

В ФЕДЕРАЛЬНЫЙ СУД СОЕДИНЕННЫХ ШТАТОВ

ЗАПАДНОГО ОКРУГА СЕВЕРНОЙ КАРОЛИНЫ

ОТДЕЛЕНИЕ г. ШАРЛОТТ

КОРПОРАЦИЯ MICROSOFT,  
Истец,  
против  
НЕУСТАНОВЛЕННЫХ ЛИЦ №№1-82,  
КОНТРОЛИРУЮЩИХ  
КОМПЬЮТЕРНУЮ БОТ-СЕТЬ (БОТНЕТ)  
И ПРИЧИНЯЮЩИХ ТЕМ САМЫМ ВРЕД  
КОРПОРАЦИИ MICROSOFT И ЕЕ  
КЛИЕНТАМ,  
Ответчиков.

**ПОДАНО В ОПЕЧАТАННОМ ВИДЕ**

№ гражданского иска 3:13cv319

**[ПРЕДЛОЖЕНО] ОДНОСТОРОННИЙ  
СУДЕБНЫЙ ПРИКАЗ О ВРЕМЕННОМ  
ЗАПРЕЩЕНИИ И ПРИКАЗ О  
ПРЕДСТАВЛЕНИИ ОБОСНОВАНИЯ В  
ОТНОШЕНИИ ПРЕДВАРИТЕЛЬНОГО  
СУДЕБНОГО ЗАПРЕТА**

Истец, корпорация Microsoft (здесь и далее «Microsoft» или «Истец»), обратился с исковым заявлением о применении обеспечительных мер (запрета) и иных мер судебной защиты в соответствии с Законом о компьютерном мошенничестве и злоупотреблении (Свод законов США, раздел 18, § 1030); Законом о контроле над активным распространением навязчивой порнографии и рекламы (CAN-SPAM) (Свод законов США, раздел 15, § 7704); Законом о защите информации, передаваемой через электронные системы связи (Свод законов США, раздел 18, § 2701); Законом о защите торговых марок в тех его частях, которые касаются нарушения торговой марки, ложного обозначения происхождения и ослабления торговой марки (Свод законов США, раздел 15, §§ 1114 *и далее*); Законом о борьбе с организованной преступностью (RICO) (Свод законов США, раздел 18, § 1962); параграфом 14-458 (Неправомерное использование компьютера) Кодекса общих законов штата Северная Каролина и общим правом по неосновательному обогащению, присвоению имущества и причинению зловредности. Истец также подал

ходатайство в одностороннем порядке о срочном предоставлении судебного приказа о временном запрещении и о конфискации, в соответствии с Правилom 65(b) Федеральных правил гражданского судопроизводства, параграфом 1116(d) раздела 15 Свода законов США («Закон о защите торговых марок») и параграфом 1651(a) раздела 28 Свода законов США («Закон о всех судебных приказах»), и приказа о предоставлении обоснований для непредоставления предварительного судебного запрета.

### **УСТАНОВЛЕННЫЕ ФАКТЫ И ПРИМЕНИМЫЕ НОРМЫ ПРАВА**

Изучив все документы, заявления, вещественные доказательства и юридические заключения, поданные Истцом в поддержку его ходатайства о предоставлении экстренного судебного приказа о временном запрещении, приказа о конфискации и приказа об обосновании причин предварительного судебного запрета (здесь и далее «Ходатайство о TRO»), Суд настоящим подтверждает следующие фактические обстоятельства и применимые нормы права:

1. Подсудность предмета спора в данном деле относится к этому суду, и существует достаточно оснований предполагать, что этот суд также будет обладать персональной юрисдикцией над участвующими в деле сторонами; Исковое заявление содержит жалобу, в ответ на которую суд может предоставить судебную защиту от Ответчиков в соответствии с Законом о компьютерном мошенничестве и злоупотреблении (Свод законов США, раздел 18, § 1030); Законом о контроле над активным распространением навязчивой порнографии и рекламы (CAN-SPAM) (Свод законов США, раздел 15, § 7704); Законом о защите информации, передаваемой через электронные системы связи (Свод законов США, раздел 18, § 2701); Законом о защите торговых марок в тех его частях, которые касаются нарушения торговой марки,

ложного обозначения происхождения и ослабления торговой марки (Свод законов США, раздел 15, §§ 1114 *и далее*); Законом о борьбе с организованной преступностью (RICO) (Свод законов США, раздел 18, § 1962); параграфом 14-458 (Неправомерное использование компьютера) Кодекса общих законов штата Северная Каролина и общим правом по неосновательному обогащению, присвоению имущества и причинению зловредности.

2. Корпорация Microsoft владеет торговыми марками «Microsoft», «Windows» и «Internet Explorer», используемыми применительно к ее услугам, программному обеспечению и продукции. Торговые марки третьих сторон и другие представители общественности также пострадали от действий Ответчиков.

3. Существуют все основания полагать, что Ответчики участвовали и с большой вероятностью намерены продолжать участвовать в действиях и занятиях, нарушающих Закон о компьютерном мошенничестве и злоупотреблении (Свод законов США, раздел 18, § 1030); Закон о контроле над активным распространением навязчивой порнографии и рекламы (CAN-SPAM) (Свод законов США, раздел 15, § 7704); Закон о защите информации, передаваемой через электронные системы связи (Свод законов США, раздел 18, § 2701); Закон о защите торговых марок в тех его частях, которые касаются нарушения торговой марки, ложного обозначения происхождения и ослабления торговой марки (Свод законов США, раздел 15, §§ 1114 *и далее*); Закон о борьбе с организованной преступностью (RICO) (Свод законов США, раздел 18, § 1962); параграф 14-458 (Неправомерное использование компьютера) Кодекса общих законов штата Северная Каролина и общее право по неосновательному обогащению, присвоению имущества и причинению зловредности.

