УДК 004.56 (043.2)

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

М.Н. БОБОВ

ОАО «АГАТ-системы управления» – управляющая компания холдинга
«Геоинформационные системы управления»
Минск, 220114, Беларусь

Рассматриваются проблемы обеспечения кибербезопасности в современных инфокоммуникационных технологиях.

Ключевые слова: информационный ресурс, защита информации, кибербезопасность.

В настоящее время инфокоммуникационные технологии (ИКТ) стремительно развиваются, усиливая свое влияние на все ключевые сферы деятельности личности, организаций и государств. Внедрение ИКТ в процессы государственного управления является основой построения эффективного и социально ответственного демократического государства в XXI веке. В то же время, вместе со значительным ростом возможностей, проникновение ИКТ во все сферы жизни вызывает возникновение ряда новых и развитие уже существующих угроз личности, обществу и государству. Трансграничный характер ИКТ, их зависимость от сложных информационных технологий, активное использование площадок и сервисов ИКТ широкими группами граждан и организаций различных государств, обеспечивая новые возможности, создают и развивают новые угрозы для нанесения урона правам, интересам и жизнедеятельности личности, организации, государственных органов. К таким угрозам можно отнести:

– проведение кибератак против защищаемых информационных ресурсов со стороны киберпреступников и кибертеррористов;

– использование кибероружия в рамках специальных операций и кибервойн, в том числе сопровождающих традиционные боевые действия.

В настоящее время специалистами по защите информации выявлено целое множество кибератак, которые используют следующие известные инструменты: фишинг, троян, DDoS-атака, ботнет, backdoor, черви, классические файловые вирусы, вирус-вымогатель (шифровальщик), вредоносная программа (зловред), руткит, фрод, флуд (flood) [1]. Все многообразие инструментов кибератак используется для достижения их основной цели – проникновение в защищаемую инфокоммуникационную среду и установление над ней контроля. Как показывает исследование компании Fortinet [2], проводником преобладающей части успешных атак, с которыми довелось столкнуться организациям, стала широкомасштабная инфраструктура «Киберпреступление как услуга», которая обусловлена следующими факторами:

– готовность инструментов атак к применению в любое время и в любом месте;

– ускоренное распространение вредоносного программного обеспечения (ПО) за счет взаимопроникновения инфраструктур;

– снижение эффективности отслеживания состояния безопасности гибких распределенных инфраструктур.

Вместе с тем, в настоящее время создан и широко используется ряд сервисов и технологий, которые, с одной стороны, обуславливают эффективность функционирования современной инфокоммуникационной среды, а с другой стороны, являются легальным каналом проникновения в защищаемую инфокоммуникационную среду и установления над ней контроля. К таким сервисам и технологиям можно отнести:

– распространение программного обеспечения;
– обновление программного обеспечения;
– аппаратная виртуализация.

На рынке программного обеспечения действуют следующие основные способы распространения продуктов: продажа лицензий, сдача в аренду, распространение условно бесплатного программного обеспечения, распространение некоммерческого программного обеспечения, продажа или распространение программного обеспечения как услуги (Software as a Service, SaaS) и его разновидностей облачных вычислений и грид-вычислений. Производителями программного обеспечения также регулярно выпускаются обновления и патчи, которые, в основном, необходимы для достижения следующих целей:

– исправление имеющихся ошибок в программе;
– устранение обнаруженных уязвимостей или дыр безопасности;
– расширение функциональных возможностей программы.

Поэтому своевременное обновление ПО является таким же массовым и приоритетным сервисом, как и его распространение. Очевидно, что при массовом использовании ИТ-устройств требуются инструменты централизованного и удаленного управления и контроля. Поэтому на рынке предлагаются специальные утилиты, которые автоматически могут отслеживать обновления программ и устанавливать их.

