УДК 621.396

Д.А. Даниленко

Кировоградский национальный технический университет, Кировоград

МЕТОДЫ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

Рассматриваются методы защиты телекоммуникационных систем и сетей от действий вредоносного программного обеспечения, в частности, анализируются методы обнаружения вторжений, основанные на использовании сигнатурного анализа и методы проактивной защиты. Показано, что наиболее перспективным направлением в развитии методов защиты телекоммуникационных систем и сетей от действий вредоносного программного обеспечения является применение проактивных технологий, построение на их основе сетевых систем обнаружения и предотвращения вторжений.

Ключевые слова: *телекоммуникационные системы и сети, система выявления вторжений.*

Введение

Результаты проведенного анализа показывают, что наибольшую угрозу безопасности современных телекоммуникационных систем и сетей представляет вредоносное программное обеспечение [1 – 8]. С его помощью злоумышленники могут получить несанкционированный доступ к вычислительным ресурсам телекоммуникационных систем и сетей, нанести значительный ущерб посредством противоправного копирования, искажения, удаления или подмены информации [7, 8]. В этой связи актуальным направлением является разработка исследование и современных методов обнаружения вредоносного программного обеспечения в телекоммуникационных системах и сетях.

Под вредоносной программой понимается любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам телекоммуникационных систем и сетей, с целью несанкционированного использования этих ресурсов или причинения вреда (нанесения ущерба) их владельцу информации путем копирования, искажения, удаления или подмены информации [1 – 3]. В качестве основных методов защиты телекоммуникационных систем и сетей от действий вредоносного программного обеспечения являются методы обнаружения вторжений: сигнатурный анализ и методы проактивной защиты [4 – 7].

Целью данной работы является анализ основных методов защиты от действий вредоносного программного обеспечения в телекоммуникационных системах и сетях, исследование особенностей их функционирования и использования.

1. Методы сигнатурного обнаружения

Обнаружение, основанное на сигнатурах, лежит в основе работы большинства антивирусных программ и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы [1 – 7].

В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в словаре, программа-антивирус может инициировать выполнение одного из следующих действий:

– удаление инфицированного файла;

– отправка файла в «карантин» (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса);

– восстановление файла, посредством удаления вируса из тела файла.

Антивирусные программы, созданные на основе метода соответствия определению вирусов в словаре, обычно просматривают файлы тогда, когда телекоммуникационная система создаёт, открывает, закрывает или посылает файлы по электронной почте. Таким образом, вирусы можно обнаружить сразу же после занесения их в компьютер и до того, как они смогут причинить какой-либо вред.

Необходимо отметить, что системный администратор может составить график для антивирусной программы, согласно которому могут просматриваться (сканироваться) все файлы на жёстком диске.

Хотя антивирусные программы, созданные на основе поиска соответствия определению вируса в словаре, при обычных обстоятельствах могут достаточно эффективно препятствовать вспышкам заражения компьютеров, авторы вирусов стараются держаться на полшага впереди таких программ-антивирусов, создавая «олигоморфические», «полиморфические» и самые новые, «метаморфические», вирусы, в которых некоторые части участки

кода перезаписываются, модифицируются, шифруются или искажаются так, чтобы невозможно было обнаружить совпадение с определением в словаре вирусов.

Сигнатуры антивирусов создаются в результате кропотливого анализа нескольких копий файла, принадлежащего одному вирусу. Сигнатура должна содержать только уникальные строки из этого файла, настолько характерные, чтобы гарантировать минимальную возможность ложного срабатывания – главный приоритет любой антивирусной компании. Разработка сигнатур – ручной процесс, тяжело поддающийся автоматизации. Несмотря на массу исследований, посвящённых автоматической генерации сигнатур, нарастающий полиморфизм (и «метаморфизм») вирусов и атак делают синтаксические сигнатуры бессмысленными.

