UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/815,452	07/31/2015	Mat Rob Powell	10033.027400	1067

31894 7590 01/31/2019
OKAMOTO & BENEDICTO, LLP
P.O. BOX 641330
SAN JOSE, CA 95164

EXAMINER
EDWARDS, LINGLAN E

ART UNIT	PAPER NUMBER
2491	

MAIL DATE	DELIVERY MODE
01/31/2019	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MAT ROB POWELL

Appeal 2018-003876
Application 14/815,452[1]
Technology Center 2400

Before CARL W. WHITEHEAD JR., IRVIN E. BRANCH, and JOHN R. KENNY, *Administrative Patent Judges*.

BRANCH, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134(a) from a final rejection of claims 1, 3–8, 10–15, and 17–20, which are all of the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

---

[1] According to Appellant, the real party in interest is Trend Micro, Incorporated. App. Br. 1.

Technology

The application relates to ransomware remediation. Spec. Abstract.

Illustrative Claim

Claims 1, 3–8, 10–15, and 17–20 are pending; of these, claims 1, 8, and 15 are independent. Claim 1 is reproduced below for reference:

> 1. A method for remediating a ransomware infection, the method comprising:
>
> monitoring network traffic of a plurality of network users for a data signature;
>
> detecting the data signature in a network traffic of a network user of the plurality of network users, the data signature indicating that the network user has been infected by a ransomware application;
>
> in response to detecting the data signature in the network traffic of the network user, extracting an encryption key from the network traffic of the network user[;]
>
> storing the encryption key with an identifier of the network user;
>
> retrieving the encryption key using the identifier of the network user; and
>
> decrypting at least one file of the network user using the encryption key.

References and Rejections[2,3]

Claims 1, 3–8, 10–15, and 17–20 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Final Act. 7.

Claims 1, 3–6, 8, 10–13, 15, and 17–20 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Niemela (US 2013/0067576 A1; Mar. 14, 2013) and Scoggins (US 2006/0212933 A1; Sept. 21, 2006). Final Act. 8–14.

Claims 7 and 14 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Niemela, Scoggins, and Tock (US 2015/0135317 A1; May 14, 2015). Final Act. 14–15.

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellant's arguments. We have considered in this Decision only those arguments Appellant actually raised in the Briefs. Any other arguments Appellant could have made but chose not to make in the Briefs are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(iv). We adopt the Examiner's findings and conclusions as our own, to the extent consistent with our analysis herein.

---

[2] Rather than repeat the Examiner's positions and Appellant's arguments in their entirety, we refer to the above mentioned Appeal Brief filed November 28, 2017 ("App. Br."), as well as the following documents for their respective details: the Final Action mailed September 26, 2017 ("Final Act."), the Examiner's Answer mailed January 4, 2018 ("Ans."), and Appellant's Reply Brief filed February 27, 2018 ("Reply Br.").

[3] The Examiner withdrew a 35 U.S.C. § 112, second paragraph, rejection of claims 10–14. Ans. 7–8.

Rejection of claims 1, 3–8, 10–15, and 17–20 under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement

The Examiner contends the claims fail to comply with the enablement requirement of 35 U.S.C. § 112, first paragraph, because the Specification does not explain how "'extracting an encryption key from the network traffic of the network user'" can be achieved. Final Act. 7.

For an enablement rejection, the PTO must "set[] forth a reasonable explanation as to why it believes that the scope of protection provided by that claim is not adequately enabled by the description of the invention." *In re Wright*, 999 F.2d 1557, 1561–62 (Fed. Cir. 1993). "[T]o be enabling, the specification of a patent must teach those skilled in the art how to make and use the full scope of the claimed invention without 'undue experimentation.'" *Id.* at 1561. Some experimentation, even a considerable amount, is not "undue" if, e.g., it is merely routine, or if the Specification provides a reasonable amount of guidance as to the direction in which the experimentation should proceed. *In re Wands*, 858 F.2d 731, 737 (Fed. Cir. 1988). The following factors are relevant in determining whether undue experimentation would have been required to make and use an invention:

> (1) the quantity of experimentation necessary, (2) the amount of direction or guidance presented, (3) the presence or absence of working examples, (4) the nature of the invention, (5) the state of the prior art, (6) the relative skill of those in the art, (7) the predictability or unpredictability of the art, and (8) the breadth of the claims.

Wands, 858 F.2d at 737. It is not necessary for an Examiner to review all Wands factors, as long as it is evident that the Examiner's analysis is at least reasonably based on some of the factors. *In re Hillis*, 484 Fed. App'x 491, 495 (Fed. Cir. 2012) (unpublished); *see also Amgen, Inc. v. Chugai Pharm.*

Co., 927 F.2d 1200, 1213 (Fed. Cir. 1991) ("[I]t is not necessary that a court review all the Wands factors to find a disclosure enabling. They are illustrative, not mandatory.").

Appellant argues that "the [S]pecification provides for a signature repository for storage of ransom ware signatures to account for different known ransomware." App. Br. 4 (citing Spec. ¶ 32 ("[D]ata signature may be detected by comparing its structure to at least one ransomware signature, which may be stored in ransomware signature repository 202 of ransomware remediator 200 of FIG. 2.")).

We do not find the Examiner to have specifically addressed the Wands factors. *See* Final Act. 7; Ans. 4–5. Nor do we find the Examiner to have responded to Appellant's argument that enabling support may be found at least at paragraph 32 of the Specification. Accordingly, on this record we are persuaded of error, and we do not sustain the Examiner's rejection.

