Д. С. Сильнов

ОСОБЕННОСТИ МЕХАНИЗМА ВЫЯВЛЕНИЯ ВИРУСОВ В MICROSOFT SECURITY ESSENTIALS (MICROSOFT FOREFRONT ENDPOINT PROTECTION)

Введение

Безопасность информационных систем государственных и частных структур на сегодняшний день является одной из приоритетных задач, поставленных перед разработчиками систем защиты информации (СЗИ). Каждый разработчик СЗИ стремится к созданию механизмов выявления вредоносных объектов, которые позволили бы более качественно и своевременно обнаруживать и обезвреживать вирусы. Несмотря на то что результат работы любого антивируса одинаков — выявление вируса, алгоритмы, которые приводят к этому, разнообразны и в ряде случаев являются интеллектуальной собственностью разработчиков СЗИ. Изучение этих алгоритмов затруднено в силу закрытости исходного кода ряда антивирусов. С другой стороны, изучение алгоритмов позволит модернизировать существующие программные системы и выявить их возможные недостатки.

Подходы к изучению механизмов работы СЗИ

Анализ исходного кода — это наиболее очевидный подход, который используется непосредственно разработчиками антивирусов. Разработчики, имея доступ к исходным кодам, получают несомненное преимущество, так как изнутри знают механизмы функционирования своего программного продукта. Выделение денежных средств для оплаты работы сотрудников, которые проводили бы анализ уже созданного кода и его аудит, не относится к профильным затратам, так как основной задачей антивируса является обнаружение вирусов, а не обновление исходного кода. Таким образом, проблема заключается в том, что с экономической точки зрения неэффективно вкладывать время сотрудников, а это должны быть сотрудники с определенным уровнем доступа, в модернизацию непрофильных алгоритмов, хотя эти алгоритмы и составляют неотъемлемую часть СЗИ.

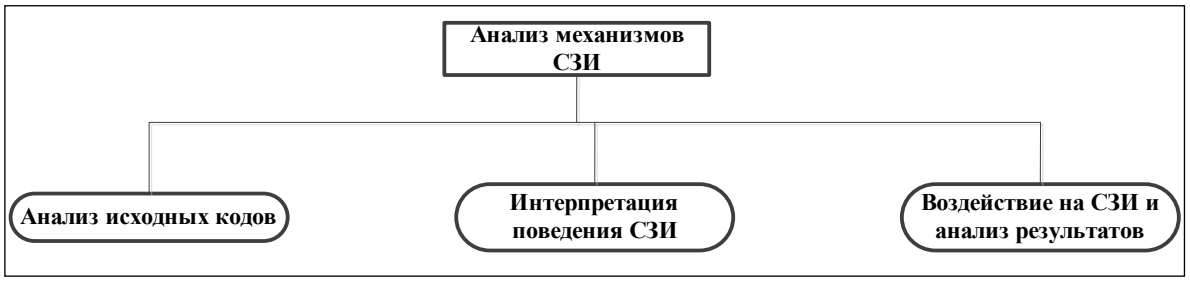

Рис. 1. Подходы к анализу механизмов работы СЗИ

Другим подходом является интерпретация поведения СЗИ на основании обнаружения или необнаружения файлов, содержащих вирусные части. Под вирусными частями следует понимать либо сигнатуру, в случае исследования сигнатурного метода обнаружения вирусов, либо же отдельные программные элементы вирусов, выполняющие операции, которые могут расцениваться эвристическим анализатором как подозрительные и (или) вредоносные. Этот подход используется, по крайней мере, разработчиками СЗИ для обнаружения ложных срабатываний своих антивирусных продуктов [1].

Третий подход, предлагаемый в данной работе (рис. 1), заключается в разработке специальных программных средств анализа и оценки эффективности работы антивирусных средств.

Разработанное программное средство служит для исследования устойчивости антивирусных средств к ложным срабатываниям. При использовании такого подхода в процессе исследования антивирусного средства Microsoft Security Essentials (MSE) [2] компании Microsoft было обнаружено его нестандартное поведение при определенных условиях. Следует отметить, что MSE — это бесплатный программный продукт, но на его базе компания Microsoft предлагает и коммерческий антивирус — Microsoft Forefront Endpoint Protection [3].

