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.
14/935,522	11/09/2015	Seyed Ali Ahmadzadeh	154576 / 1376-1767	2668

111523 7590 01/21/2020
The Marbury Law Group/Qualcomm
11800 Sunrise Valley Drive, 15th Floor
Reston, VA 20191

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
01/21/2020	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):

ocpat_uspto@qualcomm.com
ptonoticesqc@marburylaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SEYED ALI AHMADZADEH, NAYEEM ISLAM, MIHAI CHRISTODORESCU, RAJARSHI GUPTA, and SAUMITRA MOHAN DAS

Appeal 2018-008576
Application 14/935,522
Technology Center 2400

Before MICHAEL J. STRAUSS, DANIEL N. FISHMAN and NABEEL U. KHAN, *Administrative Patent Judges.*

KHAN, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1–30. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM.

[1] We use the word Appellant to refer to "applicant" as defined in 37 C.F.R. § 1.42(a). Appellant identifies the real party in interest as Qualcomm Incorporated. Appeal Br. 3.

CLAIMED SUBJECT MATTER

Appellant describes the invention as relating to "a honeypot system configured to trigger malicious activities by malicious applications using a behavioral analysis algorithm and dynamic resource provisioning." Abstract.

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

> 1. A method implemented in a honeypot system for triggering malicious activities by applications, comprising:
>
> designating, via a processor of a computing device, an application currently executing on the computing device as a target application in response to determining that the application is capable of launching a malicious activity;
>
> predicting, via the processor, a triggering condition that will cause the target application to launch the malicious activity;
>
> provisioning, via the processor, one or more resources based on the predicted triggering condition;
>
> monitoring, via the processor, activities of the target application corresponding to the provisioned resources; and
>
> determining, via the processor, whether the target application is malicious based on the monitored activities.

REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
Converse	US 2005/0166072 A1	July 28, 2005
Flores	US 2007/0240215 A1	Oct. 11, 2007

REJECTIONS

1. Claims 1–30 stand rejected under 35 U.S.C. § 102 as anticipated by Flores. Final Act. 8–10.

2. Claims 1–30 stand rejected under 35 U.S.C. § 103 as unpatentable over Flores and Converse. Final Act. 10–14.

OPINION

The Examiner finds Flores discloses each of the limitations of claim 1, including the steps of "predicting" and "provisioning." Final Act. 8–10. In doing so, the Examiner cites to the "Entire Document" of Flores, but then also provides specific citations to certain paragraphs and sections of Flores for those limitations along with a short explanation of how the cited portions apply to the claims. *See* Final Act. 8–10. The Examiner's findings for two disputed limitations are reproduced here for illustration:

> Predicting, via the processor, a triggering condition that will cause the target application to launch the malicious activity (Entire Document, for example, Abstract, Paragraphs 11, 16–18, 20–25, 28–31, 35, 36, and 40 and associated figures; triggering conditions could be APls, external function calls, state machines, other calls, etc., as examples);
>
> Provisioning, via the processor, one or more resources based on the predicted triggering condition (Entire Document, for example, Abstract, Paragraphs 11, 16–18, 20–25, 28–31, 35, 36, and 40 and associated figures; shimming/hooking the detection program into a process, creating a honeypot, using any form of monitoring resources (e.g., any form of monitoring occurring in order to detect a trigger or in response to a trigger), etc., as examples);

Final Act. 9.

The Examiner further finds Flores describes the "predicting" limitation by disclosing that "the detection program **104** scans the device desktop virtual memory space to locate functions of interest (step **304**). An example of a function of interest is a function that processes key message or stores key messages." Ans. 29 (citing Flores ¶ 27). The Examiner explains that the aforementioned disclosure "clearly shows the predicting limitation, since functions of interest are identified to be monitored for." Ans. 29.

The Examiner also finds Flores discloses the "provisioning" limitation because

> the next sentence of paragraph 27 following the portion quoted above regarding the predicting limitation states "Once the functions of interest are located, the detection program 104 replaces the functions with the detection program's monitoring functions (step 306), and thus creates a shim for monitoring malicious behavior for particular functions." This clearly shows provisioning resources based on the predicted triggering condition, since it replaces the function with the shim that will then be used to monitor.

Ans. 29 (citing Flores ¶ 27).

Whether the Examiner Has Set Forth a Prima Facie Case

Appellant argues that "the Examiner has failed to meet the burden of presenting a prima facie case of anticipation and/or obviousness because the citation to the Entire Document of Flores and Converse forces Appellants *to guess* which features in Flores and Converse the Examiner alleges discloses each of the recited elements." Appeal Br. 9. According to Appellant, "[s]uch citation renders the Office Action and the rejections 'arbitrary and capricious' under APA." Appeal Br. 9. Appellant argues the Examiner's citations are "so uninformative as to prevent Appellant from recognizing and seeking to counter the grounds of rejection." Appeal Br. 9 (quoting *In re Jung*, 637 F.3d 1356, 1362–63 (Fed. Cir. 2011)). Specifically, with respect to the "predicting" and "provisioning" limitations, Appellant argues the Examiner fails to explain how or why the cited APIs, external function calls, state machines, or other calls actually discloses predicting that those APIs and function calls will cause a target application to launch a malicious activity or how Flores provisions resources based on the cited APIs and function calls.

