https://orcid.org/0000-0002-9068-5837
https://orcid.org/0000-0001-6591-2199

УДК 621.3.019.3

Н.В. СЕСПЕДЕС ГАРСИЯ[*], П.Д. СЕСПЕДЕС ГАРСИЯ[*]

УЯЗВИМОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ – УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

[*]Институт проблем математических машин и систем НАН Украины, г. Киев, Украина

Анотація. *У статті наводиться опис певних компонентів комп'ютерного обладнання, завдяки яким можна дистанційно отримати несанкціонований доступ до комп'ютерів. До таких компонентів належать Intel Management Engine (Intel ME) і Intel AMT. Intel ME – самостійна підсистема, яка включена майже в усі чіпи Intel процесорів із 2008 року. Чіп завжди підключений до джерела живлення, тому підсистема продовжує працювати навіть при вимкненому комп'ютері. В Intel AMT були виявлені вразливості і багато комп'ютерів з процесорами Intel стали доступні для віддалених і локальних зловмисників. Також у статті наводиться опис китайських мікрочіпів, які були вбудовані в обладнання Supermicro. Дане обладнання поставлялося не тільки в комерційні, а й у державні організації США. Китайські мікрочіпи Supermicro мають здатність редагувати потік коду, що йде до процесора, вставляючи свій власний код, або здатні змінювати порядок команд для процесора. Мікрочіп може перехоплювати кодування безпеки зв'язку, а також не допускати відновлення системи безпеки в цілому. Також у статті представлено огляд гучних за останнім часом вразливостей Meltdown, Spectre і ZombieLoad у процесорах Intel і ARM, що дозволяють маніпулювати комп'ютером у тій чи іншій мірі. Ці уразливості подібні між собою і дозволяють шкідливому додатку зчитувати будь-яку пам'ять комп'ютера, включаючи пам'ять ядра. Це стало можливим завдяки системі спекулятивного виконання коду. Вкраденими можуть бути як особисті дані користувача, на зразок історії браузера, вмісту веб-сайтів, паролів, так і системні дані на кшталт ключів шифрування диска. Фахівцям з безпеки слід враховувати вищевказані моменти, так як у певних випадках це виливається у проблеми державного масштабу як фінансові, так і політичні.*

Ключові слова: *вразливість комп'ютерних систем, інформаційна безпека, Intel ME, Intel AMT, мікрочіп Supermicro, вразливість Meltdown, Spectre і ZombieLoad.*

Аннотация. *В статье приводится описание определенных компонентов компьютерного оборудования, благодаря которым можно дистанционно получить несанкционированный доступ к компьютерам. К таким компонентам относятся Intel Management Engine (Intel ME) и Intel AMT. Intel ME – самостоятельная подсистема, включенная почти во все чипы Intel процессора с 2008 года. Чип всегда подключен к источнику питания, поэтому подсистема продолжает работать даже при выключенном компьютере. В Intel AMT были обнаружены уязвимости и многие компьютеры с процессорами Intel стали доступны для удаленных и локальных злоумышленников. Также в статье приводится описание китайских микрочипов, которые были внедрены в оборудование Supermicro. Данное оборудование поставлялось не только в коммерческие, но и в государственные организации США. Китайские микрочипы Supermicro обладают способностью редактировать поток кода, идущий к процессору, вставляя свой собственный код, или способны изменять порядок команд для процессора. Микрочип может перехватывать кодирование безопасности связи, а также не допускать восстановление системы безопасности в целом. Также в статье приводиться обзор нашумевших за последнее время уязвимостей Meltdown, Spectre и ZombieLoad в процессорах Intel и ARM, позволяющих манипулировать компьютером в той или иной степени. Эти уязвимости сходны между собой и позволяют вредоносному приложению считывать любую память компьютера, включая память ядра. Это стало возможным благодаря системе спекулятивного исполнения кода. Украденными могут быть как личные данные пользователя, наподобие истории браузера, содержимого веб-сайтов, паролей, так и системные данные вроде ключей шифрования диска. Спе-*

