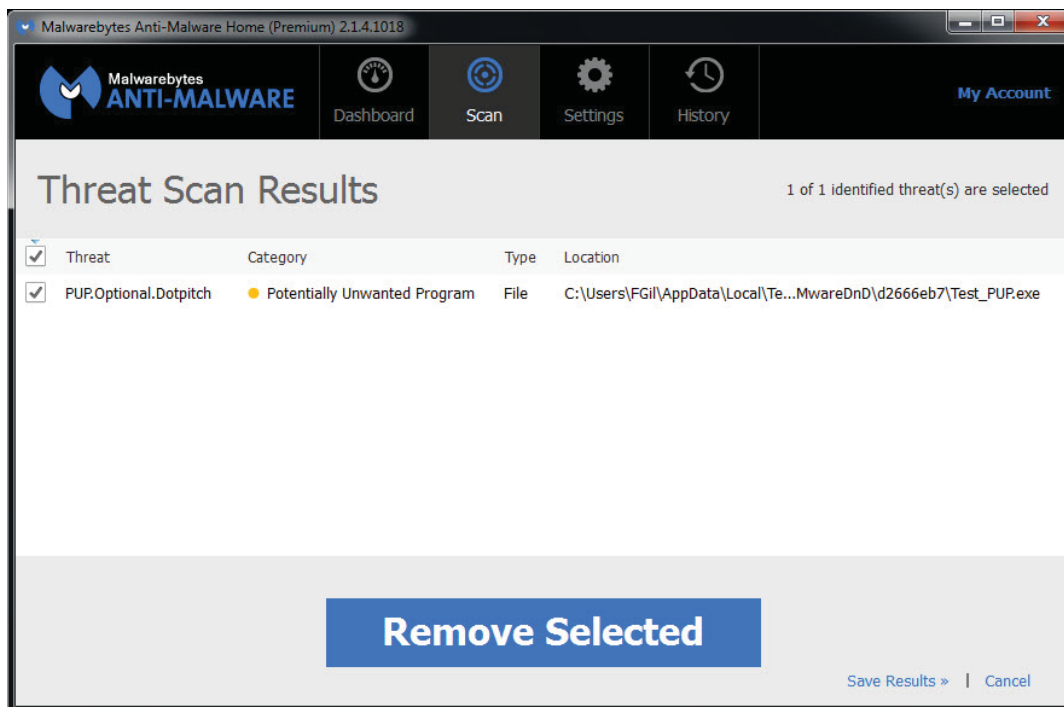


Unwanted Programs” or PUPs and automatically quarantines PUPs and flags them as “threats” for its users as shown in the screen shot below:

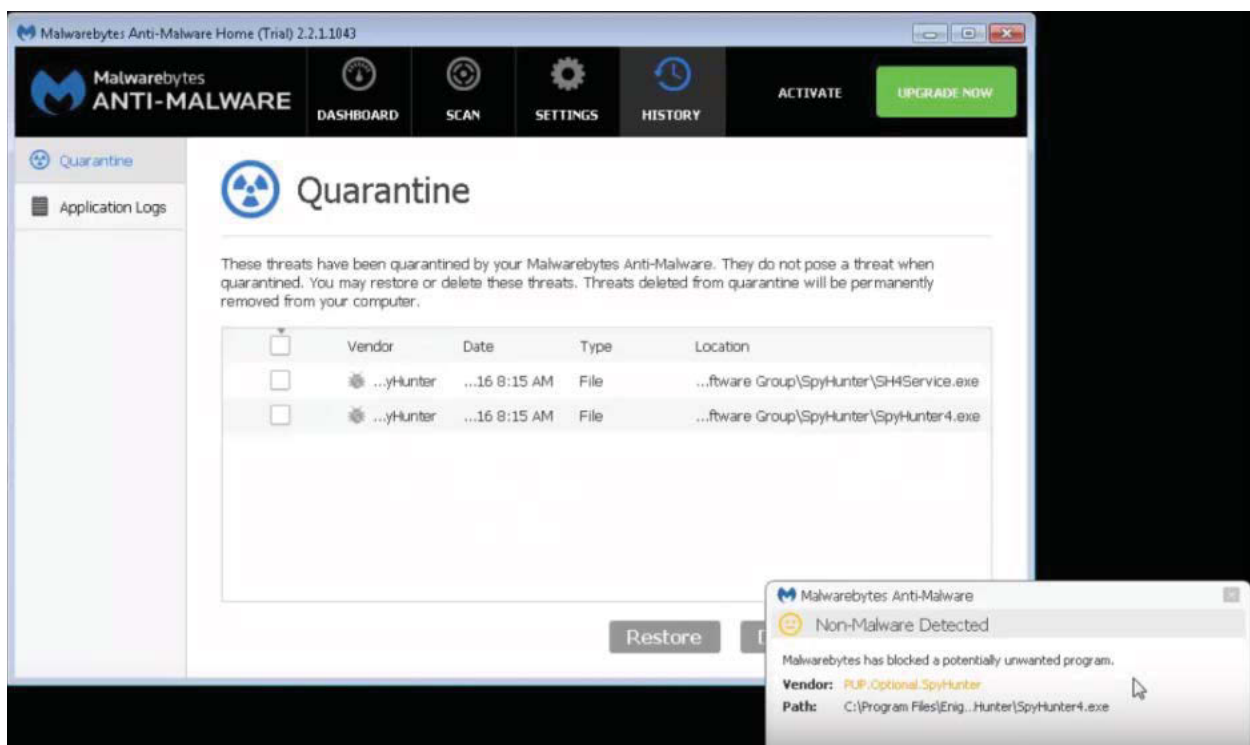


4. Malwarebytes knows that detecting and quarantining a competitor’s products like SpyHunter and RegHunter as PUPs would cause immediate harm to the competitor in the form of lost sales and revenues and also cause irreparable harm to the competitor’s business reputation as a result of being identified as a “threat” that a consumer should either not download or should remove from his or her computer.

5. Malwarebytes also knows that a decision to identify competing products like SpyHunter and RegHunter as PUPs would likely result in other anti-malware companies following suit, which would cause exponentially more harm to its competitor in a short amount of time.

6. Since its inception in 2008, Malwarebytes never identified SpyHunter or RegHunter as PUPs or any other type of malware.

7. However, on October 5, 2016, Malwarebytes' CEO, Marcin Kleczynski, announced that Malwarebytes was revising its criteria to identify PUPs. *See* Ex. 1. Immediately thereafter, Malwarebytes' MBAM product began identifying SpyHunter and RegHunter as PUPs, meaning that Malwarebytes is now falsely representing to the consuming public that Enigma's programs are a "threat" and that the consuming public's security will be compromised if they download SpyHunter or RegHunter or, if already downloaded on a consumer's computer, the consumer does not remove SpyHunter or RegHunter.



8. In addition, by identifying SpyHunter and RegHunter as PUPs, the MBAM product blocks and/or deactivates SpyHunter and RegHunter from operating on a consumer's computer.

9. Malwarebytes' deliberate decision to change its PUP definition and begin falsely identifying SpyHunter and RegHunter as PUPs was not coincidental. Rather, it was a bad faith decision made as a result of a lawsuit that ESG filed against Bleeping Computer LLC

(“Bleeping”) that is currently pending before this Court as Case No. 1:16-cv-00057-PAE (the “Bleeping Lawsuit”). Malwarebytes’ actions show the extent to which Bleeping and Malwarebytes act in concert to promote their mutual interests.

10. Malwarebytes and Bleeping have an affiliate relationship by which Bleeping promotes the MBAM product and earns commissions from Malwarebytes if a consumer purchases MBAM through a link on Bleeping’s website.

11. In the Bleeping Lawsuit, ESG alleges that Bleeping has engaged in a deliberate scheme of disseminating false, misleading and inaccurate information about ESG and its SpyHunter product and instructing consumers not to install or uninstall SpyHunter but instead to purchase Malwarebytes’ competing MBAM product, thereby earning revenues for itself and for Malwarebytes while damaging ESG and thereby promoting Malwarebytes’ business interests.

12. Malwarebytes will be a witness in the Bleeping Lawsuit and in fact must respond to a subpoena for documents in the case by October 12, 2016.

13. The transparent nature of Malwarebytes’ bad faith conduct and its connection to the Bleeping Lawsuit are numerous. For example, on Malwarebytes’ forum where Mr. Kleczynski announced Malwarebytes’ purported “New Criteria for Detecting Potentially Unwanted Products (PUPs),” the first question came from a Bleeping “Special Ops Tech” asking “what was added/removed/edited.” *See* Ex. 2. In response, Malwarebytes explained “[t]he biggest change is this criteria we use: ‘predominantly negative feedback or ratings from the user community.’”

14. Bleeping has attempted to defend its unlawful conduct in the Bleeping Lawsuit by relying on supposed negative feedback from some unidentified “user community.”

15. Further, within hours of Malwarebytes publicly announcing its new stance on

PUPs, Bleeping’s owner, Lawrence Abrams, posted a news story on the front page of Bleeping’s website lauding Malwarebytes new “policy” and copying verbatim Malwarebytes “updated PUP criteria.” *See* Exs. 3-4.

16. The charade that is Malwarebytes’ “new” policy was quickly recognized. A Bleeping “Security Colleague” who posts under the name Angoid commented on Mr. Abrams’ front page news story with a thinly veiled admission that Malwarebytes’ policy was directed specifically at ESG and SpyHunter, given Bleeping’s history of attacking ESG and the ongoing Bleeping Lawsuit: “What would be really strange is if anyone can think of any other anti-malware program that fits any one of those descriptions [the PUP criteria] not that I can think of one of course :).” *See* Ex. 4.

