IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC., OPENTEXT INC.,	§	
	§	
Plaintiffs,	§	
v.	§	
AO KASPERSKY LAB	§	**6:22-CV-00243-ADA-DTG**
TREND MICRO, INC.	§	**6:22-CV-00239-ADA-DTG**
SOPHOS LTD.	§	**6:22-CV-00240-ADA-DTG**
CROWDSTRIKE, INC. and CROWDSTRIKE HOLDINGS, INC.	§	**6:22-CV-00241-ADA-DTG**
FORCEPOINT, LLC,	§	**6:22-CV-00342-ADA-DTG**
Defendants		

OPENING CLAIM CONSTRUCTION BRIEF REGARDING PATENTS PLAINTIFFS WEBROOT AND OPENTEXT ADDED BY AMENDMENT FROM:
AO KASPERSKY LAB ("KASPERSKY"),
TREND MICRO, INC., ("TREND MICRO"),
SOPHOS LTD. ("SOPHOS"),
CROWDSTRIKE, INC. AND CROWDSTRIKE HOLDINGS, INC. ("CROWDSTRIKE"),
AND FORCEPOINT, LLC ("FORCEPOINT")

TABLE OF CONTENTS

I. ’244, ’243 AND, ’932 PATENTS 1

A. “pestware” (’244 patent, claims 1-4, 7, 9-12, and 15; ’243 patent, 1, 3, 6, 8, and 12; ’505 patent, claims 1, 2, 4, 6, 7, 9, 11, 12, 14, and 16-20; ’932 patent, claims 1, 2, 5, 7, 12, and 13) 2

B. “kernel-mode driver” (’244 patent, claims 1 and 9; ’243 patent, claims 1, 6, and 12; ’932 patent, claims 1 and 12) 3

C. “suspicion of pestware” / “suspected of originating pestware” / “suspected pestware object” / “suspected pestware process” / “suspicious activity” / “suspected pestware” / “suspected pestware-related event” / “suspected to be pestware-related” (’244 patent, claims 1, 3, 4, 6, 9, 10, 11, and 12; ’243 patent, claims 1, 3, and 12; ’932 patent, claims 1, 2, 5, 12, and 13) 4

D. “time of interest includes a time interval” / “time of interest including a time interval” (’244 patent, claims 1 and 9) 6

E. “externally networked [pestware research entity / source]” (’243 patent, claims 1, 2, 6, 12, and 13; ’244 patent, claims 1 and 7-10; ’932 patent, claims 1, 3, 5, 10, 12, and 14) 7

F. “a timestamp module . . .” (’244 patent claims 9 and 14) 10

G. “potential pestware activity” (’244 patent, claims 9, 10, and 15) 12

H. “a heuristics module” (’244 patent claims 11 and 12; ’243 patent claims 6 and 8; ’932 patent claims 5 and 7) 14

I. “identify[ing] . . . access[ing] . . . report[ing] . . .” (’243 claims 1, 6, and 12) 16

J. “monitor[ing] . . . stor[ing] . . . analyz[ing] . . . identify[ing] [a suspected pestware object] . . . identi[fying] [an externally networked source] . . . report[ing] . . .” (’932 claims 1, 5, 12) 20

K. “identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client, and a program” (’932 patent, claims 1, 9, and 12). 23

L. “kernel-level monitor” (’932 patent, claims 5, 7, and 8; ’505 patent, claim 16) 24

M. “a research portion configured . . .” (’244 patent, claim 9; ’243 patent, claim 6; ’932 patent, claim 5) 28

N. “a reporting portion configured . . .” (’244 patent, claim 9; ’243 patent, claim 6; ’932 patent, claim 5) 30

II. ’123 PATENT 31

A. "receiving . . . receiving . . . receiving . . . determining . . . determining . . ." ('123 patent, claims 1, 4, 13, and 16) 32

B. "security products" ('123 patent, claims 1, 3, 4, 6, 10, 11, 12, 13, 14, 15, and 16) 36

III. '505 PATENT 38

A. "behavior rules" ('505 patent, claims 1, 2, 6, 7, 11, 12, 16, and 17) 39

B. "scan[ning] data in a registry" ('505 patent, claims 1, 6, and 11) 40

C. "pestware management engine" ('505 patent, claims 2, 7, 12, and 16) 43

D. "the boot sequence" ('505 patent, claim 10) 45

E. Claims 1, 6, and 11 of the '505 patent 46

F. Claim 6 of the '505 patent: "a memory comprising: . . ." 49

IV. '869 PATENT 52

A. "the static data points" ('869 patent, claims 1, 10, 15, 18, 32, and 46) 52

B. "within a predetermined range" (claims 18, 32, and 46) 54

TABLE OF AUTHORITIES

CASES

Abbott Labs. v. Andrx Pharms., Inc.,
473 F.3d 1196 (Fed. Cir. 2007).....23

Abbott Labs. v. Baxter Pharm. Prod., Inc.,
334 F.3d 1274 (Fed. Cir. 2003).....23, 24

Altris, Inc. v. Symantec Corp.,
318 F.3d 1363 (Fed. Cir. 2003).....47

Apple Inc. v. Motorola, Inc.,
757 F.3d 1286 (Fed. Cir. 2014).....29, 31

Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech.,
521 F.3d 1328 (Fed. Cir. 2008).....11, 15

Audioeye, Inc. v. AccessiBe Ltd.,
No. 6:20-cv-00997-ADA, Dkt. 69 .....14, 43, 44

Avago Techs. Gen. IP (Singapore) Pte Ltd. v. Asustek Computer, Inc.,
No. 15-CV-04525-EMC, 2016 WL 3029674 (N.D. Cal. May 27, 2016).....18, 48

Baldwin Graphic Sys., Inc. v. Siebert, Inc.,
512 F.3d 1338 (Fed. Cir. 2008).....46

Bushnell Hawthorne, LLC v. Cisco Sys. Inc.,
813 F. App'x 522 (Fed. Cir. 2020) 54

DDR Holdings, LLC v. Hotels.com, L.P.,
773 F.3d 1245 (Fed. Cir. 2014).....6

Diebold Nixdorf, Inc. v. Int'l Trade Comm'n,
899 F.3d 1291 (Fed. Cir. 2018).....50

Dyfan, LLC v. Target Corp.,
28 F.4th 1360 (Fed. Cir. 2022) 29

Interval Licensing LLC v. AOL, Inc.,
766 F.3d 1364 (Fed. Cir. 2014).....5, 6

Konami Gaming, Inc. v. Marks Studios, LLC,
No. 2:14-cv-01485-JAD-CWH, 2017 WL 3174905 (D. Nev. July 25, 2017).....50

Kyocera Senco Indus. Tools Inc. v. Int'l Trade Comm'n,
22 F.4th 1369 (Fed. Cir. 2022) 2

Lenovo Holding Co. v. DoDots Licensing Sols. LLC,
Nos. 2021-1247, 2021-1521, 2021-1580, 2021 WL 5822248 (Fed. Cir. Dec. 8, 2021).....2

Lighting World, Inc. v. Birchwood Lighting, Inc.,
382 F.3d 1354 (Fed. Cir. 2004).....29

Maxim Integrated Prod., Inc. v. Silicon Mitus Tech., Inc.,
No. 17-CV-03507 NC, 2018 WL 4657384 (N.D. Cal. July 3, 2018).....18, 48

Meds Co. v. Mylan, Inc.,
853 F.3d 1296 (Fed. Cir. 2017).....3

Mformation Techs., Inc. v. Rsch. in Motion Ltd.,
764 F.3d 1392 (Fed. Cir. 2014).....18, 21, 34, 47

MonkeyMedia, Inc. v. Apple, Inc.,
Nos. A-10-CA-319-SS, A-10-CA-533-SS, 2013 WL 12076550 (W.D. Tex. Feb. 22, 2013).29

Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.,
831 F.3d 1350 (Fed. Cir. 2016).....23, 24

Nautilus, Inc. v. Biosig Instruments, Inc.,
572 U.S. 898 (2014).....7, 30, 31, 45, 53

Noah Sys., Inc. v. Intuit, Inc.,
675 F.3d 1302 (Fed. Cir. 2012).....30, 31, 51

Oak Tech. Inc. v. Int'l Trade Comm'n,
248 F.3d 1316 (Fed. Cir. 2001).....35

Omega Eng'g, Inc. v. Raytek Corp.,
334 F.3d 1314 (Fed. Cir. 2003).....9

Parity Networks, LLC v. ZyXEL Commc'ns, Inc. et al.,
No. SACV 20-697-JVS, 2020 WL 8569299 (C.D. Cal. Dec. 22, 2020).....43, 51

Phillips v. AWH Corp.,
415 F.3d 1303 9

Process Control Corp. v. HydReclaim Corp.,
190 F.3d 1350 (Fed. Cir. 1999).....33

Prolifiq Software Inc. v. Veeva Sys. Inc.,
No. C 13–03644 SI, 2014 WL 3870016 (N.D. Cal. Aug. 6, 2014) 6

Sensor Elec. Tech., Inc. v. Bolb, Inc.,
No. 18-cv-05194-LHK, 2019 WL 4645338 (N.D. Cal. Sept. 24, 2019) 45

Shire Dev., LLC v. Watson Pharms., Inc.,
848 F.3d 981 (Fed. Cir. 2017).....24

St. Isidore Research, LLC v. Comerica Inc.,
2016 WL 4988246 (E.D. Tex. Sep. 19, 2016).....50

Takadu Ltd. v. Innovyze LLC,
No. 21-291-RGA, 2023 WL 2563157 (D. Del. Mar. 17, 2023).....43

Vehicular Techs. Corp. v. Titan Wheel Int'l, Inc.,
212 F.3d 1377 (Fed. Cir. 2000).....23

Versata Software, Inc. v. SAP Am., Inc.,
No. 2:07-CV-153, 2009 WL 1408520 (E.D. Tex. May 19, 2009).....18, 35

Visto Corp. v. Good Tech., Inc.,
No. 2:06-CV-039, 2008 WL 163576 (E.D. Tex. Jan. 16, 2008).....19

Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.,
853 F.3d 1272 (Fed. Cir. 2017).....40

Wi-LAN, Inc. v. Apple, Inc.,
811 F.3d 455 (Fed. Cir. 2016).....16, 20, 33, 47

Williamson v. Citrix Online, LLC,
792 F.3d 1339 (Fed. Cir. 2015).....10, 11, 14, 15, 29, 30, 43, 44, 50

WMS Gaming, Inc. v. Int'l Game Tech.,
184 F.3d 1339 (Fed. Cir. 1999).....51

WSOU Inv. LLC v. Dell Techs. Inc., et al.,
No. 6:20-cv-00473 (Dkt. 94) (W.D. Tex. May 27, 2021).....47, 48

WSOU Investments LLC v. Dell Techs. Inc.,
No. 6:20–cv-00476-ADA, slip op. (W.D. Tex. May 27, 2021).....48

WSOU Investments, LLC v. Google,
No. 6:20-cv-00581-ADA, Dkt. No. 46 (W.D. Tex. June 2, 2021).....53

WSOU Investments, LLC v. Huawei Tech. Co.,
Dkt. No. 64 (W.D. Tex. June 1, 2021).....53

TABLE OF EXHIBITS

A	Declaration of Venkatramanan S. Subrahmanian, Ph.D.
A-1	Oxford Dictionary of Computing, 4th Ed. (1996)
A-2	Dictionary of Computer and Internet Terms (Barron's), 11th Ed. (2013)
A-3	Design Patterns: Elements of Reusable Object-Oriented Software (1995)
A-4	Operating Systems: Internals and Design Principles (2001)
A-5	Software Engineering: A Practitioner's Approach, 5th Ed. (2001)
A-6	Computer Networking: A Top-Down Approach Featuring the Internet (2001)
A-7	Software Engineering, 7th Ed. (2004)
A-8	Software Engineering: A Practitioner's Approach, 6th Ed. (2005)
A-9	US 2016/0155201 A9, June 23, 2000 (Bell)
A-10	U.S. Patent Appl. No. 2007/0242887 A1, October 7, 2005 (Matsushita)
A-11	U.S. Patent No. 7,466,713, June 16, 2005 (Saito)
A-12	U.S. Patent No. 6,745,211, November 21, 2001 (Kabasakalian)
B	Walsh-IP patent Search Report (April 6, 2023) and Non-patent Literature Review Report (April 7, 2023)
C	U.S. Patent Appl. No. 2007/0094496 A1, April 26, 2007 (Burtscher)
D	New Oxford American Dictionary, 3rd Ed. (2010)
E	Newton's Telecom Dictionary, 22nd Ed. (2006)
F	File History of U.S. Patent 8,201,243: Original Claims

G	File History of U.S. Patent 8,201,243: Amendment and Argument, Aug. 20, 2010
H	File History of U.S. Patent 8,201,243: Office Action, Nov. 10, 2010
I	File History of U.S. Patent 8,201,243: Amendment and Argument, Nov. 9, 2011
J	File History of U.S. Patent 8,201,243: Notice of Allowance, Feb. 9, 2012
K	File History of U.S. Patent 8,181,244: Original Claims
L	File History of U.S. Patent 8,181,244: Amendment and Argument, Aug. 20, 2010
M	File History of U.S. Patent 8,181,244: Office Action, Sept. 10, 2010
N	File History of U.S. Patent 8,181,244: Amendment and Argument, Sept. 28, 2011
O	File History of U.S. Patent 8,181,244: Notice of Allowance
P	File History of U.S. Patent 8,856,505: Original Claims, April 30, 2012
Q	File History of U.S. Patent 8,856,505: Non-Final Office Action, October 18, 2013
R	File History of U.S. Patent 8,856,505: Amendment and Response, January 22, 2014
S	U.S. Patent Appl. No. 2005/0268112 A1 (Wang)
T	U.S. Patent Appl. No. 2004/0024864 A1 (Porras)
U	Declaration of Kevin C. Almeroth, Ph.D.
V	The American Heritage Dictionary, 5th Ed.
W	The Authoritative Dictionary of IEEE Standards Terms, 7th Ed.
X	Webster's New World Dictionary of Computer Terms, 5th Ed.
Y	Webster's II New College Dictionary, 3rd Ed.

