ПОДШИТО
25.11.2013, 8:54
КЛЕРК, ОКРУЖНОЙ СУД США
ЗАПАДНЫЙ ОКРУГ ШТАТА ТЕХАС
[подпись]
ЗАМЕСТИТЕЛЬ

СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
ОКРУЖНОЙ СУД ЗАПАДНОГО ОКРУГА ШТАТА ТЕХАС
ОТДЕЛ ГОРОДА ОСТИН

КОРПОРАЦИЯ MICROSOFT, Вашингтонская компания, Истец против JOHN DOES 1-8 (НЕНАЗВАННЫЕ 1–8), УПРАВЛЯЮЩИЕ КОМПЬЮТЕРНЫМ БОТНЕТОМ, ПРИЧИНИВШИМ УЩЕРБ КОМПАНИИ MICROSOFT И ЕЕ КЛИЕНТАМ, Ответчики.	§ § § § § § § § § § § § §	ДЕЛО НОМЕР: **A13CV1014** **СКРЕПЛЕНО ПЕЧАТЬЮ**

ЖАЛОБА

Истец КОРПОРАЦИЯ MICROSOFT («Microsoft») этим подает жалобу и дает свои показания против JOHN DOES 1-8 (Ответчики Doe), которые управляют ботнетом «ZeroAccess» с использованием адресов Интернет Протоколов (IP) и доменов Интернет, указанных в Приложении А, («IP адреса и домены, используемые ZeroAccess для управления деятельностью, связанной с мошенничеством») в следующем порядке:

ОСНОВАНИЕ ДЕЙСТВИЙ

1. Данный иск основан на: (1) Законе о компьютерном мошенничестве и злоупотреблении, 18 U.S.C. § 1030; (2) Законе о конфиденциальности в электронных коммуникациях, 18 U.S.C. § 2701; (3) Посягательстве на торговую марку в соответствии с Законом Ланхэма, 15 U.S.C. § 1114 и след. (4) Указании ложного происхождения в соответствии с Законом Ланхэма, 15 U.S.C. § 1125 (a); (5) Причинении вреда торговой марке в соответствии с Законом Ланхэма, 15 U.S.C. § 1125 (c); (6) Законах о Посягательстве на движимое имущество; (7) Несправедливом обогащении, и (8)

Конверсии. Microsoft стремится получить возмещение ущерба со стороны операторов сети компьютеров, известной как «ZeroAccess» ботнет, контролируемой с помощью IP адресов и доменов, что причинило и продолжает причинять непоправимый ущерб Microsoft, ее клиентам и общественности.

СТОРОНЫ

2. Истец Microsoft является корпорацией, надлежащим образом организованной и действующей в соответствии с законодательством штата Вашингтон, со штаб-квартирой и основным местом деятельности в Редмонде, штат Вашингтон.

3. John Doe 1 контролирует IP адреса ZeroAccess 188.40.114.195 и 188.40.114.228, а также Домены qvhobsbzhzhdhenvzbs.com, mbbcmyjwgypdcujuuvrlt.com, wuyigrpdappakoahb9.com, jzlevndwetzyfryruytkzkb.com, glzhbnbxqtjoasaeyftwdmhzjd.com, kttvkzpwufmrditdojlgytxyb.com, vgfsowmleomwconnxmnyfhle.com и vmtsukcbbqmmndojqirbbij.com, которые изложены в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft проинформирован и считает, и в этой связи утверждает, что с John Doe 1 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: 15528566292361-b434c0@whoisprivacyservices.com.au, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net, privacy@dynadot.com, Hetzner Online AG («Hetzner»), в Datacenter 10, Stuttgarter Strasse 1, Д- 9710 Гунценхаузен , Германия, abuse@hetzner.de. IP адреса ZeroAccess 188.40.114.195 и 188.40.114.228 обозначаются как IP -адреса, поддерживаемые Hetzner.

4. John Doe 2 контролирует IP адреса ZeroAccess 83.133.120.185 и 83.133.120.187, а также Домены gozapinmagbclxbwin.com, nbqkgysciuuhadgpjfquvpu.com, cjelaglawfoyidgyapv.com, jpciukjdkqxgreoikpgya.com, qhdsxosxtvmhurwezsipzq.com, omakfdwkhrpqudxvapy.com, chvhcncpqttfpcibtmetg.com, ezcfogjitbqwnornezx.com, rwdtklvrqnffdqkyuugfklip.com, uinrpbrfrnqggtorjdpqg.com, xlotxdxtorwfmvuzfuvtspel.com, mkvrpknidkurcrftiqsfjqdxbn.com, waajenyndxxbjolsbesd.com, jgisypzilnrperlwcionbt.com и fwmavqvphidhnrxcxvcnx.com, которые изложены в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft в курсе дела и считает, и в этой связи утверждает, что с John Doe 2 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: admin@overseedomainmanagement.com, 1af43616fl37467387028c41f73e7f0a.protect@whoisguard.com, jgou.veia@gmail.com,

xlotxdxtorwfmvuzfuvtspel.com@domainsbyproxy.com, mkvrpknidkurcrftiqsfjqdxbn.com@domainsbyproxy.com, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net; privacy@dynadot.com; Greatnet New Media («Greatnet») по адресу Brentenstrasse 4a, D-83734 Hasusham, Германия; на Stromstrabe 11-5, 10555 Берлин, Германия; abuse@greatnet.de. IP адреса ZeroAccess 83.133.120.185 и 83.133.120.187 обозначаются как IP-адреса, поддерживаемые Greatnet.

5. John Doe 3 контролирует IP адрес ZeroAccess 195.3.145.108 и домены dclixvfpttrlcnindvrnyeic.com, evtrdtikvzwpscvrxpr.com, atenrqqtfrzozqrqbdzwkxzyuc.com, и oqcllyhefbhhaijaxq.com, указанные в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft в курсе дела и считает и в этой связи утверждает, что с John Doe 3 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: bdd243a7cae540e08484e24e71552520.protect@whoisguard.com, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net; RN Data SLA («RN Data») в Maskavas 322, LV-1063, Рига, Латвия; admin@altnet.lv. IP адрес ZeroAccess 195.3.145.108 обозначается как IP-адрес, поддерживаемый RN Data.

6. John Doe 4 контролирует IP адрес ZeroAccess 178.239.55.170 и домены jgvkfxhkhbbjoxggsve.com и litcyleyzrglkulaifkrx.com, указанные в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft в курсе дела и считает и в этой связи утверждает, что с John Doe 4 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: Netrouting Ellada Projects BV («Netrouting») в Boylewg 2, 3208 KA, Spikenisse, Нидерланды; abuse@netrouting.com; privacy@dynadot.com. IP адрес ZeroAccess 178.239.55.170 обозначается как IP-адрес, поддерживаемый RN Data.