ISSN 1028-9763. Математичні машини і системи, 2019, № 4

циалистам по безопасности следует учитывать вышеуказанные моменты, так как в определенных случаях это выливается в проблемы государственного масштаба как финансовые, так и политические.
Ключевые слова: *уязвимость компьютерных систем, информационная безопасность, Intel ME, Intel AMT, микрочип Supermicro, уязвимость Meltdown, Spectre и ZombieLoad.*

Abstract. *This article provides a description for a certain computer equipment components which allow remotely gain unauthorized access to computers. These components are Intel Management Engine (Intel ME) and Intel AMT. Intel ME is an independent subsystem included in almost all Intel processor chips since 2008. The chip is always connected to a power source, because the subsystem continues to work even when the computer is turned off. Vulnerabilities were discovered in Intel AMT, thereafter many computers using Intel processors became available for remote and local intruders. The article also describes Chinese microchips that have been implemented into Supermicro equipment. This equipment was supplied not only to US commercial organizations, but also to governmental. Supermicro Chinese microchips have the ability to edit the code stream that heads to the processor by inserting their own code, or else it can change the instructions order for the processor. The microchip can intercept communication security coding, as well as prevent the restoration of the security system as a whole. The article also provides an overview for recent sensational vulnerabilities Meltdown, Spectre and ZombieLoad in Intel and ARM processors that allows to manipulate a computer to one degree or another. These vulnerabilities are similar to each other, they allow a malicious application to read any type of computer memory, including kernel. It became feasible thanks to a speculative code execution system. Personal user data can be stolen, such as browser history, website content, passwords, or system data, such as disk encryption keys. Security experts should take into account the points above, as in certain cases this could possibly translate into a national scale problems, both financial and political.*
Keywords: *vulnerability of computer systems, information security, Intel ME, Intel AMT, Supermicro microchip, vulnerability Meltdown, Specter and ZombieLoad.*

DOI: 10.34121/1028-9763-2019-4-3-8

1. Введение

Повсеместное использование зарубежных технологий, оборудования и наличие скрытых уязвимостей увеличивают опасность несанкционированного вмешательства в их функционирование. Конструктивный уровень зарубежных компонентов настолько высок, что порой даже профессионалам не удается понять полноту функционирования того или иного компонента. Особенно актуальна эта проблема для сферы критической инфраструктуры, таких как атомные электростанции, химзаводы, государственные и финансовые учреждения.

В статье приводится описание определенных компонентов компьютерного оборудования, благодаря которым можно дистанционно получить доступ к компьютерам. Также приводится обзор нашумевших за последнее время уязвимостей оборудования, позволяющих манипулировать компьютером в той или иной степени.

Цель статьи – обратить внимание специалистов по безопасности на наличие критических уязвимостей, встроенных микрочипов, позволяющих злоумышленнику получать доступ к компьютерному оборудованию и управлять им на свое усмотрение.

2. Intel Management Engine и Intel AMT

В технике, использующей процессоры Intel, существует элемент, о котором должен знать каждый специалист, обеспечивающий защиту оборудования от несанкционированного доступа. Это Intel Management Engine (Intel ME).

Согласно [1], Intel Management Engine – самостоятельная подсистема, включенная почти во все чипы Intel процессоров с 2008 года. Intel ME имеет коммерческий микрокод, выполняемый индивидуальным микропроцессором. Чип всегда подключен к источнику питания, поэтому подсистема продолжает работать даже при выключенном компьютере

[1]. Intel сообщала, что ME необходима для поддержания предельной производительности [1].

Intel ME в значительной степени является недокументированным главным контроллером для процессора: он работает с системным программным обеспечением во время загрузки и имеет прямой доступ к системной памяти, экрану, клавиатуре и сети. Весь код внутри Intel ME является секретным и строго контролируемым Intel. В Intel ME было найдено несколько уязвимостей. Отмечалось, что официального документированного способа отключить ME пока нет.

