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.
14/764,670	07/30/2015	William Horne	84312830	1061

146568 7590 09/30/2019

MICRO FOCUS LLC
500 Westover Drive
#12603
Sanford, NC 27330

EXAMINER
SHOLEMAN, ABU S

ART UNIT	PAPER NUMBER
2495	

NOTIFICATION DATE	DELIVERY MODE
09/30/2019	ELECTRONIC

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

software.ip.mail@microfocus.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte WILLIAM HORNE, TOMAS SANDER, KRISHNAMURTHY VISWANATHAN, SIVA RAJ RAJAGOPALAN, and ANURAG SINGLA

Appeal 2018-007304
Application 14/764,670
Technology Center 2400

Before CAROLYN D. THOMAS, JOSEPH P. LENTIVECH, and SCOTT RAEVSKY, *Administrative Patent Judges*.

LENTIVECH, *Administrative Patent Judge*.

DECISION ON APPEAL

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1–20. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm-in-part.

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party in interest as EntIT Software LLC. App. Br. 2.

STATEMENT OF THE CASE

Appellant's Invention

Appellant's Specification provides that resources on a network can be susceptible to security attacks such as "an attempt to destroy, modify, disable, steal, and/or gain unauthorized access to use of an asset (e.g., a resource, data, and information)." Spec. ¶ 1. Appellant's invention generally relates to providing targeted security alerts to participants (e.g., computing systems (Spec. ¶ 9)) within a threat exchange community. Spec. ¶ 14. Claim 1, which is illustrative of the claimed invention, reads as follows:

> 1. A method for providing a targeted security alert, the method comprising:
>
> collecting participant data from a plurality of participants within a threat exchange community, the collected participant data including characteristics of attackers in security attacks against the plurality of participants;
>
> grouping the plurality of participants into a plurality of clusters based on the characteristics of the attackers in the security attacks against the plurality of participants;
>
> calculating, using a threat exchange server, a threat relevancy score of a participant among the plurality of participants using the collected participant data and a cluster among the plurality of clusters; and
>
> providing, from the threat exchange server to the participant, a targeted security alert based on the calculated threat relevancy score via a communication link within the threat exchange community.

Rejections[2]

Claims 1–11 and 18–20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Beckett, III et al. (US 2010/0169474 A1; published July 1, 2010) ("Beckett"), Singla et al. (US 2015/0215329 A1; published July 30, 2015) ("Singla"), and Vukelich et al. (US 7,500,266 B1; issued Mar. 3, 2009) ("Vukelich"). Final Act. 15–37.

Claims 12–17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Pearcy et al. (US 2013/0174259 A1; published July 4, 2013) ("Pearcy"), Beckett, Singla, and Vukelich. Final Act. 38–48.

ANALYSIS

Claims 1–11 and 18–20

Appellant contends the combination of Beckett, Singla, and Vukelich fails to teach or suggest "grouping the plurality of participants into a plurality of clusters based on the characteristics of the attackers in the security attacks against the plurality of participants," as recited in claim 1. App. Br. 7–8; Reply Br. 2–6. Appellant argues Vukelich, upon which the Examiner relies, teaches "the grouping of 'sources' (i.e., the **attacker** devices)" and "is entirely silent with regard to the grouping of 'destinations' (i.e., the devices being attacked)." App. Br. 8. Appellant argues Vukelich's probing report fails to teach or suggest the disputed limitation because "the field 'DIPs 520' in the 'probing report' simply indicates the **total quantity**

[2] The rejection of claims 1–15 under 35 U.S.C. § 101 has been withdrawn. Ans. 7.

of destination network devices contacted by a particular attacker device." Reply Br. 5. Appellant argues, "the meaning of grouping into clusters as understood **in the relevant art** is partitioning a set of elements into discrete sub-groups (i.e., 'clusters') according to similarity of their characteristics." Reply Br. 3 (citing *Dictionary of Information Science and Technology*, vol. 1, p. 88, Idea Group Inc. (2007)). Appellant argues this meaning is consistent with the use of the phrase in the Specification (Reply Br. 3 (citing Spec. Fig. 3, ¶¶ 58, 60)) and Vukelich (Reply Br. 4 (citing Vukelich 3:40–50)). Appellant argues, "Vukelich does not expressly or inherently disclose that this total quantity of devices is a distinct sub-group that is partitioned from a larger set of devices (i.e., a 'cluster')" and, therefore, fails to teach or suggest the disputed limitation. Reply Br. 5.

