

HIGHLY CONFIDENTIAL - ATTORNEYS' EYES ONLY - SOURCE CODE

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

FINJAN, INC., a Delaware Corporation,

Plaintiff,

v.

BLUE COAT SYSTEMS LLC, a Delaware
Corporation,

Defendant.

) CASE NO.: 15-cv-03295-BLF-SVK
)

) **REBUTTAL EXPERT REPORT OF**
) **DR. SETH NIELSON REGARDING**
) **NONINFRINGEMENT OF U.S.**
) **PATENT NOS. 6,154,844; 6,965,968;**
) **7,418,731; 8,079,086; 8,225,408;**
) **8,566,580; 8,677,494; 9,141,786;**
) **9,189,621; AND 9,219,755**

) **CERTAIN PORTIONS CONTAIN**
) **HIGHLY CONFIDENTIAL –**
) **OUTSIDE COUNSELS’ EYES ONLY**
) **– SOURCE CODE INFORMATION**

[REDACTED]

67. As for dynamic analysis, this can be performed in two ways: emulation (otherwise known as “Sandbox” or “SBX” in MAA) or virtualization (otherwise known as “iVM” or “intelliVM” in MAA). [REDACTED] For dynamic analysis, rather than reading the code of the sample to check for signatures, the sample is actually run, and the events it performs are monitored. This is sometimes referred to as “detonation,” since the file is executed, then permitted to run as intended. [REDACTED]

[REDACTED] In iVM, operations are configured to intercept various actions performed both in user programs (such as Adobe) and in the operating system kernel. [REDACTED]

[REDACTED]

[REDACTED]

328. Specifically, as discussed in Section III.E, my analysis of MAA shows that it receives a sample uploaded from requesting clients, and then “detonates” the sample by running it in either a virtualized or emulated sandbox. As the sample is running, MAA keeps track of its behavior, called “events,” such as network events and file system events. A static analysis of the sample may also be performed by NSE. The events are saved to disk in a “Google Protocol Buffers” serialization format. [REDACTED]

[REDACTED]

329. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

332. [REDACTED]

[REDACTED]

[REDACTED] But, contrary to Dr. Cole's assertion that these data stores hold "task results," the cited testimony and exhibits reflect that, at most, the only thing they can store is a log of all events generated during detonation. [REDACTED]

[REDACTED]

█ Event data cannot be “a list of suspicious computer operations”—it is a list of *all* computer operations performed by a sample. Most of these events are *not* suspicious—in fact, it may be that none are. █ █

█
█
█
█
█

333. █

█
█
█
█

█ As stated above, a listing of all events observed during detonation is not “a list of suspicious operations,” and therefore does not comprise the claimed security profile data. █

█
█
█

334. █

█
█ █
█
█

█ █
█
█
█

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.