РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2012 102 818** (13) **A**

(51) МПК
G06F 21/00 (2013.01)

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21)(22) Заявка: **2012102818/08, 07.07.2010**

Приоритет(ы):
(30) Конвенционный приоритет:
10.07.2009 GB 0912017.1

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

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **10.02.2012**

(86) Заявка PCT:
EP 2010/059762 (07.07.2010)

(87) Публикация заявки PCT:
WO 2011/003958 (13.01.2011)

Адрес для переписки:
191186, Санкт-Петербург, а/я 230, "АРС-ПАТЕНТ", пат.пов. М.В.Хмаре, рег. № 771

(71) Заявитель(и):
Ф-СЕКЬЮЭ КОРПОРЕЙШЕН (FI)

(72) Автор(ы):
НИЕМЕЛЯ Ярно (FI),
ХАРМОНЕН Тимо (FI),
ЗИРВАЛЬД Йорн (DE),
СТОХЛБЕРГ Мика (FI)

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ ПРОВЕРКИ ФАЙЛОВОЙ СИСТЕМЫ НА НАЛИЧИЕ ВИРУСОВ

(57) Формула изобретения

1. Способ выполнения антивирусного сканирования файловой системы, включающий следующие шаги:

получают, для хранящегося в файловой системе файла, результаты промежуточного сканирования до завершения сканирования указанного файла;

сохраняют результаты промежуточного сканирования в базе данных;

определяют, в ходе последующего антивирусного сканирования файловой системы и до выполнения промежуточного сканирования хранящегося в файловой системе указанного файла, наличие в базе данных результатов промежуточного сканирования, относящихся к указанному файлу; и

в случае наличия результатов промежуточного сканирования в базе данных для конкретного типа промежуточного сканирования не выполняют это промежуточное сканирование указанного файла, а в случае отсутствия результатов промежуточного сканирования в базе данных для конкретного типа промежуточного сканирования выполняют это промежуточное сканирование указанного файла.

2. Способ по п.1, отличающийся тем, что результаты промежуточного сканирования представляют собой результаты, выбранные из данных сканирования, относящихся к контрольной сумме, информации о заголовке файла, количеству секций файла, хеш-значениям для файла, хеш-значениям для частей файла, ключевым данным эмуляции, значениям циклического контроля избыточности или результатам поиска байтов.

RU 2012102818 A

RU 2012102818 A

3. Способ по п.1, отличающийся тем, что при наличии сигнатуры нового вредоносного программного обеспечения (ПО) включает определение, на основании хранящихся в базе данных результатов, тех файлов, которые не соответствуют предварительно отфильтрованной информации, связанной с сигнатурой нового вредоносного ПО, и исключение этих файлов из последующего сканирования файловой системы.

4. Способ по п.3, отличающийся тем, что предварительно отфильтрованную информацию отбирают из данных, включающих дату последнего сканирования, тип файла, размер файла, количество секций файла, информацию о заголовке файла, хеш-значения для файла, хеш-значения для частей файла, значения циклического контроля избыточности и результаты поиска байтов,

5. Способ по любому из пп.1-4, отличающийся тем, что включает следующие шаги:

сохраняют в базе данных дату последней модификации файла;

оценивают, когда впервые стало возможным заражение вредоносным ПО; и

при последующем сканировании файловой системы исключают из процесса сканирования те файлы, которые в последний раз были модифицированы раньше, чем впервые стало возможным заражение вредоносным ПО.

6. Способ по п.5, отличающийся тем, что включает следующие шаги:

сохраняют в базе данных дату последнего сканирования файла;

сравнивают дату последнего сканирования файла с датой, когда антивирусная база данных была обновлена с внесением определения нового вредоносного ПО;

при последующем сканировании файловой системы исключают из процесса сканирования те файлы, которые в последний раз были сканированы после обновления антивирусной базы данных с внесением определения нового вредоносного ПО.

7. Способ по п.1, отличающийся тем, что база данных расположена удаленно по отношению к файловой системе.

8. Способ по п.7, отличающийся тем, что включает следующие шаги:

на удаленном антивирусном сервере и до передачи сигнатуры вредоносного ПО клиентскому устройству для сканирования файлов в файловой системе используют результаты промежуточного сканирования, хранящиеся в базе данных, для определения набора сигнатур вредоносного ПО, относящихся к файлам в файловой системе; и

передают набор сигнатур вредоносного ПО на клиентское устройство.

9. Способ по п.7 или 8, отличающийся тем, что включает следующие шаги:

сохраняют в базе данных результатов промежуточного сканирования результаты промежуточного сканирования для любого множества файловых систем, хранящихся на множестве клиентских устройств;

для каждого клиентского устройства сохраняют дополнительные данные, содержащие географическое местоположение клиентского устройства или время, когда файл был сохранен в файловой системе на клиентском устройстве;

на удаленном антивирусном сервере используют эти дополнительные данные для определения набора клиентских устройств, у которых запрашивается выборка всего или части файла; и

передают запрос на выборку всего или части файла на каждое клиентское устройство из набора клиентских устройств.