17. ESG brings this lawsuit and, if necessary, will move for preliminary injunctive relief to put an immediate stop to the damage and irreparable harm that Malwarebytes has caused and will continue to cause to both ESG and the consuming public as a result of its bad faith campaign of unfair competition and false and misleading statements that identify SpyHunter and RegHunter as “threats” and PUPs and thereby deceive consumers.

THE PARTIES

18. Plaintiff ESG is a Florida limited liability company, having merged with a Connecticut limited liability company of the same name. ESG does business in this District.

19. Upon information and belief, Defendant Malwarebytes is a corporation organized under the laws of Delaware and headquartered at 3979 Freedom Circle, 12th Floor, Santa Clara, CA 95054. Malwarebytes was originally incorporated under the laws of Delaware on January 6, 2014 as Malwarebytes Corporation. On December 21, 2015, Malwarebytes filed a Restated Certificate of Incorporation with the Delaware Secretary of State that amended the company name to Malwarebytes, Inc.

20. Malwarebytes currently employs a Regional Vice President in the greater New York City area. *See* Ex. 5.

21. Even now, Malwarebytes is expanding its presence in the state and district by seeking to hire a Senior Sales Engineer in New York to work with the Regional Sales Manager to “present[] Malwarebytes security solution to prospective customers” and “work closely with customers as their primary point of feedback and resolution of issues.” *See* Ex. 6.

22. Upon information and belief, Malwarebytes advertises to, provides its software for download to, and has sold its software to consumers residing in the State of New York, including in the Southern District of New York. That software is currently wrongly detecting ESG’s SpyHunter and RegHunter as PUPs and thereby misleading and deceiving consumers in the state.

JURISDICTION AND VENUE

23. This action arises under the Lanham Act, 15 U.S.C. § 1051 *et seq.* and the laws of the State of New York. This Court has subject matter jurisdiction, *inter alia*, pursuant to 28 U.S.C. §§ 1331, 1332, 1338, and 1367.

24. Upon information and belief, this Court has personal jurisdiction over Malwarebytes because Malwarebytes regularly transacts business in the State of New York and this judicial district and Malwarebytes has committed tortious acts in the state by wrongly detecting and identifying SpyHunter and RegHunter as PUPs when its software runs scans on computers in this state and district, thereby misleading and deceiving consumers in this state and district. As a result, Malwarebytes has intentionally availed itself of the privilege of conducting business in this state and district, has purposefully directed activity at this state and district, and has established sufficient minimum contacts with this state and district such that Malwarebytes can reasonably and fairly anticipate being haled into this Court.

25. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)-(c) because Malwarebytes is subject to personal jurisdiction in, and so resides in, this district.

FACTS

Background

26. ESG develops and markets computer security products with a particular focus on protecting its millions of customers from computer hacks, system breaches, identity theft and system computing malware, as well as other computer security threats.

27. ESG protects its customers from this array of serious risks by providing software that detects and removes malware, enhances Internet privacy, and eliminates other security threats.

28. ESG's flagship anti-malware product is a software program called SpyHunter, which presently is in version 4.

29. SpyHunter is an adaptive malware detection and removal tool that provides rigorous protection against the latest malware threats including spyware, Trojans, rootkits, and other malicious software.

30. Consumers can download a free scanning version of SpyHunter through a link entitled "Download Free Scanner." The scanner detects whether a computer has malware or other threats.

31. ESG informs consumers that they also have the choice to buy a license to the full version of SpyHunter and provides consumers with a "Buy Now" link. The full version of SpyHunter includes the scanner, tools to remove malware and other security protection tools.

32. ESG's advanced Windows registry cleaner and PC optimizer is a software program called RegHunter. It repairs, restores, and boosts the performance of computers running the Windows operating system by removing registry errors, cleaning computer file clutter,

defragmenting hard drives, and other optimizations.

33. ESG sells licenses to SpyHunter and RegHunter solely over the Internet, including at its website, <<http://www.enigmasoftware.com>>. ESG enjoys worldwide sales of SpyHunter and RegHunter, including sales to citizens of the State of New York.

34. ESG's SpyHunter and RegHunter products have received top industry certifications and have both been certified as TRUSTe Certified Downloads.

35. ESG is a Better Business Bureau accredited business. Better Business Bureau accreditation standards include a "commitment to make a good faith effort to resolve any consumer complaints." ESG has received an "A+" rating from the Better Business Bureau.

36. Malwarebytes is a direct competitor of ESG in the anti-malware software market and offers free and paid versions of its competing MBAM software.

37. MBAM operates by scanning a user's computer for malware and other computer security threats, detecting any such threats, reporting to the user the results of the detection, and then taking remedial action, such as preventing a malicious download, removing the threat from the computer, or providing the user with an option to remove the detected program.

ESG Files Suit Against Bleeping Computer

38. On January 5, 2016, ESG filed a lawsuit against Bleeping seeking redress for Bleeping's pattern and practice of making false and misleading statements about ESG to drive consumers away from purchasing ESG's products, including SpyHunter, and toward purchasing Malwarebytes' products, including MBAM. The details of Bleeping's smear campaign against ESG are laid out in full in ESG's Second Amended Complaint, ECF No. 25, *Enigma Software Group USA, LLC v. Bleeping Computer LLC et al.*, Case No. 1:16-cv-00057 (PAE) (S.D.N.Y. Mar. 18, 2016).

39. As alleged in the Bleeping Lawsuit, Malwarebytes directly profited and continues

to profit from Bleeping's false and misleading statements about ESG, which drive customers away from ESG and to Malwarebytes. *See id.* at ¶ 77.

40. Indeed, Malwarebytes and/or its CEO, Mr. Kleczynski, have financially supported Bleeping in the Lawsuit by directly providing money to Bleeping in response to Bleeping's GoFundMe campaign to raise money for its defense costs.

41. After the Court denied Bleeping's Motion to Dismiss ESG's Complaint finding, among other things, that the alleged false and misleading statements "unmistakably constitute advertisements" for Malwarebytes (ECF No. 45), the parties began fact discovery.

42. On September 7, 2016, as part of that fact discovery, ESG served Malwarebytes with a subpoena to produce documents, information, or objects pursuant to Rule 45 of the Federal Rules of Civil Procedure ("Subpoena").

43. The Subpoena requested that Malwarebytes produce documents reflecting the nature of its relationship with Bleeping and the extent of its involvement in Bleeping's smear campaign against ESG.

44. Malwarebytes is required to produce documents responsive to the Subpoena by October 12, 2016.

Malwarebytes Revises its Definition of a PUP

45. Less than a week before Malwarebytes is required by law to reveal the extent of its involvement in the illegal behavior ESG has pled in the Bleeping Lawsuit, Malwarebytes chose to level a new line of attack against ESG, this time directly interfering with ESG's relationships with existing and prospective customers and engaging in false statements about ESG's SpyHunter and RegHunter products.

46. On October 5, 2016, Malwarebytes announced that it revised the criteria that its product MBAM uses to detect PUPs. *See Ex. 1.*

47. Malwarebytes markets MBAM as an “anti-malware and anti-spyware scanner” that “detects and removes malware like worms, Trojans, rogues, spyware, bots, and more.” *See* <https://www.malwarebytes.com/antimalware/>.

48. PUPs, however, are not the malware or spyware programs MBAM purports to detect and remove.

49. Instead, MBAM now defines PUPs as any program that demonstrates at least one of the criteria that Malwarebytes itself has unilaterally declared makes a program “potentially unwanted.” *See* Ex. 7.

50. Malwarebytes’ announced PUP criteria include (1) “obtrusive, misleading, or deceptive advertising, branding, or search practices”; (2) “excessive or deceptive distribution, affiliate or opt-out bundling practices”; (3) “aggressive or deceptive behavior especially surrounding purchasing or licensing”; (4) “unwarranted, unnecessary, excessive, illegitimate, or deceptive modifications of system settings or configuration (including browser settings and toolbars)”; (5) “difficulty uninstalling or removing the software”; (6) “predominantly negative feedback or ratings from the user community”; (7) “diminishes user experience”; and (8) “other practices generally accepted as riskware, scareware, adware, greyware, or otherwise commonly unwanted software by the user community.” *Id.*

51. Malwarebytes further “reserve[d] the right to adjust, expand and update our criteria” for PUP identification “without prior notice or announcements.” *Id.*

52. Malwarebytes has specifically designed these vague and unbounded criteria to enable it to block its users’ access to SpyHunter and RegHunter for anticompetitive purposes or merely at its malicious whim.

53. Unsurprisingly, Malwarebytes’ criteria for PUP identification track the allegations

Bleeping made against ESG in its Counterclaims in the Bleeping Litigation.

54. In fact, upon information and belief, Malwarebytes' revision of its PUP criteria is merely a pretense to begin identifying SpyHunter and RegHunter as PUPs, to damage ESG's business and gain leverage in the Bleeping Lawsuit.

55. Demonstrating the connection between Malwarebytes' conveniently timed "revision" to its PUP definition and the Bleeping Lawsuit, on *the same day* that Malwarebytes announced its revised definition Bleeping announced the Malwarebytes change as the main story on the front page of its website, proclaiming "Malwarebytes going to battle with PUPs and Adware." *See* Ex. 3.