Экспериментальные исследования Microsoft Security Essentials

Обнаруженная особенность поведения касается сигнатурного метода, который применяется в MSE при сканировании файлов на предмет наличия в них вирусных сигнатур. Было выявлено, что на факт обнаружения вирусной сигнатуры влияет наличие или отсутствие цифрового сертификата у исполняемого файла. Цифровые сертификаты для исполняемых файлов используются компанией Microsoft для подтверждения подлинности программного обеспечения, распространяемого сторонними разработчиками [4]. В случае отсутствия цифрового сертификата наблюдается штатное поведение, вирусные сигнатуры обнаруживаются в соответствии с их наличием в файле. В случае наличия цифрового сертификата у исполняемого файла обнаружено неожиданное поведение антивируса.

С использованием специально разработанного программного средства был поставлен такой эксперимент, который выявил закономерность наличия цифрового сертификата и обнаружения вирусной сигнатуры в исполняемом файле. Для эксперимента был выбран ряд исполняемых файлов, находящихся на тестируемом компьютере под управлением ОС Windows 7. В каждый из выбранных файлов виртуально помещалась сигнатура, так что при чтении данного файла сигнатура заменяла участок бинарного кода файла, но в случае проверки цифрового сертификата замена не выявлялась. Такую возможность предоставляет специально разработанное автором программное средство, которое в ближайшее время будет запатентовано. Механизм его работы умышленно не раскрывается более подробно. Данное программное средство использует штатные механизмы ОС семейства Windows и не нарушает целостности самих файлов. Протокол данного эксперимента наглядно показывает (см. таблицу 1), что в случае наличия цифрового сертификата у бинарного исполняемого файла (типа .exe) антивирус MSE не обнаруживает (позиции 1–11 протокола) помещенную в этот файл сигнатуру. Когда файл не подписан цифровым сертификатом (результаты 12–16 протокола), обнаружение вирусной сигнатуры происходит незамедлительно.

Таблица 1. Протокол эксперимента № 1

№	Название файла	Цифровой сертификат	Результат
1	HPAuto.exe	Hewlett-Packard Company (просрочен)	не обнаружено
2	TMExtreme.exe	ArcSoft, Inc. (действует)	не обнаружено
3	mDNSResponder.exe	Apple Inc. (действует)	не обнаружено
4	DTLite.exe	DT Soft Ltd (действует)	не обнаружено
5	avp.exe	Kaspersky Lab (просрочен)	не обнаружено
6	opera.exe	Opera Software ASA (действует)	не обнаружено
7	Picasa3.exe	Google Inc. (действует)	не обнаружено
8	uTorrent.exe	BitTorrent Inc. (действует)	не обнаружено
9	firefox.exe	Mozilla Corporation (действует)	не обнаружено

№	Название файла	Цифровой сертификат	Результат
10	iTunes.exe	Apple Inc. (действует)	не обнаружено
11	StarCraft II.exe	Blizzard Entertainment, Inc. (просрочен)	не обнаружено
12	gyazowin.exe	не подписан	обнаружено
13	MegaFon Modem.exe	не подписан	обнаружено
14	VKMusic4.exe	не подписан	обнаружено
15	xchat.exe	не подписан	обнаружено
16	Evernote.exe	не подписан	обнаружено

Для подтверждения обнаруженных особенностей поведения антивируса MSE проведен дополнительный эксперимент. Рассмотрим порядок проведения эксперимента. Проводится сканирование файла с цифровой подписью, происходит фиксация текущего результата. Затем в целях признания сертификата недействительным файл редактируется и произвольно выбранный символ (при помощи HEX-редактора [5]) меняется на случайно выбранный другой символ. Таким образом, нарушается контрольная сумма файла и, как следствие, цифровой сертификат становится недействительным. Проводится повторное сканирование, результатом которого является факт обнаружения вирусной сигнатуры. Результаты такого эксперимента представлены в протоколе (см. таблицу 2), причем во втором случае запись «(мод.)» говорит о факте модификации файла в соответствии с требованиями эксперимента.

