УДК 004.056.57

ИССЛЕДОВАНИЕ НОВЫХ ФУНКЦИЙ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ WINDOWS 8

Галковский А.С., Масальская Е.А.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, galkovskyas@gmail.com

В данной работе рассмотрены улучшения системы безопасности Windows 8, по сравнению с предыдущими версиями Windows, в рамках противодействия буткитам и обеспечения безопасного использования Интернет для обычных пользователей.

Ключевые слова – буткит, SmartScreen; ELAM; UEFI; Secure boot.

ВВЕДЕНИЕ

Ежедневно компьютеры обычных пользователей подвергаются опасности заражения вредоносным ПО. При этом наиболее опасной и трудно диагностируемой разновидностью ПО являются буткиты (англ. “bootkit”).

Буткит осуществляет модификацию загрузочного сектора MBR (Master Boot Record) – первого физического сектора на жёстком диске. При первом обращении к диску управление передаётся буткиту, который загружается в память и в дальнейшем маскирует своё присутствие, перехватывая и подменяя обращения к жёсткому диску. Такое ПО очень трудно обнаружить обычными методами, используемыми антивирусами [1].

В качестве средств защиты Windows 8 использует переход с BIOS на Unified Extensible Firmware Interface (UEFI) а также технологию Early-Launch Anti-Malware Protection (ELAM).

Также в работе описана схема функционирования фильтра SmartScreen для обеспечения безопасного пользования Интернет, т.к. именно глобальная сеть является главным источником вредоносного ПО для пользователей. В целом, использование этих средств должно еще больше повысить безопасность Windows для пользователей.

ПЕРЕХОД С BIOS НА UEFI

BIOS считается устаревшей технологией [2], она была заменена в Windows 8 на UEFI – Extensible Firmware Interface. UEFI – программный интерфейс между ОС и программами, выполняющими низкоуровневые функции. UEFI может использовать безопасный протокол загрузки (Secure Boot). Он позволяет установить один или несколько подписанных ключей в прошивку системы. После включения “безопасной загрузки” UEFI предотвращает загрузку исполняемых файлов или драйверов, если они не подписаны одним из заранее установленных ключей.

Windows 8 совместно с UEFI закрывают дыру в безопасности текущей схемы BIOS, которая позволяет любому загрузчику, в том числе содержащему руткит, загружаться раньше операционной системы. Это означает, что вредоносное ПО в загрузчиках находиться больше не сможет.

ИСПОЛЬЗОВАНИЕ ELAM

Другое улучшение в плане безопасности – это ELAM (Early-Launch Anti-Malware) – технология раннего запуска защиты от вредоносного ПО, которая позволяет антивирусным продуктам запускаться в первую очередь до загрузки остальных программ и приложений.

По сути ELAM – это драйвер, предоставляемый антивирусным вендором, которому гарантирован приоритет при загрузке драйверов режима ядра. Одна из главных возможностей этого средства заключается в том, что он гарантированно позволяет антивирусному драйверу загружаться раньше остальных драйверов в системе и, таким образом, выходить за рамки обычных правил автозагрузки.

Как видно из рисунка 1, ELAM – это часть ядра ОС, и запуск ELAM происходит после инициализации ядра. Поэтому ELAM сам по себе не может быть эффективен для борьбы с буткитами т. к. буткит получает управление гораздо раньше. ELAM эффективен при совмещении с системой UEFI Secure Boot.

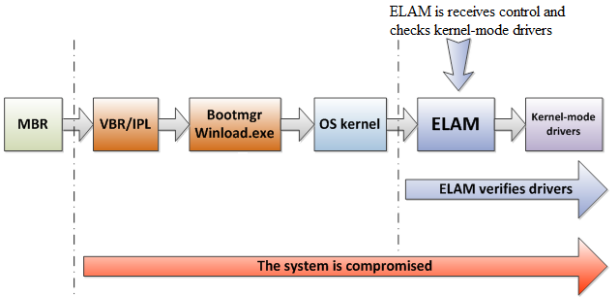

Рис.1. Положение ELAM в процессе загрузки Windows

WINDOWS SMARTSCREEN

SmartScreen – одна из возможностей веб-браузера Internet Explorer, позволяющая обнаруживать и блокировать опасные веб-сайты и предотвращать запуск вредоносного ПО.

При обнаружении вредоносного веб-сайта браузер Internet Explorer полностью блокирует его в случае необходимости. Также возможно "выборочное блокирование" вредоносного или фишингового программного обеспечения, размещенного на надежных веб-сайтах. В таком случае блокируются лишь вредоносные страницы и не затрагиваются остальные части веб-сайта.

Также Фильтр SmartScreen отслеживает загрузку и первый запуск исполняемых файлов, собирает информацию о приложении и отсылает собранную

информацию на сервера Microsoft (https://apprep.smartscreen.microsoft.com). SmartScreen собирает следующую информацию:

- хэш файл;
- цифровая подпись файла (если имеется).

Затем на серверах MS осуществляется проверка рейтинга надежности файла и, в случае опасности, пользователю выводится предупреждение об угрозе.

ВЫВОДЫ

В составе Windows 8 сделано немало улучшений в сфере безопасности. Более того, новая система может стать самой безопасной в линейке релизов Microsoft. Такую оценку защищенности Windows 8 дал специалист компании ESET Арье Горецкий [3]. Однако он сразу же оговорился, что несмотря на предпринятые Microsoft усилия, все равно нельзя исключать риск заражения теми или иными вредоносными модулями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Буткит (Электрон. ресурс). Способ досутпа: URL : http://ru.wikipedia.org/wiki/Буткит
2. UEFI придет на смену BIOS в 2011 году (Электрон. ресурс). Способ досутпа: URL: http://www.pcwork.ru/uefi_pridet_na_smenu_bios_v_2011_godu.htm
3. Aryeh Goretsky. Windows 8:FUD* for thought. (Электрон. ресурс) / Способ доступа: URL: http://go.eset.com/us/resources/white-papers/ESETNA_WP-Windows8-FUD.pdf
4. Современные буткит-технологии и детальный анализ Win32/Gapz (Электрон. ресурс). Способ доступа: URL: http://habrahabr.ru/company/eset/blog/169131/
5. Windows 8: Trusted Boot: Secure Boot – Measured Boot Gapz (Электрон. ресурс). Способ доступа: URL: http://blogs.msdn.com/b/olivnie/archive/2013/01/09/windows-8-trusted-boot-secure-boot-measured-boot.aspx
6. Unified Extensible Firmware Interface (Электрон. ресурс). Способ доступа: URL: http://en.wikipedia.org/wiki/Extensible_Firmware_Interface