В ОКРУЖНОЙ СУД СОЕДИНЕННЫХ ШТАТОВ ЗАПАДНОГО ОКРУГА ТЕХАСА, РАЙОН ОСТИНА

ЗАРЕГИСТРИРОВАНО 25 НОЯБРЯ 2013 г. 08:58

Клерк Регионального Суда США, Западный регион Техаса

(подпись неразборчиво) – заместитель.

КОРПОРАЦИЯ MICROSOFT, вашингтонская компания,	§	ДЕЛО НОМЕР:
	§	**A13CV1014**
Истец	§	
	§	
против	§	**СКРЕПЛЕНО ПЕЧАТЬЮ**
	§	
НЕНАЗВАННЫЕ 1–8, КОНТРОЛИРУЮЩИЕ КОМПЬЮТЕРНЫЙ БОТНЕТ, НАНОСЯЩИЙ УЩЕРБ MICROSOFT И ЕЕ ЗАКАЗЧИКАМ,	§	
	§	
Ответчики.	§	

ХОДАТАЙСТВО КОРПОРАЦИИ MICROSOFT О СРОЧНОМ ОДНОСТОРОННЕМ ВЫНЕСЕНИИ ВРЕМЕННОГО ЗАПРЕТИТЕЛЬНОГО СУДЕБНОГО ПРИКАЗА И ПРИКАЗА О ПРЕДОСТАВЛЕНИИ ОБОСНОВАНИЯ КАСАЕМО ПРЕДВАРИТЕЛЬНОГО СУДЕБНОГО ЗАПРЕТА

Истец, корпорация Microsoft («Microsoft»), в лице юридической службы, в соответствии с федеральными правилами гражданского судопроизводства 65(b) и (c), законом о компьютерном мошенничестве и злоупотреблении (18 U.S.C. § 1030); законом об охране права на электронную связь (18 U.S.C. § 2701); законом Ленхема (15 U.S.C. §§ 1114, 1116, & 1125); общим правом в части посягательства, присвоения и необоснованного обогащения; а также законом о вынесении судебных приказов (28 U.S.C. § 1651) испрашивает срочное одностороннее вынесение временного

запретительного судебного приказа и приказа о предоставлении обоснования того, что предварительный судебный запрет не должен быть наложен.

Как указано в прилагаемой к настоящему ходатайству справке, Microsoft испрашивает судебный приказ о блокировке некоторых адресов протокола Internet Protocol (IP) и доменов сети Интернет, посредством которых Ответчики контролируют вредоносный «ботнет», известный под именем «ботнет ZeroAccess». Ботнет ZeroAccess состоит из почти двух миллионов компьютеров конечных пользователей, инфицированных вредоносным программным обеспечением (ПО), передающим зараженные компьютеры под управление Ответчиков, которые используют их для незаконных действий, в том числе «перехвата браузера», «мошенничества со щелчками», кражи личной информации конечных пользователей и нарушения товарных знаков Microsoft. Испрашиваемая мера воздействия необходима для прекращения нанесения непоправимого ущерба Microsoft, ее заказчикам и обществу со стороны ботнета. Как указано в прилагаемой к настоящему ходатайству справке, принятие испрашиваемых мер в одностороннем порядке необходимо, так как при получении заблаговременного уведомления у Ответчиков будет возможность уничтожить, переместить, скрыть или иным способом исключить доступ к средствам, используемым для управления вредоносным ботнетом ZeroAccess. По этой причине Microsoft ходатайствует об удовлетворении данного прошения.

Ходатайство Microsoft включает в себя следующие документы: настоящее ходатайство; справка Microsoft в поддержку настоящего ходатайства; исковые заявления David Anselmi, Jason Lyons и Jacob M. Heath в поддержку ходатайства Microsoft и приложенные к ним доказательства; подаваемые состязательные бумаги; а также

аргументы и свидетельства, которые могут быть представлены на слушаниях по настоящему ходатайству.

Microsoft также ходатайствует о назначении судебных слушаний по этому делу на 25 ноября 2013 года.

Дата: 25 ноября 2013 г.

Ходатайствующие

FISH & RlCHARDSON P.C.

В лице: _____
David M. Hoffman
Texas Bar No. 24046084
hoffman@fr.com

William Thomas Jacks
Texas Bar No. 10452000
jacks@fr.com

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

В лице юридической службы:

ORRICK, HERRINGTON & SUTCLIFFE LLP

Gabriel M. Ramsey
(Заявление pro hac vice в стадии рассмотрения)
gramsey@orrick.com

Jeffrey L. Cox
(Заявление pro hac vice в стадии рассмотрения)
jcox@orrick.com

Jacob M. Heath
(Заявление pro hac vice в стадии рассмотрения)
jheath@orrick.com

Robert L. Uriarte
(Заявление pro hac vice в стадии рассмотрения)
ruriarte@orrick.com

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

Юридическая поддержка истца
КОРПОРАЦИЯ MICROSOFT

СПРАВКА К ХОДАТАЙСТВУ КОРПОРАЦИИ MICROSOFT О СРОЧНОМ ОДНОСТОРОННЕМ ВЫНЕСЕНИИ ВРЕМЕННОГО ЗАПРЕТИТЕЛЬНОГО СУДЕБНОГО ПРИКАЗА И ПРИКАЗА О ПРЕДОСТАВЛЕНИИ ОБОСНОВАНИЯ КАСАЕМО ПРЕДВАРИТЕЛЬНОГО СУДЕБНОГО ЗАПРЕТА

I. ВВЕДЕНИЕ

Истец, корпорация Microsoft («Microsoft»), ходатайствует о срочном одностороннем вынесении временного запретительного судебного приказа («ВЗСП») и предварительного судебного запрета, предписывающего провайдерам услуг Интернета в США заблокировать связь с 18 IP-адресами сети Интернет в Европе, которые используются киберпреступниками для управления «ботнетом ZeroAccess» («ZeroAccess»), наносящим вред потребителям и компаниям по всей стране, в том числе в данном судебном округе.