Сложившаяся в настоящее время технология массового распространения и обновления ПО обуславливает необходимость тотального контроля его безопасности, т.к. поставляемое и обновляемое ПО может содержать программные закладки и недекларированные возможности (НДВ). Основная опасность программных закладок заключается в том, что, являясь частью защищенной системы, они способны принимать активные меры по маскировке своего присутствия в системе. Если программная закладка написана грамотно, то после того, как она внедрена в систему, обнаружить ее стандартными средствами администрирования очень трудно, поэтому она может функционировать неограниченно долгое время, и на протяжении всего этого времени внедривший ее злоумышленник имеет практически неограниченный доступ к системным ресурсам. Закладки могут наносить ущерб как отдельным пользователям и компаниям, так и целым государствам, например, ставя под угрозу обороноспособность страны. Опасность получить закладку зависит от надежности и порядочности разработчиков ПО, а также интереса со стороны спецслужб. Во многих случаях при разработке ПО программисты используют чужие библиотеки и открытое программное обеспечение (Open source), в котором могут быть как скрытые уязвимости, так и НДВ. Интерес для спецслужб представляют широко распространенные, используемые миллионами пользователей программы, а также государственные предприятия, производители военной техники и предприятия стратегически важных отраслей.

Основными мерами противодействия программным закладкам в настоящее время являются:

– проведение проверок ПО на наличие НДВ;
– использование «песочниц».

Проверки ПО на НДВ проводятся в специализированных лабораториях как вид сертификационных испытаний и состоят из следующих основных этапов: статический анализ, динамический анализ и ручной анализ исходного кода. Процесс сертификации ПО происходит по принципу тестирования исходного кода и сопоставления результатов данных проверок с описанием, содержащимся в специальных документах, предоставляемых вместе с ПО. В крупных компаниях поиск ошибок в программах и их тестирование – это отдельный этап, построенный по строго отлаженным методикам и проводимый большим количеством сотрудников. Сертификация на НДВ – еще одна дополнительная проверка, требующая длительного периода времени и больших финансовых затрат, что существенно поднимает стоимость конечного продукта. Вместе с тем, испытательные лаборатории, осуществляющие сертификацию на отсутствие НДВ, не обладают ни людскими, ни техническими ресурсами, позволяющими в массовом порядке на должном уровне и в кратчайшие сроки проводить процедуру проверки сложного ПО. Еще одной проблемой является то, что обновление ПО и установка исправлений являются нарушениями условий действия выданного сертификата

и требуют повторной процедуры проверки. Похожая ситуация возникает, если срок действия сертификата истек.

«Песочницы» используются для запуска непроверенного кода из небезопасных источников, как средство для обнаружения и анализа вредоносных программ. Она обычно представляет собой жестко контролируемый набор ресурсов для исполнения гостевой программы, например, место на диске или в памяти. Песочницы позволяют проводить автоматизированный статистический и динамический анализ подозрительных файлов в виртуализированной среде и при необходимости блокировать их. Это позволяет безопасно оценить «поведение» и последствия открытия подозрительного файла. Анализ файла проводится в автоматическом режиме в виртуальной среде, идентичной рабочей станции пользователя, и не требует от администратора системы специальных знаний в части анализа кода. Независимость от сигнатурных методов детектирования позволяет при использовании «песочницы» обнаружить вредоносный код «нулевого дня», специально разработанный (модифицированный) для проведения целевой атаки. Тем не менее, реализация описанных выше механизмов защиты требует значительных вычислительных ресурсов. Их реализация на уровне конечных рабочих станций невозможна либо неэффективна, поэтому производители предлагают специализированные программно-аппаратные комплексы, работающие на уровне сети. Повышенная безопасность исполнения кода в «песочнице» связана с большой нагрузкой на систему. Именно поэтому их используют только в случае выявления подозрительного кода.

