US010536471B1

(12) **United States Patent**
Derbeko et al.

(10) **Patent No.: US 10,536,471 B1**
(45) **Date of Patent: Jan. 14, 2020**

(54) **MALWARE DETECTION IN VIRTUAL MACHINES**

(71) Applicant: **EMC IP Holding Company LLC**, Hopkinton, MA (US)

(72) Inventors: **Philip Derbeko**, Modiin (IL); **Shai Kappel**, Bnaya (IL); **Uriya Stern**, Lehavim (IL); **Maya Bakshi**, Beer Sheva (IL); **Yaniv Harel**, Neve-Monosson (IL)

(73) Assignee: **EMC IP Holding Company LLC**, Hopkinton, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 139 days.

(21) Appl. No.: **15/086,979**

(22) Filed: **Mar. 31, 2016**

(51) **Int. Cl.**

G06F 12/14	(2006.01)
H04L 29/06	(2006.01)
G06F 9/455	(2018.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1425*** (2013.01); ***G06F 9/45558*** (2013.01); ***H04L 63/145*** (2013.01); ***H04L 63/1416*** (2013.01); *G06F 2009/45587* (2013.01)

(58) **Field of Classification Search**
CPC . G06F 2009/45587; G06F 2009/45595; G06F 21/552; G06F 21/56; G06F 21/566; G06F 21/567; G06F 2201/815; G06F 9/45533; G06F 2009/45591; G06F 2201/84; H04L 63/1416; H04L 63/20; H04L 63/1425
USPC 726/1, 22–24
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,775,780	B1 *	8/2004	Muttik	G06F 21/53 713/165
8,056,134	B1 *	11/2011	Ogilvie	G06F 21/566 713/187
8,151,263	B1 *	4/2012	Venkitachalam	G06F 9/485 711/162
8,726,083	B1 *	5/2014	van der Goot	G06F 11/1438 714/15
8,904,525	B1 *	12/2014	Hodgman	G06F 21/562 726/22
8,949,829	B1 *	2/2015	Xing	G06F 11/1469 718/1
9,230,100	B2 *	1/2016	Wang	G06F 21/53
9,400,886	B1 *	7/2016	Beloussov	G06F 21/566
9,690,936	B1 *	6/2017	Malik	G06F 21/562
9,740,577	B1 *	8/2017	Chakraborty	G06F 11/1469
10,048,890	B1 *	8/2018	Samad	G06F 3/0619

(Continued)

FOREIGN PATENT DOCUMENTS

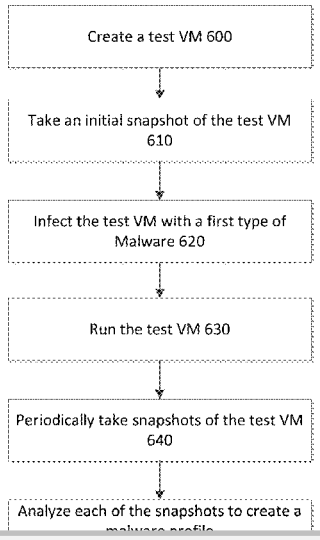
CN	105068856 A *	11/2015	
CN	105068856 A *	11/2015	
EP	3241140 A1 *	11/2017	G06F 21/53

Primary Examiner — Jason K Gee
Assistant Examiner — Lizbeth Torres-Diaz
(74) *Attorney, Agent, or Firm* — Ryan, Mason & Lewis, LLP

(57) **ABSTRACT**

A system, computer program product, and computer-executable method of detecting malware in a virtual machine (VM), the computer-executable method comprising periodically creating snapshots of the VM, analyzing each of the snapshots in comparison to one or more previous snapshots to determine whether anomalies exist, and based on a threshold amount of anomalies detected, scanning the VM to determine whether malware is detected.

