание команд CPU, что серьезно ухудшит производительность. Выявить злонамеренное приложение на мобильном телефоне также может быть непросто, если преступники используют технологии обхода. А контроль девиаций магнитного поля может сопровождаться ложными срабатываниями. Для нейтрализации магнитного канала передачи предлагаются различные варианты глушения (генераторы магнитного поля, гасители поля) и экранирования (ферромагнитные пластины), хотя обойдется это недешево.

Вообще, надо сказать, все эти экзотические каналы передачи пока остаются чистой теорией. О реальных случаях вывода информации через, например, акустику или свет пока не сообщалось; поиск в Google выдает только заголовки вроде «Ученые воруют информацию из изолированных систем» и ссылки на все того же Гури. А методы защиты, как можно видеть, либо сложны и дороги, либо экзотичны и/или непрактичны. Например, едва ли кто-то станет загружать компьютер дополнительными проверками в фоновом режиме, контролировать мерцание индикатора жесткого диска или клавиатуры либо облицовывать комнату ферромагнитными плитами. Атака представляется неправдоподобной, поэтому в защите не видится необходимости. Но если опыты Гури что-то и доказывают, то это разнообразие уязвимых мест, которыми могут воспользоваться злоумышленники, и нельзя исключать, что рано или поздно кто-то это сделает.

Поэтому, советуют знатоки, лучше исходить из предположения, что система может быть взломана, и соответственно строить защиту. Например, шифрование данных не убережет от атаки, но сделает украденную информацию бесполезной для преступников. Информацию можно сегментировать внутри компьютера – например, на виртуальных машинах (есть отдельный подход – «virtual air-gapping»). А средства машинного обучения помогут выявить аномалии в поведении процессов и тем самым предостеречь от проникновении сквозь «воздушный зазор».

Василий ТКАЧЕНКО, **СиБ**