7. John Doe 5 контролирует IP адреса ZeroAccess 217.23.3.225, 217.23.3.242, и 217.23.9.247, а также домены hzhrjmeeczcgxodmqyz.com, fnyxzjeqxzdpeocarhljdmyjk.com, sqdfmslznztfozshtidmigmsbh.com, vdlhxlmqhfafeovqohwrbaskrh.com, nmfvaofnginwocnidecxnpcs.com, euuqddlxgrnxlrjjbhytukpz.com, vzsjfnjwchfqrvylhdhxa.com, vjlvchretllifcsgynuq.com, dxgplrlsljdjhqzqajkcau.com, qbsiauhmoxfkrgfqey.com, ssarknpzvpkteqnaia.com, и adhavzpbykyffaxqtts.com, которые указаны в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft в

курсе дела и считает и в этой связи утверждает, что с John Doe 5 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: 16520144097161-049eel@whoisprivacyservices.com.au, 433f8f3c35244b459c599e0b004701c4.protect@whoisguard.com, vjlvchretllifcsgynuq.com@domainsbyproxy.com, jgou.veia@gmail.com, privacy@dynadot.com, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net, a8bd2de2c86841008163bb70ec85185e.protect@whoisguard.com, 7fele2f261e848abb774e42e6ffal615.protect@whoisguard.com; WorldStream в Industriestaat 24, 2671CT Naaldwijk, Нидерланды; abuse@worldstream.nl. IP адреса ZeroAccess 217.23.3.225, 217.23.3.242, и 217.23.9.247 обозначаются как IP-адреса, поддерживаемые Worldstream.

8. John Doe 6 контролирует IP адреса ZeroAccess 46.249.59.47 и 46.249.59.48, а также домены loanxohaktcocrovagkaa.com, mxyawkwuwxdhuaidissclggy.com, erspiwscuqslhjflgbbgcfbc.com, spujplpdupiwbghiedhqeja.com, xttfdqrsvlkvmtewgiqolttqi.com, jlcemszzlsfvtvwsszrysooca.com, eagdbqufytdxvzbavzriwzgw.com, и spujplpdupiwbghiedhqeja.com, указанные в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft в курсе дела и считает и в этой связи утверждает, что с John Doe 6 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: Serverius Holding B.V («Serverius») в De Linge 26, 8253 PJ, Dronten, Нидерланды; abuse@serverius.nl, b894a578787a6d5767d4f3cad9e25b63-1429447@contact.gandi.net, privacy@dynadot.com. IP адреса ZeroAccess 46.249.59.47 и 46.249.59.48 обозначаются как IP-адреса, поддерживаемые Serverius. Microsoft в курсе и утверждает, что с John Doe 6 также можно связаться через третье лицо Майкела Уерлингза (Maikel Uerlings) по электронному адресу: cust597@serverius.com.

9. John Doe 7 контролирует IP адреса ZeroAccess 46.19.137.19, 81.17.18.18, и 81.17.26.189, указанные в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft в курсе дела и считает и в этой связи утверждает, что с John Doe 7 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: Private Layer Inc. («Private Layer») в Zurcherstrasse 161, SPB 101280, 8010 Цюрих, Швейцария; at SwissPost 9865, Zurcherstrasse 161, 8010 Цюрих, Швейцария; abuse@privatelayer.com; Hossein Abili Nejad в Hasen Tape stl, Баку, az2156, Азербайджан; hamihost@gmail.com. IP адреса ZeroAccess 46.19.137.19, 81.17.18.18, и 81.17.26.189 обозначаются как IP-адреса, поддерживаемые Private Layer.

10. John Doe 8 контролирует IP адреса ZeroAccess 94.242.195.162, 94.242.195.163, и 94.242.195.164 указанные в Приложении А, которые используются не по назначению, чтобы причинить вред Microsoft, ее клиентам и общественности. Microsoft в курсе дела и считает и в этой связи утверждает, что с John Doe 8 можно связаться напрямую или через третьих лиц, используя следующую контактную информацию: Root SA («Root») в 3, op der Poukewiss, 7795 Roost-Bissen, Люксембург; abuse@as5577.net. IP адреса ZeroAccess 94.242.195.162, 94.242.195.163, и 94.242.195.164 обозначаются как IP-адреса, поддерживаемые Root.

11. Третьи стороны VeriSign Naming Services и VeriSign Global Registry Services (далее «VeriSign») являются доменным регистратором, который осуществляет надзор за регистрацией всех доменных имен, оканчивающихся на «.com», включая все «.com» домены ZeroAccess. Verisign Naming Services находится по адресу: 21345 Ridgetop Circle, 4th Floor, Dulles, Virginia 20166. VeriSign Global Registry Services расположен по адресу: в 12061 Bluemont Way, Reston, Virginia, 20190.

12. Ответчики владеют, используют, контролируют и поддерживают ботнет ZeroAccess и ведут свою деятельность под IP адресами и доменами злоумышленного использования ZeroAccess (ZeroAccess Fraud Control IP Addresses and Fraud Control Domains).

13. Microsoft позже внесет изменения в эту жалобу с указанием истинных имен ответчиков Doe, когда они будут установлены. Microsoft будет проявлять должную осмотрительность, чтобы определить истинные имена ответчиков Doe, а также их контактную информацию.

14. Microsoft осведомлена и считает, и, следовательно, утверждает, что каждый из фиктивно именуемых Doe Ответчиков отвечает тем или иным образом за причинение вреда Microsoft, а также то, что этот вред был непосредственно обусловлен действиями ответчиков Doe.

15. Ответчики Doe предоставили контактную информацию для доменов Bamital и IP -адресов, указанных в Приложении А к настоящей жалобе.

16. Действия и бездействие, описанные здесь, были предприняты Ответчиками каждым по отдельности, и это были действия и упущения, которые были уполномочены, контролируемы, направлены или разрешены Ответчиками, и / или это были действия и упущения, в которых Ответчики принимали участие, оказывали содействие или иным образом их поощряли, и это те действия, по которым каждый Ответчик несет

ответственность. Каждый Ответчик участвовал в действиях, изложенных ниже, тем, что каждый Ответчик знал о таких действиях и упущениях, оказывал помощь и получал выгоду от этих действий и упущений, в целом или частично. Каждый из Ответчиков являлся сообщником остальных Ответчиков в действиях, далее описанных, и действовал в рамках и масштабах своих полномочий и с разрешения и согласия других Ответчиков.

ЮРИСДИКЦИЯ И МЕСТО

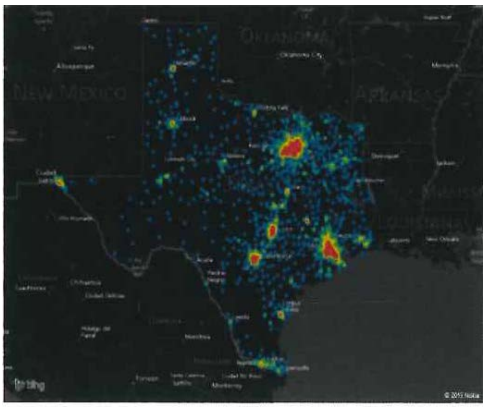
17. Данный иск основан на нарушениях Ответчиками Федерального закона о компьютерном мошенничестве и злоупотреблении (18 U.S.C. § 1030), Закона о конфиденциальности электронных коммуникаций (18 U.S.C. § 2701) и Закона Ланхэма (15 U.S.C. § § 1114 и 1125). Таким образом, Суд обладает необходимой юрисдикцией по данному иску на основании 28 U.S.C. § 1331. Данный иск также включает в себя и вопрос посягательства на движимое имущество, незаконное обогащение, конверсию и халатность. Соответственно, Суд обладает необходимой юрисдикцией по данному предмету согласно 28 U.S.C. § 1367.

