US009088606B2

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

(10) **Patent No.: US 9,088,606 B2**
(45) **Date of Patent: Jul. 21, 2015**

(54) **SYSTEM AND METHOD FOR STRATEGIC ANTI-MALWARE MONITORING**

(71) Applicant: **Tenable Network Security, Inc.**, Columbia, MD (US)

(72) Inventors: **Marcus J. Ranum**, Morrisdale, PA (US); **Ron Gula**, Marriottsville, MD (US)

(73) Assignee: **TENABLE NETWORK SECURITY, INC.**, Columbia, MD (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 245 days.

(21) Appl. No.: **13/692,200**

(22) Filed: **Dec. 3, 2012**

(65) **Prior Publication Data**

US 2014/0013434 A1 Jan. 9, 2014

Related U.S. Application Data

(60) Provisional application No. 61/668,278, filed on Jul. 5, 2012.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/145*** (2013.01); ***H04L 63/1416*** (2013.01); ***H04L 63/1433*** (2013.01)

(58) **Field of Classification Search**
CPC H04L 63/145
USPC 726/24
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,525,599 A 6/1985 Curran et al.
5,541,997 A 7/1996 Pappas et al.
5,572,729 A 11/1996 Giordano et al.
5,715,391 A 2/1998 Jackson et al.
5,721,819 A 2/1998 Galles et al.
5,838,919 A 11/1998 Schwaller et al.
5,844,817 A 12/1998 Lobley et al.
6,154,775 A 11/2000 Coss et al.
6,266,774 B1 7/2001 Sampath et al.

(Continued)

OTHER PUBLICATIONS

Hoagland, James A., "Audit Log Analysis Using the Visual Audit Browser Toolkit", Department of Computer Science, University of California, Davis.

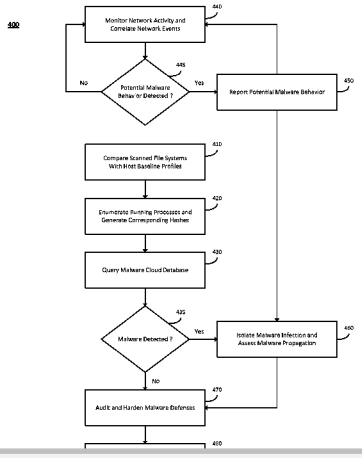
(Continued)

Primary Examiner — Justin T Darrow
(74) *Attorney, Agent, or Firm* — Muncy, Geissler, Olds & Lowe, P.C.

(57) **ABSTRACT**

The system and method described herein may leverage active network scanning and passive network monitoring to provide strategic anti-malware monitoring in a network. In particular, the system and method described herein may remotely connect to managed hosts in a network to compute hashes or other signatures associated with processes running thereon and suspicious files hosted thereon, wherein the hashes may communicated to a cloud database that aggregates all known virus or malware signatures that various anti-virus vendors have catalogued to detect malware infections without requiring the hosts to have a local or resident anti-virus agent. Furthermore, running processes and file system activity may be monitored in the network to further detect malware infections. Additionally, the network scanning and network monitoring may be used to detect hosts that may potentially be participating in an active botnet or hosting botnet content and audit anti-virus strategies deployed in the network.