Z	Modern Dictionary of Electronics, 7th Ed.
AA	U.S. Patent No. 8,181
BB	U.S. Patent No. 8,201,243
CC	U.S. Patent No. 8,719,932
DD	U.S. Patent No. 8,763,123
EE	U.S. Patent No. 8,856,505
FF	U.S. Patent No. 11,409,869

Sophos Ex. 1008
Page 9 of 69

I. ’244, ’243 AND, ’932 PATENTS[1]

Though U.S. Patent No. 8,181,244 (“the ’244 patent”) was filed the same day as U.S. Patent No. 8,201,243 (“the ’243 patent”), the two patents are not related genealogically. U.S. Patent No. 8,719,932 (“the ’932 patent”) is a continuation of the ’243 patent. All three patents share the same specification.

The patents relate to methods and systems “for detecting, controlling and/or removing pestware.” Ex. CC (“’932 patent”) at 1:45-46. The specification explains that “trojans, spyware, and adware” programs “generally act to gather information about a person organization—often without the person or organization’s knowledge”—and defines “pestware” as “these programs that collect[] information about a person or an organization,” which the specification also refers to as “malware.” *Id.* at 1:50-55, 60-61. Pestware has evolved over time, and, thus, the patents note that “current techniques and software for removing pestware are not always satisfactory.” *Id.* at 1:64-65. The patents allege that techniques at the time of invention “use[d] definitions of known pestware to search for and remove files,” but such definitions were “often slow and cumbersome to create,” assuming the pestware could even be initially located in order to be defined. *Id.* at 2:3-7. The patents are therefore directed to analyzing activities on the monitored computers (as opposed to creating and applying definitions) and identifying the source of activities that are suspected of or related to pestware. *See, e.g.*, *id.* at 2:24-37.

[1] At least one or more Defendants seek construction or indefiniteness for each disputed term briefed herein, but each Defendant was permitted to identify only a limited number of terms. Where a Defendant has not requested construction or indefiniteness for a particular term, it does not mean that Defendant agrees with Plaintiffs’ position, their requested construction, or indefiniteness.

A. "pestware" ('244 patent, claims 1-4, 7, 9-12, and 15; '243 patent, 1, 3, 6, 8, and 12; '505 patent, claims 1, 2, 4, 6, 7, 9, 11, 12, 14, and 16-20; '932 patent, claims 1, 2, 5, 7, 12, and 13)

Plaintiffs	Trend Micro / Sophos
Plain and ordinary meaning	('244, '243, '932 patents) "a trojan, spyware, or adware program that collects information about a person or an organization" ('505 patent) "any program that collects and/or reports information about a person or an organization and any 'watcher processes' related to the pestware"

Acting as their own lexicographers, the patentees defined "pestware" as follows:

'244, '243, '932 patents	'505 patent
"Personal computers and business computers are continually attacked by ***trojans, spyware, and adware***, collectively referred to as 'malware,' 'spyware' or 'pestware.' ***These types of programs*** generally act to gather information about a person or organization—often without the person or organization's knowledge. Some pestware is highly malicious. Other pestware is non-malicious but may cause issues with privacy or system performance. And yet other pestware is actually beneficial or wanted by the user. Unless specified otherwise, ***'pestware' as used herein refers to any of these programs that collects information about a person or an organization***." Ex. BB ("'243 patent") at 1:43-54; Ex. AA ("'244 patents") at 1:43-54; Ex. CC ("'932 patent") at 1:50-61 (emphases added).	"Personal computers and business computers are continually attacked by trojans, spyware, and adware, collectively referred to as 'malware' or 'pestware.' These types of programs generally act to gather information about a person or organization—often without the person or organization's knowledge. Some pestware is highly malicious. Other pestware is non-malicious but may cause issues with privacy or system performance. And yet other pestware is actual beneficial or wanted by the user. Wanted pestware is sometimes not characterized as 'pestware' or 'spyware.' But, unless specified otherwise, ***'pestware' as used herein refers to any program that collects and/or reports information about a person or an organization and any 'watcher processes' related to the pestware***." Ex. EE ("'505 patent") at 1:32-45 (emphasis added).

The patentees' lexicography governs. *Kyocera Senco Indus. Tools Inc. v. Int'l Trade Comm'n*, 22 F.4th 1369, 1378-79 (Fed. Cir. 2022); *Lenovo Holding Co. v. DoDots Licensing Sols. LLC*, Nos. 2021-1247, 2021-1521, 2021-1580, 2021 WL 5822248, at *3-4 (Fed. Cir. Dec. 8, 2021). Defendants' proposed constructions adopt the patentees' lexicography, with a clarification that

"these programs" in the definition for the '243, '244, and '505 patents refer to the aforementioned trojans, spyware, and adware.

These definitional statements satisfy the standard that Plaintiffs have argued is required for lexicography. During claim construction on the first set of Plaintiffs' patents, Plaintiffs argued that "quotation marks" were required in order to establish a definition for "stack walk processing" for their '591 patent. Dkt. 98 at 60. Plaintiffs admitted that the '591 patent defined terms using a similar format as the "pestware" definitions. For example, Plaintiffs admitted that the '591 patent defined the word "low" using the phrase, "[t]he word 'low' refers to . . . ." Dkt. 147 at 35. Here, "pestware" is likewise set off in quotation marks, followed by a definition introduced with the phrase "as used herein refers to." Under Plaintiffs' own reasoning, the definitional statements for "pestware" display a clear expression of intent for the patentee to act as their own lexicographer. *See Meds Co. v. Mylan, Inc.*, 853 F.3d 1296, 1306 (Fed. Cir. 2017) (patentee defined terms when using "quotations marks, followed by the terms 'refers to' or 'as defined herein'"); Dkt. 147 at 35.

Accordingly, the term "pestware" should be construed pursuant to its express definitions in the specification.

B. "kernel-mode driver" ('244 patent, claims 1 and 9; '243 patent, claims 1, 6, and 12; '932 patent, claims 1 and 12)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	CrowdStrike disagrees with Plaintiffs' proposed constructions for the "kernel-mode" terms in CrowdStrike's Counterclaim patents. Dkt. 196. To the extent the Court construes those terms as proposed by Plaintiffs, CrowdStrike contends that a similar construction be applied to "kernel-mode driver." On that basis only, CrowdStrike proposes the following construction: "**driver operating in kernel-mode**." Should the Court agree with CrowdStrike that the "kernel-mode" terms in CrowdStrike's Counterclaim patents be afforded its plain and ordinary meaning, CrowdStrike will withdraw this construction.

CrowdStrike incorporates its arguments as to "kernel-level monitor" term below (*infra*

Section I.L) by reference here as they apply equally to this term.[2] Applying Plaintiffs' arguments against CrowdStrike's Counterclaim patents to this term (Dkt. 196 at 7-16; Dkt. 251 at 5-11) demonstrates that there is even more support for construing "kernel-mode driver" here to mean "driver operating in kernel-mode" than there is to limit the "kernel-level" and "kernel-mode" terms in CrowdStrike's Counterclaim patents. For example, the '932 patent discloses "a kernel-mode driver that may be loaded during a boot sequence for the protected computer," *i.e.*, ***before*** user mode is initiated. *See, e.g.*, '932 patent at 5:53-55. The claim language also requires that the "kernel-mode driver" monitor "API call activity," and the specification explains that "the API call utilized by the process is intercepted before it is carried out by an operating system of the protected computer." *Id.* at 5:55-61; *id.* at claim 1. In addition, according to Plaintiffs, the lack of disclosure of the same driver operating in user mode and the use of the term "kernel mode" itself precludes any operation in user mode. *See* Dkt. 196 at 9, 14. Therefore, to the extent the Court grants Plaintiffs' proposed construction of "kernel-mode" to mean operating in kernel mode when construing terms in CrowdStrike's Counterclaim patents, the Court should do the same here.

C. "suspicion of pestware" / "suspected of originating pestware" / "suspected pestware object" / "suspected pestware process" / "suspicious activity" / "suspected pestware" / "suspected pestware-related event" / "suspected to be pestware-related" ('244 patent, claims 1, 3, 4, 6, 9, 10, 11, and 12; '243 patent, claims 1, 3, and 12; '932 patent, claims 1, 2, 5, 12, and 13)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	Indefinite

These terms are indefinite because they are "facially subjective" terms whose language "provide[] little guidance." *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371, 1373 (Fed.

[2] Although the term "driver" is used for this claim term instead of "monitor," U.S. Pat. Pub. No. 2007/0094496 ("'496 Publication") discloses that the "kernel-level process monitor is a kernel-mode driver" and is incorporated by reference into these three asserted patents. Ex. C ('496 Publication) at claim 7.

Cir. 2014). Notably, the specification does not provide any disclosures that would allow a POSITA to determine the objective boundaries of "suspicion" with any reasonable certainty.

Although the claims across the three asserted patents are riddled with the use of these terms, the specification largely repeats these terms without providing any guidance as to when or how an object, process, event, or activity is suspicious or can be suspected of being pestware or related to pestware. *See, e.g.*, Ex. AA ("'244 patent") at 4:63-5:4 ("[T]he heuristics module 108 provides the user with information about ***suspect activity*** on the computer 100."), 9:14-19 ("[T]he activity log 120 and/or one or more of the N files 130 are accessed and analyzed to determine whether any activity during the time of interest is suspicious (e.g., ***the activity indicates in some way that it may be associated with pestware***).") (emphases added). The subjective nature of these terms is further confirmed by a 2002 dictionary that defined the terms "suspect" and "suspicion" as being predicated on "slight evidence or without proof"—in other words, the subjective opinions of a POSITA. Ex. D (Oxford American Dictionary – Third Edition) at CROWDSTRIKE-WEBROOT00034848-49.

The specification identifies examples of "suspicious activit[ies]" that fall within the scope of these terms, such as "pop-ups or a system crash" or where "access to the registry was carried out in connection with a downloaded file or the launch of a process." '244 patent at 8:61-63, 9:19-25. But citing to examples falling within the claim scope does not inform a POSITA what falls outside the claim scope (*i.e.*, the metes and bounds of these terms).[3] Indeed, for "facially subjective

[3] CrowdStrike's arguments here do not contradict its arguments for the terms "model" and "situational model" in the CrowdStrike Counterclaim patents (Dkt. 239 at 20-25) for several reasons: (1) those terms are terms of art and well understood by a POSITA (*id.* at 20-22); (2) Plaintiffs have not contended that those terms are facially subjective (*see id.* at 15-20); (3) Plaintiffs' main thrust for indefiniteness for those terms is based on the use of modal verbs ("may") and non-limiting language ("other") in the specification of the CrowdStrike Counterclaim patents describing those claim terms as boundless while ignoring the disclosure of immediately preceding

terms" such as these, providing examples does not satisfy the definiteness requirement. *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1260 (Fed. Cir. 2014); *Interval Licensing* , 766 F.3d at 1371-73 (Fed. Cir. 2014) (finding that a single example in the specification did not render the term definite because the example did not "provide a reasonably clear and exclusive definition, leaving the facially subjective claim language without an objective boundary"); *Prolifiq Software Inc. v. Veeva Sys. Inc.*, No. C 13–03644 SI, 2014 WL 3870016, at *6 (N.D. Cal. Aug. 6, 2014) (finding a term "aesthetically pleasing" as "subjective" and indefinite even though the patent "[p]rovid[ed] examples of things that are generally considered 'aesthetically pleasing'"). What may be suspicious to one POSITA may not be suspicious to another and would depend on the subjective opinions of a POSITA. Since the specification does not provide any bounds for these facially subjective terms, they are indefinite.

D. "time of interest includes a time interval" / "time of interest including a time interval" ('244 patent, claims 1 and 9)

Plaintiffs	Sophos
Plain and ordinary meaning	Indefinite

Claim 1 of the '244 patent recites in relevant part "receiving . . . a time of interest relating to a suspicion of pestware on the computer, ***wherein the time of interest includes a time interval***" ('244 patent at 10:14-17), and claim 9 recites in relevant part "a timestamp module . . . to generate ***a time of interest including a time interval*** in response to detected activity on the computer that is indicative of pestware[.]" *Id.*, 10:66-11:2 (emphases added). The ordinary meaning of a "time"—e.g., 8:01 am—is different and distinct from a "time interval"—e.g., between 9:00 am and 10:00 am. As such, the recited requirement that the "time of interest" include a "time interval"

examples (Dkt. 196 at 16-20; Dkt. 239 at 22-25; Dkt. 251 at 12-14); and (4) the examples in the specification of the CrowdStrike Counterclaim patents serve to provide further clarity as to the bounds of those terms of art. Dkt. 239 at 22-25.

has no discernable meaning based on the face of the claims. And the specification provides no clarity because it never uses the phrase "time interval." It is therefore unclear how a time of interest can include a time interval, and how, if at all, the "time interval" relates to that time of interest, meaning that scope of the "time interval" associated with the time of interest is unbounded.

For example, it is unclear if the "time of interest" needs to be within the "time interval" or if the time of interest needs to be at the beginning or end of the interval. It is likewise unclear how long the alleged "time interval" can be. For example, it is not clear if the entire time period for which the activity log is kept could qualify as such a "time interval," which would effectively read out the time interval out of the claims. The '244 patent provides no objective boundaries as to the length of time a time interval.

Because the claim language, read in light of the specification, "fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of the invention," the claims are indefinite. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014).

E. "externally networked [pestware research entity / source]" ('243 patent, claims 1, 2, 6, 12, and 13; '244 patent, claims 1 and 7-10; '932 patent, claims 1, 3, 5, 10, 12, and 14)

Plaintiffs	Trend Micro / Forcepoint
Plain and ordinary meaning	"networked [pestware research entity / source] that is external to the computer's internal network"

Defendants' proposal that "externally networked" means "networked . . . external to the computer's internal network" directly reflects the patentee's express statements during prosecution securing allowance of the claims.

The term "externally networked" was not recited in the originally filed claims of the '243

and ’244 patents.[4] *See* Ex. F (’243 FH, Original Claims), at 23-28; Ex. K (’244 FH, Original Claims), at 23-27. The term did not appear anywhere in these patents’ specifications either. Four years after the Applicants filed the ’243 and ’244 patent applications, the Applicants amended the claims to add the “externally networked” source limitation to overcome rejections of all claims based on the *Porras* prior art (U.S. Pat. Pub. No. 2004/0024864). *See* Ex. G (’243 FH, Aug. 20, 2010 Amendment and Response), at 3-7; Ex. L (’244 FH, Aug. 20, 2010 Amendment and Response), at 2-4, 6.

