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 3292/19 - 3.5.06

Application Number: 13167436.8

Publication Number: 2629232

IPC: G06F21/56, G06F21/57

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. 56, 112
RPBA 2020 Art. 13(2)

Keyword:
Inventive step - (no)
Referral to the Enlarged Board of Appeal (no)

Decisions cited:
G 0001/19, T 0115/85, T 0528/07, T 0543/14

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 3292/19 - 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. 13167436.8 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. 13 167 436.8. According to the reasons for the decision, the application had been amended introducing subject-matter extending beyond that of the parent application, Article 76(1) EPC. Claim 1 was unclear, Article 84 EPC, and the invention was insufficiently disclosed, Article 83 EPC. The claimed subject-matter also lacked inventive step, Article 56 EPC, in view of the following document:

D1: US 2003/0131256 A1.

II. The present application is a divisional application of European patent application No. 06755686.0 (the "parent application"), published as WO 2007/003916 A2. The parent application was refused, leading to an appeal in case T 1901/18 which was withdrawn on 25 April 2022. There is a second divisional application from the same parent application, namely European patent application No. 13 167 434.3, published as EP 2 629 231, which was refused, leading to appeal case T 3295/19 which is being treated by the present board in the same composition.

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 a patent granted based on the requests on file.

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

that the decision be set aside and a patent granted based on the requests on file. The appellant also made an auxiliary request for oral proceedings.

V. In an annex to a summons to oral proceedings the board set out its provisional view on the appeal, as follows. The subject-matter of the application did not extend beyond that of the parent application, Article 76(1) EPC. The invention was disclosed in a manner sufficiently clear and complete for it to be carried out by the skilled person, Article 83 EPC. The board did not agree with the clarity objection, Article 84 EPC, raised in the decision against all requests but did raise a clarity objection of its own against the second and third auxiliary requests. The subject-matter of the independent claims of all requests seemed to lack inventive step in view of D1, Article 56 EPC.

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

VII. At the oral proceedings, held on 12 December 2023, the appellant referred to the following two documents which had been filed in the related case T 3295/19:

D2: Wikipedia entry on "Malware" from 28 June 2005.

D3: "Will anti-virus programs protect against malware?", downloaded on 10 November 2023 from the URL https://arstechnica.com/information-technology/2004/11/malware/

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

submitted with the statement setting out the grounds of appeal or, alternatively, based on auxiliary request 4 submitted with the letter of 12 November 2023. The appellant also submitted a request for referral of a question to the Enlarged Board of Appeal under Article 112 EPC which reads, editorial amendments by the board aside, as follows:

1. In the assessment of inventive step, can the provision of information about not detecting processes run on a computer being marked as malware (with a selected security product configuration) contribute to solving a technical problem by producing a technical effect according to case law T 543/14 and T 528/07 or not?

2. If the answer to the first question is no, what are the relevant criteria for assessing whether the said information providing a technical condition of the computer is considered to be a technical feature capable of contributing to solving a technical problem?

After deliberation by the board, the Chairman announced that the board rejected the request for referral of a question to the Enlarged Board of Appeal. He further announced the decision of the Board not to admit auxiliary request 4 into the appeal proceedings under Article 13(1,2) RPBA 2020. At the end of the oral proceedings the board announced its decision on the appeal.

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

Description (all requests):
pages 1 to 3, 5 to 32, 34 and 35, received on 13 May 2013, 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 5.
First auxiliary request: 1 to 5.
Second auxiliary request: 1 to 5.
Third auxiliary request: 1 to 5.

Claims (received on 13 November 2023):
Fourth auxiliary request: 1 to 5.

Drawings (all requests):
Pages 1/3 to 3/3, received on 13 May 2013.

IX. Claim 1 of the main request reads as follows:

"A method of determining the protection that a first remote computer of a plurality of remote computers has from malware, the method comprising: receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2); receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7); receiving at the database (7) details of processes run by said plurality of remote computers (2); storing the information and the details in the database (7); searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and providing information to the user of said first remote computer (2) that said first

remote computer (2) may be susceptible to attack by said identified any processes marked as being malware."