The Examiner finds the broadest reasonable interpretation of "characteristics of the attackers" and "clusters" includes "any data related to the attackers" and "groups," respectively. Ans. 3. The Examiner finds Vukelich teaches generating a probing report from which potentially malicious probing activity may be identified. Ans. 3–4 (citing Vukelich Fig. 3; 5:1–3, 8–11, 26–35). The Examiner further finds:

> Probing report 370 of fig. 5 groups the plurality of destination network devices (participants that includes five destination devices, DIPs 720, col 8, lines 50–51) into a plurality of clusters (e.g. each row of the probing report 370 illustrates a cluster having a number of destination network devices (participants) as indicated by field DIPs 520, 1st row has 26 destination network devices, 2nd row has 1 destination network device, 3rd row has 1 destination network device, and so on) based on characteristics associated with the source devices (attack devices) used by attackers in the probing attacks (see col. 1, ll. 22–27 which discloses that probing is an initial stage of a

> network attack by a source device), as indicated by fields SOURCE IP 510 and PORTS 530 of the probing report 370, the characteristics associated with the source devices (attack devices) used by attackers include IP addresses used by the source devices and the ports or services visited by the source devices in the probing attacks against the plurality of destination network devices (e.g. fig. 5, col. 7, ll. 7–16, 28–32).

Ans. 4.

We find Appellant's arguments persuasive. Vukelich teaches "DIPs field 520 may display a value representing the number of destination network devices contacted by the source device identified in Source IP field 510." Vukelich 7:9–12. Although we agree with the Examiner that the broadest reasonable interpretation of "clusters" includes "groups" (Ans. 3), we agree with Appellant (Reply Br. 5) that a value representing the number of destination network devices fails to teach or suggest that the destination network devices are grouped into a plurality of groups or clusters, as required by claim 1. As such, we are persuaded that the Examiner erred in finding Vukelich teaches or suggests the disputed limitation.

Accordingly, we do not sustain the Examiner's rejection of claim 1; independent claim 6, which recites corresponding limitations; and claims 2–5, 7–11, and 18–20, which depend from claims 1 and 6.

Because we find this issue to be dispositive as to the rejection of claims 1–11 and 18–20, we do not reach Appellant's remaining allegations of error regarding these claims.

Claims 12–17

Claims 12–17 stand rejected under 35 U.S.C. § 103(a) based on Pearcy, Beckett, Singla, and Vukelich. Final Act. 38. Independent claim 12

recites, "dynamically group the plurality of participants into a plurality of clusters based on the characteristics of the attackers in the security attacks against the plurality of participants included in the security data." Appellant contends the cited references fail to teach or suggest the above limitation of claim 12 for substantially the same reasons discussed *supra* with respect to claim 1. *See* App. Br. 11–12. In particular, Appellant argues Vukelich teaches grouping of sources or attacker devices and not the grouping of destinations or devices being attacked, as required by claim 12. *Id.*

We do not find Appellant's arguments persuasive. The Examiner finds Pearcy teaches "a grouping of assets included in the plurality of asset groupings" and that "asset groupings can be distinct, user-defined asset groupings, while in other instances, asset groupings can correspond to a range of IP addresses of assets in the particular computing system." Final Act. 39 (citing Pearcy ¶¶ 11, 14, 33, 38, 39). The Examiner finds Vukelich teaches grouping devices based on characteristics of the attackers. Final Act. 42–43 (citing Vukelich Abstract, Fig. 3, 5:29–40, 8:20–40). Based on these findings, the Examiner concludes the combination of Pearcy and Vukelich teaches or suggests the disputed limitation. *See* Final Act. 43. Appellant's arguments fail to address the combined teachings of Pearcy and Vukelich and, therefore, are unpersuasive of error.

Accordingly, we are not persuaded the Examiner erred in rejecting claim 12 and claims 13–17, which depend from claim 12 and are not separately argued with particularity.

CONCLUSION

In summary:

Claims Rejected	Basis	Affirmed	Reversed
1–11, 18–20	§ 103(a) Beckett, Singla, Vukelich		1–11, 18–20
12–17	§ 103(a) Pearcy, Beckett, Singla, Vukelich	12–17	
Overall Outcome		12–17	1–11, 18–20

DECISION

We reverse the Examiner's rejection of claims 1–11 and 18–20.

We affirm the Examiner's rejection of claims 12–17.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART