

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X	
ENIGMA SOFTWARE GROUP USA, LLC,	:
	:
Plaintiff,	:
	:
-against-	:
	:
BLEEPING COMPUTER LLC and	:
DOES 1-10,	:
	:
Defendants.	:
-----X	

Case No.: 1:16-cv-00057-PAE

**DEFENDANT’S ANSWER, AFFIRMATIVE DEFENSES AND COUNTERCLAIMS IN
RESPONSE TO PLAINTIFF’S SECOND AMENDED COMPLAINT**

Defendant Bleeping Computer, LLC (“Bleeping” or “Defendant”), by and through undersigned counsel, hereby answers the allegations of the Second Amended Complaint (the “Complaint”), filed by Plaintiff Enigma Software Group USA, LLC (“Plaintiff” or “Enigma”), paragraph by corresponding paragraph, as follows:

1. Admitted Plaintiff seeks the relief sought but denied it is entitled to any relief.
2. Admitted Bleeping owns the domain name referenced and operates certain functions on the associated website while other functions are performed by volunteers, and that some of the statements referenced have appeared on the website, otherwise denied.
3. Admitted that some of the statements asserted have appeared on Bleeping’s website, otherwise denied.
4. Deny knowledge or information sufficient to form a belief as to the state of mind of consumers as referenced, admitted that Bleeping’s website if publicly available to be accessed by anyone, otherwise denied.
5. Admitted that Bleeping’s website provides information regarding anti-malware

software, otherwise deny knowledge or information as to what might be most important to particular users and otherwise denied.

6. Deny knowledge or information as to the state of mind of users, otherwise denied.

7. Admitted that Bleeping receives commissions on certain sales of certain anti-malware products, including Plaintiff's products, otherwise denied.

8. Admitted that Bleeping has received commissions for the sale of software products through hyperlinks, including commissions received from Plaintiff, otherwise denied.

9. Denied.

10. Admitted that Bleeping receives commissions from sales of Malwarebytes and other software companies, including Plaintiff; deny knowledge or information sufficient to form a belief as to the true competitive relationship between the parties referenced, otherwise denied.

11. Denied that Bleeping does not receive and has not received commission from Plaintiff and otherwise denied.

12. Denied.

13. Denied.

14. Denied.

15. Denied.

Parties

16. Admitted that Plaintiff alleges it is a Florida limited liability company, otherwise deny knowledge or information sufficient to form a belief as to the remaining allegations.

17. Admitted.

18. Denied.

Jurisdiction & Venue

19. The allegations of paragraph 19 consist of jurisdictional allegations to which no response is required.

20. Denied.

21. Admitted that Enigma markets computer security products, otherwise deny knowledge or information sufficient to form a belief as to the remaining allegations.

22. Admit the FTC has published the statements asserted.

23. Deny knowledge or information sufficient to form a belief.

24. Admitted that Plaintiff markets SpyHunter, otherwise deny knowledge or information sufficient to form a belief as to the remaining allegations.

25. Admitted that Plaintiff markets and sells SpyHunter over the Internet, through various websites, otherwise deny knowledge or information sufficient to form a belief as to the remaining allegations.

26. Deny knowledge or information sufficient to form a belief.

27. Deny knowledge or information sufficient to form a belief.

28. Deny knowledge or information sufficient to form a belief.

29. Denied.

30. Deny knowledge or information sufficient to form a belief.

31. Deny knowledge or information sufficient to form a belief.

32. Admitted that Bleeping has stated that its owner and certain volunteers are adept at certain computer security technical and operational matters, otherwise denied.

33. Denied.

34. Admitted that Bleeping owns the domain name referenced and operates certain functions on the associated website while other functions are performed by volunteers, and that

the website contains the sections referenced, otherwise denied.

35. Admitted that Bleeping has generated revenue through hyperlinks on its website, including revenue paid by Plaintiff.

36. Admitted that Bleeping has participated in the program offered and utilized by SkimLinks.

37. Admitted that Bleeping has participated in the program offered and utilized by SkimLinks, and that commissions have been paid for purchases made on Bleeping's website through said program, including commissions paid by Plaintiff.

38. Denied.

39. Admitted that Bleeping's website contains the quoted language, but deny Plaintiff's characterization of same, otherwise denied.

40. Admitted that Bleeping's website contains the quoted language, but deny Plaintiff's characterization of same, otherwise denied.

41. Admitted that the Bleeping website utilizes the Skimlinks program in the forums section of the Bleeping website, otherwise denied.

42. Admitted that Bleeping's website contains the quoted language, but deny Plaintiff's characterization of same, otherwise denied.

43. Admitted that Bleeping's website generates revenues through advertising and commissions from affiliates and other advertisers, including Plaintiff, otherwise denied.

44. Denied.

45. Admitted that various member groups associated with the Bleeping website have been formed and evolved over time, otherwise denied.

46. Admitted that Bleeping identifies individuals in member groups and information

about them, otherwise denied.

47. Admitted that Admin & Site Admins are the highest level member groups, that Lawrence Abrams is the overall Admin of the Bleeping website, otherwise denied.

48. Admitted that the second-highest level member group is Global Moderator & Moderators, otherwise denied.

49. Admitted that the quoted language appears on Bleeping's website but deny Plaintiff's characterization of same, otherwise denied.

50. Admitted that the third-highest member group is Advisors, otherwise denied.

51. Admitted.

52. Denied

53. Admitted that when a Global Moderator, Moderator, or Advisor makes a post, the software for the site automatically identifies the poster as a Global Moderator, Moderator, or Advisor; otherwise denied.

54. Admitted that Bleeping runs a free training program referred to as the Malware Study Hall; otherwise denied.

55. Denied.

56. Admitted that volunteers work with Bleeping in running the referenced training program, otherwise denied.

57. Admitted.

58. Denied.

59. Denied.

60. Admitted that Bleeping has referred to the volunteers in the referenced positions as staff members, otherwise denied.

61. Admitted that Bleeping does not require the referenced disclosures that the vast majority of its volunteer “staff members” voluntarily make.

62. Denied.

63. Admitted that the quoted language appears on Bleeping’s site; otherwise denied.

64. Admitted.

65. Admitted that the individual identified by the pseudonym Quietman7 has been identified as a staff member and Global Moderator on the Bleeping website; otherwise denied.

66. Admitted that the referenced announcement was made on the Bleeping website in March, 2006; otherwise denied.

67. Admitted that the referenced announcement was made on the Bleeping website in March, 2006; otherwise denied.

68. Admitted.

69. Admitted.

70. Admitted.

71. Admitted.

72. Denied.

73. Admitted that Quietman7 performs some of the referenced functions for other volunteers associated with the Bleeping website; otherwise denied.

74. Denied.

75. Admitted that Quietman7 and other volunteers who have been referenced as staff members have recommended Malwarebytes’ products; otherwise denied.

76. Denied.

77. The information alleged in the first sentence of Paragraph 77 relates to

information that is or may be privileged and thus no response is required. The remaining allegations are denied.

78. Denied.

79. Deny knowledge or information sufficient to form a belief as to understandings held by consumers and users as referenced.

80. Denied.

81. Denied.

82. Denied.

83. Denied.

84. Denied.

85. Denied.

86. Denied.

87. Admit the quoted language appeared in the post referenced, otherwise denied.

88. Admitted.

89. Denied.

90. Deny knowledge or information sufficient to form a belief as to understandings held by consumers and users as referenced.

91. Denied.

92. Admitted that Bleeping has removed spam posts in accordance with the policies posted on its site, otherwise denied.

93. Denied.

94. Denied.

95. Denied.

96. Admitted that Bleeping has received cease and desist demands from Plaintiff;
otherwise denied.

97. Denied.

98. Denied.

99. Denied.

100. Denied.

FIRST CAUSE OF ACTION (Violations of Lanham Act § 43(a))

101. Prior averments incorporated.

102. Denied.

103. Denied.

104. Denied.

105. Denied.

106. Denied.

107. Denied.

SECOND CAUSE OF ACTION (Trade Libel/Commercial Disparagement)

108. Dismissed. No response required.

109. Dismissed. No response required

110. Dismissed. No response required.

111. Dismissed. No response required

112. Dismissed. No response required.

113. Dismissed. No response required

114. Dismissed. No response required.

115. Dismissed. No response required.

THIRD CAUSE OF ACTION (Libel)

- 116. Prior averments incorporated.
- 117. Denied.
- 118. Denied.
- 119. Denied.
- 120. Denied.
- 121. Denied.
- 122. Denied.
- 123. Denied.

FOURTH CAUSE OF ACTION (Libel *per se*)

- 124. Prior averments incorporated.
- 125. Denied.
- 126. Denied.
- 127. Denied.

As To All Counts

The remaining allegations are prayers for relief that do not require an admission or denial. To the extent a response is required, the allegations are denied. Unless specifically admitted herein, all allegations are denied. Defendants further deny that Plaintiff is entitled to any relief, including the relief requested in the Second Amended Complaint.

AFFIRMATIVE DEFENSES

First Affirmative Defense

Plaintiff fails to state a cause of action upon which relief can be granted.

Second Affirmative Defense

Plaintiff's claims are barred, in whole or in part, by applicable statutes of limitation.

Third Affirmative Defense

Plaintiff's claims are barred, in whole or in part, by Section 230 of the Communications Decency Act, 47 U.S.C. §230.

Fourth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the statements at issue were not published by the Defendant, Bleeping Computer, LLC.

Fifth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the statements at issue are true or substantially true.

Sixth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the statements at issue consist of opinion and/or rhetorical hyperbole, protected under the Constitution of the State of New York, the U.S. Constitution, and applicable common law.

Seventh Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the statements at issue are privileged under one or more of the following privileges: common/corresponding interest privilege, judicial proceedings privilege, fair report privilege, matter of public concern.

Eighth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the statements at issue are privileged under one or more of the foregoing privileges and Plaintiff cannot demonstrate malice.

Ninth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because Plaintiff is a public figure and cannot demonstrate actual malice with clear and convincing evidence or otherwise.

Tenth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the statements at issue are not defamatory or reasonably susceptible of a defamatory meaning.

Eleventh Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the relief Plaintiff seeks would amount to a prior restraint in violation of the Constitution of the State of New York, the U.S. Constitution, applicable common law and principles of equity.

Twelfth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, because the Plaintiff is libel proof, in that its reputation in the computer security community has been so low and so badly tarnished for so long that it is incapable of being further damaged.

Thirteenth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, by the doctrine of unclean hands.

Fourteenth Affirmative Defense

Plaintiff's claims are barred, in whole or in part, by the doctrine of laches, waiver or estoppel.

Further Affirmative Defenses

Defendant reserves the right to amend or supplement this statement of affirmative defenses.

BLEEPING COMPUTER'S COUNTERCLAIMS

Defendant and Counterclaimant Bleeping Computer, LLC hereby sues Plaintiff Enigma Software Group USA, LLC ("Enigma"). This action is for violation of the Anti-Cybersquatting Consumer Protection Act, the Lanham Act, the Florida Deceptive and Unfair Trade Practices,

and Defamation. As set forth below, Enigma has been engaged in a pattern and practice of misusing and infringing upon Bleeping's name and trademark in various formats and through various means, defaming and disparaging Bleeping in domain names, subdomain names, URLs, webpage content, and webpage source code, all with the intent and purpose of trading upon Bleeping's goodwill, promoting the download and sale of Enigma's own products, and misleading the public at the expense of Bleeping.