Malwarebytes Begins Detecting and Blocking SpyHunter and RegHunter

56. Once Malwarebytes announced its new PUP criteria, MBAM began to detect SpyHunter and RegHunter as PUPs and to block their download and installation.

57. Before October 5, 2016, MBAM had *never* designated SpyHunter or any other ESG program a PUP or any other type of "threat" for which the program scans, despite the fact that Malwarebytes and SpyHunter have coexisted in the market for over seven years.

58. Instead, Malwarebytes designated SpyHunter and RegHunter a "threat" only after it was served with the Subpoena in the Bleeping Litigation and was approaching the date it would have to reveal the extent of its involvement in Bleeping's unlawful and anticompetitive smear campaign.

59. Since Malwarebytes revised its PUP criteria to specifically target ESG's products, when a user has MBAM installed and attempts to download and install SpyHunter and RegHunter, MBAM prevents the download and installation from completing.

60. MBAM places the SpyHunter and RegHunter files in a "quarantine." It further explains to the user that the "threats," *i.e.* legitimate and non-malicious SpyHunter and

RegHunter files, placed in the quarantine “do not pose a threat when quarantined” and if “deleted from quarantine will be permanently removed from [the user’s] computer.”

61. MBAM then provides the user with the option to “delete,” “delete all,” or “restore” the quarantined files.

62. Even if the user ignores MBAM’s unjustified warning against SpyHunter and RegHunter and restores the SpyHunter and RegHunter files on the computer, every subsequent time MBAM scans the computer for threats, it again detects and reports SpyHunter and RegHunter as PUPs and encourages the user to remove the associated files.

63. As of October 6, 2016, in at least some instances MBAM even more aggressively was automatically preventing the installation of SpyHunter entirely, without the user’s consent and without providing the user an option to override MBAM’s block.

64. SpyHunter and ESG’s other products are legitimate and pose no security threat to a user’s computer.

65. Malwarebytes knows ESG’s products do not pose any security threat.

66. Malwarebytes has listed ESG’s products as PUPs solely as an anticompetitive attempt to avoid adverse consequences in the Bleeping Lawsuit and attempt to drive ESG out of business.

67. Malwarebytes’ conduct is willful and malicious.

68. Malwarebytes’ unlawful conduct is causing and will continue to cause harm to ESG.

69. Shortly after Malwarebytes began unlawfully identifying SpyHunter and RegHunter as PUPs, ESG began suffering a drop in its sales of SpyHunter and RegHunter licenses.

70. Additionally, by recommending to users who have already purchased a SpyHunter or RegHunter license and installed the programs that they delete SpyHunter and RegHunter because they are a “threat,” ESG will be harmed as users request refunds for the previously purchased licenses.

71. ESG has no adequate remedy at law for certain of the relief requested below.

FIRST CAUSE OF ACTION

(Violations of Lanham Act § 43(a))

72. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

73. Malwarebytes’ use in commerce of false and misleading statements about ESG SpyHunter and RegHunter constitutes false advertising in violation of 15 U.S.C. § 1125(a)(1)(B).

74. Malwarebytes’ use in commerce of false and misleading statements about ESG, SpyHunter and RegHunter is likely to deceive consumers as to the nature, quality, and efficacy of SpyHunter and RegHunter, including causing consumers to believe that SpyHunter and RegHunter are malicious or a threat.

75. Such deception is material as it is likely to influence consumers not to purchase SpyHunter or RegHunter and/or to do business with ESG and to continue to utilize and subscribe to Malwarebytes’ MBAM product.

76. Malwarebytes’ false and misleading statements have actually deceived or have the capacity to deceive a substantial portion of their intended audience, *i.e.*, users of MBAM who are also existing or potential customers of ESG and users of SpyHunter and/or RegHunter.

77. Malwarebytes’ false and misleading statements are shown to users of MBAM *every time* a user attempts to download and install SpyHunter or RegHunter and are part of an organized campaign by Malwarebytes to strengthen its position in the market for anti-malware

products by unfairly driving consumers away from ESG and SpyHunter and/or RegHunter.

78. As a direct and proximate result of Malwarebytes' unlawful acts, ESG has suffered and will continue to suffer significant monetary and reputational injury, including losses of sales and a lessening of goodwill associated with its products, in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

SECOND CAUSE OF ACTION

(Violations of New York General Business Law § 349)

79. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

80. Section 349 of New York's General Business Law prohibits the use of deceptive acts or practices in the conduct of business, trade or commerce or in the furnishing of any service in the State of New York.

81. Malwarebytes' unfair competition through the wrongful detection of SpyHunter and RegHunter as PUPs in MBAM constitutes deceptive and unfair trade practices.

82. Each time a consumer who has MBAM installed and running on his or her computer attempts to download and install SpyHunter or RegHunter, MBAM displays to the consumer the deceptive statement that SpyHunter and/or RegHunter is a PUP. In certain instances, MBAM even automatically blocks the download of SpyHunter and RegHunter without giving consumers the option to override the block.

83. Malwarebytes' statement that SpyHunter and RegHunter are PUPs and blocking of program downloads are materially misleading to consumers because these acts wrongly suggests that SpyHunter and RegHunter -- two legitimate and highly regarded programs -- are malicious or a threat.

84. As a result, consumers are harmed by being misled into not downloading effective

antimalware software on false pretenses and even prevented from downloading the software without their consent.

85. ESG has been and continues to be injured as a result of Malwarebytes' deceptive and unfair trade practices, including through losses of sales and a lessening of goodwill associated with its products, in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

THIRD CAUSE OF ACTION

(Tortious Interference with Contractual Relations)

86. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

87. ESG has licensed the SpyHunter and RegHunter software to numerous customers.

88. Malwarebytes knows that individuals seeking to download SpyHunter and/or RegHunter on their computer or who have SpyHunter and/or RegHunter already installed on their computer have licensed that software from ESG.

89. By displaying messages that SpyHunter and RegHunter are PUPs to MBAM users that either also had SpyHunter or RegHunter installed on their computer or that were seeking to install SpyHunter or RegHunter, and by automatically blocking the download and installation of SpyHunter and RegHunter without user consent, Malwarebytes (i) has intentionally induced users to choose not to install SpyHunter or RegHunter or to delete SpyHunter or RegHunter and (ii) has disabled SpyHunter and RegHunter programs that ESG customers have paid to install and use, causing confusion and anger among ESG's customers.

90. ESG has already begun receiving customer requests for refunds as a result of Malwarebytes' improper conduct.

91. As a result of Malwarebytes' tortious interference, ESG has been damaged at least

through loss of license fees in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

FOURTH CAUSE OF ACTION

(Tortious Interference with Business Relations)

92. ESG repeats and incorporates by reference all of the foregoing paragraphs as if fully set forth herein.

93. Certain computer users who seek to install SpyHunter and/or RegHunter are prospective customers of ESG who have not yet paid the SpyHunter or RegHunter license fee required to obtain full product functionality.

94. Malwarebytes knows that individuals seeking to install SpyHunter or RegHunter may enter into a business relationship with ESG.

95. By displaying messages that SpyHunter and RegHunter are PUPs to MBAM users that were seeking to install SpyHunter or RegHunter and by automatically blocking the download and installation of SpyHunter and RegHunter without user consent, Malwarebytes intentionally interfered with the prospective business relationship between those users and ESG by inducing the users not to complete the download and not to license SpyHunter and/or RegHunter.

96. Wrongfully and misleadingly informing users that SpyHunter and RegHunter are PUPs and automatically blocking their download and installation without user consent is an improper and illegitimate means of competition that Malwarebytes undertook for the purpose of harming ESG's business.

97. As a result of Malwarebytes' tortious interference, ESG has been damaged at least through loss of license fees in amounts that will be proven at trial but that are believed to or will exceed \$75,000, exclusive of interest and costs.

PRAYER FOR RELIEF

WHEREFORE, ESG respectfully requests that the Court enter judgment in its favor as follows:

- a. Declaring that Malwarebytes' conduct violates 15 U.S.C. § 1125(a);
- b. Declaring that Malwarebytes' conduct constitutes a violation of New York General Business Law § 349;
- c. Declaring that Malwarebytes' conduct constitutes tortious interference with contractual relations under the laws of the State of New York;
- d. Declaring that Malwarebytes' conduct constitutes tortious interference with business relations under the laws of the State of New York;
- e. Preliminarily and permanently enjoining Malwarebytes from programming MBAM to detect SpyHunter or RegHunter as PUPs and to notify users of that detection;
- f. Preliminarily and permanently enjoining Malwarebytes from programming MBAM to prevent the download and installation of SpyHunter or RegHunter;
- g. Awarding ESG damages in an amount proven at trial and believed to be in excess of \$75,000, plus interest;
- h. Awarding ESG punitive damages;
- i. Awarding ESG its attorneys' fees and costs incurred in bringing this action; and
- j. Awarding such other and further relief as the Court deems proper.

JURY TRIAL DEMANDED

ESG demands a trial by jury of all issues so triable in this action.