Таблица 2. Протокол эксперимента № 2

№	Название файла	Сертификат	Результат
1	picasa3.exe	Google Inc. (действует)	не обнаружено
	picasa3.exe (мод.)	Google Inc. (не действителен)	обнаружено
2	iTunes.exe	Apple Inc. (действует)	не обнаружено
	iTunes.exe (мод.)	Apple Inc. (не действителен)	обнаружено
3	firefox.exe	Mozilla Corporation (действует)	не обнаружено
	firefox.exe (мод.)	Mozilla Corporation (не действителен)	обнаружено

Анализ полученных результатов

Представленные результаты выявляют закономерность между наличием действительной цифровой подписи и фактом обнаружения вирусной сигнатуры антивирусов MSE в исполняемых файлах. Безусловно, требуются дополнительные и полномасштабные исследования данной особенности с использованием легитимно выданных цифровых сертификатов. Вероятно, подобная особенность проявляется не для всех типов цифровых сертификатов, а также не для всех организаций, имеющих в своем распоряжении цифровой сертификат. В работе установлено, что в бинарном файле, подписанном цифровым сертификатом с истекшим сроком годности, вирусные сигнатуры также не обнаруживаются.

Фактически можно говорить о расширении привилегий и повышении доверия для подписанных исполняемых файлов со стороны MSE, но границы такого доверия не изучены в полном объеме. Важным и актуальным является вопрос: возможно ли распространять вредоносное

программное обеспечение при наличии у него цифровой подписи на компьютерах с установленным антивирусом от компании Microsoft?

В связи с этим возникает вопрос, является ли наличие цифрового сертификата, с точки зрения компании Microsoft, фактом подтверждения легальности подписанного программного обеспечения в условиях, когда понятие вредоносности программного обеспечения порой затруднительно установить (например, так называемые «фиктивные антивирусы» [6], которые предлагают пользователю оплатить регистрацию продукта в обмен на очистку компьютера от несуществующих вирусов).

Дополнительно стоит отметить тот факт, что аналогичные эксперименты были проведены с применением других антивирусных средств, таких как Kaspersky Internet Security, Антивирус dr.Web, Bitdefender [7], и некоторых других. На данный момент описанная особенность обнаружена только у антивируса Microsoft Security Essentials. Вероятно, это связано с тем, что разработчиком ОС семейства Windows и антивируса MSE является одна и та же организация — Microsoft и при создании своего антивируса разработчики, вероятно, опираются на дополнительные знания, которых нет у разработчиков других антивирусов.

Заключение

Обнаруженная и исследованная особенность антивируса Microsoft Security Essentials говорит о целесообразности разработки специальных программных средств исследования и анализа различных антивирусов. Такого рода исследования позволят разработчикам СЗИ совершенствовать собственные программные продукты и получать информацию о недоработках во внутренних механизмах, которые могут эксплуатироваться разработчиками вредоносного ПО с целью достижения своих интересов. С другой стороны, вероятно, данная особенность антивируса MSE является специально созданной закладкой, которая могла использоваться при распространении вируса Stuxnet на целевые компьютеры, так как данный вирус был подписан легитимным цифровым сертификатом [6].

Специально подчеркну: даже если это не связано с вирусом Stuxnet, то такая особенность может использоваться для распространения подобных вирусов.

СПИСОК ЛИТЕРАТУРЫ:

1. *Сильнов Д. С.* Проблемы ложных срабатываний антивирусных средств // Прикладная информатика. 2012. С. 63–66.
2. Microsoft Security Essentials — бесплатный антивирус [Электронный ресурс]. URL: http://windows.microsoft.com/ru-RU/windows/products/security-essentials (дата обращения: 05.09.2012).
3. Microsoft Forefront Endpoint Protection / Антивирус / Защита от вредоносного ПО [Электронный ресурс]. URL: http://www.microsoft.com/ru-ru/server-cloud/forefront/endpoint-protection.aspx (дата обращения: 05.09.2012).
4. Introduction to Code Signing [Электронный ресурс]. URL: http://msdn.microsoft.com/en-us/library/ms537361%28v=vs.85%29.aspx (дата обращения: 05.09.2012).
5. WinHEX [Электронный ресурс]. URL: http://www.winhex.com/winhex/ (дата обращения: 05.09.2012).
6. Ложные антивирусные программы и связанные с ними угрозы / Центр безопасности Microsoft [Электронный ресурс]. URL: http://www.microsoft.com/ru-ru/security/pc-security/antivirus-rogue.aspx (дата обращения: 05.09.2012).
7. Антивирус BitDefender [Электронный ресурс]. URL: http://www.bitdefender.ru (дата обращения: 05.09.2012).
8. The Stuxnet Sting [Электронный ресурс]. URL: http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx (дата обращения: 05.09.2012).