РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2012 106 465** (13) **A**

(51) МПК
G06F 12/14 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2012106465/08, 24.02.2012**

Приоритет(ы):
(22) Дата подачи заявки: **24.02.2012**

(43) Дата публикации заявки: **27.08.2013** Бюл. № **24**

Адрес для переписки:
123060, Москва, 1-й Волоколамский пр-д, 10, корп.1, ЗАО Лаборатория Касперского, Управление по интеллектуальной собственности, Н.В. Кащенко

(71) Заявитель(и):
Закрытое акционерное общество "Лаборатория Касперского" (RU)

(72) Автор(ы):
Павлющик Михаил Александрович (CA)

(54) СИСТЕМА И СПОСОБ ПРОВЕРКИ ИСПОЛНЯЕМОГО КОДА ПЕРЕД ЕГО ВЫПОЛНЕНИЕМ

(57) Формула изобретения

1. Способ проверки исполняемого кода перед его выполнением включает этапы, на которых:

а) определяют значения атрибутов страницы памяти в момент ее выделения или модификации атрибутов;

б) сохраняют адрес страницы памяти при одновременно установленных значениях атрибутов страницы памяти, связанных с разрешением на запись и разрешением на выполнение исполняемого кода;

в) меняют, по меньшей мере, один из атрибутов страницы памяти, связанный с разрешением на запись или выполнением исполняемого кода;

г) получают исключение при обращении к странице памяти, адрес который был сохранен на этапе б);

д) определяют атрибуты и адрес страницы памяти, при обращении к которой было получено исключение;

е) производят проверку потока процесса, обращение которого к странице памяти вызвало исключение, и/или проверку исполняемого кода, записанного в странице памяти, при обращении к которой было получено исключение.

2. Способ по п.1, в котором исключение срабатывает при запрещенных действиях с данными сохраненными в странице памяти, при обращении к которой было получено исключение.

3. Способ по п.2, в котором исключением является EXCEPTION_ACCESS_VIOLATION.

4. Способ по п.1, в котором проверка исполняемого кода включает анализ исполняемого кода, записанного в странице памяти, при помощи одного из: сигнатурной проверки, эвристического анализа, эмуляции.

5. Способ по п.1, в котором проверка потока процесса включает анализ потока, обращение которого к странице памяти вызвало исключение, при помощи одного из:

RU 2012106465 A

RU 2012106465 A

сигнатурной проверки, эвристического анализа, эмуляции.

6. Система проверки исполняемого кода перед его выполнением, которая включает:

а) перехватчик, связанный с базой данных работы с памятью, при этом перехватчик отслеживает операции с атрибутами страницы памяти процесса, во время которых:

i. определяет значения атрибутов страницы памяти в момент ее выделения или модификации атрибутов:

ii. сохраняет адрес страницы памяти в базе данных работы с памятью при одновременно установленных значениях атрибутов страницы памяти, связанных с разрешением на запись и разрешением на выполнение исполняемого кода;

iii. меняет, по меньшей мере, один из атрибутов страницы памяти, связанный с разрешением на запись или выполнением исполняемого кода;

iv. получает исключение при обращении к странице памяти и передает антивирусному приложению информацию об исключении, которая включает, по меньшей мере, одно из: информацию о потоке процесса, обращение которого к странице памяти вызвало исключение; адрес страницы памяти;

б) базу данных работы с памятью, предназначенную для хранения адресов страниц памяти;

в) антивирусное приложение, предназначенное для проверки, по меньшей мере, одного из: потока процесса, обращение которого к странице памяти вызвало исключение; исполняемого кода, записанного в странице памяти, при обращении к которой было получено исключение.

7. Система по п.6, в которой исключение срабатывает при запрещенных действиях с данными сохраненными в странице памяти, при обращении к которой было получено исключение.

8. Система по п.6, в которой исключением является EXCEPTION_ACCESS_VIOLATION.

9. Система по п.6, в которой проверка исполняемого кода включает анализ исполняемого кода, записанного в странице памяти, при помощи одного из: сигнатурной проверки, эвристического анализа, эмуляции.

10. Система по п.6, в которой проверка потока процесса включает анализ потока, обращение которого к странице памяти вызвало исключение, при помощи одного из: сигнатурной проверки, эвристического анализа, эмуляции.

11. Система по п.6, где в качестве базы данных адресов используется Page Table, где в Page Table Entry (PTE) соответствующей страницы выставляется один из зарезервированных битов.

RU 2012106465 A

RU 2012106465 A