X. Claim 1 according to the first auxiliary request differs from that of the main request, editorial amendments aside, in further specifying that "said details comprise whether or not a process has been detected as malware".

XI. Claim 1 of the second auxiliary request differs from that of the main request in the replacement of the paragraph at the end of the claim "providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware." by the following passage: "providing information to the user of said first remote computer (2) that **the security products on said first remote computer (2) expose the first remote computer to a risk of being infected** by said identified any processes marked as being malware **and offering the user software to download and install to remove the risk.**" (amendments **highlighted** by the board).

XII. Claim 1 of the third auxiliary request combines the amendments of the two previous requests with respect to that of the main request.

XIII. Claim 1 of the fourth auxiliary request differs from that of the main request in the addition of the following two passages: "wherein the malware is an executable object that contains malicious code including a virus, Trojan, worm, spyware, and/or adware" and "allowing the user to download and install a software arranged to remove risk of being infected by the processes marked as being malware".

Reasons for the Decision

1. Admissibility of the appeal

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 The application relates to determining the protection that a remote computer has from malware, the remote computer apparatus being connected via the internet to a base computer; see the fourth and fifth aspects of the invention, page 9, line 1, to page 10, line 5.

2.2 The base computer classifies computer objects (referred to below as "objects") as malware or not, the application using the term "malware" to refer to an executable computer file, such as a virus, a Trojan, a worm, spyware or adware; see page 1, lines 13 to 15.

2.3 To classify an object, the base computer receives data about the object via the internet from a plurality of other remote computers, on which the object is stored, compares the data and, based on the result, classifies the object.

2.4 The data stored about the object comprises 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 23, line 4, to page 24, line 22.

2.5 As shown in figure 1, the base computer (3) is linked to a community database (7) connected via the internet (1) to a plurality of remote computers (2). The database contains signatures or keys relating to objects (4) and their effects; see page 17, lines 10 to 22. As shown in figure 2, if an object is known not to be malware from the database of a remote computer then it is allowed to run on that computer. If the object is known to be unsafe, then the user may be asked for approval before running it. If the object is unknown then a signature is created and passed via the base computer (3) to the database (7); see page 18, line 8, to page 19, line 20. Figure 3 illustrates the use of a mask to classify an object as malware if its behaviour extends beyond a safe limit defined by the mask; see page 26, line 22, to page 27, line 2. Figure 4 shows how local security products (40) generate keys (41) of objects which are sent to the community database (42). The database returns potential "risks" of computers having a given product and settings; see page 29, lines 10 to 23.

3. Clarity, Article 84 EPC

Despite the doubts regarding clarity raised by the board in its preliminary opinion, the board finds that claim 1 of the main and first three auxiliary requests is sufficiently clear for the assessment of inventive step.

4. The board's understanding of the invention

4.1 The board understands the term "malware" in claim 1 of all requests to mean, as explained on page 1, lines 13 to 15, of the description, any executable computer file, that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware and adware. For the purposes of the following assessment, the board interprets the term "malware" accordingly, to the appellant's benefit even where the claim lacks that definition.

4.2 Claim 1 of all requests sets out searching the database to identify any processes (run by the plurality of remote computers) "marked" as being malware without an indication as to how that marking occurred. Accordingly, the board understands "marked" to mean "deemed". In other words, the claim is not restricted to malware being identified as such, for instance by a virus checking program. The claim covers "marking" in accordance with a company policy, for instance, that all programs from a certain vendor are deemed malware.

4.3 The term in claim 1 of all requests "security product" is a program able to detect malware as defined above. The references to security products being "loaded on or available to" a remote computer cover the case that the product is either stored in the remote computer itself or on a network memory device accessible from the remote computer.

