US 20230231872A1

(19) United States
(12) Patent Application Publication
MacLeod et al.
(10) Pub. No.: US 2023/0231872 A1
(43) Pub. Date: Jul. 20, 2023

(54) DETECTION OF AND PROTECTION FROM MALWARE AND STEGANOGRAPHY

(71) Applicant: **Cyemptive Technologies, Inc.**, Woodinville, WA (US)

(72) Inventors: **Stewart P. MacLeod**, Woodinville, WA (US); **Robert Pike**, Woodinville, WA (US)

(21) Appl. No.: **18/147,478**

(22) Filed: **Dec. 28, 2022**

Related U.S. Application Data

(63) Continuation of application No. 15/993,426, filed on May 30, 2018, now Pat. No. 11,575,704.

(60) Provisional application No. 62/512,659, filed on May 30, 2017.

Publication Classification

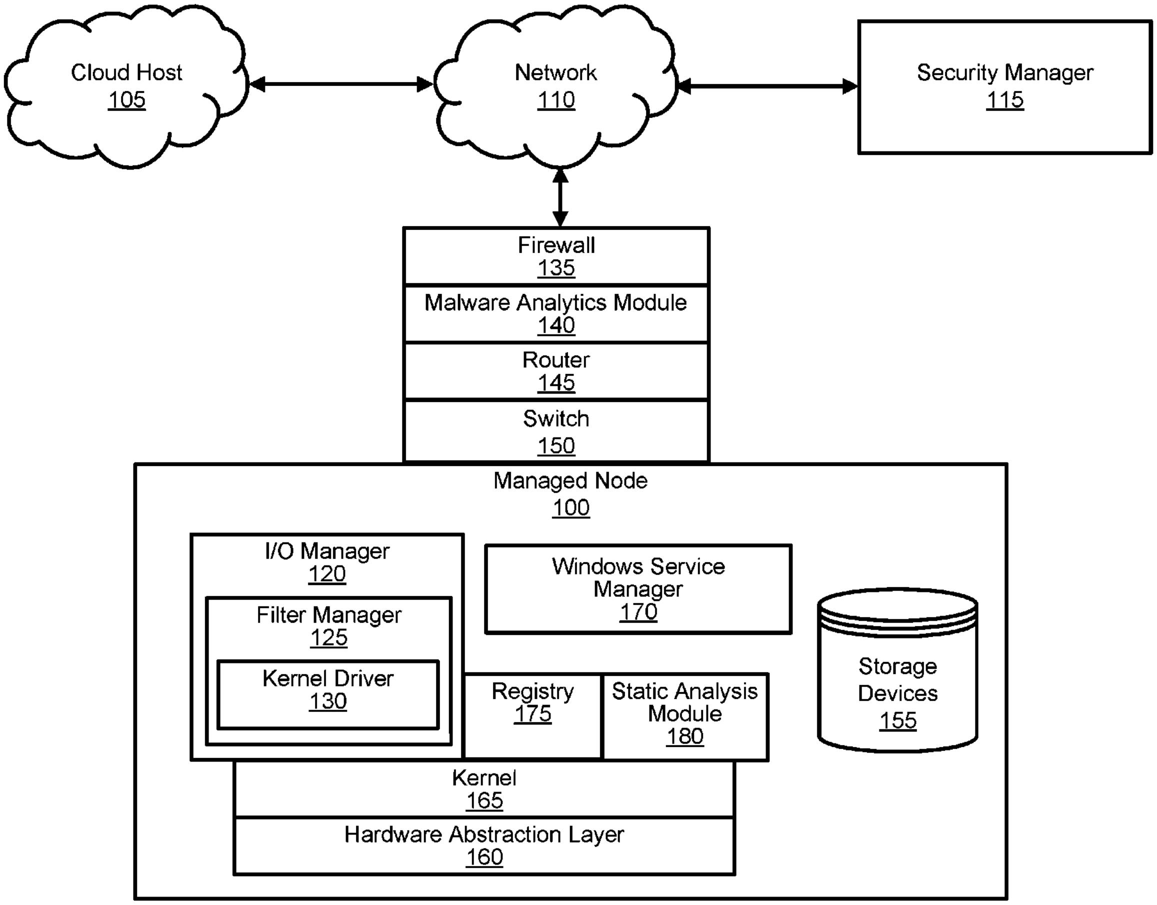
(51) **Int. Cl.**

H04L 9/40	(2006.01)
G06F 11/20	(2006.01)
G06F 21/55	(2006.01)
G06F 21/56	(2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/145*** (2013.01); ***G06F 11/2038*** (2013.01); ***G06F 21/554*** (2013.01); ***G06F 21/566*** (2013.01); ***H04L 63/0236*** (2013.01); ***H04L 63/1416*** (2013.01)

(57) ABSTRACT

A method for real-time detection of and protection from steganography in a kernel mode comprises detecting transmission of a file via a firewall, an operating system, or an e-mail system. A size of the file is determined. From a file system, a stored filesize of the file is retrieved. The determined size of the file is compared to the stored filesize of the file. Responsive to the determined size of the file being larger than the stored filesize of the file, steganography detection analytics are executed on the file. Responsive to the steganography detection analytics indicating presence of steganography in the file, a steganography remediation action is executed, and information is transmitted describing the steganography to a client device.


Cloud Host
105
Network
110
Security Manager
115
Firewall
135
Malware Analytics Module
140
Router
145
Switch
150
Managed Node
100
I/O Manager
120
Filter Manager
125
Kernel Driver
130
Windows Service Manager
170
Registry
175
Static Analysis Module
180
Storage Devices
155
Kernel
165
Hardware Abstraction Layer
160