Rejection of claim 1 under 35 U.S.C. § 103(a)

The Examiner finds Niemela discloses the subject matter of claim 1, except that, although "Niemela teaches obtaining/extracting and storing information for de-obfuscation in order to restore infected files[, it] does not explicitly disclose such information being [an] 'encryption key.'" Final Act. 10. The Examiner finds "Scoggins disclose[s] security parameters such as security keys may be obtained by intercepting network traffic data." *Id.* The Examiner concludes "it would have been obvious to one of ordinary skill in the art . . . , to modify the system of Niemela to incorporate the extracting key from intercepted traffic data as disclosed by Scoggins, in order to restor[e] ransomware affected files modified via encryption." *Id.*

Appellant argues error for several reasons under four headings: 1) "running Niemela's method in multiple devices will result in separate instances of the method, but does not necessarily result [in] monitoring of network traffic of a plurality of network users in a single" (Reply Br. 3; *see also* App. Br. 4–5); 2) "the combination of Niemela and Scoggins does not teach or suggest where to obtain the encryption key employed by the ransom ware application" and Scoggins is non-analogous art (Reply Br. 3–4; *see also* App. Br. 5–7); 3) "Because Niemela discloses ransomware detection and remediation for a particular network device, there is no objective reason in Niemela to store encryption keys with an identifier of an infected network user" (App. Br. 8); and 4) "the combination of Niemela and Scoggins does not disclose retrieving an encryption key using an identifier of the network user." *Id.* at 4–8.

Appellant's arguments under the first heading are unpersuasive of error because the claim does not require implementation of the method in a single device. We agree with the Examiner that Niemela discloses monitoring of multiple devices for malware. Ans. 6 (citing Niemela ¶¶ 1, 6, 57), which is sufficient to meet the "monitoring network traffic of a plurality of network users for a data signature" limitation.

Appellant's arguments under the second heading are unpersuasive for the reasons stated by the Examiner. *Id.* at 9–10. In particular, Appellant's arguments against the references individually (App. Br. 5–7) do not undermine the Examiner's case as to what the combined teachings of the references would have taught or suggested to one of skill in the art. Ans. 9–10. Further, Appellant does not convince us that Scoggins in non-analogous art. *See* App. Br. 6 ("Scoggins is not analogous art in that it does not pertain

to combating malware."). It has been held that a prior art reference must either be in the field of Applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. *See In re Oetiker*, 977 F.2d 1443 (Fed. Cir. 1992). With respect to this argument, we agree with the Examiner that "Niemela and Scoggins are analogous art because they are both directed to the general field of network communication and data security." Ans. 10. Appellant's arguments in the Reply Brief do not squarely rebut the Examiner's finding. *See* Reply Br. 3–4 ("Scoggins requires advance knowledge of a particular network traffic that would carry the encryption key.").

Appellant's argument under the third heading, *supra*, that "there is no objective reason in Niemela to store encryption keys with an identifier of an infected network user" is unpersuasive. First, Appellant does not persuasively establish the absence of any "objective reason." Moreover, Appellant's argument does not overcome the Examiner's findings that Niemela is applicable to multi-user systems, and Niemela discloses storing both de-obfuscation information and information for restoring user access rights in a database. Ans. 11 (citing Niemela ¶¶ 42, 43).

Similarly, Appellant's argument under the fourth heading that "there is no objective reason for one of ordinary skill in the art to retrieve an encryption key using the identifier of a network user in the combination of Niemela and Scoggins" (Reply Br. 5) is unpersuasive because it does not overcome the Examiner's findings. Specifically, the Examiner cites Niemela's disclosure that "the computer device may be configured to request support from a server in network in restoration [including,] sending a

file to the server where the restoration is accomplished[after which the] restored file is returned to the computer device." Niemela ¶ 42; Ans. 12.

For the foregoing reasons, we are unpersuaded of error in the Examiner's rejection of claim 1. We sustain the rejection.

Rejection of claim 3–6, 15, and 17–20 under 35 U.S.C. § 103(a)

Claims 3–6 depend from claim 1. Appellant argues these claims based on claim 1. App. Br. 8. We sustain the rejection of these claims. We also sustain the rejection of independent claim 15 and claims 17–20, which depend therefrom, because Appellant argues these claims based on claim 1. *Id.* at 8–9. Appellant also argues the rejection of claim 7 based on arguments presented for claim 1. *Id.* at 8. Accordingly, we sustain the rejection of claim 7.

Rejection of claims 8 and 10–14 under 35 U.S.C. § 103(a)

Claim 8 recites "memory storing an infection log" and "stor[ing] the encryption key in the infection log." The Examiner finds "'infection log' is interpreted as stored data related to and used for malware detection," and finds Niemela to disclose as infection log. Ans. 13–14.

Appellant argues Niemela does not disclose "storing an encryption key along with the identifier of a network user that has been infected by ransomware." App. Br. 9.

Appellant argues claim 8 for the same reasons as claim 1, argued under the third heading, which we find unpersuasive for the reasons discussed above. Accordingly, we sustain the rejection of claim 8 and of claims 10–14, which depend, therefore, and which Appellant argues on the same bases.

DECISION

For the reasons above, we reverse the Examiner's decision rejecting claims 1, 3–8, 10–15, and 17–20 under 35 U.S.C. § 112, first paragraph, but we affirm the Examiner's decision to reject these claims as obvious under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 41.50(f).

AFFIRMED