ЛЕКЦИЯ 2. УЯЗВИМОСТИ ИНТЕРФЕЙСА USB И THUNDERBOLT

2.1. УЯЗВИМОСТИ ИНТЕРФЕЙСА USB

Подключение любого устройства через шину USB — дело небезопасное. Уязвимость интерфейса USB позволяет внедрить вредоносный код (BadUSB) непосредственно в микроконтроллер USB-устройства (флешки, клавиатуры и любого другого устройства) — там, где его не обнаружит, увы, ни одна антивирусная программа, даже самая хорошая. Тем, кому есть что терять, эксперты по безопасности советуют просто не пользоваться USB-портами. Вот только для новых Макбуков такая рекомендация нереализуема в принципе — зарядку же нужно подключать!

Скептики могут возразить, что в стандартном адаптере питания вредоносный код не запишешь, ибо некуда. Но это беда поправимая: при желании зарядку можно «творчески доработать» (аналогичная задача по инфицированию iPhone через зарядное устройство была решена уже больше двух лет назад).

Дальше остается только стратегически грамотно поместить такое «троянское питание» для публичного использования в каком-нибудь публичном месте. Или подменить зарядку жертвы, если речь идет об адресной атаке.

2.1.1. BadUSB

BadUSB — класс хакерских атак, основанный на уязвимости USB-устройств. Благодаря отсутствию защиты от перепрошивки в некоторых USB-устройствах, злоумышленник может видоизменить или полностью заменить оригинальную прошивку и заставить устройство имитировать любое другое устройство.

Программа BadUSB устанавливается в прошивку периферийного устройства и полностью берёт под контроль компьютер при подключении к нему по USB. На компьютере жертвы BadUSB творит что угодно, в том числе видоизменяет файлы, которые устанавливаются в системе, и перенаправляет интернет-трафик на произвольные адреса, изменив DNS-записи. Зловред всегда может выдать себя за клавиатуру и ввести произвольные команды.

Установленная на компьютере программа может изменить прошивку по USB, а та, в свою очередь, может установить зловреда в системе. Из-за такого двустороннего взаимодействия ни одному устройству и компьютеру больше нельзя доверять. Вы не только должны ограничить свой ПК от посторонней периферии, но и сами не можете безопасно вставить чистую флэшку в посторонний ПК.

Поскольку код находится в прошивке, его довольно трудно обнаружить и удалить.

Самая действенная защита — вообще запретить подключение к компьютеру новых USB-устройств: флешек, мышек, клавиатур, смартфонов и других приборов. А в будущем производители обязаны будут чётко указывать, какие конкретно микросхемы установлены в их устройствах. Как вариант, можно использовать криптографическую проверку обновлений прошивки.

BadUSB пользуется тем фактом, что производители не защищают свои устройства от перепрошивки, а хосты не проверяют USB устройства на подлинность. Благодаря этому злоумышленник может подменить прошивку микроконтроллера и выдать одно устройство за другое. Также, так как все коммуникации ведутся через этот микроконтроллер, злоумышленник может перехватывать и подменять любые данные и команды между устройством и хостом. Возможно и автоматическое заражение устройств: устройство заражает хост, запуская на нём вредоносное ПО, затем хост автоматически заражает все подключенные к нему USB устройства.

Уязвимости подвержены все устройства с незащищенными USB контроллерами на борту: флеш-накопители, вебкамеры, мышки, клавиатуры, андроид-устройства. BadUSB не требует особого программного обеспечения на компьютере жертвы и работает под любыми операционными системами, поддерживающими USB-HID устройства.

Несмотря на то, что ряд средств комплексной антивирусной защиты, такие как ESET Endpoint Antivirus, Kaspersky Endpoint Security, компонент «Родительский контроль» у Dr.Web AV-Desk, позволяют ограничивать доступ к сменным носителям и разрешать активацию согласно «белому списку», в случае с Bad USB, таких мер недостаточно.

Защита от атак BadUSB появилась в Kaspersky Endpoint Security 10, обновлённом 7 декабря 2015 года. Защитные решения Dr.Web с 11-й версии защищают от BadUSB-уязвимости для устройств, имитирующих клавиатуру.

