5-22-00   A/PROV

Please type a plus sign (+) inside this → +

Docket Number: 40492.00013

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Large Entity)

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Nimrod Itzhak	Vered	Moshav Mismeret #81, Goosh Tel-Mond 40695, Israel
Yigal Mordechai	Edery	Hashikma 11, POB 1115, Pardesia 42815, Israel
David R.	Kroll	1233 Klee Court, Sunnyvale, CA 94087

☐ *Additional inventors are being named on page 2 attached hereto*

TITLE OF THE INVENTION (280 characters max)

COMPUTER NETWORK MALICIOUS CODE RUN-TIME MONITORING

CORRESPONDENCE ADDRESS

Direct all correspondence to:

23840

☒ Customer Number: 23840 → *Place Customer Number Bar Code Label here*

OR

☒ Firm *or* Individual Name: **Graham & James LLP**

Address	**600 Hansen Way**
Address	
City	**Palo Alto**
State	**CA**
ZIP	**94304-1043**
Country	**US**
Telephone	**650-856-6500**
Fax	**650-856-3619**

ENCLOSED APPLICATION PARTS (check all that apply)

☒ Specification   *Number of Pages*   **6**

☒ Drawing(s)   *Number of Sheets*   **1**   ☐ Other (specify) _____

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)

☒ A check or money order is enclosed to cover the filing fees

FILING FEE AMOUNT ($)

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: **05-0150**   **$150.00**

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE _____   DATE **May 17, 2000**

TYPED or PRINTED NAME   **Marc A. Sockol**

REGISTRATION NO. *(if appropriate)*   **40,823**

TELEPHONE   **650-856-6500**

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

[Page 1 of   2   ]   P19LARGE/REV04

JC541 U.S. PTO
60/205591
05/17/00

PROVISIONAL APPLICATION FOR PATENT COVER SHEET (Large Entity)

INVENTOR(S)/APPLICANT(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (city and either State or Foreign Country)

Certificate of Mailing by Express Mail

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, DC 20231

P19LARGE/REV04

PROVISIONAL APPLICATION FOR
UNITED STATES PATENT
IN THE NAME

of

NIMROD ITZHAK VERED, YIGAL MORDECHAI EDERY

AND DAVID R. KROLL

for

COMPUTER NETWORK MALICIOUS CODE

RUN-TIME MONITORING

DOCKET NO. 40492.00013

Please direct communications to:
GRAHAM & JAMES LLP
600 Hansen Way
Palo Alto, CA 94304-1043
(650) 856-6500
Express Mail Number: EL515156294US

Finjan   Product Management

Computer Network Malicious Code Run-time Monitoring
(Patent Application)

Nimrod Vered, Director Product Management
Yigal Edery, Director R&D
Dave Kroll, Director of Marketing

Abstract

A network security content-inspection server with a sandbox agent that performs runtime monitoring of application programs (e.g. Executables (.exe files) or ActiveX controls) received over the Internet or an Intranet. Static scanning at the network server level (e.g., HTTP proxy server or plug-in to an existing Proxy or Firewall server) identifies application programs and wraps the application programs with a sandbox agent. During runtime of the program at the client computer, the sandbox agent self-extracts and modifies certain programs running in the memory, thereby creating a sandbox environment that monitors for security policy violations. Execution of an instruction is prevented in the event of a policy violation.

Claims

1) A method of detecting application programs while arriving through the Internet or Intranet (e.g. SMTP, HTTP or FTP traffic) and wrapping them with a sandbox agent.
2) The method of claim 1, wherein the computer network includes a server and client computers, and wherein the wrapping takes place at the server, wherein the executing the application program takes place at the client.
3) The method of claim 1, wherein the sandbox agent contains the code needed to create the sandbox environment without instrumenting the original application program.
4) The method of claim 1, further using a white list to create exception list of those application programs that are not to be wrapped with the sandbox agent.
5) The method of claim 4, wherein the identification of those specific application programs that are not to be wrapped will be done using either MD-5 hash for all the users or all the application programs for a specific user or a group of users.
6) A method of creating a sandbox environment for a secure execution of an application program on a client computer while no installation of a software module is taking place.
7) The method of claim 6, wherein the sandbox agent checks the specific client computer security policy before starting the execution of the application program.
8) The method of claim 6, wherein the sandbox agent facilitates a filtering layer where all of the application programs calls are compared in to the given security policy.

1

9) The method of claim 8, wherein if the application program violated the security program it will be either automatically stopped from running or the user will manually stop it from running. In both cases a message will be presented to the computer user.

Field of Invention

The invention pertains to computer network security and specifically to secure execution of program applications.

Background

The rapid development of the Internet brought the concept of distributed computing, where small application programs 'travel' over the Internet from Web servers to client computers and execute on the clients, saving the processing resources of the servers. This concept is now being implemented by businesses worldwide, especially in the era of e-commerce. Because of the connectivity that the Internet provides, computer users are sharing and opening more programs voluntarily. In addition, there are active Web programs run automatically in Web browsers without user permission. Hackers are taking advantage of technologies and techniques to develop malicious code for attacking unsuspecting and protected computer users.

Executable programs (.exe) are a popular technology used to create self-contained programs for commercial use as well as for hacking purposes. An example of commercial usage of executables is in the e-greeting card/e-games market where tens of thousands of small executable programs are sent between users every day. An example of a popular hacking tool that is delivered as an executable is Back Orifice, a remote access tool used to take control of PCs. There are many tools available freely on the Internet that allow hackers to combine or "bind" a benign e-greeting card and a malicious attack together so only the greeting card will be visible to the user.

However, no products exist that monitor the behavior of executable programs during runtime. Many computer users have been attacked while running executables that they trusted. Often, as with a computer worm attack, malicious code arrives from a spoofed e-mail source, which the user might trust without knowing that the e-mail was spoofed.

Executable files are written in a low-level computer language and cannot be scanned by a gateway server because its behavior can only be determined at the time it runs on a specific computer. In fact, its behavior might change from computer to computer or may have instructions only to execute on a specific date or at a specific time

Hence programs that will be able to monitor application programs during runtime are needed.

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.