КАТАЛОГ ЗАКЛАДОК АНБ (SPIGEL). ЧАСТЬ 1. ИНФРАСТРУКТУРА

Клянчин Александр Иванович

Рассмотрены закладки по версии журнала Spiegel. Представлена теоретическая база программно–аппаратных закладок. Приведено описание закладок, возможность встраивания, вероятные применения. Предложены организационно–технические меры по защите компьютерных ресурсов от закладок в свете современной нормативно–методической базы.

***Ключевые слова**: программные и аппаратные закладки, уязвимость аппаратной платформы, механизмы безопасности, кибербезопасность, кибероружие.*

THE NSA'S SPY CATALOG. PART 1. INFRASTRUCTURE

Alexander I. Klyanchin

The infrastructure NSA implants (reviewed in Spiegel) are considered. The theory of the hardware and software are shown. There are descriptions, implanting features, application of the implants. The organizational and technical measures to protect the computer resources from targeted malware in light of the current regulatory basis are proposed.

***Keyword**: software implant, hardware implant, hardware vulnerability, security controls, information security management, cybersecurity, cyber weapons.*

Введение

Информационно-коммуникационные технологии являются одной из наиболее развивающихся областей науки и технологии на ближайший период. Среди основных проблем ИКТ, требующих принятия комплексных мер, является рост киберпреступности, а также защита от применения кибероружия. Осознавая важность защиты конфиденциальной информации, защиты государственной тайны, а также принимая во внимание миниатюризацию специальных технических средств, которые дают возможность негласного снятия информации с компьютера, необходимо принимать опережающие меры по поиску и исключению программно-аппаратных закладок в устройствах массового применения.

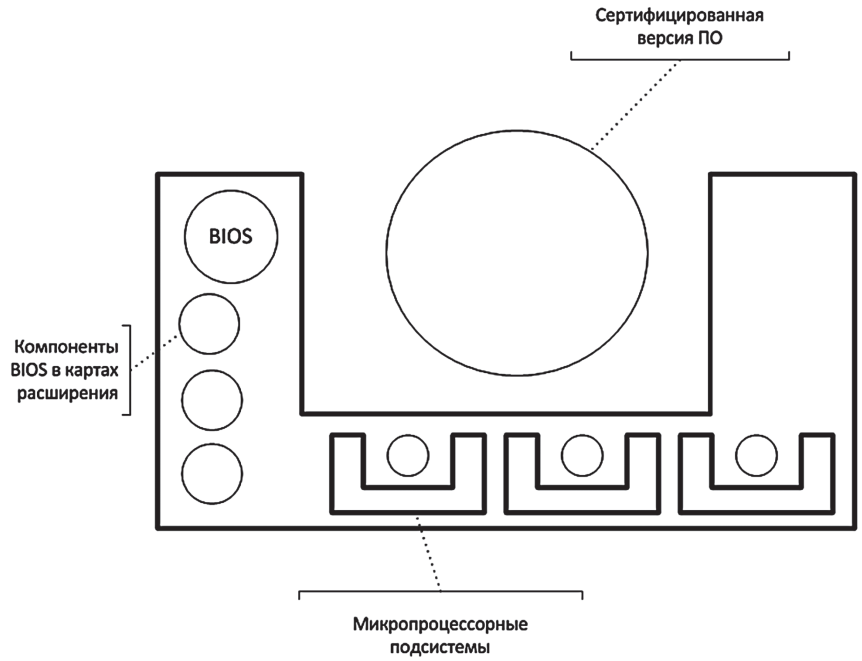


***Рис. 1**. Виды программного обеспечения аппаратной платформы*

Код программного обеспечения выполняется центральным процессором с использованием оперативной памяти (см. Рис. 1. Виды программного обеспечения аппаратной платформы). Существует также так называемый код поддержки оборудования, который размещается в области базовой системы ввода вывода (basic input/output system - BIOS). Кроме того, в постоянном запоминающем устройстве (ПЗУ) некоторых плат расширений размещается код, который также может выполняться.