30 Claims, 5 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

6,324,656	B1	11/2001	Gleichauf et al.
6,393,568	B1	5/2002	Ranger et al.
6,415,321	B1	7/2002	Gleichauf et al.
6,487,666	B1	11/2002	Shanklin et al.
6,499,107	B1	12/2002	Gleichauf et al.
6,510,509	B1	1/2003	Chopra et al.
6,606,663	B1	8/2003	Liao et al.
6,704,874	B1	3/2004	Porras et al.
6,711,127	B1	3/2004	Gorman et al.
6,789,202	B1	9/2004	Ko et al.
6,847,982	B2	1/2005	Parker et al.
6,873,617	B1	3/2005	Karras
6,882,728	B1	4/2005	Takahashi et al.
6,886,020	B1	4/2005	Zahavi et al.
6,952,779	B1	10/2005	Cohen et al.
6,957,348	B1	10/2005	Flowers et al.
6,968,377	B1	11/2005	Gleichauf et al.
7,013,395	B1	3/2006	Swiler et al.
7,017,186	B2	3/2006	Day
7,073,198	B1	7/2006	Flowers et al.
7,093,287	B1	8/2006	Gusler et al.
7,120,148	B1	10/2006	Batz et al.
7,134,141	B2	11/2006	Crosbie et al.
7,139,819	B1	11/2006	Luo et al.
7,162,742	B1	1/2007	Flowers et al.
7,181,769	B1	2/2007	Keanini et al.
7,237,264	B1	6/2007	Graham et al.
7,243,366	B2	7/2007	Medvinsky et al.
7,272,646	B2	9/2007	Cooper et al.
7,290,145	B2	10/2007	Falkenthros
7,310,687	B2	12/2007	Psounis et al.
7,324,551	B1	1/2008	Stammers
7,483,986	B2	1/2009	Hanson et al.
7,509,681	B2	3/2009	Flowers et al.
7,530,104	B1	5/2009	Thrower et al.
7,562,388	B2	7/2009	Hackenberger et al.
7,571,482	B2	8/2009	Polyakov et al.
7,594,273	B2	9/2009	Keanini et al.
7,603,711	B2	10/2009	Scheidell
7,653,647	B2	1/2010	Borthakur et al.
7,661,134	B2	2/2010	Radatti
7,735,100	B1	6/2010	Sallam
7,735,140	B2	6/2010	Datla et al.
7,739,377	B2	6/2010	Benedetti et al.
7,752,671	B2	7/2010	Kotler et al.
7,761,918	B2	7/2010	Gula et al.
7,774,848	B2	8/2010	D'Mello et al.
7,882,542	B2	2/2011	Neystadt et al.
7,895,651	B2	2/2011	Brennan
7,904,479	B2	3/2011	Zuk
7,904,962	B1	3/2011	Jajodia et al.
7,908,254	B2	3/2011	Suemondt et al.
7,926,113	B1	4/2011	Gula et al.
7,966,358	B2	6/2011	Deolalikar et al.
7,971,252	B2	6/2011	Lippmann et al.
7,975,298	B1	7/2011	Venkatasubrahmanyam
7,996,836	B1	8/2011	McCorkendale et al.
8,001,606	B1	8/2011	Spertus
8,015,284	B1	9/2011	Isenberg et al.
8,032,489	B2	10/2011	Villella et al.
8,126,853	B2	2/2012	Sakamoto
8,135,815	B2	3/2012	Mayer
8,135,823	B2	3/2012	Cole et al.
8,191,149	B2	5/2012	Yun et al.
8,201,257	B1	6/2012	Andres et al.
8,239,942	B2	8/2012	Shanklin et al.
2001/0034847	A1	10/2001	Gaul, Jr.
2002/0019945	A1	2/2002	Houston et al.
2002/0093527	A1	7/2002	Sherlock et al.
2002/0100023	A1	7/2002	Ueki et al.
2002/0107841	A1	8/2002	Hellerstein et al.
2002/0138762	A1	9/2002	Horne
2002/0166063	A1	11/2002	Lachman, III et al.
2003/0056116	A1	3/2003	Bunker, V et al.
2003/0135517	A1	7/2003	Kauffman
2003/0145225	A1	7/2003	Bruton, III et al.
2003/0196123	A1	10/2003	Rowland et al.