Dated: New York, New York
October 7, 2016

Respectfully submitted,

By: /s/ Eric A. Prager

Eric A. Prager
K&L GATES LLP
599 Lexington Avenue
New York, NY 10022
Telephone: 212.536.3900
Facsimile: 212.536.3901
eric.prager@klgates.com

&

Terry Budd
Christopher M. Verdini
Anna Shabalov
(pro hac vice applications to be filed)
K&L GATES LLP
210 Sixth Avenue
Pittsburgh, PA 15222
Telephone: 412.355.6500
Facsimile: 412.355.6501
terry.budd@klgates.com
christopher.verdini@klgates.com
anna.shabalov@klgates.com

Attorneys for Plaintiffs

Exhibit 1

Blog

Threats

Scams

MBTV

Forums



CEO ANNOUNCEMENTS | MALWAREBYTES NEWS

Malwarebytes gets tougher on PUPs

Posted October 5, 2016 by [Marcin Kleczynski](#)

Several years ago, I blogged that we would be increasing how aggressive we would be in detecting Potentially Unwanted Programs (PUPs) and our fantastic malware intelligence and research teams have delivered on that promise. Last year, we removed approximately *500 million traces of PUPs per month!*

In response, a lot of the PUP developers are making efforts to circumvent our criteria and continue distributing their damaging software to users. This is why we are getting even more critical about what we call a PUP, and what we are going to be detecting and removing from user systems.

Earlier this morning, [Malwarebytes posted a revision](#) to the criteria that we use to identify PUPs.

These changes are to help continue that fight against products and companies that scam users on the Internet.

Our efforts have resulted in making users' systems safer and more productive by removing these kinds of software. Unfortunately, we have also received a lot of negative attention from the PUP developers. This has resulted in backlash ranging from nasty blog posts and comments from fake profiles defending the products to, of course, a mountain of letters with legal letterheads demanding that we stop.

Now some people might think of this as something that would slow us down, but we see it as proof that we are making a dent in the development and distribution of PUPs.

You can learn more about our new PUP criteria [here](#).

SHARE THIS ARTICLE



COMMENTS

- *Mike Yanczysin*

Marcin: Good post, but I am wondering – during your long walks on beaches, how do you avoid the fish?

- *Uncle_AI*

Marcin, I have never understood why security companies avoided dealing directly with PUPs. They are infections and instead of being PUPs, I have always viewed them as PUSS. Instead of Potentially >> Positively Unwanted Surreptitious Software or whatever one may feel fits best. I, however, hope you not are limited by law with respect to any of the definitions you posted in the explanation. Otherwise, you have certainly bitten off a big chunk. I will recommend that all of my friends, relatives, and those who ask me about security, buy your product if I am convinced it meets the tests. Over the years I have dealt with PUSS – starting with Windows 3.0. I think that it is more insidious than the more – uh – nefarious programs, including ransomware.

- *Marcin Kleczynski*

It's complicated.

- <https://vivaldi.net/unity/profile/chas476-blog-Chas4>

I reported a big developer who has been abusing their Developer ID and has 7 pieces of Malware in their 2 macOS apps (the malware changes Safari homepage, search and adds extensions, and displays ads, does it to other browsers also) and they have been doing so for a few years now, the malware, Malwarebytes for Mac detects

RELATED ARTICLES

CEO ANNOUNCEMENTS | MALWAREBYTES NEWS

Welcome to Malwarebytes Unpacked

April 20, 2012 - Malwarebytes was founded with the community in mind. Facebook, Twitter, our forums, and countless other outlets have allowed us to communicate with you, our community. We felt a major piece was missing. Welcome to Malwarebytes Unpacked. Malwarebytes Unpacked is the official Malwarebytes blog providing you with the latest exciting news and cutting edge research directly...

[CONTINUE READING](#)

 6 Comments

CEO ANNOUNCEMENTS | MALWAREBYTES NEWS

Yesterday's Database Update Issue

April 16, 2013 - It saddens me to report that at around 3 PM PST yesterday, Malwarebytes released a definitions update that disabled thousands of computers worldwide. Within 8 minutes, the update was pulled from our servers. Immediately thereafter, users flocked to our support helpdesk and forums to ask us for a fix. I want to offer my sincere...

[CONTINUE READING](#)

 6 Comments

CEO ANNOUNCEMENTS | MALWAREBYTES NEWS

Improvements to our Updating Process

April 18, 2013 - It's been a rough week here at Malwarebytes, and I'm sure for many of you as well. We've spent the entire week focused on supporting the users affected by Monday's false positive, as well as implementing systems to prevent this type of problem from ever happening again. If you have not yet received help, please route...

[CONTINUE READING](#)

 2 Comments

[CEO ANNOUNCEMENTS](#) | [MALWAREBYTES NEWS](#)

Vulnerability Bounty Hunting In Action

July 23, 2013 - Last week, security researcher Roy Castillo posted a recount of interactions with Facebook about a bug that he had found. Will bug bounty hunting become the norm?

[CONTINUE READING](#)

 0 Comments

[CEO ANNOUNCEMENTS](#) | [MALWAREBYTES NEWS](#)

Malwarebytes Adopts Aggressive PUP Policy

July 26, 2013 - Malwarebytes Anti-Malware previously detected only harmful or deceiving PUPs. Today, We're revising our policy to include PUPs that our users find annoying or misleading.

[CONTINUE READING](#)

 10 Comments

ABOUT THE AUTHOR



Marcin Kleczynski 

CEO and Co-Founder of Malwarebytes

Likes long walks on the beach and hates fish.

CATEGORIES

101

Cybercrime

Malwarebytes news

Security world

Threat analysis

SUBSCRIBE

Email

[Subscribe to RSS](#)

TOP POSTS

Top 10 ways to secure your mobile phone

PSA: DetoxCrypto Ransomware imitating Malwarebytes

IT companies unite against illegal online hate speech

Surfacing HTA infections

PUP Friday: Nikoff Security

COMPANY

[For Home](#)

[For Business](#)

[About/Leadership](#)

[Partnerships](#)

[Success stories](#)

[Webinars](#)

NEED HELP?

[Support](#)

[Forums](#)

[Release history](#)

[User Guides](#)

LABS

[Blog](#)

[Threats](#)

[Contributors](#)

[Glossary](#)

NEWSLETTER

CONTACT

Malwarebytes

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

[EULA](#) [Privacy](#) [Terms of Service](#) © 2016 Malwarebytes

Language: **English**



Exhibit 2



New Criteria for Detecting Potentially Unwanted Products (PUPs)

Sign in to follow this

Followers 2

Started by Rubber DuckY, Wednesday at 12:04 PM

4 posts in this topic

Rubber DuckY

Marcin



Topic Starter



Root Admin

4,210 posts

Posted Wednesday at 12:04 PM

ID: 1

Hi all, we've made some changes to our PUP detection criteria. I urge you to take a look:

<https://blog.malwarebytes.com/malwarebytes-news/2016/10/malwarebytes-gets-tougher-on-pups/>

Thanks!

Aura

Bleepin' Special Ops Tech Warrior



Trusted Advisors

1,986 posts

Location: Québec, Canada

Posted Wednesday at 01:13 PM

ID: 2

Since the changes aren't highlighted, is it possible to tell us what was added/removed/edited?

Interests: Technical Support, Malware Removal & Analysis, Information Security, Gaming.

celee

Staff



Administrators

448 posts

Location: San Jose, Calif.

Posted Wednesday at 03:04 PM

ID: 3

Hi **@Aura**, according to our researchers, we're being more aggressive now i.e. Reg cleaners, optimizers, etc.

The biggest change is this criteria we use: "predominantly negative feedback or ratings from the user community"

<https://www.malwarebytes.com/pup/>

-Cecile

Aura

Bleepin' Special Ops Tech Warrior



Trusted Advisors

1,986 posts

Location: Québec, Canada

Interests: Technical Support, Malware Removal & Analysis, Information Security, Gaming.

Posted Wednesday at 03:04 PM

ID: 4

Gussed as much, thanks Cecile! 😊

Create an account or sign in to comment

You need to be a member in order to leave a comment

Create an account

Sign up for a new account in our community. It's easy!

Register a new account

Sign in

Already have an account? Sign in here.

Sign In Now

 **GO TO TOPIC LISTING**
Malwarebytes News

Recently Browsing 0 members

No registered users viewing this page.

 Home > [Announcements](#) > [Malwarebytes News](#) >

 All Activity

[New Criteria for Detecting Potentially Unwanted Products \(PUPs\)](#)

[Privacy Policy](#) [Contact Us](#)

[▲ Back to Top](#)

Malwarebytes

Community Software by Invision Power Services, Inc.

Exhibit 3



MalwareBytes

THE WAR ON PUPS
Malwarebytes going to battle with PUPs and Adware



WildFire rises from the grave as the rebranded Hades Locker



Cerber Ransomware switches to a Random Extension and Ends Database Processes



Kaspersky decrypts Ransomware from TeamXrat



A ROYAL MESS
Introducing Her Royal Highness, the Princess Locker Ransomware



The Donald Trump Ransomware tries to Build Walls around your Files



The Week in Ransomware - September 30 2016 - Princess Locker, Locky switching to ODIN, Decryptors, and More!

LATEST ARTICLES

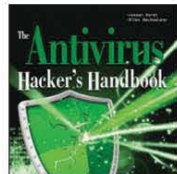


SECURITY

Tech Support Scams use new Tricks to Hold Browsers Hostage

With malvertising and shady advertisers, it is becoming all too common to run into browser based tech support scams that try to trick you into calling a remote support number. These scams continue to evolve and use new and innovative approaches to prevent users from closing their browsers.

LAWRENCE ABRAMS | OCTOBER 07, 2016 | 12:56 PM | 0

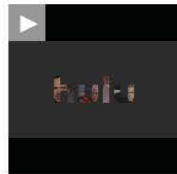


SPONSORED EBOOKS

Learn Reverse Engineering Basics with the Free Antivirus Hacker's Handbook

The Antivirus Hacker's Handbook guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense.