Microsoft испрашивает судебное решение в рамках федеральных правил гражданского судопроизводства 65(b), закона Ленхема, 15 § 1116(a), закона о вынесении судебных приказов, 28 U.S.C. § 1651 и общей правомочности суда для прекращения вреда, сохранения статус-кво и обеспечения сохранности свидетельств деятельности Ответчиков на время рассмотрения этого дела.

Чрезвычайные меры являются оправданными, поскольку ZeroAccess непрерывно наносит непомерный и невосполнимый ущерб Microsoft, ее заказчикам и обществу. Будучи уведомленными заранее, Ответчики получат возможность сокрыть свою незаконную деятельность и уничтожить основные улики.

Ботнет — это обширная сеть компьютеров, зараженных вредоносным программным обеспечением (вредоносное ПО), которое превращает данные компьютеры в средство реализации преступных замыслов, от кражи личной информации до

крупномасштабного мошенничества. Ботнеты одинаково опасны для конечных пользователей, компаний и государственных учреждений.

Ботнет ZeroAccess состоит из миллионов зараженных компьютеров конечных пользователей. Так, только лишь 23 октября 2013 г. наблюдалась активность около 20 000 зараженных ZeroAccess компьютеров в Техасе, многие из которых находились на территории Остина (с пригородами). Вредоносное ПО загружается на компьютеры, когда те обращаются к любому из множества веб-сайтов, созданных или взломанных Ответчиками. Будучи загруженным на компьютер пользователя, вредоносное ПО маскируется под полезную программу, убеждая пользователя выполнить установку. При установке ZeroAccess наносит урон операционной системе Microsoft Windows, отключая ее средства безопасности, подменяя драйверы и изменяя настройки реестра. Затем ZeroAccess заражает браузер Internet Explorer, превращая его в средство реализации преступных намерений.

Также ZeroAccess добавляет компьютер к армии зараженных компьютеров, которые Ответчики контролируют посредством группы серверов, расположенных в Европе. Указанные вредоносные серверы подключены к сети Интернет с помощью 18 адресов протокола Internet Protocol («IP») и 49 доменов сети Интернет, которые приведены Microsoft в приложении А. Эти 18 IP-адресов и 49 доменов — прямое средство нанесения Ответчиками ущерба и контроля компьютеров пострадавших с США.

Зараженный компьютер становится инструментом в преступной схеме Ответчиков, которые используют его для кражи денег путем мошенничества с системами интернет-рекламы. Поскольку защитные средства компьютера отключаются, он становится уязвимым для заражения иными видами вредоносного ПО. В их числе Zeus, печально известный ботнет финансового мошенничества, который отслеживает

проведение банковских операций владельцем компьютера и использует собранную информацию для кражи средств со счетов, а также других видов мошенничества с участием вредоносного ПО[1].

Ботнет ZeroAccess наносит серьезный ущерб репутации и нематериальным активам Microsoft. Он подрывает и искажает нормальное функционирование операционной системы Microsoft Windows®, браузера Internet Explorer® и поисковой системы Bing®, фактически превращая эти широко используемые приложения, несущие на себе узнаваемые логотипы Microsoft, в средства мошенничества. Он также понижает производительность зараженных компьютеров, использующих операционную систему Microsoft Windows, что часто воспринимается пользователями как признак низкого качества самой системы Windows.

Испрашиваемый ВЗСП направлен на прекращение возможности связи компьютеров, зараженных ZeroAccess, с IP-адресами («IP-адреса контроля мошенничества») и доменами («домены контроля мошенничества»), с которых эти компьютеры получают указания по совершению мошенничества, что составляет основу функционирования ZeroAccess. Каждому из IP-адресов контроля мошенничества Ответчики сопоставили один или несколько специализированных компьютеров («серверы контроля мошенничества»), которые передают такие указания зараженным компьютерам. Отключение связи с IP-адресами и доменами контроля мошенничества ZeroAccess позволит прекратить связь между Ответчиками и зараженными компьютерами. Если серверы контроля мошенничества ZeroAccess не смогут связываться

[1] По осторожным оценкам исследователей, киберпреступники провели через Zeus более 100 миллионов долларов.

с зараженными компьютерами, Ответчики не будут иметь возможность передавать таким компьютерам указания относительно перехвата браузера и мошенничества со щелчками.

Принятие мер в одностороннем порядке необходимо, поскольку, будучи уведомленными, Ответчики смогут уничтожить, переместить, скрыть или иным способом исключить доступ к средствам, используемым для контроля ZeroAccess — основной улике их незаконных действий. Представляется бесспорным, что при получении уведомления Ответчики внесут изменения в инфраструктуру контроля мошенничества до того, как испрашиваемый ВЗСП будет выдан, и (или) предпримут меры, затрудняющие пресечение деятельности по перехвату браузеров и мошенничеству со щелчками, а также поиск и устранение вредоносного ПО с зараженных компьютеров. Испрашиваемый судебный приказ позволит заблокировать текущие 18 IP-адресов контроля мошенничества и 49 доменов контроля мошенничества, а также позволит Microsoft дополнять приказ новыми IP-адресами или доменами, если Ответчики попытаются обойти запрет, используя новые адреса или домены.

Испрашиваемая односторонняя мера не является новой при отключении опасных ботнетов; в семи случаях суд выносил такое чрезвычайное решение для отключения ботнета (истцом выступала не только Microsoft). Так, в феврале 2010 г. при рассмотрении дела о ботнете «Waledac» окружной суд Восточного округа Вирджинии (судья Бринкема) применил следующих подход:

1. суд издал особый односторонний ВЗСП, предусматривающий меры, необходимые для эффективного отключения вредоносной инфраструктуры ботнета, сохранения всех свидетельств его функционирования и остановки непоправимого ущерба Microsoft и ее заказчикам;

2. немедленно после вступления ВЗСП в силу Microsoft предприняла комплекс мер по уведомлению Ответчиков о слушаниях по предварительному судебному запрету и вручению им судебного документа, в том числе с использованием одобренных судом способов доставки: по электронной почте, средствам электронной связи, почте, факсу, путем публикации и предусмотренными договорами средствами; а также
3. после уведомления суд провел слушания по предварительному судебному запрету и наложил предварительный судебный запрет на время рассмотрения дела, чтобы исключить текущее совершение ботнетом вреда.