Given the entirety of the record before us, we are unpersuaded by Appellant's argument. We agree that citation to the "Entire Document" is generally unhelpful, but the immediately following citations direct the Appellant to specific portions of the reference that the Examiner finds disclose the disputed limitations. Further, the Examiner provided a short explanation of how the cited portions map to the claim limitations. For example, the Examiner specifically cites to paragraphs 11, 16-18, 20-25, 28-31, 35, 36, and 40 of Flores, along with its Abstract, and explains that the APIs, external function calls, state machines, other calls are examples of the claimed "triggering conditions." Final Act. 9. Similarly, for the "provisioning" limitation the Examiner cites to the same portions of Flores and finds that "shimming/hooking the detection program into a process, creating a honeypot, using any form of monitoring resources" discloses provisioning resources based on the predicted triggering condition. Final Act. 9.

Moreover, the Examiner provides further citation and explanation in the Answer, finding that paragraph 27 of Flores teaches both the "predicting" and "provisioning" limitations. Ans. 29. Here, the Examiner specifically identifies the cited "functions of interest" as disclosing the claimed "predicting . . . triggering conditions" and the cited replacement of the functions of interest with monitoring functions (i.e. shim) as the claimed "provisioning one or more resources based on the predicted triggering condition." The Examiner also provides sufficient explanation and reasoning supporting the findings. Ans. 30.

The aforementioned findings by the Examiner meet the notice requirements of 35 U.S.C. § 132. The Examiner has set forth the statutory basis for the rejection and explained the rejection in sufficient detail to permit Appellant to respond meaningfully.

Rejection Under 35 U.S.C. § 102

Appellant next argues that Flores fails to teach the "predicting" and "provisioning" limitations. Appeal Br. 14–26. We are unpersuaded by Appellant's arguments. Instead, under the broadest reasonable interpretation, we agree with the Examiner's findings as presented in the Answer that Flores's teaching of locating functions of interest such as key messages discloses "predicting . . . triggering conditions." Ans. 28 (citing Flores ¶ 27). Key messages may be used by key logger programs when engaging in malicious behavior. *See* Flores ¶ 25. Thus, we agree, by determining that key messages may indicate malicious behavior and locating these key messages, Flores discloses predicting a possible triggering condition (key messages from a possible key logger). Once the functions of interest are located, Flores's detection program replaces those functions with the detection program's own monitoring functions, thus creating a shim. Ans. 29 (citing Flores ¶ 27). The creation of the shim occurs as a result of finding the functions of interest. We therefore agree that the creation of the shim provisions resources (replacing functions of interest with the monitoring functions) based on the predicted triggering condition (the key messages) as required by the disputed limitation.

Appellant does not address the aforementioned Examiner's findings. *See* Reply Br. 7–8. Accordingly, we sustain the Examiner's rejection of claims 1–30 as anticipated by Flores.

Rejection Under 35 U.S.C. § 103

The Examiner rejects claim 1–30 as obvious over Flores and Converse. The Examiner finds Converse teaches both the "predicting" and the "provisioning" limitations. Final Act 10. The Examiner explains that Converse teaches the "predicting" and "provisioning" limitations by disclosing a database of known vulnerabilities that is compiled through observation (Ans. 31 (citing Converse ¶ 37)) and by disclosing that a "new vulnerability might be chosen for use by the emulated service in order to attract a probing operations by other malicious users, after which the morphing honeypot repeats the process" (Ans. 32 (citing Converse ¶ 80)). The Examiner also relies on Converse's teaching of an emulation phase in which calls to a service are logged and analyzed and then the service is reconfigured in response to the analysis. Ans. 32 (citing Converse ¶ 43).

Appellant contends that "Converse discloses that the morphing honeypot dynamically adjusts its *advertised characteristics (e.g., operating system version, services, etc.)* to invite probes and attacks by malicious users." Appeal Br. 28. Appellant argues "[e]ven assuming *arguendo* that adjusting advertised characteristics as disclosed by Converse suggest[s] the 'provisioning . . . one or more resources', Converse fails to teach or suggest that the adjustment of advertised characteristics is 'based on the predicted triggering condition' as recited in the claims." Appeal Br. 28. Appellant goes through each of the paragraphs cited by the Examiner and summarizes their content. Appeal Br. 28–45.

We are unpersuaded by Appellant's argument. Converse teaches a "morphing honeypot" that sets a vulnerability within an emulated service which might be exploited by a malicious user. Converse ¶ 79. The morphing honeypot then monitors the service for suspicious activity such as a probing operation by a suspicious client. Converse ¶ 79. If a probe is detected the honeypot reports the event and then "a new vulnerability might be chosen for use by the emulated service in order to attract a probing operations by other malicious users, after which the morphing honeypot repeats the process." Converse ¶ 80. If a probe is not detected, then the morphing honeypot reconfigures itself to present a different vulnerability to attract a probing operation by a malicious user. Converse ¶ 81. We, therefore, agree with the Examiner that Converse teaches "predicting . . . a triggering condition" by choosing a vulnerability that may attract malicious probing operations. We also agree with the Examiner that Converse teaches "provisioning . . . one or more resources based on the predicted triggering condition" by reconfiguring a morphing honeypot to set another vulnerability that may attract malicious behavior. *See* Ans. 32.

Accordingly, we sustain the Examiner's rejection of claims 1–30 under 35 U.S.C. § 103.

DECISION SUMMARY

In summary:

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
1–30	102	Flores	1–30	
1–30	103	Flores, Converse	1–30	
Overall Outcome			1–30	

TIME PERIOD FOR RESPONSE

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. § 1.136(a)(1)(iv).

AFFIRMED