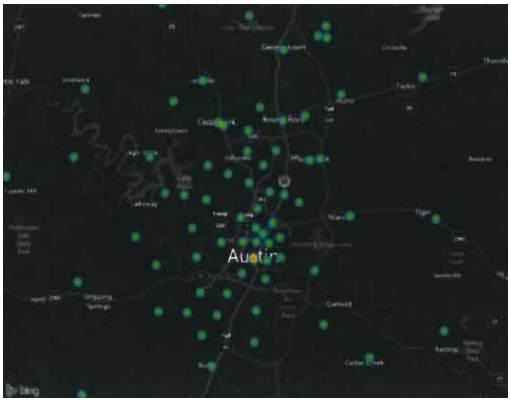
18. На основании информации, которая имеется, Ответчики поддерживают работу компьютеров и интернет-сайтов и занимаются также иной деятельностью, пользуясь привилегиями для ведения бизнеса, которая состоит в использовании определенных инструментов, расположенных в Техасе и Западном округе штата Техас для осуществления действий, обжалуемых в настоящем документе.

19. Ответчики, как утверждается, занимались своей деятельностью в Техасе и Западном округе штата Техас, направляя вредоносный компьютерный код на компьютеры индивидуальных пользователей, расположенных в Техасе и Западном округе штата Техас, пытаясь заразить компьютеры этих пользователей вредоносным кодом и сделать эти компьютеры частью «ботнета», который используется, чтобы причинить вред Microsoft, ее клиентам и общественности. На следующем **рисунке 1** изображено географическое положение компьютеров пользователей в Техасе и Западном округе штата Техас, на которые Ответчики, как известно, направляли вредоносный код, пытаясь заразить эти компьютеры и сделать их частью ботнета:

Рисунок 1.

Техас **Остин**





20. Ответчики предприняли действия, зная то, что такие действия могут нанести вред компьютерам пользователей, расположенным в Западном округе штата Техас, причиняя тем самым ущерб Microsoft, ее клиентам и другим лицам, находящимся в Западном округе штата Техас и других местах в Соединенных Штатах. Таким образом, Суд имеет личную юрисдикцию над Ответчиками.

21. В соответствии с 28 U.S.C. § 1391 (b), место проведения соответствует данному судебному округу. Значительная часть событий или упущений, породивших претензии от Microsoft, вместе со значительной частью имущества, являющегося предметом претензий Microsoft, относятся к данному судебному округу. Место проведения соответствует данному судебному округу согласно 28 U.S.C. § 1391 (c), потому что Ответчики могут иметь личную юрисдикцию в этом судебном округе.

ОБСТОЯТЕЛЬСТВА ДЕЛА

Программное обеспечение Microsoft, услуги и репутация

22. Компания Microsoft® является поставщиком операционной системы Windows®, веб-браузера Internet Explorer®, поисковой системы Bing®, а также рекламной площадки Bing® Ads, а также разного другого программного обеспечения и услуг. Microsoft вложила значительные ресурсы в разработку высококачественных продуктов и услуг. В связи с высоким качеством и эффективностью продуктов и услуг компании Microsoft, а также со значительными расходами корпорации Microsoft на продвижение на рынок своих товаров и услуг, Microsoft создала значительную ценность для своих клиентов, создала сильный бренд и сделала имя Microsoft известным мировым брендом, который стал хорошо узнаваемым в пределах своих каналов торговли. Microsoft имеет

зарегистрированные товарные знаки, представляющие качество ее продукции и услуг, в том числе Microsoft®, Windows®, Internet Explorer®, а также Bing®. Копии регистрационных номеров товарных знаков 2872708, 2463526, 2277112 и 3883548 для товарных знаков Microsoft, Windows, Internet Explorer и Bing, приводятся в Приложении С к настоящей жалобе.

Интернет-реклама и мошенничество, связанное с «кликами»

23. Интернет-реклама является индустрией с оборотом в миллиарды долларов в год. В США расходы на онлайн рекламу достигли $20,1 млрд. за первую половину 2013 года, и растут на 18 % в год. Размер данной индустрии и ее быстрый рост в сочетании с высокой технической и организационной сложностью сделал сферу интернет-рекламы привлекательной средой для киберпреступников, которые разработали большое количество схем манипулирования бизнес-моделью интернет-рекламы, перекачивая тем самым много миллионов долларов в год. Киберпреступники разработали методы получения контроля над компьютерами пользователей, как правило, путем заражения компьютеров вредоносными программами, известными как «вредоносные программы».

24. Microsoft заключает контракты с компаниями, которые хотят размещать рекламу в Интернете. Через платформу Microsoft Bing Ads рекламодатели могут управлять своими интернет-кампаниями, используя результаты своих прошлых рекламных кампаний для планирования будущих кампаний в Интернете. Microsoft размещает рекламу также и в других местах, на сайтах третьих лиц, именуемых «издатели», которые также могут участвовать в рекламной программе Microsoft. Google, Yahoo! и другие также обеспечивают крупномасштабные рекламные площадки, аналогичные Bing Ads.

25. Пользователь во время просмотра сайта издателя может нажать на рекламу, которая переведет его на сайт рекламодателя, где будет отображаться дополнительная информация о рекламируемом продукте или услуге. Целью рекламодателя является поощрить конечного пользователя принять дополнительные меры - например, запросить больше информации или купить товар или услугу. Эти дополнительные действия, предпринятые на сайте рекламодателя, могут отслеживаться и контролироваться рекламодателями.

26. В рекламной модели «оплата за клик», когда потребитель нажимает на рекламу, рекламная площадка снимает деньги с рекламодателя и платит издателю сайта, на котором был произведен «клик». Рекламодатели, однако, как правило, не платят за

клики сомнительного качества или происхождения или которые являются нелегитимными. Система оплаты за клик позволяет издателям получать прибыль за то время, усилия и деньги, которые были вложены в разработку интересных и полезных веб-сайтов, не требуя того, чтобы издатели непосредственно взимали с пользователей плату за доступ к веб-сайтам. Рекламодатели получают выгоду от размещения рекламы на тех веб-сайтах, которые могут привлечь конечных пользователей, которые заинтересованы в данной продукции или услугах. В модели оплаты за клик, рекламодатели получают пользу, непосредственно передавая информацию тем лицам, которые, нажав на рекламу, проявляют интерес к их продукции или услугам.

27. Система оплаты за клик, однако, не застрахована от мошенничества. Недобросовестные издатели могут, например, использовать автоматизированные скрипты, компьютеры конечных пользователей, зараженные вредоносными программами или наемных людей для того, чтобы генерировать большое количество кликов на рекламные объявления, размещенные на своих веб-сайтах с помощью Bing Ads или других рекламных площадок. Эти методы создают имитацию законного пользователя, щелкнувшего на рекламу, с единственной целью получения платы за клик, но не отражают какого-либо интереса к рекламируемому продукту или услуге. Такие клики считаются мошенническими, а такие действия называются «клик-мошенничество». Издатель, который занимается клик-мошенничеством, может получать нечестную прибыль, потому что за каждый клик издателю платит рекламодатель, чья реклама была нажата.

