Internal distribution code:

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

Datasheet for the decision of 12 December 2023

Case Number: T 3295/19 - 3.5.06

Application Number: 13167434.3

Publication Number: 2629231

IPC: G06F21/56

Language of the proceedings: EN

Title of invention:
Methods and apparatus for dealing with malware

Applicant:
Webroot Inc.

Headword:
Dealing with Malware/WEBROOT

Relevant legal provisions:
EPC Art. 84

Keyword:
Claims - clarity (no)

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 3295/19 - 3.5.06

D E C I S I O N
of Technical Board of Appeal 3.5.06
of 12 December 2023

Appellant: (Applicant)	Webroot Inc. 385 Interlocken Crescent Broomfield, CO 80021 (US)
Representative:	Betten & Resch Patent- und Rechtsanwälte PartGmbB Maximiliansplatz 14 80333 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 25 July 2019 refusing European patent application No. 13167434.3 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	M. Müller
Members:	A. Teale
	K. Kerber-Zubrzycka

Summary of Facts and Submissions

I. This is an appeal against the decision, dispatched with reasons on 25 July 2019, to refuse European patent application No. 13 167 434.3. According to the reasons for the decision, the main and first to third auxiliary requests did not comply with Article 76(1) EPC, regarding added subject-matter over the parent application (see below), and Article 56 EPC, regarding inventive step in view of the combination of either D1 or D5 with D4, these documents being:

D1: US 2002/0194490 A1,
D4: US 2002/0147923 A1 and
D5: EP 1 549 012 A1.

II. This is a divisional application of European patent application (the "parent application") No. 06755686.0, published as WO 2007/003916 A2.

III. A notice of appeal and the appeal fee were received on 4 October 2019, the appellant requesting that the decision be set aside and that a patent be granted on the basis of the documents on file. The appellant also made an auxiliary request for oral proceedings.

IV. In a statement of grounds of appeal, received on 4 December 2019, the appellant reiterated the requests made in the notice of appeal.

V. In an annex to a summons to oral proceedings the board set out its provisional opinion on the appeal, as follows. The board had doubts as to whether the subject-matter of claims 1 and 9 of all requests involved an inventive step, Article 56 EPC, in view of

the disclosure of D5 alone. The board also had doubts regarding the clarity of claims 1 and 9 of all requests, Article 84 EPC. The application seemed however to comply with Article 76(1) EPC regarding amendments vis-à-vis the parent application.

VI. With a response, received on 13 November 2023, the appellant filed amended pages of the description and amended claims according to a new fourth auxiliary request.

VII. At the oral proceedings, held on 12 December 2023, the appellant requested that the decision under appeal be set aside and that a patent be granted based on the main request or one of the auxiliary requests 1 to 3 filed with the statement setting out the grounds of appeal or, alternatively, on auxiliary request 4, submitted with the letter of 13 November 2023.

VIII. The application is being considered in the following form:

Description (all requests):
pages 1 to 3, 5 to 32 and 34 to 35, as originally filed, pages 4 and 4a, received on 4 September 2018, and pages 33 and 36, received on 13 November 2023.

Claims (received on 31 May 2019):
Main request: 1 to 10.
First auxiliary request: 1 to 10.
Second auxiliary request: 1 to 10.
Third auxiliary request: 1 to 10.

Claims (received on 13 November 2023):
Fourth auxiliary request: 1 to 10.

Drawings (all requests):
Pages 1/3 to 3/3, as originally filed.

IX. Claim 1 according to the main request reads as follows:

"A method of classifying a computer object as safe or unsafe, the method comprising: at a base computer holding a database (7), receiving data about a computer object from each of plural remote computers on which the computer object is stored; storing at the database said data received from plural remote computers, wherein the data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the respective remote computers, said information including at least a key of the computer object initiating the event, an event type, and a key of a computer object on which the event is being performed, wherein the key uniquely identifies the respective computer object; and classifying the computer object as safe or unsafe on the basis of relationships between the computer object and other computer objects based on the event information and a classification of said other computer objects as known, unknown, known safe or known unsafe, wherein the computer object is considered to have a relationship based upon an event performed by the computer object upon another of the plural computer objects or upon the computer object by another of the plural computer objects."