LAWRENCE ABRAMS | OCTOBER 06, 2016 | 01:48 PM | 1



SPONSORED

This won't last - at \$5.99/month, all the shows and movies are yours for less

Get ready for fall watching with Hulu.

AD BY HULU



SECURITY

Malwarebytes going to battle with PUPs and Adware

Today, Marcin Kleczynski, the Chief Executive Officer of Malwarebytes, announced in a blog post that Malwarebytes is going to battle with PUPs (Potentially Unwanted Programs) and thus the companies that make them.

LAWRENCE ABRAMS | OCTOBER 05, 2016 | 07:31 PM | 6



SECURITY

WildFire rises from the grave as the rebranded Hades Locker

The WildFire Locker ransomware has risen from the dead and rebranded itself using the name of Hades Locker. Its previous incarnation was shutdown after authorities seized the command & control servers. Unfortunately, the ransomware developers were not apprehended and have been biding their time before releasing a new ransomware.

LAWRENCE ABRAMS | OCTOBER 05, 2016 | 05:39 PM | 2



SECURITY

SPONSORED DEALS

New Deal: 96% off a Xamarin Cross Platform Development Bundle

This online course bundle contains 6 courses with over 57 hours in training on how to use Xamarin to create mobile apps. These courses would be normally priced at \$1,046.00 if bought together, but have been discounted 96% to \$35. Please note that certificates of completion will not be provided.

LAWRENCE ABRAMS | OCTOBER 04, 2016 | 05:20 PM | 0



SECURITY

Medical Community... (truncated)

THE #1 MANAGED CLOUD COMPANY

- Certified in AWS, Microsoft Azure, OpenStack, and VMware
- Serving over 1/2 of the Fortune 100
- 3,000+ cloud experts accessible 24x7x365

rackspace | YOUR CLOUDS. OUR EXPERTISE.

LEARN MORE

LATEST FORUM TOPICS

CORRUPT SYSTEM FILES
passacaglia in Windows 7

Hp power supply on ASROCK motherboard
alexcomputer500 in Internal Hardware

BSOD problem
Atoz44 in Windows Crashes, BSOD, and Hangs Help and Support

NEWSLETTER SIGN UP

To receive periodic updates and news from BleepingComputer, please use the form below.

Email Address...

Submit

LATEST VIRUS REMOVAL GUIDES

Web-start.org Browser Hijacker Removal Guide
LAWRENCE ABRAMS | READ 211 TIMES

Tech-connect.biz Browser Hijacker Removal Guide
LAWRENCE ABRAMS | READ 641 TIMES

Isanalyze.com Browser Redirect Removal
LAWRENCE ABRAMS | READ 513 TIMES



Hacked Steam Accounts Spreading Remote Access Trojan
 A Remote Access Trojan is being distributed through hacked Steam Accounts sending SPAM that contain download links to the Trojan. Once the Trojan is installed, it will allow the attacker to gain full access to the computer and all the files contained on it.

LAWRENCE ABRAMS SEPTEMBER 30, 2016 08:26 PM 5



GOOGLE, SECURITY
Google Chrome 53.0.2785.143 m fixes Remote Code Execution Vulnerabilities

Version 53.0.2785.143 m of Google Chrome was released today that fixes for 2 remote code execution vulnerabilities that were submitted to Pwnium; Remote code execution vulnerabilities are considered critical as it could allow attackers and malicious web sites to remotely execute any command they wish on an affected computer.

LAWRENCE ABRAMS SEPTEMBER 30, 2016 01:51 PM 3



SECURITY
The Week in Ransomware - September 30 2016 - Princess Locker, Locky switching to ODIN, Decryptors, and More!

This week really picked up when it comes to ransomware news. Lots of new variants, new decryptors, and new ransomware. Of particular interest this week is Locky switching to using the ODIN extension and for security companies releasing a lot of decryptors this week.

LAWRENCE ABRAMS SEPTEMBER 30, 2016 11:20 AM 0



SPONSORED DEALS
New Deal: 98% off the The Ultimate Software Testing Bundle

This online course bundle contains 11 courses with over 84 hours in training on how to be a software tester. These courses would be normally priced at \$3,300.00 if bought together, but have been discounted 98% to \$59. Please note that certificates of completion will be provided, but no vouchers for any exams come with this deal.

LAWRENCE ABRAMS SEPTEMBER 30, 2016 09:00 AM 0



SECURITY
Kaspersky decrypts Ransomware from TeamXrat

Kaspersky posted a great article about their TeamXrat Ransomware analysis and how they were able to create a decryptor for its victims. Reported back in mid September in our forums, I and other security researchers were never able to find an actual sample of the malware.

LAWRENCE ABRAMS SEPTEMBER 29, 2016 05:23 PM 1



SECURITY
Introducing Her Royal Highness, the Princess Locker Ransomware

Today we bring you Princess Locker; the ransomware only royalty could love. First discovered by Michael Gillespie, Princess Locker encrypts a victim's data and then demands a hefty ransom amount of 3 bitcoins, or approximately \$1,800 USD, to purchase a decryptor.

LAWRENCE ABRAMS SEPTEMBER 28, 2016 06:42 PM 5

1 2 3 4 5 > >

VIEW MORE

Start your 30-day trial

START YOUR MEETING

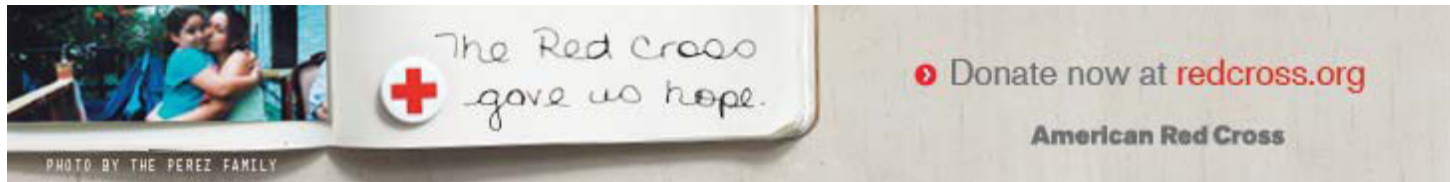
LATEST DOWNLOADS

	Windows Repair (All In One) Version: 3.9.12	844,674 DOWNLOADS
	VoodooShield Version: NA	13,924 DOWNLOADS
	VirtualBox for Windows Version: 5.1.6	12,728 DOWNLOADS
	Malwarebytes Anti-Ransomware Version: 0.9.17.661	166,982 DOWNLOADS
	Hardware Identify Version: 2.1.1	32,145 DOWNLOADS

FEEL EVERY WORD

DOWNLOAD YOUR FIRST AUDIOBOOK WITH A 30-DAY FREE TRIAL

Exhibit 4



Home > News > Security > Malwarebytes going to battle with PUPs and Adware

106

6

Malwarebytes going to battle with PUPs and Adware

By Lawrence Abrams

October 5, 2016

07:31 PM

6



Today, Marcin Kleczynski, the Chief Executive Officer of Malwarebytes, announced in a blog post that Malwarebytes is going to battle with PUPs (Potentially Unwanted Programs) and thus the companies that make them. With adware and PUP programs getting out of hand and many of them exhibiting malware-like characteristics, Malwarebytes had previously decided to be more aggressive against adware and PUP programs.

Unfortunately, over time the PUP developers and distributors created more aggressive distribution methods and new techniques to avoid security programs that detect them. Due to

this, Malwarebytes has updated their PUP criteria to be even more aggressive on how they categorize PUPs and target them.

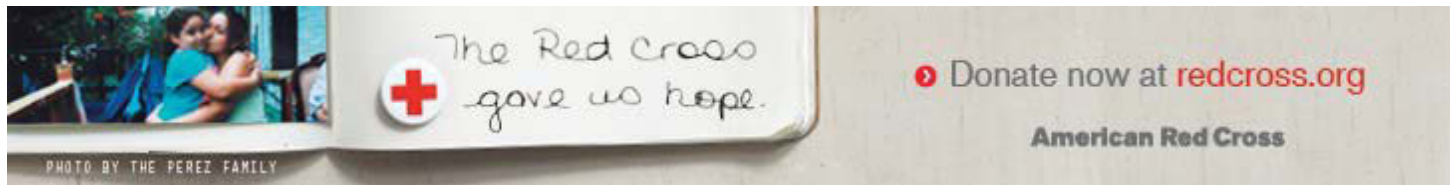
Based on Malwarebyte's updated PUP criteria, starting today their products will detect programs that exhibit the following behavior:

- obtrusive, misleading, or deceptive advertising, branding, or search practices
- excessive or deceptive distribution, affiliate or opt-out bundling practices
- aggressive or deceptive behavior especially surrounding purchasing or licensing
- unwarranted, unnecessary, excessive, illegitimate, or deceptive modifications of system settings or configuration (including browser settings and toolbars)
- difficulty uninstalling or removing the software
- predominantly negative feedback or ratings from the user community
- diminishes user experience
- other practices generally accepted as riskware, scareware, adware, greyware, or otherwise commonly unwanted software by the user community

As I have said numerous times, PUP distributors and developers are getting out of control and need to be stopped. They are creating adware and PUPs that are not only distributed in a deceptive manner, but in many cases also include characteristics that are only found in computer infections. These characteristics could include backdoors, rootkits, and persistence techniques that make the programs difficult to remove.

