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.
14/905,496	01/15/2016	Frank Chijeen Hsueh	90141270	6467

146568 7590 09/28/2020

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

EXAMINER	
TURCHEN, JAMES R	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
09/28/2020	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):

software.ip.mail@microfocus.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte FRANK CHIJEEN HSUEH
and SEJAL PRANLAL KAMANI

Appeal 2019-003869
Application 14/905,496
Technology Center 2400

Before: JEREMY J. CURCURI, GREGG I. ANDERSON, and DAVID J. CUTITTA II, *Administrative Patent Judges.*

ANDERSON, *Administrative Patent Judge.*

DECISION ON APPEAL

Pursuant to 35 U.S.C. § 134(a), Appellant appeals from the Examiner's Final decision to reject claims 1–4, 6–8 and 10–18.[1,2] Claims 5 and 9 were previously cancelled. *See* fn.2. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

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

[2] The Final Action Office Action Summary sheet includes claim 5 as a pending claim, i.e., "claims 1–8 and 10–18 are rejected." However, neither the Final Action nor the Appeal Brief include claim 5 as part of this appeal. *See also* Request for Continuation Examination, Amendment filed January 24, 2018, cancelling claims 5 and 9. We determine the Summary's inclusion of claim 5 is an error.

CLAIMED SUBJECT MATTER

The claims are directed to an approach to generate signal tokens to help detect malware applications, particularly to mobile devices such as smartphones and tablets.[3] Spec. ¶¶ 7, 8. "A static analysis engine can be used to perform byte code analysis on binaries that may be stored" to generate tokens. *Id.* ¶ 9. Signal tokens may be "a set of raw data of the application that causes a rule to fire." *Id.* The results of the byte code analysis are evaluated to "generate signal tokens that can be used to categorize unknown application as being either malware or benign." *Id.*

"[S]ignal tokens are processed items that can be recorded as a discrete entry in a malware likeliness database." *Id.* A comparison of the signal tokens to tokens of an application which is being investigated results in a determination whether the application includes malware. Spec. ¶¶ 9, 33–36 and Fig. 3.

Independent claim 1, reproduced below, claims a "computing device" and is illustrative of the claimed subject matter:[4]

[3] We use the following for the references in our review: "Spec.," to refer to the Specification filed January 15, 2016; "Final Act.," to refer to the Final Action mailed July 27, 2018; "Appeal Br.," to refer to the Appeal Brief filed December 14, 2018; "Ans.," to refer to the Examiner's Answer mailed February 19, 2019; and "Reply Br.," to refer to the Reply Brief filed April 18, 2019.

[4] Independent claims 8 and 14 are directed to a "method" and "non-transitory machine readable storage medium" respectively.

1. A computing device comprising:

at least one processor;

a memory to store machine executable instructions that, when executed by the at least one processor, cause the at least one processor to:

apply a set of rules to determine a first set of tokens based on a static code analysis performed on a first set of known malware application code, wherein the first set of tokens comprises a given token comprising raw data of the known malware application code identified by a given rule of the applied rules;

determine a second set of tokens based on a static code analysis performed on a second set of known clean application code;

apply machine learning to the first and second sets of tokens to determine a third set of tokens indicative of malware; and

apply machine learning to classify the third set of tokens into groups associated with different categories of malware, wherein the machine learning is based on training sets of applications associated with malware and applications that are known to be benign.

Appeal Br. 17, Claims App.

REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
Walls	US 7,284,274 B1	Oct. 16, 2007
Titonis	US 2013/0097706 A1	Apr. 18, 2013
Sikorski	US 2014/0283037 A1	Sept. 18, 2014

REJECTIONS

1. Claims 1, 2, and 16 are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Sikorski. Final Act. 3–4.

2. Claims 8, 14, 17, and 18 are rejected under 35 U.S.C. 103 as being unpatentable over Sikorski and Walls. *Id.* at 7–9.

3. Claims 3, 4, 6, and 7 are rejected under 35 U.S.C. 103 as being unpatentable over Sikorski and Titonis. *Id.* at 5–7.

4. Claims 10, 11, 12, 13, and 15 are rejected under 35 U.S.C. 103 as being unpatentable over Sikorski, Walls, and Titonis. *Id.* at 9–11.