Summary of Counterclaims

In a matter of stunning irony and sheer hypocrisy, Enigma filed this lawsuit against Bleeping Computer, claiming Enigma's reputation was somehow damaged due to an innocuous review of Enigma's product, posted by a volunteer moderator on Bleeping's site, which simply echoed, and cited to, the opinions of knowledgeable computer security professionals. Enigma's lawsuit is plainly nothing more than an attempt to bully and censor Bleeping Computer, and to deter anyone who might criticize it – one more attempt in Enigma's long pattern of threats, intimidation and litigation. Worse, however, is that all the while, Enigma has been engaged in aggressive, secretive, and cowardly attacks against Bleeping Computer, including ripping off Bleeping Computer's content and pretending it was authored by Enigma, repeatedly misusing Bleeping's registered trademark to trade upon its goodwill, and publishing blatantly false claims about Bleeping. As the following allegations demonstrate, Enigma conducts its business in a manner that is illegal, unethical and simply immoral, thereby demonstrating that Quietman7's mildly critical statements about Enigma's product, that so enraged Enigma and led to this lawsuit, pale in comparison to the egregious misconduct Enigma perpetrates on a regular basis.

Parties

1. Counterclaimant Bleeping Computer, LLC, is a New York limited liability company, with a principal place of business in the State of New York.

2. Upon information and belief, Counterclaim Defendant Enigma Software Group USA, LLC, is a Florida limited liability company with a principal place of business in the States of Florida and/or Connecticut.

Jurisdiction & Venue

3. This Court has personal jurisdiction over Enigma pursuant to N.Y. CPLR § 302(a) as, per its allegation, it transacts business in this District and, therefore, this State, and otherwise committed tortious acts within and without the State causing injury within the State, which injury in the State was reasonably anticipated.

4. This Court has subject matter jurisdiction over this Counterclaim pursuant to 28 U.S.C. §§ 1331, 1332, 1338, & 1367, as it arises under the Lanham Act and is a matter against a citizen of a different state involving an amount in controversy in excess of \$75,000.

5. Venue is appropriate in this Court pursuant to 28 U.S.C. § 1391(b)(2) or (3) as a substantial part of the events giving rise to this action occurred in the District and Enigma is otherwise subject to this Court's personal jurisdiction.

Factual Allegations Common to All Counts

6. Bleeping owns and operates a website at <www.bleepingcomputer.com> ("Website") and did so at all relevant times herein.

7. Bleeping is the registered owner of the trademark BLEEPING COMPUTER, bearing Registration Number 4065790, issued by the U.S. Patent & Trademark Office on December 6, 2011. *See Exhibit "A"*.

8. The Website operates as a community where over 700,000 individual members may discuss and learn how to use their computers in a helpful and welcoming atmosphere.

9. The Website publishes guides and tutorials, and it also hosts forums where members ask questions that other members answer.

10. Some volunteer, non-employee members have been identified, such as “Global Moderator.”

11. One such Global Moderator is an individual who uses the moniker “Quietman7.”

12. One of the forums is devoted to computer security, with subjects such as “Anti-Virus, Anti-Malware, and Privacy Software,” “Backup, Imaging, and Disk Management Software,” “Firewall Software and Hardware,” and “Encryption Methods and Programs.”

13. Enigma describes itself as a “systems integrator and developer of PC security software” and claims it is “best known for SpyHunter, its anti-malware software product and service.” *See* <http://www.enigmasoftware.com/about-us/>.

14. Enigma offers its SpyHunter software for download on its website and, upon information and belief, markets and sells licenses in commerce throughout the United States for the use of SpyHunter and other software.

15. As alleged by Enigma in its Second Amended Complaint, Quietman7 made statements on the Website critical of Enigma and SpyHunter. *See* SAC at ¶¶ 80 & 86-90.

16. Enigma filed the instant lawsuit seeking, among other things, to enjoin Bleeping from publishing the said critical statements of Quietman7. *See* SAC at Prayers for Relief (d), (e), & (f).

A. bleepingcomputerregistryfix.com

17. Upon information and belief, on or about March 25, 2015, Enigma or its agent registered the domain name bleepingcomputerregistryfix.com.

18. Although the identity of the registrant of that domain name is hidden from public view, the website at <http://bleepingcomputerregistryfix.com> promotes and markets Enigma's SpyHunter product, and contains a link that, when a user clicks on the link, will ultimately download Enigma's SpyHunter software from:

<http://download.enigmasoftware.com/spyhunter-free-download/revenuewire/SpyHunter-Installer.exe>.

19. Upon information and belief, Enigma created, or has actual or constructive knowledge of, the content of the website at <http://bleepingcomputerregistryfix.com>.

20. Upon information and belief Enigma profits and otherwise gains financially from the content of the website at <http://bleepingcomputerregistryfix.com>.

B. Infringing and Defamatory URLs

21. Upon information and belief, Enigma, directly or through an agent, created, published and disseminated over the internet multiple "host names" or "subdomains" or URLs that use and incorporate Bleeping's registered trademark, attempt to disparage and defame Bleeping, and attempt to confuse consumers, including but not limited to:

<http://adware.bleeping.computer.remover.getridofspywareonphone.com> and

<http://browser.hijack.bleeping.computer.virus.spywareremovalfreetrial.com>

22. Upon information and belief, Enigma, directly or through an agent, created and published all of the nearly one-hundred URLs identified in **Exhibit "B"** annexed hereto, all of which incorporate Bleeping's registered trademark (hereinafter "the Infringing URLs").

23. Most of the websites associated with the Infringing URLs contain a prominent "headline" or other content that: (a) infringes Bleeping's trademark; (b) disparages and defames Bleeping; (c) attempts to mislead and confuse consumers into thinking that Bleeping Computer

itself is somehow a virus or other malware or is associated with malware; and (d) promotes and markets the sale of Enigma's SpyHunter.

24. As but one example, content appearing at one of the Infringing URLs, <browser.hijack.bleeping.computer.virus.spywareremovalfreetrial.com>, contains a prominent "headline" that reads "Browser Hijack Bleeping Computer Virus." As with the other Infringing URLs, upon information and belief Enigma created and published this content for multiple purposes, including but not limited to: (a) to trade upon Bleeping's goodwill and the goodwill associated with its registered trademark without authorization; (b) to confuse consumers and users into mistakenly believing that Bleeping Computer consists of a virus, spyware, or other malware, and specifically malware that can be removed by Enigma's SpyHunter product; (c) to falsely suggest or imply that Bleeping Computer somehow promotes, markets, sells or is otherwise connected or associated with viruses, spyware or other malware and thereby disparage and defame Bleeping and damage its reputation; (d) to confuse consumers into downloading Enigma's SpyHunter product in the false and mistaken belief that it is required in order to remedy some malware or other problem allegedly caused by Bleeping.

25. The website at <http://adware.bleeping.computer.remover.getridofspywareonphone.com> directs visitors to download SpyHunter from:

<http://signup09.enigma.revenuewire.net/spyhunter2/download?sphytemp3-overlaynew10-14>.

26. The website at:

<http://browser.hijack.bleeping.computer.virus.spywareremovalfreetrial.com>

also directs visitors to download SpyHunter from:

<http://signup09.enigma.revenuewire.net/spyhunter2/download?sphytemp3-overlaynew10-14>.

27. Upon information and belief, subdomains on <revenuewire.net> are operated and maintained by RevenueWire, Inc., on behalf of companies such as Enigma to use affiliates to market products on behalf of those companies. *See* <http://thesource.revenuewire.com/index.php/faq>.

28. Upon information and belief, Enigma uses RevenueWire to market and promote SpyHunter and even uses the name “RevenueWire” in the Uniform Resource Locator (URL) of a download link on its own domain. *See supra*.

29. Upon information and belief, the other subdomains identified in **Exhibit “B”** at relevant times directed visitors to download SpyHunter.

30. Upon information and belief, Enigma created or has actual or constructive knowledge of the content of the websites at the Infringing URLs identified in **Exhibit “B.”**

31. Upon information and belief, Enigma profits and gains from the publication and dissemination of the Infringing URLs and from the content on the associated websites.

32. Upon information and belief, Enigma owns, operates and/or controls the Infringing URLs, directly or through its agents.

C. ComboFix

33. ComboFix is a free spyware remover program.

34. The download page for ComboFix at <http://www.combofix.org/download.php> directs visitors to download the program via Bleeping’s Website at <http://www.bleepingcomputer.com/download/combofix/dl/12>.

35. As of January 30, 2016, Enigma, directly or through an agent, caused the download page for ComboFix at <http://www.combofix.org/download.php> to display a “Download Now!” link that, instead of directing visitors to Bleeping’s Website and allowing them to download ComboFix, caused them to download SpyHunter through <http://3bsoftwa.enigma.revenuewire.net/spyhunter2/download>.

36. Upon information and belief, Enigma directly or through its agent, created or has actual or constructive knowledge of the content of the ComboFix download page.

D. Infringing Source Code

37. Bleeping's name and mark and other content from Bleeping's Website appears in the source code for the web pages at <http://fixspywarenowreview.com/davinci.php> and others identified in **Exhibit "C."**

38. Such source code falsely includes a copyright notice and other content on behalf of Bleeping.

39. Upon information and belief, such source code causes search engines such as Google to yield such web pages in searches including Bleeping's name and mark.

40. The use of Bleeping's name and mark is not authorized.

41. Such webpages include software removal guides recommending visitors download SpyHunter to remove certain software.

42. A visitor to the page who was referred by a search engine result using Bleeping's name and mark would reasonably, but incorrectly, believe that Bleeping endorses the removal methodology set forth therein.

43. Bleeping makes no such endorsement or authorizes the use of its mark in such a manner.

44. The removal methodology so described directs visitors to download SpyHunter.

45. Upon information and belief, Enigma published the content of the source code or otherwise directs and controls the content of the source code of the webpages set forth in **Exhibit "D."**

46. Upon information and belief, Enigma has actual or constructive knowledge of the misuse of Bleeping's mark and content in the source code and profits and gains from such use.

E. "Rkill" and "Unhide" Programs

47. Bleeping authored and developed computer software programs known as "Rkill" and "Unhide." Rkill is a computer software program that attempts to terminate running malware processes to enable security software to clean infected computers. Unhide is a computer software program that reveals files that otherwise would be hidden as the result of a computer virus or malware.

48. Upon information and belief, Enigma has published, on multiple websites that market and promote the downloading and sale of SpyHunter, numerous false and defamatory statements of and concerning Bleeping and its programs, RKill.com and Unhide.

49. For example, Enigma owns or controls a website at: [spywareremove.com](http://www.spywareremove.com). *See*, <http://www.spywareremove.com/about-us/>. On said website, Enigma markets and promotes the sale of its product, SpyHunter. On said website, Enigma published false and defamatory statements claiming that Rkill and Unhide are "malware." *See* **Exhibit "F"** annexed hereto.