Появление новых процессоров с поддержкой технологии аппаратной виртуализации расширило возможности, как для средств защиты информации, так и для средств, нарушающих информационную безопасность. Программное обеспечение, использующее технологию аппаратной виртуализации, работает в новом, более привилегированном, чем операционная система, режиме. С одной стороны, такое ПО, выполняющее функции монитора виртуальных машин (МВМ), повышает сервисные возможности электронной вычислительной машины (ЭВМ) и снижает стоимость ее эксплуатации. Но с другой стороны, появляется возможность для негласного внедрения программной закладки с бесконтрольными возможностями. В настоящее время подавляющее большинство процессоров Intel и AMD поддерживают технологию аппаратной виртуализации и поэтому потенциально все ЭВМ с такими процессорами подвержены угрозам нарушения информационной безопасности, поскольку становится возможной реализация тотального контроля компьютера. Основная задача состоит в захвате управления оборудованием виртуализации. Тот, кто первый захватил оборудование виртуализации, тот в состоянии создать для всех последующих желающих с ней поработать соответствующую программно-аппаратную среду. Для этой цели служит уже отработанная и реально существующая технология, основанная на использовании двух компонент, которые можно условно называть гипердрайвером и гиперагентом.

Гипердрайвер – программа, резидентно находящаяся в оперативной памяти и осуществляющая контроль над аппаратурой и программной средой вычислительной системы. Для ее работы используется аппаратная виртуализация центрального процессора, с помощью которой создается виртуальная среда, и в ней запускается операционная система. Основные функции гипердрайвера:

– обеспечивать работоспособности своего кода в любой программной среде;

– оставаться незамеченным для любых программных средств, загруженных на ЭВМ;

– осуществлять постоянный контроль выбранных аппаратных и программных объектов в вычислительной среде;

– обеспечивать связь с компонентами визуализации и управления его работой.

Гиперагент – программа, осуществляющая управление гипердрайвером и получение информации от гипердрайвера. Гиперагент организует интерфейс между гипердрайвером и пользователем системы. Эта программа функционирует на прикладном уровне и выполняет следующие функции:

– действует как редактор оперативной памяти, редактор памяти ввода / вывода (в адресном пространстве памяти), позволяет просматривать область БИОС;

– выполняет дампирование в файл заданных областей адресного пространства;

– оперативно выполняет сложные поисковые операции в памяти, используя для этого специально зарезервированный процессор в гипердрайвере;

– сохраняет в дампе события, связанные с выполнением команды CPUID (идентификация процессора);

– включает / выключает режим подстановок в блоках параметров, получаемых в результате выполнения команды CPUID.

При запуске гипердрайвер переводит процессоры в виртуальный режим, а последний из них изолирует от ЭВМ и использует исключительно для скоростного сканирования оперативной памяти. После развертывания гипердрайвера, уже находясь в виртуальном режиме, он осуществляет загрузку хостовой операционной системы.

Таким образом, гипердрайвер является средством оперативного и тотального контроля за любым аппаратным и программным ресурсом вычислительной системы. Это свойство определяет область его основного применения – регистрация интересующих программных и аппаратных событий, а также эмуляция несуществующего оборудования. С помощью гипердрайвера также могут подвергаться исследованию и контролю программные комплексы ядра гипервизоров, поскольку не представляет сложности пропустить гипервизор любой известной системы виртуализации под управлением ранее запущенного гипердрайвера. Размер кода гипердрайвера позволяет выполнить его безболезненное размещение в БИОС вместе с функциями из арсенала шпионских технологий. Универсальные способы размещения дополнительных программных модулей во флеш-памяти БИОС уже давно отработаны и используются даже в легальных коммерческих продуктах. Обнаружить в них программный код гипердрайвера, даже после выпаивания микросхемы флеш-памяти, абсолютно невозможно.

ACTUAL PROBLEMS OF CYBERSECURITY SUPPORT

M.N. BOBOU

Abstract

The problems of cybersecurity support in modern infocommunication technologies are considered.

Keywords: information resource, information security, cyber security.

Список литературы

1. ISO/IEC 27032 2012. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».
2. Tadviser [Электронный ресурс]. URL: https://www.tadviser.ru (дата обращения: 20.04.2018).