См. Microsoft v. John Does 1-27, Дело № 1:10-cv-00156 (E.D. Va. 2010) (Brinkema, J.) (приказы, приложенные к исковому заявлению Jacob M. Heath («Heath Decl.»), Exs. 14 и 15.) Впоследствии федеральные суды использовали тот же подход в шести других случаях, где фигурировали опасные ботнеты. См. Microsoft v. John Does, 1-11, Дело № 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (Heath Decl., Exs. 16 и 17; касаемо ботнета «Rustock»); Microsoft v. Piatti, et al., Дело № 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (Heath Decl., Exs. 18 и 19; касаемо ботнета «Kelihos»); Microsoft Corp. et al. v. John Does 1-39 et al., Дело № 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (Heath Decl. Exs. 20 и 21; касаемо ботнетов «Zeus»); Microsoft Corp. v. Peng Yong et al., Дело № 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (Heath Decl., Ex. 22; касаемо ботнета «Nitol»); Microsoft Corp. v. John Does 1-18 et al., Дело № 1:13-cv-139-LMB/TCB (E.D. Va.) (Brinkema, J.) (Heath Decl. Exs. 30 и 31; касаемо ботнета «Bamital»); Microsoft v. John Does 1-82, Дело № 3:13-CV-00319-GCM (W.D.N.C.) (Mullen, J.) (Heath Decl. Exs. 32 и 33; касаемо ботнетов «Citadel»).

При удовлетворении судом заявления корпорации Microsoft та, немедленно после выполнения ВЗСП, в соответствии с надлежащей правовой процедурой предпримет все

необходимые усилия для доставки уведомления о слушаниях по предварительному судебному запрету и исполнении дела в отношении Ответчиков. Microsoft немедленно ознакомит Ответчиков со своей жалобой и всеми сопутствующими материалами, используя контактную информацию, известную ей, а также третьим сторонам, предоставляющим услуги хостинга и регистрации доменов, используемые в контролирующей инфраструктуре Ответчиков.

II. ОБСТОЯТЕЛЬСТВА ДЕЛА: БОТНЕТ ZEROACCESS

«ZeroAccess», также известный как «Sirefef» или «max++», — это вредоносное программное обеспечение (вредоносное ПО), которое скрытно инфицирует компьютер без ведома пользователя и присоединяет этот компьютер к сети компьютеров, называемой «ботнет». (Исковое заявление David Anselmi ISO TRO («Anselmi Decl.») ¶ 3) По недавним подсчетам, по всему миру заражено около 1,9 миллиона компьютеров, и каждый день около 800 000 из них участвуют в мошеннических операциях. (там же, ¶ 3) Большинство зараженных компьютеров расположены в США и Западной Европе. Недавно Microsoft зафиксировала примерно 20 000 зараженных компьютеров за один день только в Техасе. (там же, ¶ 3)

Ботнет в сущности представляет собой очень эффективную систему управления большим числом компьютеров, конечной целью которой являются действия против содержимого этих компьютеров или против других компьютеров в сети Интернет. (там же, ¶ 39) Операторы ботнета могут использовать сеть зараженных персональных компьютеров для самых разных неблаговидных и преступных действий, в том числе рассылки спама, выполнения атаки отказа в обслуживании других компьютеров сети Интернет, кражи финансовых и банковских данных, перехвата сообщений, слежки и т.п.

(там же, ¶ 39) Возможность доступа к таким персональным компьютерам может продаваться, сдаваться в аренду или переходить от одной преступной группе к другой. (там же, ¶ 39)

Расследование Microsoft показало, что киберпреступники, контролирующие ботнет ZeroAccess, используют зараженные компьютеры для различных форм незаконной деятельности, связанной с интернет-рекламой, в том числе «перехвата браузера» и «мошенничества со щелчками».[2] (там же, ¶ 5) Используя перехват браузера, киберпреступники, контролирующие ZeroAccess, могут по своему желанию подключать компьютеры к небезопасным веб-сайтам. (там же, ¶ 5) Тем самым они получают возможность продать трафик посещения веб-сайтам, содержащим рекламу на базе платформ доставки интернет-рекламы. Иногда, однако, веб-сайт, приобретающий такой трафик, принадлежит другой группе киберпреступников, которые используют генерируемый ZeroAccess трафик для распространения собственного вредоносного ПО. Используя мошенничество со щелчками, Ответчики могут направить зараженные компьютеры на нужные им веб-сайты и сымитировать щелчки по рекламной информации на них, что повышает ценность трафика, генерируемого ZeroAccess, для веб-сайтов, зарабатывающих на интернет-рекламе.

A. Интернет-реклама и мошенничество

Темпы роста, размер и сложность многомиллиардного рынка интернет-рекламы делают его привлекательной целью для мошенников. (там же, ¶¶ 10-11) Киберпреступники разработали немало схем манипулирования бизнес-моделью

[2] ZeroAccess также содержит модуль для «добычи Bitcoin». Bitcoin представляет собой нерегулируемую электронную криптографическую валюту, популярную среди киберпреступников. Чтобы «добыть» Bitcoin, необходимо найти решение исключительно сложного уравнения. Ответчики используют объединенные вычислительные мощности компьютеров, составляющих ботнет ZeroAccess, для извлечения дохода помимо прибыли от мошенничества со щелчками и перехвата браузера.