50. Rkill.com and Unhide are not malware.

51. Likewise, the webpage at <http://www.enginesupplymachineshop.com/rkill-com/>, which markets and promotes the sale of SpyHunter, repeatedly refers to Rkill as a "virus" or "infection," including without limitation the following statements (emphasis added):

rkill.com is a dangerous computer virus which can destroy the infected computer and record your personal information.... The computer user's personal information may be got by the virus makers through the virus, such as credit card or bank account details and social contacts' information. ...

rkill.com is a high-risk Trojan virus infection designed by cyber criminals recently, which bursts in the life of many computer users and causes serious damages [*sic*] to the infected computer. The hateful virus is brimful of mischief. ... The virus makers may use every opportunity to control the computer remotely.

With the cover of the virus they can remove or modify your important documents wantonly and steal or encrypt your personal data, resulting in inconvenience as well as unnecessary losses. Therefore, getting rid of rkill.com is quite urgent.

Exhibit “E” annexed hereto is a true and correct copy of content appearing on webpages published at <http://www.enginesupplymachineshop.com/rkill-com/> containing the above-referenced false and defamatory statements.

52. The above-quoted statements are false and defamatory in that RKill.com is not a computer virus or infection, RKill.com does not seriously slow down a computer’s performance, RKill.com does not collect a computer user’s personal information, RKill.com is not a high-risk Trojan virus, was not designed by cyber criminals, and does not cause damage to users’ personal computers or result in the loss or theft of their personal data.

53. The webpage at <http://www.enginesupplymachineshop.com/rkill-com> directs visitors to remove RKill.com by downloading Enigma’s product, SpyHunter.

54. The removal methodology so described directs visitors to download SpyHunter through RevenueWire by clicking on the link <http://www.enginesupplymachineshop.com/wp-content/themes/images/spyhunter.php>.

55. The said link redirects to:
<http://luogoodluck.enigma.revenuewire.net/spyhunter2/download> which redirects to
<http://luogoodluck.enigma.safecart.com/spyhunter2/download> which redirects to
<http://download.enigmasoftware.com/spyhunter-free-download/revenuewire/SpyHunter-Installer.exe>.

56. By naming RevenueWire in its own URL and accepting referral links from <revenuewire.net>, Enigma has acted in a manner that demonstrates RevenueWire is Enigma’s agent.

57. In the alternative, such nomenclature and acceptance would induce visitors to believe that RevenueWire has been authorized to act on behalf of Enigma.

58. Upon information and belief, Enigma directly or through an agent caused the publication of the foregoing false and disparaging statements about RKkill and Unhide.

59. The foregoing false and defamatory statements have caused damage to Bleeping's reputation and goodwill, and if not enjoined will cause further damage.

Count I

Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d)

60. Bleeping restates and realleges the foregoing factual allegations of its Counterclaim as if fully set forth herein.

61. Bleeping is the owner of the distinctive, federally registered trademark BLEEPING COMPUTER.

62. Upon information and belief, Enigma, directly or through an agent, registered the domain name <bleepingcomputerregistryfix.com>.

63. The domain name <bleepingcomputerregistryfix.com> is identical to or confusingly similar to Bleeping's registered trademark.

64. At all relevant times herein, Enigma had a bad faith intent to profit from Bleeping's mark by registering said domain name and by inducing visitors to purchase a license for Enigma's SpyHunter software through it.

65. As a result of such registration, Bleeping has been damaged, including a loss of goodwill.

66. Therefore, Enigma is directly or, in the alternative, vicariously, liable for violation of 15 U.S.C. § 1125(d).

67. Alternatively, Enigma, by continuing to supply its software to the domain registrant, is contributorily liable for the violation of 15 U.S.C. § 1125(d).

Count II
Violation of the Lanham Act, 15 U.S.C. §§ 1114 and 1125(a)

68. Bleeping restates and realleges the foregoing factual allegations of its Counterclaim as if fully set forth herein.

69. Bleeping is the owner of the distinctive trademark BLEEPING COMPUTER.

70. Bleeping has not authorized the use of its mark in any of the Infringing URLs identified at **Exhibit “B”** annexed hereto.

71. Bleeping has not authorized the use of its mark in the source code for the website at <http://fixspywarenowreview.com/davinci.php> and others identified in **Exhibit “D.”**

72. Enigma, directly or through an agent, caused the foregoing unauthorized and infringing uses of Bleeping’s trademark in order to market, promote, sell and distribute its SpyHunter software and licenses.

73. Such unauthorized uses constitute a reproduction, counterfeit, copy, or colorable imitation of that mark in connection with the sale, offering for sale, distribution, and advertising of software provided by Enigma in such a manner as is likely to and with the intent to cause confusion, mistake, or to deceive, in violation of 15 U.S.C. § 1114(1)(b).

74. Such unauthorized uses represent a false designation of origin, false or misleading description and/or a misrepresentation of fact likely to cause confusion, mistake, or deceive as to the affiliation, connection, or association of Enigma with Bleeping or which is likely to cause confusion, mistake or deceive as to whether Bleeping has anything to do with the origin, sponsorship, or approval of the goods, services, or commercial activities of Enigma in violation of 15 U.S.C. § 1125(a).

75. Therefore, Enigma is directly or, in the alternative, vicariously, liable for violation of 15 U.S.C. §§ 1114 and 1125(a).

76. Alternatively, Enigma, by continuing to supply its software to the operators of those subdomains and URLs, is contributorily liable for the violation of 15 U.S.C. §§ 1114 and 1125(a).

Count III
Florida Deceptive and Unfair Trade Practices Act

77. Bleeping restates and realleges the factual allegations of its Counterclaim as if fully set forth herein.

78. Enigma, a Florida limited liability company, is subject to the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201 *et seq.*

79. Fla. Stat. § 501.204(1) declares deceptive acts or practices in the conduct of any trade or commerce to be unlawful.

80. Fla. Stat. § 501.205(1) authorizes the Florida Attorney General to promulgate rules specifying deceptive acts or practices in trade or commerce.

81. Chapter 2-9, Florida Administrative Code (F.A.C.), sets forth the rules pertaining to advertising and sales of goods or services.

82. Rule 2-9.002(3), F.A.C., declares it a deceptive act or practice to misrepresent the sponsorship, endorsement, approval or certification of goods or services.

83. The above-described acts and practices of Enigma detailed in the factual allegations of Bleeping's Counterclaim constitute a far-reaching and extensive pattern of deceptive, unfair, and unconscionable acts and practices in the conduct of trade or commerce.

84. By registering [<bleepingcomputerregistryfix.com>](http://bleepingcomputerregistryfix.com) and causing visitors to said site to download and purchase SpyHunter, Enigma misrepresented that Bleeping sponsored, endorsed,

approved, or certified such software, improperly and without authorization infringed upon Bleeping's goodwill and trademark, and sought to confuse, mislead and deceive consumers.

85. By creating and utilizing the Infringing URLs, including but not limited to s <http://adware.bleeping.computer.remover.getridofspywareonphone.com> and <http://browser.hijack.bleeping.computer.virus.spywareremovalfreetrial.com>, identified in **Exhibit "B,"** and causing visitors to such site to download and purchase SpyHunter, Enigma misrepresented that Bleeping sponsored, endorsed, approved, or certified such software, improperly and without authorization infringed upon Bleeping's goodwill and trademark, and sought to confuse, mislead and deceive consumers.

86. By utilizing URLs bearing Bleeping's name, such as <http://www.fixpcspywarehelp.com/how-to-remove-malware-bleeping-computer.php> and others and causing visitors to such site to download and purchase SpyHunter, Enigma misrepresented that Bleeping sponsored, endorsed, approved, or certified such software.

87. By utilizing source code in web pages including Bleeping's name and content, such as in the source code for the web pages at <http://fixspywarenowreview.com/davinci.php> and causing visitors to such site to download and purchase SpyHunter, Enigma misrepresented that Bleeping sponsored, endorsed, approved, or certified such software, improperly and without authorization infringed upon Bleeping's goodwill and trademark, and sought to confuse, mislead and deceive consumers.

88. By causing visitors seeking to download ComboFix from Bleeping to instead download SpyHunter, Enigma misrepresented that Bleeping sponsored, endorsed, approved, or certified such software, improperly and without authorization infringed upon Bleeping's goodwill and trademark, and sought to confuse, mislead and deceive consumers.

89. By making the foregoing false statements about Bleeping and Bleeping's software programs RKill.com and Unhide, Enigma deceived consumers into believing Bleeping promulgated a virus and into downloading and purchasing SpyHunter and otherwise engaged in deceptive and unfair business practices and acts.

90. By instituting litigation with the intent to remove negative opinions and/or truthful statements about Enigma and SpyHunter, Enigma seeks to deceive consumers of malware removal software into downloading and purchasing SpyHunter.

91. The foregoing conduct, directly or vicariously, constitutes a violation of Rule 2-9.002(3), F.A.C., by Enigma and constitutes a pattern and practice of deceptive and unconscionable acts and practices in violation of Fla. Stat. § 501.204(1).

92. The deceptive and unfair trade practices of Enigma, as alleged herein, have injured and will continue to injure and prejudice Bleeping and the public.

93. Enigma has willfully, intentionally, and wantonly, or with reckless indifference, engaged in the deceptive, unfair and unconscionable acts and trade practices alleged herein when Enigma knew or should have known that said acts and practices were unfair, deceptive, or prohibited by rule.

94. Unless Enigma is enjoined from engaging further in the acts and practices alleged herein, the continued activities of Enigma will result in irreparable injury to Bleeping for which there is no adequate remedy at law.

Count IV
Defamation

95. Bleeping restates and realleges the factual allegations of its Counterclaim as if fully set forth herein.

96. Enigma published the foregoing statements of and concerning Bleeping and its software programs Rkill and Unhide on the internet to millions of users.

97. The foregoing statements, published and disseminated by Enigma about Bleeping and its software programs, are false and defamatory.

98. Enigma published the false and defamatory statements about Bleeping with malice.

99. Such statement tends to injure Bleeping in its trade and business as a reputable source in the fight against viruses and malware and go directly against the nature, characteristics, and quality of its business, impugning its integrity.

100. Therefore, such statements constitute defamation or libel *per se* for which Enigma is liable.

PRAYER FOR RELIEF

WHEREFORE, Bleeping Computer, LLC respectfully demands judgment as follows:

- A. Actual damages, in the form of Defendant's profits or otherwise;
- B. Statutory damages as available under applicable law;
- C. Punitive damages;
- D. Pre-judgment and post-judgment interest, to the extent permitted by applicable law;
- E. Attorneys' Fees and Costs as permitted by applicable law;
- F. An injunction requiring Enigma and/or its agents to transfer the domain at bleepingcomputerregistryfix.com to Bleeping and to never register another domain containing Bleeping's name and/or mark
- G. An injunction requiring Enigma and/or its agents to cease from utilizing and permanently delete the subdomains <http://adware.bleeping.computer.remover.getridofspywareonphone.com>, <http://browser.hijack.bleeping.computer.virus.spywareremovalfreetrial.com>, and all of the other Infringing URLs identified herein, and to never utilize another subdomain or URL containing Bleeping's name and/or mark.