20 Claims, 10 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2007/0240222	A1*	10/2007	Tuvell	G06F 21/56 726/24
2009/0158432	A1*	6/2009	Zheng	G06F 21/562 726/24
2016/0321455	A1*	11/2016	Deng	G06F 21/577
2017/0034198	A1*	2/2017	Powers	G06F 21/552
2019/0235973	A1*	8/2019	Brewer	G06F 11/1469

* cited by examiner

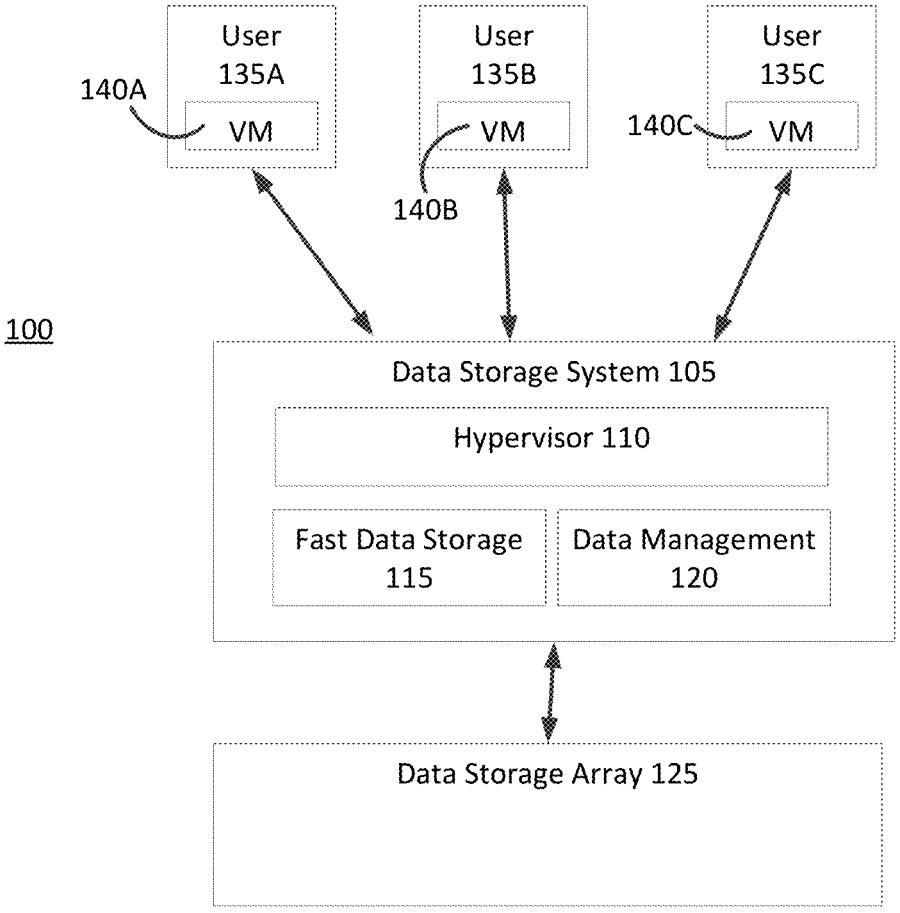


FIG. 1

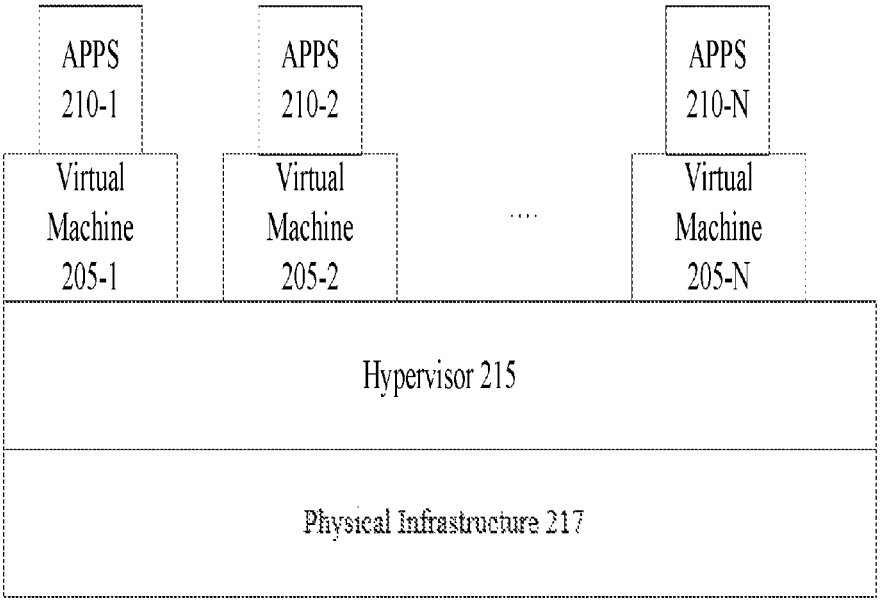


FIG. 2

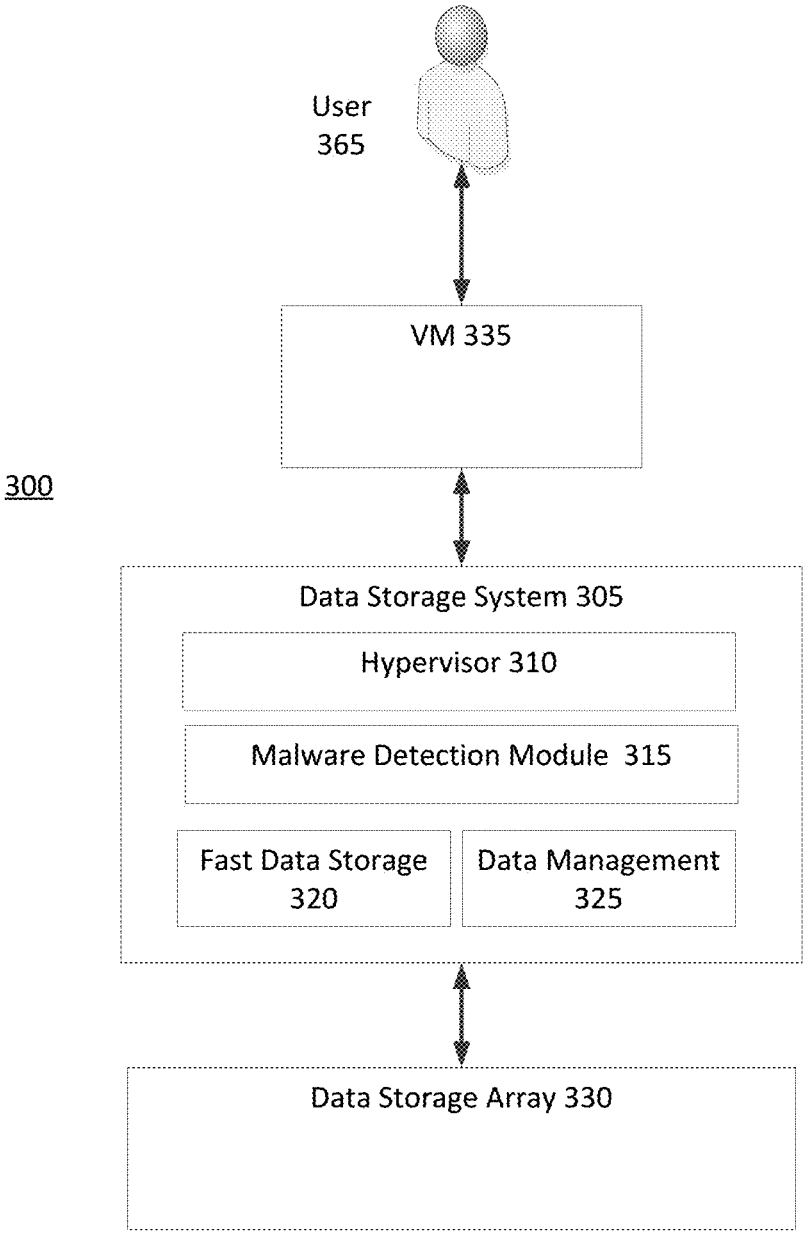


FIG. 3A

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.