4. Существуют все основания предполагать, что в том случае, если действия Ответчиков не будут пресечены и запрещены приказом данного суда, такие действия нанесут прямой и невозместимый вред, поскольку являются постоянным нарушением Закона о компьютерном мошенничестве и злоупотреблении (Свод законов США, раздел 18, § 1030); Закона о контроле над активным распространением навязчивой порнографии и рекламы (CAN-SPAM) (Свод законов США, раздел 15, § 7704); Закона о защите информации, передаваемой через электронные системы связи (Свод законов США, раздел 18, § 2701); Закона о защите торговых марок в тех его частях, которые касаются нарушения торговой марки, ложного обозначения происхождения и ослабления торговой марки (Свод законов США, раздел 15, §§ 1114 и далее); Закона о борьбе с организованной преступностью (RICO) (Свод законов США, раздел 18, § 1962); параграфа 14-458 (Неправомерное использование компьютера) Кодекса общих законов штата Северная Каролина; общего права по неосновательному обогащению, присвоению имущества и причинению зловредности. Доказательства, перечисленные в ходатайстве Истца о предоставлении TRO и подкрепляющие это ходатайство заявления и экспонаты указывают на то, что у Истца будет преимущественная сила в доказательстве того, что Ответчики нарушили вышеупомянутые законы, совершая следующие действия:

- a. Разработали и ввели в коммерческий оборот пакет разработчика для ботнета Citadel, с обеспечением техподдержки, с целью предоставления другим Ответчикам возможность создавать, запускать и использовать ботнеты Citadel с целью хищения информации, удостоверяющей личность, информации,

относящейся к личной безопасности, и денежных средств через проникновение в программное обеспечение корпорации Microsoft, в компьютеры ее клиентов и в защищенные компьютеры третьих сторон, включая банки и прочих представителей общественности;

- b. Распространили украденную версию Windows XP и украденный ключ продукта Windows XP для того, чтобы предоставить возможность другим Ответчикам создавать, запускать в действие и использовать преступные ботнеты с целью хищения информации, удостоверяющей личность, информации, относящейся к личной безопасности, и денежных средств, а также проникновения в программное обеспечение корпорации Microsoft и в компьютеры ее клиентов;
- c. Создали, запустили и обеспечили функционирование преступных ботнетов с целью хищения информации, удостоверяющей личность, информации, относящейся к личной безопасности, и денежных средств через неправомерное использование принадлежащих Истцу операционной системы Windows и программного обеспечения Internet Explorer;
- d. Умышленно без полномочия получали доступ и рассылали вредоносные программные средства на принадлежащую корпорации Microsoft лицензированную операционную систему Windows и программное обеспечение Internet Explorer, на

- защищенные компьютеры пользователей Microsoft, а также на защищенные компьютеры третьих сторон, включая банки и прочих представителей общественности, с целью инфицирования этих компьютеров и превращения их в часть ботнета Citadel;
- e. Рассылали вредоносные программные средства для настройки, использования и управления ботнетом;
  - f. Занимались рассылкой нежелательных сообщений электронной почты на учетные записи Microsoft Hotmail;
  - g. Рассылали нежелательные электронные сообщения с ложной информацией о том, что они посланы или одобрены к рассылке Истцом или третьими сторонами, включая банки, Национальную ассоциацию автоматизированных клиринговых палат (НАСНА) или другие компании и организации – имея целью обманным путем спровоцировать пользователей на совершение действий, которые приведут к заражению их компьютеров кодом ботнета и (или) раскроют их личную или финансовую информацию;
  - h. Похищали личную и финансовую информацию пользователей операционной системы Windows и программного обеспечения Internet Explorer, принадлежащих корпорации Microsoft;
  - i. Использовали украденную информацию для хищения денег с финансовых счетов пользователей операционной системы Windows и программного обеспечения Internet Explorer, принадлежащих компании Microsoft;

ј. Установили связь друг с другом в рамках общего преступного предприятия, занятого совершением этих незаконных действиях.

5. Существуют все основания полагать, что, если эти действия продолжатся, невозместимый вред будет причинен Истцу и населению, включая клиентов Истца, финансовые учреждения, Национальную ассоциацию автоматизированных клиринговых палат (НАСНА) и прочих представителей общественности.

6. Существуют все основания полагать, что Ответчики продолжают в настоящее время и продолжат в будущем заниматься этой противозаконной деятельностью, если на них приказом суда не будет наложен немедленный запрет. Существуют все основания полагать, что возможностям этого суда по эффективному предоставлению окончательной правовой защиты будет нанесен немедленный и невозместимый вред в результате продажи, передачи или любого другого отчуждения или сокрытия Ответчиками контролирующего ботнет программного обеспечения, которое в настоящее время размещено и функционирует на интернет-доменах, перечисленных в приложении «А», и на IP-адресах, перечисленных в приложении «В», и в результате уничтожения или сокрытия расположенных там же поддающихся обнаружению улик, подтверждающих незаконную деятельность Ответчиков, если Ответчикам станет заранее известно об этих действиях суда.

7. Существуют все основания полагать, что, исходя из доказательств, упомянутых в ходатайстве Истца о предоставлении ТРО и подкрепляемых приложенными заявлениями и экспонатами, Истец сможет доказать, что: (1) Ответчики занимаются деятельностью, являющейся прямым нарушением законов

США и причиняющей вред Истцу и обществу, включая клиентов Истца, финансовые учреждения третьих сторон, Национальную ассоциацию автоматизированных клиринговых палат (NACHA) и прочих представителей общественности; (2) Ответчики продолжают заниматься своей противозаконной деятельностью, несмотря на очевидный вред, который она наносит интересам вышеперечисленных сторон; (3) в том случае, если Ответчикам станет известно о действиях Истца, велика вероятность того, что Ответчики уничтожат или переместят указанное в ходатайстве Истца о предоставлении TRO программное обеспечение, контролирующее ботнет, и вредительское, вредоносное, нарушающее торговую марку программное обеспечение, распространяемое через эти IP-адреса и домены, и предупредят о действиях Истца своих сообщников.

8. Существуют все основания полагать, что ходатайство Истца о предоставлении срочной судебной защиты в одностороннем порядке не является результатом недостаточного усердия со стороны Истца, но, напротив, основано на самом характере противозаконной деятельности Ответчиков. Исходя из этого, в соответствии с пунктом 65(b) Федеральных правил гражданского судопроизводства и параграфом 1116(d) раздела 15 Свода законов США, достаточные основания и интересы правосудия требуют, чтобы соответствующий приказ суда был выдан без предварительного уведомления Ответчиков, в связи с чем Истец освобождается от обязанности предварительного вручения Ответчикам извещения о ходатайстве Истца.

9. Существуют все основания полагать, что Ответчики совершали противозаконные действия, используя центры хранения и обработки данных и (или) провайдеров интернет-хостинга, указанных в приложении «В», для размещения



управляющего и контролирующего программного обеспечения и вредоносного кода ботнета, а также контента, используемого для технической поддержки и функционирования ботнета в компьютерах, серверах, электронных устройствах для хранения данных или электронных носителях информации по IP-адресам, указанным в приложении «В».

10. Существуют все основания полагать, что для того чтобы немедленно прекратить причинение вреда Ответчиками, вся информация Ответчиков и улики, содержащиеся на IP-адресах Ответчиков в центрах обработки данных и (или) у провайдеров интернет-хостинга, указанных в приложении «В», должны быть сохранены и будут оставаться у третьей стороны до дальнейших распоряжений суда. Компьютерные ресурсы Ответчиков, связанные с вредоносными доменами, расположенными на таких IP-адресах, должны быть отключены от сети Интернет. Ответчикам должен быть запрещен доступ к компьютерным ресурсам Ответчиков, имеющим отношение к таким IP-адресам, а информация и улики, содержащиеся в этих компьютерных ресурсах, должны быть защищены и сохранены. Существуют все основания полагать, что Ответчикам нужно запретить пользоваться всеми IP-адресами, о которых известно, что они имеют отношение к ботнетам, проходящим по данному делу и перечисленным в приложении «В».

11. Существуют все основания полагать, что, для того чтобы немедленно прекратить причинение ущерба со стороны Ответчиков и для гарантии того, что их дальнейшее преследование по данному делу не окажется безрезультатным из-за того, что они попытаются стереть, спрятать, укрыть или любым другим образом закрыть доступ к компонентам программного обеспечения, через которые производится

распространение нелегальных копий продукции с торговой маркой Истца, и что они будут продолжать свою преступную деятельность, поскольку сейчас Ответчики полностью контролируют и используют IP-адреса, расположенные в центрах обработки данных, находящихся в ведении Linode LLC/Linode VPS Hosting и Network Operations Center, Inc./BurstNET Technologies, Inc., Федеральному бюро расследований и Службе маршалов США, действующим в тех судебных округах, где расположены центры обработки данных, должно быть дано указание изъять, конфисковать и доставить на временное хранение третьей стороне – Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067 – все принадлежащие Ответчикам компьютеры, серверы, электронные устройства для хранения информации, программное обеспечение, данные и носители информации или их копии, имеющие отношение к IP-адресам в этих центрах, в соответствии со списком в приложении «В».

12. Существуют все основания полагать, что код вредоносной программы Citadel, заражая компьютеры конечных пользователей, представляет собой реальную и непосредственную угрозу таковым пользователям, а также третьим сторонам – финансовым учреждениям, в которых эти конечные пользователи хранят свои сбережения, и что таким образом как конечные пользователи, так и финансовые учреждения, пострадавшие от вредоносной программы Citadel, получат выгоду, если эта программа будет обезврежена и удалена из компьютеров конечных пользователей.

13. Существуют все основания полагать, что код вредоносной программы Citadel, заражая компьютеры конечных пользователей, не позволяет этим

компьютерам соединяться с веб-сайтами, предлагающими приобрести или обновить антивирусные программы, таким образом подвергая эти компьютеры угрозе многократного заражения вирусами – до тех пор пока не будут предприняты действия по обезвреживанию или полному удалению вредоносной программы Citadel.

14. Существуют все основания полагать, что код вредоносной программы Citadel, заражая компьютеры конечных пользователей, продолжить отслеживать процесс просмотра веб-страниц с этих компьютеров до тех пор, пока не будут предприняты действия по его обезвреживанию или полному удалению.

15. Существуют все основания полагать, что Ответчики занимались противозаконной деятельностью, используя интернет-домены, перечисленные в приложении «А» к данному приказу, чтобы размещать на них контролирующее программное обеспечение и контент, используемые для функционирования и технической поддержки ботнета. Существуют все основания полагать, что, для того чтобы немедленно прекратить причинение Ответчиками ущерба, все домены Ответчиков, как действующие сейчас, так и ожидаемые в перспективе, указанные в приложении «А», должны быть немедленно перенаправлены на находящиеся под контролем Microsoft серверы имен NS5.microsoftinternetsafety.net и NS6.microsoftinternetsafety.net, чтобы у Ответчиков больше не было к ним доступа.

16. У суда есть все основания для того, чтобы поручить третьим сторонам – компаниям, предоставляющим услуги по регистрации доменов и веб-хостингу, и центрам обработки данных, находящимся в Соединенных Штатах, оказать все возможное содействие в приведении данного приказа в действие и воздержаться от нарушения планов по его приведению в действие и невыполнения поставленных им

задач, как следует из параграфа 1651(a) раздела 28 Свода законов Соединенных Штатов (Закон о всех судебных приказах).

17. Существуют все основания полагать, что если Ответчикам будет сообщено заранее о ходатайстве Истца о TRO или о настоящем приказе суда, они перебазируют всю инфраструктуру ботнета, что позволит им продолжать их преступную деятельность, и уничтожат, перенесут, спрячут, укроют или любым другим способом сделают недоступными для суда улики, подтверждающие их правонарушения, деятельность ботнета, контрафактные материалы, инструментарий, необходимый для их изготовления, и все записи, свидетельствующие о производстве и распространении контрафактных материалов.

18. У суда есть все основания разрешить вручение уведомления о данном судебном приказе, уведомления о слушании по поводу предварительного судебного запрета и на вручение копии искового заявления в установленной форме или альтернативными способами – принимая во внимание чрезвычайные обстоятельства и необходимость срочной правовой защиты. Следующие способы вручения копии искового заявления разрешены законом, являются надлежащей правовой процедурой, соответствуют указанному в разделе 4(f)(3) Федеральных правил гражданского судопроизводства и позволяют в разумные сроки известить Ответчиков о данном приказе, о слушании по поводу предварительного судебного запрета и о настоящем иске: (1) вручение посредством электронной почты, на адрес электронных сообщений, по факсимильной связи и обычной почтой, используя те имеющиеся адреса электронной почты и электронных сообщений и контактную информацию Ответчиков, которые Ответчики предоставляли регистраторам доменов, центрам

хранения и обработки данных и провайдером интернет-хостинга, которые размещали у себя код программного обеспечения, имеющий отношение к IP-адресам в приложении «В», или через которые были зарегистрированы домены, перечисленные в приложении «А»; (2) доставка лично в руки для тех Ответчиков, кто предоставил центрам хранения и обработки информации и провайдером интернет-хостинга свою контактную информацию в США; (3) доставка лично в руки, по условиям Гаагской конвенции о вручении за границей судебных и внесудебных документов или по условиям других международных соглашений, для тех Ответчиков, кто предоставил контактную информацию за пределами Соединенных Штатов; и (3) публикация извещения для Ответчиков на общедоступном интернет-сайте. Более того, принимая во внимание размер ущерба, причиняемого обществу действиями Ответчиков, у суда имеются все основания разрешить Истцу обнародовать свои действия любым другим способом, с тем чтобы с помощью соответствующих средств обезвредить ботнет Citadel сразу после того, как это дело будет распечатано.

19. Существуют все основания полагать, что ущерб, который понесет Истец, если ему будет отказано в предоставлении правовой защиты в ответ на его ходатайство о TRO, превосходит любое ущемление законных интересов Ответчиков и что на третьи стороны не ляжет чрезмерное обременение.

### **ВРЕМЕННЫЙ ЗАПРЕТИТЕЛЬНЫЙ ПРИКАЗ И**

### **ПРИКАЗ О ПРЕДСТАВЛЕНИИ ОБОСНОВАНИЯ**

**НАСТОЯЩИМ ПРИКАЗЫВАЮ** следующее:

А. Ответчикам, их представителям и лицам, действующим по активному соглашению или совместно с ними, временно запрещается: (1) умышленно и без

полномочия приобретать доступ и рассылать вредоносные компьютерные программы Истцу, в его защищенную операционную систему Windows и программное обеспечение Internet Explorer, в защищенные компьютеры клиентов Истца и в компьютеры третьих сторон – финансовых учреждений и прочих представителей общественности, с намерением инфицировать эти компьютеры вирусами и сделать их частью ботнета; (2) рассылать вредоносные программные средства с целью настройки, развертывания и эксплуатации ботнета; (3) рассылать нежелательные электронные сообщения на учетные записи Microsoft Hotmail; (4) рассылать нежелательные электронные сообщения с ложной информацией о том, что они посланы или одобрены к рассылке Истцом или третьими сторонами, включая банки, Национальную ассоциацию автоматизированных клиринговых палат (НАСНА) или другие компании и организации; (5) создавать веб-сайты с ложной информацией о том, что они связаны с Истцом или третьими сторонами или созданы с их одобрения; (6) похищать информацию, деньги или имущество Истца, клиентов Истца или третьих сторон – финансовых учреждений и прочих представителей общественности или предпринимать любые подобные действия, которые могут повредить Истцу или общественности, включая клиентов Истца, финансовые учреждения и Национальную ассоциацию автоматизированных клиринговых палат (НАСНА).

В. Ответчикам, их представителям и лицам, действующим по активному соглашению или совместно с ними, временно запрещается настраивать, развертывать, эксплуатировать или любым другим образом участвовать или способствовать функционированию ботнетов, перечисленных в ходатайстве о TRO, включая, среди прочего, управление программным обеспечением, размещенным и функционирующим

на доменах и IP-адресах, указанных в данном документе и через другие компоненты или элементы ботнетов, размещенные в любом месте.

С. Ответчикам, их представителям и лицам, действующим по активному соглашению или совместно с ними, временно запрещается использовать торговые марки Истца «Microsoft», «Windows», «Internet Explorer» и торговые марки третьих сторон, включая Национальную ассоциацию автоматизированных клиринговых палат (НАСНА), логотип НАСНА, торговые марки финансовых учреждений и (или) другие торговые марки; торговые названия; знаки обслуживания; адреса или названия интернет-доменов; или совершать любые другие действия, предполагающие каким-либо образом, что продукты или услуги Ответчиков могут быть спонсированы или любым образом связаны с Истцом или другими компаниями и организациями, составляя таким образом незаконную конкуренцию Истцу, незаконно присваивая себе то, что по праву принадлежит Истцу, его клиентам или третьим сторонам, включая финансовые учреждения, Национальную ассоциацию автоматизированных клиринговых палат (НАСНА) или прочих представителей общественности; или выдавать свои товары и услуги за товары и услуги Истца или третьих сторон, включая финансовые учреждения, Национальную ассоциацию автоматизированных клиринговых палат (НАСНА) или прочих представителей общественности.

Д. Ответчикам, их представителям и лицам, действующим по активному соглашению или совместно с ними, временно запрещается нарушать официально зарегистрированные торговые марки Истца: регистрационные номера 2872708 («Microsoft»), 2463510 («Windows») 2277112 («Internet Explorer») и другие.

Е. Ответчикам, их представителям и лицам, действующим по активному

соглашению или совместно с ними, временно запрещается использовать, в связи с деятельностью Ответчиков, любые ложные или вводящие в заблуждение обозначения, представления или описания деятельности Ответчиков или их представителей – сделанные посредством символов, слов, изображений или высказываний, которые могут навредить или причинить ущерб Истцу, либо дадут Ответчикам преимущество в нечестной конкуренции, либо приведут к обману клиентов.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** что регистраторы доменов на территории Соединенных Штатов должны предпринять следующие действия в отношении всех зарегистрированных в настоящее время доменов, перечисленных в приложении «А»:

A. Поддерживать без изменений контактную и иную личную информацию в службе WHOIS, в том виде, в котором эта информация представлена на момент получения этого Приказа, и не менять регистраторов доменов;

B. Домены должны оставаться активно действующими и продолжать свою деятельность, как это предписано настоящим Приказом;

C. Не допускать переноса или модификации доменов Ответчиками или третьими сторонами в регистраторе;

D. Домены должны быть перенаправлены на защищенные серверы путем замены полномочных имен серверов на NS5.microsoftinternetsafety.net и NS6.microsoftinternetsafety.net и (при необходимости) IP-адресов, связанных с именами серверов, или другими способами, разработанными совместно с Microsoft с целью перенаправления доменов и недопущения их использования Ответчиками для контролирования ботнета.

E. Предпринимать все действия, необходимые для распространения



вышеназванных изменений в системе доменных имен (DNS), включая регистраторов доменов;

F. Сохранять все улики, которые могут быть использованы для идентификации Ответчиков, пользующихся доменами.

G. Воздерживаться от того, чтобы отправлять любые извещения или предупреждения или вступать любым другим способом в контакт с Ответчиками или их представителями и воздерживаться от обнародования настоящего Приказа до тех пор, пока он полностью не вступит в силу, за исключением тех случаев, когда контакт с регистраторами и реестрами доменов необходим для выполнения данного приказа.

H. В отношении регистраторов и реестров доменов, находящихся за пределами Соединенных Штатов, суд обращается к ним с почтительной просьбой, но не с приказом, предпринять такие же или во многом схожие действия для того, чтобы нейтрализовать угрозу, которую ботнет Citadel представляет собой для граждан и финансовых учреждений всех стран, включая их собственную. Ответчикам, их представителям и лицам, действующим по активному соглашению или совместно с ними, приказано подчиняться любым действиям, которые регистраторы и реестры доменов, находящиеся за пределами Соединенных Штатов, сочтут необходимыми для выполнения этой просьбы.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ** регистраторам доменных имен на территории Соединенных Штатов предпринять следующие действия в отношении всех не зарегистрированных в настоящее время доменов, перечисленных в приложении «А»:

A. Перевести эти домены под контроль корпорации Microsoft таким образом, чтобы Microsoft являлся их регистрантом с возможностью контролировать хостинг и администрирование. Домены должны быть переведены на аккаунт корпорации Microsoft в

в компании-регистраторе MarkMonitor.

В. В службе WHOIS должна быть зарегистрирована следующая контактная, административная и техническая информация регистранта:

Domain Administrator  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA 98052  
United States  
Phone: +1.4258828080  
Facsimile: +1.4259367329  
domains@microsoft.com

С. Домены должны оставаться активно действующими и продолжать свою деятельность, как это предписано настоящим Приказом или согласно указаниям корпорации Microsoft.

Д. Домены должны быть направлены на полномочные серверы доменных имен NS5.microsoftinternetsafety.net и NS6.microsoftinternetsafety.net и (при необходимости) на IP-адреса, связанные с серверами имен, или другими способами, выработанными совместно с Microsoft для того, чтобы домены и поддомены находились под контролем корпорации Microsoft и чтобы Ответчики не могли их использовать для контролирования ботнета.

Е. Воздерживаться от того, чтобы отправлять любые извещения или предупреждения или вступать любым другим способом в контакт с Ответчиками или их представителями и воздерживаться от обнародования настоящего Приказа до тех пор, пока он полностью не вступит в силу, за исключением тех случаев, когда контакт с регистраторами и реестрами доменов необходим для выполнения данного приказа.

И. В отношении регистраторов и реестров доменов, находящихся за пределами Соединенных Штатов, суд обращается к ним с почтительной просьбой, но не с приказом,

предпринять такие же или во многом схожие действия для того, чтобы нейтрализовать угрозу, которую ботнет Citadel представляет собой для граждан и финансовых учреждений всех стран, включая их собственную. Ответчикам, их представителям и лицам, действующим по активному соглашению или совместно с ними, приказано подчиняться любым действиям, которые регистраторы и реестры доменов, находящиеся за пределами Соединенных Штатов, сочтут необходимыми для выполнения этой просьбы.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** чтобы материалы Ответчиков, несущие на себе контрафактные торговые знаки, способы производства контрафактных торговых знаков, материалы, используемые для их изготовления и применения, а также все относящиеся к этому записи, находящиеся в центрах обработки данных в ведении Linode LLC/Linode VPS Hosting и Network Operations Center, Inc./BurstNET Technologies, Inc., были изъяты в соответствии с параграфом 1116(d) раздела 15 Свода законов США:

А. Изъятие в вышеперечисленных центрах хранения и обработки информации и у провайдеров интернет-хостинга должно быть произведено 5 июня, около 9:30 по североамериканскому восточному времени, не позднее чем через семь (7) дней после издания настоящего приказа. Изъятие может продолжаться на ежедневной основе в течение периода времени, не превышающего два (2) дня, до тех пор, пока все не будет изъято. Изъятие будет производить Федеральное бюро расследований и (или) Служба маршалов США. Федеральному бюро расследований и (или) Службе маршалов США, действующим в тех судебных округах, где расположены центры обработки данных, даны инструкции согласовывать свои действия друг с другом и с корпорацией Microsoft и ее адвокатами при выполнении распоряжений настоящего Приказа таким образом, чтобы выведение из строя и (или) изъятие материалов Ответчиков на таких серверах

происходило одновременно, с тем, чтобы у Ответчиков не было возможности осуществлять деятельность ботнета, пока это дело находится в процессе рассмотрения. В целях оказания содействия такому согласованию ниже приводятся адреса офисов Службы маршалов США в соответствующих судебных округах:

- a. District of New Jersey  
U.S. Marshal: Juan Mattos Jr.  
U.S. Courthouse  
50 Walnut Street  
Newark, NJ 07102  
(973) 645-2404
  
- b. Middle District of Pennsylvania  
U.S. Marshal: Martin J. Pane  
Federal Building  
Washington Avenue & Linden Street, Room 231  
Scranton, PA 18501  
(570) 346-7277

В. В процессе вышеназванного изъятия, агентов Федерального бюро расследований и (или) федеральных маршалов и их помощников должны сопровождать адвокаты корпорации Microsoft и эксперты-криминалисты с целью оказания содействия в идентификации, составлении описи, захвате и изоляции принадлежащих Ответчикам компьютерных ресурсов, контролирующих компьютерных программ и других компонентов программного обеспечения, на которые будет наложен арест. Агенты Федерального бюро расследований и (или) федеральные маршалы должны будут при необходимости изолировать злонамеренную деятельность Ответчиков, захватить компьютеры Ответчиков, их серверы, электронные устройства для хранения информации или носители информации, связанные с IP-адресами Ответчиков в перечисленных выше хостинговых компаниях,

или обеспечить прямое изображение данных и информации Ответчиков на этих компьютерах, серверах, электронных устройствах для хранения информации или носителях информации – по усмотрению агентов Федерального бюро расследований, представителей Службы маршалов США и экспертов-криминалистов и (или) юристов корпорации Microsoft. До того отключения этих компьютеров от сети Интернет необходимо сохранить четыре последних часа интернет-трафика на серверах Ответчиков, связанных с IP-адресами в хостинговых компаниях, упомянутых выше.

C. Компания Stroz Friedberg (1925 Century Park East, Suite 1350, Los Angeles, CA 90067) выступит в качестве временного хранителя всей изъятой информации и имущества и всех сохраненных улик согласно настоящему приказу и освободит Федеральное бюро расследований и Службу маршалов США от ответственности за любые действия, инциденты или происшествия, связанные с арестом и принятием во владение собственности Ответчиков, включая заявления от третьих сторон, и Федеральное бюро расследований и Служба маршалов США будут освобождены от своих обязанностей и ответственности за хранение изъятых материалов.

D. Агентам Федерального бюро расследований и (или) федеральным маршалам, производящим таковое изъятие, выдано разрешение входить в помещения центров обработки данных, находящихся в ведении Linode LLC/Linode VPS Hosting и Network Operations Center, Inc./BurstNET Technologies, Inc., с тем чтобы вручить копии настоящего Приказа, выполнить условия настоящего Приказа и убедиться в исполнении настоящего Приказа. Агенты Федерального бюро расследований и (или) федеральные маршалы должны будут использовать все разумные средства,

необходимые для выполнения условий настоящего Приказа и проверки содержимого всех компьютеров, серверов, электронных устройств для хранения информации, носителей информации и содержимого всех комнат, стенных и обычных шкафов, автомобилей, контейнеров, рабочих столов или документов, а также для демонтажа всего оборудования, используемого Ответчиками для занятий деятельностью, на которую настоящим Приказом налагается запрет.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** что провайдеры интернет-хостинга, перечисленные в приложении «В», должны действовать следующим образом в отношении IP-адресов, перечисленных в приложении «В»:

А. Не способствовать и предпринять все возможные шаги для предотвращения попыток Ответчиков или их представителей или любых других лиц уклониться от выполнения условий настоящего Приказа в отношении этих IP-адресов;

В. Заблокировать доступ и отказать в доступе Ответчикам и их представителям ко всем «резервным» системам, возможностям и услугам резервного копирования, которые могут быть использованы для поддержки доменов Ответчиков или для злонамеренных действий с использованием IP-адресов, указанных в приложении «В», или для уклонения от выполнения условий настоящего Приказа;

С. Регистрировать все попытки установить соединение или связь с IP-адресами, указанными в приложении «В»;

Д. Сохранить, удержать у себя и передать корпорации Microsoft все документы и информацию, достаточные для того, чтобы идентифицировать и установить контакт с Ответчиками и представителями Ответчиков, эксплуатирующими или контролирующими IP-адреса, указанные в приложении «В», включая всех физических и юридических лиц,

почтовые адреса, адреса электронной почты, номера факсов и телефонов или подобную этой контактную информацию, включающую, среди прочего, контактную информацию, указываемую на счетах, при пользовании, получении доступа и регистрации, а также все записи, документы и регистрационные записи, имеющие отношение к использованию Ответчиками или их представителями IP-адресов и доступа к ним.

Е. Полностью воздерживаться от того, чтобы отправлять любые извещения или предупреждения или вступать любым другим способом в контакт с Ответчиками или их представителями и воздерживаться от обнародования настоящего Приказа, до тех пор пока он полностью не вступит в силу, за исключением случаев, прямо предусмотренных в настоящем Приказе;

Ф. Перевести любой контент и программы, размещенные на IP-адресах Ответчиков, перечисленных в приложении «В», и не имеющие отношения к Ответчикам, на новые IP-адреса, не перечисленные в приложении «В»; известить владельцев такового контента и программ, не являющихся стороной в настоящем деле, о новых IP-адресах и сообщить им, чтобы они связались с адвокатом корпорации Microsoft Габриэлем М. Рэмзи по адресу: Orrick Herrington & Sutcliffe, 1000 Marsh Road, Menlo Park, CA 90425-1015, (тел.: 650-614-7400), для получения помощи в любых последующих действиях;

Г. Оказывать разумную помощь в исполнении положений настоящего Приказа и не предпринимать никаких действий, которые могут помешать исполнению настоящего Приказа: предоставлять достаточный доступ в разумных пределах в офисы, помещения, компьютерные сети, компьютеры и сервисы с тем, чтобы Федеральное бюро расследований, Служба маршалов США, корпорация Microsoft и ее юристы и (или) представители имели возможность вести непосредственное наблюдение за исполнением

положений Приказа в отношении Ответчиков и могли подтвердить его выполнение;

Н. В отношении полного списка IP-адресов, о которых известно, что они связаны с ботнетами, проходящими по этому делу, перечисленными в приложении «В», любая компания, предоставляющая услуги веб-хостинга и несущая ответственность за эти IP-адреса, находящаяся в Соединенных Штатах, должна оказывать любую разумную помощь корпорации Microsoft с тем, чтобы подтвердить, поддерживают ли эти IP-адреса ботнеты и, если это так, принять все необходимые меры для предотвращения их использования Ответчиками.

И. В отношении регистраторов и реестров доменов, находящихся за пределами Соединенных Штатов, суд обращается к ним с почтительной просьбой, но не с приказом, предпринять такие же или во многом схожие действия для того, чтобы нейтрализовать угрозу, которую ботнет Citadel представляет собой для граждан и финансовых учреждений всех стран, включая их собственную. Ответчикам, их представителям и лицам, действующим по активному соглашению или совместно с ними, приказано подчиняться любым действиям, которые регистраторы и реестры доменов, находящиеся за пределами Соединенных Штатов, сочтут необходимыми для выполнения этой просьбы.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** чтобы копии настоящего Приказа, извещение о слушании по поводу предварительного судебного запрета и копия искового заявления были вручены любым способом, предусмотренным законом, включая (1) вручение посредством электронной почты, по факсимильной связи и обычной почтой, используя те имеющиеся адреса электронной почты и электронных сообщений и контактную информацию Ответчиков, которые Ответчики предоставляли регистраторам доменов, центрам хранения и обработки данных и провайдерам интернет-хостинга,