- H. An injunction requiring Enigma and/or its agents to cease from using Bleeping's name, mark or other content authored by Bleeping in the source code for the web pages at <http://fixspywarenowreview.com/davinci.php> or any elsewhere;
- I. An injunction requiring Enigma and/or its agents to cease causing visitors to ComboFix.org to download any Enigma product;
- J. An injunction requiring Enigma and/or its agents to remove the webpage at <http://www.enginesupplymachineshop.com/rkill-com> and otherwise refrain from publishing false statements about Bleeping, or any of its programs, including RKill.com, or Unhide;
- K. An injunction requiring Enigma and/or its agents to cease from using Bleeping's name or mark in any advertisement or marketing of Enigma's products.
- L. Judgment dismissing with prejudice all of Enigma's claims in the SAC; and
- M. Such other and further relief as the Court deems just and proper.

JURY DEMAND

Defendant hereby demands a jury trial as to all issues so triable as raised by any of the parties' claims, counterclaims, crossclaims and defenses in this matter.

Dated August 8, 2016

Respectfully Submitted,

/s/ Marc J. Randazza
Marc J. Randazza, Esq.
Admitted *pro hac vice*
RANDAZZA LEGAL GROUP, PLLC
4035 South El Capitan Way
Las Vegas, Nevada 89147
Tele: 702-420-2001
Fax: 305-437-7662
Email: ecf@randazza.com

Jay M. Wolman (JW0600)
RANDAZZA LEGAL GROUP, PLLC
100 Pearl Street, 14th Floor
Hartford, CT 06103
Tele: 702-420-2001
Fax: 305-437-7662
Email: ecf@randazza.com

/s/ Gregory W. Herbert
Gregory W. Herbert, Esq.
New York Bar Registration No. 2502755
GREENBERG TRAUERIG, P.A.

450 South Orange Avenue, Suite 650
Orlando, FL 32801
Telephone: (407) 420-1000
Facsimile: (407) 841-1295
herbertg@gtlaw.com

Exhibits:

- A: Bleeping Trademark Registration**
- B: List of (96) Infringing URLs**
- C: Sample of URLs using Bleeping TM/content in source code**
- D: List of URLs using Bleeping TM/content in source code**
- E: Statements re Rkill at <http://www.enginesupplymachineshop.com/rkill-com/>**
- F: spywareremove.com pages claiming Rkill and Unhide are malware**



United States Patent and Trademark Office

[Home](#) | [Site Index](#) | [Search](#) | [FAQ](#) | [Glossary](#) | [Guides](#) | [Contacts](#) | [eBusiness](#) | [eBiz alerts](#) | [News](#) | [Help](#)**Trademarks > Trademark Electronic Search System (TESS)**

TESS was last updated on Mon Aug 8 03:21:08 EDT 2016

[TESS HOME](#) | [NEW USER](#) | [STRUCTURED](#) | [FREE FORM](#) | [BROWSE DICT](#) | [SEARCH OG](#) | [BOTTOM](#) | [HELP](#)[Logout](#) Please logout when you are done to release system resources allocated for you.**Record 1 out of 1**[TSDR](#) | [ASSIGN Status](#) | [TTAB Status](#) (*Use the "Back" button of the Internet Browser to return to TESS*)**BLEEPING COMPUTER****Word Mark BLEEPING COMPUTER****Goods and Services** IC 038. US 100 101 104. G & S: providing online user forums in the field of personal computing issues. FIRST USE: 20040200. FIRST USE IN COMMERCE: 20040200

IC 041. US 100 101 107. G & S: providing online tutorials and instruction in the fields of personal computing and information security. FIRST USE: 20040200. FIRST USE IN COMMERCE: 20040200

IC 042. US 100 101. G & S: providing websites featuring news, information, and commentary in the fields of personal computing and personal and consumer computer technology; computer services, namely, online detection and removal of malware and spyware; technical support services, namely, online troubleshooting, diagnostics, and repair of computer software problems and optimization of computer performance; software as a service (SAAS) services featuring third-party computer software used for malware and spyware removal, troubleshooting, diagnostics, and repair of computer software problems, and optimization of computer performance. FIRST USE: 20040200. FIRST USE IN COMMERCE: 20040200

Standard Characters Claimed**Mark Drawing Code** (4) STANDARD CHARACTER MARK**Serial Number** 85156083**Filing Date** October 19, 2010**Current Basis** 1A**Original Filing Basis** 1A**Published for Opposition** September 20, 2011

Exhibit "A"

Registration Number 4065790
Registration Date December 6, 2011
Owner (REGISTRANT) Bleeping Computer LLC LIMITED LIABILITY COMPANY NEW YORK P.O. Box 1025 Melville NEW YORK 11747
Attorney of Record Daniel I. Schloss
Disclaimer NO CLAIM IS MADE TO THE EXCLUSIVE RIGHT TO USE "COMPUTER" APART FROM THE MARK AS SHOWN
Type of Mark SERVICE MARK
Register PRINCIPAL
Live/Dead Indicator LIVE

[TESS HOME](#)
[NEW USER](#)
[STRUCTURED](#)
[FREE FORM](#)
[BROWSE DICT](#)
[SEARCH OG](#)
[TOP](#)
[HELP](#)

[|.HOME](#) | [SITE INDEX](#) | [SEARCH](#) | [eBUSINESS](#) | [HELP](#) | [PRIVACY POLICY](#)

<http://adware.bleeping.computer.remover.getridofspywareonphone.com/>
<http://adware.cleaner.bleeping.computer.adware.adawareremoval.com/>
<http://adware.cleaner.bleeping.computer.scam.getridofspywareonmac.com/>
<http://adware.my.bleeping.computer.adware.removespywarefrommac.com/>
<http://adware.my.bleeping.computer.hijack.removespywarefrommac.com/>
<http://borrar.adware.cleaner.bleeping.computer.spywareremovalfreetrial.com/>
<http://borrar.malwarebytes.bleeping.computer.removeadwarefromipad.com/>
<http://browser.hijack.bleeping.computer.get.rid.of.removeadwarefromipad.com/>
<http://browser.hijack.bleeping.computer.virus.spywareremovalfreetrial.com/>
<http://delete.adware.my.bleeping.computer.chrome.removeadwarefromipad.com/>
<http://delete.adware.my.bleeping.computer.chrome.removespywarefrommac.com/>
<http://remove.adware.bleeping.computer.windows.removeadawarefree.com/>
<http://eliminate.adware.my.bleeping.computer.removeadwarefromipad.com/>
<http://exe.bleeping.computer.pcfregistrycleaner.com/>
<http://fix.exe.bleeping.computer.pcregistryerrorsfix.com/>
<http://fixpcspywarebot.com/how-to-uninstall-bleeping-computer-malwarebytes-anti.php>
<http://fixpcspywarefree.com/how-to-remove-vista-security-2012-bleeping-computer.php>
<http://fixpcspywarejobs.com/how-to-remove-antimalware-doctor-bleeping-computer.php>
<http://fixpcspywarelaws.com/system-fix-malware-bleeping-computer.php>
<http://fixpcspywarenews.com/remove-qone8-adwcleaner-bleeping-computer.php>
<http://fixpcspywarenews.com/remove-qone8-download-bleeping-computer.php>
<http://fixpcspywarenuker.com/remove-fbi-fbi-malware-bleeping-computer.php>
<http://get.rid.of.adware.bleeping.computer.windows.getridofspywareonmac.com>
<http://get.rid.of.adware.my.bleeping.computer.internet.explorer.removespywarehunter.com/>
<http://get.rid.of.malwarebytes.bleeping.computer.chrome.removeadwarefromipad.com/>

<http://permanant.removal.of.malwarebytes.bleeping.computer.getridofspywarefree.com/>

<http://removal.adware.bleeping.computer.removespywarefromipad.com/>

<http://remove.adware.cleaner.bleeping.computer.firefox.removeadwarefromipad.com/>

<http://remove.malwarebytes.bleeping.computer.chrome.getridofspywarefree.com/>

<http://removing.adware.cleaner.bleeping.computer.removespywarefreeware.com/>

<http://uninstall.error.1711.windows.7.bleepingcomputerregistryfix.com/>

<http://www.fixpcspyware2014.com/remove-xp-internet-security-2012-bleeping-computer.php>

<http://www.fixpcspywarehelp.com/how-to-remove-malware-bleeping-computer.php>

<http://www.fixpcspywaremac.com/remove-spyware-protection-bleeping-computer.php>

<http://www.fixpcspywarenames.com/remove-malware-bleeping-computer.php>

<http://www.fixpcspywarenews.com/remove-malware-protection-bleeping-computer.php>

<http://www.whgspc.com/is-bleeping-computer-exe-virus-fix-bleeping-computer-exe-error-and-issues/>

<http://www.pcspywarescanjet.com/yontoo-bleeping-computer.php>

<http://fixpcspywarequake.com/remove-adwares-adwcleaner-bleeping-computer-download.php>

<http://pcspywarescanusb.com/whitesmoke-bleeping-computer.php>

<http://www.pcspywarescancnet.com/adware-remover-bleeping-computer.php>

<http://bleeping.computer.virus.removal.guides.uninstallconduitfast.com/>

<http://fixpcspywarequake.com/remove-adwares-adwcleaner-bleeping-computer.php>

<http://fixpcspywarequake.com/remove-adwares-rkill-download-bleeping-computer.php>

<http://ms.removal.tool.bleeping.computer.conduituninstaller.com/>

<http://pcspywarescanjet.com/yontoo-bleeping-computer.php>

<http://pcspywarescanjobs.com/conduit-bleeping-computer.php>

<http://pcspywarescanmac.com/search-conduit-bleeping-computer.php>

<http://pcspywarescanusb.com/whitesmoke-bleeping-computer.php>

<http://pcspywarescanxl.com/search-conduit-bleeping-computer.php>

<http://virus.removal.tools.bleeping.computer.conduitremover.com/>

<http://www.fixpcspywarequake.com/remove-adwares-adwcleaner-bleeping-computer-download.php>

<http://www.fixpcspywarequake.com/remove-adwares-my-bleeping-computer-rkill.php>

<http://www.pcfixspeedspyware.com/free-spyware-redirect-virus-removal-bleeping-computer.php>

<http://www.pcspywarescancnet.com/adware-remover-bleeping-computer.php>

<http://www.pcspywarescancnet.com/avg-removal-tool-bleeping-computer.php>

<http://www.pcspywarescanjet.com/yontoo-bleeping-computer.php>

<http://bleepingcomputer.conduit.removal.getridofconduitsearchonchrome.com/>

<http://com.surrogate.bleeping.computer.removespywareandadwareforfree.com/>

<http://conduit.removal.bleeping.computer.getridofconduitengine.com/>

<http://conduit.toolbar.removal.bleeping.computer.getridofconduitionie.com/>

<http://crypto.lock.removal.bleeping.computer.removespywarewindows8.com/>

<http://crypto.locker.removal.bleeping.computer.removespywarefromwindows7.com/>

<http://cryptolocker.bleeping.computer.removespywarehijacker.com/>

<http://ctb.locker.bleeping.computer.removespywareclearfromcontrolpanel.com/>

<http://ctb.locker.bleeping.computer.removespywarefromchrome.com/>

<http://delta.search.malware.bleeping.computer.getridofadwareonamac.com/>

<http://delta.search.malware.bleeping.computer.getridofadwareonfirefox.com/>

<http://how.to.remove.crypto.locker.bleeping.computer.fixspyware2015.com/>

<http://remove.conduit.bleeping.computer.getridofconduitmac.com/>

<http://remove.conduit.search.bleeping.computer.getridofconduitvirus.com/>

<http://remove.crypto.locker.bleeping.computer.removespywareclearfromcontrolpanel.com/>

