Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 19 June 2018

Case Number: T 2052/15 - 3.5.06

Application Number: 10176515.4

Publication Number: 2306356

IPC: G06F21/00

Language of the proceedings: EN

Title of invention:
Asynchronous processing of events for malware detection

Applicant:
Kaspersky Lab, ZAO

Headword:
Asychronous antivirus processing/KASPERSKY

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - after amendment (yes)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 2052/15 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 19 June 2018

Appellant: (Applicant)	Kaspersky Lab, ZAO 39A/3 Leningradskoe Shosse Moscow 125212 (RU)
Representative:	Sloboshanin, Sergej V. Füner, Ebbinghaus, Finck, Hano Mariahilfplatz 3 81541 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 11 June 2015 refusing European patent application No. 10176515.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	W. Sekretaruk
Members:	M. Müller
	G. Zucka

Summary of Facts and Submissions

I. The appeal is against the decision of the examining division dated 11 June 2015 to refuse European patent application No. 10176515.4 for lack of inventive step in view of the documents

D2: WO 2007/003916 A2,
D3: US 2008/022407 A1, and
D8: US 6 973 577 B1.

II. Notice of appeal was filed on 5 August 2015, the appeal fee being paid on the same day. A statement of grounds of appeal was received on 25 September 2015. The appellant requested that the decision be set aside and a patent granted on the basis of claims 1-15 according to the main or the auxiliary request as filed with the grounds of appeal.

III. In an annex to a summons to oral proceedings, the board informed the appellant of its provisional opinion that the claimed invention lacked inventive step over D8.

IV. In response to the summons, by letter of 16 May 2018, the appellant filed amended claims and arguments. During the oral proceedings, held as scheduled on 19 June 2018, the appellant filed further amended claims, now numbered 1-12, and new description pages 6 and 7 and requested the grant of a patent on this basis, in combination with the following documents:

description, pages
1, 2, 2b, 3 and 5 filed on 22 September 2011
2a filed on 4 February 2012
4 and 8-18 as originally filed
and drawings, sheets

1-10 as originally filed.

V. The independent claims 1 and 6 read as follows:

"1. A method for asynchronous processing of system events (210) on a computer system, the method comprising:

(a) detecting a system event (210) on the computer system and intercepting the system event for filtering, wherein the system event (210) comprises a system call;

(b) filtering the system event (210) through at least one filter (240) to determine if the system event (210) matches a security criteria [sic];

(c) if the system event (210) does not pass through at least one filter (240), sending the system event for further processing; and

if the system event (210) passes through the at least one filter (240), creating a copy of the system event (210) which is passed through the at least one filter (240) for asynchronous anti-virus processing the copy of the system event (210), and releasing the original system event (210) so that the process which caused the event continues its uninterrupted execution;

(d) placing the copy of the system event (210) into a queue for asynchronous anti-virus processing;

(e) creating a control record based on the event copy by using information about the event;

(f) deleting the copy of the system event (210) from the queue;

(g) performing asynchronous anti-virus processing on the control record of the system event (210), wherein the asynchronous anti-virus processing of the control record comprises a signature scanning of the control record of the system event (210) and analysing the process that caused the system event by executing the process in an emulator and by generating a behavior log

for the process and terminating the process that caused the system event (210), if the anti-virus processing reveals a malicious nature of the system event (210); and

(h) for a process that has behavior differences compared to a previous known non-malicious version of the process but also substantial similarities to the previous known non-malicious process, classifying the process as non-malicious."

"6. A system for asynchronous processing of system events (210), the system comprising a processor, a memory coupled to the processor, and computer code loaded into the memory for implementing the steps of claim 1."

VI. At the end of the oral proceedings, the chairman announced the decision of the board.

Reasons for the Decision

The invention

1. The application relates to the field of malware detection.

1.1 Several types of prior-art system are discussed. Signature scanning systems search for known malicious code patterns and allow a program to execute only if it is found to be "clean" (page 2, paragraph 2; all references hereinafter to the description are to the description as originally filed). Emulation-based systems analyse the behaviour of unknown programs in a

protected environment (paragraph 3). Other systems allow unknown programs to run, but intercept "events" which may cause harm and perform an analysis at that point (paragraph 5).

1.2 It is said that the prior-art methods are too time-consuming and thus cause inconvenient delays in the operation of a computer system (see page 2, line 2, to page 3, line 7).

1.3 The invention thus proposes a system based on event interception and *asynchronous*, on-the-fly behavioural analysis.

1.4 More specifically, system events are intercepted and passed through one of several filters (see e.g. figure 2, no. 240). Each of the filters represents a "security criterion", and an event not fulfilling such a criterion is said "not [to] pass through" the corresponding filter (see page 6, paragraph 2, and figure 3). If an event "does not pass through at least on[e] of the filters", i.e. if it does not fulfil at least one "filtering security criteri[on]", it is considered safe and "sent for further processing"; if it passes through all the filters, a "copy" of the event is created and added to an event queue before the event is "released for further processing" (*loc. cit.*). The copy is then asynchronously processed. It is "converted into a control record" by adding "information about the event" and passed to an antivirus (AV) utility (see page 6, paragraph 3, and figure 4, in particular step 440), which performs "signature scanning" using "short signatures" representing "behaviour characteristics taken over a period of time" and executes the process which caused

the event in an emulator. Emulation of the process produces a "behavior log" for further analysis (see figure 5 and page 6, last paragraph, to page 7, paragraph 2).