Таким образом, можно выделить следующие недостатки и достоинства синтаксических сигнатур: позволяют определять конкретную атаку с высокой точностью и малой долей ложных вызовов; неспособны выявить какие-либо новые атаки; беззащитны перед полиморфными вирусами и изменёнными версиями того же вируса; требуют регулярного и крайне оперативного обновления; требуют кропотливого ручного анализа вирусов.

2. Методы проактивной защиты

Проактивные технологии – совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе [1 – 8].

Технология эвристического анализа позволяет на основе анализа кода выполняемого приложения, скрипта или макроса обнаружить участки кода, отвечающие за вредоносную активность. Эвристическим анализатором называется набор подпрограмм, которые анализируют код исполняемых файлов, макросов, скриптов, памяти или загрузочных секторов для обнаружения в нем разных типов вредоносных компьютерных программ, не определяемых обычными (сигнатурными) методами. Другими словами, эвристические анализаторы предназначены для поиска неизвестного вредоносного ПО. Эффективность данной технологии является низкой, что обусловлено большим количеством ложных срабатываний при повышении чувствительности анализатора, а также большим набором техник, используемых авторами вредоносного программного обеспечения для обхода эвристического компонента антивирусного программного обеспечения.

Технология эмуляции позволяет запускать приложение в среде эмуляции, эмулируя поведение операционной системы или центрального процессора. При выполнении приложения в режиме эмуляции приложение не сможет нанести вреда системе пользователя, а вредоносное действие будет детектировано эмулятором. Несмотря на кажущуюся эффективность данного подхода, он также не лишен недостатков – эмуляция занимает слишком много времени и ресурсов компьютера пользователя, что негативно сказывается на быстродействии при выполнении повседневных операций, также, современные вредоносные программы способны обнаруживать выполнение в эмулированной среде и прекращать свое выполнение в ней.

Технология анализа поведения основывается на перехвате всех важных системных функций или установке т.н. мини-фильтров, что позволяет отслеживать всю активность в системе пользователя. Технология поведенческого анализа позволяет оценивать не только единичное действие, но и цепочку действий, что многократно повышает эффективность противодействия вирусным угрозам. Также поведенческий анализ является технологической основой для целого класса программ – поведенческих блокираторов (HIPS – Host-based Intrusion Systems).

Технология ограничение привилегий выполнения работает по принципу ограничения активности потенциально вредоносных приложений таким образом, чтобы они не могли нанести вреда системе пользователя. Ограничение активности достигается за счет выполнения неизвестных приложений в ограниченной среде, откуда приложение не имеет прав доступа к критическим системным файлам, веткам реестра и другой важной информации. Технология ограничения привилегий выполнения является эффективной технологией противодействия современным угрозам, но следует понимать, что пользователь должен обладать знаниями, необходимыми для правильной оценки неизвестного приложения.

Технология виртуализации рабочего окружения работает с помощью системного драйвера, который перехватывает все запросы на запись на жесткий диск и вместо выполнения записи на реальный жесткий диск выполняет запись в специальную дисковую область – буфер. Таким образом, даже в том случае, если пользователь запустит вредоносное программное обеспечение, оно проживет не далее чем до очистки буфера, которая по умолчанию выполняется при выключении компьютера. Однако следует понимать, что технология виртуализации рабочего окружения не сможет защитить от вредоносных программ, основной целью которых является кража конфиденциальной информа-

ции, т.к. доступ на чтение к жесткому диску не запрещен.

Технология обеспечения безопасности на основе политик. Политика безопасности является необходимым атрибутом любой продуманной стратегии защиты от ИТ-угроз. Продуманная политика позволяет в несколько раз уменьшить риск заражения вредоносной программой, атаки хакеров или утечки конфиденциальной информации. К разработке политики всегда нужно подходить очень взвешенно и учитывать потребности и бизнес-процессы всех подразделений и работников компании. Кроме вышеописанного подхода к политике безопасности, в материалах различных производителей встречаются упоминания безопасности на основе политик (policy-based security). На сегодняшний день существует несколько подходов к такому способу обеспечения безопасности. Политика безопасности является необходимым атрибутом любой продуманной стратегии защиты от ИТ-угроз.