<http://remove.mysearchdial.bleeping.computer.getridofadwarespyware.com/>

<http://remove.mysearchdial.bleeping.computer.removeadwareandspywarefree.com/>

<http://remove.qone8.bleeping.computer.getridofadwareonfirefox.com/>

http://remove.qone8.bleeping.computer.removespywarefromyourcomputer.com/
http://remove.qone8.bleeping.computer.spywarefixnet.com/
http://remove.search.conduit.bleeping.computer.getridofconduitsearchchrome.com/
http://remove.search.protect.bleeping.computer.getridofadwareonpc.com/
http://remove.sweetpacks.bleeping.computer.removemalwarefrombrowser1.com/
http://remove.trovi.bleeping.computer.getridofadware.com/
http://removeadwaremicrosoft.com/v9-removal-bleeping-computer.php
http://removing.conduit.bleeping.computer.getridofconduithomepage.com/
http://search.conduit.removal.bleepingcomputer.getridofconduitsearchfirefox.com/
http://snapdo.removal.bleeping.computer.getridofadwareonmac.com/
http://sweetpacks.removal.bleeping.computer.instantspywarefix1.com/
http://sweetpacks.removal.bleeping.computer.repairadware1.com/
http://sweetpacks.virus.bleeping.computer.easyadwareremoval1.com/
http://sweetpacks.virus.bleeping.computer.fixbrowseradware1.com/
http://trovi.virus.bleeping.computer.removespywareandvirusesabsolutelyfree.com/
http://v9.removal.bleeping.computer.getridofadwareonmac.com/
http://vosteran.malware.bleeping.computer.removespywarecookies.com/
http://exe.bleeping.computer.totallyfreepcregistryfix.com/
<http://www.infoproductinsider.com/spyhunter-bleeping-computer/>
http://adware.cleaner.bleeping.computer.scam.getridofspywareonmac.com/
http://browser.hijack.bleeping.computer.scam.removespywareapple.com/

```
1 <!DOCTYPE html>
2 <!--BEGIN html-->
3 <html class=" js cssanimations csstransitions" lang="en-US"><!--BEGIN head--><head>
4
5
6 <!-- Meta Tags -->
7 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
8 <meta name="viewport" content="width=device-width, initial-scale=1.0">
9 <title>How to Completely Delete Davinci Completely | Davinci Removal Guide</title>
10 <meta name="description" content="Get Rid Of Davinci completely and get your PC running
normal once again.">
11
12 <link rel="stylesheet" id="parallaxcss-css"
href="remove_adware_spyware_virus_hijacker_files/parallax.css" type="text/css" media="all">
13 <link rel="stylesheet" id="googlefont-css"
href="remove_adware_spyware_virus_hijacker_files/css.css" type="text/css" media="all">
14 <link rel="stylesheet" id="fontawesomecss-css"
href="remove_adware_spyware_virus_hijacker_files/font-awesome.css" type="text/css" media="all">
15 <link rel="stylesheet" id="maincss-css"
href="remove_adware_spyware_virus_hijacker_files/style.css" type="text/css" media="all">
16 <link rel="stylesheet" id="bootstrapcss-css"
href="remove_adware_spyware_virus_hijacker_files/bootstrap.css" type="text/css" media="all">
17 <link rel="stylesheet" id="bootstrapcsstheme-css"
href="remove_adware_spyware_virus_hijacker_files/bootstrap-theme.css" type="text/css"
media="all">
18 <link rel="stylesheet" id="dynamic-css-css"
href="remove_adware_spyware_virus_hijacker_files/admin-ajax.css" type="text/css" media="all">
19 <link rel="stylesheet" id="A2A_SHARE_SAVE-css"
href="remove_adware_spyware_virus_hijacker_files/addtoany.css" type="text/css" media="all">
20
21
22
23 <!--END head-->
24
25 <!--BEGIN body-->
26 <body class="single single-post postid-6566 single-format-standard">
27
28 <div id="wrapper">
29
30 <div id="top"></div>
31
32 <!--BEGIN .header-->
33 <div class="header">
34
35 <!--BEGIN .container-->
36 <div class="container container-header custom-header">
37
38
39 <!--BEGIN #righttopcolumn-->
40 <div id="righttopcolumn">
41
42 <!--BEGIN #subscribe-follow-->
43
44 <div id="social">
45
46
47 <ul class="sc_menu">
48
49 <div class="clearfix2">How to monitor someones texts from your iphone? Your answer will help you
find the best solution. <a href="webguard.php">Webguard</a> <a href="9q3ck0u-com-pop-up-
ads.php">9q3ck0u Com Pop Up Ads</a> <a href="mystart-dealwifi-com.php">Mystart Dealwifi Com</a>
<a href="win32ptcasino.php">Win32ptcasino</a> <a
href="securitytoolbar71.php">Securitytoolbar71</a> <a
href="trojanjsredirectoryf.php">Trojanjsredirectoryf</a> <a
href="windowsantibreakingsystem.php">Windowsantibreakingsystem</a> <a
```

```
href="pornlinks.php">Pornlinks</a> </div>
50
51 </ul></div>
52
53 <!--END #subscribe-follow-->
54
55 </div>
56
57
58 <!--BEGIN .title-container-->
59 <div class="title-container">
60
61
62
63 <div id="logo"><a href="">Fix Your Computer </a></div>
64
65
66 <div id="tagline">Fast & Easy PC Fixes</div>
67
68 <!--END .title-container-->
69 </div>
70
71 <!--END .container-->
72 </div>
73
74
75
76
77 <!--END .header-->
78 </div>
79
80
81
82
83 <div class="menu-container">
84
85
86 <div class="clearfix2">Always keep Windows Operating System updated. SpyBHORemover
SpyBHORemover 6.0 Our Rating: stars User Rating: 5(2) Popularity:44 SpyBHORemover examines all
your installed Internet Explorer BHOs (Browser Helper Objects) and produces a risk assessment
report that shows which BHOs might be dangerous or are suspicious. <a
href="zedocom.php">Zedocom</a> <a href="trojffspy-a.php">Trojffspy A</a> <a
href="antivirusmaster.php">Antivirusmaster</a> <a href="queryservicenet.php">Queryservicenet</a>
<a href="020-3514-0515-pop-ups.php">020 3514 0515 Pop Ups</a> <a
href="trojanwin32fakegdfa.php">Trojanwin32fakegdfa</a> <a
href="telluriumgenerate.php">Telluriumgenerate</a> <a href="idptrojan.php">Idptrojan</a> </div>
87
88
89 <div class="menu-header">
90
91 <!--BEGIN .container-menu-->
92 <div class="container nacked-menu container-menu">
93
94
95 <div class="primary-menu">
96 <nav id="nav" class="nav-holder">
97 <div class="nav-menu"><ul class="nav-menu sf-js-enabled sf-arrows">
98 <li class="page_item page-item-2738"><a href="download.php">About Us</a></li><li
class="page_item page-item-3955"><a href="download.php">Computer Services</a></li><li
class="page_item page-item-3953"><a href="download.php">Download Virus Removal Tool</a></li></ul>
</div>
99
100 <div style="width: 100%;" class="dd-container" id="undefined"><div style="width: 100%;"
class="dd-select"><input value="" class="dd-selected-value" type="hidden"><a class="dd-selected">
```

```
<label class="dd-selected-text"><span class="glyphicon glyphicon-align-justify"></span></label>
</a></div><ul style="width: 100%;" class="dd-options dd-click-off-close"><li><a class="dd-option
dd-option-selected"> <label class="dd-option-text"><span class="glyphicon glyphicon-align-
justify"></span></label></a></li><li><a class="dd-option"> <input class="dd-option-value"
value="about-us/" type="hidden"> <label class="dd-option-text">About Us</label></a></li><li><a
class="dd-option"> <input class="dd-option-value" value="computer-services/" type="hidden">
<label class="dd-option-text">Computer Services</label></a></li><li><a class="dd-option"> <input
class="dd-option-value" value="download-virus-removal-tool/" type="hidden"> <label class="dd-
option-text">Download Virus Removal Tool</label></a></li></ul></div></nav>
101 </div>
102
103 <header style="display: none;" id="header" class="sticky-header">
104 <div class="container">
105
106 <div class="clearfix">These are stubborn ads and I ma just fed-up of it. Download Now
1.92 Mb Aug 27, 2015 XP/Vista/7/8/10 Free RKill screenshot View all screenshots... <a
href="antivirus-scannerv12com.php">Antivirus Scannerv12com</a> <a
href="trojanrevetonc.php">Trojanrevetonc</a> <a href="win32delfqcz.php">Win32delfqcz</a> <a
href="trojanwin32regrunbac.php">Trojanwin32regrunbac</a> <a
href="downloaderparshell.php">Downloaderparshell</a> <a
href="hacktoolwin32flooderah.php">Hacktoolwin32flooderah</a> <a href="offerapp.php">Offerapp</a>
<a href="browsingclear.php">Browsingclear</a> </div>
107 <nav id="nav" class="nav-holder">
108 <div class="nav-menu"><ul class="nav-menu sf-js-enabled sf-arrows"><li class="page_item page-
item-2738"><a href="about-us/">About Us</a></li><li class="page_item page-item-3955"><a
href="computer-services/">Computer Services</a></li><li class="page_item page-item-3953"><a
href="download-virus-removal-tool/">Download Virus Removal Tool</a></li></ul></div>
109 </nav>
110 </div>
111 </header>
112
113 </div>
114
115 </div>
116
117 <div class="menu-back">
118
119 </div>
120
121
122
123 </div>
124
125
126 <!--BEGIN .content-->
127 <div class="content lilysingular single s-category-adware s-author-none">
128
129
130 <!--BEGIN .container-->
131 <div class="container container-center row">
132
133 <!--BEGIN #content-->
134 <div id="content">
135
136 <!--BEGIN #primary .hfeed-->
137 <div id="primary" class=" col-xs-12 col-sm-6 col-md-8 col-md-8 col-single
138 ">
139
140
141 <ul class="breadcrumbs"><li><a class="home" href="">Home</a></li><li><a
href="category/adware/" title="adware">adware</a></li><li>How to Permanantly Delete Davinci
Completely?(Step by Step Removal Guide)</li></ul>
142
143 <!-- attachment begin -->
```

```

144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176