Though anyone with common sense would say that these programs should be considered malware, instead they are classified as PUPs, or not detected at all, because security companies are afraid of legal threats from the PUP developers. In fact, the term PUP, or Potentially Unwated Program, was created to avoid calling these programs malware and to avoid legal consequences of doing so.

With that said, kudos to Malwarebytes for taking a stand against aggressive adware and PUPs.



ADWARE MALWAREBYTES PUP

LAWRENCE ABRAMS

Lawrence Abrams is the creator and owner of BleepingComputer.com. Lawrence's area of expertise includes malware removal and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

← PREVIOUS ARTICLE	NEXT ARTICLE →
------------------------------------	--------------------------------

Comments



TheJokerz - 1 day ago

Go Malwarebytes!! Thanks for the share!



Angoid - 1 day ago

What would be really strange is if anyone can think of any other anti-malware program that fits any of those descriptions not that I can think of one of course :)



Gorbulan - 1 day ago

GOOD!



Tonst3r - 1 day ago

THANK GOD!! It's about time SOMEONE took a stand on this BS! PuP's are malware by every definition and I've been over their nonsense for years!!!!



kenhall5551 - 22 hours ago

Bundled software is a real problem for many "free" programs and apps. If they made it clear and easy to "opt-out" of these bundled offers, they might be O.K. Nothing wrong with trying to make a buck, but to be deceptive about it or to add new "features" to your device without your consent is just plain wrong.



Bambinoo - 2 hours ago

Excellent...thumbs up MWB!

Post a Comment

Community Rules

You need to login in order to post a comment

Login

Not a member yet? Register Now

You may also like



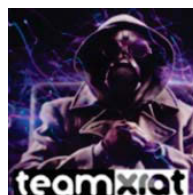
WILDFIRE
RISES FROM
THE GRAVE AS
THE
REBRANDED
HADES
LOCKER



CERBER
RANSOMWAR
E SWITCHES
TO A RANDOM
EXTENSION
AND ENDS
DATABASE
PROCESSES



HACKED
STEAM
ACCOUNTS
SPREADING
REMOTE
ACCESS
TROJAN



KASPERSKY
DECRYPTS
RANSOMWAR
E FROM
TEAMXRAT

ROCK YOUR NEW PHONE **BEST BUY**

SAVE \$70

On Sony Extra Bass
Wireless Headphones

[Shop Now](#)



[See Details](#)

LATEST FORUM

TOPICS

Hp power supply on
ASROCK
motherboard
alexcomputer500 in Internal
Hardware

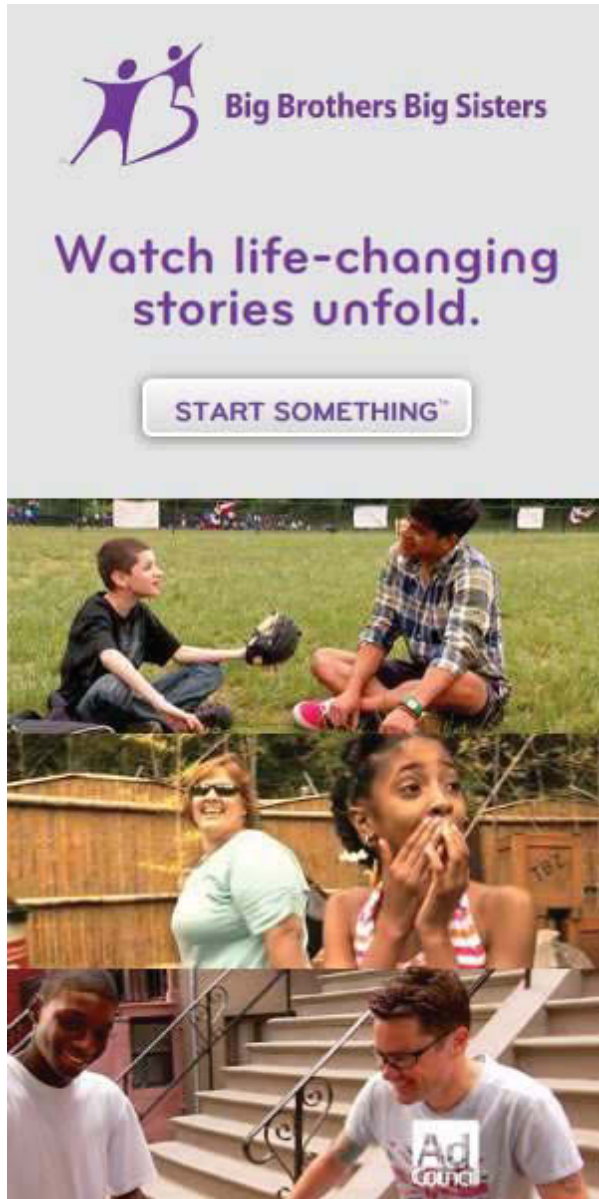
BSOD problem
Atoz44 in Windows Crashes,
BSOD, and Hangs Help and
Support

Seeing Traffic from
195.22.26.248. Not
sure if this is bad.
Lerxst23 in Am I infected?
What do I do?

**NEWSLETTER
SIGN UP**

To receive
periodic updates
and news from
BleepingComputer,
please use the
form below.

Submit



LATEST

DOWNLOADS

	<p>Windows Repair (All In One)</p>
<p>Version: 3.9.12</p>	
<p>844,667 DOWNLOADS</p>	
	<p>VoodooShield</p>
<p>Version: NA</p>	
<p>13,924 DOWNLOADS</p>	



VirtualBox for Windows

Version: 5.1.6

12,728
DOWNLOADS



Malwarebytes Anti- Ransomware

Version:
0.9.17.661

166,981
DOWNLOADS



Hardware Identify

Version: 2.1.1

32,145
DOWNLOADS

G Suite

LEARN MORE

PHOTO BY THE PEREZ FAMILY

The Red Cross gave us hope.

Donate now at redcross.org

American Red Cross

NEWSLETTER SIGN UP

SUBMIT

Follow us:    

MAIN SECTIONS

[News](#)

[Downloads](#)

[Virus Removal Guides](#)

[Tutorials](#)

[Startup Database](#)

[Uninstall Database](#)

[File Database](#)

[Glossary](#)

COMMUNITY

[Forums](#)

[Forum Rules](#)

[Chat](#)

USEFUL RESOURCES

[Welcome Guide](#)

[Sitemap](#)

COMPANY

[About BleepingComputer](#)

[Contact Us](#)

[Advertising](#)

[Write for BleepingComputer](#)

[Social & Feeds](#)

[Changelog](#)

[User Agreement - Privacy Policy](#)

Copyright @ 2003 - 2016 **Bleeping Computer**[®] LLC - All Rights Reserved

Exhibit 5



RJ Singh

3rd

Regional Vice President at Malwarebytes

Greater New York City Area | Computer & Network Security

Previous Zscaler Inc., NitroSecurity (Intel Security), Q1 Labs (IBM Security)

Education NYU

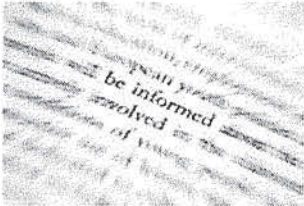
Send RJ InMail

500+ connections

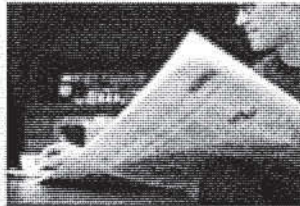
https://www.linkedin.com/in/singhrj

Posts

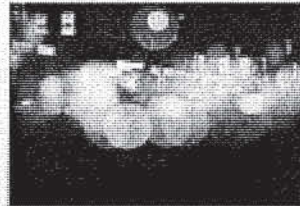
Published by RJ



Ransomware growing and damaging across all...
September 15, 2016



Major institutional funding comes as...
January 22, 2016



Malwarebytes Tops \$100 Million Run-Rate
December 14, 2015

Background

Summary

RJ Singh is a seasoned sales leader with long history of successful coach and player roles at multiple technology start-ups. He shares deep and wide knowledge of technology industry and it's innovation that empowers people and businesses globally.

He has spent 25 plus years performing active roles in sales leadership, business development, partner relationships, and consulting services at variety of fast-growing technology companies and start-ups resulting in high growth revenue and increased shareholder value.

RJ leads as Regional Vice President at Malwarebytes. Previously, RJ led as Regional Sales Director at Zscaler, Sales Director at NitroSecurity (acquired by Intel Security) and Director of Eastern Sales at Q1 Labs (acquired by IBM). At these companies, RJ was instrumental in building business from ground-up, recruiting right channel partners and leading sales team to rapidly win high profile customers in key vertical markets. RJ spent eight years at Protegrity where he joined as Sales Director and rose through the ranks to lead North American sales team. Prior to this, RJ had successful careers at Memco (acquired by CA) and Trusted Information Systems (acquired by Network Associates).