28. Есть более сложные схемы, когда злоумышленники могут генерировать большое количество недействительных кликов путем перенаправления веб-браузеров невинных конечных пользователей на веб-сайты, обманным путем вынуждающие конечных пользователей нажимать на рекламу в Интернете. Методы для направления пользователей на конкретные веб-сайты могут включать в себя инсталляцию вредоносного ПО на компьютеры конечных пользователей, которое вынуждает пользователей посещать сайты или приобретать интернет-трафик у лиц, которые контролируют такие вредоносные программы. Сеть таких компьютеров, зараженных вредоносными программами данного класса, называется ботнет и может генерировать огромное количество мошеннических кликов на рекламные объявления или веб-сайты без ведома и согласия жертвы, платформы интернет-рекламы и поставщиков технологий, таких как Microsoft. Ботнеты, которые специализируются в этих целях, называются «клик-ботами».

29. «Плохой трафик», полученный при помощи таких ботнетов, продается и покупается в сложной экосистеме брокеров и торговли трафиком. Стороны, которые покупают плохой трафик, сознательно или бессознательно, в конечном итоге могут извлечь из этого выгоду, используя его для создания большого количества кликов за рекламные объявления, размещенные на веб-сайтах. Рекламодатели, которые заплатили за рекламу в Интернете, ожидая того, что она будет работать законными методами, в конечном итоге могут заплатить за недействительные клики, генерируемые с помощью этих схем.

30. Конечные пользователи также могут пострадать от клик-мошенничества. Их компьютеры могут быть задействованы в незаконных схемах, результаты их браузеров могут контролироваться, а производительность самих компьютеров ухудшаться. После того, как компьютер пользователя заражается вредоносными программами, это дает злоумышленнику контроль над компьютером для одной цели, чтобы компьютер стал активом, который злоумышленник может продать или арендовать другим киберпреступникам, ведущим иную незаконную деятельность, которая зачастую направлена непосредственно на шпионаж или кражу у ничего не подозревающего владельца зараженного компьютера. Клик-мошенничество и те деньги, которые оно приносит злоумышленникам, имеет гораздо более широкое влияние, чем только на рекламную индустрию, и это ставит под угрозу всех тех, кто пользуется Интернетом.

Компьютерные «Ботнеты»

31. «Ботнет» представляет собой набор отдельных компьютеров, на каждом из которых работает программное обеспечение, которое обеспечивает связь между этими компьютерами и позволяет централизованную или децентрализованную связь с другими компьютерами, которые обеспечивают управление. Отдельные компьютеры в ботнете часто принадлежат отдельным пользователям, которые неосознанно загрузили или были инфицированы вредоносными программами для ассимиляции компьютера в ботнет. Компьютер пользователя, например, может стать частью ботнета, когда пользователь случайно взаимодействует с рекламой с вредоносного веб-сайта, нажимает на вредоносные вложения электронной почты или загружает вредоносное ПО. В каждом таком случае, код программного обеспечения загружается на компьютер пользователя, в результате чего этот компьютер становится частью ботнета. Как только компьютер пользователя становится частью ботнета, он может отправлять и получать сообщения, код или инструкции с других компьютеров ботнета.

32. Некоторые компьютеры ботнета полностью находятся под контролем создателя ботнета. Они могут иметь специализированные функции, такие как отправка команды управления. Они могут называться компьютерами «контроля и управления».

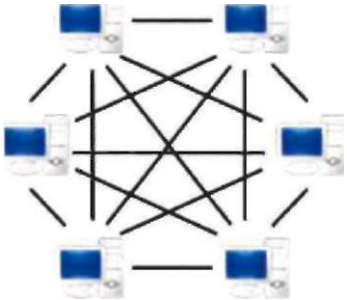
33. Ботнеты часто создаются и контролируются сложными преступными организациями и используются для проведения неправомерных действий, что вредит правам других лиц. Киберпреступники, например, могут использовать компьютер в ботнете для анонимной рассылки большого объема электронный писем без ведома и согласия физического лица пользователя, владеющего зараженным компьютером. Кроме того, они могут также использовать компьютер для дальнейшего распространения вредоносного ПО на другие компьютеры, что делает их также частью ботнета. Киберпреступники также могут использовать зараженный компьютер для осуществления мошенничества, компьютерных вторжений или других проступков. Ботнет компьютер может также использоваться в качестве «прокси» или реле Интернет-коммуникаций, происходящих с других компьютеров, с целью скрытия истинного источника этих сообщений.

Ботнеты ZeroAccess: Общая структура

34. Microsoft подает этот иск, чтобы остановить причинение вреда Ответчиками Microsoft и ее клиентам через злоумышленное использование доменов и IP-адресов, которые имеют критическое значение для ботнета, известного как «ZeroAccess» ботнет - также известный как «Sirefef» или «max++».

35. ZeroAccess ботнет имеет топологию Peer-To-Peer, которая может быть представлена следующим образом:

Сеть «Peer-To-Peer»



36. Эта структура используется в качестве способа противостояния контрмерам. В сети Peer-To-Peer, участвующие зараженные компьютеры называются «узлами», или «пирами». Они находятся в постоянной связи друг с другом и могут быстро и легко обновить друг друга новыми версиями вредоносных программ и новыми инструкциями.

Другими словами, в сети Peer-To-Peer, любой из зараженных компьютеров может функционировать в качестве командно-контрольного сервера. Следовательно, нет единой точки управления и контроля, которая была бы легкой целью для тех, кто стремится сорвать всю сеть. Так как ботнет Peer-To-Peer является наиболее сложным из бот-сетей с точки зрения срыва его деятельности, он является особенно привлекательным для киберпреступников, проектирующих и распространяющих ботнеты. Peer-To-Peer топологии также выгодны для киберпреступников, так как их архитектура позволяет установить более надежные связи между взломанными компьютерами, что делает ботнет в целом более устойчивым против попыток сорвать ботнет. Благодаря своей сетевой архитектуре, ZeroAccess является одним из самых надежных и долговечных ботнетов в Интернете сегодня.

37. Когда ничего не подозревающий пользователь просматривает один из веб-сайтов, его компьютер переводится на другой сайт, с которого загружаются вредоносное программное обеспечение, которое называется «пакет пользователя», после чего оно молча исследуют компьютер на наличие уязвимых мест с целью поиска возможности размещения вредоносного ПО в системе. После установки пакет пользователя скачивает и устанавливает вредоносные программы ZeroAccess.

38. После заражения, Ответчики направляют компьютеры, которые были заражены ZeroAccess, для участия в клик-мошенничестве через контроль веб-браузеров этих компьютеров или направляя зараженные компьютеры на создание автоматизированного интернет-трафика. Модульная структура ZeroAccess позволяет Ответчикам использовать компьютеры, которые были заражены ZeroAccess, для выполнения другой незаконной деятельности, в том числе кражи личных данных и «DDOS» атак, которые выводят целые компьютерные сети из строя. Большинство, если не все владельцы, компьютеров, которые были заражены ZeroAccess, не знают, что их машины заражены и являются частью ботнета ZeroAccess.