2.1.2. Имитация клавиатуры

Устройство представляется компьютеру жертвы клавиатурой, а по истечении некоторого времени начинает отправлять последовательности нажатий клавиш. В результате злоумышленник может выполнить на компьютере жертвы любые действия, доступные авторизованному пользователю с помощью одной только клавиатуры. К примеру, злоумышленник может загрузить из интернета и запустить вредоносное ПО.

Существенным минусом данного вида атак является отсутствие доступа к информации на экране и, как следствие, отсутствие обратной связи на любые действия со стороны зараженного устройства. Например, злоумышленник не может определить как текущую раскладку клавиатуры, так и произведен ли вход в систему.

2.1.3 Имитация сетевой карты

Устройство представляется компьютеру жертвы сетевой картой и, таким образом, может перехватывать или перенаправлять сетевой трафик. В частности, отвечая на DHCP запрос адресом DNS сервера злоумышленника и не предоставляя шлюза по умолчанию, злоумышленник может перенаправить трафик жертвы: компьютер жертвы будет производить разрешение адреса через DNS сервер злоумышленника, но, в отсутствие шлюза по умолчанию, будет использовать другой, настоящий сетевой интерфейс.

2.1.4. Boot Injection

Устройство с достаточным местом для хранения вредоносного кода, например,

флеш-накопитель, может определить момент включения компьютера и в момент определения BIOS'ом выдать на загрузку вирус для заражения операционной системы. Это становится возможным благодаря тому, что по поведению хоста при общении с USB микроконтроллером возможно определить ОС хоста, в частности Windows, Linux, MacOSX, а также BIOS.

2.1.5. Выход из виртуального окружения

Атака использует возможность повторной инициализации устройства. Выполняясь в виртуальной машине, вирус заражает любое подключенное по USB устройство. Зараженная прошивка выполняет переинициализацию и представляется двумя независимыми устройствами: неким новым и тем, которое уже было подключено к виртуальной машине. Новое устройство будет автоматически подключено к хостовой ОС, а старое — обратно в виртуальную машину. Таким образом, может быть произведен выход за пределы виртуального окружения, то есть осуществлен переход от клиентской до хостовой ОС.

2.1.6. Разработка зараженной прошивки BadUSB

Обратная разработка и модификация прошивки подразумевает получение ее исходной копии. Для этого USB-Flash накопитель надо перевести в служебный режим с помощью инженерной утилиты, или просто закоротив определённые контакты в момент подключения.

Оригинальная прошивка занимает не весь отведённый для неё объём, поэтому увеличение размера микрокода после добавления новых функций не стало проблемой.

По результатам реверс-инжиниринга создается альтернативная прошивка с открытым исходным кодом. Её можно записать на любой USB-Flash носитель с соответствующим контроллером, превратив его в хакерский инструмент.

При подключении к компьютеру такая флэшка с модифицированной прошивкой может опознаваться как другое устройство и скрыто выполнять функции, предусмотренные атакующей стороной.

2.1.7. USB KeySniffer

Клавиатуры с беспроводным подключением от некоторых крупных производителей уязвимы для перехвата нажатий клавиш. Из-за того, что в таких устройствах используются незашифрованные протоколы радиосвязи, киберпреступники могут увидеть все, что печатает жертва, с расстояния 75 метров.

Уязвимые (и, как правило, дешевые) беспроводные клавиатуры передают нажатия клавиш на USB-ключ вообще без какого-либо шифрования.

Атака KeySniffer позволяет перехватить любые символы — логины и пароли, номера кредитных карт и другую конфиденциальную информацию в виде обычного текста. Более того, злоумышленники могут не только "слушать", но и передавать свои собственные нажатия клавиш, что позволяет им печатать непосредственно на компьютере жертвы. Таким способом хакеры могут устанавливать вредоносные программы и выполнять любые другие действия — как если бы у них был физический доступ к компьютеру.

