

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS LTD. and SOPHOS INC.
Petitioner,

v.

OPEN TEXT INC.,
Patent Owner

IPR2023-00633
Patent 8,726,389 B2

Before GARTH D. BAER, AARON W. MOORE, and SCOTTRAEVSKY,
Administrative Patent Judges.

BAER, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Sophos Ltd. and Sophos Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–30 (the “challenged claims”) of U.S. Patent No. 8,726,389 B2 (Ex. 1001, “the ’389 patent”). Paper 2, 1 (“Pet.”). Open Text Inc. (“Patent Owner”) filed a Preliminary Response. Paper 13 (“Prelim. Resp.”).

Under 35 U.S.C. § 314, an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” Upon consideration of the Petition in view of the present record and for the reasons explained below, we determine that Petitioner has not shown a reasonable likelihood of prevailing with respect to at least one of the challenged claims. Accordingly, we do not institute an *inter partes* review.

B. Related Proceedings

The parties identify the following related matters:

Webroot, Inc. v. Trend Micro Inc., No. 6:22-cv-00239 (W.D. Tex.); *Webroot, Inc. v. Sophos Ltd.*, No. 6:22-cv-00240; *Webroot, Inc. v. CrowdStrike, Inc.*, No. 6:22-cv-00241 (W.D. Tex.); (W.D. Tex.); *Webroot, Inc. v. AO Kaspersky Lab*, No. 6:22-cv-00243 (W.D. Tex.); and *Webroot, Inc. v. Forcepoint LLC*, No. 6:22-cv-00342 (W.D. Tex.). Pet. 2; Paper 5, 1.

C. The ’389 Patent (Ex. 1001)

The ’389 patent “relates generally to methods and apparatus for dealing with malware.” Ex. 1001, 1:9–10. Figure 2 of the ’389 patent is reproduced below.