5. Document D1 (US 2003/0131256 A1)

5.1 As shown in figure 1, D1 relates to a computer network (2) having a managing computer (32) which logs reports of malware detections from computers (10-26), each

having a malware scanner, in the network. The management computer can detect patterns of malware detection (see figure 3; 44 and [28]) and trigger predefined anti-malware actions (50; see [29]), such as forcing particular computers to update their malware definition data (see figure 4 and [30]), changing their security settings or isolating parts of the network; see abstract.

5.2 A goal in D1 is to avoid the response to a malware attack disrupting the network more than the malware itself; see [11], lines 6 to 17. This can take the form of only causing those computers whose malware definitions are not up-to-date to update them; see [11], lines 31 to 37, and figure 4 and [30], line 9 onwards.

5.3 In view of the disclosure in D1 of computers with out-of-date malware definitions not detecting a malware infection, whilst those with up-to-date malware definitions do (see [30], lines 1 to 13), the board takes the view that D1 discloses a method for determining the protection that a first remote computer of a plurality of remote computers has from malware.

6. Inventive step, Article 56 EPC

6.1 The main request

6.1.1 According to the decision (point 3), the subject-matter of the independent claims differed from the disclosure of D1 in that

i. the information that the computer may be susceptible to attack was provided to the user, and

ii. the search of the database was performed in a different way.

Difference "i", being a presentation of information, could not contribute to inventive step. Difference "ii" was not allowable, as it was open to objection under Articles 76(1), 84 and 83 EPC. Hence the independent claims did not involve an inventive step in view of D1.

6.1.2 According to the appellant, feature "i" was not a mere presentation of information, but rather had a technical effect on the system. Moreover feature "ii" complied with Articles 76(1), 84 and 83 EPC and lent inventive step to the claim. The difference features not only presented information to the user, but also had the technical effect of increasing the computer's effective security, since the user could be expected to take action, once they became aware that their computer had a previously undetected vulnerability.

6.1.3 In view of the above analysis of D1, the board is of the opinion that the subject-matter of claim 1 differs from the disclosure of D1 in almost all its features, namely:

"receiving at a database (7) of a base computer (3) information of all or selected security products loaded on or available at a point in time on said first remote computer (2); receiving at the database (7) information of all or selected security products loaded on or available at a point in time on other remote computers (2) of said plurality of remote computers connected to the database (7); receiving at the database (7) details of processes run by said plurality of remote computers (2); storing the information and the details in the

database (7); searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected; and providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware."

6.1.4 According to the appellant, D1 disclosed a different approach to increasing computer security to that claimed, namely forcing computers to update the malware definition data used by their malware scanning software if it was out of date; see [30], last ten lines. The invention involved remote computers providing information on their security products and all running processes to a community database which warned the remote computers of undetectable vulnerabilities of their configuration to malware that had not reached the remote computers yet. Hence, although the security product on a remote computer had not identified a process running on it as malware, the database on the base computer could identify that process as malware and warn the user of the remote computer of its vulnerability. This was possible because the base computer and the remote computer had different security products, the base computer having the database. The appellant disputed whether the "marking" of an object as malware, which included viruses, worms and adware, could be based on non-technical criteria such as the identity of the vendor. The warning to the user constituted functional data and was not a mere "presentation of information". Hence the difference features over D1 allowed a fast propagation of malware through the computer network to be prevented and

precautionary measures to be taken. Referring to decisions T 543/14 and T 528/07, the appellant argued that informing the user of a computer of a malware vulnerability concerned indicating the technical conditions, in other words the internal state, of the computer which helped the user to properly operate the computer and thus had a technical effect. The objective technical problem being solved was to enable, efficiently and in real time, reducing or even stopping propagation of malware across a plurality of remote computers. Thus the claimed solution was not obviously derivable from D1.

6.1.5 The board finds that the difference features over D1 lack a technical effect and thus cannot contribute to inventive step. The result of the difference features is namely to inform the user of the first remote computer about "malware" that has "occurred" on a remote computer and that has not been locally detected.