In the very same responses in which those amendments were made, the Applicants argued that prior art “Porras is interested **not in an externally networked source** . . . **but in the internal network’s** user or process session . . . .” Ex. G (’243 FH, Aug. 20, 2010 Amendment and Response), at 10 (emphasis added); *id*. at 10-11 (arguing that *Porras* does not disclose the “externally networked source” limitation because it “is interested only in activity in the **internal network**”) (emphasis added); Ex. L (’244 FH, Aug. 20, 2010 App. Amendment and Response), at 8. The Applicant additionally provided examples of “externally networked sources,” identifying “an internet URL or Web site”—none of which are within the computer’s internal network. Ex. G (’243 FH, Aug. 20, 2010 Amendment and Response), at 10; Ex. L (’244 FH, Aug. 20, 2010 Amendment and Response), at 8. These amendments and corresponding arguments overcame the then-existing rejections. *See* Ex. H (’243 FH, Nov. 10, 2010 Office Action), at 2; Ex. M (’244 FH, Sept. 10, 2010 Office Action), at 2-3.

One year later, the Applicants amended the claims again, this time, to recite an “externally networked” pestware research entity. *See* Ex. I (’243 FH, Nov. 9, 2011 Amendment and

[4] The ’932 patent, which is a continuation of the ’243 patent, was filed after the ’243 and ’244 patent claims were amended to recite “externally networked” and thus included the term in its original claims.

Response), at 2, 4-6; Ex. N ('244 FH, Sept. 28, 2011 Amendment and Response), at 9-10. In the '243 patent prosecution, the Applicants argued this amendment distinguished the claims from the *Wang* prior art (U.S. Pat. Pub. No. 2005/0268112), specifically, that the "eventlog described by *Wang* is **not an externally networked pestware research entity [because it] resides within the computer**." Ex. I ('243 FH, Nov. 9, 2011 Amendment and Response), at 9 (emphasis added); *id*. ("Nowhere does Wang describe the BHO reporting results to any entity external to the computer running the Gatekeeper engine."); Ex. S (Wang), at FIG. 3 (disclosing the event log 332 and BHO 328 within the computer system, and not reporting results to any entity external to the computer system). Similarly, in the '244 patent prosecution, the Applicants argued that the amended claim should be allowed over the *Porras* prior art that "requires a[n] internal analysis engine, [and therefore] it cannot disclose an 'externally networked pestware research engine.'" Ex. N ('244 FH, Sept. 28, 2011 Amendment and Response), at 18; Ex. T (Porras), at Fig. 1 (disclosing the analysis engine 107 internal to the Intrusion Detection System (IDS) system 100). After these amendments and arguments, the Examiner allowed the claims. *See* Ex. J ('243 FH, Feb. 9, 2012 Notice of Allowance), at 1, 6; Ex. O ('244 FH, Jan. 23, 2012 Notice of Allowance), at 1. The patentee's repeated statements during prosecution indicate "how the inventor understood the invention" (*Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (citations omitted)) and make clear that "externally networked" means "networked . . . external to the computer's internal network."

Separately, these statements also constitute prosecution disclaimer as they clearly and unmistakably demonstrate that "externally networked," as recited in the claims, cannot mean within the computer's internal network, but instead requires the source and pestware research entity be external to that internal network. *Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003). Having disclaimed any pestware source or research entity within the

pestware system's internal network, Plaintiffs cannot now recapture that scope, which the patentee repeatedly argued was beyond the reach of its claims to secure allowance of the claims. But that is precisely what Plaintiffs, with their plain and ordinary meaning construction, seek to do.

The term "externally networked [pestware research entity / source]" should therefore be construed as "networked [pestware research entity / source] that is external to the computer's internal network."

F. "a timestamp module . . ." ('244 patent claims 9 and 14)

Plaintiffs	Trend Micro
Plain and ordinary meaning	Subject to § 112 ¶ 6. **Functions**: (claim 9) to generate a time of interest including a time interval in response to detected activity on the computer that is indicative of pestware, to issue a timestamp after generating the time of interest, and to initiate, in response to the issuance of the timestamp, identification of indicia of pestware (claim 14) [in addition to claim 9 function,] generate the time of interest as a point in time **Structure**: Indefinite

As with "heuristics module" discussed below, "timestamp module" is another "module" term that does not connote structure and is thus subject to § 112 ¶ 6, and no corresponding structure is disclosed in the specification such that the term is indefinite.

This Term Invokes 35 U.S.C. § 112 ¶ 6. The Federal Circuit found that "'[m]odule' is a well-known nonce word that can operate as a substitute for 'means' in the context of § 112, para. 6." *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1350 (Fed. Cir. 2015). The term "timestamp" does not impart any structure into the term "module." Rather, the '244 patent describes a "time stamp" as nothing more than a time reference, which is not structure. '244 patent at 5:12-15. ("[T]he heuristics module 110 also prompts the time stamp module 112 to send a time stamp 112

to the research module 108 so that the research module 108 is provided with a time reference as well as information about the pestware activities."); Ex. U (Almeroth Decl.) ¶ 71. Even when the two words are combined, the term "timestamp module" does not connote structure. Ex. U ¶¶ 70-71.

The '244 patent likewise describes the "timestamp module" as a black box labeled "Time Stamp" in Figure 1, which is described as "depict[ing] functional capabilities" rather than structure. '244 patent at 2:53-61, 5:57-59, FIG. 1. Rather than describing the structure of the "timestamp module," the patent states only that it "can be implemented in software or hardware" as with other generic "modules." '244 patent at 2:62-63, 5:59-63; Ex. U ¶ 72. These modules are not limited to specific structure, but could be implemented separately or "consolidated into a single module." *Id*. at 5:59-63. And even the functional name "timestamp module" does not describe all of the claimed functions, which are not limited to issuing a timestamp, but also include identifying a time of interest of pestware activity and initiating identification of indicia of pestware. Since "timestamp module" does not connote definite structure, it is subject to § 112 ¶ 6.

No Sufficient Structure is Disclosed. Since "timestamp module" is subject to § 112 ¶ 6, the specification must disclose structure corresponding to the claimed functions. *Williamson*, 792 F.3d at 1351-52; *Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech.*, 521 F.3d 1328, 1333 (Fed. Cir. 2008) (structure for computer-implemented invention is an algorithm). The '244 patent does not disclose any structure for performing the claimed functions. Ex. U ¶¶ 74-80. For example, the patent never explains how a "timestamp module" generates a time of interest in response to detected activity on the computer that is indicative of pestware. At best, the patent only says that a ***user*** may establish the time of interest based upon events the user observed, but does not explain how the timestamp module may generate the time of interest. '244 patent at 8:61-63. Thus, the

term "timestamp module" is indefinite.

G. "potential pestware activity" ('244 patent, claims 9, 10, and 15)

Plaintiffs	Trend Micro
Plain and ordinary meaning	Indefinite

Plaintiffs are taking the position that the term "potentially malicious script" in Trend Micro's '992 patent is indefinite, which is inconsistent with their position on their own patents that the term "potential pestware activity" is not indefinite. Plaintiffs cannot have it both ways. To the extent the Court finds the "potentially malicious script" term indefinite—it should not for the reasons set forth in Trend Micro's briefing on the counterclaim patents—the term "potential pestware activity" must also be found indefinite.

Plaintiffs argue that "potentially malicious script" is indefinite because "whether a script is potentially malicious is dependent on context." Dkt. 194 at 21; Dkt. 194-1 ¶¶ 37-42. As support, Plaintiffs present various made-up scenarios of scripts that, in one context, are viewed as "normal scripts," whereas in another context, could be considered "potentially malicious." Dkt. 194 at 22. For example, Plaintiffs contend that a script that reads a keyboard buffer to monitor a user's keystrokes could be considered a normal script in some contexts—*i.e.*, where used to create audio playback for the vision impaired—or as a potentially malicious script in another context—*i.e.*, where used to steal a user's password. *Id*. at 17.

That same logic applies here to "potential pestware activity." Plaintiffs' patents explain that "[s]ome pestware is highly malicious," "[o]ther pestware is non-malicious," and "yet other pestware is actually beneficial or wanted by the user." '244 patent at 1:48-51. But while beneficial pestware is still considered pestware ***some*** of the time, the patents explain that "[w]anted pestware is sometimes not characterized as 'pestware.'" '505 patent at 1:39-41. By the logic of Plaintiffs' own expert, a POSITA would not be able to tell whether activity constitutes potential pestware

activity since it is context-dependent. Using one of Plaintiffs' contrived examples, reading a keyboard buffer may constitute normal activity in some contexts—*e.g.*, where used to create audio playback for the visually impaired—but may constitute potential pestware activity in other contexts—*e.g.*, where used to steal a user's password. And even worse, according to the patent, even the beneficial use of the keyboard buffer for the visually impaired may still be considered potential pestware activity. '505 patent at 1:39-41 ("And yet other pestware is actually beneficial or wanted by the user. Wanted pestware is ***sometimes*** not characterized as 'pestware' or 'spyware.'") (emphasis added). Thus, by Plaintiffs' own logic, "potential pestware activity" is indefinite because it is context-dependent.

Plaintiffs also argue that the term "potentially malicious script" in Trend Micro's patent is indefinite because other than "four example attributes, the '992 patent provides no guidance as to how a script can be identified as a 'potentially malicious script.'" Dkt. 194 at 24; Dkt. 194-1 ¶ 43. Here, the '244 patent does not provide ***any*** example attributes for identifying "potential pestware activity." The term "potential pestware activity" (and "potential pestware-related activity") is used only twice in the patent where the patent simply states what happens if such activity is detected and that such activity may be identified by the heuristics module, without explaining how one can determine whether activity is "potential pestware activity." '244 patent at 8:11-22. The patent only explains that the heuristics module may compare activities with factors that are weighted by the likelihood that the activity is associated with pestware, but does not state what those factors are or provide any examples of such factors or how it is determined that they are associated with actual pestware activity, let alone "potential pestware activity." *Id.* at 4:45-50.

Thus, to the extent the Court finds the term "potentially malicious script" in Trend Micro's '992 patent indefinite, the term "potential pestware activity" must also be found indefinite.

H. "a heuristics module" ('244 patent claims 11 and 12; '243 patent claims 6 and 8; '932 patent claims 5 and 7)

Plaintiffs	Trend Micro / Forcepoint
Plain and ordinary meaning	Subject to § 112 ¶ 6. **Functions**: ('244 patent, claim 11) evaluate whether the event is a suspected pestware-related event before the research portion accesses information in at least one log that relates the event to the suspected pestware object ('243 patent, claim 6) to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold ('932 patent, claim 5) analyze the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold Additional functions recited in dependent claims **Structure**: Indefinite

The term "heuristics module" is a nonce term that does not connote definite structure. The term is thus subject to § 112 ¶ 6. Since the patent does not disclose any corresponding structure, the term is indefinite. Indeed, the term "heuristics module" is no different from the "heuristic engine" term this Court found to be a means-plus-function term and indefinite.[5] *Audioeye, Inc. v. AccessiBe Ltd.*, No. 6:20-cv-00997-ADA, Dkt. 69 at 6.

This Term Invokes 35 U.S.C. § 112, ¶ 6. The Federal Circuit has found that "'[m]odule' is a well-known nonce word that can operate as a substitute for 'means' in the context of § 112, para. 6." *Williamson*, 792 F.3d at 1350. The term "heuristic" is similarly a nonce term that does not impart any structure into the term "module." Rather, the term "heuristic" covers an ill-defined

[5] The Court found the term was not a means-plus-function term in claims that did not recite any function. *AudioEye*, Dkt. 69 at 6 and Dkt. 36 at 30-31. Here, each of the claims at issue recites a function for the "heuristics module."

array of approaches to problem solving and does not connote any particular structure. Ex. V (American Heritage Dictionary) at 825-26 ("Relating to or using a problem-solving technique in which the most appropriate solution of several found by alternative methods is selected at successive stages of a program for use in the next step of the program"); *see also* Ex. W (IEEE dictionary) at 513 (additional definition showing "heuristic" generically refers to problem solving and does not connote structure); Ex. X (Webster's New World Dictionary) at 271 (same); Ex. Y (Webster's II New College Dictionary) at 532 (same); Ex. U (Almeroth Decl.) ¶ 57. Even when the two words are combined, the term "heuristics module" does not connote structure. Ex. U ¶¶ 56-57.

The patents describe the "heuristics module" as a black box labeled "Heuristics" in Figure 1, which is described as "depict[ing] functional capabilities" rather than structure. Ex. BB ("'243 patent") 2:53-61, 5:57-59, FIG. 1; Ex. U ¶ 58. Instead of describing the structure of the "heuristics module," the patents state only that it "can be implemented in software or hardware" like the other generic "modules." '243 patent at 2:62-63; *see also id*. at 5:59-63 ("[T]he functions described with reference to FIG. 1 may be realized by various implementations of software in connection with hardware or hardware alone."). These functional modules are not limited to any particular structure but could be implemented separately or "consolidated into a single module." *Id*. at 5:59-63. Since "heuristics module" does not connote definite structure, it is subject to § 112 ¶ 6.

No Sufficient Structure is Disclosed. Where a term is subject to § 112 ¶ 6, as here, the specification must disclose structure corresponding to each of the claimed functions. *Williamson*, 792 F.3d at 1351-52. For a computer-implemented invention, the structure is an algorithm. *Aristocrat*, 521 F.3d at 1333. The patents do not disclose any structure for performing the claimed functions. Ex. U ¶¶ 60-68. For the '243 patent, the patent only restates the claimed function of

identifying and analyzing activity to determine whether weighted factors associated with the activity exceed a threshold, but does not explain how the "heuristics module" obtains the weighted factors, how it determines whether those factors are associated with the activity, or how the threshold is determined for comparison. '243 patent at 4:45-55. As to the '932 patent, the patent never even describes the "heuristics module" as analyzing API call activity, let alone disclosing an algorithm or other structure for performing such analysis to determine whether weighted factors associated with such activity exceeds a threshold. As to the '244 patent, the patent does not disclose an algorithm or other structure for evaluating whether an event is a suspected pestware-related event. Thus, the term "heuristics module" is indefinite.