```

`<div class="clearfix2">`This proverb hold good and is applicable here as well. search downloads Platforms Windows Audio Development Educational Networking Photos & Images Security Utilities Mac Linux Weekly Downloads in Windows AdwCleaner Logo AdwCleaner Version: 5.0.1.3 282,493 Downloads ComboFix Logo ComboFix Version: 15.10.15.1 162,629 Downloads Junkware Removal Tool Logo Junkware Removal Tool Version: 7.6.4.0 50,475 Downloads RKill Logo RKill Version: 2.8.2.0 39,056 Downloads TDSSKiller Logo TDSSKiller Version: NA 18,541 Downloads Newsletter Sign Up Follow us: Main Sections News Downloads Virus Removal Guides Tutorials Startup Database Uninstall Database File Database Glossary Community Forums Chat Useful Resources Welcome Guide Sitemap Company About BleepingComputer Contact Us Advertising Social & Feeds Changelog User Agreement - Privacy Policy Copyright @ 2015 Bleeping Computer LLC - All Rights Reserved Remove Spyware from PC Best PC Protection Guide Skip to content Home Free Download Buy Contact Us Privacy Policy Disclaimer Security Articles DMCA Remove NaviWatcher Ads Adware - How to Remove NaviWatcher Ads Adware Hi. When you are satisfied with the selection, simply click on the Clean button, which will cause AdwCleaner to reboot your computer and remove the files and registry entries associated with the various adware that you are removing. The tool is designed to remove the Superfish adware and remove all traces from the files system and registry. scan scheduler download button NaviWatcher Ads: Prevention Tips & Conclusion for Better Protection "Prevention is always better than cure". Download Now 2.56 Mb Aug 21, 2015 XP/Vista/7/8/10 Free FreeFixer screenshot View all screenshots... However it is essential that your PC must be turned on during the time the scanner has been scheduled. Visit Site #3 FlexiSpy Unlike some other spyphone companies, who are forced to charge EU buyers VAT, or USA buyer Sales Tax, FlexiSPY ecommerce system is smart, and can ensure that no FlexiSPY customer needs to pay sales tax if they don't want to. As a causal click on such ads or pop-ups help its creators to generate revenue. It helps to prevent NaviWatcher Ads from modifying your Internet and its DNS settings. ``Windowsdebuggingcenter`` ``Showpasssmartbar`` ``Speeditup`` ``Hyperbrows`` ``Backdoor Rarstone`` ``Carberptrojan`` ``Antivirus360`` ``Trojagentaana`` `</div>`

```

<!--BEGIN .hentry-->
<div id="post-6566" class="post-6566 post type-post status-publish format-standard hentry category-adware p publish first-post cat untagged col-md-12">

```

`<h1 class="entry-title">`How to Permanantly Remove Davinci (Step by Step Removal Guide)`</h1>`

```

<!--BEGIN .entry-meta .entry-header-->
<div class="entry-meta entry-header"><!--END .entry-meta .entry-header-->
</div>

```

```

<!--BEGIN .entry-content .article-->
<div class="entry-content article">

```

`<p>`Is your computer infected with Davinci virus? Have you tried a lot of anti-malware programs to remove it but it just stays in your computer and doesn't go away? How does this Trojan come to your computer? If you get infected by this virus and still have no idea on how to remove it, you can get help from the following post.`</p>`

```

<p>What Problems Davinci Causes?<br>
1 The network connection becomes slow, and the system performance is decreased.<br>
2 A pile of advertisements are popping up on your PC when you use the computer to surf the Internet.<br>
3 Default browser homepage and search engine are changed to new ones without any consent.<br>
4 Browsers runs out of control and you are always forced to visit some websites irrelevant to your requests.<br>

```

177 5 Unknown toolbars, plug-ins or extensions appear on your browsers and
178 you are sure that you have never installed them onto your browsers.

179 6 Personal information and data are collected and exposed to unknown people.</p>
180 <div align="center">
</div>
181 <h2>What is Davinci?

182 </h2>
183 <p>Davinci is regarded as a pesky program which attacks your
184 browsers and causes a lot of chaos. The pesky program is able to enter
185 random system without any consent. It installs new add-ons to your IE,
186 Firefox and Chrome stealthily. After then, lots of Davinci ads
187 will pop up on the screen when you surf the Internet. The adware will
188 trace your browsing details for sensitive information. It displays
189 charming ads so as to catch your eyes. Meanwhile, it's rather dangerous
190 when Davinci adware collects your personal information. It
191 could sell your data for illegal activities.</p>
192 <p>Davinci inserts automatic pop-ups and ads onto your
193 IE/Chrome/Firefox after making changes to the default browser settings.
194 Those commercials will cover large part of your web page and prevent you
195 browse website as usual. Right after booting up the PC, you will notice
196 processes of this adware running in the Task Manager. You may stop
197 those unwanted processes from running at Windows star-tup easily,
198 however, those ads are the most trickiest part. This adware may even
199 keep record of your online activities in the background and steal your
200 information from you. Moreover, other threats may take advantage of this
201 adware and come inside without notice. For these reasons, a thorough
202 removal of Davinci is a must. A manual removal guide is
203 provided below for you. But you should keep in mind that manual method
204 is highly risky since any tiny mistake is made may lead to system
205 malfunction. A reliable free antimalware tool is also recommended to
206 you.</p>
207 <h3>How to Delete Davinci?</h3>
208 <p>Method 1: Remove Davinci automatically with
SpyHunter.

209 SpyHunter is a reputable and professional removal tool which can detect
210 and delete various kinds of threats from your computer automatically
211 within minutes. You can follow the simple steps given below to install
212 in on your PC and then use it to remove the threat from your completely
213 completely.</p>
214 <div class="clearfix2">More Browser Hijackers October 15, 2015 Remove Search.autocompletepro.com
Remove Search.autocompletepro.com Search.autocompletepro.com is a browser hijacker that can also
be categorized as a potentially unwanted program. Download Monitoring App Now Filed Under: mSpy
Tagged With: activities, employees, mSPY, software Comments Speak Your Mind Name * Email *
Website Track iPhone I want to track a cell phone without them knowing How Can I Track My Fiance
Text Messages On His Cellphone Can You Track Text Messages with an application? Enhanced Shopping Assistant Backdoorircaryan1 Adwaremegasearch Ads By
Enterprise1 1v17 09 Healer Console Ads Adsbyquizgames Easydocmergetoolbar Thecouponexplorertoolbar </div>
215 <p>Step 1: Download SpyHunter on your computer by clicking on the below button.</p>
216 <p>Downlaod Spyhunter Now.</p>
217 <div align="center">
</div>
218 <p>2. And then double click on the file, and execute it.</p>
219 <div align="center"></div>
220 <div align="center"></div>
221 <p>3.Start a scan on your computer.</p>
222 <div align="center"><img class="img-responsive" alt="SpyHunter-scan"


```

src="remove_adware_spyware_virus_hijacker_files/SpyHunterscan.jpg"></div>
223 <p>4.Once the scan is finished, a message box saying the scan is
224 complete will appear. Click OK button to close the box then click SHOW
225 RESULTS button.</p>
226 <div align="center"></div>
227 <p>&nbsp;</p>
228 <p><strong>Method 2: Manual Davinci Removal Guides:</strong></p>
229 <p>Since the adware can cause various computer issues, you'd better
230 remove this it from your operating system as soon as possible. Since it
231 disables your antivirus program and blocks you from detecting and
232 removing it, you can consider manually removing it manually. Follow the
233 steps below:</p>
234 <div align="center"><a href="download.php" rel="nofollow"></a>
</div>
235 <p>1. Restart the Infected Computer into Safe Mode with Networking</p>
236 <p>Restart your computer and press F8 key constantly when the computer loads.</p>
237 <div align="center"></div>
238 <p>For Windows 7, Windows Vista and Windows XP</p>
239 <p>Restart your computer, immediately, quickly and repeatedly hit F8 key
240 before the Windows start-up screen shows. Select "Safe Mode with
241 Networking", and then press Enter key.</p>
242 <div class="clearfix2">Download Now 22.5 Mb Sep 23, 2015 Win (All) Free
SUPERAntiSpyware Free screenshot View all screenshots... Is there a way i can intercept someones
text messages without touching their phone Free Keylogger Android Download How can I spy on cell
phones without having the phone Incoming and Outgoing Conversations - Can You Spy on Calls? It
offers daily (manual... more Details... Download Now 379 Kb Oct 25, 2014 Win (All) portable Free
HijackThis screenshot View all screenshots... Degrades the performance of the browser with
frequent crashing. Download Now 11.0 Mb May 13, 2015 Vista/7 Free Microsoft Security Essentials
screenshot View all screenshots... It has been designed in such a way anyone can easily operate
this NaviWatcher Ads Removal Tool even if they lack technical skills. So, when comparing the
price of FlexiSPY to another company, make sure you include the VAT or Sales tax in the equation.
One can select for any day of the week or month for scheduling the scan for. The Scan button
will cause AdwCleaner to search your computer for unwanted programs and then display all the
files, folders, and registry entries found on your computer that are used by adware programs. <a
href="vbssosyos.php">Vbssosyos</a> <a href="ads-by-istreamer.php">Ads By Istreamer</a> <a
href="win32generic497472.php">Win32generic497472</a> <a href="poinbag.php">Poinbag</a> <a
href="trojan-stimilik.php">Trojan Stimilik</a> <a href="systemsoappro.php">Systemsoappro</a> <a
href="trojandownloadermsiltruadoc.php">Trojandownloadermsiltruadoc</a> <a
href="w32gosys.php">W32gosys</a> </div>
243
244 <div align="center"></div>
245 <p>For Windows 8</p>
246 <p>(1). Sign out to get the log-in screen</p>
247 <div align="center">
</div>
248 <p>(2). Keep holding down Shift key then click on the Shut Down icon to select Restart</p>
249 <div align="center">
</div>
250 <p>(3). If you do it right, you will see 'Choose An Option' screen. Choose 'troubleshoot'</p>
251 <div align="center"></div>
252 <p>(4). Click on 'Advance Options'</p>
253 <div align="center">
</div>
254 <p>(5). Click on 'Startup Settings'</p>
255 <div align="center"></div>
256 <p>(6). Click on 'Restart'</p>
257 <div align="center"></div>
258 <p>(7). The system will go through a reboot, please wait till you get
259 the following screen. Choose 'Enable safe mode with networking' (or any
260 other option you want to start up the system with)</p>
261 <div align="center"></div>
262 <p>Then you can get into safe mode with networking in Windows 8 and see a desktop like this</p>
263 <div align="center"></div>
264 <p>2. Stop the Processes Related to Windows AntiBreach Module in Windows Task Manager</p>
265 <p>For Windows 7, Windows Vista and Windows XP</p>
266 <p>Press Ctrl+Shift+Esc keys together and end the virus processes in the Processes tab of Windows
Task Manager.</p>
267 <div align="center"></div>
268 <p>For Windows 8</p>
269 <div class="clearfix2">Friends, Each time I opened my system NaviWatcher
Ads constantly appears on my desktop. The program uses aggressive methods and is intended as a
last... more Details... Open the Registry Editor, search and delete NaviWatcher Ads Registry
Entries regedit HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options\msmpeng.exe "Debugger" = 'svchost.exe'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\mssecex.exe "Debugger" = 'svchost.exe'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NaviWatcher Ads
HKEY_LOCAL_MACHINE\SOFTWARE\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet
Settings "WarnOnHTTPSToHTTPRedirect" = '0'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
"WarnOnHTTPSToHTTPRedirect" = '0' HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\SystemRestore "DisableSR" = '1' HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Image File Execution Options\ekrn.exe "Debugger" = 'svchost.exe'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\msascui.exe "Debugger" = 'svchost.exe'
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "3948550101"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "xas"
HKEY_CURRENT_USER\Software\NaviWatcher Ads Turn on Safe Browsing Features to Prevent NaviWatcher
Ads infection in Future IE: How to Activate SmartScreen Filter The latest version of IE 8 & 9 is
enabled with SmartScreen Filter. Automatic NaviWatcher Ads Removal Tool: Getting Started Step 1-
Scanner: Soon after Downloading and installing NaviWatcher Ads Removal tool, select Scan Computer
Now Option to initiate the scanning process. More Adware October 15, 2015 Read SpyHunter review
Read SpyHunter review SpyHunter 4 is a highly effective malware remover with a simple and easy-
to-use interface. Once activated it can detect unsafe websites that can be infected with
NaviWatcher Ads. Download Now 1.64 Mb Dec 18, 2014 XP/Vista/7/8/10 Free Ad-Aware Free Antivirus
screenshot View all screenshots... Powered by esolutions.lt SnapFiles Home Freeware Shareware
Latest Downloads Editor's Selections Top 100 Portable Apps More expand Login/Join Home navigation
Freeware navigation Security Tools Adware and Spyware Removal Freeware Featured Download (Not
limited to freeware) Emsisoft Emergency Kit Emsisoft Emergency Kit Emsisoft Emergency Kit
portable malware removal kit Emsisoft Emergency Kit is a portable malware detection and removable
kit that includes the Emsisoft dual-scan engine as well as portable versions of HiJackFree and
BlitzBlank. By using AdwCleaner you can easily remove many of these types of programs for a
better user experience on your computer and while browsing the web. Many of the users get
confused and consider it to be an useful program and end up installing it themselves. <a
href="lp-playerpage4080-info-pop-ups.php">Lp Playerpage4080 Info Pop Ups</a> <a
href="allvideos283xyzpopups.php">Allvideos283xyzpopups</a> <a
href="windowsdebugcenter.php">Windowsdebugcenter</a> <a href="search-lexside-com.php">Search
Lexside Com</a> <a href="windealist.php">Windealist</a> <a href="two-free-southwest-airlines-
tickets-facebook-scam.php">Two Free Southwest Airlines Tickets Facebook Scam</a> <a
href="downloadersninfbsb.php">Downloadersninfbsb</a> <a href="ads-by-hdqplayer.php">Ads By
Hdqplayer</a> </div>