IP Адреса и Домены злоумышленного использования ZeroAccess

39. ZeroAccess ботнет использует IP-адреса и интернет домены для управления компьютеров, которые были заражены ZeroAccess, для связи их друг с другом и расширения ботнета. Эти IP-адреса и домены являются дискретными и относительно неизменными.

40. Зараженные компьютеры в сети Peer-To-Peer отнесены к отдельным серверам, расположенным на 18 IP-адресах и 49 Интернет доменах, поддерживаемых

Ответчиками в хостинговых компаниях в Латвии, Люксембурге, Швейцарии, Нидерландах и Германии. Когда ZeroAccess впервые заражает компьютер, инфицированный компьютер не содержит файлы или модули, необходимые для совершения фактического клик-мошенничества или контроля браузера. Скорее всего, вновь инфицированный компьютер вначале приобретает файлы и модули из первых компьютеров, с которыми он контактирует. Каждый раз, когда компьютер, который был заражен ZeroAccess, связывается с любым другим участником ботнета, он также запрашивает у него о том, какие другие модули ZeroAccess или файлы есть у другого участника. Файлы, которые зараженный ZeroAccess компьютер может приобрести таким образом, содержат список IP-адресов, представленных серверами, которые не являются частью сети Peer-To-Peer, но вместо этого могут обеспечить зараженный компьютер четкими инструкциями о том, как совершать дальнейшие мошеннические действия. Список IP -адресов постепенно меняется. В настоящее время существует 18 IP адресов (далее «IP Адреса для управления мошенническими действиями»). Microsoft сообщает и в этой связи утверждает, что операторы ZeroAccess ботнетов используют 49 Интернет доменов («Домены для управления мошенническими действиями») в качестве запасного варианта механизма поддержки и сохранения ботнета ZeroAccess в случае, если ботнет попадет под атаку. Домены для управления мошенническими действиями перечислены в Приложении А к жалобе.

41. IP Адреса для управления мошенническими действиями отправляют зараженную информацию и инструкции на компьютеры через Интернет, что заставляет эти компьютеры затем заниматься хакерской деятельностью. Хакерская деятельность осуществляется после того, как вредоносная программа ZeroAccess берет под контроль веб-браузер зараженного компьютера и перенаправляет пользователя на сайт, выбранный ботнет оператором. ZeroAccess специально ориентирована на поисковую систему Bing от Microsoft, а также Google и Yahoo! Пользователь, например, может использовать веб-браузер Microsoft Internet Explorer и поисковую систему Microsoft Bing для поиска продуктов, услуг или вопросов, представляющих для него интерес. Затем система поиска выдает список результатов, которые пользователь рассматривает и в конечном итоге «кликает». Как только пользователь нажимает на одну из ссылок, вредоносная программа, запущенная ZeroAccess на компьютере пользователя, перенаправляет браузер пользователя Internet Explorer и результаты поиска Bing на мошеннические IP адреса, а затем перенаправляет пользователя на один из нескольких возможных сайтов,

предопределенных Ответчиками. При этом вредоносная программа ZeroAccess заставляет пользователя полагать, что он использует поисковую систему, содержащую товарный знак Bing от Microsoft и Internet Explorer, браузер Microsoft. На самом деле, сервер на IP адресах мошенников перенаправляет браузер Internet Explorer пользователя и поисковую систему Bing к веб-сайтам заданным операторами ботнетов.

42. IP Адреса для управления мошенническими действиями также отправляют такую информацию и инструкции на зараженные компьютеры в Интернете, которая заставляет эти компьютеры заниматься «клик-мошенничеством». Клик-мошенничество происходит, когда вредоносная программа ZeroAccess заставляет компьютер без ведома пользователя генерировать автоматизированный интернет-трафик на любом веб-сайте, который Ответчики выбирают. Когда инфицированные ZeroAccess компьютеры включаются, вредоносная программа ZeroAccess, которая работает на этих компьютерах, соединяется с одним или несколькими из IP адресов для управления мошенническими действиями, указанными в Приложении А. Компьютеры на этих IP адресах и доменах обеспечивают зараженный ZeroAccess компьютер списком URL, каждый из которых указывает на сайт, с которым нужно соединиться. Вредоносные программы ZeroAccess затем запускают «скрытый» экземпляр веб-браузера, например, Internet Explorer от Microsoft на зараженных компьютерах и заставляют скрытый браузер посещать веб-сайты, выбранные Ответчиками, как если бы это был реальный пользователь. Когда инфицированный ZeroAccess компьютер подключается к веб-сайту, который содержит рекламу, браузер на зараженном компьютере загружает рекламу. В этот момент вредоносная программа ZeroAccess стимулирует клик на рекламу. Затем компьютер переходит к следующему сайту в этом списке и повторяет процесс. Владелец зараженного компьютера, даже если он сидит за компьютером, не видит скрытый браузер. Владелец, однако, будет испытывать потери в производительности компьютера и подключении к Интернету, учитывая значительное количество подключений к Интернету со стороны ZeroAccess.

43. Направляя зараженные ZeroAccess компьютеры на подключение к IP Адресам, изложенным в Приложении А, а затем заставляя эти компьютеры получать указания с этих IP адресов на участие в хакерстве и клик-мошенничестве, Ответчики используют каждый из этих IP Адресов для поддержки и для распространения ботнета ZeroAccess и продолжения своей вредоносной деятельности. По информации и

убеждению, Ответчики кроме этого используют домены для управления мошенническими действиями в качестве запасного механизма поддержки ботнета ZeroAccess.

Вред, причиненный ботнетом ZeroAccess Microsoft и ее клиентам

44. Вредоносные программы ZeroAccess тайно вводятся на компьютеры пользователей, заражая эти компьютеры и делая их частью ботнета. Эти действия представляют собой несанкционированное вторжение в операционную систему Microsoft Windows®, которую Microsoft поставляет свои конечным пользователям. ZeroAccess, например, пишет отдельные записи в реестр операционной системы Windows®, без согласия Microsoft или ее клиентов, в том числе команды, которые предписывают компьютеру, какие команды выполнять, команды, которые облегчают общение между компьютерами ботнетов, команды, которые заставляют компьютер участвовать в клик-мошенничестве, команды, которые указывают компьютеру, как получать инструкции от оператора ботнета и данные, идентифицирующие компьютер в ботнете. Реестр представляет собой первичное хранилище важной информации для правильной работы компьютера.

45. ZeroAccess создает скрытые каталоги, переписывает программные драйверы, необходимые для работы операционной системы и внедряется в процессы низкого уровня. ZeroAccess отключает функции безопасности на зараженных компьютерах, снижает учетные данные безопасности и проводит отключение обеспечения безопасности Windows, оставляя компьютер восприимчивым к вторичным инфекциям. Он отключает службы Filtering Engine, IP-Helper, Windows firewall, Windows Defender, Windows Security Center Service, и Proxy Auto Discovery Service. ZeroAccess, отключив эти услуги, предотвращает получение обновлений сервисов безопасности от Microsoft. Эти события происходят без ведома и согласия пользователя, а ZeroAccess работает в фоновом режиме незаметно для пользователя без какого-либо пользовательского интерфейса, не давая владельцу компьютера никаких признаков того, что она есть и работает.