1.5 If the AV utility reveals that an event is malicious, the process causing it is "blocked and terminated" (*loc. cit.*). It is disclosed that the "harm caused by malware during the delay period can be easily compensated by roll backs, incremental backups (snapshots), virtual copies etc." (see page 6, penultimate paragraph). No further details on these "repair" activities are disclosed.

Article 123(2) EPC

2. The wording of claim 1 as it now reads is disclosed in the application as originally filed, in figures 3-5 and the corresponding passages of the description. More specifically, the "by" phrase in step (e) is disclosed in figure 4, item no. 440, and the use of an emulator and the creation of a behavior log are disclosed in figure 5, items no. 530 and 580. Feature (h) as it now reads corresponds to feature (h) in claim 1 as originally filed.

Article 84 EPC

3. Claim 1 comprises some very broad features.

3.1 The control record is created from the queued copy of the system event to be analysed and undergoes "signature scanning" (see claim 1, lines 9-10, and steps (e) and (g)) and must thus be construed as a data structure. Compared with the copy of the system event, the control record contains some additional - albeit

undefined - "information about the event". The control record and the copy of the system event are therefore different from each other. Although the signature scanning of the control record (see step (g)) is not further defined in the claim, the board takes the view that the skilled person would interpret it, by analogy with the signature scanning of program code (as explained on page 2 of the description, in paragraph 2), as a comparison of the control record with predetermined patterns in order to determine whether it represents a malicious or non-malicious system event.

3.2 Step (h) specifies that a process may be found to be non-malicious - even though it has "behavior differences" from a known non-malicious process - if it also has "substantial similarities" to that process. This feature does not define what similarities are considered or which ones might be considered "substantial" enough for the process under consideration to benefit from the classification of the earlier process as non-malicious. The board understands this feature to imply, in very broad terms, that the decision whether a process is malicious is based on behaviour and code similarity.

3.3 The board considers that the breadth of these features does not render the claims unclear.

The prior art

4. D8 discloses "dynamically detecting computer viruses through associative behavioral analysis" (see abstract and column 2, lines 32-41). A "monitor/analyzer" component is used to intercept system calls (see figures 2, 3 and 5, and column 4, lines 15-22

and 53-58). If the intercepted event is a "monitored event" (see column 5, lines 26-39, and column 6, lines 26-42), it is determined whether the calling application performs a sequence of actions which are known to be characteristic of computer viruses and thus suspicious (column 4, lines 22-25); such actions may, for instance, be the writing of a few bytes to the end of a file or the sending of an email to a name in an address book (see column 5, line 43, to column 6, line 7). If a suspicious sequence of actions is detected, the event is stored in a database (see figure 2, no. 37) in the form of an "event log record" (figure 4; see also column 6, lines 55-58). Based on the event log records in the database, histograms are generated and analysed so as to detect "repetitions of suspicious behavioral patterns" (column 4, lines 25-27, 35-36 and 62-67; column 5, lines 7-17 and 55-58; and column 6, lines 5-7). If suspicious behaviour is detected, an "alert" is produced (column 5, lines 24-25).

5. Documents D2 and D3 were cited in the decision (see points 3.5 and 3.6 of the reasons) to establish that it was known in the art to block or terminate processes determined to be unsafe and to classify processes as safe or unsafe based on comparison with known objects. As the appellant did not challenge these assumptions, no further reference to D2 and D3 is required.

Inventive step, Article 56 EPC

6. Irrespective of whether D8 discloses or suggests "asynchronous antivirus processing" in general, which was the decisive issue for the appellant (see the grounds of appeal, page 6, point e)), D8 does not

disclose or suggest the use of an emulator for that purpose. More explicitly, D8 clearly does not disclose carrying out behavioural analysis on a copy of a suspicious process while the process itself is allowed to proceed.

6.1 The board takes the view that this set-up provides a new balance between the security provided by antivirus processing and the responsiveness of a process which is being analysed. In other words, the invention makes it possible to carry out antivirus processing whilst disturbing the user owning that process only when necessary.

6.2 The board takes the view that increasing the responsiveness of a computer in a way which does not depend on which - or which type of - software it is executing affects the computer technically and thus is a technical problem. Moreover, using the available computing resources in an asynchronous - and thus possibly parallel - manner is a technical solution to that problem.

6.3 As the subject-matter of claim 1 - and, as a consequence, of claim 6 - is the non-obvious technical solution to a technical problem, a patent is to be granted for the claimed invention.

Order

For these reasons it is decided that:

1. The decision under appeal is set aside.
2. The case is remitted to the examining division with the order to grant a European patent based on the following documents:

claims 1-12	filed on 19 June 2018
description, pages	
1, 2, 2b, 3 and 5	filed on 22 September 2011
2a	filed on 4 February 2012
6 and 7	filed on 19 June 2018
4 and 8-18	as originally filed
and drawings, sheets	
1-10	as originally filed.

The Registrar: The Chairman:

B. Atienza Vivancos W. Sekretaruk

Decision electronically authenticated