интернет-рекламы и зарабатывают на них миллионы долларов ежегодно. (там же, ¶ 11) Например, придуманы способы имитации «щелчков» или просмотров рекламы — событий, которые генерируют доход для веб-сайта, на котором была размещена эта реклама. (там же, ¶ 11) Компьютер жертвы заражается вредоносным программным обеспечением (вредоносным ПО), которое заставляет компьютер выполнять такие щелчки без ведома своего владельца. (там же, ¶ 12) Эта схема хорошо работает для киберпреступников, поскольку при большом количестве разнесенных географически зараженных компьютеров на каждый компьютер приходится не так много сгенерированных фальшивых щелчков, что позволяет обойти систему защиты от мошенничества, используемую в рекламных платформах. (там же.)

Microsoft владеет одной из крупнейших рекламных платформ в сети Интернет, и поэтому является объектом сетевого мошенничества. Microsoft владеет и заведует поисковой системой Bing® и платформой интернет-рекламы Microsoft Bing® Ads. (там же, ¶ 13) В рамках платформы Bing Ads корпорация Microsoft сотрудничает с различными компаниями, желающими разместить рекламу в сети Интернет («Рекламодатели»). (там же, ¶ 13) Microsoft размещает рекламу рекламодателя, помимо прочих мест, в сети веб-сайтов, принадлежащих другим лицам («Публикаторы»), которые также участвуют в программе сетевой рекламы Microsoft.

Принцип состоит в том, что пользователь щелкает заинтересовавшую его рекламу и выполняет дополнительные действия, например, приобретает продукты и услуги Рекламодателя. (там же, ¶ 14) Когда пользователь щелкает рекламное объявление, Рекламодатель выплачивает вознаграждение Публикатору веб-сайта, где произошел щелчок. (там же, ¶¶ 15-16). К сожалению, злоумышленники используют компьютеры конечных пользователей, зараженные вредоносным ПО, скриптами автоматизации и

другими средствами, для выполнения большого числа щелчков и (или) просмотров рекламных объявлений, размещенных на веб-сайтах в рамках платформы Microsoft Bing Ads и других платформ. (там же, ¶ 17) Эта мошенническая деятельность наносит ущерб рекламодателям и Microsoft, поскольку рекламодатели оплачивают «щелчки», которые не представляют реальных пользователей, заинтересованных в рекламируемом продукте или услуге. (там же, ¶¶ 17-21) Такая деятельность называется «мошенничество со щелчками». (там же, ¶ 17)

В рассматриваемом случае Ответчики заражали компьютеры конечных пользователей вредоносным ПО, встраивая их в ботнет ZeroAccess. Вредоносное ПО ZeroAccess скрытно устанавливается на компьютер пользователя для выполнения «перехвата поиска» и «мошенничества со щелчками», направленного против Microsoft и рекламодателей в сети Интернет. ZeroAccess вызывает принудительное посещение веб-сайтов и выполняет щелчки на рекламных объявлениях с целью мошеннического заработка путем злоупотребления платформой Microsoft Bing Ads и другими крупными рекламными платформами и рекламодателями. (там же, ¶ 20)

B. Вредоносное ПО ZeroAccess устанавливается на компьютер обманным путем и без согласия пользователя

ZeroAccess устанавливается на компьютер пользователя обманным путем. Большинство случаев заражения ZeroAccess происходит в результате так называемой «скрытой загрузки». (там же, ¶ 43) Киберпреступники создают или взламывают веб-сайт и размещают на нем специализированное программное обеспечение, «пакет использования уязвимостей», предназначенное для заражения компьютера конечного пользователя. (там же, ¶ 43) Такие веб-сайты называются «веб-сайтами использования уязвимостей». (там же, ¶ 43) Когда компьютер пользователя подключается к такому веб-

сайту, пакет использования уязвимостей скрытно проверяет этот компьютер на наличие незакрытых уязвимостей в операционной системе или популярных приложениях, или на отсутствие актуальной антивирусной программы, что позволило бы выполнить код или внедрить вредоносное ПО в операционную систему. (там же, ¶ 43) Если пакет использования уязвимостей обнаруживает незакрытую уязвимость или отсутствие актуальной антивирусной программы, он загружает и устанавливает на компьютер вредоносное ПО ZeroAccess или другое вредоносное ПО. (там же, ¶ 43)

Чтобы заставить пользователя посетить веб-сайт использования уязвимостей, киберпреступники обычно размещают код перенаправления на других веб-сайтах Интернета. (там же, ¶ 44) Это могут быть популярные веб-сайты, которые киберпреступники специально для этой цели взламывают, либо веб-сайты, изначально созданные для завлечения ничего не подозревающих пользователей и перенаправления их на веб-сайт использования уязвимостей. (там же, ¶ 44) Когда ничего не подозревающий пользователь переходит на один из таких веб-сайтов, код перенаправления на нем скрытно и автоматически переводит компьютер пользователя на сайт использования уязвимостей. (там же, ¶ 44) После заражения компьютер пользователя становится частью ботнета, способной связываться с операторами ботнета и получать от них указания, как описано ниже, а операторы ботнета получают контроль над компьютером пользователя. (там же, ¶ 46)

C. ZeroAccess при установке повреждает операционную систему Windows и браузер Internet Explorer

Вредоносному ПО ZeroAccess для установки требуются права администратора. В большинстве случаев для получения такого уровня доступа пользователя обманным путем склоняют к запуску этого ПО с нужными правами. (там же, ¶ 47) Для этого

вредоносное ПО маскируется под обновление программы, установленной на компьютере, и убеждает пользователя запустить мнимое «обновление» с правами администратора. (там же, ¶¶ 47-48) Получив возможность установки, ПО ZeroAccess вносит повреждающие изменения в операционную систему Windows и браузер Internet Explorer. (там же, ¶ 49) Оно создает скрытые каталоги, подменяет системные драйверы, необходимые операционной системе, внедряется в низкоуровневые процессы и вносит изменения в системный реестр — основное хранилище информации, необходимой для правильной работы компьютера. (там же, ¶ 49) Оно также внедряет свой код в процесс Internet Explorer, фактически превращая Internet Explorer во вредоносную программу, которая, хоть и сохраняет имя Internet Explorer, на самом деле уже является инструментом мошенничества. (там же, ¶ 49)