46. Вторжение ботнета ZeroAccess в операционную систему Windows от Microsoft® производится без разрешения Microsoft или ее клиентов и превышает любые полномочия, предоставленные корпорацией Microsoft или ее клиентам третьим лицам, в том числе операторам ботнета ZeroAccess.

47. ZeroAccess ботнет вредит клиентам Microsoft, неправильно используя операционную систему Windows® на зараженных компьютерах этих пользователей.

ZeroAccess ботнет причиняет вред клиентам Microsoft среди прочего, заставляя компьютеры:

a. устанавливать и запускать программное обеспечение без ведома или согласия клиентов, в том числе программное обеспечение для поддержки ботнет инфраструктуры, программное обеспечение, которое заставляет компьютер участвовать в клик-мошенничестве через хакерство и создание автоматизированного Интернет-трафика, а также программное обеспечение, позволяющее компьютеру участвовать в других неразрешенных видах деятельности;

b. ухудшать производительность из-за управления несанкционированным программным обеспечением;

c. устанавливать и запускать программное обеспечение без ведома и согласия клиентов, которое может собирать личную информацию, в том числе запросы поисковой системы и результаты поиска поисковой системы Bing компании Microsoft, которые содержат личную информацию конечных пользователей; а также

d. передавать собранную личную информацию конечных пользователей на IP Адреса и домены ZeroAccess.

48. Несанкционированный доступ и вторжение в операционную систему Microsoft Windows® и в компьютеры клиентов Microsoft, вводит потребителя в заблуждение. Для вторжения в компьютеры конечных пользователей и для их участия в клик-мошенничестве, Ответчики неоднократно используют торговые марки «Microsoft», такие как «Windows», «Internet Explorer» и «Bing» для ввода пользователей в заблуждение. Ответчики используют товарные знаки корпорации Microsoft для вторжения в компьютер пользователя и для клик-мошенничества, для хакерства через компьютер пользователя, а также для создания незаконного автоматизированного трафика. Это заставляет пользователя поверить, что операционная система Windows, Internet Explorer и Bing плохо работают и ненадежные, хотя это не так. Клиенты Microsoft, уведомили Microsoft об ущербе, причиненном ботнетом ZeroAccess. Такие клиенты были введены в заблуждение и поверили, что Microsoft была источником ущерба, деятельности ZeroAccess ботнета и результатов этой деятельности, и поэтому неправильно отнесли свой ущерб на Microsoft и ее продукты и услуги.

49. ZeroAccess также причиняет ущерб путем обмана рекламодателей Microsoft. Рекламодатели, которые платят Microsoft и другим рекламным площадкам за увеличение целевого трафика на свои веб-сайты, ожидают, что рекламные услуги Microsoft сделают

более вероятным то, что конечные пользователи, которые ищут соответствующие товары или услуги, посетят их веб-сайты. ZeroAccess грубо искажает этот рекламный канал путем создания кликов и посещений веб-сайтов, не инициированных пользователем, увеличивая тем самым трафик на некоторых веб-сайтах рекламодателей и перехватывая действия пользователей. Мошеннический трафик ZeroAccess, однако, не приводит к росту потенциальных продаж, вводя в заблуждение рекламодателей, которым приходится платить дистрибьюторам рекламы, как будто их объявления были законно нажаты. Проще говоря, рекламодатель в таком случае платит за интернет-трафик, который не имеет смысла. ZeroAccess также искажает значение конкретных мест размещения объявлений. Число кликов на объявление рекламодателя определяет, среди прочего, где рекламодатель будет размещать свою рекламу в будущем. ZeroAccess меняет эти результаты на зараженном компьютере конечного пользователя и объявление рекламодателя не нажимается. Рекламодателю наносится ущерб, потому что его объявления оцениваются в таком случае как менее актуальные, что усложняет процесс получения хорошего размещения в будущих результатах поиска. Существует значительный риск того, что рекламодатели могут приписать эту проблему Microsoft и связать эти проблемы с плохой работой поисковой системы Bing и рекламных продуктов Microsoft, тем понижая ценность этих торговых марок и брендов.

50. Таким образом, ботнет ZeroAccess, а также IP-адреса и домены ZeroAccess причинили ущерб бренду и деловой репутации Microsoft. Такое неверное отнесение последствий работы ботнета ZeroAccess, а также IP-адресов и доменов ZeroAccess на результаты работы Microsoft причиняет вред бренду Microsoft, а также бросает тень на репутацию компании, ее продукты и услуги. Microsoft пришлось вложить значительные ресурсы в попытке помочь своим клиентам и исправить сложившееся неправильное понимание ситуации, ведь Microsoft не является источником ущерба, причиненного ботнетом ZeroAccess, а также IP-адресами и доменами ZeroAccess.

51. На основании информации и убеждения, Ответчики, которые управляют работой ботнета ZeroAccess, получают выгоду от его работы и от деятельности, описанной выше, выступая как «брокеры трафика», увеличивая число посетителей на определенных веб-сайтах с помощью контроля браузера и автоматизированной генерации трафика, продавая захваченный таким образом трафик другим брокерам трафика.

ПЕРВОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Нарушение Закона о компьютерном мошенничестве и злоупотреблении, 18 U.S.C. § 1030

52. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

53. Ответчики: (a) сознательно и преднамеренно получили доступ к защищенным компьютерам Microsoft и ее клиентов, без разрешения или с превышением любого разрешения и тем самым смогли получить информацию из защищенных компьютеров в рамках операции с использованием связи между штатами или иностранной связи (18 U.S.C. § 1030 (a) (2) (C)), (b) сознательно и преднамеренно получили доступ к защищенным компьютерам, без разрешения или с превышением любого разрешения, и тем самым смогли получить информацию из этих защищенных компьютеров, которую затем Ответчики использовали для дальнейших неправомерных действий и получения ценности (18 U.S.C. § 1030 (a) (4)), (c) сознательно осуществили передачу программ, информации, кода и команд, и в результате такого поведения умышленно причинили ущерб не защищенным компьютерам (18 U.S.C. § 1030 (a) (5) (A)), и (d) намеренно получили доступ к защищенным компьютерам без разрешения, и в результате такого поведения нанесли ущерб и потери (18 U.S.C. § 1030 (a) (5) (C)).

54. Поведение Ответчиков привело к потерям Microsoft в размере как минимум $ 5000 за год.

55. Microsoft понесла убытки в результате поведения ответчиков.

56. Microsoft добивается применения компенсационных и штрафных санкций по отношению к Ответчикам согласно 18 U.S.C. § 1030 (g) в количестве, которое будет подтверждено в ходе судебного разбирательства.

57. Как прямой результат действий ответчиков, Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

ВТОРОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Нарушение Закона о конфиденциальности электронных коммуникаций, 18 U.S.C. § 2701

58. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

59. Компьютеры и серверы, а также лицензионная операционная система Microsoft, являются объектами, посредством которых Microsoft предоставляет услуги электронной коммуникации для своих пользователей и клиентов.

60. Ответчики сознательно и преднамеренно получили доступ к защищенным компьютерам Microsoft и ее клиентов, без разрешения или с превышением любого разрешения, выданного Microsoft.

