US010783241B2

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

(10) **Patent No.: US 10,783,241 B2**
(45) **Date of Patent: Sep. 22, 2020**

(54) **SYSTEM AND METHODS FOR SANDBOXED MALWARE ANALYSIS AND AUTOMATED PATCH DEVELOPMENT, DEPLOYMENT AND VALIDATION**

(71) Applicant: **QOMPLX, Inc.**, Reston, VA (US)

(72) Inventors: **Jason Crabtree**, Vienna, VA (US); **Andrew Sellers**, Monument, CO (US)

(73) Assignee: **QOMPLX, INC.**, Tysons, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 209 days.

(21) Appl. No.: **15/887,496**

(22) Filed: **Feb. 2, 2018**

(65) **Prior Publication Data**

US 2018/0276372 A1 Sep. 27, 2018

Related U.S. Application Data

(63) Continuation-in-part of application No. 15/818,733, filed on Nov. 20, 2017, which is a

(Continued)

(51) **Int. Cl.**

G06F 21/53	(2013.01)
G06F 21/56	(2013.01)
G06F 21/57	(2013.01)
G06F 8/65	(2018.01)
G06F 9/455	(2018.01)
H04L 29/06	(2006.01)

(Continued)

(52) **U.S. Cl.**
CPC ***G06F 21/53*** (2013.01); ***G06F 8/65*** (2013.01); ***G06F 9/455*** (2013.01); ***G06F 21/566*** (2013.01); ***G06F 21/577*** (2013.01); ***G06Q 40/08*** (2013.01); ***H04L 63/1425*** (2013.01); ***H04L 63/1433*** (2013.01); *G06F 2221/033* (2013.01); *G06F 2221/2149* (2013.01); *G06N 20/00* (2019.01); *G06Q 50/01* (2013.01)

(58) **Field of Classification Search**
CPC . G06F 21/53; G06F 9/455; G06F 8/65; G06F 21/577; G06F 21/566; G06F 2221/2149; G06F 2221/033; G06F 11/3058; H04L 63/1433; H04L 63/1425; G06Q 40/08; G06Q 50/01; G06N 20/00
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,256,544 B1	7/2001	Weissinger	
9,141,360 B1 *	9/2015	Chen	G06F 8/52

(Continued)

FOREIGN PATENT DOCUMENTS

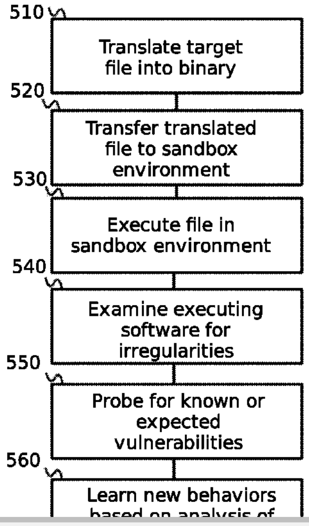
WO	2014159150 A1	10/2014
WO	2017075543 A1	5/2017

Primary Examiner — Cheng-Feng Huang
(74) *Attorney, Agent, or Firm* — Brian S. Boon; Brian R. Galvin; Galvin Patent Law LLC

(57) **ABSTRACT**

A system and methods for sandboxed malware analysis and automated patch development, deployment and validation, that uses a business operating system, vulnerability scoring engine, binary translation engine, sandbox simulation engine, at least one network endpoint, at least one database, a network, and a combination of machine learning and vulnerability probing techniques, to analyze software, locate any vulnerabilities or malicious behavior, and attempt to patch and prevent undesired behavior from occurring, autonomously.

2 Claims, 12 Drawing Sheets


510
Translate target file into binary
520
Transfer translated file to sandbox environment
530
Execute file in sandbox environment
540
Examine executing software for irregularities
550
Probe for known or expected vulnerabilities
560
Learn new behaviors based on analysis of