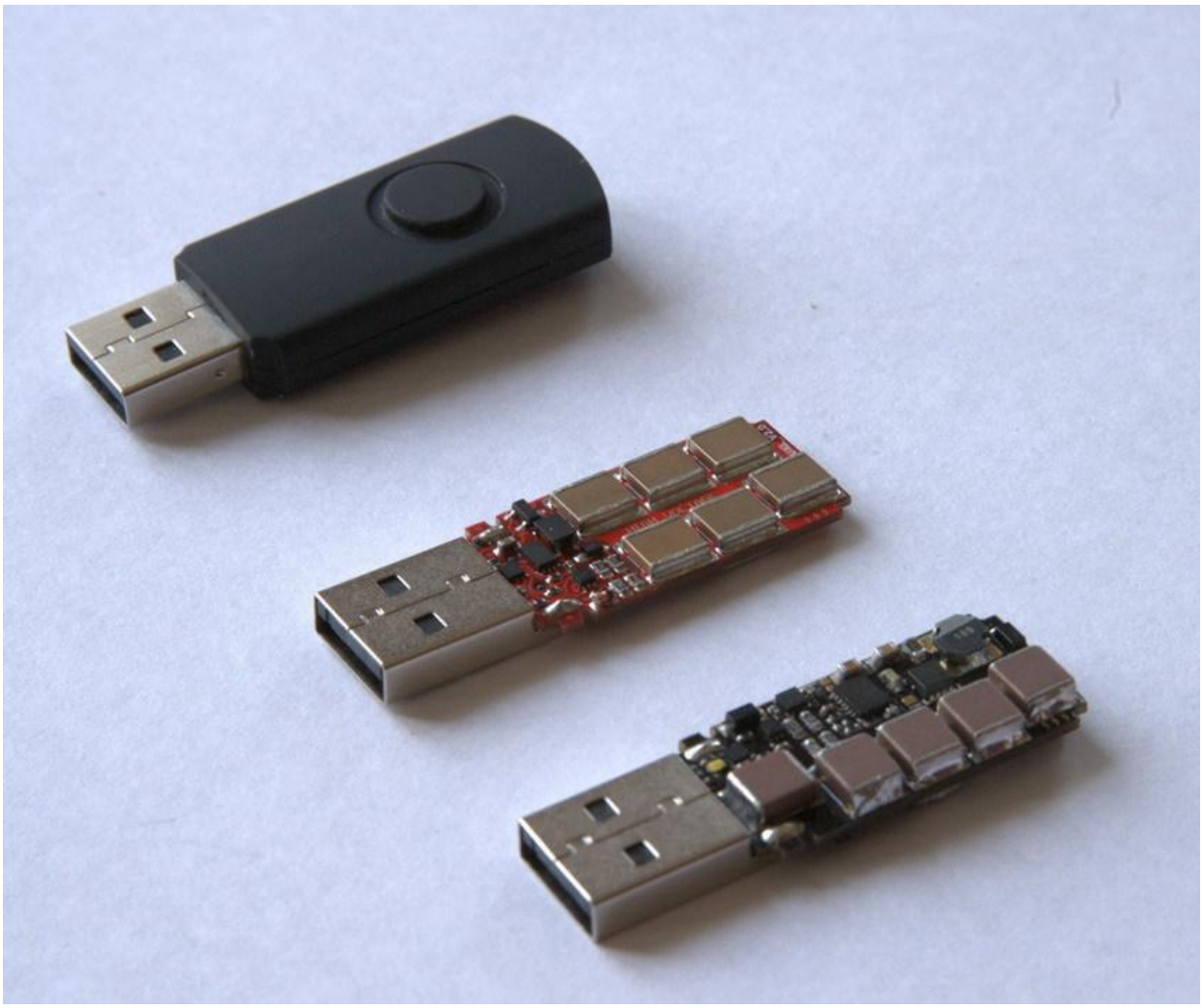
С расстояния 75 метров атаку можно KeySniffer можно выполнять "со 100-процентной точностью". Уязвимости, в частности, подвержены клавиатуры производства HP, Toshiba, Kensington, Insignia, General Electric, EagleTec, Radio Shack и Anker. При этом

способа установить патч и залатать "дыру" не существует, поскольку продукты этих компаний используют протоколы радиосвязи общего назначения. Обладателям Bluetooth-клавиатур беспокоиться не о чем, поскольку этот протокол передает данные по защищенному радиоканалу.