Часто Intel ME путают с другим модулем – Intel AMT (Intel Active Management Technology). На многих чипах Intel модуль управления поставляется с установленным модулем AMT. Он предназначен для того, чтобы системные администраторы могли удаленно контролировать компьютеры, используемые организацией и ее сотрудниками. В начале мая 2017 уязвимости в модуле Intel AMT в некоторых механизмах управления привели к тому, что многие компьютеры с процессорами Intel стали катастрофически уязвимы для удаленных и локальных злоумышленников и сама корпорация Intel подтвердила присутствие уязвимости удалённого повышения привилегий (SA-00075) в Management Technology [1]. Хотя Intel AMT можно отключить, в настоящее время нет способа отключить или ограничить механизм управления в целом. Данная уязвимость позволяет обойти аутентификацию по паролю для модуля удаленного управления AMT. Это означает, что во многих ситуациях удаленно можно получить те же возможности, что и у ИТ-отдела организации, при условии, что AMT была включенной и активной. Получив доступ к AMT, злоумышленники могут взаимодействовать с экраном или консолью, как если бы пользователь делал это самостоятельно. Также можно дистанционно загрузить произвольную или установить новую ОС и при наличии определенных навыков красть пароли шифрования диска. Авторитетная организация Electronic Frontier Foundation (EFF), защищающая гражданские права и конфиденциальность пользователей в цифровом пространстве, считает, что Intel должна обеспечить минимальный уровень прозрачности и пользовательского контроля над механизмами управления внутри компьютеров, чтобы предотвратить повторение случая с удаленной уязвимостью Intel AMT. Если этого не произойдет, то EFF считает нецелесообразным использование процессоров Intel во многих видах систем для критически важных инфраструктур [1].

3. Китайские микрочипы – угроза информационной безопасности США

В октябре 2018 года, ввиду большого количества сообщений из правительственных и корпоративных источников Bloomberg Businessweek, китайские специалисты провели успешную хакерскую атаку на более чем 30 американских компаний, включая Amazon и Apple. Указывалось, что похищенной могла быть также и информация спецслужб США [2].

Согласно расследованию Bloomberg Businessweek, микрочипы на серверных материнских платах компании Super Micro Computer стали главной угрозой информационной безопасности США.

Компания Super Micro Computer Inc. производила для предприятия Elemental дорогие серверы, которые пользователи размещали в своих сетях для обработки и сжатия видео.

Компания Amazon.com Inc. имела государственный контракт с Elemental на приобретение оборудования для облачного сервиса с высокой степенью безопасности и программного обеспечения для сжатия объемных видеофайлов и доводки их под разные устройства [2]. Возникли подозрения и приобретенное оборудование решили отправить для проверки независимым экспертам по безопасности.

Тестирование показало, что на материнские платы установлены крошечные микрочипы, которые не предусмотрены в оригинальных схемах. Amazon сообщила об обнару-

женных микрочипах властям США. Серверы Elemental были установлены в службах обработки данных Министерства обороны, на беспилотных аппаратах ЦРУ и бортовых сетях военных кораблей ВМФ [3]. Также эксперты подтвердили, что чипы были установлены на заводах в Китае. Оборудование Elemental стало мишенью хакеров из-за того, что сама компания Elemental в своих рекламных проспектах широко распространяла список своих клиентов, в число которых входило немалое количество правительственных организаций.

Атака с использованием подобных микрочипов стала более серьезной проблемой, чем проникновение в программное обеспечение. Аппаратные взломы сложнее обнаружить и потенциально они более разрушительны, так как дают скрытый долгосрочный доступ к сетям, ради которого соответствующие организации готовы тратить много ресурсов и лет работы [2].

Имея, по некоторым оценкам, объем производства в 75% мобильных телефонов и 90% компьютеров в мире, Китай обладает огромным преимуществом в осуществлении атак и внесении всякого рода шпионских компонентов на этапе изготовления оборудования.