6.1.6 The board notes that the claims do not define the "security products" in question, what service they provide and when they provide it. The claims do not specify whether or not the malware in question was identified as malware at the remote computers where it "occurred"; alternatively, the remote computer might have simply reported to the base computer, as a matter of course, the download of a program which was "known" to the database to be malware. The claims also do not setout whether the remote computer was able to identify the malware before it was run, and thus whether it was, effectively, already sufficiently protected or not.

6.1.7 If the remote computer was sufficiently protected, the local computer would appear to be sufficiently protected as well, as it is equipped with "the same

particular combination of security products" as the remote computer. Informing the user about a potential future "attack" may then not represent a security problem at all.

6.1.8 If the remote computer was not sufficiently protected, then the user would be informed about the risk of being "attacked" by the malware in question before it had "occurred" at the local computer. The appellant has argued that the user could be expected to take action, once they became aware of that risk. However the claims are not limited to such action being taken, and thus cover the case where the user ignores the information and takes no action.

6.1.9 The board does not regard a warning of an undetected potential "attack" in the first remote computer as necessarily falling under the definition of gaining insight into the internal technical state of the first computer; see G 1/19, reasons 98. Firstly, as just explained, the claim language does not allow the conclusion that the potential attack poses an actual risk to the first computer. Secondly, the definition of what is deemed ("marked as") malware can involve non-technical considerations, for instance relating to the identity of the vendor of a digital object, e.g. a piece of software; see page 17, lines 14 to 20. The malware definition could merely implement a company policy that products from a certain vendor are deemed to be "malware" and not to be loaded onto company computers. Such a policy could also be required by law in government agencies.

6.1.10 In the present case the board is not persuaded that an indication that a computer is "susceptible to attack" by a certain executable file (malware) can be

considered to shed light on the "internal state" of the computer. Firstly, the "attack" in question does not imply an actual threat. While the potential attacker (the process flagged by the database) is identified, it is not established, due to the vagueness of the notion of "security products", that an actual vulnerability exists (e.g. because the length of data written to a buffer is not checked). Moreover, given the vague definitions of what is "marked as being malware" and "security products", the user is, at best (see point 6.1.9 above), informed that they might be at risk of violating a possibly non-technical policy. Such a policy need not be actually security relevant. In the board's judgment, compliance with a non-technical policy is not a technical property of a computer system, the mere display of which can be acknowledged as a technical effect.

6.1.11 Hence the board finds that the difference features over D1 do not have a technical effect, so that the subject-matter of claim 1 does not involve an inventive step, Article 56 EPC.

6.2 The requested referral to the Enlarged Board of Appeal

6.2.1 Editorial amendments by the board aside, the question formulated by the appellant reads as follows:

1. In the assessment of inventive step, can the provision of information about not detecting processes run on a computer being marked as malware (with a selected security product configuration) contribute to solving a technical problem by producing a technical effect according to case law T 543/14 and T 528/07 or not?

2. If the answer to the first question is no, what are the relevant criteria for assessing whether the said information providing a technical condition of the computer is considered to be a technical feature capable of contributing to solving a technical problem?

6.2.2 A condition for referring a question, such as that formulated by the appellant (see point VII above), to the Enlarged Board of Appeal is that an answer to the referred question is considered necessary to decide the case to ensure uniform application of the law or if a point of law of fundamental importance has arisen.

6.2.3 The board finds that both parts of the question are intimately linked to the technical facts of the case and so do not concern a "point of law of fundamental importance".

6.2.4 Moreover the board sees no reason why the board's decision in the present case would be contrary to a uniform application of the law.