2.1.8. USB killer

USB killer – это устройства, выполняющего лишь одну функцию, – уничтожение компьютеров и практически любой техники, оборудованной USB Host интерфейсом. Это могут быть практически все смартфоны, TV, роутеры, модемы и т.д.

Основная особенность этого устройства - это “выходное” напряжение в минус 220В. Принцип работы: подключение к USB порту запускает работу преобразователя напряжения, который заряжает конденсаторы до 220В. По достижению этого напряжения преобразователь выключается, и запасённая в конденсаторах энергия подается на сигнальные линии USB интерфейса. После разряда конденсаторов цикл повторяется. Частота импульсов уничтожения: 4-8 раз/сек, импульсный ток при этом: ≥180А. Время накопления напряжения – около 2 минут.



Пока только компания Apple озаботилась защитой своего железа от подобных атак, тогда как устройства сотен других производителей по-прежнему уязвимы. При этом цена защиты в данном случае – это пара центов, которые нужно потратить на оптосоединитель.

2.1.9. Шпионские закладки USB

COTTONMOUTH-I аппаратная закладка на USB, предоставляющая беспроводной мост к целевой сети, а также загрузки эксплойтов на целевой системе. Может создавать скрытый канал связи для передачи команд и данных между аппаратными и программными закладками. При помощи встроенного радиопередатчика может взаимодействовать с другими COTTONMOUTH. В основе лежит элементная база TRINITY, в качестве радиопередатчика используется HOWLERMONKEY. Существует версия под названием MOCCASIN, представляющая собой закладку в коннекторе USB-клавиатуры.

COTTONMOUTH-II аппаратная USB-закладка предоставляющая скрытый канал доступа к сети цели. Данная закладка предназначена для работы на шасси компьютера и представляет собой двухпортовый USB-коннектор на плату. Может создавать скрытый канал связи для передачи команд и данных между аппаратными и программными закладками.

COTTONMOUTH-III аппаратная закладка в USB предоставляющая беспроводной мост к целевой сети, а также загрузки эксплойтов на целевой системе. В основе лежит элементная база TRINITY, в качестве радиопередатчика используется HOWLERMONKEY. Представляет собой блок разъемов(RJ45 и два USB) устанавливаемых на шасси, может взаимодействовать с другими COTTONMOUTH установленными на этом же шасси.

2.2. УЯЗВИМОСТИ ИНТЕРФЕЙСА THUNDERBOLT

Thunderbolt 3 — это технология ввода-вывода, обеспечивающая обмен данными между компьютером и подключенными к нему устройствами на скорости 40 Гбит/с. Технология Thunderbolt 3 объединяет функцию передачи данных, видеовывода и зарядки в одном компактном разъеме. Она обеспечивает более высокую скорость передачи данных, чем Thunderbolt 2 — до 40 Гбит/с при использовании совместимого с Thunderbolt 3 кабеля. Thunderbolt 3 также поддерживает подключение устройств USB 3.1 2-го поколения на скорости до 10 Гбит/с.

Оказывается, подключение через Thunderbolt также весьма небезопасно. Соответствующий сценарий атаки для устройств под управлением Mac OS X продемонстрировал в конце прошлого года исследователь в области безопасности Тремелл Хадсон.

Созданный им буткит Thunderstrike (кстати, первый буткит для яблочной операционной системы) использует функцию загрузки дополнительных модулей прошивки с внешних устройств. Thunderstrike подменяет ключи цифровых подписей в BIOS, которые используются для проверки обновлений, после чего с компьютером можно творить все что заблагорассудится.

Thunderstrike осуществляет контроль над каждым процессом инфицированной системы, что позволяет злоумышленнику фиксировать нажатия клавиш, получать ключи шифрования накопителей, внедрять бэкдоры в ядро OS X и обходить пароли. Удалить Thunderstrike программным методом невозможно, так как зловред управляет ключами цифровых подписей и обновлений. Переустановка ОС не решает проблему, как и замена SSD, — на накопителе зловреда тоже нет.

После публикации исследования Хадсона Apple заблокировала возможность такой атаки в обновлении операционной системы (OS X 10.10.2). Правда, по словам Хадсона, этот патч — всего лишь временное решение. Принципиальная основа уязвимости по-прежнему остается нетронутой, так что история явно ждет продолжения.