Подход Trend Micro – Trend Micro Outbreak Prevention Services. Данный сервис подразумевает распространение неких политик, позволяющих предотвратить эпидемию. Т.е. политика распространяется до появления обновления антивирусных баз или патчей. С первого взгляда кажется, что данное решение выглядит разумным, но дело в том, что скорость добавления процедур обнаружения нового malware в Trend Micro низка и данное решение сделано для того, чтобы «заткнуть дыру» медленной работы антивирусной лаборатории TrendLab.

Кроме этого, на формирование политики также требуется время (не всегда меньшее, чем на анализ вируса для добавления процедур детектирования в AB базу) и все равно есть промежуток времени, в который пользователь остается беззащитным перед новой угрозой. Другим недостатком данного подхода является частота смены политик безопасности. Все плюсы от безопасности на основе политик заключаются в малой частоте смены самой политики. Это позволяет персоналу привыкнуть к тому, что и как делать можно, а что запрещено. Если же политики будут меняться по нескольку раз в день, это просто внесет сумятицу и приведет к тому, что никакой политики безопасности не будет. Корректнее всего назвать метод Trend Micro не policy-based security, а ускоренным выпуском неких сигнатур. Следовательно, такой подход не является в большинстве случаев проактивным. Исключение составляют политики, которые делают невозможной эксплуатацию тех или иных уязвимостей в программном обеспечении.

Подход Cisco-Microsoft. Ограничение доступа в корпоративную сеть для компьютеров, которые не соответствуют политике безопасности компании (например, отсутствуют необходимые обновления операционной системы, нет последних обновлений антивирусных баз и т.д.). Для приведения компьютера в соответствие политике выделяется доступ только на специальный сервер обновлений. После установки всех необходимых обновлений и выполнения других действий, требуемых политикой безопасности, компьютер получает доступ в корпоративную сеть.

Технология обеспечения безопасности на основе Intrusion Prevention System

Системы предотвращения вторжений (IPS) предусматривают возможность закрытия наиболее часто используемых вредоносными программами уязвимостей компьютера перед новой угрозой еще до выхода обновления антивирусных баз: блокировка портов, т.е. возможности попадания инфекции на компьютер и ее дальнейшего размножения; создание политик для ограничения доступа к директориям или отдельным файлам; обнаружение источника инфекции в сети и блокировка дальнейших коммуникаций с ним. Данная технология отлично работает против атак хакеров и бесфайловых червей и вирусов, но против почтовых червей, классических вирусов и троянских программ IPS не эффективна.

Технология обеспечения безопасности на основе защиты от переполнения буфера.

Идея технологии – не допустить переполнения буфера для наиболее распространенных программ, сервисов Windows, включая Word, Excel, Internet Explorer, Outlook и SQL Server. При большинстве современных атак задействуются различные уязвимости, использующие переполнение буфера. Предотвращение переполнения буфера также можно отнести к проактивной защите, т.к. эта технология просто исключает использование такой уязвимости любым вредоносным кодом или атакой.

Технология обеспечения безопасности на основе поведенческих блокираторов.

Основная идея блокиратора – анализ поведения программ и блокировка выполнения любых опасных действий. Теоретически блокиратор может предотвратить распространение любого, как известного, так и неизвестного (написанного после блокиратора) вируса. Именно в этом направлении и движется большинство разработчиков антивирусного ПО. В последнее время большинство систем предотвращения распространения почтовых червей по механизму являются поведенческими блокираторами.

Первое поколение поведенческих блокираторов появилось еще в середине 90-х годов. Принцип их действия был прост – при обнаружении потенциально опасного действия задавался вопрос поль-

зователю – разрешить или запретить действие. Во многих случаях такой подход работал, но «подозрительные» действия производили и легитимные программы (вплоть до операционной системы) и если пользователь не обладал должной квалификацией, вопросы антивируса вызывали непонимание. С проникновением персональных компьютеров все глубже в повседневную жизнь снижался средний уровень квалификации пользователей, и первые поведенческие блокираторы перестали быть востребованными рынком.