61. Благодаря такому несанкционированному доступу, Ответчики смогли изменить и / или предотвратить попытки пользователей Microsoft получить законный доступ к электронным сообщениям, в том числе, но не ограничиваясь, поисковым запросам пользователей системы, содержащим личную информацию в электронном виде в компьютерах и серверах Microsoft и ее клиентов и в рамках лицензионной операционной системы Microsoft.

62. Как прямой результат действий ответчиков, Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

ТРЕТЬЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Посягательство на торговую марку в соответствии с Законом Ланхэма – 15 U.S.C. § 1114 и далее

63. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

64. Ответчики использовали такие торговые марки Microsoft, как «Microsoft», «Windows», «Internet Explorer» и «Bing» («марки Microsoft») в торговле между штатами.

65. Ботнет Sirefef создает и использует поддельные копии марок Microsoft, в процессе клик-мошенничества путем создания и распространения поддельных марок Microsoft, а также манипулирует работой веб-сайтов браузера Internet Explorer и поисковой системы Bing компании Microsoft, а также использует на мошеннических сайтах торговые марки Microsoft. Поступая таким образом, ответчики вызывают путаницу, ошибки или обман относительно происхождения, спонсорства или подтверждения поддельных веб-сайтов, а также продуктов и услуг, продвигаемых через поддельные веб-сайты.

66. С помощью торговых марок Microsoft, в связи с вторжением на компьютеры конечных пользователей с целью клик-мошенничества, Ответчики вызвали и могут вызвать путаницу, ошибки или обман относительно происхождения, спонсорства или подтверждения поддельных веб-сайтов, которые создаются и используются ботнетом ZeroAccess. Поступая таким образом, Ответчики вызвали и могут вызвать путаницу,

ошибки или обман относительно происхождения, спонсорства или подтверждения действий, продуктов и услуг, осуществляемых или продвигаемых Ответчиками и ботнетом ZeroAccess.

67. Ботнет ZeroAccess создает ключи, вносит записи в реестр Windows®. Создавая ключи и внося записи в пути реестра, который включает в себя торговые марки Microsoft, Ответчики могут вызвать путаницу, ошибки или обман в отношении происхождения, спонсорства или подтверждения установленного на ботнете ZeroAccess вредоносного программного обеспечения, в том числе через IP -адреса и домены ZeroAccess.

68. В результате своих противоправных действий, Ответчики ответственны перед Microsoft за нарушение 15 U.S.C. § 1114.

69. Microsoft добивается применения компенсационных и штрафных санкций по отношению к Ответчикам в сумме, которая будет утверждена в ходе судебного разбирательства.

70. Как прямой результат действий ответчиков, Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

71. Противоправное и несанкционированное использование торговых знаков Microsoft ответчиками для продвижения или продажи товаров и услуг составляет нарушение законодательства о торговых знаках в соответствии с 15 U.S.C. § 1114 и далее.

ЧЕТВЕРТОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Ложные указания происхождения в соответствии с Законом Ланхэма - 15 U.S.C. § 1125 (a)

72. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

73. Торговые марки Microsoft – это отличительные знаки, которые связаны с Microsoft и уникальным образом обозначают деятельность Microsoft, ее продукты и услуги.

74. ZeroAccess ботнет создает и использует поддельные копии марок Microsoft, в процессе клик-мошенничества путем создания и распространения поддельных марок Microsoft, а также манипулирует работой веб-сайтов браузера Internet Explorer и поисковой системы Bing компании Microsoft, а также использует на мошеннических

сайтах торговые марки Microsoft. Поступая таким образом, ответчики вызывают путаницу, ошибки или обман относительно происхождения, спонсорства или подтверждения поддельных веб-сайтов, а также продуктов и услуг, продвигаемых через поддельные веб-сайты.

75. С помощью торговых марок Microsoft, в связи с вторжением на компьютеры конечных пользователей с целью клик-мошенничества, Ответчики вызвали и могут вызвать путаницу, ошибки или обман относительно происхождения, спонсорства или подтверждения поддельных веб-сайтов, которые создаются и используются ботнетом ZeroAccess. Поступая таким образом, Ответчики вызвали и могут вызвать путаницу, ошибки или обман относительно происхождения, спонсорства или подтверждения действий, продуктов и услуг, осуществляемых или продвигаемых Ответчиками и ботнетом ZeroAccess.

76. Ботнет ZeroAccess создает ключи и вносит записи в реестр Windows®. Создавая ключи и внося записи в пути реестра, который включает в себя торговые марки Microsoft, Ответчики могут вызвать путаницу, ошибки или обман в отношении происхождения, спонсорства или подтверждения установленного на ботнете ZeroAccess вредоносного программного обеспечения, в том числе через IP -адреса и домены ZeroAccess.

77. В результате своих противоправных действий, Ответчики ответственны перед Microsoft за нарушение 15 U.S.C. § 1125 (a).

78. Microsoft добивается применения компенсационных и штрафных санкций по отношению к Ответчикам в сумме, которая будет утверждена в ходе судебного разбирательства.

79. Как прямой результат действий ответчиков, Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

ПЯТОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Подрыв доверия к торговой марке в соответствии с Законом Ланхэма - 15 U.S.C. § 1125 (c)

80. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

81. Торговые марки Microsoft – это отличительные знаки, которые связаны с Microsoft и уникальным образом обозначают деятельность Microsoft, ее продукты и услуги.

82. ZeroAccess ботнет создает и использует поддельные копии марок Microsoft, в процессе клик-мошенничества путем создания и распространения поддельных марок Microsoft, а также манипулирует работой веб-сайтов браузера Internet Explorer и поисковой системы Bing компании Microsoft, а также использует на мошеннических сайтах торговые марки Microsoft. Поступая подобным образом, Ответчики могут вызвать подрыв доверия к торговым маркам и компании Microsoft.

83. С помощью торговых марок Microsoft, в связи с вторжением на компьютеры конечных пользователей с целью клик-мошенничества, Ответчики вызвали и могут вызвать подрыв доверия к торговым маркам и компании Microsoft. Поступая подобным образом, Ответчики вызвали и могут вызвать подрыв доверия к торговым маркам и компании Microsoft из-за несправедливой связи торговых марок Microsoft с неправомерными действиями, продуктами и услугами, осуществляемыми или продвигаемыми Ответчиками и ботнетом ZeroAccess.

84. Ботнет ZeroAccess создает ключи и вносит записи в реестр Windows®. Создавая ключи и внося записи в пути реестра, который включает в себя торговые марки Microsoft, Ответчики могут, вызвать подрыв доверия к торговым маркам и запятнать репутацию компании Microsoft.

85. Используя торговые марки Microsoft, в связи со своей злонамеренной деятельностью, Ответчики могут вызвать подрыв доверия к торговым маркам и запятнать репутацию компании Microsoft, в том числе через IP Адреса и домены ZeroAccess.

86. В результате своих противоправных действий, Ответчики ответственны перед Microsoft за нарушение 15 U.S.C. § 1125 (c).

87. Microsoft добивается применения компенсационных и штрафных санкций по отношению к Ответчикам в сумме, которая будет утверждена в ходе судебного разбирательства.