В состав аппаратных платформ входит ряд дополнительных микропроцессорных подсистем со своим кодом. Практически любая логика средней сложности реализуется с помощью микропроцессоров, ПЛИС[1] и т.д. Наличие потенциала по изменению функциональности только с помощью перепрограммирования отдельных

1 Программируемая логическая интегральная схема

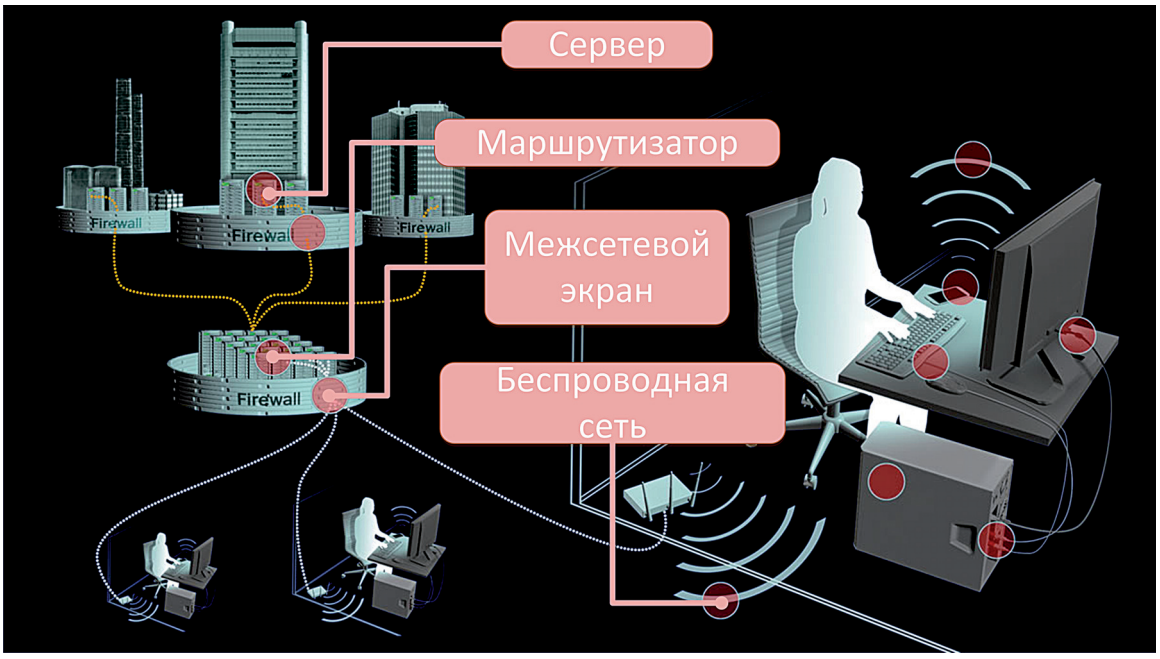


***Рис. 2.** Потенциальная возможность установки закладок на элементы инфраструктуры*

узлов чрезвычайно расширяет возможности внедрения зловредного кода.

Зловредный код, внедренный в область BIOS, обладает следующими характеристиками:

- слабо поддается обнаружению. Как правило, это функциональный модуль, который только обеспечивает установку настоящего зловредного кода, а сам может проявляться как не декларированная возможность или дефект;
- устойчив к перезагрузке или переустановке операционной системы;
- не подлежит контролю согласно текущей нормативной базы в системах Минобороны и ФСТЭК. На компрометированной аппаратной платформе может выполняться сертифицированный код.

Согласно 1 части каталога Spiegel практически все потенциальные закладки используют технологию внедрения в BIOS функционального модуля (импланта), который обеспечивает установку зловредного кода (см. Рис. 2. Потенциальная возможность установки закладок на элементы инфраструктуры..).

Рассмотрим список закладок по версии каталога Spiegel, которые ориентированы на инфраструктуру автоматизированной системы: межсетевые экраны, маршрутизаторы, сервера.

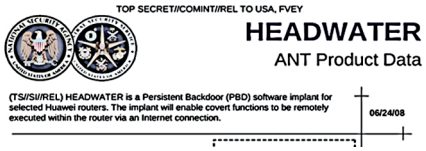
1. Сетевое оборудование

1.1. Маршрутизаторы

Маршрутизаторы - это специальные компьютеры, которые предназначены для подключения к внутренней сети компании или внешней сети, а также для передачи и обработки интернет-трафика. Согласно каталогу обзора SPIEGEL, AHT подразделение АНБ имеет среди его предложений закладки для использования в профессиональных маршрутизаторах, выпущенных, по крайней мере, двумя производителями — **Juniper** и **Huawei**. Скорее всего, существуют дополнительные продукты подразделения AHT для подобных устройств. Закладки, по версии каталога, устанавливаются в **BIOS**, на самом низком уровне программного обеспечения в каждом устройстве. Это гарантирует, что другие **дополнительные вредоносные программы** также могут быть установлены, даже если компьютер перезагружается или установлена новая операционная система. Модели маршрутизаторов, которые представлены в каталоге ANT, предназначены для использования малого, среднего и крупного бизнеса, а также для центров обработки данных Интернет и мобильных провайдеров телефонных услуг.