10. Компьютерное устройство, включающее:

память для хранения файловой системы;

антивирусную функцию для выполнения антивирусного сканирования, по меньшей мере, одного хранящегося в файловой системе файла, причем антивирусная функция осуществляет, по меньшей мере, одно промежуточное сканирование указанного файла;

средства хранения результатов, по меньшей мере, одного промежуточного сканирования в базе данных результатов промежуточного сканирования;

RU 2012102818 A

RU 2012102818 A

при этом антивирусная функция осуществляет последующее сканирование указанного файла в файловой системе и определяет, перед выполнением промежуточного сканирования указанного файла, наличие в указанной базе данных результатов промежуточного сканирования;

причем, в случае наличия результата промежуточного сканирования в указанной базе данных, антивирусная функция не выполняет это промежуточное сканирование указанного файла, а в случае отсутствия результата промежуточного сканирования в базе данных, антивирусная функция выполняет это промежуточное сканирование указанного файла.

11. Компьютерное устройство по п.10, отличающееся тем, что включает базу данных результатов промежуточного сканирования.

12. Компьютерное устройство по п.10, отличающееся тем, что включает передатчик для передачи результатов промежуточного сканирования на удаленный узел с целью наполнения базы данных результатов промежуточного сканирования.

13. Антивирусный сервер для использования в коммуникационной сети, включающий:

средства связи с клиентским устройством, имеющим файловую систему, в которой хранится множество файлов;

процессор для осуществления антивирусного сканирования, по меньшей мере, одного файла в файловой системе, при этом антивирусное сканирование включает, по меньшей мере, одно промежуточное сканирование указанного файла;

средства хранения результатов промежуточного сканирования в базе данных результатов промежуточного сканирования.

14. Антивирусный сервер по п.13, отличающийся тем, что процессор выполнен с возможностью использования результатов промежуточного сканирования, хранящихся в базе данных, для определения набора сигнатур вредоносного ПО, относящихся к файлам в файловой системе на клиентском устройстве; а средства связи с клиентским устройством выполнены с возможностью передачи набора сигнатур вредоносного ПО на клиентское устройство.

15. Антивирусный сервер по п.13 или 14, отличающийся тем, что процессор выполнен с возможностью использования данных, хранящихся в базе данных результатов промежуточного сканирования, для определения набора клиентских устройств, у которых запрашивается выборка всего или части файла; а средства связи с клиентским устройством выполнены с возможностью передачи запроса на выборку всего или части файла с клиентского устройства.

16. Компьютерная программа, содержащая машиночитаемый код, который при запуске на программируемом компьютере заставляет его выполнять антивирусное сканирование файловой системы, включающая команды:

получения, для хранящегося в файловой системе файла, результатов промежуточного сканирования до завершения сканирования указанного файла;

хранения результатов промежуточного сканирования в базе данных;

определения, в ходе последующего антивирусного сканирования файловой системы и до выполнения промежуточного сканирования хранящегося в файловой системе указанного файла, наличия в базе данных результатов промежуточного сканирования, относящихся к указанному файлу; и

в случае наличия результатов промежуточного сканирования в базе данных для конкретного типа промежуточного сканирования, невыполнения этого промежуточного сканирования указанного файла, а в случае отсутствия результатов промежуточного сканирования в базе данных для конкретного типа промежуточного сканирования, выполнения этого промежуточного сканирования указанного файла.

17. Компьютерная программа по п.16, включающая команды определения, при

RU 2012102818 A

RU 2012102818 A

наличии сигнатуры нового вредоносного ПО, на основании результатов, хранящихся в базе данных, тех файлов, которые не соответствуют предварительно отфильтрованной информации, связанной с сигнатурой нового вредоносного ПО, и исключения этих файлов из последующего сканирования файловой системы.

18. Компьютерная программа по п.16 или 17, включающая команды хранения в базе данных даты последней модификации файла, оценки момента времени, когда впервые стало возможным заражение вредоносным ПО и, при последующем сканировании файловой системы, исключения из процесса сканирования тех файлов, которые в последний раз были модифицированы раньше, чем стало возможным заражение вредоносным ПО.

19. Компьютерная программа по п.18, включающая команды хранения в базе данных даты последнего сканирования файла, сравнения даты последнего сканирования файла с датой, когда антивирусная база данных была обновлена с внесением определения нового вредоносного ПО и, при последующем сканировании файловой системы, исключения из сканирования тех файлов, которые в последний раз были сканированы после обновления антивирусной базы данных с внесением определения нового вредоносного ПО.

20. Компьютерная программа по п.16, включающая команды осуществления связи с базой данных, расположенной удаленно по отношению к файловой системе.

21. Компьютерная программа по п.20, включающая команды получения от удаленного антивирусного сервера набора сигнатур вредоносного ПО, определенных на удаленном антивирусном сервере при помощи результатов промежуточного сканирования, хранящихся в базе данных, с целью определения набора сигнатур вредоносного ПО, относящихся к файлам в файловой системе.

22. Компьютерная программа, содержащая машиночитаемый код, который при запуске на программируемом компьютере заставляет его выполнять антивирусное сканирование файловой системы для реализации способа, охарактеризованного в любом из пп.1-9.

23. Компьютерная программа, содержащая машиночитаемый код, который при запуске на компьютерном устройстве заставляет его вести себя как компьютерное устройство, охарактеризованное в любом из пп.10-12.

24. Компьютерная программа, содержащая машиночитаемый код, который при запуске на сервере заставляет его вести как антивирусный сервер, охарактеризованный в любом из пп.13-15.

25. Носитель информации, на котором записана компьютерная программа, охарактеризованная в любом из пп.16-24.

RU 2012102818 A

RU 2012102818 A