Trials@uspto.gov
571-272-7822

Paper 9
Entered: August 13, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET, INC.,
Petitioner,

v.

SOPHOS INC.,
Patent Owner.

Case IPR2015-00619
Patent 8,607,347 B2

Before BRYAN F. MOORE, PETER P. CHEN, and
MICHELLE N. WORMMEESTER, *Administrative Patent Judges.*

CHEN, *Administrative Patent Judge.*

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

I. INTRODUCTION

A. Background

Fortinet, Inc. ("Petitioner") filed a Petition (Paper 3, "Pet.") requesting an *inter partes* review of claims 1, 2, 5, 7, 9, 13, 17, 19, and 21 of U.S. Patent No. 8,607,347 B2 (Ex. 1001, "the '347 patent"). Sophos Inc. ("Patent Owner") did not file a Preliminary Response. We have jurisdiction under 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition."

Upon consideration of the Petition, and for the reasons explained below, we determine that Petitioner has shown that there is a reasonable likelihood that it would prevail with respect to at least one of the challenged claims. We institute an *inter partes* review of claims 1, 2, 5, 7, 9, 13, 17, 19, and 21 of the '347 patent.

B. Related Proceedings

The parties identify the following case involving the '347 patent: *Fortinet, Inc. v. Sophos Inc.*, Case No. 3:13-cv-005831-EMC (N.D. Cal.). Pet. 4; Paper 5. Patent Owner further identifies two pending requests for *inter partes* review involving patents commonly owned with the '347 patent: IPR2015-00617 and IPR2015-00618. Paper 5.

C. The '347 Patent

The '347 patent is titled "Network Stream Scanning Facility," and describes a content request and retrieval system and method to protect client machines from potentially malicious content. Ex. 1001, Abstract. In

particular, the ’347 patent discloses a system and method to “provide improved throughput capabilities related to malware scanning of a file or stream of data within the constraints of a network environment.” *Id*. at 1:33–39. Figure 2 of the ’347 patent is reproduced below.