2003/0212779	A1	11/2003	Boyter et al.
2003/0220940	A1	11/2003	Futoransky et al.
2004/0003266	A1	1/2004	Moshir et al.
2004/0015719	A1	1/2004	Lee et al.
2004/0042470	A1	3/2004	Cooper et al.
2004/0093521	A1	5/2004	Hamadeh et al.
2004/0193918	A1	9/2004	Green et al.
2004/0250169	A1	12/2004	Takemori et al.
2005/0044390	A1	2/2005	Trostle
2005/0068928	A1	3/2005	Smith et al.
2005/0097199	A1	5/2005	Woodard et al.
2005/0108578	A1	5/2005	Tajalli et al.
2005/0128988	A1	6/2005	Simpson et al.
2005/0188419	A1	8/2005	Dadhia et al.
2005/0203886	A1	9/2005	Wong
2005/0203921	A1	9/2005	Newman et al.
2005/0229255	A1	10/2005	Gula et al.
2006/0010245	A1	1/2006	Carnahan
2006/0018466	A1	1/2006	Adelstein et al.
2006/0031476	A1	2/2006	Mathes et al.
2006/0117091	A1	6/2006	Justin
2006/0130144	A1	6/2006	Wernicke
2006/0184682	A1	8/2006	Suchowski et al.
2007/0028110	A1	2/2007	Brennan
2007/0028302	A1	2/2007	Brennan et al.
2007/0028304	A1	2/2007	Brennan
2007/0169190	A1	7/2007	Kolton et al.
2007/0240220	A1	10/2007	Tuvell et al.
2007/0271598	A1	11/2007	Chen et al.
2007/0277238	A1	11/2007	Margalit et al.
2008/0002725	A1	1/2008	Alicherry et al.
2008/0022400	A1	1/2008	Cohen et al.
2008/0046393	A1	2/2008	Jajodia et al.
2008/0047009	A1	2/2008	Overcash et al.
2008/0072285	A1	3/2008	Sankaran et al.
2008/0086772	A1*	4/2008	Chesla 726/23
2008/0155084	A1	6/2008	Yu et al.
2009/0013141	A1	1/2009	Kinoshita
2009/0044024	A1	2/2009	Oberheide et al.
2009/0049016	A1	2/2009	Sakamoto
2009/0077666	A1	3/2009	Chen et al.
2009/0177782	A1	7/2009	Blatherwick et al.
2010/0030780	A1	2/2010	Eshghi et al.
2010/0043066	A1	2/2010	Miliefsky
2010/0058431	A1	3/2010	McCorkendale et al.
2010/0058456	A1	3/2010	Jajodia et al.
2010/0077479	A1	3/2010	Viljoen
2010/0083381	A1	4/2010	Khosravi et al.
2010/0114842	A1	5/2010	Forman et al.
2010/0138925	A1	6/2010	Barai et al.
2010/0169975	A1	7/2010	Stefanidakis et al.
2010/0174921	A1	7/2010	Abzarian et al.
2010/0175106	A1	7/2010	Diebler et al.
2010/0175134	A1	7/2010	Ali-Ahmad et al.
2010/0175135	A1	7/2010	Kandek et al.
2010/0262688	A1	10/2010	Hussain et al.
2010/0281539	A1	11/2010	Burns et al.
2010/0281543	A1	11/2010	Golomb et al.
2010/0332593	A1	12/2010	Barash et al.
2011/0029772	A1	2/2011	Fanton et al.
2011/0047597	A1	2/2011	Mahaffey et al.
2011/0061104	A1	3/2011	Sarraute Yamada et al.
2011/0099620	A1	4/2011	Stavrou et al.
2011/0126287	A1	5/2011	Yoo
2011/0162070	A1	6/2011	Krasser et al.
2011/0185055	A1	7/2011	Nappier et al.
2011/0185431	A1	7/2011	Deraison
2011/0191854	A1	8/2011	Giakouminakis et al.
2011/0231934	A1	9/2011	Davis et al.
2011/0231935	A1	9/2011	Gula et al.
2011/0277034	A1	11/2011	Hanson
2011/0314245	A1	12/2011	Hanes et al.
2012/0011590	A1	1/2012	Donovan