X. Claim 1 of the first auxiliary request differs from that of the main request in the addition of the following features at the end of the claim: "deducing how a behavior of the computer object is changed by its association with another computer object using the relationship between the computer object and the other

computer objects, wherein the computer object is classified as unsafe if the deduced behavior is malevolent."

XI. Claim 1 of the second auxiliary request has been amended considerably with respect to that of the main request and reads as follows, additions being indicated in **bold**.

"A method of **determining whether** a computer object **is** safe or unsafe, the method comprising: **storing at a database (7) of a base computer information received from plural remote computers, wherein the database is populated over time with the information relating to each computer object run on the plural remote computers, the received information including captured events of the computer objects;** and **determining whether** the computer object **is** safe or unsafe on the basis of relationships between the computer object and other computer objects based on the information and a classification of said other computer objects as known, unknown, known safe or known unsafe, wherein the computer object is considered to have a relationship based upon an event performed by the computer object upon another of the plural computer objects or upon the computer object by another of the plural computer objects."

XII. Claim 1 of the third auxiliary request combines the amendments of the two previous requests.

XIII. Claim 1 of the fourth auxiliary request differs from that of the main request in the addition of the following two passages:

"wherein an unsafe computer object is a computer object that has been found to be malware, wherein the malware is an executable object that contains malicious code including a virus, Trojan, worm, spyware, and/or adware" and

"and wherein, if at least one of the other computer objects, to which said computer object is related, is classified as unsafe, the computer object is classified as unsafe; and if the computer object is classified as unsafe, stopping execution of the computer object".

Reasons for the Decision

1. Admissibility of the appeal

1.1 In view of the facts set out at points I, III and IV above, the appeal fulfills the admissibility requirements under the EPC and is consequently admissible.

2. Summary of the invention

2.1 According to claim 1, the invention relates to classifying computer objects (referred to below as "objects") as "safe" or "unsafe". As illustrated in figure 1, the application concerns a "base" computer (3) classifying objects which are potentially malware. The application uses the term "malware" to refer to an executable computer file, such as a virus, a Trojan, a worm, spyware and adware; see page 1, lines 13 to 15.

2.2 The base computer classifies an object based on data about the object received via the internet (1) from a plurality of other "remote" computers (2) on which the object is stored. The data is stored in a "community

database" (7) located in the base computer. The object data includes executable instructions in the object, the size of the object, its name, the logical storage location or path of the object on the remote computers, the vendor of the object, the software product and version associated with the object and "events" initiated by or involving the object when the object is created, configured or runs on the remote computers; see page 17, lines 14 to 20.

2.3 The relationship between objects is used to identify malware, two objects being related if one object performs an "event" (see above) on the other. A related object can be classified as "known", "unknown", "known safe" or "known bad"; see page 20, lines 6 to 8.

2.4 The volume of data sent by the remote computers to the base computer may be reduced by sending a hash function of an object, termed a "key", instead of the object itself; see page 17, line 24, to page 18, line 15.

2.5 As shown in figure 2, each remote computer has a "local" database (see step 22) containing keys, also known as "signatures" (see page 14, line 26) relating to objects and their effects. If an object is known to not be malware from the local database then it is allowed to run on that computer; see step 23. If the object is known from the local database to be unsafe, then the user may be asked for approval before running it, if at all. If the object is unknown on the local database, then a signature is created (step 28) and passed to the community database (7); see page 14, line 22, to page 17, line 8.

2.6 The application sets out five distinct processes for establishing whether an object is safe, unsafe or

"suspicious" (see page 19, line 1, to page 23, line 2), the claims of all requests being directed to the second process which uses the relationships between objects to classify them; see page 19, line 29, to page 21, line 8.

2.7 The first auxiliary request is directed to classifying an object as unsafe if its association with another object causes it to behave malevolently; see page 20, lines 14 to 15. The second auxiliary request goes in a different direction, being no longer restricted to the use of keys in the database, and setting out its population over time using data received from the remote computers; see page 14 to 16. The third auxiliary request combines the amendments of the two previous requests. The fourth auxiliary request adds an explicit definition of the term "malware" (see page 1, lines 13 to 15) and sets out stopping the execution of an object classified as unsafe; see page 15, lines 1 to 2.