По мнению американских следователей, чипы были установлены на платы сотрудниками секретных служб Китая прямо во время производственного процесса. Также было обнаружено, что атака коснулась почти 30 компаний, одного крупного банка и правительственных подрядчиков. Компания Apple Inc. была крупным клиентом Supermicro и планировала заказать у них более 30 тыс. серверов для новой глобальной сети дата-центров [3]. Согласно информации от трех достоверных источников, в Apple еще летом 2015 года в продукции Supermicro обнаружены вредоносные чипы со странной сетевой активностью и проблемами с прошивкой. К 2016 году компания Apple разорвала сотрудничество с Supermicro без объяснения причин. Также компания Amazon обнаружила странности в своем оборудовании и предоставила разведслужбам США доступ к ним. Согласно документам расследования, микрочипы были похожи на соединители для формирования сигнала, поэтому их было сложно обнаружить без специального оборудования [2].

В общем, 17 человек указали на факт манипуляций с аппаратными средствами Supermicro и другие подробности атаки. Это были и бывшие высокопоставленные сотрудники национальной безопасности, и инсайдеры крупных компаний Amazon и Apple. Источникам была предоставлена анонимность из-за чувствительного и, в некоторых случаях, секретного характера информации [2]. По мнению одного из инсайдеров, целью Китая являлся долгосрочный доступ к ценным корпоративным секретам и правительственным сетям. Персональные данные украдены не были.

Компания Supermicro является самым крупным в мире производителем серверных плат. Она также лидирует на рынке плат, которые используются в специализированных компьютерах, от МРТ-машин до оружейных систем, объемом в 1 миллиард долларов. Материнские платы Supermicro можно встретить в серверах банков, хедж-фондов, поставщиков облачных сервисов, услуг веб-хостинга и не только [2].

Специалисты, осведомленные о результатах расследования, утверждали, что микрочипы Supermicro обладают способностью редактировать поток кода, идущий к процессору, вставляя свой собственный код, или способны изменять порядок команд для процессора. Понятно, что любые изменения в инструкциях процессора ведут к катастрофическим последствиям. Вредоносные микрочипы могли все это выполнять, потому что они подключались к BMC (Baseboard Management Controller) – суперчипу [4]. Этот суперчип используется для удаленного входа на проблемные серверы, предоставляет им доступ к самому «чувствительному» коду даже на сломанных и выключенных компьютерах. Микрочип может перехватывать кодирование безопасности связи, а также не допускать восстановление системы безопасности в целом [3].

Служба безопасности Amazon разработала метод мониторинга микрочипов. В последующие месяцы они обнаружили короткие сообщения между злоумышленниками и «зараженными» серверами, но попыток удалить данные не было [3].

Относительно Apple, по словам инсайдеров, после обнаружения в 2015 году вредоносных микрочипов, компания начала удалять все серверы Supermicro из своих датацентров. В итоге все 7 тысяч серверов Supermicro были заменены в течение нескольких недель.

Эта ситуация с микрочипами стала предметом долгих переговоров США с Китаем, в результате которых Китай пообещал, что он больше не будет участвовать в поддержке краж хакерами интеллектуальной собственности США в интересах китайских компаний [3]. Также Пентагоном была проведена встреча с десятками технических руководителей и инвесторов, было сообщено о недавнем нападении и вынесено предложение о создании коммерческих продуктов, которые могли бы обнаружить аппаратные микрочипы.

4. Уязвимости Meltdown, Spectre, ZombieLoad и их последствия

В средствах массовой информации стала известна новость о появлении критических уязвимостей в процессорах Intel и ARM, благодаря которым процессоры могут быть подвержены вредоносным хакерским атакам. В данном случае атаки получили названия Meltdown и Spectre.

Компания Apple на своем сайте также заявляла о наличии критической уязвимости для процессоров всех моделей iMac и iPhone. В компании утверждали, что эти две угрозы – Meltdown и Spectre – касаются всех устройств и операционных систем, всех компьютеров Mac и устройств iOS [4]. При этом уточнялось, что на момент появления уязвимостей не было известно о вредоносном коде, способном повлиять на конечного пользователя. Компания Apple утверждала, чтобы воспользоваться уязвимостью необходимо установить зараженное приложение на устройство, а чтобы обезопасить себя, необходимо загружать приложения с официальных и проверенных источников.