Одно из самых опасных изменений, выполняемых ZeroAccess при заражении компьютера — отключение его защитных средств: ослабление учетных данных и отключение служб безопасности Windows. (тем же, ¶¶ 50-52) Отключение этих служб позволяет ZeroAccess, помимо прочего, блокировать установку обновлений безопасности от Microsoft. Отключаются следующие службы Windows: служба базовой фильтрации, вспомогательная служба IP, служба брандмауэра Windows, служба защитника Windows, служба центра обеспечения безопасности Windows и служба автоматического обнаружения прокси. (там же, ¶ 50) Это особенно опасно, поскольку ZeroAccess непрерывно заставляет зараженный компьютер подключаться к веб-сайтам, откуда их может атаковать другое вредоносное ПО. Когда защитные средства Windows отключены, у компьютера практически не остается шансов избежать волн вторичного инфицирования, некоторые из которых исключительно опасны.

D. Архитектура ботнета ZeroAccess

1. ZeroAccess представляет собой всемирную сеть зараженных компьютеров с продуманной защитой от противодействия

В целом при проектировании и развертывании ZeroAccess Ответчиками использовалась так называемая одноранговая топология сети. (там же, ¶ 36) Такая архитектура используется для защиты от мер противодействия. (там же, ¶¶ 35-36) В одноранговой сети зараженные компьютеры-участники («узлы») постоянно связываются друг с другом и могут быстро и надежно передавать друг другу обновленную версию вредоносного ПО и новые указания. (там же, ¶ 36) Иными словами, в одноранговой сети любой из зараженных компьютеров может выполнять функцию контролирующего сервера. (там же, ¶ 36) Поэтому невозможно указать единую командную точку, отключение которой позволило бы нарушить работу всей сети. (там же, ¶¶ 36-37) Не так давно ботнет выдержал попытку своей нейтрализации со стороны крупной компании, занимающейся вопросами безопасности ПО, и быстро восстановился. (там же, ¶ 37) После этой попытки нейтрализации киберпреступники, стоящие за ZeroAccess, добавили в одноранговую сеть новые слои избыточности, сделав ее еще устойчивее к внешнему воздействию. (там же, ¶¶ 37, 53-54)

2. Ответчики контролируют ZeroAccess посредством 18 IP-адресов, расположенных в Европе

Не умаляя устойчивости одноранговой сети к внешнему воздействию, следует отметить, что принципиальная уязвимость архитектуры ZeroAccess состоит в том, что инфраструктура, контролирующая мошенничество со щелчками и перехват браузера, представляет собой довольно обособленный и сравнительно постоянный набор IP-адресов. Зараженные компьютеры одноранговой сети полагаются на отдельный список серверов, доступных по 18 IP-адресам, которые Ответчики арендуют у хостинговых

компаний в Латвии, Люксембурге, Швейцарии, Нидерландах и Германии. (там же, ¶¶ 55-56) Когда ZeroAccess впервые заражает компьютер, на нем еще нет файлов и модулей, необходимых для непосредственного совершения мошенничества со щелчками или перехвата браузера. (там же, ¶ 55) Такие файлы будут получены компьютером от первого узла одноранговой сети, с которым он вступает в контакт. (там же, ¶ 55) Каждый раз, когда один зараженный ZeroAccess компьютер подключается к другому, он помимо прочего запрашивает у него имеющиеся модули и файлы. (там же, ¶ 55) В числе полученных инфицированным ZeroAccess компьютером файлов имеется список IP-адресов серверов, которые не входят в одноранговую сеть, а выдают зараженному компьютеру непосредственные указания по совершению мошенничества со щелчками или перехвата браузера. (там же, ¶ 56) Этот список IP-адресов постепенно изменяется, но в данный момент имеется 18 адресов. (там же, ¶ 56) Эти «IP-адреса контроля мошенничества» приведены в приложении A. (там же, ¶ 56) Отключение этих адресов приведет к прекращению мошенничества со щелчками и перехвата поиска, подробнее описанного ниже. Далее, указанные IP-адреса связаны с 49 «доменами контроля мошенничества», которые, как считается, являются резервным механизмом (также перечислены в приложении A).

E. Ответчики используют ZeroAccess для мошенничества на рынке интернет-рекламы

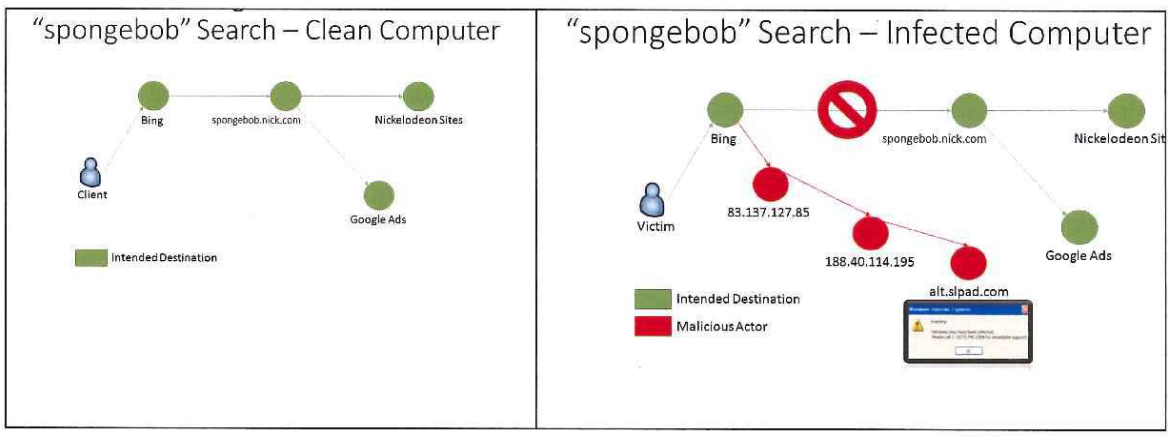
1. Мошенничество ZeroAccess с перехватом браузера

Один из основных видов мошенничества, осуществляемых Ответчиками посредством ZeroAccess, выступает перехват браузера. Принцип перехвата браузера состоит в следующем. Пользователь запускает браузер, например, Internet Explorer, и вводит в поисковую систему, например, Bing, Yahoo! или Google, какой-либо запрос.