```

270

271 <p>(1). Press Ctrl+Shift+Esc keys together to get Windows Task Manager</p>

272 <div align="center"></div>

273 <p>(2). Click More details</p>

274 <div align="center"></div>

275 <p>(3). Then scroll down to end the virus processes</p>

276 <p>3. Show Hidden Files</p>

277 <p>(1). Press Win+R to get Run window</p>

278 <div align="center"></div>

279 <p>(2). Type Control Panel in the Run window and hit enter to get Control Panel</p>

280 <div align="center"></div>

281 <p>(3). Click on Appearance and Personalization</p>

282 <div align="center"></div>

283 <p>(3). Click on Folder Options </p>

284 <p>(4). Click on View tab in Folder Options window</p>

285 <p>(5). Tick Show hidden files, folders, and drives under Hidden files and folders tab</p>

286 <div align="center"></div>

287 <p>(6). Click Apply to take effect, then click OK at the bottom of the Folder Options window</p>

288 <p>4. Delete Virus Files</p>

289 <p>(1). Using Registry Editor to delete or adjust all the related registry entries of Windows AntiBreach Module scam virus</p>

290 <p>*Guides to open Registry Editor:</p>

291 <p>Press Win+R key together to get the Run box, type in 'regedit' then click OK, Registry Editor window will pop up</p>

292 <div align="center"></div>

293 <p>(2). Find out and remove the associated files of this adware</p>

294 <p>Kindly remind:</p>

295 <p>1) Several ways that available for unwanted program like Ads By

296 SpeedItUp to penetrate into your system: spam attachment, corrupt

297 website and bundled download etc. To avoid getting malware out of

298 awareness, you could not pay too much attention when enjoying the

299 internet. Especially you are highly recommended to choose the custom

300 installation when adding something new to your program list.</p>

301 <p>2) Adware removal is necessary. Having run out of ways to deal with

302 Davinci Ads, but just gained no positive result? No worries,

303 the following removal tutorials including manual removal, video guide

304 and automatic removal instruction will be greatly helpful. Please feel

305 free to pick one that fix your situation most to help yourself out

306 timely.</p>

307 <p>Why You Need a Removal Tool?</p>

308 <p>Not everyone is a computer geek who can handle the manual removal

309 well. If you are a novice computer user, it will be a better option to

310 remove the Trojan horse by using a removal tool. This will save you much

311 time and trouble. An advanced removal tool, equipped with the latest

312 scanning algorithm, will be able to thoroughly scan your whole system

313 and detect out the Trojan horse as well as other potential threats on

314 your computer. Then, you can easily remove all detected threats within

315 clicks of the mouse. The whole process would not take you much time and

316 damage your system. In addition, the removal tool can also safeguard

317 your computer from future threats. Just download an advanced removal

318 tool and let it serve you right now!</p>

319 <div align="center"></div>

320 <h4>Conclusion


```
321 </h4>
322 <p>Davinci is an annoying adware that can sneak into the
323 computer secretly and is capable to perform some malicious activities.
324 The victim browser will have its domain as the default homepage and you
325 cannot change it back. You won't get the good search results since some
326 unwanted malicious advertisements which may contain viruses pop up
327 crazily. Furthermore, your computer will suffer from many potential
328 threats as it can help other malware or spyware to invade your computer.
329 As a result, the computer performance will be very slow and your work
330 efficiency will be affected seriously on the computer.</p>
331 <div class="addtoany_share_save_container addtoany_content_bottom"><div style="line-height:
332 32px;" class="a2a_kit a2a_kit_size_32 addtoany_list a2a_target" id="">
333 </div></div> <!--END .entry-content .article-->
334 <div class="clearfix"></div>
335 </div>
336
337
338 <!--BEGIN .entry-meta .entry-footer-->
339 <div class="entry-meta entry-footer row">
340 <div class="col-md-6">
341
342 <div class="entry-categories"> <a
343 href="category/adware/" rel="category tag">adware</a></div> <!--END .entry-meta .entry-
344 footer-->
345 </div>
346
347 <div class="col-md-6">
348 <div class="share-this">
349
350 </div>
351 </div>
352
353 </div>
354
355
356
357
358 </div>
359
360
361 <!--BEGIN .navigation-links-->
362 <div class="navigation-links single-page-navigation clearfix row">
363 <!--END .navigation-links-->
364 </div>
365 <div class="clearfix"></div>
366
367
368
369
370
371 <div id="comments">
372 <span class="comments-title-back"><h3 class="comment-title">&nbsp;</h3>
373 </span></div>
374 </div>
375
376
377
378
379
380 <div align="center"></div>
381 <p>&nbsp;</p>
382 <p>&nbsp;</p>
```

```
383 <a href="download.php" rel="nofollow"><div align="center">
</div></a>
384 <!--BEGIN #secondary .aside-->
385 <div id="secondary" class="aside col-sm-6 col-md-4"><!--END #secondary .aside-->
386 <a href="download.php" rel="nofollow"><div align="center"></div>
</a>
387 <a href="download.php" rel="nofollow"><div align="center"></div></a>
388 </div>
389
390
391 <!--END #content-->
392 </div>
393
394 <!--END .container-->
395 </div>
396
397
398
399 <!--END .content-->
400 </div>
401
402
403
404
405 <!--BEGIN .content-bottom-->
406 <div class="content-bottom">
407
408 <!--END .content-bottom-->
409 </div>
410
411 <!--BEGIN .footer-->
412 <div class="footer">
413
414
415 <!--BEGIN .container-->
416 <div class="container container-footer">
417
418
419
420
421 <div class="clearfix2">Click Here to Scan Windows PC Now Severe Impacts of NaviWatcher Ads on
your PC & Browser Adware RemovalNaviWatcher Ads employs deliberate techniques and get installed
on targeted system. Messages of your children, GPS data and even restriction of calls from
suspicious contacts will be very beneficial! <a
href="trojandownloaderagentejh.php">Trojandownloaderagentejh</a> <a href="ads-by-godzilla-
shopper.php">Ads By Godzilla Shopper</a> <a
href="websearchsearchisbestmyinfo.php">Websearchsearchisbestmyinfo</a> <a
href="adcloud.php">Adcloud</a> <a href="trojanpswonlinegamesdat.php">Trojanpswonlinegamesdat</a>
<a href="easylink.php">Easylink</a> <a href="rocketfindcom.php">Rocketfindcom</a> <a
href="websearchsearchmaniainfo.php">Websearchsearchmaniainfo</a> </div>
422
423 Copyright © 2015 - 2016 All Rights Reserved<!--END .container-->
424 </div>
425
426
427
428
429
430 <!--END .footer-->
431 </div>
432
433
```

```
<!--END body-->
434 <!-- Start of StatCounter Code for Default Guide -->
435 <script type="text/javascript">
436 var sc_project=10659930;
437 var sc_invisible=1;
438 var sc_security="804c650f";
439 var scJsHost = (("https:" == document.location.protocol) ?
440 "https://secure." : "http://www.");
441 document.write("<sc"+"ript type='text/javascript' src='" +
442 scJsHost+
443 "statcounter.com/counter/counter.js'"></"+"script">");
444 </script>
445 <noscript><div class="statcounter"><a title="shopify traffic
446 stats" href="http://statcounter.com/shopify/"
447 target="_blank"></a></div></noscript>
450 <!-- End of StatCounter Code for Default Guide -->
451
452
453
454 </body><!--END html(kthxbye)--></html>
```

<http://fixspywarenowreview.com/davinci.php>

<http://spyware-fix.com/malbifrose-z.php>

<http://systemrepairspywareremoval.com/trojanwin32jorikkoobfacebc.php>

<http://uninstalling.browser.hijack.check.getridofspywareonpc.com/>

<http://www.adwarefix2016.com/prizepartyhijacker.php>

<http://www.fixadwareonmac.com/pcscanner2011net.php>

<http://www.fixandrepairspyware.com/dealsaddon.php>

<http://www.gpsfixadware.com/marezercom.php>

<http://www.smartrepairspyware.com/ekoblock.php>

<http://www.systemrepairadware.com/videostripe.php>

<http://www.systemrepairspyware.com/gaelicuma.php>

<http://spywarerepairfree.com/immunizr.php>

How to Remove rkill.com – rkill.com Removal Ways

Posted on by [admin](#)



My computer is affected by the rkill.com virus and become strange and slow. It is easy to freeze at startup, shut down computer and other activities. I scanned the whole system with my advanced security software, but the antivirus can't seem to solve rkill.com. I don't want to leave my computer in a mess. What action should I take to clean up the computer? Trojan virus delete any clues that will help me a lot.

rkill.com Information:

- ➔ FileDescription: - ➔
- ➔ LegalCopyright: - ➔
- ➔ ProductName: - ➔
- ➔ ProductVersion: - ➔
- ➔ Company: - ➔
- ➔ FileMd5: 8cc534ecee1b4213af8c92bea9271c2c ➔
- ➔ FileVersion: - ➔
- ➔ Memos: - ➔
- ➔ [Download rkill.com fix tool](#) ➔
- ➔ 88100714 ➔

rkill.com usually gets into the computer without user's knowing and consent, and then suddenly pop ups the infecting warning just mentioned above on the computer. This is a trick the hacker use to promote their rogue antivirus program, they want to make users believe that there is a serious security problem on their computers and you should immediately fix it, and the best or most powerful it recommending to you is the rogue program designed by the same hacker. When you meet such thing on your computer, please ignore everything about the rogue program, you just need to quickly employ an authentic security program to help you get rid of rkill.com infection before the rouge program successfully getting into your computer.