Уязвимость Meltdown позволяет приложению считывать любую память компьютера, включая память ядра. В то же время Spectre, из-за уязвимости, позволяет злоумышленнику получить информацию из других приложений [5].

Атака Meltdown была обнаружена в середине 2017 года. Но подробную информацию обнародовали только в январе 2018 года, одновременно с атакой Spectre. В это же время были выпущены обновления безопасности Windows для исправления уязвимости. Однако в системах с AMD процессорами эти обновления стали причиной полного отключения компьютеров.

Уязвимость Meltdown использует ошибку реализации спекулятивного выполнения кода процессора. Другими словами, система спекулятивного исполнения кода – это когда у процессора есть необходимый код, но нет необходимых данных, и он начинает предугадывать их. Если данные оказались неправильными, то процессор скидывает их, и, получая правильные данные, начинает выполнять код. «Забракованные» данные некоторое время доступны в специальной памяти, используемой ядром операционной системы, к которому можно получить доступ.

В мае 2019 года появилась информация еще об одной уязвимости под названием ZombieLoad. Этой уязвимости подвержены все процессоры Intel, выпущенные после 2011 года (кроме Core 8-го и 9-го поколения, в которых имеется защита от атак спекулятивного исполнения), в том числе и обычные компьютеры, ноутбуки, а также серверы [6]. Процессоры AMD и ARM не подвержены ей. Атака осуществлялась с помощью четырех ошибок в микрокоде чипа Intel. Атака ZombieLoad напоминает Meltdown и Spectre и использовала ошибки в системе опережающего выполнения команд. Во время атаки на процессор поступает большое количество данных, которое он не способен обработать, что заставляет

его обращаться к микрокоду для предотвращения сбоя. В результате этой перегрузки ZombieLoad способна получить любые данные, используемые ядрами процессора, обходя ограничения. Исследователи, обнаружившие уязвимость, отмечают, что атака ZombieLoad позволяет красть конфиденциальные данные и ключи во время доступа к ним компьютера. Это могут быть как личные данные пользователя, наподобие истории браузера, содержимого веб-сайтов, паролей, так и системные данные вроде ключей шифрования диска [6].

5. Выводы

В статье были рассмотрены различные способы несанкционированного проникновения в компьютерную систему, как программные, так и аппаратные. Можно дать краткие рекомендации по обеспечению защиты компьютерных систем от несанкционированного вторжения. Одним из методов защиты оборудования является экранирование оборудования от передачи или приема любых сигналов.

Для критических сфер инфраструктур, военной сферы, сфер, где обязательным является условие недопустимости какого-либо стороннего вторжения в систему, рекомендуется использовать технику и программное обеспечение собственного производства. Это должно быть специализированное оборудование определенного назначения, выполняющее ряд функций. Но даже в собственном оборудовании должна быть продумана система защиты от перехвата информации и система определения незаявленных производителем аппаратных компонентов.

Обеспечение информационной безопасности является комплексной проблемой, требующей значительных технических, финансовых ресурсов и привлечения специалистов разного профиля.

СПИСОК ИСТОЧНИКОВ

1. Intel Management Engine. URL: https://ru.wikipedia.org/wiki/Intel_Management_Engine.
2. Большой взлом: как Китай проникал в американские сети через микрочип (Ч. 1). URL: https://telekritika.ua/smi/bolshoi-vzlom-kak-kitai-pronikal-v-amerikanskie-seti-cherez-mikrochip-chast-1/.
3. Большой взлом: как Китай проникал в американские сети через микрочип (Ч. 2). URL: https://telekritika.ua/smi/bolshoi-vzlom-kak-kitai-pronikal-v-amerikanskie-seti-cherez-mikrochip-chast-2/.
4. Apple признала уязвимость всех iPhone. URL: https://lenta.ru/news/2018/01/05/ meltdown_spectre/.
5. Microsoft выпустила обновление Windows и убила компьютеры. URL: https://lenta.ru/news/2018/01/09/microsoft/.
6. Миллионы компьютеров с процессорами Intel оказались под угрозой. URL: https://lenta.ru/news/2019/05/15/intel//.

Стаття надійшла до редакції 23.09.2019