Exhibit 9

Attorney's Docket No.: FIN0008-DIV1 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of:	)	
	)	Examiner: Ponnoreay Pich
David Gruzman	)	
Yuval Ben-Itzhak	)	Art Unit: 2435
	)	
Application No: 12/814,584	)	
	)	
Filed: June 14, 2010	)	
	)	
For: SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE	)	

Mail Stop AMENDMENT
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

UNDER 37 C.F.R. §1.111

Sir:

In response to the Office Action dated June 28, 2011, applicants respectfully request that the above-identified application be amended as follows.

IN THE SPECIFICATION:

Please amend paragraph [0003] of the original specification as follows:

[0003] Originally computer viruses were transmitted as executable code inserted into files. As each new ~~viruses~~ virus was discovered, a signature of the virus was collected by anti-virus companies and used from then on to detect the virus and protect computers against it. Users began routinely scanning their file systems using anti-virus software, which regularly updated its signature database as each new virus was discovered.

Please amend paragraph [0008] of the original specification as follows:

[0008] Assignee's US Patent No. 6,092,194 entitled SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES, the contents of which are hereby incorporated by reference, describes gateway level behavioral analysis. Such behavioral analysis scans and parses content received at a gateway and generates a security profile for the content. A security profile is a general list or delineation of suspicious, or potentially malicious, operations that executable content may perform. The derived security profile is then compared with a security policy for the computer being protected, to determine whether or not the content's security profile violates the computer's security policy. A security policy is a general set of simple or complex rules, that may be applied logically in series or in parallel, which determine whether or not a specific operation is permitted

or forbidden to be performed by the content on the computer being protected. Security policies are generally configurable, and set by an administrator of the computer that [[are]] is being protected.

Please amend paragraph [0044] of the original specification as follows:

[0044] The following definitions are employed throughout the specification and claims.

SECURITY ~~POUCY~~ POLICY – a set of one or more rules that determine whether or not a requested operation is permitted. A security policy may be explicitly configurable by a computer system administrator, or may be implicitly determined by application defaults.

SECURITY PROFILE – information describing one or more suspicious operations performed by executable software.

Please amend paragraph [0052] of the original specification as follows:

[0052] Reference is now made to **FIG. 2**, which is a simplified block diagram of a system for protecting a computer from dynamically generated malicious executable code, in accordance with a preferred embodiment of the present invention. Three major components of the system are a gateway computer **205**, a client computer **210**, and a security computer **215**. Gateway computer [[**220**]] **205** receives content from a network, such as the Internet, over a communication channel **220**. Such content may be in the form of HTML pages, XML documents, Java applets and other such web content that is generally rendered by a web browser. Client computer **210** communicates with gateway computer **205** over a communication channel **225**, and

communicates with security computer **215** over a communication channel **230**. Gateway computer **205** receives data at gateway receiver **235**, and transmits data at gateway transmitter **240**. Similarly, client computer **210** receives data at client receiver **245**, and transmits data at client transmitter **250**; and security computer **215** receives data at security receiver **260** and transmits data at security transmitter **265**.

Please amend paragraph [0053] of the original specification as follows:

[0053] It will be appreciated by those skilled in the art that the network topology of **FIG. 2** is shown as a simple topology, for purposes of clarity of exposition. However, the present invention applies to general architectures including a plurality of client computers **210** that are ~~services~~ serviced by one or more gateway computers **205**, and by one or more security computers **215**. Similarly, communication channels **220**, **225** and **230** may each be multiple channels using standard communication protocols such as TCP/IP.

Please amend paragraph [0058] of the original specification as follows:

[0058] Preferably, when call **(*2*)** is made, the substitute function sends the input to security computer **215** for inspection. Preferably, content modifier **265** also inserts program code for the substitute function into the content, or a link to the substitute function. Such a substitute function may be of the following general form shown in **TABLE I**.

TABLE I: Generic substitute function

```
Function Substitute_function(input)
{
```

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.