1.1.1. Маршрутизаторы Huawei

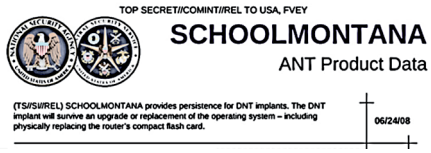
Компания Huawei (Китай) зарекомендовала себя как один из крупнейших в мире производителей сетевого оборудования. По данным исследовательской фирмы Infonetics, компания Huawei занимает **второе место** на мировом рынке во втором квартале 2013 года по продаже маршрутизаторов и коммутаторов для мобильной связи и Интернет-провайдеров, сразу за Cisco и впереди Juniper. Многие западные телекоммуникационные компании активно используют аппаратные средства Huawei, в том числе Deutsche Telekom (Германия).



Закладка Headwater представляет собой программную закладку для маршрутизаторов Huawei, которая обеспечивает уязвимость класса BackDoor в модуле памяти ROM. **Закладка устойчива к прошивке обновления** и предоставляет возможность **дистанционного** управления устройством. Позволяет удаленно перехватывать и анализировать все проходящие через роутер пакеты.

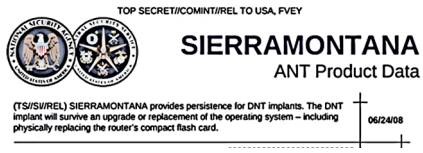
1.1.2. Маршрутизаторы Juniper

Маршрутизаторы Juniper J – Series предназначены для соединения серверов и настольный компьютеров с корпоративной сетью и Интернетом.



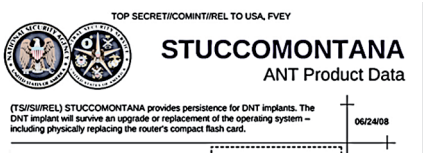
Закладка SCHOOLMONTANA представляет собой программную закладку для устройств Juniper J Series , **устойчивую к обновлениям** программного обеспечения. Сохраняется при перезагрузке, обновлении ОС маршрутизатора и даже при физической замене карты памяти с прошивкой (!).

Маршрутизаторы Juniper M – Series компании Juniper предназначены для организации магистральных сетей в крупных компаниях и поставщиков сетевых услуг. Они также используются в центрах обработки данных компаний, которые предоставляют другие корпорации и для частных клиентов для соединения с сетью Интернет.



Закладка SIERRAMONTANA представляет собой программную закладку для маршрутизаторов серии Juniper M, которая **устойчива к обновлениям** прошивки и размещается в BIOS. Сохраняется при перезагрузке, обновлении ОС маршрутизатора и даже при физической замене карты памяти с прошивкой (!).

Маршрутизаторы Juniper T – Series компании Juniper по словам производителя «используются ведущими поставщиками услуг фиксированной связи, мобильных, видео и облачных сетей».



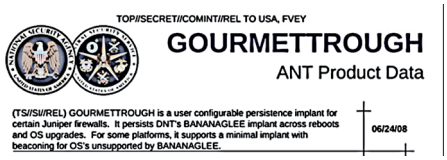
Закладка STUCCOMONTANA является программной закладкой для маршрутизаторов Juniper T-Series. Существует в качестве модификации BIOS и устойчива к **обновлению программного обеспечения**. Сохраняется при перезагрузке, обновлении ОС маршрутизатора и даже при физической замене карты памяти с прошивкой (!).