I. "identify[ing] . . . access[ing] . . . report[ing] . . ." ('243 claims 1, 6, and 12)

Plaintiffs	Forcepoint / Sophos
Plain and ordinary meaning	Order of steps: "identify[ing]," "access[ing]," and "report[ing]" must occur in order

All of the asserted claims of the '243 patent require (1) "monitoring . . . [a] computer for activity," (2) "analyzing . . . computer activity" to determine that the activity is indicative of pestware," (3) "identifying, based upon the activity, an object" that is a suspected pestware object," (4) "accessing, in response to the identifying an object," a recorded history to identify a reference to a particular externally networked source," and (5) "reporting the identity of the particular externally networked source." '243 patent, claims 1 and 12; *see also id.*, claim 6. Although claims are ordinarily presumed to not require an order, claims are construed to require an order where, as here, the language of the claims mandates that the steps are performed in a particular order—for example, because later-recited steps depend on the results of previous steps. *See, e.g.*, *Wi-LAN, Inc. v. Apple, Inc.*, 811 F.3d 455, 460 (Fed. Cir. 2016).

Here, the claims require some of the recited steps to be performed in order, because certain steps rely upon input from the previous steps. For example, claim 1 of the '243 patent recites:

> **[1PRE]** A method for identifying an origin of activity on a computer that is indicative of pestware comprising:
>
> [1A] monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log;
>
> [1B] analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;
>
> **[1C]** ***identifying,*** based upon the activity, ***an object*** residing on the computer that is a suspected pestware object;
>
> **[1D]** ***accessing, in response to the identifying an object,*** at least a portion of a recorded history of externally networked sources that the computer received files from ***so as to identify a reference to an identity of a particular externally networked source*** that the suspected pestware object originated from; and
>
> **[1E]** ***reporting the identity of the particular externally networked source to an externally networked pestware research entity*** so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.

(emphases added).

As set forth above, claim 1 describes a method for identifying an origin of activity on a computer that is indicative of pestware. In the identifying step [1C], the method identifies an object residing on the computer that is a so-called suspected pestware object. In response to identifying the object, the accessing step [1D] then further identifies a reference to a particular externally networked source that the object originated from. Finally, the reporting step [1E] then reports the identity of that particular externally networked source to a research entity. In sum, based on the

unambiguous claim language, [1C], [1D], and [1E] must occur in order, because [1E] needs the identity of the particular externally networked source from [1D], and [1D] is performed "in response to" [1C].

In addition to the unequivocal language of the claims, which is dispositive, every embodiment discussed in the specification requires this order. *See Mformation Techs., Inc. v. Rsch. in Motion Ltd.*, 764 F.3d 1392, 1400 (Fed. Cir. 2014) (noting order of steps "is consistent with the sole embodiment in the specification"). For example, the patent describes this order in connection with Figures 3 through 5. Each figure begins with the step of monitoring the computer for activity indicative of pestware. *See* '243 patent Fig. 3 (Block 302); Fig. 4 (Block 402); Fig. 5 (Block 502); 7:27–29, 8:11–12, 8:59–61. After that, based on the activity, a suspected pestware object on the computer is identified. *See* Fig. 4 (Block 404); Fig. 5 (Block 504, 506); 7:29–35, 8:13–16, 9:37–44. Then, recorded information is accessed to identify the source of the previously identified pestware object. *See* Fig. 3 (Blocks 304, 306, 308); Fig. 4 (Blocks 406, 408); Fig. 5 (Blocks 508, 510); 7:36–40, 8:23–26, 9:45–50. Only after the source of the pestware object is identified is the source then reported (e.g., to a research entity). *See* Fig. 3 (Block 310); Fig. 4 (Block 410); Fig. 5 (Block 512); 7:61–63, 8:32–35, 9:50–52.

Furthermore, computer-readable medium (CRM) and system claims can have an order of steps when they are similar to the method claim. *See Avago Techs. Gen. IP (Singapore) Pte Ltd. v. Asustek Computer, Inc.*, No. 15-CV-04525-EMC, 2016 WL 3029674, at *12 (N.D. Cal. May 27, 2016) (noting case law supporting, and absence of any case law refuting, that "order can be required by a system/apparatus claim"); *Maxim Integrated Prod., Inc. v. Silicon Mitus Tech., Inc.*, No. 17-CV-03507 NC, 2018 WL 4657384, at *9 (N.D. Cal. July 3, 2018) (collecting cases); *Versata Software, Inc. v. SAP Am., Inc.*, No. 2:07-CV-153, 2009 WL 1408520, at *13 (E.D. Tex.

May 19, 2009) (construing claim 23—a claim for "[a] program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method"—to "require the limitations to be performed in the order recited"); *Visto Corp. v. Good Tech., Inc.*, No. 2:06-CV-039, 2008 WL 163576, at *6 (E.D. Tex. Jan. 16, 2008) (construing claim 22—a computer-readable storage medium claim—to require certain recited steps to be performed in order). Here, CRM claim 12 and system claim 6 of the '243 patent contain virtually identical limitations as method claim 1, including the same referential language back to the prior steps:

Claim 1 and 12	Claim 6
monitoring, [using/with] a kernel-mode driver, the computer for activity that is indicative of pestware . . .	[an activity monitor configured to] monitor API calls and to store a history of at least a portion of the API calls in an activity log . . .
analyzing, heuristically, computer activity . . . so as to arrive at a determination that the activity is indicative of pestware; ***identifying,*** based upon the activity, ***an object residing on the computer that is a suspected pestware object;***	*[a heuristics module configured to]* ***identify an activity on the computer that is indicative of pestware residing on the computer*** and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold . . .
accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from ***so as to identify*** a reference to ***an identity of a particular externally networked source*** that the suspected pestware object originated from; and	[a research portion configured to] ***access, in response to a prompt from the heuristics module,*** . . . ***recorded information*** on the computer that relates the at least one file to an externally networked source from which the file was received; and generate a report that ***identifies the externally networked source of the file***
reporting the identity of the particular externally networked source to an externally networked pestware research entity . . .	[a reporting portion configured to] ***report an identity of the externally networked source to an externally networked pestware research entity*** . . .

(emphases added).

For the reasons above, all claims of the '243 patent should be construed such that ***"identifying"*** a suspected pestware object, ***"accessing"*** a recorded history to identify a particular

externally networked source, and then ***"reporting"*** the identity of that externally networked source must be performed in order.

J. "monitor[ing] . . . stor[ing] . . . analyz[ing] . . . identify[ing] [a suspected pestware object] . . . identi[fying] [an externally networked source] . . . report[ing] . . ." ('932 claims 1, 5, 12)

Plaintiffs	CrowdStrike / Forcepoint / Sophos
Plain and ordinary meaning	Order of steps: (a) "monitoring" comes before "storing," "analyzing," and "identifying" [a suspected pestware object]; and then (b) "identify[ing]" [a suspected pestware object], "identi[fying]" [an externally networked source], and "report[ing]" must occur in order

All of the asserted claims of the '932 patent require (1) "monitoring . . . API call activity on [a] computer," (2) "storing information related to the API call activity," (3) "analyzing . . . the API call activity," (4) "identifying, based upon the API call activity, a suspected pestware object," (5) "identifying, in response to the identifying the suspected pestware object," an externally networked source, and (6) "reporting the identity of the externally networked source." '932 patent, claims 1 and 12; *see also id.*, claim 5.

Here, certain steps must be performed in order because they rely upon input from previous steps. *See, e.g.*, *Wi-LAN*, 811 F.3d at 460. For example, claim 1 of the '932 patent recites:

> **[1PRE]** A method for identifying an origin of activity on a computer that is indicative of pestware comprising:
>
> **[1A]** ***monitoring***, using a kernel-mode driver, ***API call activity*** on the computer;
>
> **[1B]** ***storing*** information related to ***the API call activity*** in a log;
>
> **[1C]** ***analyzing***, heuristically, ***the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;***
>
> **[1D]** ***identifying,*** based upon ***the API call activity***, ***a suspected pestware object*** on the computer;

[1E] ***identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source*** of the suspected pestware object; and

[1F] ***reporting the identity of the externally networked source to an externally networked pestware research entity,*** wherein the identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client and a program.

(emphases added).

As set forth above, the monitoring step [1A] recites monitoring the computer for API call activity, and the storing step [1B], analyzing step [1C] and first identifying step [1D] each use that monitored API call activity (i.e., "***the*** API call activity") to store information in a log, determine whether the activity is indicative of pestware, and identify a suspected pestware object on the computer. In response to identifying the object, the second identifying step [1E] then further identifies a reference to an externally networked source of the previously identified computer object. Finally, the reporting step [1F] then reports the identity of that externally networked source to a research entity. In sum, based on the unambiguous claim language, [1B], [1C], and [1D] must occur after [1A], because [1B], [1C], and [1D] each act on ***the*** API call activity monitored from [1A]. Indeed, ***the*** API call activity cannot be stored or analyzed until after it is monitored in [1A], and the identifying in [1D] is specifically performed "based upon" ***the*** API call activity monitored in [1A]. Similarly, [1D], [1E], and [1F] must occur in order, because [1F] needs the identity of the externally networked source from [1E], and [1E] is performed "in response to" [1D].

Although the unequivocal language of the claims is dispositive, like the '243 patent, every embodiment discussed in the specification requires this order. *See Mformation*, 764 F.3d at 1400. Specifically, the '932 patent explains that the monitoring of "a series of particular API calls [] made in a pattern known to be associated with pestware" can trigger this process (i.e., the monitoring step comes first). '932 patent, 8:50–52. After such API calls are detected, the process

making the calls (and its associated file) are identified. *Id.*, 8:51–56. "In turn," a source of the file is identified. *Id.*, 8:54–57. In all embodiments, only after the source of the pestware is identified is the source then reported (e.g., to a research entity). *See, e.g.*, 7:61–63, 8:32–35, 9:50–52.

Furthermore, as previously explained (*see supra* p. 18-19), CRM and system claims can have an order of steps when they are similar to the method claim. Here, CRM claim 12 contains identical limitations, and system claim 5 contains virtually identical limitations, to method claim 1—including the same referential language back to the prior steps:

Claims 1 and 12	Claim 5
monitoring, using a kernel-mode driver, ***API call activity*** on the computer; ***storing*** information related to ***the API call activity*** in a log;	[a kernel-level monitor configured to] ***monitor API call activity*** on the computer and to ***store*** information related to ***the API call activity*** in a log;
analyzing, heuristically, ***the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;***	[a heuristics module configured to] ***analyze the API call activity to determine whether one or more weighted factors associated with the API call activity exceeds a threshold;***
identifying, based upon ***the API call activity***, ***a suspected pestware object*** on the computer;	[a research portion configured to] ***identify, in response to a prompt from the heuristics module, a suspected pestware object*** on the computer; and
identifying, in response to the identifying the suspected pestware object, a reference to an identity of an externally networked source of the suspected pestware object; and	[a reporting portion configured to] generate a report including a reference to an ***identity of an externally networked source of the suspected pestware object***
reporting the identity of the externally networked source to an externally networked pestware research entity . . .	and to ***report the identity of the externally networked source to an externally networked pestware research entity*** . . .

(emphases added).

For the reasons above, all claims of the '932 patent should be construed such that (a) ***"monitoring"*** for API call activity comes before ***"storing"*** and ***"analyzing"*** that activity, and before ***"identifying"*** a suspected pestware object "based upon" that activity; and such that

(b) ***"identifying"*** a suspected pestware object, ***"identifying"*** an externally networked source, and then ***"reporting"*** the identity of that externally networked source must be performed in order.

K. "identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client, and a program" ('932 patent, claims 1, 9, and 12).

Plaintiffs	Kaspersky
Plain and ordinary meaning	The identity of the externally networked source is selected from a closed group of specified alternatives, that is, either an I.P. address, or a URL, or an email client, or a program, and nothing else

Plaintiffs unequivocally claimed a "Markush Group" when they drafted this claim limitation. A Markush Group is a well-known claim drafting convention, typically expressed as "a member selected from the group consisting of A, B, and C," approved by the USPTO to serve a particular purpose when used by a patentee: to limit the claim to one of a list of specified alternatives. *Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1357 (Fed. Cir. 2016); *Abbott Labs. v. Andrx Pharms., Inc.*, 473 F.3d 1196, 1210 (Fed. Cir. 2007). Such a claim limitation is also referred to as "closed-ended," signifying restriction or exclusion, as opposed to "open ended" limitations using the transitional term "comprising." *Multilayer*, 831 F.3d at 1358; *see also Vehicular Techs. Corp. v. Titan Wheel Int'l, Inc.*, 212 F.3d 1377, 1382-83 (Fed. Cir. 2000). If by asserting "plain and ordinary meaning," Plaintiffs seek no construction, that is legal error. *Abbott Labs. v. Baxter Pharm. Prod., Inc.*, 334 F.3d 1274, 1280-81 (Fed. Cir. 2003). The "plain meaning" of a Markush Group limits Plaintiffs to a single source selected from the group. *Id.*

"Consisting of" creates two presumptions when recited in a Markush Group: (1) a presumption that group members cannot be combined and (2) an "exceptionally strong presumption" that the group excludes unrecited members. *See Multilayer*, 831 F.3d at 1358, 1363. "Consisting of" is a patent law term of art with a well-established meaning. *Id*. at 1358. It limits a

Markush Group to "one and only one" of the identified members, even when indefinite articles are used (e.g., "an I.P. address" or "a URL"). *Id*. at 1363 (citing *Abbott*, 334 F.3d at 1281). It also creates a "very strong presumption" that the group excludes any members not specified in the claim, which can be overcome only if the specification and prosecution history unmistakably manifest another meaning. *Shire Dev., LLC v. Watson Pharms., Inc.*, 848 F.3d 981, 984 (Fed. Cir. 2017).

Plaintiffs cannot overcome either presumption. Plaintiffs invoked the Markush Group language: "identity of the externally networked source ***is selected from a group consisting of*** an I.P. address, a URL, an email client, and a program." ('932 patent, claims 1, 9, 12.) (emphasis added). Neither the specification nor the prosecution history unmistakably manifests another meaning nor an intent to claim this limitation in an open-ended manner. "[S]elected from a group consisting of" and "consisting of" only appear in the claims; the written description does not recite either phrase, much less "unmistakably" redefine them.

L. "kernel-level monitor" ('932 patent, claims 5, 7, and 8; '505 patent, claim 16)[6]

Plaintiffs	CrowdStrike
Plain and ordinary meaning	CrowdStrike disagrees with Plaintiffs' proposed constructions for the "kernel-level" terms in CrowdStrike's Counterclaim patents. Dkt. 196. To the extent the Court construes those terms as proposed by Plaintiffs, CrowdStrike contends that a similar construction be applied to "kernel-level monitor." On that basis only, CrowdStrike proposes the following construction: **"monitor operating in kernel-mode."** Should the Court agree with CrowdStrike that the "kernel-level" terms in CrowdStrike's Counterclaim patents be afforded its plain and ordinary meaning, CrowdStrike will withdraw this construction.

