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.
14/838,889	08/28/2015	Yonatan Fridman	20141556	7861

25537 7590 01/31/2020

VERIZON
PATENT MANAGEMENT GROUP
1300 I STREET NW
5TH FLOOR
WASHINGTON, DC 20005

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
01/31/2020	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):

VZPatent25537@verizon.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte YONATAN FRIDMAN, KENNETH J. MCKEEVER, and KARL STANG

Appeal 2019-000248
Application 14/838,889
Technology Center 2400

Before ERIC S. FRAHM, JAMES W. DEJMEK, and STEPHEN E. BELISLE, *Administrative Patent Judges*.

BELISLE, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–20. Appeal Br. 7. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

[1] Throughout this Decision, we use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42 (2017). Appellant identifies the real party in interest as "Verizon Communications Inc. and its subsidiary companies." Appeal Br. 3.

STATEMENT OF THE CASE

The Claimed Invention

Appellant's invention generally relates to systems and methods for botnet beaconing detection and mitigation, where a "botnet" generally refers to "a collection of compromised hosts (often referred to as 'zombie' computers/devices) running a malicious application (referred to as a 'bot') that allows the compromised hosts to be remotely controlled." Spec. ¶¶ 1, 12–15.

Claim 1, reproduced below, is illustrative of the subject matter on appeal:

> 1. A method comprising:
>
> collecting, by a processor, flow data associated with flows between a plurality of network elements;
>
> processing, by the processor, the flow data to identify that a subset of the flows, between a first network element and a second network element of the plurality of network elements, occur at a regular interval;
>
> determining, by the processor, sessions of packet transmission associated with each flow of the subset of flows;
>
> identifying, by the processor, one or more of the sessions that exceed a threshold amount of time;
>
> identifying, by the processor, at least one of the one or more sessions in which the packet transmission is below a threshold number of packets;
>
> determining, by the processor, that the at least one of the one or more sessions is associated with a botnet beacon and the regular interval corresponds to a botnet beaconing interval;
>
> using, by the processor, the botnet beaconing interval to identify a third network element of the plurality of network elements associated with a same botnet as the first and second network elements; and

> forwarding, by the processor, a notification, wherein the notification includes information identifying the first, second, and third network elements as being associated with the same botnet.

Appeal Br. 15 (Claims Appendix).

The Applied References

The Examiner relies on the following references as evidence of unpatentability of the claims on appeal:

Wei	US 2010/0082800 A1	Apr. 1, 2010
Cowan	US 8,578,493 B1	Nov. 5, 2013
Suzio	US 2014/0215624 A1	July 31, 2014

The Examiner's Rejections

The Examiner made the following rejections of the claims on appeal:

Claims 1–4, 8–11, and 15–18 stand rejected under 35 U.S.C. § 102(a)(1) as being anticipated by Cowan. Final Act. 3–5.

Claims 5–7, 12, 14, 19, and 20 stand rejected under 35 U.S.C. § 103 as being unpatentable over Cowan and Wei. Final Act. 5–6.

Claim 13 stands rejected under 35 U.S.C. § 103 as being unpatentable over Cowan, Wei, and Suzio. Final Act. 7.

ANALYSIS[2]

Appellant disputes the Examiner's findings that Cowan, alone or in combination with Wei or Suzio, renders unpatentable claims 1–20, including

[2] Throughout this Decision, we have considered Appellant's Appeal Brief filed May 21, 2018 ("Appeal Br."); Appellant's Reply Brief filed October 11, 2018 ("Reply Br."); the Examiner's Answer mailed August 24,

independent claims 1, 8, and 15. *See* Appeal Br. 8–13; Reply Br. 2–5. Appellant argues the appealed claims as a group. *See* Appeal Br. 8–13. Thus, for purposes of our analysis, we select independent claim 1 as the representative claim, and any claim not argued separately will stand or fall with our analysis of the rejection of claim 1. *See* 37 C.F.R. § 41.37(c)(1)(iv).

Appellant argues, *inter alia*, that the Examiner has not shown by a preponderance of the evidence that Cowan discloses, explicitly or inherently, "using . . . the *botnet beaconing interval* to identify a third network element of the plurality of network elements associated with a same botnet as the first and second network elements," as recited in claim 1. Appeal Br. 9–10; Reply Br. 3–4. We find Appellant's argument persuasive, and turn first to Cowan's disclosure.