6.2.5 With its questions, the appellant implicitly refers to the case law of the boards of appeal going back to case T 115/85, which held in its headnote 1 that "Giving visual indications automatically about conditions prevailing in an apparatus or system is basically a technical problem", and implies that the ratio of that decision has an impact on the present case. The decision T 528/07, referred to by the appellant, discussed this decision and identified two interpretations of it (see reasons 3.4): "either the visual indications must concern technical conditions of the system in order to relate to a technical problem [...] or they may also concern non-technical conditions", but "follow[ed] the more restrictive approach according to

which only technical conditions of a system can be taken into account" (see reasons 3.5). Further decisions were identified sharing this view. The present board also endorses it.

6.2.6 More specifically, in decision T 528/07 (see reasons 3.6) it was decided that in the assessment of the inventive step of a computer system for providing a business-to-business relationship portal the indication of conditions relating to a business undertaking did not establish a technical effect and could therefore not be taken to contribute to inventive step. In the present case, a "susceptibility to an attack" may simply be a potential non-compliance with a non-technical company policy prohibiting the installation or execution of software from a certain source. Hence the board considers that informing a user of that vulnerability does not provide the user with technical information about the internal state of the remote computer at all.

6.2.7 Decision T 543/14 concerned a portable electronic device having a touch-sensitive display, application icons on the display changing according to a mode of operation of the device. The board found that informing the user of the device mode of operation was an indication of the technical state of the device; see point 2.1, page 6, 2nd para. In the present case, a vulnerability may be a non-compliance with a non-technical company policy and thus is not a technical mode of operation of the first remote computer.

6.2.8 Hence the board cannot see why its finding in the present case should be considered inconsistent with the conclusions in the cited cases T 528/07 and T 543/14. Regarding the former decision, it seems to be rather

consistent regarding its restrictive approach vis-à-vis indications of non-technical conditions. As regards the latter one, the conclusions may be different, but so are the technical circumstances. The board cannot see why the positive finding in T 543/14 should imply a positive conclusion in the present case. Consequently the cited cases do not suggest any lack of uniform application of the law.

6.2.9 For these reasons the board finds that an answer to the above question from the Enlarged Board of Appeal is not required for a decision in the present case, Article 112(1) EPC. In the board's view, the answer to the first part of the question is "no", at least when limited to the circumstances of the present case, and the answer to the second part is that it depends on the facts of the case.

6.3 The first auxiliary request

6.3.1 Claim 1 has been limited by adding the feature that the details of the processes run by the remote computers received at the database

"comprise whether or not a process has been detected as malware".

6.3.2 The appellant has argued that the additional feature emphasises the inventive technical contribution of the claimed invention over the prior art.

6.3.3 As the additional feature merely states explicitly what the board had already taken to be implicit and does not limit claim 1 to the information provided to the user

having a technical effect, the board finds that it cannot lend inventive step to claim 1.

6.4 The second auxiliary request

6.4.1 The paragraph at the end of claim 1

"providing information to the user of said first remote computer (2) that said first remote computer (2) may be susceptible to attack by said identified any processes marked as being malware."

has been amended (amendments having being **highlighted** by the board) to read

"providing information to the user of said first remote computer (2) that **the security products on said first remote computer (2) expose the first remote computer to a risk of being infected** by said identified any processes marked as being malware **and offering the user software to download and install to remove the risk**."

6.4.2 According to the decision, the added features lacked technical character and were thus unable to contribute to inventive step.

6.4.3 The appellant has argued that the additional features further emphasised the technical effect of increasing system security, since the software, for instance anti-malware software, that was offered to the user of the first remote computer was arranged to remove the risk of infection by the processes marked as malware. The difference features over D1 enabled the efficient and real time reduction or even stopping of propagation of malware in a plurality of remote computers. The Guidelines for Examination at the EPO (G-II,3.7)

referred to decision T 528/07, stating that if the information presented to a user of a technical system related to its internal state, in particular an operating mode, technical condition or event, and enabled the user to properly operate the system then it had a technical effect. Hence the information presented to the user in the present case also had a technical effect. As the difference features over D1 were not known from the cited prior art, the subject-matter of claim 1 involved an inventive step.

