Filed on behalf of: Blue Coat Systems, Inc.
By: Michael T. Rosato (mrosato@wsgr.com)
       Andrew S. Brown (asbrown@wsgr.com)
       Matthew A. Argenti (margenti@wsgr.com)_
       WILSON SONSINI GOODRICH & ROSATI
       701 Fifth Avenue, Suite 5100
       Seattle, WA 98104-7036

UNITED STATES PATENT AND TRADEMARK OFFICE
_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

BLUE COAT SYSTEMS, INC.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

_____

Patent No. 8,677,494

_____

**PETITION FOR INTER PARTES REVIEW OF
U.S. PATENT NO. 8,677,494**

.

I. INTRODUCTION

Pursuant to the provisions of 35 U.S.C. § 311 and § 6 of the Leahy-Smith America Invents Act ("AIA"), and to 37 C.F.R. Part 42, Blue Coat Systems, Inc., ("Petitioner") hereby requests review of United States Patent No. 8,677,494 to Edery *et al.* (hereinafter "the '494 patent," EX1001) that issued on March 18, 2014, and is currently assigned to Finjan, Inc. ("Patent Owner"). This Petition demonstrates that there is a reasonable likelihood that Petitioner will prove by a preponderance of the evidence that claims 7-9 and 16-18 of the '494 patent are unpatentable for failing to distinguish over prior art. Thus, claims 7-9 and 16-18 of the '494 patent should be found unpatentable and canceled.

The Board has previously instituted *inter partes* review of the '494 patent, including of the independent claims from which claims 7-9 and 16-18 depend, in Nos. IPR2015-01892 and IPR2016-00159. This Petition presents essentially the same disclosure and arguments for those independent claims. The additional requirements of the challenged dependent claims 7-9 and 16-18 are insufficient to lend them patentability.

The challenged claims generally recite systems and methods for detecting suspicious "Downloadables" (executable application programs), including: (1) receiving a Downloadable software program, (2) deriving Downloadable security profile data ("DSP data") for the Downloadable; and (3) saving that DSP data in a database. EX1002 ¶16. Similar systems and methods, however, were known in the art since as late as 1995. For example, a system that analyzed executable programs to derive a DSP was demonstrated in in "Dynamic Detection and Classification of

Computer Viruses Using General Behaviour Patterns," by Morton Swimmer *et al.* ("Swimmer," EX1003, Abstract). The DSP contained a list of suspicious operations that may be attempted by the Downloadable, as shown highlighted below:

```
                           ⋮
<CS=3911 Type=0 Fn=30 arg() ret( AX=5)>
<CS=3911 Type=0 Fn=29 arg() ret( BX=128 ES=3911)>
<CS=3911 Type=0 Fn=64 arg( AL=61 CL=3 str1=*.COM) ret( AL=0 CF=0)>
<CS=3911 Type=0 Fn=51 arg( AL=0 str1=COMMAND.COM) ret( AL=0 CX=32 CF=0)>
<CS=3911 Type=0 Fn=51 arg( AL=1 str1=COMMAND.COM) ret( AL=0 CX=32 CF=0)>
<CS=3911 Type=0 Fn=45 arg( AL=2 CL=32 str1=COMMAND.COM) ret( AL=0 AX=5 CF=0)>
<CS=3911 Type=0 Fn=73 arg( BX=5) ret( CX=10241 DX=6206 CF=0)>
<CS=3911 Type=0 Fn=27 arg() ret( CX=5121 DX=8032)>
<CS=3911 Type=0 Fn=47 arg( BX=5 CX=3 DX=828 DS=3911) ret( AX=3 CF=0)>
<CS=3911 Type=0 Fn=50 arg( AL=2 BX=5 CX=0 DX=0) ret( AL=0 AX=50031 DX= CF=0)>
<CS=3911 Type=0 Fn=48 arg( BX=5 CX=648 DX=313 DS=3911) ret( AX=648 CF=0)>
<CS=3911 Type=0 Fn=50 arg( AL=0 BX=5 CX=0 DX=0) ret( AL=0 AX=0 DX=0 CF=0)>
<CS=3911 Type=0 Fn=48 arg( BX=5 CX=3 DX=831 DS=3911) ret( AX=3 CF=0)>
<CS=3911 Type=0 Fn=74 arg( BX=5 CX=10271 DX=6206) ret( CF=0)>
<CS=3911 Type=0 Fn=46 arg( BX=5) ret( CF=0)>
<CS=3911 Type=0 Fn=51 arg( AL=1 str1=COMMAND.COM) ret( AL=0 CX=32 CF=0)>
                           ⋮
```

IDs of suspicious operations

Figure 3: Excerpt from an audit trail for the Vienna virus

EX1003 at FIG. 3; Ex. 1002 ¶67.

It was also well-known in the art that a number of specific types of information could be utilized when detecting suspicious code. Based on the foregoing, the specific components of the DSP required by the challenged dependent claims (i.e., a URL, a digital certificate, or disassembled Downloadable code) also fail to render those claims patentable over the prior art as described in more detail below. Accordingly, the systems and methods claims in the '494 patent were well known and obvious. EX1002 ¶¶ 55-109.

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.

fastcase
Smarter legal research.