Поведенческие блокираторы второго поколения. Второе поколение поведенческих блокираторов отличает то, что они анализируют не отдельные действия, а последовательность действий, и уже на основании этого делается заключение о вредоносности того или иного ПО. Это значительно сокращает количество запросов к пользователю и повышает надежность детектирования.

Выводы

В настоящее время проактивные технологии являются важным и неотъемлемым компонентом антивирусного программного обеспечения. Более того, как правило, в антивирусных продуктах используется сочетание сразу нескольких технологий проактивной защиты, например эвристический анализ и эмуляция кода успешно сочетаются с поведенческим анализом, что позволяет многократно повысить эффективность современных антивирусных продуктов против новых, все более и более изощренных вредоносных программ. Перспективным направлением является исследование проактивных технологий защиты телекоммуникационных систем и сетей от вредоносного программного обеспечения и построение на их основе сетевых систем обнаружения вторжений.

Список литературы

1. *Mihai Christodorescu, Somesh JhaTesting. Malware Detectors. Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'04), Boston, Massachusetts, USA, July 11-14, 2004, 11 p.*
2. *McAfee AVERT. Virus information library. Published online at http://us.mcafee.com/virusInfo/default.asp.*
3. *Symantec Antivirus Research Center. Expanded threat list and virus encyclopedia. Published online at http://securityresponse.symantec.com/avcenter/venc/data/cih.html.*
4. *West Coast Labs. Anti-virus Checkmark level 2. Published online at http://www.check-mark.com/checkmark/pdf/Checkmark_AV2.pdf.*
5. *[Электронный ресурс]. – Режим доступа к ресурсу: http://www.symantec.com/security_response/definitions.jsp.*
6. *[Электронный ресурс]. – Режим доступа к ресурсу: http://www.av-test.org/down/papers/2004-02_vb_outbreak.pdf.*
7. *[Электронный ресурс]. – Режим доступа к ресурсу: http://www.securelist.com/ru/analysis/170273483/Proaktivnaya_zashchita_kak_ona_est?print_mode=1*
8. *Brunnstein K. "Heureka-2" AntiVirus Tests. Virus Test Center, University of Hamburg, Computer Science Department, Mar. 2002. Published online at http://agn-www.informatik.uni-hamburg.de/vtc/ en0203.htm.*
9. *Snort 2.1. Обнаружение вторжений / Джей Бил. и др. – М.: ООО «Бином-Пресс», 2006 г. – 656 с.*

Поступила в редколлегию 22.02.2012

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОДИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Д.О. Даниленко

Розглядаються методи захисту телекомунікаційних систем і мереж від дій шкідливого програмного забезпечення, зокрема, аналізуються методи виявлення вторгнень, засновані на використанні сигнатурного аналізу й методи проактивного захисту. Показано, що найбільш перспективним напрямком у розвитку методів захисту телекомунікаційних систем і мереж від дій шкідливого програмного забезпечення є застосування проактивних технологій, побудова на їхній основі мережних систем виявлення й запобігання вторгнень.

Ключові слова: *телекомунікаційні системи й мережі, система виявлення вторгнень.*

METHODS OF THE FINDING OF BAD SOFTWARE IN TELECOMMUNICATION SYSTEM AND NETWORKS

D.A. Danilenko

They are considered methods of protection of the telecommunication systems and networks from action of bad software, in particular, are analysed methods of the finding the invasions, founded on use the signature analysis and methods proactive protection. It is shown by that the most perspective direction in development of the methods of protection of the telecommunication systems and networks from action of bad software is an using proactive technology, building on their base of the network systems of the finding and preventions of the invasions.

Keywords: *telecommunication systems and network, system of the revealing the invasions.*