Conclusion:

rkill.com is a dangerous computer virus which can destroy the infected computer and record your personal information. If you're not careful when you visit websites or use online resources, your computer is vulnerable to virus attacks. It has the ability to slow down the computer performance seriously. The computer user's personal information may be got by the virus makers through the virus, such as credit card or bank account

details and social contacts' information. Therefore, the best way to cancel the malicious behaviors of rkill.com is to get rid of it as soon as possible.

The above manual removal is quite dangerous and complicated, which needs sufficient professional skills. Therefore, only computer users with rich computer knowledge are recommended to implement the process because any errors including deleting important system files and registry entries will crash your computer system.

Manual Removal Guides:

Please carefully read the notes before you start to remove any file :This guide is based on the first version of rkill.com, but this infection keeps adding its features and updating its codes, files and locations, thus you may not be able to find out all its related files listed above. It requires expert skills and experience to identify all the files of rkill.com infection, if you are not familiar with it, do not risk to delete any file by yourself, since you may disable your PC for deleting wrong files which are crucial for your system. This guide is just for reference, we do not promise it will work for all the victims of different PCs in varied situations and conditions. Any problem and consequence incurred by your mistake should be borne by yourself.

Step1: Stop the virus processes in the Windows Task Manager by Pressing Ctrl+Alt+Del keys together

Step2: Show all hidden files:

- ➔ Close all programs so that you are at your desktop. ➔
- ➔ Click on the Start button. This is the small round button with the Windows flag in the lower left corner.
- ➔ Click on the Control Panel menu option. ➔
- ➔ When the control panel opens click on the Appearance and Personalization link. ➔
- ➔ Under the Folder Options category, click on Show Hidden Files or Folders. ➔
- ➔ Under the Hidden files and folders section select the radio button labeled Show hidden files, folders, or drives.
- ➔ Remove the checkmark from the checkbox labeled Hide extensions for known file types.
- ➔ Remove the checkmark from the checkbox labeled Hide protected operating system files (Recommended).
- ➔ Press the Apply button and then the OK button. ➔

Step3: Erase the Virus associated files

Step4: Terminate these Registry Entries created by rkill.com.

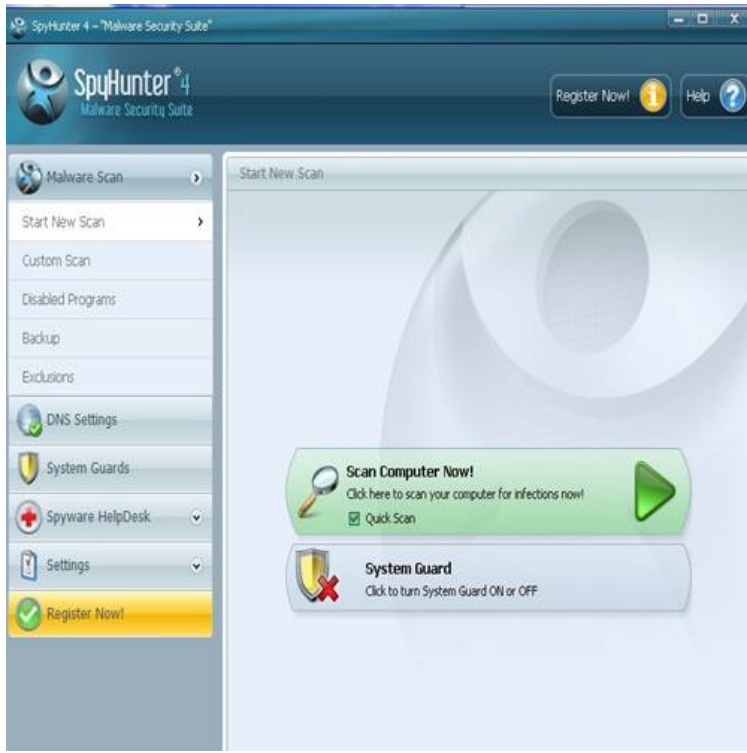
Method: Automatic Removal with SpyHunter

Step 1: Press the following button to download SpyHunter



Step 2: Save it into your computer and click on the Run choice to install it step by step.

Step 3: Click Finish then you can use it to scan your computer to find out potential threats by pressing Scan computer now!



Step 4: Tick Select all and then Remove to delete all threats.



Useful Automatic removal rkill.com with SpyHunter from the Infected Computer

You can use the manual removal procedures above step by step to get rid of rkill.com, but it is quite complicated actually. So, if you are not a computer savvy, I recommend you to solve this problem with removing rkill.com automatically with SpyHunter.

Step 1: Download Spyhunter antivirus program by clicking the icon below:



Step 2. Install SpyHunter on your computer step by step.

Step 3. After finishing installation, you need to do a full scanning with SpyHunter to find out every threats in your computer. After that, you should select every detected threats and remove them all.



Step 4. Reboot your computer and check it again to make sure that rkill.com is terminated completely

rkill.com is a high-risk Trojan virus infection designed by cyber criminals recently, which bursts in the life of many computer users and causes serious damages to the infected computer. The hateful virus is brimful of mischief. Once it gets in the target computer, it is able to be hidden deep so as to undermine the entire system. Many computer users have no clue until the computer becomes worse and worse. It also can confuse antivirus programs with advanced technology so that it won't be removed by any removal tools. The virus makers may use every opportunity to control the computer remotely. With the cover of the virus, they can remove or modify your important documents wantonly and steal or encrypt your personal data, resulting in inconvenience as well as unnecessary losses. Therefore, getting rid of rkill.com is quite urgent.

The above manual removal is quite dangerous and complicated, which needs sufficient professional skills. Therefore, only computer users with rich computer knowledge are recommended to implement the process because any errors including deleting important system files and registry entries will crash your computer system.

rkill.com is located in:

→ C:/Documents and Settings/Utente/Documenti/Download/rkill.com →



SpyHunter is a powerful, real-time anti-spyware application certified by West Coast Labs' Checkmark Certification System and designed to assist the average computer user in protecting their PC from malicious threats.

[Click Here Download Now www.enigmasoftware.com](http://www.enigmasoftware.com)

Similar Information:

[What is rac9ut.exe and How to Remove rac9ut.exe Virus Safely](#)

[Clean Up recipe10-13.exe - Complete and Easy recipe10-13.exe Removal](#)

[How to Uninstall and Remove ric.exe from Computer](#)

[rassymi.exe Removal Instruction - How Could You Remove rassymi.exe from Your PC](#)

[Cannot Remove rbrcl55.bpl virus](#)

[How to Clean Up rmcpulite-x86.exe - Get Rid of rmcpulite-x86.exe Right Now](#)

[Helpful Guidance On rtlupd.exe Removal](#)

[HackTool:rasadhlp.dll.dskp Removal - How to Remove HackTool:rasadhlp.dll.dskp easily](#)

[The Most Effective Way to Remove pathfinderrfstatus.dll from PC](#)

[hexedfull.exe Removal Guide - How to Get Rid of hexedfull.exe for Good](#)

[Removing dsmsg.dll with Practicable Tips](#)

[tn3d.dll Removal Guide - How to Get Rid of tn3d.dll for Good](#)

[Good Way to Clean the pcmlcatevouch.dll from Computer](#)

[ctxcpubulk.dll Removal](#)

[hspicturebox.dll Removal](#)

[How to Remove g21.exe within Few Clicks](#)



rkill.com Details


Share:  0  Like 0  Tweet  Share  Submit  Pin it  More



This is a malware file.

This file is considered malware because it exhibits certain malicious, intrusive or otherwise undesirable behavior. Malware files may alter a system's settings, execute malicious code, hide to avoid detection, download unwanted software and potentially allow hackers to gain remote access to a computer without the computer user's consent or knowledge.

File Analysis

File Name:	rkill.com
Threat Level:	 8/10
Detection Count:	21
File Type:	Command, executable file
MD5:	25b4aeb25fe427f7f7228786cf2526
Path:	%USERPROFILE%\Escritorio
Mime Type:	application/x-msdos-program
Description:	The rkill.com file is installed and associated with <u>Trojan.Downloader.Tracur.X</u> . This entry has been reported 21 times.

File Variations:

#	Detection Count	File Size (bytes)	MD5
1	1,581	363,520	0d0ab98088d3b46d0a1c08005910aa5c
2	340	363,520	30b3be082c2c4f5ceba48228868a9c55
3	321	363,520	2b5cfefa206020111318bed49eb7ebfa
4	98	364,032	af270c92821a9a924fa83801e82dd23e
5	77	363,520	df63f95c8d3066f08d6adf24902c068a
6	66	363,520	62b04c274f1b47a46e3c2918bbd02d41
7	49	363,520	af81918581a3df0c8a32485187a83851
8	49	363,520	c653e7964e5d461d20f027c218c838e9
9	37	363,008	255a71f7db6dd6d3e3b33ce68365f64b
10	35	363,520	ff4d230a167016a67293cc5148014621
11	30	363,520	1c3c603a2b52b71c3c6665a7299dfca9
12	109	263,168	ba0bfa88eea070836bde3ae479eaf3c
13	256	420,864	a7968511db9cf934ab3d1a8615f05229
14	44	433,152	08c7a0c60006942ab5df86922d6bd797
15	100	262,656	f0c3eb8d0ac7e927576e31c747ce4836

16	269	363,008	3252d582cdcd3ad154cf097faf3622da
17	219	262,656	4c445fbdf92fd2dc5d9e18c4f2a7ae2
18	206	363,008	74203ab4927386c457e9cc2e3e61f94e
19	75	363,520	2ccb34bd36518cded6e918f726397586
20	19	246,536	d49d7b6f1f27e627179ecffba13cebff
21	75	363,008	b050acd997d84253046d487139f4caa4

Other programs which contained the file name rkill.com:

Rkill

Last Updated:

07/04/2011 11:23:26 EST

unhide.exe Details

Share: 0 Like 0 Tweet Share Submit Pin it More



This is a malware file.

This file is considered malware because it exhibits certain malicious, intrusive or otherwise undesirable behavior. Malware files may alter a system's settings, execute malicious code, hide to avoid detection, download unwanted software and potentially allow hackers to gain remote access to a computer without the computer user's consent or knowledge.

File Analysis

File Name:	unhide.exe
Threat Level:	8/10
Detection Count:	26
File Type:	Executable File
File Size:	606.1K (606104 bytes)
MD5:	8df658a0867e80c05d7bd6fc1e128caf
Path:	D:\Downloads\Maleware
Mime Type:	application/x-msdos-program
Description:	The unhide.exe file is installed and associated with <u>Trojan.Downloader.Tracur.X</u> . This entry has been reported 26 times.
Last Updated:	07/04/2011 11:23:26 EST