IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Control Number	:	90/013,016	Confirmation No.:	9521
Patent No.	:	7,647,633		
Inventors	:	Edery et al.		
Issued	:	June 12, 2010		
Title	:	MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS		
TC/Art Unit	:	3992		
Examiner:	:	Adam L. Basehoar		
Attorney Dckt No.	:	FINREXM0005		

Mail Stop *Ex Parte* Reexam
Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NON-FINAL OFFICE ACTION

Sir:

In response to the pending non-final Office Action dated November 19, 2013 (response due February 19, 2014 with granted extension), please consider the following remarks regarding the above-captioned patent.

AMENDMENT TO THE SPECIFICATION

Kindly replace the first paragraph of the specification on page 2 with the following:

This application is a continuation of and incorporates by reference patent application Ser. No. 09/861,229, filed May 17, 2001 now U.S. Pat. No. 7,058,822, which claims benefit of reference provisional application Ser. No. 60/205,591 entitled "Computer Network Malicious Code Runtime Monitoring," filed on May 17, 2000 by inventors Nimrod Itzhak Vered, et al. This application also incorporates by reference the provisional application Ser. No. 60/205,591. This application is also a Continuation-In-Part of and hereby incorporates by reference patent application Ser. No. 09/539,667, now U.S. Pat. No. 6,804,780, entitled "System and Method for Protecting a Computer and Network from Hostile Downloadables" filed on Mar. 30, 2000 by inventor Shlomo Touboul, which is a continuation of U.S. patent application Ser. No. 08/964,388, now U.S. Patent No. 6,092,194, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables" filed on November 6, 1997 by inventor Shlomo Touboul. This application is also a Continuation-In-Part of and hereby incorporates by reference patent application Ser. No. 90/551,302 now U.S. Pat. No. 6,480,962, entitled "System and Method for Protecting a Client During Runtime From Hostile Downloadables", filed on Apr. 2000 by inventor Shlomo Touboul, which is a continuation of U.S. application Ser. No. 08/790,097, now U.S. Patent No. 6,167,520 entitled "System and Method For Protecting a Client From Hostile Downloadables", filed January 29, 1997 by inventor Shlomo Touboul.

AMENDMENTS TO THE CLAIMS

1. (**Original; Rejected**) A computer processor-based method, comprising:

receiving, by a computer, downloadable-information;

determining, by the computer, whether the downloadable-information includes executable code; and

based upon the determination, transmitting from the computer mobile protection code to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

2. (**Original; Rejected**) The method of claim 1, wherein the receiving includes monitoring received information of an information re-communicator.

3. (**Original; Rejected**) The method of claim 2, wherein the information re-communicator is a network server.

4. (**Original; Rejected**) The method of claim 1, wherein the determining comprises analyzing the downloadable-information for an included type indicator indicating an executable file type.

5. (**Original; Rejected**) The method of claim 1, wherein the determining comprises analyzing the downloadable-information for an included type detector indicating an archive file that contains at least one executable.

6. (**Original; Rejected**) The method of claim 1, wherein the determining comprises analyzing the downloadable-information for an included file type indicator and an information pattern corresponding to one or more information patterns that tend to be included within executable code.

7. (**Original; Rejected**) The method of claim 1, further comprising receiving, by the computer, one or more executable code characteristics of executable code that is capable of being executed by the information-destination, and wherein the determining is conducted in accordance with the executable code characteristics.

8. (**Original; Not Rejected**) A computer processor-based system for computer security, the system comprising

an information monitor for receiving downloadable-information by a computer;

a content inspection engine communicatively coupled to the information monitor for determining, by the computer, whether the downloadable-information includes executable code; and

a protection agent engine communicatively coupled to the content inspection engine for causing mobile protection code ("MPC") to be communicated by the computer to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

9. (**Original; Not Rejected**) The system of claim 8, wherein the information monitor intercepts received information received by an information re-communicator.

10. (**Original; Not Rejected**) The system of claim 9, wherein the information re-communicator is a network server.

11. (**Original; Not Rejected**) The system of claim 8, wherein the content inspection engine comprises a file type detector for determining whether the downloadable-information includes a file type indicator indicating an executable file type.

12. (**Original; Not Rejected**) The system of claim 8, wherein the content inspection engine comprises a parser for parsing the downloadable-information and a content analyzer communicatively coupled to the parser for determining whether one or more downloadable-information elements of the downloadable-information correspond with executable code elements.

13. (**Original; Not Rejected**) A processor-based system for computer security, the system comprising:

means for receiving downloadable-information;

means for determining whether the downloadable-information includes executable code; and

means for causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

14. (**Original; Not Rejected**) A computer program product, comprising a computer usable medium having a computer readable program code therein, the computer readable program code adapted to be executed for computer security, the method comprising:

providing a system, wherein the system comprises distinct software modules, and wherein the distinct software modules comprise an information re-communicator and a mobile code executor;

receiving, at the information re-communicator, downloadable-information including executable code; and

causing mobile protection code to be executed by the mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code.

15. (**Original; Not Rejected**) The method of claim 14, wherein the mobile code executor is a Java Virtual Machine.

16. (**Original; Not Rejected**) The method of claim 14, wherein the mobile code executor is the operating system, running native code executables.

17. (**Original; Not Rejected**) The method of claim 14, wherein the mobile code executor is a subsystem of the operating system.

18. (**Original; Not Rejected**) The method of claim 14, wherein the mobile code executor is a scripting host.

19. (**Original; Not Rejected**) The method of claim 14, wherein the re-communicator is at least one of a firewall and a network server.

0. (**Original; Not Rejected**) The method claim 14, wherein executing the mobile protection code at the destination causes downloadable interfaces to resources at the destination to be modified such that at least one attempted operation of the executable code is diverted to the mobile protection code.

21. (**Original; Not Rejected**) A processor-based system for computer security, the system comprising:

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.