Should the Court agree with Plaintiffs that the similar "kernel-level" terms in CrowdStrike's Counterclaim patents are limited to operating in kernel-mode, then CrowdStrike

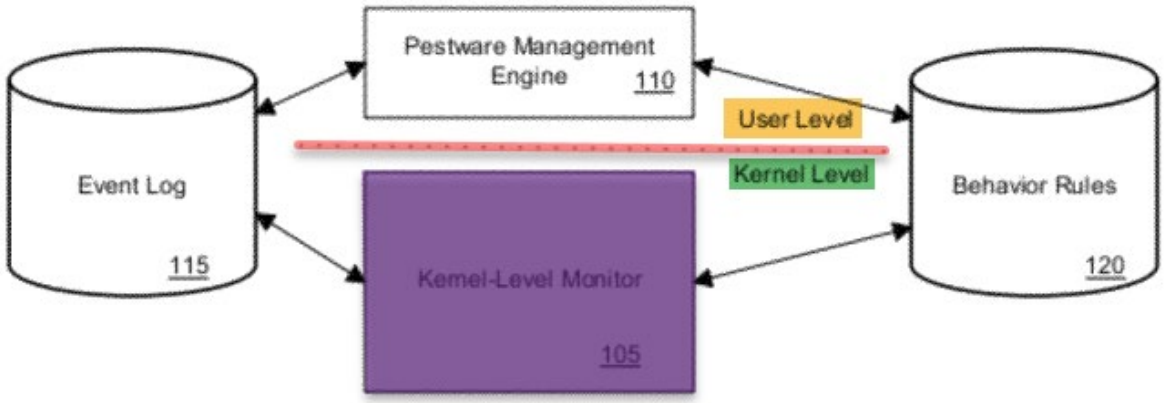
[6] U.S. Patent No. 8,856,505 ("the '505 patent") is further described below in Section III.

contends that, under Plaintiffs' arguments, the "kernel-level" terms in Plaintiffs' '932 and '505 patents must also be limited to operating in kernel-mode. Dkt. 196 at 7-10, 13-16; Dkt. 251 at 5-8, 9-11. CrowdStrike contends that the similar "kernel-level" terms in CrowdStrike's Counterclaim patents be afforded plain and ordinary meaning and opposes Plaintiffs' proposed constructions, which diverge significantly from the plain and ordinary meaning of those terms in the context of that intrinsic evidence. Dkt. 239 at 7-12, 13-16. CrowdStrike objected to Plaintiffs' proposed constructions on a number of grounds, including improperly reading limitations into the claims while reading out certain embodiments and violating canons of claim differentiation.[7] *See id*.

CrowdStrike's proposed constructions here carry a stronger level of intrinsic support than Plaintiffs' proposed constructions on CrowdStrike's Counterclaim patents. The '932 and '505 patents both describe the "kernel-level monitor" as being initiated during the boot process of the computer, *i.e.*, before user mode is initialized, to protect shared resources, such as the operating system, from unauthorized actions or access. '932 patent at 5:53-67 ("[T]he activity monitor 116 is realized by a kernel-mode driver that ***may be loaded during a boot sequence***[8] for the protected computer . . . ."), 5:45-52 ("[T]he activity monitor 116 may inject code" which can "raise a flag if the existing process is attempting to create a new pestware process or attempting to alter one or more settings (e.g., ***a registry setting***) of the protected computer 100."); '505 patent at 4:32-36 (describing that the kernel-level monitor may "be initialized first, before any boot drivers are initiated"), 3:32-38 ("The kernel-level monitor 105 additionally uses several techniques that allow it to intercept and monitor various operating system behaviors . . ."), 4:53-62 ("During the time

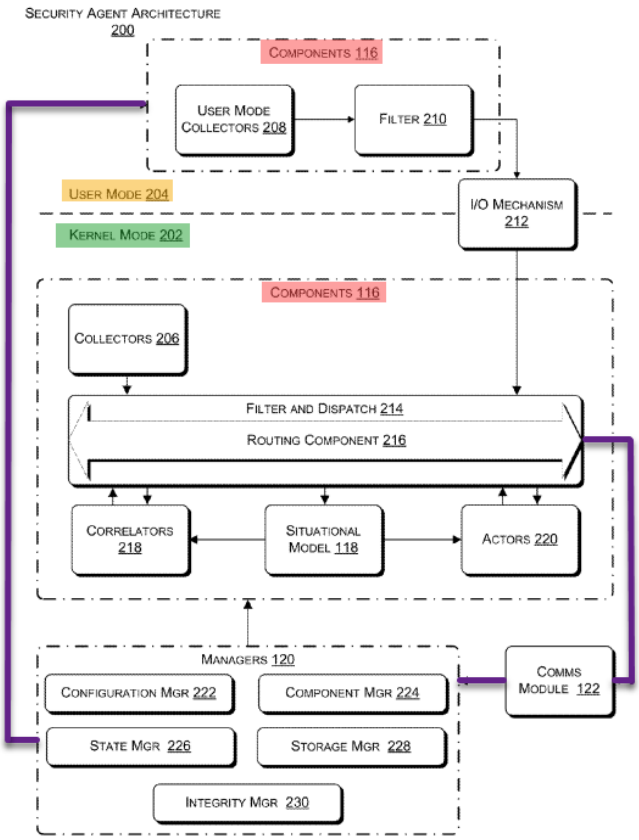
[7] Plaintiffs raise several new arguments against the "kernel-level" terms in their Reply (*see* Dkt. 251 at 5-8, 9-11), including changing their proposed construction to one such term, which CrowdStrike addresses in its Sur-Reply filed concurrently with this briefing.
[8] All emphasis herein are added by Defendants unless otherwise noted.

when the kernel-level monitor 105 is loaded and initialized, ***driver hooks and monitoring mechanisms that are utilized by the kernel-level monitor 105 are placed into the operating system kernel***."); 5:5-12 ("[I]f a detected event is marked for denial or deletion in the behavior rules, the kernel-level monitor 105 either prevents the operating system from receiving the request ***or it forces the operating system to reject the request***."). Figure 1 in the '505 patent explicitly shows that "**kernel-level monitor**" operates entirely within the "**Kernel Level**" and that there are no components of the "**kernel-level monitor**" in the "**User Level**":



'505 patent, Fig. 1.

The specification support in the '932 and '505 patents is stronger evidence that the "kernel-level" terms in those patents operate in "kernel-mode" compared to the evidence Plaintiffs rely upon in their briefing on CrowdStrike's Counterclaim patents. *See* Dkt. 196 at 7-10, 13-16; Dkt. 251 at 5-8, 9-11. Figure 2 and other disclosures throughout the specification and claims of the CrowdStrike Counterclaim patents demonstrate that the "kernel-level" terms in CrowdStrike's Counterclaim patents operate in ***both*** the "kernel-level" and the "user-level":



’903 patent, Fig 2 (illustrated to show that **components 116** of the “kernel-level security agent” are in both user mode and kernel mode); Dkt. 239 at 10. As evidenced in the disclosures above, that is not the case for the ’932 and ’505 patents—there is no disclosure in the ’932 or ’505 patents that suggests that the “monitor” can operate at the user-level or include user-mode components. *Id.* at 9-10, 14-15.

Plaintiffs also argued with respect to the CrowdStrike Counterclaim patents that the use of the term “kernel-level” itself “forecloses the [] module operating in user mode.” Dkt. 196 at 9. While CrowdStrike disagrees with this argument with respect to the “kernel-level” terms in the CrowdStrike Counterclaim patents (Dkt. 239 at 13-16), if the Court finds Plaintiffs’ argument persuasive, the same argument applies here with even more force. Accordingly, should the Court agree with Plaintiffs on their construction of the “kernel-level” terms in CrowdStrike’s

Counterclaim patents, it should apply those same constructions here as to Plaintiffs' patents.

M. "a research portion configured . . ." ('244 patent, claim 9; '243 patent, claim 6; '932 patent, claim 5)

Plaintiffs	Sophos/Trend Micro/Forcepoint/Kaspersky
Plain and ordinary meaning	Subject to § 112 ¶ 6 **Functions:** ('244 patent, claim 9) to be executed by the hardware processor and to access at least one log on a file storage device of the computer to relate the time of interest to at least one externally networked source of potential pestware activity on the computer ('243 patent, claim 6) a research portion configured to access, in response to a prompt from the heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received ('932 patent, claim 5) to identify, in response to a prompt from the heuristics module, a suspected pestware object on the computer **Structure:** Indefinite; no corresponding structure

As supported by the expert witness declaration of V.S. Subrahmanian, Ph.D., "research portion" is not a term of art. Ex. A, ¶28. It does not appear in technical dictionaries or learned treatises. Ex. A, ¶¶22-24. The term is not used in the publications cited on the face of the three patents. *Id.*, ¶26; Ex. B. A database search of patents and patent applications using the Cooperative patent Classification, which is jointly managed by the European and U.S. Patent Offices, revealed use of the term in only a single patent application (other than patents owned by Plaintiffs). Ex. A, ¶25; Ex. B. In that application, "research portion" referred not to cybersecurity but to steps taken by a real estate agent to prepare an information disclosure relating to characteristics of a parcel of real property. Ex. A, ¶25; Ex. B. Dr. Subrahmanian opined that he has never encountered the term "research portion" in the context of cybersecurity and malware detection and that the term is not

understood as a name for a structure or a class of structures. Ex. A, ¶¶19-21, 27-28, 31-33, 36-38. Rather, "research portion" is a coined term.

None of the claims identify any input, output, connection, or describe operation of the "research portion" to explain how its recited functions are achieved in the context of the invention. *See Apple Inc. v. Motorola, Inc*., 757 F.3d 1286, 1299 (Fed. Cir. 2014), overruled on other grounds by Williamson v. Citrix Online, 792 F.3d 1339 (Fed. Cir. 2015) (finding recited "finger contact" to be an input connoting structure for disputed term). Unlike *Apple*, here the claims that recite a "research portion" provide nothing recognized as structure. Ex. A, ¶¶27-28, 33, 38. Rather, "research portion" is recited in purely functional language. As shown by the scarcity of its use, the term has not "achieved recognition as a noun denoting structure." *Lighting World, Inc. v. Birchwood Lighting, Inc*., 382 F.3d 1354, 1360 (Fed. Cir. 2004), overruled on other grounds by Williamson v. Citrix Online, 792 F.3d 1339 (Fed. Cir. 2015).

Despite the absence of "means" in the claims, the presumption that 35 U.S.C. § 112 ¶ 6 does not apply is overcome because the term "research portion" is not used or defined in the specification, lacks a dictionary definition, and does not connote structure to a POSITA. *See MonkeyMedia, Inc. v. Apple, Inc*., Nos. A-10-CA-319-SS, A-10-CA-533-SS, 2013 WL 12076550 (W.D. Tex. Feb. 22, 2013). Because there is no evidence that "research portion" is a known or conventional structure, the presumption cannot endure. *Cf*., *Dyfan, LLC v. Target Corp*., 28 F.4th 1360, 1369 (Fed. Cir. 2022) (finding presumption not overcome given unrebutted testimony that a POSITA understood functions of disputed term could be performed by "conventional off-the-shelf software"). Rather, the intrinsic and extrinsic evidence demonstrate that a POSITA would have been unfamiliar with the term altogether. There is no evidence to support a conclusion that a

POSITA would have understood the claim term to have a "sufficiently definite meaning as the name for structure." *Williamson*, 792 F.3d at 1349.

Because "research portion" is written in means-plus-function format, the specification must disclose corresponding structure to perform the recited functions. *Noah Sys., Inc. v. Intuit, Inc.*, 675 F.3d 1302, 1312 (Fed. Cir. 2012). But the specifications of the '244 patent, '243 patent, and '932 patent disclose no structure. The lack of structure renders the term indefinite because the patents fail to inform, with reasonable certainty, a POSITA as to the scope of the invention. *Nautilus*, 572 U.S. at 901.

N. "a reporting portion configured . . ." ('244 patent, claim 9; '243 patent, claim 6; '932 patent, claim 5)

Plaintiffs	Trend Micro/Forcepoint/Kaspersky
Plain and ordinary meaning	Subject to § 112 ¶ 6 **Functions:** ('244 patent, claim 9) to be executed by the hardware processor and to generate a report that identifies at least one externally networked source of potential pestware activity ('243 patent, claim 6) to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware ('932 patent, claim 5) to generate a report including a reference to an identity of an externally networked source of the suspected pestware object and to report the identity of the externally networked source to an externally networked pestware research entity **Structure:** Indefinite; no corresponding structure

As with "research portion," Dr. Subrahmanian opined that "reporting portion" is neither a term of art nor understood as a name for a structure or a class of structures. Ex. A, ¶¶47-48, 50-52, 54-56. Likewise, no definition of the term appears in technical dictionaries, treatises, or the

publications cited in the patents. *Id*., ¶¶42-44, 46. And a database search of patent references revealed use of the term on only three occasions relating to different components outside the field of cybersecurity. *Id*. ¶¶45; Ex. B. Dr. Subrahmanian further testified that, other than the Plaintiffs' patents, he has never encountered the term "reporting portion" in the context of malware. Ex. A, ¶¶40-41, 52, 56.

The specifications of the '243 patent, '244 patent, and '932 patent provide no structural definition for "reporting portion" and never use the term. Here, the "claim nakedly recites ["reporting portion"] and the written description fails to place clear structural limitations" on it. *Apple*, 757 F.3d at 1303 (citation omitted). In fact, the specifications place ***no*** structural limits on "reporting portion." Neither the claims nor specifications identify any input, output, or connection, or explain how the recited functions are achieved in the context of the invention. *See id*. at 1299. And the claims recite the term only functionally.

The presumption that § 112 ¶ 6 does not apply to "reporting portion" is overcome for the same reasons applicable to "research portion." And as a means-plus-function term, the specifications must disclose corresponding structure to perform the recited functions. *See Noah*, 675 F.3d at 1312. They do not. As such, the term is indefinite for failing to inform, with reasonable certainty, a POSITA as to the scope of the invention. *See Nautilus*, 572 U.S. at 901.

