UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SYMANTEC CORPORATION
Petitioner

v.

THE TRUSTEES OF COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK
Patent Owner

CASE IPR2015-00375
Patent 8,074,115

DECLARATION OF SCOTT M. LEWANDOWSKI

Mail Stop "PATENT BOARD"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

I. INTRODUCTION

1. My name is Scott Lewandowski. Since 2006, I have provided information technology consulting services, with a focus on cyber security, to government and commercial customers through my company The Wynstone Group, Inc. I have served as the Chief Cyber Scientist for the U.S. Department of Defense's National Cyber Range since 2011. From 2000 to 2006, I was a Member of Technical Staff at MIT Lincoln Laboratory. I have a Master's degree in Computer Science, a Bachelor's degree in Computer Science, and a Bachelor's degree in Business Economics, all from Brown University. I am a co-inventor, along with Roger Khazan, Jesse Rabek, and Robert Cunningham, on U.S. Patent Publication No. 2005/0108562 ("Khazan"). My professional biography is attached to this declaration as Exhibit 1.

2. I have been asked by The Trustees of Columbia University in the City of New York ("Columbia") to provide factual information relevant to two *Inter Partes* reviews in the U.S. Patent and Trademark Office, IPR2015-00375 and IPR2015-00377. I understand that in these proceedings, Petitioner Symantec Corporation ("Symantec") has submitted my Khazan patent application publication and has alleged that Khazan invalidates Columbia's U.S. Patent Nos. 8,074,115 (the "'115 patent") and 8,601,322 (the "'322 patent"). I am not providing an expert opinion in this declaration, and I am not a lawyer. However, to understand

how my patent application publication is being characterized by Symantec in these cases, I have reviewed certain documents, which are listed as Exhibit 2.

3. I am being compensated for my time by Columbia at the rate of $800 per hour. My compensation is not contingent upon any aspect of this testimony, the outcome of this matter, or any issues involved in or related to this matter. Other than owning index funds, which I understand may own Symantec stock, I have no financial interest in Symantec or Columbia. I have no financial interest in the ’115 patent or the ’322 patent.

4. I have had intermittent contact with named inventor Prof. Salvatore Stolfo on several occasions, such as at academic conferences. I am currently a sub-contractor on a Defense Advanced Research Projects Agency (“DARPA”) program that is part of named inventor Prof. Angelos Keroymtis’ portfolio as a Program Manager at DARPA. Neither of these relationships have influenced anything that I state in this declaration.

II. BACKGROUND ON KHAZAN

5. The material in Khazan relates to my work at MIT Lincoln Laboratory in the early 2000s. At MIT Lincoln Laboratory, I worked on the Department of Defense’s (“DoD”) most pressing computer security challenges. At that time, a prominent internet threat was the computer worm. Highly publicized cases, such as ILOVEYOU and Slammer, showed the public the devastation and havoc that

small, easily created attacks could create on an internet-scale within a matter of minutes. The worm threat was perceived by the DoD community as a particularly acute risk to the effectiveness of warfighter and command and control systems that were essential to DoD readiness. Some of my earliest projects at the Laboratory focused on autonomically detecting and responding to propagating malware, including worms. I served as the Principal Investigator on several efforts focused on this problem, and implemented the prototype of SARA: Survivable Autonomic Response Architecture.

6. Of particular concern to the DoD was novel computer worms that exploited previously undisclosed vulnerabilities, or so-called “zero-day worms.” These worms had been eluding detection and effective response from commercial systems, and no vendor had a viable roadmap to address the challenge.

7. I came to the realization that a simple, stop-gap response to the zero-day worm crisis was to detect code running on a computer system that was not authorized to run there. Identifying such malicious binaries on disk was easy; hashing and other techniques could be readily applied. Many worms, however, posed a unique challenge in that they are dynamically injected into processes running on a computer system.

8. I eventually came to the realization that previously unauthorized code, in and of itself, was not the primary risk. Rather, the most significant risk arose

when that code interacted with the operating system in a way that could compromise system integrity. I wondered if we could build a system that would detect when this was happening, and alert that unknown – and thus presumably malicious – code was executing, thus stopping zero-day worms immediately, and without reliance on other hosts. This idea was in sharp contrast with other research at the time, which focused either on using community-wide host-level behavior or network activity to detect worms. The system that I was thinking of would be capable of stopping worms without communicating with any other computers.

9. Having conducted my thesis research on interception of API calls, I realized that API interception could be the perfect technique for implementing my idea. By monitoring critical APIs and matching the origin of the calls with known good caller locations, newly introduced calling locations – i.e., dynamically injected worm code, or other code not previously identified as known good caller locations – could be easily identified without the typical false positive challenges inherent to most probabilistic detection approaches.

10. I started to document my ideas for publication as a concept to be presented at a research conference; eventually this morphed into a published paper in a refereed conference. I also began discussing my idea with several of my colleagues, including Roger Khazan. After refining the idea, we realized that the implementation would be so simple that we could task a person with a Bachelor's

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**