RJ holds M.S. and B.S. degrees in Computer Science and double minors in Mathematics and Business Administration from Northern Illinois University. RJ studied Investment Banking and related topics at

Ad

Chris, picture yourself at Malwarebytes



Senior Software Engineer

Clearwater, Florida

View now

People Also Viewed



Thomas Miller
SVP Sales at Malwarebytes



Brian Henger
Regional Vice President - Central US at Malwarebytes



Roger Cobb
Vice President of Worldwide Channel Sales at Malwarebytes



Marcin Kleczynski
CEO at Malwarebytes



Linh Mings
Director, Enterprise Sales at Malwarebytes



Anthony O'Mara
Vice President EMEA at Malwarebytes



Peter Brownell
Regional Vice President-West at Malwarebytes

Rebecca Kline
CMO at Malwarebytes

Wendy Sanchez
Regional Sales Manager- Southeast at Malwarebytes

Monty Venkersammy
Vice President of Business Development at Malwarebytes



People also viewed
Thomas Miller SVP Sales at Malwarebytes

 Experience

Regional Vice President

Malwarebytes

September 2015 – Present (1 year 2 months) | Greater New York City Area

Malwarebytes provides software designed to protect consumers and businesses against malicious threats that consistently escape detection by other antivirus solutions. Malwarebytes Anti-Malware Premium the company's flagship product, employs a highly advanced behavior-based detection engine that has removed more than five billion malicious threats from computers worldwide. More than 50,000 SMBs and enterprise businesses worldwide trust Malwarebytes to protect their data. Founded in 2008, the self-funded company is headquartered in California, operates offices in Europe, and employs a global team of researchers and experts. For more information, please visit us at www.malwarebytes.org.

Regional Sales Director - New York

Zscaler Inc.

January 2013 – August 2015 (2 years 8 months) | Greater New York City Area

Zscaler Cloud Security Solution delivers unified, carrier-grade Internet security, advanced persistent threat (APT) protection, data loss prevention, SSL decryption, traffic shaping, policy management and threat intelligence – all without the need for on-premise hardware, appliances or software.

- Impacted revenue within 100 days closing 4 deals in excess of million dollars.
- Recognized as "Top Global Sales" during Zscaler 2013-2014 Third-QTR Review..
- Finished Fiscal 2013-2014 strong and won "Presidents Club" at Zscaler Annual Awards.
- Recognized as "Top USA Sales Performer" during Zscaler 2014-2015 First-QTR Review.
- Finished Top-3 in Fiscal 2014-2015 and won Presidents Club at Zscaler Annual Awards.
- Increased ARR (Annual Recurring Revenue) five-fold during the tenure at the company.

▼ 12 recommendations, including:

Mike Basoah

Experienced Corporate Marketing & De...

I worked with RJ at Zscaler and it was an absolute pleasure ! He is the consummate sales professional. He has a great... View ↓

Diederik Klijn

Named Account Manager at Zscaler

RJ is a person that understands what it takes to start a company in a certain region. He will focus on creating revenue. We... View ↓

10 more recommendations ↓

Sales Director

NitroSecurity (Intel Security)

August 2010 – December 2012 (2 years 5 months)

- Intel / McAfee acquired NitroSecurity.
- Technology sold included Log Mgmt, SIEM, IDS/IPS, Database and Application Monitoring.
- Sold over \$200K revenue within 60 days of joining the company.
- Tripled number of customers in my region within 12 months.
- Achieved 100% quota every year.
- Actively participated in growing company revenue from \$15M to \$25M in 16 months.
- Actively participated in taking company from Niche player to Leader in Gartner Quadrant.
- Put company on the map with Financials, HealthCare, Pharma, NJ State and NYC agencies.
- Recruited and trained half a dozen VARs to independently sell Nitro solution.

▼ 2 recommendations

Kevin Norr

Security - Partner Development Mgr. - N...

RJ is a very professional sales person and is consultative in his approach to customers needs. He also has very strong... View ↓

Pablo "Paul" Lupo

Manager Sales & Support

I really enjoyed working with RJ during our time at NitroSecurity Inc together. His knowledge of the region, the accounts... View ↓

Director of Eastern Area Sales


Q1 Labs (IBM Security)

August 2007 – July 2010 (3 years)

- IBM acquired Q1 Labs.
- Technology sold included Log Mgmt, SIEM and Application Monitoring
- Doubled number of customers in my region within 90 days – a company first.


Justin Stark

Justin can introduce you to someone who knows RJ →



RJ Singh

People also viewed



Thomas Miller SVP Sales at Malwarebytes

- Recruited and trained a dozen VARs to independently sell Q1 Labs' solution.
- Teamed with billion dollar OEM partners to win major accounts.
- Put company on the map with Federal, NYC financials, State and City agencies.
- Actively participated in taking company from Niche player to Leader in Gartner Quadrant
- Actively participated in growing company revenue from \$5M to \$20M in two years.
- Won 5 major category Awards and President's Club in 24 months – a company first.

Head of North American Sales

Protegrity

May 1999 – July 2007 (8 years 3 months)

- Technology sold included Database and File Level Encryption.
- Sold first beach head accounts at leading Financial, eCommerce and Consumer markets.
- Achieved 100% revenue and corporate objectives year after year.
- Increased revenue 10 fold (\$300K to \$3M) in 36 months.
- Executed Sales and Business Development Strategies to drive revenue.
- Built 12 members senior team throughout U.S. and Canada over the years.
- Built and executed channel strategy successfully for the company.
- Multiple Awards and Recognitions.

5 recommendations, including:

Tobias Brink

Head MDU and business city network a...

My working experience after college started at Protegrity. There I had the pleasure having RJ as my boss. He proved to be... [View ↓](#)

Tamojit Das

Sr. Managing Consultant at IBM

RJ is a very rare talent, specially when it comes to selling. I had the pleasure of working with RJ for several years at... [View ↓](#)

[3 more recommendations ↓](#)

Director of Systems Engineering

CA Technologies

May 1995 – April 1999 (4 years)

- Technology sold included Root and App Control, Security Audit, SSO and Firewall solutions.
- CA acquired Platinum which acquired Memco which acquired NIT.
- Network Associates acquired TIS (Trusted Information Systems) which acquired Haytack Labs.
- Led 3 member team as pre-sales and post-sales resource to win Fortune 1000 clients.
- Achieved over 100% team sales objectives.

Scientific Computing Programmer

Northern Illinois University

May 1989 – April 1995 (6 years)

- Prepared and taught TCP/IP Internet technologies to Faculty and Graduate Students.
- Installed, maintained, and provided user support for Internet client/server TCP/IP systems.
- Wrote and published various technical articles on University Computing News publication.
- Provided technical leadership to 3 graduate students.



Volunteer Experience & Causes

Founder / Co-ordinator

TND Foundation


1992 – 2008 (16 years) | Social Services

Opportunities RJ is looking for:

- Joining a nonprofit board

Causes RJ cares about:

- Arts and Culture
- Children
- Economic Empowerment
- Education


People also viewed
×

Thomas Miller SVP Sales at Malwarebytes
 >

Organizations RJ supports:

- Peace Corps

 Education

NYU

Graduate Studies, Investment Banking
2008 – 2009

Activities and Societies: Venture Capital, Private Equity and Hedge Fund Seminars

Northern Illinois University

Master of Science (M.S.), Computer Systems Networking and Telecommunications
1989 – 1991

Activities and Societies: International Student Organization

Northern Illinois University

Bachelor of Science (B.S.), Computer Science, Mathematics and Business Administrations
1985 – 1989

Activities and Societies: International Student Organization, The ViewPoints Publication

The Air Force School Academy


Pre-College, Physics, Chemistry, Mathematics, English and Engineering Drawing
1983 – 1985

Activities and Societies: Music Group

St. Xavier's School


High School
1973 – 1983

Activities and Societies: Elocution Contests, Essay Competition, Spelling Contests, One-Act Play Festivals, Music Club

 Courses


Independent Coursework

- Investment Banking, IPO, M&A, Hedge Funds and Corporate Finance
- Enterprise Sales and Marketing Strategies
- Stocks & Bonds Investment Seminars
- REITS for profit Seminars
- Business Risk and Information Security
- TCP/IP Systems and Network Administration
- Microsoft Certified Systems Engineer
- Novell Certified Systems Engineer
- MVS System and Applications Administration

 Skills

Top Skills

People also viewed ×

 **Thomas Miller** SVP Sales at Malwarebytes ➤

- 26 Network Security
- 19 Enterprise Software
- 16 Pre-sales
- 16 Channel Partners
- 14 Business Development
- 14 Strategic Partnerships
- 11 Encryption
- 11 SaaS

RJ also knows about...

- 9 Sales Process
- 8 Solution Selling
- 7 Vulnerability Management
- 7 DLP
- 7 Start-ups
- 7 Firewalls
- 7 Strategy
- 6 Cloud Security
- 6 SIEM
- 6 Data Security
- 6 Sales Management
- 6 IPS
- 6 Professional Services
- 5 Sales Enablement
- 5 Business Alliances
- See 17+ >



Languages

English

Hindi

Nepali

Additional Info

• Interests

I am a voracious broad reader and observer of global businesses, world history, capitalism, current events, and strategic innovations. These interests and knowledge are building blocks to my professional skills adding strong profitable value to the success of my employer.

• Personal Details

Marital Status Married



Certifications

MCSE
Microsoft

CNE
Novell

WWW and TCP/IP Networks
Netscape



People also viewed ×
Thomas Miller SVP Sales at
Malwarebytes >

Recommendations

Received (19) Given (3)

Regional Sales Director - New York

Zscaler Inc.



Mike Basoah

Experienced Corporate Marketing & Demand Generation Executive. Building & Accelerating Revenue Growth

I worked with RJ at Zscaler and it was an absolute pleasure ! He is the consummate sales professional. He has a great ability to listen and focus on the customer needs, build relationships at all levels, marshal all internal resources to home in on the customer needs, is dedicated, and very hard working. At the end of the day he is focused on the end result and always hits... **more**

October 14, 2015, Mike worked with RJ at Zscaler Inc.