OPINION

Does Sikorski disclose a "first set of tokens" as recited in claim1?

"Before considering the rejections[], we must first [determine the scope of] the claims." *In re Geerdes*, 491 F.2d 1260, 1262 (CCPA 1974). For claim 1, Appellant argues that "Sikorski fails to, however, disclose determining a first set of tokens, when the expressly-recited elements of claim 1 are properly construed." Appeal Br. 9.

The Specification describes a "token" as "a set of raw data of the application that causes a rule to fire." Spec. ¶ 9. The relevant language of claim 1 recites "a set of rules to determine *a first set of tokens* based on a static code analysis. . . wherein the first set of tokens comprises a given token comprising *raw data* of the known malware application code." The Examiner finds Sikorski's "features" are the recited tokens. Final Act. 3 (citing Sikorski Figs. 2 and 3 "and corresponding text" ("plugins.PEFeaturesPlugin")). The description of the drawing figures 2 and 3 explains that the plugins use, for example system memory, to "identify and

label malicious software." Sikorski ¶ 36; *see also* Final Act. 3–4 (citing Sikorski ¶¶ 35–39, Figs. 2 and 3).

In response, the Examiner further explains that in Sikorski, Figures 2 and 3, "the user (investigator of corresponding text paragraphs 35–38) chooses where the set of benign samples and where the set of malicious samples are." Ans. 3–4. The Examiner specifically finds that "[a]nalyzing a known malicious sample produces a feature (token) for that known malicious sample." *Id.* at 4. The Examiner then cites examples of features in Sikorski system as "classify[ing] malicious and benign software" by

> [a]nalyz[ing] *more features than conventional software* including, but not limited to, number of entry points, ratio of instructions disassembled to file size, count of anti-virtual machine instructions, count of functions, count of code blocks, analysis of first code block based on location and count of functions therein, count of XOR operations with different operands, and proximity of API calls.

Id. (citing Sikorski ¶ 10) (emphasis added).

In its Reply, Appellant argues that Sikorski discloses "statistics" in paragraph 10, including "count of blocks" of code. Reply Br. 2. According to Appellant, counting blocks of code "is not 'raw data' <u>of</u> the code." *Id.* We agree.

We agree with Appellant that Sikorski paragraph 10's description of "features" is not the raw data the Specification defines as tokens. *See* Spec. ¶ 9. Figure 4 of Sikorski differentiates "Executable Code," i.e., "raw data," from "Features." Sikorski, Fig. 4 (*see* 3 (Executable Code), *see* 7 (Features)). As shown in Figure 4, "[t]he Feature Extractor System provides one or more disassembly *statistics* to the plugins configured for future extraction." Sikorski ¶ 45 (emphasis added). We agree with Appellant that

the "Features" described in Sikorski's paragraph 10 and Figure 4 are "statistics of the plugins, which are analyzed by the machine learning system." Appeal Br. 10. Accordingly, the Examiner's reliance on the "plugins.PEFeaturesPlugin" of Sikorski's Figures 2 and 3 does not disclose the recited "tokens." *See* Final Act. 3 (citing Sikorski Figs. 2, 3 ("*[B]enign samples and creates a model using the features of the known benign.)*). For the above reasons, we are not persuaded that Sikorski's paragraph 10 disclosure of "more features than conventional software" means those features are the recited "tokens." *See* Final Act. 2.

The Examiner's rejection of claim 1 as anticipated by Sikorski is not sustained. The same teachings of Sikorski regarding "features" as teaching "tokens" are relied on for the remaining independent claims 8 and 14. Final Act. 7 (claim 8), 8 (claim 14). For the reasons we do not sustain the rejection of claim 1, the rejection of claims 8 and 14 is likewise not sustained. Dependent claims 2–7, 9–13, and 15–19 depend from claims 1, 8, or 14 and are allowable because the independent claims are allowable.

DECISION SUMMARY

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1, 2, 16	102(a)(1)	Sikorski		1, 2, 16
3, 4, 6, 7	103	Sikorski, Titonis		3, 4, 6, 7
8, 14, 17, 18	103	Sikorski, Walls		8, 14, 17, 18
10, 11, 12, 13, 15	103	Sikorski, Walls, Titonis		10, 11, 12, 13, 15
Overall Outcome				1–4, 6–8, 10–18

REVERSED