1.2. Межсетевые экраны

Аппаратные межсетевые экраны - это специальные компьютеры, которые размещаются между внутренней сетью компании или интернет - провайдера и остальной частью Интернета или разными сегментами. Они предназначены для предотвращения взлома, атак отказ в обслуживании, спама. Обеспечивают доступ терминалов сотрудников , которые регистрируются в сети компании через виртуальную частную сеть (VPN). Подразделение АНТ АНБ разработало аппаратные и программные закладки для аппаратных межсетевых экранов от основных производителей - Cisco, Juniper и Huawei - которые **превращают эти продукты** (первоначальная цель – построение защитных цифровых барьеров) **в шлюзы для поддержки атак хакеров АНБ**. Большинство закладок **размещаются в BIOS**. Это гарантирует, что закладка будет по-прежнему в активном состоянии и что вредоносные программы могут успешно закладку использовать, даже если компьютер перезагружается или проводилось обновление операционной системы.

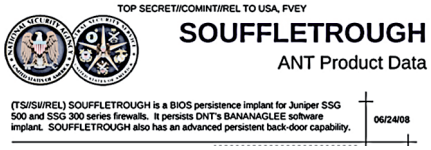
1.2.1. Межсетевые экраны Juniper

Межсетевые экраны Juniper SSG , Netscreen G5 , Netscreen 25 и 50 , SSG Series предназначены для малых и средних компаний, а также филиалов крупных корпораций.



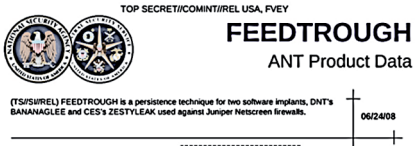
Закладка GOURMETTROUGH представляет собой настраиваемую программную закладку для устройств Juniper . Позволяет полностью управлять маршрутизатором, используя скрытые каналы передачи информации. Сохраняется при перезагрузке и апгрейде операционной системы маршрутизатора.

Межсетевые экраны Juniper SSG300 и SSG500 являются аппаратными брандмауэры, которые предназначенны для малых и средних компаний и филиалов крупных корпораций.



Закладка SOUFFLETROUGH обеспечивает полный контроль над межсетевым экраном. Сохраняется при перезагрузке и апгрейде ОС. Может быть установлена удаленно если на межсетевом экране установлена другая закладка АНБ - BANANAGLEE.

Межсетевые экраны Juniper Netscreen / ISG 1000 являются аппаратными брандмауэры, они подходят для использования Интернет-провайдеров и операторов мобильной телефонной связи.

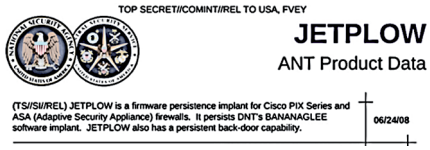


Закладка FEEDTROUGH позволяет обеспечивать удаленный доступ к N5XT компании, NS25, NS50, NS200, NS500, ISG1000 моделей.

1.2.2. Межсетевые экраны Cisco

Межсетевые экраны Cisco PIX-Series, Cisco ASA-Series. Продукты серии PIX от производителя Cisco (США) являются аппаратными межсетевыми экранами, в зависимости от модели, для малых и средних компаний, в том числе и для крупных компаний и поставщиков услуг. Производство линейки продуктов закончилась в 2008 году.

Серия ASA представляет моделью преемником PIX, и они предназначены для предприятий различных размеров, а также корпоративных центров обработки данных.



Закладка JETPLOW: Дает полный удаленный доступ к межсетевому экрану и трафику. Сохраняется при перезагрузке. Возможен удаленный апгрейд закладки и удаленная инсталляция если на экране стоит другая закладка АНБ BANANAGLEE. **«Широко используется в настоящее время!»**. Подходит не для всех версий ОС.

1.2.3. Межсетевые экраны Huawei

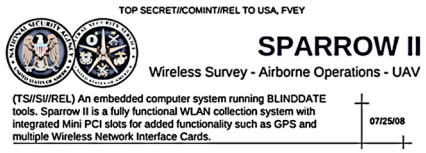
Межсетевые экраны серии Huawei Eudemon. Серия Eudemon представляет собой аппаратные брандмауэры Китайского производителя Huawei и предназначены для малых и средних компаний (серии 200) и для сервис-провайдеров и крупных корпораций (1000 серии). Технология Huawei используется по всему миру в компаниях, которые включают европейские телекоммуникационные гиганты, такие как O2, Vodafone и Deutsche Telekom.

Закладка HALLUXWATER дает полный доступ к экрану и проходящему трафику. Остается при перезагрузке и апгрейде операционной системы (в том числе загрузочной области!). Проверена в деле.