3. The admittance of the fourth auxiliary request into the proceedings, Article 13(2) RPBA 2020

3.1 These amended claims, received more than a month before the oral proceedings, contained amendments aimed at overcoming the board's objections in its summons under Articles 84 and 56 EPC.

3.2 The board consequently admitted this request into the proceedings.

4. Clarity, Article 84 EPC

4.1 The distinction between "safe" and "unsafe" objects

4.1.1 In the annex to the summons to oral proceedings the board raised a clarity objection against claims 1 and 9 of all requests regarding the terms "safe" and "unsafe" in relation to adware, mentioned in the definition of malware on page 1, lines 13 to 15. Whilst adware might be seen as undesirable, even annoying, "malware", the board doubted whether the skilled person would have considered it "unsafe". Moreover the claims did not set out establishing from first principles whether an object, i.e. a program, was "safe" or "unsafe", for instance using antivirus software; see page 1, lines 17 to 20. Objects were merely "marked" as, i.e. deemed to be, "unsafe". It was consequently unclear how, based only on the knowledge of the *relationships* between objects, related objects could be classified as "safe" or "unsafe"; see page 30, line 30, to page 32, line 13.

4.1.2 Categorising objects as "safe" or "unsafe" based on their relationships - in the claimed generality - also seemed *prima facie* to raise some issues which were not explained in the application which would have caused the skilled person to doubt whether two cases, in particular, were covered by the claims.

4.1.3 Firstly, the operating system itself of the remote computer could be considered to be an "object" and categorized as "unsafe" if an "unsafe" program was created or executed by the operating system. In the case of the fourth auxiliary request, according to claim 1, the "unsafe" object, i.e. the operating system, would not be executed, thus stopping the remote computer.

4.1.4 Secondly, it seemed that the email program of the remote computer would be marked as "unsafe" if an

"unsafe" program caused any email to be sent, even if the email itself was safe.

4.1.5 The board also questioned the clarity of the term "known" in the (pre-)classification of objects set out in claim 1 as "known", "unknown", "known safe" and "known unsafe" as a precursor to their classification as "safe" or "unsafe".

4.1.6 The appellant argued that the invention aimed to detect malware, i.e. "unsafe" software, as soon as possible. New objects were "preclassified" at the remote computers and then "classified" at the community database (7) (see figure 2) which collected information from the remote computers. Moreover it was reasonable to shut down the remote computer under certain circumstances.

4.1.7 The board finds that the skilled person could not have understood from claim 1 of the main request, even when interpreted in the light of the description, whether an object was to be classified as "safe" or "unsafe". Already due to the case of the initial object being undefined, it is unclear whether a related object, which is deemed "unsafe", is actually harmful, or whether objects are classified as being "unsafe" based on a mere, and possibly non-technical, policy decision, e.g. to consider all objects from a particular software manufacturer as unsafe. Moreover, it is not evident what harm, if any, could occur. For instance, "adware" might reasonably be considered "malware", but at the same time "safe". Also, since the "events" are only vaguely defined, it is unknown whether or when the fact that an "unsafe" object is involved with another object in an event allows the conclusion that the other object is also "unsafe", or in what sense. Again, therefore,

an object classified as "unsafe" according to the claimed method may not actually be harmful, and it remains unclear what other properties of interest it has. There is also no limitation in claim 1 regarding how an object became "known" so that the distinction between the expressions in claim 1 "known", "unknown", "known safe" and "known unsafe" was unclear.

4.2 Conclusion on clarity

4.2.1 The board concludes that the central terms "safe" and "unsafe", as well as "known", "unknown", "known safe" and "known unsafe", are unclear and render the subject-matter of claim 1 of the main request unclear as a whole, Article 84 EPC.

4.2.2 As the unclear terms are present in claim 1 of all four auxiliary requests, this means that claim 1 of all requests is unclear. The same conclusion also applies to the corresponding independent apparatus claim of each request.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

L. Stridde M. Müller

Decision electronically authenticated