Related U.S. Application Data

continuation-in-part of application No. 15/725,274, filed on Oct. 4, 2017, now Pat. No. 10,609,079, which is a continuation-in-part of application No. 15/655,113, filed on Jul. 20, 2017, which is a continuation-in-part of application No. 15/616,427, filed on Jun. 7, 2017, and a continuation-in-part of application No. 15/237,625, filed on Aug. 15, 2016, now Pat. No. 10,248,910, which is a continuation-in-part of application No. 15/206,195, filed on Jul. 8, 2016, which is a continuation-in-part of application No. 15/186,453, filed on Jun. 18, 2016, which is a continuation-in-part of application No. 15/166,158, filed on May 26, 2016, which is a continuation-in-part of application No. 15/141,752, filed on Apr. 28, 2016, which is a continuation-in-part of application No. 15/091,563, filed on Apr. 5, 2016, now Pat. No. 10,204,147, and a continuation-in-part of application No. 14/986,536, filed on Dec. 31, 2015, now Pat. No. 10,210,255, and a continuation-in-part of application No. 14/925,974, filed on Oct. 28, 2015, application No. 15/887,496, which is a continuation-in-part of application No. 15/823,285, filed on Nov. 27, 2017, which is a continuation-in-part of application No. 15/788,718, filed on Oct. 19, 2017, which is a continuation-in-part of application No. 15/788,002, filed on Oct. 19, 2017, which is a continuation-in-part of application No. 15/787,601, filed on Oct. 18, 2017, which is a continuation-in-part of application No. 15/616,427, filed on Jun. 7, 2017, which is a continuation-in-part of application No. 14/925,974, filed on Oct. 28, 2015.

(60) Provisional application No. 62/568,307, filed on Oct. 4, 2017, provisional application No. 62/568,305, filed on Oct. 4, 2017, provisional application No. 62/568,312, filed on Oct. 4, 2017.

(51) **Int. Cl.**

G06Q 40/08	(2012.01)
G06N 20/00	(2019.01)
G06Q 50/00	(2012.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0289072	A1	12/2005	Sabharwal	
2007/0011659	A1	1/2007	Venolia	
2013/0097706	A1 *	4/2013	Titonis	H04W 12/12 726/24
2016/0004858	A1 *	1/2016	Chen	G06F 21/57 726/17
2016/0028758	A1	1/2016	Ellis et al.	
2016/0099960	A1 *	4/2016	Gerritz	H04L 63/1433 726/23
2016/0275123	A1	9/2016	Lin et al.	
2017/0126712	A1	5/2017	Crabtree et al.	
2017/0139763	A1	5/2017	Ellwein	
2017/0149802	A1	5/2017	Huang et al.	