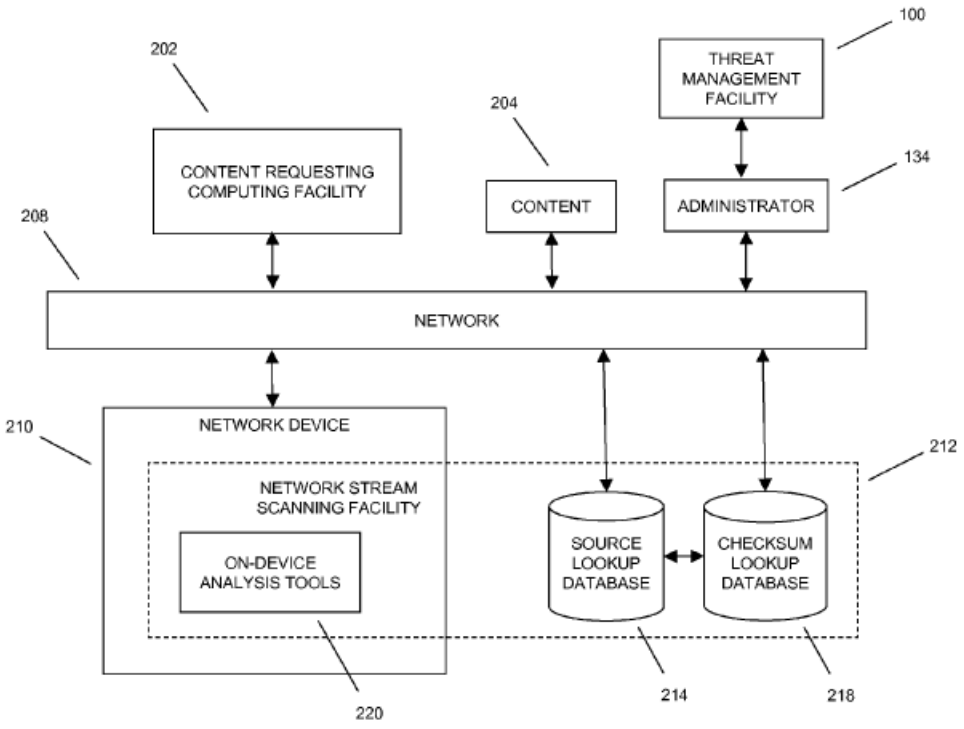

FIG. 2

Figure 2 is a block diagram of the system disclosed in the ’347 patent and depicts content requesting computing facility 202 (for example, a user acting on a client machine), content 204, network 208 (for example, the Internet, an intranet, a LAN, a WAN, or a cell phone network), network device 210 (for example, a server, router, application device, switch, bridge, hub, or repeater) with on-device analysis tools 220, network stream scanning facility 212, and source lookup database 214 and checksum lookup database 218 associated with network stream scanning facility. Ex. 1001, 18:11–20, 47–48, 52–56.

Content requesting computing facility 202 may request content 204. Network device 210 may utilize network stream scanning facility 212 to protect against malware threats in content 204, such as by using a combination of on-device analysis tools 220 and off-device source lookup database 214 and checksum lookup database 218. *Id*. at 18:20–28.

Figure 4 of the ’347 patent is reproduced below.

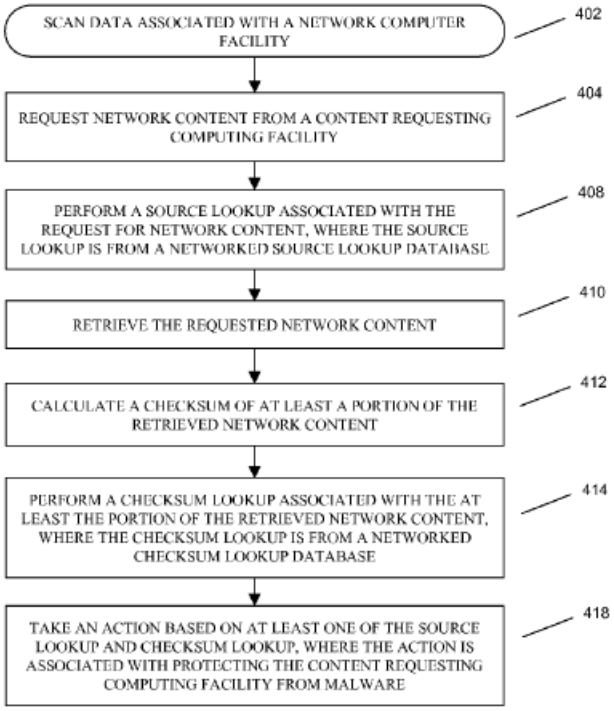

FIG. 4

Figure 4 is a process flow diagram of the method disclosed by the ’347 patent. Ex. 1001, 2:49–50. At step 404, the content requesting computing facility (computer) sends a request to the network device. *Id*. at 21:8–10. The request includes a source from which the network device is to retrieve content from the network. *Id*. At step 408, the network device performs a lookup of the source against a database of known sources. *Id*. at 21:10–14.

The database may include, for example, a "white list" of known trustworthy URLs, or a "black list" of known untrustworthy URLs. *Id*. at 21:29–35.

At step 410, the network device retrieves the requested content and at step 412, the network device calculates a checksum of the content. *Id*. at 21:13–15. At step 414, the network device performs a lookup of the checksum against a database of checksums for known malware. *Id*. at 21:15–20. At step 418, the network device takes action based on at least one of the source database lookup and the checksum lookup. *Id*. at 21:20–25.

D. The Challenged Claims

Petitioner challenges claims 1, 2, 5, 7, 9, 13, 17, 19, and 21 of the '347 patent. Independent claim 1 is illustrative of the claimed subject matter and is reproduced below:

1. A method of scanning data comprising:

receiving a request for network content at a scanning facility, the request received from a content requesting computing facility remote from the scanning facility, and the request including a source from which to retrieve the network content;

performing a source lookup for the request at the scanning facility, wherein the source lookup requests data concerning the source of the request from a networked source lookup database, and wherein the networked source lookup database responds with a characterization of the source;

retrieving the network content to the scanning facility;

calculating a checksum of the network content;

performing a checksum lookup on the checksum, wherein the checksum lookup is from a networked checksum lookup database that stores checksums for known malware content; and

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.