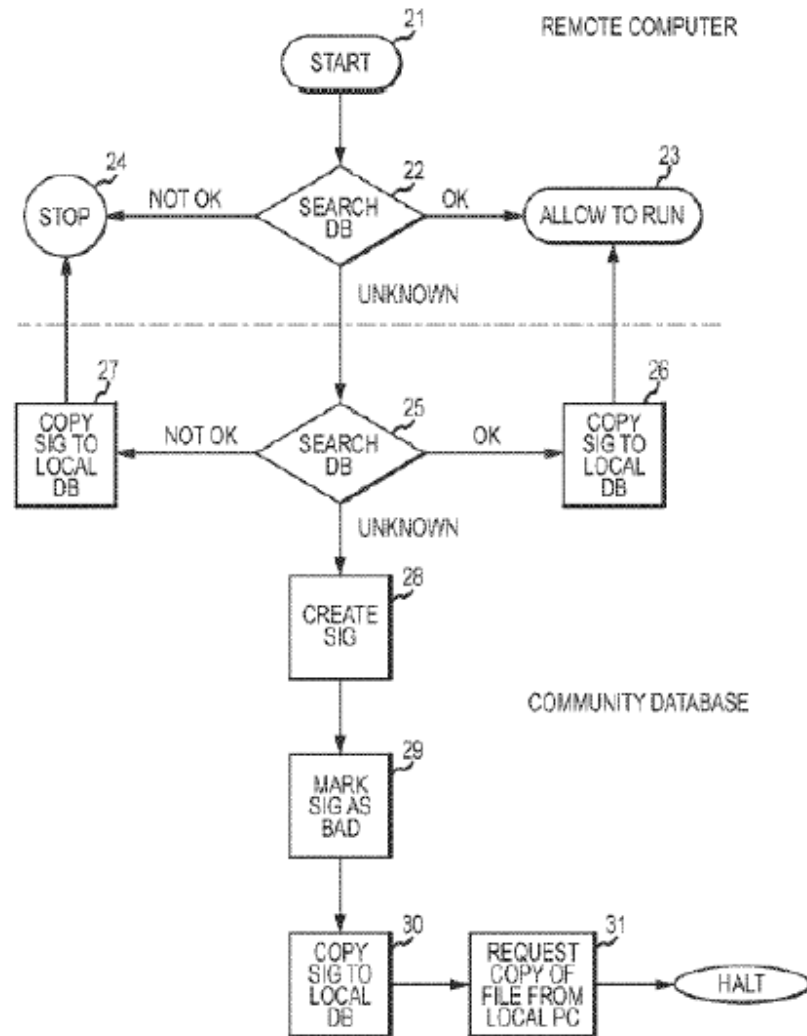


FIG.2

Figure 2 is a flowchart illustrating a method that starts at step 21 by running an object, such as a process, at a remote computer. *Id.* at 7:51–53, 8:21–22. At step 22, operation of such a process is hooked using local software running on the remote computer to search a local database for a signature or key representing that process and related objects. *Id.* at 8:22–28. If the signature indicates that the process is safe, it is allowed to run at step 23; if the signature indicates that the process is not safe, it is stopped at step 24. *Id.* at 8:33–37.

If the object is unknown locally, details of the object are passed over a network to the base computer for storing in the community database and for further analysis at the base computer. *Id.* at 8:47–50. The community database is then searched at step 25 for a signature for that object. *Id.* at 8:51–52. If found and identified as safe, then “a copy of the signature or at least a message that the object is safe” is sent to the remote computer at step 26; similarly, if found and identified as unsafe, a copy is provided to the remote computer with such a designation at step 27. *Id.* at 8:63–9:13. If the object is unknown to the community database, a signature is created at step 28 and marked as unsafe at step 29. *Id.* at 9:14–20. Such an unsafe designation may be changed as experience with the object is collected. *See id.* at 9:29–42.

D. Illustrative Claim

Challenged claims 1 and 15 are independent. Claim 1 is illustrative and is reproduced below.

1. A method of classifying a computer object as malware, the method comprising:

at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;

at the base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the

computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;

storing, at the base computer, said data received from the first and second remote computers;

correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;

comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and

classifying, by the base computer, the computer object as malware on the basis of said comparison.

Ex. 1001, 20:27–62.

E. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability. Pet. 7.

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–6, 8–13, 15–20, 22–27, 29, 30	103(a) ¹	Halperin ²
3, 5, 7, 9–13, 17, 19, 21, 23–27	103(a)	Halperin, Kirby ³

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), included revisions to 35 U.S.C. § 103 that became effective after the filing of the application that led to the challenged patent. Therefore, we apply the pre-AIA version of 35 U.S.C. § 103.

² US 2004/0111632 A1, Pub. June 10, 2004 (Ex. 1006).

³ US 7,694,150 B1, Apr. 6, 2010 (Ex. 1007).

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
14, 28	103(a)	Halperin, Kirby, Mankins ⁴

II. DISCUSSION

A. Claim Construction

We find that no claim terms require express construction to determine whether to institute *inter partes* review. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

B. Level of Ordinary Skill in the Art

Petitioner contends a skilled artisan would have had “at least a bachelor’s degree in Computer Science, Computer Engineering, Electrical Engineering, or an equivalent discipline, and at least two years’ worth of experience developing dynamic malware detection and computer networking or network architecture, or a Master’s degree in a related field.” Pet. 9. “Alternatively,” according to Petitioner, “a POSITA could have four or more years of work experience in computer networking and in the development of client-server systems.” *Id.* Petitioner also asserts that “[a] POSITA would either have six months’ experience as a network or system administrator, or have taken two advanced computer-security courses.” *Id.* Patent Owner’s formulation for a skilled artisan is substantively similar. *See Prelim. Resp.* 30. On this record, we agree with Petitioner’s formulation.

⁴ US 7,900,194 B1, Mar. 1, 2011 (Ex. 1008).