Diederik Klijn

Named Account Manager at Zscaler

RJ is a person that understands what it takes to start a company in a certain region. He will focus on creating revenue. We worked together on several deals, which was a pleasure.

October 11, 2015, Diederik worked with RJ at Zscaler Inc.



Vincent Vermeulen

Sr. Security Architect at Comodo

RJ is a consummate sales professional and top performer. Working as his technical resource was a pleasure, as he was always prepared, prompt and poised to bring the best solution to his clients.

September 29, 2015, Vincent worked directly with RJ at Zscaler Inc.



Jean-David Faurie

Director of Strategic Accounts

RJ has always overachieved and is customer driven senior sales professional. He has demonstrated his abilities in maintaining relationships with clients resulting in add-on sales and renewals. He has always a positive attitude. He is definitely an incredible sales leader for any organization. I would definitely recommend him. It was pleasure working with him and would... **more**

September 25, 2015, Jean-David worked with RJ at Zscaler Inc.



Matt Drugan

National Channel Manager

RJ is high performance oriented sales leader. A team player who leads by example, RJ works very well with employees, customers and partners alike. He is extremely valuable asset in any company.

September 23, 2015, Matt worked with RJ at Zscaler Inc.

See More


 People also viewed
Thomas Miller SVP Sales at Malwarebytes

Exhibit 6

Malwarebytes

Click for Full Company Profile (companyprofile.php?cid=12079)

Senior Sales Engineer - NY (Remote)

Investors :

[Highland Capital Partners \(investorprofile.php?cid=168\)](http://investorprofile.php?cid=168) | [Highland Europe \(investorprofile.php?cid=15185\)](http://investorprofile.php?cid=15185)


Location :

10 Almaden Blvd
Tenth Floor
San Jose, CA 95138

Overview :

Malwarebytes is community. Malwarebytes is technology. Malwarebytes is a belief that every person has a fundamental right to a malware-free existence.f

[Hide company information](#)

Send to Friend: 

Job Details



Senior Sales Engineer - NY (Remote)

New York, US

Malwarebytes - Full-Time | Job date : 09-21-2016

Description

Who We Are

Malwarebytes is a leading provider of anti-malware software solutions to consumers and businesses alike. Our flagship technologies and products protect more than 120 million computers around the world! In the highly competitive security software sector, we have earned an international reputation for our rapid response and high success rate in combating new malicious threats. We're growing fast and we need your help!

Who We Need

As a Malwarebytes Senior Sales Engineer you and your Regional Sales Manager will be responsible for presenting Malwarebytes security solution to prospective customers, creating and delivering demonstrations of the products, gathering customer technical requirements, creating evaluation test plans with customers, and then managing the evaluation process to a successful conclusion. You will work closely with customers as their primary point of contact for feedback and resolution of issues, and will be the customers' advocate for issues that require assistance from the HQ Customer Success team. You will provide feedback to the Product Management team on new feature requests and product enhancements from your customer base. Extensive domestic travel within the territory is required.

What You'll Do

We are looking for a skilled Security Engineer to analyze software designs and implementations from a security perspective, and identify and resolve security issues. You will include the appropriate security analysis, defences and countermeasures at each phase of the software development lifecycle, to result in robust and reliable software.

Skills You'll Need to Have

Identifies current and future customer service requirements by establishing personal rapport with potential and actual customers and other persons in a position to understand service requirements. Provides product, service, or equipment technical and engineering information by answering questions and requests.

Establishes new accounts and services accounts by identifying potential customers; planning and organizing sales call schedule.

Prepares cost estimates by studying blueprints, plans, and related customer documents; consulting with engineers, architects, and other professional and technical personnel.

Gains customer acceptance by explaining or demonstrating cost reductions and operations improvements.

Develops customer's staff by providing technical information and training.

Complies with federal, state, and local legal requirements by studying existing and new legislation; anticipating future legislation; advising customer on product, service, or equipment adherence to requirements; advising customer on needed actions.

Prepares sales engineering reports by collecting, analyzing, and summarizing sales information and engineering and application trends.

Maintains professional and technical knowledge by attending educational workshops; reviewing professional publications; establishing personal networks; participating in professional societies.

Contributes to sales engineering effectiveness by identifying short-term and long-range issues that must be addressed; providing information and commentary pertinent to deliberations;

recommending options and courses of action; implementing directives.

Contributes to team effort by accomplishing related results as needed.

Who We Are

Malwarebytes is a leading provider of anti-malware software solutions to consumers and businesses alike. Our flagship technologies and products protect more than 120 million computers around the world! In the highly competitive security software sector, we have earned an international reputation for our rapid response and high success rate in combating new malicious threats. We're growing fast and we need your help!

Who We Need

Malwarebytes is growing rapidly. We are engaged in a constant, escalating fight against malware writers who play by no rules. As a result, we face challenges requiring more than just intelligence and technical fluency. Of equal importance are flexibility, independence, a drive to learn new skills, and a creative approach to problem-solving. We're not looking for people who know all the answers; we want people who can create solutions.

What You'll Do

Work in an agile development environment on our Mac OS product, collaborating with the team to deliver quality software iteratively

Convert requirements into test cases and help define use case scenarios based on product and domain knowledge

Find defects according to test case execution steps. Provide specific steps to reproduce reported problems

Work with developers to debug and identify defect root cause. Independently perform the testing effort for a component of the product

Plan and scope the test strategy for a small feature or component of a feature

Simulate customer environments and work with Customer Facing Teams to perform escalation root cause analysis and convert them to test cases

Design and implement automated testing for product components

Skills You'll Need to Have

Experience on installation and configuration of Mac OSx 10.7 or higher

Experience with scripting languages like Python/BASH/Perl or object-oriented programming languages like Java/C++ is required

Experience with Malware and Adware removal Testing on a Mac is a strong plus

Knowledge of how to apply test automation for efficient testing practices is preferred

Knowledge about various types Consumer and Enterprise level Mac AV Products is a big plus

2-4 years of software industry experience with hands-on QA experience

BS/MS in Computer Science or a related technical discipline, or equivalent work experience is required

Experience working in a fast-paced, cross-geography engineering environment

Understanding of QA methodologies, best practices and terminology

Strong technical, analytical and problem-solving skills

Able to work independently and as part of a team

Excellent verbal and written communication skills

What We Offer

An opportunity to do something great for yourself and the world

A great work environment that supports growth and development

Competitive compensation and benefit packages

401(k) matching program

Open time off policy

Stocked kitchen with healthy (and some unhealthy) drinks, snacks, fruit and lunch options

A company who enjoys having fun; holiday and summer parties, annual global company off-site, experienced a private Star Wars pre-opening day viewing and lots of other great stuff

[APPLY NOW \(JOBAPPLY.PHP?JOBID=551201\)](#)

Disclaimer: Local Candidates Only

Jobseekers

[Register Now \(register.php\)](#)

[Search Jobs \(job_search.php\)](#)

[Login \(login.php\)](#)

[Contact us \(contactus.php\)](#)

Information

[About Us \(aboutus.php\)](#)

[Advertise With Us \(mailto:sales@ventureloop.com\)](mailto:sales@ventureloop.com)

[Terms & Conditions \(termsofservice.php\)](#)

[Privacy Policy \(privacy.php\)](#)

[Help \(help.php\)](#)

Contact Us

✉ [help@ventureloop.com \(mailto:help@ventureloop.com\)](mailto:help@ventureloop.com)

Get the latest startup news in your email box:

VentureLoop Startup Newsletter



Enter Your Email Here

©2007-2016 VentureLoop. All Rights Reserved.



Exhibit 7

PUP Reconsideration Information

How do we identify potentially unwanted software?

Analyzing and categorizing potentially unwanted software is a complex problem. Developers of potentially unwanted software rapidly evolve their products. Some even contain a few characteristics that resemble legitimate software to mask the unwanted functionality. It's an on-going process, and we work hard to identify common behaviors that help provide you the highest level of protection. In some cases, where the behavior is questionable, we will list the application even if it does not neatly fit into the listed criteria. In other words, we use our judgment.

While we highlight potentially unwanted programs, you then make a choice in the exclusions list and select what you want to keep or remove.

Here are some of the criteria we use:

- obtrusive, misleading, or deceptive advertising, branding, or search practices
- excessive or deceptive distribution, affiliate or opt-out bundling practices
- aggressive or deceptive behavior especially surrounding purchasing or licensing
- unwarranted, unnecessary, excessive, illegitimate, or deceptive modifications of system settings or configuration (including browser settings and toolbars)
- difficulty uninstalling or removing the software
- predominantly negative feedback or ratings from the user community
- diminishes user experience
- other practices generally accepted as riskware, scareware, adware, greyware, or otherwise commonly unwanted software by the user community

To keep our analysis useful, we regularly update our software with applications meeting our criteria. While we work hard not to, sometimes we get it wrong. If you want to submit your application for reconsideration, please email legal@malwarebytes.com.

For the most part, publishers of potentially unwanted software are not hobbyists. They are sophisticated businesses with big budgets and infrastructure. Given this, new forms of potentially unwanted software frequently emerge and proliferate. To respond promptly, we reserve the right to adjust, expand and update our criteria without prior notice or announcements.



NEWSLETTER

SUBMIT

CONTACT

Malwarebytes

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

[EULA](#) [Privacy](#) [Terms of Service](#) © 2016 Malwarebytes

Language: English

