Trials@uspto.gov
571-272-7822

Paper 9
Entered: January 14, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

SYMANTEC CORP.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

---

Case IPR2015-01547
Patent 8,141,154 B2

---

Before THOMAS L. GIANNETTI, RICHARD E. RICE, and MIRIAM L. QUINN *Administrative Patent Judges.*

QUINN, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
*37 C.F.R. § 42.108*

Symantec Corp. ("Petitioner") filed a Petition to institute *inter partes* review of claims 1–12 of U.S. Patent No. 8,141,154 B2 ("the '154 patent") pursuant to 35 U.S.C. § 311–319. Paper 1 ("Pet."). Finjan, Inc. ("Patent Owner") timely filed a Preliminary Response. Paper 8 ("Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314.

For the reasons that follow, we deny the Petition.

## I. BACKGROUND

### A. RELATED MATTERS

Petitioner identifies that the patent-at-issue is the subject matter of a district court case filed in the U.S. District Court for the Northern District of California (Case No. 3:14-cv-02998-RS). Pet. 1. Petitioner also states that petitions for *inter partes* review have been filed regarding patents at issue in the foregoing litigation. *Id.*

### B. ASSERTED GROUNDS

Petitioner contends that claims 1–12 ("the challenged claims") are unpatentable under 35 U.S.C. § 102 and § 103 based on the following specific grounds:

| **Reference[s]** | **Basis** | **Claims challenged** |
|---|---|---|
| Ross[1] | § 102 | 1–5 |
| Ross | § 103 | 2, 4–8, 10, and 11 |

[1] Patent Application Pub. No. US 2007/0113282 (Exhibit 1002) ("Ross").

| Reference[s] | Basis | Claims challenged |
|---|---|---|
| Ross and Calder[2] | § 103 | 9 and 12 |
| Calder and Sirer[3] | § 103 | 1–12 |

C. THE '154 PATENT (EX. 1001)

The '154 patent relates to computer security, and, more particularly, to systems and methods for protecting computers against malicious code such as computer viruses. Ex. 1001, 1:7–9; 8:38–40. The '154 patent identifies the components of one embodiment of the system as follows: a gateway computer, a client computer, and a security computer. *Id.* at 8:45–47. The gateway computer receives content from a network, such as the Internet, over a communication channel. *Id.* at 8:47–48. "Such content may be in the form of HTML pages, XML documents, Java applets and other such web content that is generally rendered by a web browser." *Id.* at 8:48–51. A content modifier modifies original content received by the gateway computer and produces modified content that includes a layer of protection to combat dynamically generated malicious code. *Id.* at 9:13–16.

[2] Patent Application Pub. No. US 2002/0066022 A1 (Exhibit 1003) ("Calder").
[3] Sirer et al., *Design and Implementation of a Distributed Virtual machine for Networked Computers*, (1999) (Exhibit 1004) ("Sirer").

### D. ILLUSTRATIVE CLAIM

Challenged claims 1, 4, 6, and 10 are independent, and illustrative claim 1 is reproduced below.

1. A system for protecting a computer from dynamically generated malicious content, comprising:

a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;

a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and

a receiver for receiving an indicator from the security computer whether it is safe to invoke the second function with the input.

## II. ANALYSIS

### A. CLAIM INTERPRETATION

The Board interprets claims using the "broadest reasonable construction in light of the specification of the patent in which [they] appear[]." 37 C.F.R. § 42.100(b). We presume that claim terms have their ordinary and customary meaning. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) ("The ordinary and customary meaning is the meaning that the term would have to a person of ordinary skill in the art in question.").

Petitioner proposed a construction for one term: "dynamically generate[d]". *See* Pet. 14–15. Patent Owner submitted that the term has a plain and ordinary meaning understood to a person of ordinary skill in the art and that no construction is needed. Prelim. Resp. 7–9. We do not need to construe a proposed term if the construction is not helpful in our

determination of whether to institute trial. Because the construction of the term "dynamically generate[d]" is not germane to our determination whether to institute trial, we will not consider either of the parties' arguments. No term will be construed.

### B. Grounds Based on Ross, and Ross in Combination with Calder

Petitioner asserts three grounds predicated on, at a minimum, Ross disclosing the limitation identified in the Petition as limitation "[A]." Pet. 12 (identifying overlapping limitations in the four independent claims), 18–20 (describing Petitioner's contention regarding Ross's disclosure of limitation 1[A] and 4[A]); 27–28 (stating Petitioner's contention that for claims 6 and 10, limitations are "substantially similar" with the exception of limitations [B2], [E2], and [G]). Limitation [A] in claim 1 recites "a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input . . ." Ex. 1001, 17:34–36. We do not agree with Petitioner that Ross discloses this limitation for, at least, the reasons discussed below and outlined by Patent Owner in the Preliminary Response. *See* Prelim. Resp. 12–15.

#### *1. Overview of Ross (Exhibit 1002)*

Ross describes one embodiment where a device receives and processes "data content having at least one original function call [and it] includes a hook script generator and a script processing engine." Ex. 1002 ¶ 10. One such device is depicted in Figure 2, reproduced below.

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.