(56) **References Cited**

U.S. PATENT DOCUMENTS

OTHER PUBLICATIONS

Tenable Network Security, "Log Correlation Engine 4.0 High Performance Configuration Guide", Jul. 10, 2012, Revision 2.
Tenable Network Security, "Log Correlation Engine Best Practices", Mar. 2, 2012, Revision 2.
Gula, Ron, "Tenable Event Correlation", Tenable Network Security, Mar. 1, 2012, Revision 1.
FortiAnalyzer TM, Administration Guide, Version 4.0 MR2, Mar. 21, 2011, Revision 13.
Wack, John, et al., NIST Special Publication 800-42, "Guideline on Network Security Testing", Computer Security Division, National Institute of Standards and Technology, Oct. 2003, pp. 1-92.
Deraison, Renaud, et al., "Passive Vulnerability Scanning Introduction to NeVo", Revision 9, Tenable Network Security, Aug. 2003, pp. 1-13.
Deraison, Renaud, et al., "Unified Security Monitoring (USM); Real-Time Situational Awareness of Network Vulnerabilities, Events and Configurations", Revision 2, Tenable Network Security, Jan. 27, 2009, 12 pages.
Zhang, Yin, et al., "Detecting Backdoors", Proceedings of the 9th USENIX Security Symposium, Denver, Colorado, Aug. 2000, 11 pages.
"Basic Cryptanalysis", Department of the Army, Field Manual No. 34-40-2, Sep. 13, 1990, 363 pages.
Kim, Gene H., et al., "The Design and Implementation of Tripwire: A File System Integrity Checker", Proceedings of the 2nd ACM Conference on Computer and Communications Security, 1994, (Purdue Technical Report CSD-TR-93-071), 18 pages.
Oline, Adam, et al., "Exploring Three-Dimensional Visualization for Intrusion Detection", Workshop on Visualization for Computer Security, IEEE, Oct. 26, 2005, 9 pages.
Gula, Ron, "Predicting Attack Paths: Leveraging active and passive vulnerability discovery to identify trusted exploitable weak points in your network", Tenable Network Security, Inc, Mar. 20, 2012, Revision 2.
"Strategic Anti-malware Monitoring with Nessus, PVS, & LCE", Tenable Network Security, Inc, May 29, 2012, Revision 1.