(там же, ¶ 58) Поисковая система возвращает список результатов, пользователь просматривает ссылки и выбирает, какую щелкнуть. (там же, ¶ 58) Как только пользователь щелкнет ссылку, работающее на компьютере вредоносное ПО ZeroAccess перенаправляет браузер на сервер, расположенный по одному из IP-адресов контроля мошенничества, и передает этому серверу ключевые слова, использованные при поиске. (там же, ¶ 58) Получив эту информацию, контролирующий сервер перенаправляет компьютер пользователя на один из многочисленных веб-сайтов по выбору операторов ботнета, при пользователю кажется, что он использует поисковую систему Microsoft под торговой маркой Bing и браузер под торговой маркой Internet Explorer. (там же, ¶ 58) Ниже приведены примеры обманных схем, используемых Ответчиками при перехвате поиска с помощью ZeroAccess.

Ложная служба поддержки. Средства перехвата поиска ZeroAccess используются для вымогания у пользователей денег за мнимые услуги поддержки. Так, на рисунке 1 ниже показаны различные результаты поиска ключевого слова «spongebob» (мультипликационный персонаж) на «чистом» компьютере и на компьютере, зараженном ZeroAccess. (там же, ¶ 58)

Рис. 1



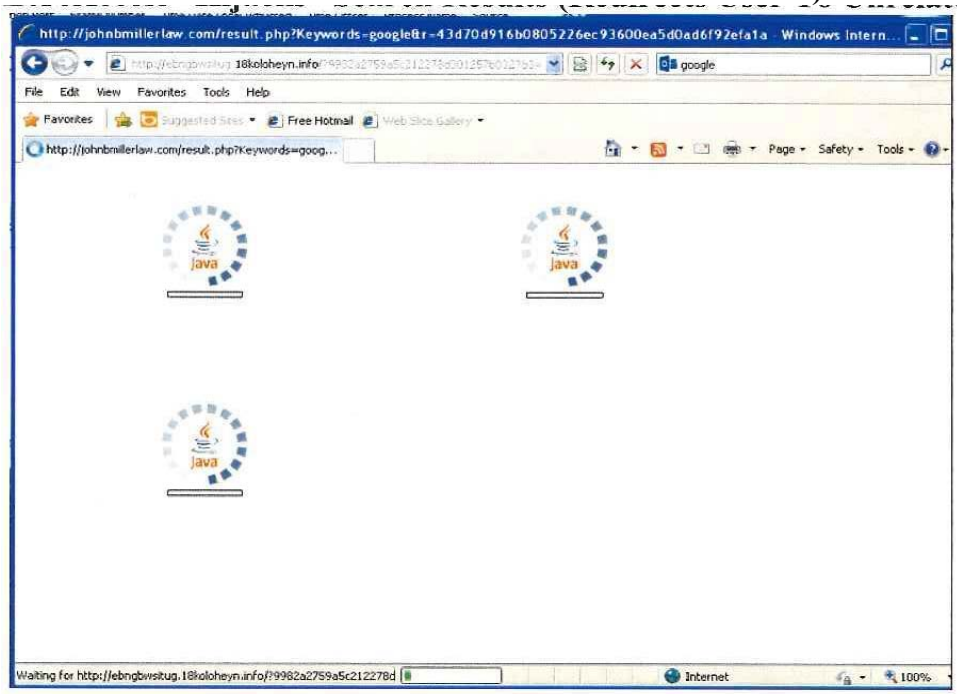
На «чистом» компьютере браузер подключается к веб-сайту «spongebob.nick.com» и загружает необходимую информацию с веб-сайтов Nickelodeon и объявления рекламной платформы Google. (там же, ¶ 58) На компьютере, зараженном ZeroAccess, браузер перехватывается и перенаправляется сначала на два безымянных IP-адреса в сети Интернет, а оттуда — на веб-сайт «alt.slpad.com». (там же, ¶ 58) В этот момент отображается сообщение об ошибке, сообщающее пользователю, что компьютер был заражен. Оно тоже является частью аферы. (там же, ¶ 58) Если пользователь позвонит по указанному номеру телефона, его попытаются убедить оплатить «очистку» компьютера. (там же, ¶ 58)

Ложный антивирус. Средства перехвата поиска ZeroAccess используются для предложения пользователю вредоносной программы, представляющей собой ложный антивирус, предназначенный для сбора информации о банковских картах. На рис. 2–4 ниже показана типичная схема такого мошенничества, выполняемая Ответчиками посредством ZeroAccess. (там же, ¶ 62) Пользователь выполняет поиск ключевого слова «Google» в поисковой системе Microsoft Bing. Bing возвращает правильные результаты, и пользователь щелкает первую ссылку, ожидая, что попадет на страницу Google. (там же, ¶ 62)

Рис. 2 – Начало поиска

Вместо того, чтобы открыть страницу Google.com, браузер подключается к набору несвязанных веб-сайтов:

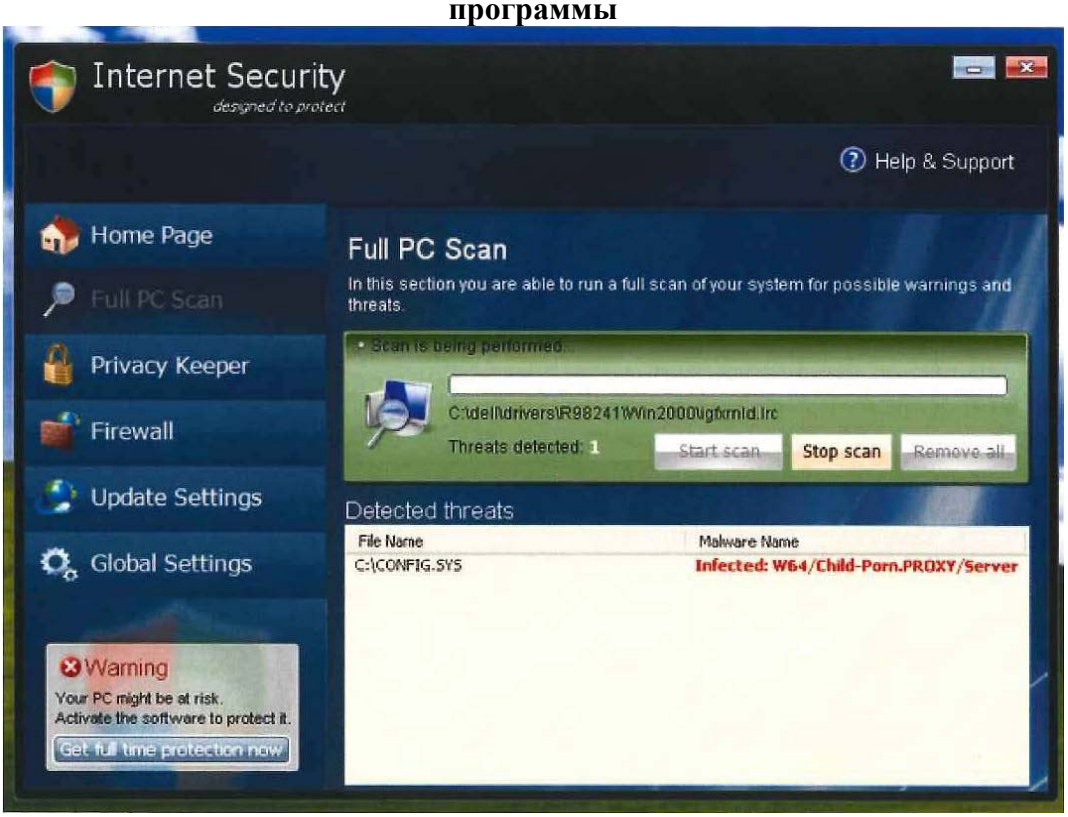
Рис. 3 – ZeroAccess «перехватывает» результаты поиска (перенаправляет пользователя на несвязанные веб-сайты)



Неожиданно на компьютере пользователя запускается вредоносное ПО с веб-сайта, на который ZeroAccess перенаправил компьютер. (там же, ¶ 62) Это вредоносное ПО имитирует проверку состояния защищенности компьютера (на самом деле никакой

проверки не выполняется), в ходе которой была найдена угроза, имеющая отношение к детской порнографии. (там же, Цель этого вредоносного ПО — вынудить пользователя щелкнуть кнопку «Получить круглосуточную защиту» в нижнем левом углу. (там же, ¶ 62) Обычно в итоге пользователю предлагается выполнить платеж по банковской карте, чтобы «получить круглосуточную защиту». (там же, ¶ 62) Тем временем компьютер фактически становится бесполезным, поскольку пользователь не может закрыть ложное сообщение о сканировании, не затратив значительного времени и сил. (там же, ¶ 62)

Рис. 4 – ZeroAccess направляет пользователя на веб-сайт фальшивой антивирусной программы



<u>Кража финансовой информации.</u> Средства перехвата поиска ZeroAccess также используются для направления пользователей на веб-сайты, поставляющие иной вредоносный код, предназначенный для перехвата учетных данных интернет-банкинга и кражи денежных средств. В частности, проведенное Microsoft расследование показало, что ZeroAccess перенаправляет пользователей на веб-сайты, с которых на их компьютеры

загружается вредоносное ПО «Zeus». (там же, ¶ 64) Zeus — это ботнет финансового мошенничества, который отслеживает действия владельца компьютера и крадет его банковскую информацию, в том числе учетные данные, номера счетов, остатки по счетам и пароли к системам интернет-банкинга. (там же, ¶ 64) Стоящие за Zeus преступники используют эти сведения для скрытного опустошения банковских счетов владельцев. (там же, ¶ 64) В декабре 2012 г. Microsoft и другие истцы, представляющие финансовую отрасль, добились вынесения заочного решения против операторов Zeus в процессе Microsoft Corp. et al. v. John Does 1-39 et al., Дело № 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.), что привело к отключению значительной части ботнета. (там же, ¶ 64) Несмотря на согласованность и успешность этих действий, отдельные ветви Zeus продолжают существовать, а операторы Zeus, со всей очевидностью, используют генерируемый ZeroAccess трафик для заражения новых компьютеров в попытке восстановить свою преступную сеть. (там же, ¶ 64)

2. Мошенничество ZeroAccess со щелчками

Вторая крупная незаконная деятельность, осуществляемая инфицированными ZeroAccess компьютерами — мошенничество со щелчками. (там же, ¶ 65) При включении зараженного ZeroAccess компьютера вредоносное ПО ZeroAccess подключается к одному или нескольким из 18 IP-адресов, приведенных в приложении A. (там же, ¶ 65) Компьютеры, расположенные по этим IP-адресам, передают зараженному ZeroAccess компьютеру список адресов веб-сайтов. (там же, ¶ 65) Когда зараженный ZeroAccess компьютер подключается к одну из веб-сайтов из этого списка, перехваченный браузер компьютера имитирует щелчок на рекламном объявлении этого веб-сайта. (там же, ¶ 65) Затем компьютер переходит к следующему веб-сайту из списка, и процесс повторяется. (там же, ¶ 65)

Схема мошенничества ZeroAccess опирается на то, что как правило рекламодатели в сети Интернет платят за каждый щелчок, и часть этой суммы выплачивается веб-сайту, на котором размещена реклама. На практике оператор веб-сайта платит Ответчикам за внесение его веб-сайта в список веб-сайтов, ежедневно посещаемых армией зараженных ZeroAccess компьютеров, либо Ответчики изначально контролируют такие веб-сайты и получают отчисления от рекламной сети. Затем зараженные компьютеры посещают эти веб-сайты и выполняют щелчки на рекламных объявлениях, что выглядит так, словно это реальные пользователи просматривали и щелкали объявления. Рекламодатели и компании, в том числе Microsoft, которые размещают объявления, платят оператору веб-сайта за фальшивые щелчки, думая, что они выполнены реальными посетителями.