* cited by examiner

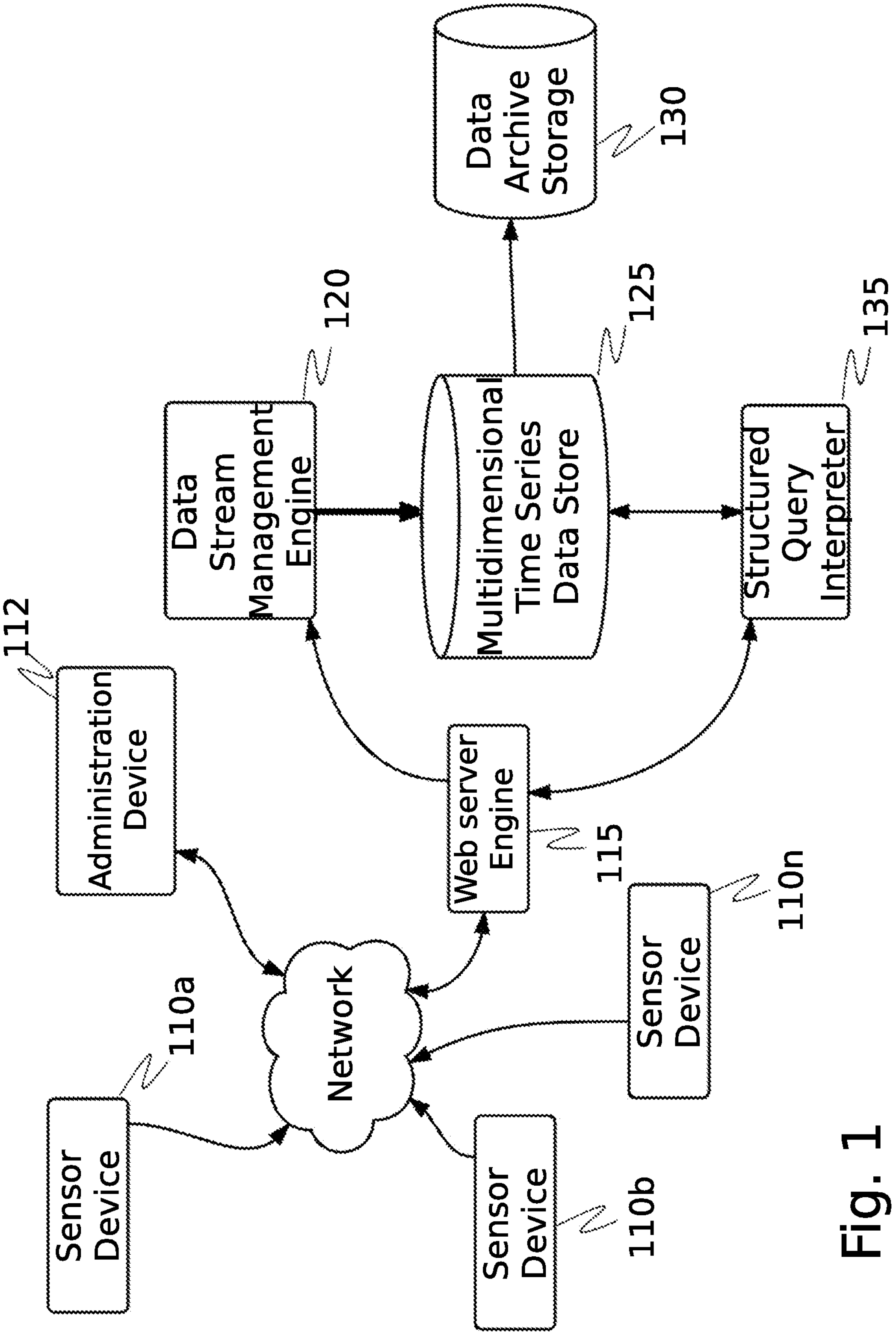

Data Archive Storage
130
Data Stream Management Engine
120
Multidimensional Time Series Data Store
125
Structured Query Interpreter
135
Administration Device
112
Web server Engine
115
Network
Sensor Device
110a
Sensor Device
110b
Sensor Device
110n