Cowan is titled "Botnet Beacon Detection," and generally relates to "detecting malicious activities in [a] computer network." Cowan, col. 1:10–11, code (54). More specifically, Cowan discloses a method and system "to detect botnet beaconing event[s] based on a beacon detection rule set to generate a beacon alert," which in turn is used "to trigger an elevated exfiltration detection activity by reducing (i.e., tightening) various thresholds in an exfiltration detection rule set." Cowan, col. 3:58–63. Cowan's system monitors IP (Internet Protocol) traffic flows based on the beacon detection rule set in order to identify hosts within a network "that are *beaconing at substantially regular intervals* to external IPs . . . that are not in a pre-determined list of 'well known and likely to be benign' IPs." Cowan,

2018 ("Ans."); the Final Office Action mailed November 29, 2017 ("Final Act."); and Appellant's Specification filed August 28, 2015 ("Spec.").

cols. 3:64–4:4 (emphasis added); *see* col. 9:1–20 (analyzing "timestamps of the [IP traffic] flows" to detect whether such flows have "substantially regular occurrences" and to determine whether such flows indicate potential bots in a botnet). IPs exhibiting "questionable behavior" are tracked in a table, and "network traffic associated with such IP is analyzed using [an] elevated exfiltration detection scheme." Cowan, col. 4:45–52. When other traffic flows exiting a network are detected as being associated with an IP tracked in the table, Cowan discloses using "more stringent thresholds and baselines to adjust the exfiltration rule set" for analyzing the flow records to detect exfiltration events and generate exfiltration alerts more expediently. Cowan, col. 4:55–62.

To serve as an anticipatory reference, Cowan "must disclose each and every element of the claimed invention, whether it does so explicitly or inherently." *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009). The Examiner finds "Cowan uses the *IP address* of the C&C [i.e., botnet 'command-and-control'] server discovered when analyzing [a] first network element," which *IP address* is "stored in [a] hint table," to identify and track any other *IP address* in the network that is in "communication with . . . [the stored] botnet *IP address*." Ans. 5 (emphases added). The Examiner concludes, "[t]herefore it is clear from Cowan that 3 or even more *IP addresses* can all be deemed part of the same botnet when any number of internal devices are communicating with the external botnet C&C *address*." Ans. 5 (emphases added). But, as argued by Appellant, "claim 1 recites using the *botnet beaconing interval* to identify a third network element, and not *a botnet address*, *a destination address*, *an IP address*, or *a botnet C&C address*, as allegedly described in COWAN's detection scheme." Reply

Br. 4. We agree with Appellant, and find the Examiner does not sufficiently show how Cowan explicitly or inherently discloses (i.e., anticipates) using a *botnet beaconing interval*, as opposed to suspicious IP addresses, to identify a third network element. Because the Examiner rejected independent claim 1 only under 35 U.S.C. § 102(a)(1) (anticipation), and not under 35 U.S.C. § 103 (obviousness), we do not opine herein on whether Cowan, alone or in combination with other cited art, renders obvious claim 1.[3]

Based on the foregoing, we find the Examiner has not persuasively shown how Cowan discloses "using . . . the botnet beaconing interval to identify a third network element of the plurality of network elements associated with a same botnet as the first and second network elements," as recited in independent claim 1. The Examiner also has not persuasively shown how the other cited art remedies this deficiency. Because we find this issue dispositive here, we do not address Appellant's other arguments.

Accordingly, we do not sustain the Examiner's rejection under 35 U.S.C. § 102(a)(1) of independent claim 1. For similar reasons, we do not sustain the Examiner's rejection under 35 U.S.C. § 102(a)(1) of independent claims 8 and 15, which recite commensurate limitations, and claims 2–4, 9–11, and 16–18, which depend therefrom. Additionally, we do not sustain the Examiner's rejection under 35 U.S.C. § 103 of claims 5–7, 12–14, 19, and 20, which depend therefrom.

---

[3] Although the Board is authorized to reject claims under 37 C.F.R. § 41.50(b), no inference should be drawn when the Board elects not to do so. *See* MPEP § 1213.02.

DECISION SUMMARY

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1–4, 8–11, 15–18	102(a)(1)	Cowan		1–4, 8–11, 15–18
5–7, 12, 14, 19, 20	103	Cowan, Wei		5–7, 12, 14, 19, 20
13	103	Cowan, Wei, Suzio		13
Overall Outcome				1–20

REVERSED