C. Description of Primary Prior Art Reference Halperin (Ex. 1006)

Halperin discloses “detecting malicious activity in a computer network.” Ex. 1006, code (57). Halperin’s Figure 6 is reproduced below.

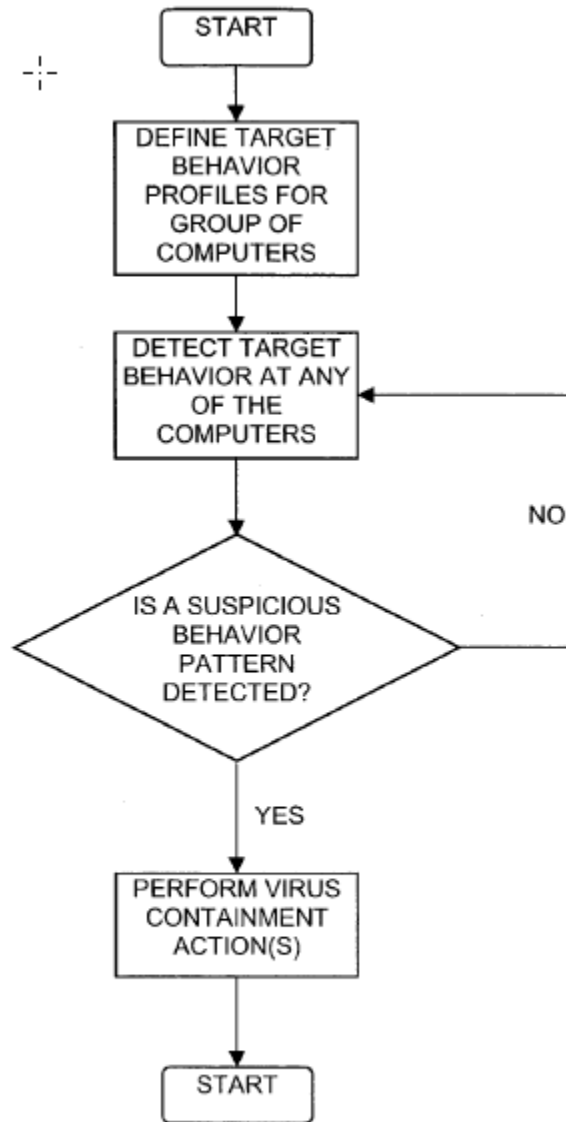


Fig. 6

Figure 6 is an “exemplary method of operation” of Halperin’s “computer virus detection and containment system.” Ex. 1006 ¶¶ 15, 16.

D. Obviousness Analysis

Independent claim 1 requires “at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes . . . information including at least an identity of an object initiating the event.” Ex. 1001, 20:29–36. Independent claim 15 has a similar limitation. *See id.* at 22:6–14. Petitioner maps Halperin’s server 502 to the claimed base computer. Pet. 17. Petitioner alleges that Halperin teaches “receiving” event information because Halperin’s server “collect[s] information regarding target behavior detected at two or more [remote] computers 500.” *Id.* at 18 (quoting Ex. 1006 ¶ 47). In addition, Petitioner asserts Halperin teaches the claimed “identity of an object initiating the event” because “Halperin discloses a ‘characteristic code may be generated’ for an ‘e-mail attachment that when activated causes the malicious software to spread,’ such as by ‘using well known “checksum” algorithms.”” *Id.* at 21 (quoting Ex. 1006 ¶ 73); *see id.* (explaining that “Halperin’s ‘predefined suspicious event’ information includes ‘at least an identity of an object initiating the event,’ which can be determined by checksum”).

We agree with Patent Owner that Petitioner’s obviousness challenge fails because Halperin does not disclose receiving the characteristic code or checksum at Halperin’s base computer, i.e., server 502. *See* Prelim. Resp. 48–50. Specifically, as Patent Owner explains, Halperin’s server does not receive the checksum because it is not generated until after the server completes its collection step. *Id.* at 49 (citing Ex. 1006 ¶¶ 72–73; Ex. 2001 ¶ 83). That is, because Halperin’s checksum is generated after malicious software has been identified, “it would be impossible for the collection of information about computer behavior—which is done long before the server

has even detected viral activity—to include the checksum (*i.e.*, alleged ‘*identity of an object*’).” *Id.* at 49–50; *see* Ex. 1006 ¶¶ 38, 47, 73.

Moreover, to the extent Halperin discloses distributing the checksum, it does so only from the server to remote computers, not vice versa, as the challenged claims require. *See* Ex. 1006 ¶ 73 (teaching that the “checksum may then be sent to neighboring computers . . . which may then use the checksum to identify suspicious malicious software”); *see* Pet. 21 (quoting Ex. 1006). Thus, we agree with Patent Owner that Halperin’s checksum disclosure does not teach “at a base computer, receiving . . . information including at least an identity of an object initiating the event,” as the challenged claims require.

Beyond relying on Halperin’s checksum teaching, Petitioner asserts a one-sentence inherency argument that “a POSITA would understand the identity of the object initiating the event necessarily must be collected” to perform Halperin’s correlation and determination analysis. Pet. 21. We disagree with this argument because it does not explain why Halperin’s server must necessarily collect the identity of an object initiating the event. *See In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (“Inherency . . . may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.”). Moreover, as Patent Owner explains, “collecting ‘*an identity of an object initiating the event*’ would not, in fact, be necessary to Halperin’s correlation analysis.” Prelim. Resp. 51. That is so because “Halperin is directed to detecting target computer behavior, evaluating the collective behavior of computers across the network for suspicious behavior patterns, and initiating virus containment actions.” Prelim. Resp. 52 (citing

(Ex. 2001 ¶ 92); *see* Ex. 1006 ¶¶ 23–30, 38–57. We agree with Patent Owner that “[n]one of these steps correspond to a determination of whether a particular object is malware, nor do they rely on the identity of objects initiating events within the target behavior profile.” Prelim. Resp. 52.

Lastly, Petitioner asserts another single-sentence argument that “[a]t a minimum, it would have been obvious to include an identity of an object initiating the event, e.g., the checksum of the email attachment Halperin discloses, in the suspicious-event information logged in the central database in Halperin.” Pet. 21–22; *see* Ex. 1004 ¶ 74 (Petitioner’s expert asserting the same). We disagree with this argument because it does not explain why it would have been obvious to have Halperin’s server collect this information or what would have motivated a skilled artisan to configure Halperin’s server to do so. Absent some rationale, as Patent Owner notes, “[s]uch conclusory assertions are inadequate to satisfy Petitioner’s burden on institution.” Prelim. Resp. 53 (citing *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016)).

Given the deficiencies outlined above, Petitioner has not adequately explained how the asserted prior art accounts for “at a base computer, receiving . . . information including at least an identity of an object initiating the event,” as the challenged claims require.

III. CONCLUSION

For the foregoing reasons, we determine that the information presented in the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing claims 1–30 are unpatentable. We therefore do not institute an *inter partes* review of claims 1–30.

IV. ORDER

Accordingly, it is:

ORDERED that the Petition is denied as to the challenged claims of the '389 patent; and

FURTHER ORDERED that no *inter partes* review is instituted.

For PETITIONER:

Benjamin Hershkowitz
Joshua A. Krevitt
Brian A. Rosenthal
Timothy P. Best
GIBSON, DUNN & CRUTCHER LLP
bhershkowitz@gibsondunn.com
jkrevitt@gibsondunn.com
brosenthal@gibsondunn.com
tbest@gibsondunn.com

For PATENT OWNER:

Brian Eutermoser
Russell Blythe
Mikaela Stone
KING & SPALDING LLP
beutermoser@kslaw.com
rblythe@kslaw.com
mikaela.stone@kslaw.com