Fig. 1

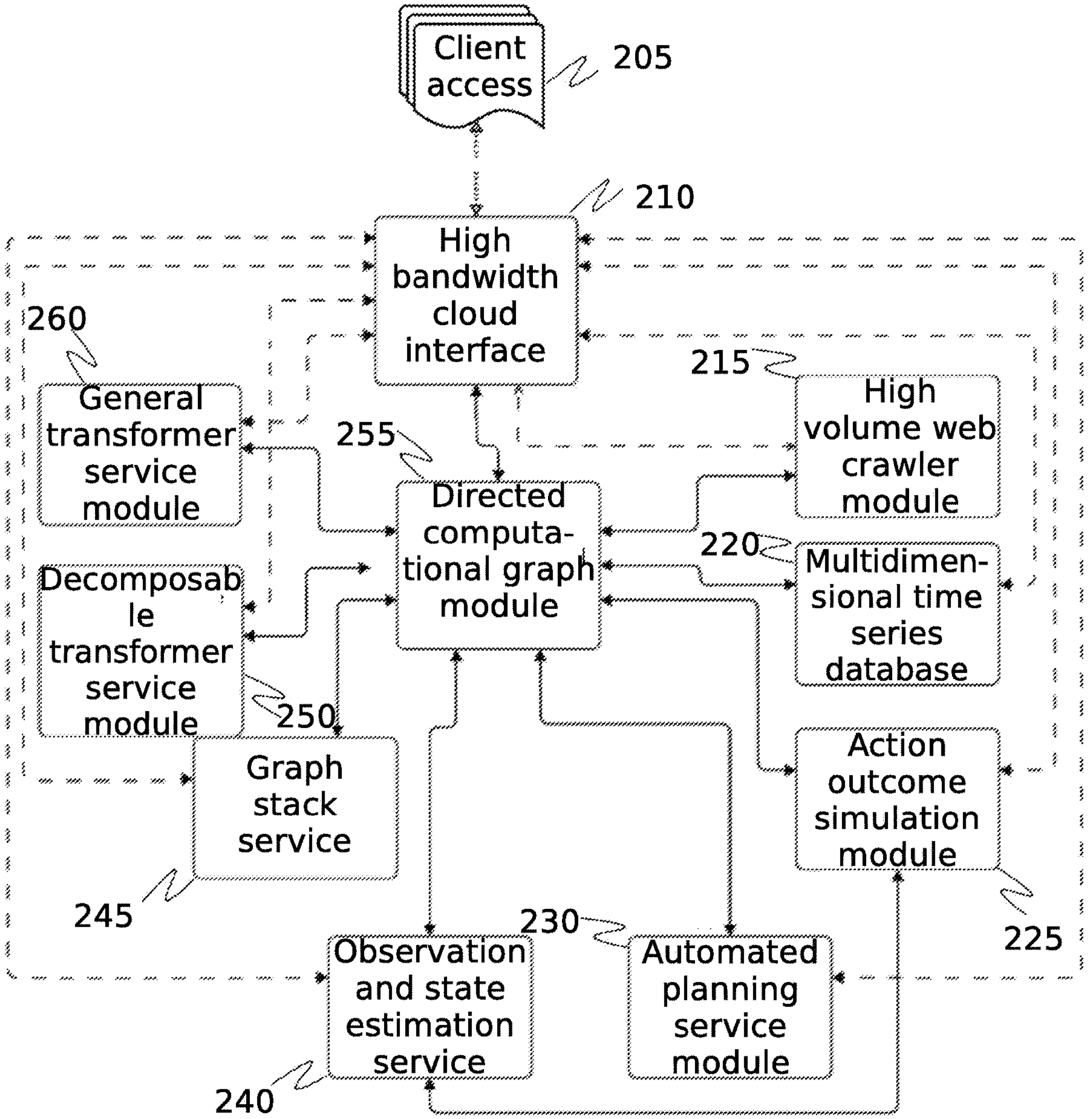

Client access
205
210
High bandwidth cloud interface
260
215
General transformer service module
255
High volume web crawler module
Directed computa-tional graph module
220
Multidimen-sional time series database
Decomposab le transformer service module
250
Graph stack service
Action outcome simulation module
245
230
225
Observation and state estimation service
Automated planning service module
240

Fig. 2

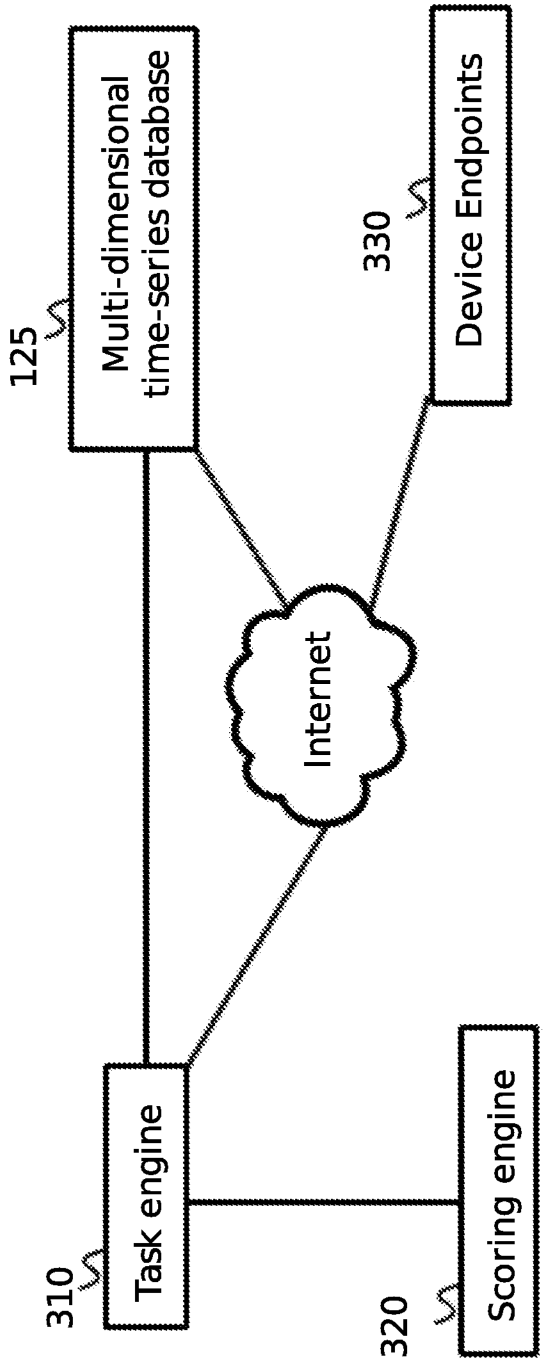

125
Multi-dimensional time-series database
330
Device Endpoints
Internet
310
Task engine
320
Scoring engine

Fig. 3

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**