88. Как прямой результат действий ответчиков, Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

ШЕСТОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Посягательство на движимое имущество

89. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

90. Действия Ответчиков в отношении деятельности ботнета ZeroAccess, которые заключаются в несанкционированном доступе к компьютерам и серверам, связанным с Internet Explorer, Bing и услугами Bing Ads компании Microsoft, повлекли за собой несанкционированный доступ к фирменной операционной системе Windows от Microsoft и к компьютерам клиентов, имеющим данную операционную систему, заставляя их участвовать в клик-мошенничестве, направляя компьютеры, сессии веб-браузера Internet Explorer и результаты поисковой системы на веб-сайты, выбранные Ответчиками, без разрешения или согласия Microsoft или ее клиентов.

91. Ответчики умышленно занимались такой деятельностью, и это поведение было несанкционированным.

92. Действия ответчиков причинили вред Microsoft и ее клиентам, а также привели к затратам времени, денег, возросшей нагрузке на компьютеры Microsoft и ее клиентов, а также причинили ущерб деловой репутации Microsoft и уменьшили стоимость компьютеров и программного обеспечения Microsoft.

93. В результате несанкционированных и преднамеренных действий Ответчиков, Microsoft понесла ущерб в размере, который предстоит подтвердить в ходе судебного разбирательства.

94. Как прямой результат действий ответчиков, Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

СЕДЬМОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Незаконное обогащение

95. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

96. Действия ответчиков, указанные здесь, представляют собой незаконное обогащение Ответчиков за счет компании Microsoft в нарушение общего права.

97. Ответчики получили доступ, без разрешения, к компьютерам под управлением программного обеспечения от Microsoft.

98. Ответчики использовали без разрешения или лицензии, средства программного обеспечения от Microsoft, среди прочих действий, распространяли вредоносное программное обеспечение, управляли ботнетом ZeroAccess и участвовали в клик-мошенничестве.

99. Действия Ответчиков в отношении деятельности ботнета ZeroAccess, которые заключаются в несанкционированном доступе к компьютерам и серверам, связанным с Internet Explorer, Bing и услугами Bing Ads компании Microsoft, повлекли за собой несанкционированный доступ к фирменной операционной системе Windows от Microsoft и к компьютерам клиентов, имеющим данную операционную систему, заставляя их участвовать в клик-мошенничестве, направляя компьютеры, сессии веб-браузера Internet Explorer и результаты поисковой системы на веб-сайты, выбранные Ответчиками, без разрешения или согласия Microsoft или ее клиентов.

100. Ответчики несправедливо получали прибыль путем несанкционированного и нелицензионного использования программного обеспечения Microsoft, а также компьютеров Microsoft и ее клиентов, среди прочего, отвлекая доход Microsoft и ее рекламодателей и направляя мошеннический интернет-трафик на объявления платформы Microsoft Bing Ads, а также с помощью других средств монетизации, обмана Microsoft и ее клиентов-рекламодателей.

101. Ответчики были осведомлены о тех выгодах, которые они получали путем несанкционированного и нелицензионного использования программного обеспечения Microsoft и компьютеров Microsoft и ее клиентов, а также при помощи деятельности, описанной здесь.

102. Сохранение Ответчиками прибыли, которую они получили путем несанкционированного и нелицензионного использования программного обеспечения Microsoft и компьютеров Microsoft и ее клиентов, а также при помощи деятельности, описанной здесь, было бы несправедливым.

103. В результате несанкционированного и нелицензионного использования программного обеспечения Microsoft, а также компьютеров Microsoft и ее клиентов, Microsoft понесла ущерб в размере, который предстоит подтвердить в ходе судебного разбирательства, а Ответчики должны вернуть незаконно полученную прибыль.

104. В результате действий ответчиков Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных

законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

ВОСЬМОЕ ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ

Конверсия

105. Microsoft еще раз заявляет и включает в свою поддержку утверждения, содержащиеся в пунктах с 1 по 51 выше.

106. Ответчики умышленно вмешивались и преобразовывали личную собственность Microsoft, не имея на то законных оснований, в результате чего Microsoft лишилась части своего имущества.

107. В результате действий Ответчиков, Microsoft понесла ущерб в размере, который предстоит подтвердить в ходе судебного разбирательства.

108. В результате действий ответчиков Microsoft пострадала и продолжает страдать от непоправимого вреда, для устранения которого Microsoft не имеет адекватных законных мер, и который будет продолжаться до тех пор, пока действия ответчиков не будут пресечены.

ХОДАТАЙСТВО О СУДЕБНОЙ ЗАЩИТЕ ПРАВ

Таким образом, истец Microsoft призывает Суд:

1. Принять решение в пользу Microsoft и против обвиняемых;

2. Постановить то, что поведение Ответчиков было умышленным и что ответчики действовали с целью мошенничества, в злобе и угнетении;

3. Издать бессрочное судебное постановление, запрещающее Ответчикам и их должностным лицам, директорам, руководителям, агентам, служащим, сотрудникам и правопреемникам, а также всем лицам и организациям, соучаствующим с ними, участие в любой деятельности, обжалованной здесь, или причинение любого ущерба, обжалованного здесь, а также помощь, пособничество или подстрекательство любых других лиц или субъектов хозяйствования в участии или выполнении любой деятельности, обжалованной здесь, либо причинении любого ущерба, обжалованного здесь;

4. Издать бессрочный судебный запрет, предотвращающий Ответчиков от использования IP -адресов и доменов ZeroAccess;

5. Постановить о возмещении Ответчиками действительного ущерба, причиненного Microsoft, в размере, адекватном для того, чтобы компенсировать Microsoft последствия деятельности Ответчиков, обжалованной здесь, а также любого ущерба,

обжалованного здесь, в том числе, но не ограничиваясь, проценты и издержки в количестве, которое будет подтверждено в ходе судебного разбирательства;

6. Постановить возвращение прибыли Ответчиками;

7. Постановить о возмещении награждения увеличенных, образцовых и специальных убытков в размере, который будет установлен в ходе судебного разбирательства;

8. Постановить о назначении сборов и расходов на адвокатов; и

9. Принять иное решение по данному иску, которое Суд сочтет справедливым и разумным.

Дата: 25 ноября 2013

Документы поданы:

FISH & RICHARDSON P.C.

В лице: _____

Дэвид М. Хофман (David M. Hoffman)
Texas Bar No. 24046084
hoffman@fr.com

Уиллиам Томас Джекс (William Thomas Jacks)
Texas Bar No. 10452000
jacks@fr.com

111 Congress Ave, Suite 810
Austin, TX 78701
Тел: +1 (512) 472-5070
Факс: +1 (512) 320-8935

Юристами компании:

ORRICK, HERRINGTON & SUTCLIFFE LLP

Гэбриэл М. Рэмзи (Gabriel M. Ramsey)
(заявление на рассмотрении)
gramsey@orrick.com

Джефри Л. Кокс (Jeffrey L. Cox)
(заявление на рассмотрении)
jcox@orrick.com

Якоб М. Хелс (Jacob M. Health)
(заявление на рассмотрении)
jheath@orrick.com

Роберт Л. Уриат (Robert L. Uriarte)
(заявление на рассмотрении)
ruriarte@orrick.com

1000 Marsh Road
Menlo Park, California 94025
Тел: +1 (650) 614-7400
Факс: +1 (650) 614-7401

Юрист Истца
КОРПОРАЦИЯ MICROSOFT