Trials@uspto.gov
571-272-7822

Paper No.10
Entered: November 9, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZSCALER, INC.,
Petitioner,

v.

SYMANTEC CORPORATION,
Patent Owner.

Case IPR2017-01345
Patent 7,392,543 B2

Before RAMA G. ELLURU, DANIEL N. FISHMAN, and STACEY G. WHITE, *Administrative Patent Judges*.

FISHMAN, *Administrative Patent Judge.*

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

I. INTRODUCTION

Zscaler, Inc. ("Petitioner") filed a Petition (Paper 3, "Pet.") requesting *inter partes* review of claims 1–31, all of the claims of the '543 patent,(hereinafter the "challenged claims") of U.S. Patent No. 7,392,543 B2 (Ex. 1001, "the '543 patent") pursuant to 35 U.S.C. §§ 311–319. Symantec Corporation ("Patent Owner") filed a Patent Owner Preliminary Response (Paper 9, "Prelim. Resp."). We have authority to determine whether to institute a trial under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). An *inter partes* review may be instituted only if "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a).

Upon consideration of the Petition, the Preliminary Response, and the evidence of record, we conclude Petitioner has failed to establish a reasonable likelihood of prevailing in showing that any of the challenged claims are unpatentable. Accordingly, we deny institution of an *inter partes* review for all of the challenged claims of the '543 patent.

A. Real Parties-in-Interest and Related Matters

Petitioner identifies Zscaler, Inc. as the sole real party-in-interest. Pet. 56. Both Petitioner and Patent Owner identify a related litigation matter captioned *Symantec Corp. v. Zscaler, Inc.*, Case No. 1:16-cv-01176-SLR-SLF, filed in the U.S. District Court for the District of Delaware. Pet. 56; Paper 5, 2.

B. The '543 Patent

According to the '543 patent, conventional computer immune systems that protect against malicious infection of computer systems utilize file-

based scanning at client nodes and, when suspicious content is detected, a client node sends the suspicious content to a global analysis center for further processing. Ex. 1001, 1:11–15. The global analysis center generates a malicious code signature based on the received suspect content and returns the signature to the client nodes for use in subsequent detection. *Id.* at 1:16–20. Further, according to the '543 patent, prior conventional immune systems detect only suspicious content stored in files and generally do not detect malicious content as it is transmitted over networks. *Id.* at 21–25. Some prior network-based intrusion detection systems employed protocol analyzers to monitor for malicious content embedded within portions of exchanges using known protocols. *Id.* at 1:26–48. Other network-based intrusion systems use a "network sniffer" to detect known signatures of malicious code content. *Id.*

The '543 patent suggests a problem with prior network-based systems because updating the system for signatures of newly detected malicious content is slow—taking hours or days to update, while malicious content may still be exchanged over the network. *Id.* at 49–56. The '543 patent purports to address this problem by providing a host system with local capability to detect malicious code affecting the host system and to generate a malicious code packet for transmission to a local analysis center system. *Id.* at 1:60–2:8. If the local analysis center detects an attack in progress from the received packet, it sends the malicious code packet to a global analysis center for rapid dissemination to other host systems. *Id.*

Figure 3, reproduced below, describes exemplary processing of malicious content in a host system in accordance with the '543 patent.

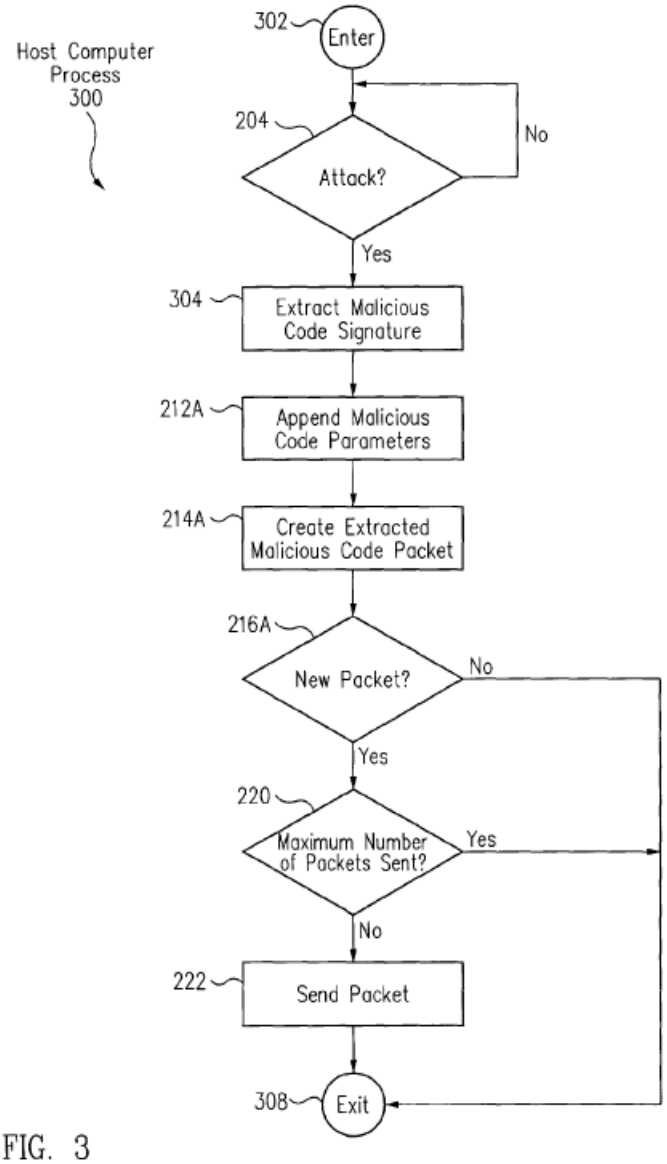

FIG. 3

Figure 3 above is a flow diagram of a host system for processing detected malicious content over a network in accordance with an embodiment of the '543 patent. *Id.* at 9:3–4. Step 204 awaits detection of an attempted attack on the host system by malicious code received over the network. *Id.* Step 304 then extracts/generates a malicious code signature representing the detected malicious, attacking content. *Id.* at 9:25–10:4. Steps 212A and 214A create a malicious code packet based on the signature and other parameters of the detected malicious code. *Id.* at 10:5–36. Steps 216A

through 222 then send the generated packet to an analysis system for further dissemination of a signature for detected malicious content. *Id.* at 10:37–12:20.

C. Illustrative Claim

Claims 1, 6, 20, and 29–31 are the independent claims of the '543 patent. Independent claim 1, reproduced below, is exemplary of the challenged claims:

> 1. A method comprising:
>
> detecting an attack by malicious code on a first computer system;
>
> extracting a malicious code signature from said malicious code comprising:
>
> locating a caller's address of said malicious code in a memory of said first computer system; and
>
> extracting a specific number of bytes backwards from said caller's address;
>
> creating an extracted malicious code packet including said malicious code signature; and
>
> sending said extracted malicious code packet from said first computer system to a second computer system.

D. Alleged Grounds of Unpatentability

The Petition sets forth the following asserted grounds of unpatentability:

Reference(s)	Basis	Challenged Claims
Arnold[1]	102(b)	1–3, 5–8, 20, 22, 26, and 29–31
Arnold	103(a)	4, 9–19, and 21

[1] U.S. Patent No. 5,440,723. Ex. 1008 ("Arnold").

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.