которые размещали у себя код программного обеспечения, имеющий отношение к IP-адресам и доменам, указанным в приложениях «А» и «В»; (2) лично в руки для тех Ответчиков, кто предоставил свою контактную информацию в США; (3) лично в руки, по условиям Гаагской конвенции о вручении за границей судебных и внесудебных документов для тех Ответчиков, кто предоставил контактную информацию за пределами Соединенных Штатов; (4) через публикацию извещения для Ответчиков на общедоступном сайте в сети Интернет.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** что, в соответствии с пунктом 65(b) Федеральных правил гражданского судопроизводства, Ответчики должны явиться в этот суд 10th июня 2013 г., в 10:00AM, чтобы обосновать причину, если таковая имеется, по которой суд не должен выдавать предварительный судебный запрет до принятия окончательного решения по исковому заявлению против Ответчиков, каковой запрет не позволит им заниматься деятельностью, на которую наложено временное ограничение согласно предыдущим положениям настоящего Приказа.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** чтобы корпорация Microsoft внесла судебный залог в размере 300 тыс. долларов США, который должен быть уплачен в канцелярии суда.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** что, для того чтобы полностью обезвредить вредоносные программы ботнета Citadel, которые захватили контроль над собственностью корпорации Microsoft, включая ее операционную систему Windows, браузер Internet Explorer и связанные с ними файлы; чтобы вернуть корпорации Microsoft контроль над этой собственностью; чтобы остановить причинение

невозмещимого вреда корпорации Microsoft и ее клиентам, устранения источника зловредности, вызванной деятельностью Ответчиков, и информировать клиентов о том, какие меры они могут предпринять для перманентного удаления вредоносного кода Citadel со своих компьютеров, в соответствии с условиями лицензии корпорации Microsoft, выдаваемой на пользование ее операционной системой Windows, корпорации Microsoft дается разрешение сделать следующее:

1. Через контролирование корпорацией Microsoft доменов и IP-адресов, перечисленных в приложениях «А» и «В», разрешенное настоящим Приказом, перенаправлять все зараженные Citadel компьютеры конечных пользователей, пытающиеся установить соединение с любым командным сервером Citadel, для соединения с одним или несколькими серверами, находящимися под контролем корпорации Microsoft («Лечебные серверы корпорации Microsoft»);
2. В течение двух или более недель с даты подписания настоящего Приказа установить на Лечебном сервере корпорации Microsoft первый лечебный файл конфигурации («Первый лечебной файл конфигурации»), за которым обращается вредоносное программное средство Citadel, установленное на компьютерах конечных пользователей, с тем чтобы после установления соединения с Лечебным сервером корпорации Microsoft вредоносная программа ботнета Citadel начала бы проводить загрузку и расшифровку, а после этого стала бы следовать командам Первого лечебного файла конфигурации;
3. Разрешить корпорации Microsoft подготовить Первый лечебный файл

конфигурации таким образом, чтобы он (а) остановил пагубные действия вредоносной программы ботнета Citadel; (b) позволил зараженному компьютеру выйти на антивирусные веб-сайты для получения содействия и инструментария для удаления вируса Citadel из компьютера, каковые веб-сайты в настоящее время заблокированы программой ботнета Citadel; (c) предотвращал соединение вредоносного программного средства Citadel на компьютере с любым из известных командных серверов Citadel и перенаправлял его для соединения с Лечебными серверами корпорации Microsoft.

4. Не раньше чем через две недели после подписания настоящего Приказа разрешить корпорации Microsoft установить на Лечебном сервере корпорации Microsoft второй лечебный файл конфигурации («Второй лечебный файл конфигурации»), с запросом о котором, как известно, обращается вредоносное программное средства Citadel;
5. Разрешить корпорации Microsoft подготовить Второй лечебный файл конфигурации таким образом, чтобы, когда конечный пользователь зараженного компьютера попытается выйти на любой веб-сайт в сети Интернет, кроме антивирусного, используя браузеры Internet Explorer, Google Chrome или Mozilla Firefox, он увидит в своем браузере извещение («Лечебное извещение»), которое будет оставаться там примерно двадцать минут, в течение которых пользователь сможет установить соединение только с Лечебными серверами корпорации Microsoft или с антивирусными веб-сайтами;

6. Разрешить корпорации Microsoft, если она сочтет это необходимым и целесообразным, пропагандировать дальнейшую дезинфекцию компьютеров, в настоящее время зараженных Citadel, в качестве альтернативы установке Первого и Второго лечебных файлов конфигурации на Лечебных серверах, таким образом, что Лечебное извещение будет появляться на мониторах пользователей компьютеров, зараженных вредоносной программой ботнета Citadel, на двадцать минут каждые пять часов на протяжении суток, один раз в неделю, до тех пор пока корпорация Microsoft не решит, что больше нет необходимости напоминать владельцам зараженных компьютеров о необходимости очистить их компьютеры от вирусов ботнета Citadel.

**ДАЛЕЕ НАСТОЯЩИМ ПРИКАЗЫВАЮ,** что Ответчики должны предоставить в суд, с вручением копий адвокатам корпорации Microsoft, все ответные заявления, объяснения, ходатайства, отчеты экспертов или уведомления и (или) юридические заключения не позднее чем за два (2) дня до начала слушания по поводу предварительного судебного запрета по просьбе корпорации Microsoft. Корпорация Microsoft может подать в суд встречные или дополнительные объяснения, материалы, заявления или юридические заключения, с вручением их копий адвокатам Ответчиков, не позднее чем за один (1) день до начала слушания по этому делу. Копии должны быть переданы в руки курьерской почтой (лично в руки), экспресс-доставкой, по факсимильной связи или электронной почте, и документы должны быть доставлены так, чтобы принимающая сторона получила их не позднее 16:00 (по североамериканскому восточному времени) соответствующих чисел месяца,

перечисленных в этом параграфе.

**ПРИКАЗАНО**

Вынесено \_\_\_\_ мая 2013 г. \_\_\_\_\_

Судья федерального суда Соединенных Штатов Америки