II. '123 PATENT

U.S. Patent No. 8,763,123 (the "'123 patent") is a division of U.S. Patent No. 8,418,250 (the "'250 patent").[9] The claims of the '123 patent are directed to an embodiment described at column 16, line 5 through column 17, line 15. In that embodiment, the anti-malware system gathers information about the processes and security products running on multiple remote computers, then

[9] Plaintiffs asserted the '250 patent in their original complaint, which was addressed in earlier claim construction briefing. *See* Dkt. 1 at 3.

analyzes that information to determine whether certain remote computers are vulnerable. In an example set forth in the specification, if a computer running "version A of anti-virus product B" fails to detect a particular malware process, the system infers that other computers running "version A of anti-virus product B" are vulnerable to that same malware process because those computers are running the same security product or products. Ex. DD ("'123 patent") at 16:51-61.

A. "receiving . . . receiving . . . receiving . . . determining . . . determining . . ." ('123 patent, claims 1, 4, 13, and 16)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	Order of steps: Step [1C] before Step [1D]; Steps [1A] to [1D] must all occur before Step [1E]

Claims 1, 4, 13, and 16 inherently require certain operations to occur in sequence. For example, a base computer must gather information about "a process" before it can determine that the process is malware. Also, the base computer must receive information about the security products running on multiple computers before it can compare those security products to determine that those computers have similar security vulnerabilities.

Claim 1 exemplifies the sequence:

[1PRE] A method comprising:

[1A] receiving, at a base computer, details uniquely identifying one or more **security products operating at a point in time on a remote computer**;

[1B] receiving, at the base computer, details uniquely identifying one or more **security products operating on other remote computers** in communication with the base computer;

[1C] receiving, at the base computer, details of **a process** that has been executed by at least one of the other remote computers;

[1D] determining, by the base computer and ***based on*** the received details of **the process** that has been executed by the least one of the other remote computers, that **the process is a malware process** not identified by the one or more security products operating on the at

least one of the other remote computers; and;

[1E] determining, by the base computer, that the remote computer is vulnerable to **the malware process**, wherein the determination is **based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer**.

(emphases added).

Step [1C] must occur before step [1D]. At step [1C], the base computer receives information about "**a process**," and then at step [1D], "based on" the information received at step [1C], the base computer determines that "**the process is a malware process**."[10] *Wi-LAN*, 811 F.3d at 462-63 (claims have an "ordering requirement" when steps refer back to results of previous steps).

Likewise, step [1E] cannot be completed until after steps [1A] through [1D]. At step [1E], the base computer determines that "the remote computer" is vulnerable to "**the malware process**" (determined at step [1D]), because it has the same or similar **security products** as "other remote computers" (comparison of information received at steps [1A] and [1B]) that were also vulnerable to that process.

The order of steps dictated by the claim language aligns with the specification. In the example below, the base computer first knows that a computer bearing a particular set of security products failed to detect "malware process P." Only after learning this information, and also that "computer 2" has the same set of security products, can the base computer determine that "computer 2" is also vulnerable to malware process P:

[10] The term "***the*** process" in [1D] must refer back to "***a*** process" in [1C]. *See Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1356-57 (Fed. Cir. 1999) (construing "the discharge rate" to refer to the antecedent "a discharge rate" to "avoid[] any lack of antecedent basis problem").

> In a simple example, if for example the database knows that a computer in the past has version A of anti-virus product B with downloaded signature update C, and also has a firewall D with particular settings E, and perhaps anti-spyware software F with signature updates G, but that a particular malware process P was not detected by this combination of programs at that point in time, then this information can be provided to a computer 2 that is known as having that combination of security programs/settings, and can be used to indicate that that computer 2 is vulnerable in the short term to attack by that particular malware process.

16:51-61; *see Mformation*, 764 F.3d at1400 (noting order of steps "is consistent with the sole embodiment in the specification").

Claims 4, 13 and 16 recite the same steps with the same dependencies.[11]

'123 patent, Claim 4	'123 patent, Claim 13	'123 patent, Claim 16
a base computer constructed and arranged to receive details uniquely identifying **one or more security products operating at a point in time on a remote computer**;	receiving, at a base computer, details uniquely identifying **one or more security products operating at a point in time on a remote computer**;	receiving, at a base computer, details of **one or more security products operating at a point in time on a remote computer**;
the base computer being constructed and arranged to receive details uniquely identifying **one or more security products operating on other remote computers** in communication with the base computer;	receiving, at the base computer, details uniquely identifying **one or more security products operating on other remote computers** in communication with the base computer;	receiving, at the base computer, details of **one or more security products operating on other remote computers** in communication with the base computer;
the base computer being constructed and arranged to receive **details of a process that has been executed by at least one of the other remote computers**;	receiving, at the base computer, **details of a process that has been executed by at least one of the other remote computers**;	receiving, at the base computer, **details of a process that has been executed by at least one of the other remote computers**;
the base computer being constructed and arranged to determine, **based on the received details of the**	determining, by the base computer and **based on the received details of the process that has been**	determining, by the base computer and **based on the received details of the process that has been**

[11] Claims 13 and 16 also recite two additional "identifying" steps, which are not part of the proposed order-of-steps construction.

’123 patent, Claim 4	’123 patent, Claim 13	’123 patent, Claim 16
process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and	**executed by the least one of the other remote computers, that the process is a malware process**;	**executed by the least one of the other remote computers, that the process is a malware process**;
the base computer being constructed and arranged to determine that **the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computers**.	determining, by the base computer, that **the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer**. . . .	determining, by the base computer, that **the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer**. . . .

(emphases added).

Although claim 4 is an apparatus claim, it requires an order of steps because its limitations are otherwise the same as method claim 1. For apparatus claims, courts impose an order of steps when “the claim language contemplates and explicitly describes a sequential process.” *Oak Tech. Inc. v. Int’l Trade Comm’n*, 248 F.3d 1316, 1323-25 (Fed. Cir. 2001) (construing apparatus claim for a “compact disk drive controller”). This is particularly true where an apparatus claim “perform[s] essentially similar steps” as a sequential method claim. *Versata Software*, 2009 WL 1408520, at *13. That is the case here. In claim 4 and in claim 1, the claim language requires the method/apparatus to gather information about a process before determining that process to be malware “based on” the information gathered about the process, and to gather information about security products on multiple computers before determining vulnerability “based on” the

information gathered about those security products.

B. "security products" ('123 patent, claims 1, 3, 4, 6, 10, 11, 12, 13, 14, 15, and 16)

Plaintiffs	Sophos
Plain and ordinary meaning	anti-malware systems including anti-virus software, anti-spyware, firewall, and anti-adware

The intrinsic evidence supports Sophos's construction that "security product" refers to "anti-malware systems including anti-virus software, anti-spyware, firewalls, and anti-adware." The purpose of the invention, and specification's use of "security product" is consistent with Sophos's proposed construction.

As the specification explains, the alleged invention of the '123 patent relates generally to detecting and subsequently "dealing with malware." '123 patent at 1:9-10. To do so, the '123 patent describes remedying the vulnerabilities of existing "anti-malware systems" detection capabilities, and the claims set out to effectuate such a remedy. '123 patent at 1:65-67, 2:1-34. The patent focuses on identifying security products that fail to detect malware because, for example, the security products do not have the malware in their signature database. The patent purports to then use that information to identify other computers that have the same combination of security products, as those computers are likely to fail to detect (and thus be susceptible to) the same malware. To that end, the claims, and the patent as a whole, recite that the security products *must* be designed to detect malware—they must be anti-malware systems. *See* '123 patent at claim 1 ("determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer"). This is consistent with the '123 patent's description of "security products": "anti-malware systems including anti-virus software, anti-spyware, anti-

adware and so on." *E.g.*, '123 patent at 16:10-12. To determine the security products on each remote computer as required by the claims, the patent discloses "agent software" that provides that information to the central server. *Id.*, 16:5-9. This agent software is not one of the security products, which are separately described. *Id.*, 16:10-12.

The explicit example in the specification further supports Sophos's construction:

> In a simple example, if for example the database knows that a computer in the past has version A of *anti-virus product B* with downloaded signature update C, and also has a firewall D with particular settings E, and perhaps *anti-spyware software F* with signature updates G, but that a particular malware process P was not detected by this combination of programs at that point in time, then this information can be provided to a computer 2 that is known as having that combination of security programs/settings, and can be used to indicate that that computer 2 is vulnerable in the short term to attack by that particular malware process.

Id. at 16:51-61 (emphasis added). This example contemplates a plethora of security products, from different vendors, which are designed to *detect* different kinds of malware. The database knows what *combination* of anti-malware systems a given remote computer has, and then identifies other computers with the same combination of security products because said combination is "not detect[ing]" a particular malware process and thus the other computers are "vulnerable . . . to attack." *Id.* Critically, as described throughout the specification and claims, the described system is not a centrally controlled network-wide security product installed on the base computer with agents on each of the remote computer. *Id.*, claim 1, 16:5-12. To the contrary, this system where each of the remote computers may have their own combination of different "security products" installed and the system simply keeps a database of those different "security products" on the different remote computers to identify potential vulnerabilities. *See id.*

Expanding the term "security products" beyond anti-malware systems would be contrary to the specification of the '123 patent. Accordingly, Sophos's construction should be adopted.

III. ’505 PATENT

U.S. Patent No. 8,856,505 (“the ’505 patent”) is generally directed to the ***timing*** of executing security software. According to the specification’s “Background,” some pestware loads very early in a computer’s boot sequence, even earlier than security software. Ex. EE (“’505 patent”) at 1:46-67. By loading this early, the patent alleges that the pestware can modify the computer’s operating system such that, when the security software loads later, the security software may fail to detect the pestware because it relies on operating system behaviors that the pestware has already corrupted. *Id.* To allegedly combat these “cloaking techniques,” *id.*, the ’505 patent simply calls for security software that “begins execution early in the boot and operating system loading process.” *id.* at 3:25-26. This early load time allegedly allows the software to “intercept and monitor . . . attempts by pestware to modify the behavior of the operating system.” *id.* at 3:32-43.

Claim 1 is exemplary:

1. A method for managing pestware on a computer comprising:

monitoring events during a boot sequence of the computer;

managing pestware-related events during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded;

managing pestware-related events in accordance with a set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications;

generating, in response to the monitoring, a record of events, the record of events including the pestware-related events;

analyzing the record of events so as to identify the pestware-related events

modifying the set of behavior rules so as to prevent the pestware related events; and

scanning data in a registry of the computer for pestware during the second period in the boot sequence.

A. "behavior rules" ('505 patent, claims 1, 2, 6, 7, 11, 12, 16, and 17)

Plaintiffs	Sophos
Plain and ordinary meaning	Plain-and-ordinary meaning wherein the plain-and-ordinary meaning does not include the static attributes of the monitored application.

The intrinsic evidence supports Defendants' construction—the term "behavior rules" has a plain-and-ordinary meaning that does not include the static attributes of the monitored application. The Court previously recognized the plain and ordinary meaning of the "behavior" terms for the '250 and '721 patents did not include static attributes. Case No. 22-cv-243, Dkt. 236 (Claim Construction Order) at 3. Here, the '505 patent is no different, and the term "behavior rules" has an analogous plain and ordinary meaning.

As the specification shows, "behavior rules" focus on the *actions* of the monitored applications. The specification describes that "attempts" are located using "behavior rules":

> [T]he kernel-level monitor 105 in the exemplary embodiment also provides mechanisms that can prevent, disable or disallow ***attempts*** by pestware to use or create patches, hooks and other methods required for intercepting or altering operating system information. In addition, the *kernel-level monitor 105 identifies* ***specific attempts*** *by other software* by ***locating the specific instance within the set of behavior rules*** 120 generated by the pestware management engine 110.

'505 patent at 3:39-46 (emphases added). These specific attempts are not static attributes—indeed, a static attribute like a "file name" cannot be described as an "attempt" to use or create something.

The specification also discusses the "behavior" noted in the "behavior rules" as "events." "[W]hen the kernel-level monitor 105 begins execution, it acquires the most recent set of behavior rules (e.g., in a secure manner) from behavior rule storage 120 (Block 206) and *begins monitoring for the* ***events*** *specified in the rules* (Block 208)." *Id.* at 4:63-67 (emphases added). Events that are "marked for denial or deletion in the behavior rules" are then either prevented from being received

by the operating system, or rejected by the operating system. *Id.* at 5:8-11. These events are actions—not static attributes.

Defendants construction is further bolstered by U.S. Non-Provisional Pat. App. 11/237,291 (U.S. Published Pat. App. No. 20070074289) ("Maddaloni"), which is incorporated into the '505 patent by reference. The specification of the '505 patent specifically points to Maddaloni because it "includes details about developing behavior rules." Maddaloni does not use the word "behavior" and instead uses "activity" to discuss "factors indicative of pestware" that were compared against the "*activity* of the process," or "factors that correspond to patterns in the *activities*" of a plurality of computers. Maddaloni at [0007], [0008] (emphases added). The specification's incorporation of Maddaloni further confirms that behavior does not include static attributes.

Lastly, construing the term "behavior rules" to include the static attributes of the monitored application would eliminate the word "behavior." "It is highly disfavored to construe terms in a way that renders them void, meaningless, or superfluous." *Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.*, 853 F.3d 1272, 1288 n.10 (Fed. Cir. 2017). As Defendants previously explained in the context of the '250 patent, the everyday understanding of behavior' connotes action and is the opposite of passivity. Thus, the plain and ordinary meaning of "behavior rules" should not include passive information like static attributes, and the Court should adopt Sophos' proposed construction.

B. "scan[ning] data in a registry" ('505 patent, claims 1, 6, and 11)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	Plain-and-ordinary meaning, wherein the plain-and-ordinary meaning of "scan[ning] data in a registry" does not include detecting reads of a registry.

Each independent claim of the '505 patent requires "scanning data in a registry." As the plain language of the term indicates, scanning data ***in*** a registry means scanning the contents of the registry itself. It does not encompass detecting events in which ***other objects*** interact with the

registry, such as detecting if a malware object reads from the registry. The applicant confirmed this distinction during prosecution to overcome the prior art, and CrowdStrike proposes that the Court reaffirm this plain meaning distinction for the jury, as these concepts may appear to be similar to a juror but are in fact different.