* cited by examiner

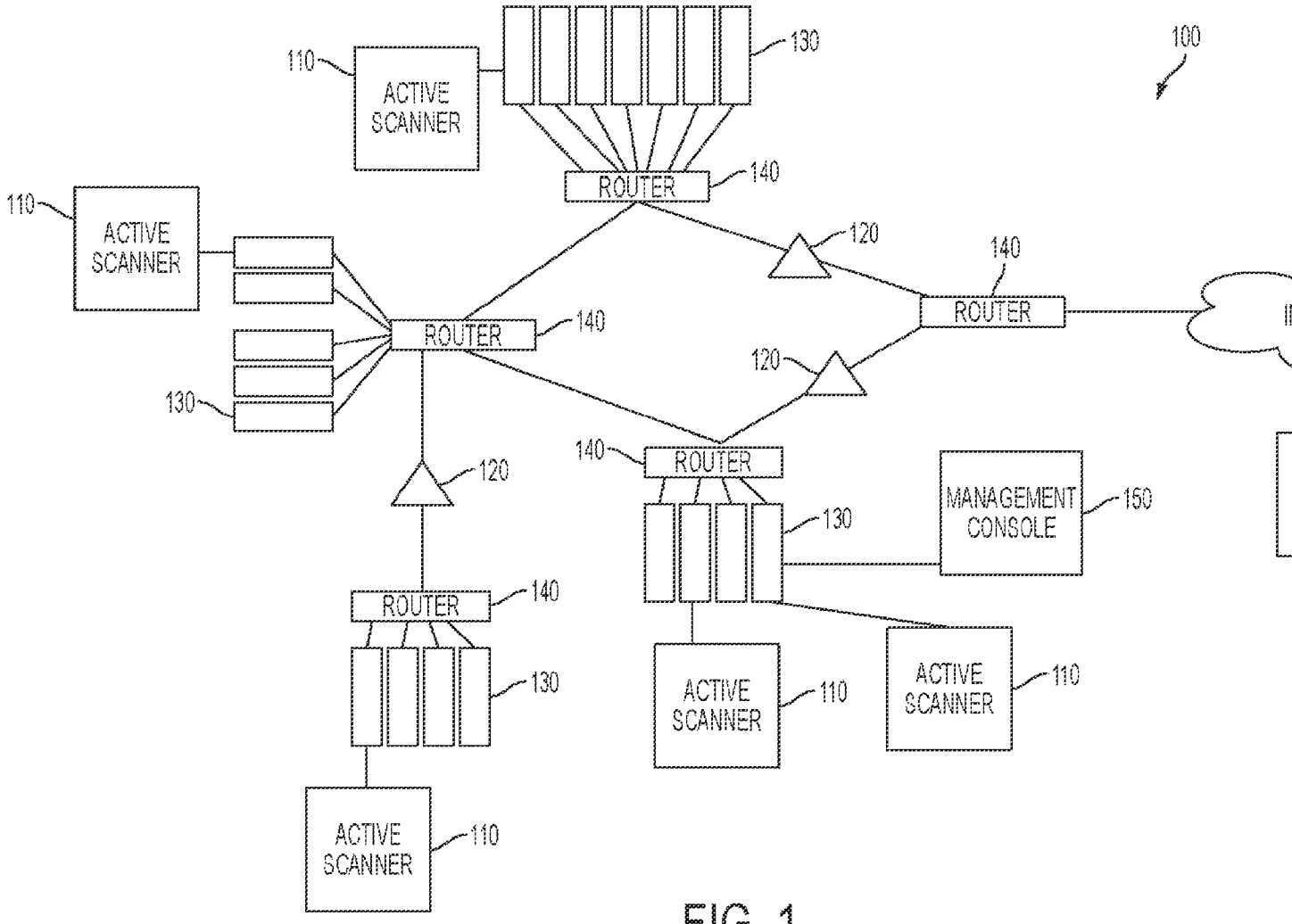


FIG. 1

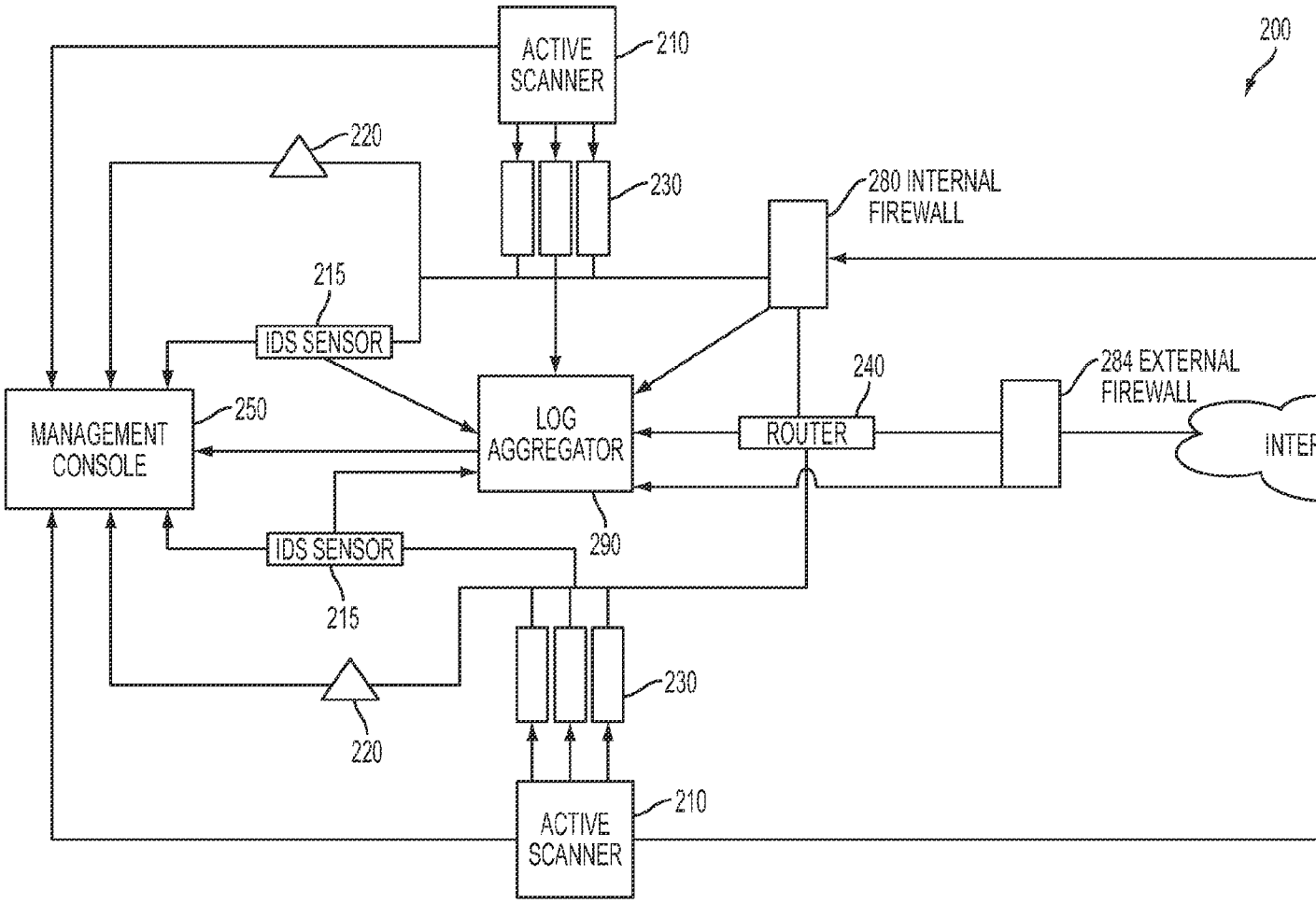


FIG. 2

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.