1.3. Беспроводные сети

АНТ Подразделение АНБ разрабатывает методы для получения доступа к сети беспроводных сетей извне, позволяя им подключиться к этим сетям и распространять свое собственное зловредное программное обеспечение. Закладка NIGHTSTAND, например, может удаленно внедрить пакеты данных для различных вредоносных Windows программ. Закладка SPARROW II, предназначена для выявления сетей беспроводной локальной сети с воздуха. Система достаточно мала для установления на беспилотный аппарат (БЛА).

Закладка NIGHTSTAND представляет собой мобильную систему для беспроводной инъекции зловредного кода через уязвимости систем Windows, использующих стандарт 802.11. Согласно спецификации он работает на расстояниях до 13 километров (восемь миль).

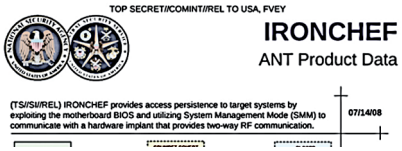


Закладка SPARROW II является средством выявления и составление карты беспроводных сетей, например с беспилотных аппаратов (БЛА).

2. Сервера

Сервера – это специальные компьютеры, которые обеспечивают доступность данных в сети компании или в сети Интернет. АНТ Подразделение АНБ разрабатывают несколько аппаратных и программных закладок для серверов производителей Dell и Hewlett-Packard. Программная закладка «DEITYBOUNCE» размещается внутри BIOS, самом низком уровне программного обеспечения, серверов Dell PowerEdge. Это расположение обеспечивает функционирование закладки по установке дополнительных шпионских программ, даже если компьютер перезагружается или осуществляется переустановка операционной системы. Предполагается, что аппаратные имплантаты для серверов Dell и HP устанавливаются на этапе доставки оборудования путем перехвата и манипулирования.

HP DL380 G5 это сервер хранения данных пятого поколения. Он используется в корпоративных центрах обработки данных.



Закладка IRONCHEF основана на изменении BIOS. Закладка применяется для установления связи с АНБ инфраструктурой используя скрытые аппаратные средства. Закладка разработана для серверов семейства Proliant, которые выпускаются компанией Hewlett-Packard.

Dell PowerEdge server это сервер хранения для использования в корпоративных центрах обработки данных.

Закладка DEITYBOUNCE основана на изменении BIOS. Закладка применяется для установления связи с NSA инфраструктурой используя скрытые аппаратные средства.

3. Выводы

Данные, опубликованные журналом Spigel, технологически воспроизводимы и могут являться реальной угрозой. Основным уязвимым механизмом проникновения закладок, в частности, для сетевого оборудования, является BIOS. После перепрошивки платформы становится возможным как устанавливать закладки 2-го уровня, так и обеспечивать их постоянное присутствие. Наиболее очевидным средством контроля образа BIOS является модуль доверенной загрузки. Анализ BIOS в данный момент находится на начальной стадии и не является обязательным. Также отсутствуют простейшие способы фиксации окружения при проведении анализа на НДВ. Возможным усилением этого механизма контроля может являться единая подпись удостоверяющего центра на все BIOS, а также обязательное наличие в ПО возможность расчета и отображения контрольных сумм BIOS и ОС.

Отдельно можно отметить системный подход по покрытию целевой инфраструктуры закладками. Получается, что практически все потенциальные каналы активного взаимодействия со зловредным кодом присутствуют в каталоге – это внешние межсетевые экраны, магистральное оборудование, беспроводная связь.

Наибольший потенциал, в частности, в развитии надежного коммуникационного оборудования (маршрутизатор, межсетевой экран, поддержка беспроводных технологий), возможен на базе защищенной компонентной базы, например Эльбрус.

Имеется также предложение организации в рамках сертификации единого регистра профилей ПАК, прошедших сертификацию. Предполагается, что данный регистр должен содержать все потенциальные уязвимости аппаратной платформы и давать числовую оценку доверия.

Литература (References)

1. Shopping for Spy Gear: Catalog Advertises NSA Toolbox. //Spiegel. http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html .
2. Inside TAO: Documents Reveal Top NSA Hacking Unit. //Spiegel. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html .
3. Interactive Graphic: The NSA's Spy Catalog. //Spiegel.http://www.spiegel.de/international/world/a-941262.html .