The specification describes that security software can detect and act upon pestware-related events, such as "events associated with the loading, execution, and behaviors of pestware." '505 patent at 3:66-4:1. In the first several limitations of claim 1, the claimed security system "monitors," "manages," "generates a record of," and "analyzes" events executed by the pestware. These detections and analysis enable the security system to modify a set of "behavior rules" to prevent the pestware from executing the problematic events. *See id.* at 3:32-50 (describing security techniques to detect pestware events, "including attempts by pestware to modify the behavior of the operating system").

But the final limitation is of a different nature. It does not require the security system to observe or act upon events being performed by pestware, but rather requires the security system itself to scan data in a registry to look for pestware stored there.[12] *See id.* at 6:4-7 (describing "native scanner 502" that is "configured to examine registry").

During prosecution, the applicant confirmed the distinction between ***scanning data in*** a registry and ***detecting events*** that involve the registry, such as a malware process reading from the registry. As originally presented to the Examiner, the final limitation of claim 1 recited: "scanning a registry of the computer for pestware during the second period in the boot sequence." Ex. P (File

[12] The registry is a database of information, specifically a "central hierarchical database in the Windows operating system used to store information necessary to set your computer up, for users, for applications, for attached hardware devices." Ex. E (Newton's Telecom Dictionary – 22nd Edition) at CROWDSTRIKE-WEBROOT00034862.

History of U.S. Patent 8,856,505: Original Claims, April 30, 2012). In a nonfinal office action, the Examiner rejected all claims as obvious, and found specifically that U.S. Pat. Pub. No. 2005/0216759 ("Rothman") taught the "scanning a registry" limitation. Ex. Q (File History of U.S. Patent 8,856,505: Non-Final Office Action, October 18, 2013). In response, the Applicant amended the claims to add "data in" to that limitation:

> 1. (Currently Amended) A method for managing pestware on a computer comprising:
>
> monitoring events during a boot sequence of the computer;
>
> managing pestware-related events during a first period in a boot sequence of the computer, the first period in the boot sequence ~~occuring~~occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded;
>
> managing pestware-related events in accordance with a set of behavior rules during a second period in the boot sequence ~~occuring~~occurring when the computer is configured to run native applications; and
>
> scanning data in a registry of the computer for pestware during the second period in the boot sequence.

Ex. R (File History of U.S. Patent 8,856,505: Amendment and Response, January 22, 2014) at 2. The applicant argued that Rothman did not teach the claim element as amended:

> [N]owhere does Rothman teach at least scanning data in a registry of the computer for pestware during the second period in the boot sequence. Instead, Rothman clearly teaches detecting suspicious reads of system files, such as registry information, that indicate a virus is looking for vulnerabilities in the computer system. ***Detecting suspicious reads of a registry is not the same as scanning data in a registry of the computer*** for pestware during the second period in the boot sequence.

Id. at 10 (underlining in original, bold-italic added). The applicant made clear that "scanning data in a registry for pestware" is different from detecting actions performed by pestware, such as "reads of a registry." The Court should therefore affirm that "scanning data in a registry" carries its plain, literal meaning, and may not be broadened to encompass any event that involves the registry, such

as a malware process attempting to read the registry.

C. "pestware management engine" ('505 patent, claims 2, 7, 12, and 16)

Plaintiffs	Trend Micro
Plain and ordinary meaning	This limitation is a means-plus function limitation governed by 35 U.S.C. § 112, ¶ 6 **<u>Functions</u>: (Claims 2, 7, 12):** compile behavior rules to include in the set of behavior rules **(Claim 16):** modify the behavior rules utilized by a kernel-level monitor **<u>Structure</u>:** Indefinite for failure to disclose corresponding structure or algorithm

This Term Invokes 35 U.S.C. § 112, ¶ 6. As courts have held, "engine" is a "nonce word that can operate as a substitute for 'means' in the context of [§ 112, ¶ 6]." *Parity Networks, LLC v. ZyXEL Commc'ns, Inc. et al.*, No. SACV 20-697-JVS (KESx), 2020 WL 8569299, at *6 (C.D. Cal. Dec. 22, 2020) (quoting *Williamson*, 792 F.3d at 1350); *see also Takadu Ltd. v. Innovyze LLC*, No. 21-291-RGA, 2023 WL 2563157, at *8 (D. Del. Mar. 17, 2023) ("'[e]ngine' appears to be synonymous with 'module,' which is recognized as a common 'nonce' word.") (citing *Williamson*, 792 F.3d at 1350). Indeed, this Court has previously found the term "heuristics engine" to be subject to § 112, ¶ 6.[13] *Audioeye, Inc. v. AccessiBe Ltd.*, No. 6:20-cv-00997-ADA, Dkt. 69 at 6.

Here, the patent simply pairs the common nonce term "engine" with the functional term "pestware management." Adding that prefix does not provide the requisite structure to remove the claimed "engine" from the realm of § 112, ¶ 6. To the contrary, "pestware management engine" is neither a term of art, nor otherwise known to POSITAs to convey a particular structure. Ex. U (Almeroth Decl.) ¶¶82-83.

[13] The Court found the term was not means-plus-function in claims that did not recite any function. *AudioEye*, Dkt. 69 at 6 and Dkt. 36 at 30-31. Here, each of the claims at issue recites a function for the "pestware management engine."

The specification does not disclose such structure either, but instead broadly discloses that the "pestware management engine [] can be implemented in software or hardware." '505 patent, at 3:4-8. Providing no specific structure, the specification uses the terms "pestware management engine" and "pestware management module" interchangeably. *Id*. at 3:66-4:7; *see also id.* at 3:4-8; *Williamson*, 792 F.3d at 1350 ("'Module' is a well-known nonce word that can operate as a substitute for 'means' in the context of § 112, para. 6."). The specification exclusively depicts the "pestware management engine" as a box. *See* '505 patent at Figs. 1 (showing "Pestware Management Engine" as box 110), 5 (same). Such black box disclosures confirm this term invokes § 112, ¶ 6. *See Williamson*, 792 F.3d at 1351 (finding that "merely set[ting] forth 'the same black box without recitation of structure for providing the same specified function'" invokes § 112, ¶ 6); *see also* Ex. U ¶¶ 84-85.

No Sufficient Structure is Disclosed. While broadly disclosing that the "pestware management engine [] can be implemented in software or hardware," the specification discloses neither a specific hardware structure nor an algorithm for performing the claimed functions—*i.e.*, "compile behavior rules to include in the set of behavior rules" (claims 2, 7, 12), or "modify the behavior rules utilized by a kernel-level monitor" (claim 16). Instead, the specification simply parrots the claimed functions without disclosing the hardware or algorithm to perform those functions. *See* '505 patent at Abstract ("[T]he pestware management system . . . *compiles the set of behavior rules*…"), 3:29-31 ("*behavior rules* … *compiled* by the pestware management engine"), 3:58-59 ("the pestware management engine [] can add to or *modify the* common set of *behavior rules* . . ."), 6:8-10 (emphases added); *see also* Ex. U ¶¶ 86-94.

Since the specification does not disclose the requisite structure of or an algorithm for the "pestware management engine" for performing the claimed functions, a POSITA cannot discern

the scope of claims 2, 7, 12, and 16 and these claims are indefinite.

D. "the boot sequence" ('505 patent, claim 10)

Plaintiffs	Trend Micro
Plain and ordinary meaning	Indefinite

Claim 10 of the '505 patent is indefinite because it is not reasonably certain what "the boot sequence," as claimed, refers to. *See Nautilus*, 572 U.S. at 910. To explain, claim 10 depends on claim 6, which recites "**a boot sequence** of the computer" twice. *See* Ex. '505 patent at 7:7-8 (emphasis added), 7:10-11, 7:45-47. Given claim 6 recites multiple boot sequences, the reference in claim 10 to "the boot sequence" is indefinite.

The term "boot," is well known by those of ordinary skill in the art and refers to the "initial starting-up" of a computer. Ex. Z (Modern Dictionary of Electronics), at 80; Ex. X (Webster's New World Dictionary of Computer Terms), at 58; Ex. Y (Webster's II New College Dictionary), at 131. This "boot" or "initial starting-up" can include multiple operations and sequences. *See*, *e.g.*, Ex. Z (Modern Dictionary of Electronics), at 80 (explaining "boot" to involve "clear[ing] the memory," "load[ing] the operating system," and "prepar[ing] a computer for use"); *id*. (explaining that a "cold boot" involves switching power from off to on, "clearing the memory and reloading the operating system" while a "warm boot" involves "clearing the memory and reloading the operating system" when the computer "is already turned on").

This understanding is consistent with the specification, which discloses multiple boot sequences, and does not clarify which "boot sequence" is referenced in claim 10. *See*, *e.g.*, '505 patent at 2:18-29 (disclosing "a boot sequence" and another "boot sequence"), 2:49, 2:51 ("depicting a boot sequence"), 2:57 ("depicting another boot sequence"); Figs. 3, 4, 6.

Courts have found claims with similar ambiguity indefinite. *See*, *e.g.*, *Sensor Elec. Tech., Inc. v. Bolb, Inc.*, No. 18-cv-05194-LHK, 2019 WL 4645338, at *31 (N.D. Cal. Sept. 24, 2019)

(finding claim reciting "the material" indefinite in light of ambiguity presented by two separate recitations of "a material"); *see also Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1343 (Fed. Cir. 2008) ("if two different levers are recited earlier in the claim, the recitation of 'said lever' in the same or subsequent claim would be unclear where it is uncertain which of the two levers was intended"); MPEP § 2173.05(e). Because it is not reasonably certain which of the multiple "boot sequence[s]" recited earlier in the claims it is that "the boot sequence" refers to, claim 10 is indefinite.

E. Claims 1, 6, and 11 of the '505 patent

Plaintiffs	Sophos / CrowdStrike
Plain and ordinary meaning	Order of steps: the managing and generating steps happen before the analyzing step, which happens before the modifying step.

All asserted claims of the '505 patent require performing steps in a specific order: (1) managing pestware-related events during the boot sequence using a set of rules; (2) generating a record of those events; (3) analyzing that record; and (4) modifying the set of rules based upon that analysis. Indeed, precise timing is a key part of the patent because monitors need to be set up ***before*** malware-related events in the boot sequence take place to detect those events. And, the analysis then takes place later, after the boot sequence, to analyze the full record of events and then modify the behavior rules based upon that analysis. Indeed, the claim language itself mandates that order. For example, claim 1 recites:

> [1A] monitoring events during a boot sequence of the computer;
>
> [1B] managing ***pestware-related events*** during a first period in a boot sequence of the computer, the ***first period in the boot sequence*** occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded;
>
> [1C] managing ***pestware-related events*** in accordance with ***a set of behavior rules*** during a ***second period in the boot sequence*** occurring when the computer is configured to run native applications;

[1D] generating, in response to the monitoring, ***a record of events***, the record of events including ***the pestware-related events***;

[1E] analyzing ***the record of events*** so as to identify the pestware-related events

[1F] modifying ***the set of behavior rules*** so as to prevent the pestware related events.

(emphases added).

As detailed above, the claims require that, ***during the boot sequence***, the system manages pestware-related events based upon a set of behavior rules. The system then generates a record of those events, including those managed pestware-related events. Then, after the generation of the record of events, that full record is analyzed and the set of behavior rules is modified. For clarity, Sophos is not arguing that the record of events has to be generated only after the management of pestware-related events completes. But, the intrinsic record, including the claim language above, makes clear that analyzing the record of events and modifying the behavior rules needs to take place ***after*** the managing and generating steps.

Any presumption against an ordering of steps is overcome where a later step recites and relies on the results of an earlier step, as is the case here depicted above. *Mformation*, 764 F.3d at 1392("[A] claim requires an ordering of steps when the claim language, as a matter of logic or grammar, requires that the steps be performed in the order written[.]"); *Wi-LAN*, 811 F.3d at 460; *Altris, Inc. v. Symantec Corp*., 318 F.3d 1363, 1369-70 (Fed. Cir. 2003) ("[W]e look to the claim language to determine if, as a matter of logic or grammar, they must be performed in the order written."); *see also WSOU Inv. LLC v. Dell Techs. Inc., et al*., No. 6:20-cv-00473 (Dkt. 94) (W.D. Tex. May 27, 2021).

This is consistent with every single embodiment in the specification, which stress the timing of when the monitoring and analysis occurs. For example, Figures 3 and 4 contrasts the prior art boot sequence (Figure 3) with the alleged invention (Figure 6) to show that, the alleged

advantage over the prior art is that the monitor and behavior rule enforcement occurs at specific times during of the boot sequence—while drivers are loaded and initialized. '505 patent at Figs. 3, 6. Figure 6 also adds in a "native scanner" "***before*** the Win32 subsystem and most services are loaded and executed," consistent with step [1C]. *Id*., 6:6-7 (emphasis added). According to the patent, the native scanner generates additional information that the system "can ***later*** examine and utilize in order to generate new behavior rules." *Id*., 6:9-10 (emphasis added). In other words, the patent itself states that the analysis of the full event log and modification of behavior rules happens "***later***," i.e., after the boot sequence completes, during normal operation of the computer. *See id*. (emphasis added).

Furthermore, Courts, including this one, commonly find that apparatus and system claims have an order of steps when they are similar to the method claim, which is the case as shown in the table below. *See Avago*, 2016 WL 3029674, at *12 (noting case law supporting, and absence of any case law refuting, that "order can be required by a system/apparatus claim"); *Maxim*, 2018 WL 4657384, at *9 (collecting cases); *WSOU Investments LLC v. Dell Techs. Inc*., No. 6:20–cv-00476-ADA, slip op. at 9 (W.D. Tex. May 27, 2021).

Claim 1	Claim 6	Claim 11
managing ***pestware-related events*** during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded	a second instruction set configured to manage ***pestware-related events*** during first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a WIN32 subsystem is loaded, and after a kernel is loaded	managing ***pestware-related events*** during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a WIN32 subsystem is loaded, and after a kernel is loaded
managing ***pestware-related events*** in accordance with ***a***	a third instruction set configured to manage	managing ***pestware-related events*** in accordance with ***a***

Claim 1	Claim 6	Claim 11
set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications	***pestware-related events*** in accordance with ***a set of behavior rules*** during a second period in the boot sequence occurring when the computer is configured to run native applications	***set of behavior rules*** during a second period in the boot sequence occurring when the computer is configured to run native applications
generating, in response to the monitoring, ***a record of events***, the record of events including ***the pestware-related events***	a fourth instruction set configured to generate, in response to the monitoring, ***a record of events***, the record of events including ***the pestware-related events***	generating, in response to the monitoring, ***a record of events***, the record of events including ***the pestware-related events***
analyzing ***the record of events*** so as to identify the pestware-related events	a fifth instruction set configured to analyze ***the record of events*** so as to identify the pestware-related events	analyzing ***the record of events*** so as to identify the pestware-related events
modifying ***the set of behavior rules*** so as to prevent the pestware related events	a sixth instruction set configured to modify ***the set of behavior rules*** so as to prevent the pestware related events	modifying ***the set of behavior rules*** so as to prevent the pestware related events

(emphases added).