6.4.4 The board is not persuaded that the additional features have a technical effect, at least since the user may not take up the offer to download and install the software, and thus agrees with the decision that it cannot lend inventive step to claim 1.

6.5 The third auxiliary request

6.5.1 Claim 1 incorporates the amendments according to both of the previous requests, the appellant having argued that the two amendments were related and had a synergistic effect lending inventive step to the claim. Both amendments related to avoiding a malware infection of the first remote computer and solved the objective technical problem of enabling, efficiently and in real time, reducing or even stopping propagation of malware in a plurality of remote computers. As the difference features over D1 were not known from the cited prior art, the subject-matter of claim 1 involved an inventive step.

6.5.2 Contrary to the appellant's argument, the board finds that the two amendments are unrelated and thus lack a synergistic effect. Their joint effect is no greater than the sum of their individual contributions. The

details received by the database (see first auxiliary request) are independent of offering the user software (see second auxiliary request). Hence, for the reasons set out above for the first and second auxiliary requests, the board finds that the additional features cannot lend inventive step to claim 1.

6.6 The fourth auxiliary request

6.6.1 Claim 1 of the fourth auxiliary request differs from that of the main request in the addition of the following two passages: "wherein the malware is an executable object that contains malicious code including a virus, Trojan, worm, spyware, and/or adware" (see page 1, lines 13 to 15) and "allowing the user to download and install a software arranged to remove risk of being infected by the processes marked as being malware" (see the second auxiliary request).

6.6.2 This request was filed with the appellant's response to the board's preliminary opinion on the appeal, the appellant arguing that the request was a response in exceptional circumstances caused by the board's different assessment of inventive step, set out in its preliminary opinion, to that of the appealed decision. The amendments were consistent with procedural economy because the new features supported and clarified those previously discussed. The amendments defined the term "malware" in more detail, thus restricting the definition of malware to technical considerations, and responded to the board's argument that the user could ignore the information that the first remote computer was at risk of a malware infection, since claim 1 now set out an interaction between the user and the first remote computer which allowed the user to increase the computer's effective security very quickly. The objec-

tive technical problem was thus to enable, efficiently and in real time, reducing or even stopping propagation of malware in a plurality of remote computers.

6.6.3 This additional request constitutes an amendment to the appellant's case. Under Article 13(1) RPBA 2020, any such amendment after the appellant has filed its grounds of appeal is subject to the party's justification for its amendment and may be admitted only at the discretion of the board. The board shall exercise its discretion in view of *inter alia* the suitability of the amendment to resolve the issues raised by the board. Under Article 13(2) RPBA 2020, if the amendment to the party's case is made after notification of the summons to oral proceedings, the amendment shall, in principle, not be taken into account unless there are exceptional circumstances, which have been justified with cogent reasons by the party concerned.

6.6.4 Under these circumstances the board decided in the oral proceedings, Article 13(1,2) RPBA 2020, not to admit this request, as the amendments in claim 1 did not limit the information provided to the user to that having a technical effect.

6.6.5 Specifically, the definition that "malware" is of one of the specified types does not affect the fact that the relevant information in the database only contains an approximation of this by "marking" processes as malware, and possibly a cautious one based on mere policy considerations. For example, it is common practice that programs are considered as malware until cleared by being put on a "whitelist", and even that may be not be based on insights about the specific functioning of or risks caused by the programs in question. An additional concern arises, albeit not immediately, as to whether

the potential security risks of the mentioned types of malware, if identified as such, were all relevant for computer security - and therefore, potentially, for a technical contribution - to the same extent. As a consequence, the amendment was unsuitable for overcoming the inventive step objection raised against claim 1 of the previous requests.

6.6.6 Moreover the board does not see how referring to "allowing" a user to download and install software restricts claim 1 to an interaction between the user and the first remote computer.

Order

For these reasons it is decided that:

1. The appeal is dismissed.
2. The request for referral to the Enlarged Board of Appeal is refused.

The Registrar: The Chairman:

L. Stridde M. Müller

Decision electronically authenticated