Since claims 6 and 11 recite a substantively identical limitations, both require the same order of steps as claim 1.

F. Claim 6 of the '505 patent: "a memory comprising: . . ."

Plaintiffs	Sophos
Plain and ordinary meaning	Subject to § 112, ¶ 6. Functions: (1) monitor events during a boot sequence of the computer (2) manage pestware-related events during first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a WIN32 subsystem is loaded, and after a kernel is loaded

	(3) manage pestware-related events in accordance with a set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications (4) generate, in response to the monitoring, a record of events, the record of events including the pestware-related events (5) analyze the record of events so as to identify the pestware-related events (6) modify the set of behavior rules so as to prevent the pestware related events (7) scan data in a registry of the computer for pestware during the second period in the boot sequence Structure: no corresponding structure (no algorithm)

Claim 6 recites "a memory comprising" seven instruction sets, each of which states the function that the instruction set is to perform. This is the very definition of functional claiming. Even if a claim does not use the word "means," § 112, ¶ 6 applies if the term fails to "recite sufficiently definite structure" or recites "function without reciting sufficient structure for performing that function." *Williamson*, 792 F.3d at 1349. The claim describes the "memory" by solely describing its functions. *Diebold Nixdorf, Inc. v. Int'l Trade Comm'n*, 899 F.3d 1291, 1298 (Fed. Cir. 2018) ("cheque standby unit" invoked § 112, ¶ 6 because the claims described the term "solely in relation to its function and location in the apparatus").

The term "memory" is a prototypical, black-box, and nonce word. Indeed, memory by itself does not perform any of the recited function, it simply stores data, and every computer system utilizes memory of some sort. It is therefore just a verbal construct that is tantamount to using "means for." *See Williamson*, 792 F.3d at 1350. Courts have frequently found that generic computer terms—like memory and processor—are subject to means-plus-function constructions. *E.g.*, *Konami Gaming, Inc. v. Marks Studios, LLC*, No. 2:14-cv-01485-JAD-CWH, 2017 WL 3174905, at *6 (D. Nev. July 25, 2017) ("processor configured to execute a game"); *St. Isidore Research, LLC v. Comerica Inc.*, 2016 WL 4988246, at *15 (E.D. Tex. Sep. 19, 2016) ("processor

configured to verify the authenticity of the account access request based on the response" and "processor configured to identify a second device associated with the account"); *Parity Networks*, 2020 WL 8569299, at *11 ("packet processor" that categorizes incoming packets).

Under § 112, ¶ 6, claim 6 is indefinite because there is no structure whatsoever in the specification that corresponds to at least the (1) modify the behavior rules and (2) manage pestware-related events functions. For means-plus-function claims "in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm," the Federal Circuit has held that "the disclosed structure is not the general purpose computer, but rather the ***special purpose computer programmed to perform the disclosed algorithm***." *WMS Gaming, Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1349 (Fed. Cir. 1999) (emphasis added). The 3.5 column "detailed" description in this patent is utterly devoid of any such algorithms for at least these two functions.

First, the patent has no disclosure of an algorithm (i.e., structure) for modifying the behavior rules. Instead, the patent only recites that "the pestware management engine 110 can add to or modify the common set of behavior rules." *See* '505 patent at Fig. 1. That is it; there is no algorithm disclosed, only the functional language itself. *Noah,* 675 F.3d at 1317 ("This type of purely functional language, which simply restates the function associated with the means-plus-function limitation, is insufficient to provide the required corresponding structure.").

Second, the claim recites two managing functions, one during a first period and another during a second period. For the first period, the patent recites that, during that time, "driver hooks and monitoring mechanisms are utilized," but that does not provide an algorithm/structure for ***managing*** pestware-related events. '505 patent at 4:54-56. Similarly, for the second period, the patent explains that the system may "examine registry, filesystem, and other portions of a protected

computer," but, again, that does not provide any algorithm/structure for ***managing*** pestware-related requests as recited. '505 patent at 6:4-6.

Because claim 6 recites a nonce term with functional language and lacks corresponding structure/algorithms in the limited specification, it should be found indefinite under § 112, ¶ 6.

IV. '869 PATENT

A. "the static data points" ('869 patent, claims 1, 10, 15, 18, 32, and 46)

Plaintiffs	Sophos
Plain and ordinary meaning	Indefinite

The term "the static data points" lacks a reasonably certain antecedent basis. Each asserted claim recites "*identified* static data points" and the "*plurality* of static data points." After reciting different types of static data points, the claim language recites "the static data points" without providing clarity as to whether "the static data points" refers to the "identified" or "plurality of" static data points. Because a person of ordinary skill in the art could not ascertain the boundaries of "the static data points," the term is indefinite.

The asserted claims of the '869 patent recite "identified static data points" (green below) and "plurality of static data points" (blue below):

> 1. A computer-implemented method comprising:
>
> identifying, by a knowledge module, static data points that may be indicative of either a harmful or benign executable file;
>
> associating, by the knowledge module, the identified static data points with one of a plurality of categories of files, the plurality of categories of files including harmful files and benign files;
>
> identifying an executable file to be evaluated;
>
> extracting, by the knowledge module, a plurality of static data points from the identified executable file;

> generating a feature vector from the plurality of static data points using a classifier trained to classify ***the static data points*** based on training data, the training data comprising files known to fit into one of the plurality of categories of files, wherein one or more features of the feature vector are selectively turned on or off based at least in part on evaluation of whether a value of one of the plurality of static data points is within a predetermined range; and
>
> providing the generated feature vector to one or more support vector machines to build a probabilistic model that indicates whether the executable file fits into one of the categories of files.

Ex. FF ("'869 patent) at claim 1 (emphases added). However, in the "generating" limitation, the claim recites "the static data points" (red). But since there are two different sets of static data points recited, it could refer to either the identified static data points, or the plurality of static data points. The specification also does not provide any clarity on the antecedent basis for "the static data points." This is important because a classifier may or may not be infringing depending on what data points the classifier is trained to classify. *E.g.*, *Nautilus*, 572 U.S. at 909 ("[A] patent must be precise enough to afford clear notice of what is claimed, thereby 'appris[ing] the public of what is still open to them.'") (internal quotations and citation omitted). Because "the static data points" could refer to either the "identified" or "plurality of" static data points, the lack of clarity makes this term indefinite.

In similar circumstances, this Court has found terms indefinite. For example, the term "the terminal" was found to be indefinite when it could have referred to either a "mobile communication terminal" or "another communication terminal." *WSOU Investments, LLC v. Google*, No. 6:20-cv-00581-ADA, Dkt. No. 46 at 3 (W.D. Tex. June 2, 2021); *see also WSOU Investments, LLC v. Huawei Tech. Co.*, Dkt. No. 64 at 14 (W.D. Tex. June 1, 2021) (finding "the message" indefinite; claim to "a message to the upstream device" or "a message reporting the depth of the queue");

Bushnell Hawthorne, LLC v. Cisco Sys. Inc., 813 F. App'x 522, 526 (Fed. Cir. 2020) (finding term "said different IP Address" indefinite when the claim described three different IP addresses).

Because it is not reasonably certain as to what "the static data points" refers, the term is indefinite.

B. "within a predetermined range" (claims 18, 32, and 46)

Plaintiffs	CrowdStrike / Forcepoint / Sophos / Trend Micro
Plain and ordinary meaning	Plain-and-ordinary meaning, wherein the plain-and-ordinary meaning of "range" is a numerical range or a subset of a "particular scale" with at least a lower limit or an upper limit, but not necessarily both.

The '869 patent is a continuation of U.S. Patent No. 10,599,844 and therefore shares the same written description. The Court already addressed this exact term in connection with the '844 patent, ordering that the term should be given its plain-and-ordinary meaning, "wherein the plain-and-ordinary meaning of 'range' is numerical range or a subset of a 'particular scale' with at least a lower limit or an upper limit, but not necessarily both." Dkt. 236 (Claim Construction Order) at 18. The same meaning applies to this term in the context of the related '869 patent.

Dated: April 12, 2023

Respectfully submitted,

/s/ Brian C. Banner

Brian C. Banner (TX Bar No. 24059416)
Darryl J. Adams
SLAYDEN GRUBERT BEARD PLLC
401 Congress Ave., Ste. 1650
Austin, Texas 78701
Telephone: (512) 402-3562
Facsimile: (512) 402-6865
Email: bbanner@sgbfirm.com
Email: dadams@sgbfirm.com

Counsel for Sophos Ltd.

Josh Krevitt (*Pro hac vice*)
Brian Rosenthal
Katherine Dominguez
Allen Kathir (*Pro hac vice*)
Allyson Parks (*Pro hac vice*)
Michael M. Polka (*Pro hac vice*)
Benjamin Z. Bistricer (*Pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, New York 10166-0005
Telephone: (212) 351-4000
Facsimile: (212) 716-0839
Email: jkrevitt@gibsondunn.com
Email: brosenthal@gibsondunn.com
Email: kdominguez@gibsondunn.com
Email: akathir@gibsondunn.com
Email: aparks@gibsondunn.com
Email: mpolka@gibsondunn.com
Email: bbistricer@gibsondunn.com

Timothy P. Best (*Pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, California 90071-1504
Telephone: (213) 229-7659
Facsimile: (213) 229-6659
Email: tbest@gibsondunn.com

Ryan Iwahashi (*Pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
1881 Page Mill Road
Palo Alto, California 94304-1211
Telephone: (650) 849-5300
Facsimile: (650) 849-5067
Email: riwahashi@gibsondunn.com

David Brzozowski (*Pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Ave., N.W.
Washington, D.C. 20036
Telephone: (202) 955-8500
Facsimile: (202) 467-0539
Email: dbrzozowski@gibsondunn.com

Dated: April 12, 2023

Respectfully submitted,

s/Steven Callahan
DAVID NELSON
QUINN EMANUEL URQUHART & SULLIVAN, LLP
191 N Upper Wacker Dr #2700
Chicago, IL 60606
Tel.: (312) 705-7400
Fax: (312) 705-7401

VICTORIA F. MAROULIS
QUINN EMANUEL URQUHART & SULLIVAN, LLP
555 Twin Dolphin Dr., 5th Floor
Redwood Shores, CA 94065
Tel.: (650) 801-5000
Fax: (650) 801-5100

DEEPA ACHARYA
QUINN EMANUEL URQUHART & SULLIVAN, LLP
1300 I Street, NW, Suite 900
Washington, D.C. 20005
Tel.: (202) 538-8000
Fax: (202) 538-8100

STEVEN CALLAHAN
Texas State Bar No. 24053122
scallahan@ccrglaw.com
CHARHON CALLAHAN ROBSON & GARZA, PLLC
3333 Lee Parkway, Suite 460
Dallas, Texas 75219
Tel.: (214) 521-6400
Fax: (214) 764-8392

Counsel for Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc.

Dated: April 12, 2023

Respectfully submitted,

/s/ Kat Li

Kat Li (SBN 24070142)
kat.li@kirkland.com
Nadia E. Haghighatian (SBN 24087652)
nadia.haghighatian@kirkland.com
Austin Teng (SBN 24093247)
austin.teng@kirkland.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

Adam R. Alper (admitted *pro hac vice*)
aalper@kirkland.com
Akshay S. Deoras (admitted *pro hac vice*)
adeoras@kirkland.com
Laura Ashley Harris (admitted *pro hac vice*)
lauraashley.harris@kirkland.com
KIRKLAND & ELLIS LLP
555 California Street
San Francisco, CA 94104
Telephone: (415) 439-1400
Facsimile: (415) 439-1500

Michael W. De Vries (admitted *pro hac vice*)
michael.devries@kirkland.com
KIRKLAND & ELLIS LLP
555 South Flower Street
Los Angeles, CA 90071
Telephone: (213) 680-8400
Facsimile: (213) 680-8500

Leslie M. Schmidt (admitted *pro hac vice*)
leslie.schmidt@kirkland.com
KIRKLAND & ELLIS LLP
601 Lexington Ave.
New York, NY 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Attorneys for Forcepoint LLC

DATED: April 12, 2023

By: */s/ Yar R. Chaikovsky*

Yar R. Chaikovsky, Bar No. 39625
yar.chaikovsky@whitecase.com
Philip Ou
philip.ou@whitecase.com
Bruce Yen
bruce.yen@whitecase.com
Radhesh Devendran
radhesh.devendran@whitecase.com

3000 El Camino Real
2 Palo Alto Square, Suite 900
Palo Alto, CA 94306
Telephone: 1(650) 213-0300
Facsimile: 1(650) 213-8158

THE DACUS FIRM
Deron Dacus
TX Bar No. 00790553
ddacus@dacusfirm.com
821 ESE Loop 323, Suite 430
Tyler, TX 75701
Telephone: (903) 705-1117
Facsimile: (903) 581-2543

Attorneys for Defendant Trend Micro Inc.

DATED: April 12, 2023

By: */s/ Joseph T. Miotke*

Eric H. Chadwick (pro hac vice)
Minnesota Bar No. 248769
ehc@dewittllp.com
Joseph T. Miotke (pro hac vice)
Wisconsin Bar No. 1033986
jtm@dewittllp.com
DeWitt LLP
2100 AT&T Tower
900 S. Marquette Avenue
Minneapolis, MN 5540
Telephone: (612) 305-1426

Harry "Gil" Gillam, Jr.
Texas Bar No. 07921800
gil@gillamsmithlaw.com
J. Travis Underwood
Texas Bar No. 24102587
travis@gillamsmithlaw.com
Gillam & Smith LLP
303 S. Washington Ave.
Marshall, TX 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Counsel for AO Kaspersky Lab

CERTIFICATE OF SERVICE

A true and correct copy of the foregoing instrument was served or delivered electronically via U.S. District Court [LIVE]- Document Filing System, to all counsel of record, on this the 12th day of April, 2023.

/s/ Brian C. Banner