F. ZeroAccess наносит прямой ущерб Microsoft и ее заказчикам

1. ZeroAccess наносит ущерб инфицированным компьютерам

Как было отмечено выше, вредоносное ПО ZeroAccess вносит деструктивные изменения в операционную систему Windows. (там же, ¶ 68) Оно создает скрытые каталоги, подменяет системные драйверы, необходимые операционной системе, внедряется в низкоуровневые процессы и вносит изменения в системный реестр — основное хранилище информации, необходимой для правильной работы компьютера. (там же, ¶ 68) Оно также отключает защитные средства зараженного компьютера, ослабляя учетные данные и отключая службы безопасности Windows, что делает компьютер уязвимым для вторичного заражения. (там же, ¶ 69) Отключаются служба базовой фильтрации, вспомогательная служба IP, служба брандмауэра Windows, служба защитника Windows, служба центра обеспечения безопасности Windows и служба автоматического обнаружения прокси. (там же, ¶ 69) Отключение этих служб позволяет ZeroAccess, помимо прочего, блокировать получение обновлений безопасности от

Microsoft. (там же, ¶ 69) Эти действия производятся без ведома и без одобрения конечного пользователя, поскольку ZeroAccess представляет собой фоновый процесс (то есть, он работает в фоне, не имеет пользовательского интерфейса и никак не сообщает владельцу компьютера о своем присутствии или работе). (там же, ¶ 69) Как упоминалось выше, тот факт, что ZeroAccess отключает защитные средства компьютера, представляет особую опасность в свете того, что ZeroAccess заставляет такой компьютер подключаться к различным веб-сайтам, на которых возможно вторичное заражение вредоносным ПО. (там же, ¶ 69) Далее, как упоминалось выше, ZeroAccess также внедряет свой код в процесс Internet Explorer, фактически превращая Internet Explorer во вредоносную программу, которая, хоть и сохраняет имя Internet Explorer, на самом деле уже является инструментом интернет-мошенничества, перехватывающим поисковые запросы пользователя. (там же, ¶ 70)

В результате упомянутых выше действий вычислительная мощность, память, каналы связи и другие ресурсы зараженного ZeroAccess компьютера будут в значительной степени использоваться для обработки, передачи данных и интернет-подключений, навязываемых ZeroAccess. (там же, ¶ 71) Пользователи сообщали о снижении производительности компьютеров, что было отнесено на счет вредоносного ПО ZeroAccess. (там же, ¶ 71)

Владельцы зараженных ZeroAccess компьютеров, как правило, не знают, что их компьютеры заражены и входят в ботнет ZeroAccess, или что их компьютеры скрытно участвуют в незаконных действиях. (там же, ¶ 72) Вредоносное ПО ZeroAccess проектировалось в расчете на скрытность. Пользователю, узнавшему, что на его компьютере неправомерно присутствует ZeroAccess, придется потратить значительное время и силы, чтобы удалить это вредоносное ПО. (там же, ¶ 72) С учетом способа,

которым ZeroAccess устанавливается в систему, неквалифицированная попытка его удаления может привести к неработоспособности браузера или компьютера. (там же, ¶ 72)

2. ZeroAccess наносит непоправимый ущерб Microsoft и ее бренду

ZeroAccess наносит Microsoft непоправимый ущерб, подрывая ее репутацию, бренды и отношение пользователей. (там же, ¶ 73) Microsoft поставляет операционную систему Windows, браузер Internet Explorer, поисковую систему Bing, рекламную платформу Bing Ads, службу электронной почты Hotmail и гамму других программных продуктов и услуг. (там же, ¶ 73) Microsoft вложила существенные средства в разработку продуктов и услуг высокого качества. (там же, ¶ 73) Благодаря высокому качеству и эффективности продуктов и услуг Microsoft, а также значительным средствам, потраченным Microsoft на продвижение этих продуктов и услуг, Microsoft сумела заслужить прочное доверие пользователей, создать стабильный бренд, превратить имя Microsoft и названия продуктов и услуг в прочные, узнаваемые по всему миру символы, хорошо известные на рынках. Microsoft обладает зарегистрированными товарными знаками, отражающими качество ее продуктов и услуг и прочность бренда, в том числе товарные знаки Windows, Internet Explorer и Bing. (там же, ¶ 73)

Действия ZeroAccess наносят ущерб Microsoft и ее репутации, бренду и доверию пользователей, поскольку пользователи, пострадавшие от негативных эффектов работы данных вредоносных приложений, ошибочно полагают, что источником проблем с их компьютером являются Microsoft, Windows, Internet Explorer, Bing или Bing Ads. (там же, ¶ 74) Так, из-за ZeroAccess пользователи получают менее релевантные и зачастую вредоносные результаты поиска, поскольку их браузер и поисковая система Bing перехватываются и перенаправляются на менее релевантные, опасные или

оскорбительные веб-сайты. (там же, ¶ 74) Имеется существенный риск того, что конечные пользователи отнесут эти проблемы на счет Microsoft, браузера Internet Explorer, поисковой системы Bing или платформы Bing Ads, чем будет нанесен значительный вред этим торговым маркам и брендам. (там же, ¶ 74)

Пользователи могут ошибочно отнести негативные проявления работы ботнета ZeroAccess и другого вредоносного ПО, загруженного на их компьютер в результате перехвата и перенаправления браузера на веб-сайты с вредоносным содержимым, на счет Microsoft, и часто так и поступают. (там же, ¶ 76) Кроме того, вернуть таких заказчиков было бы сложно, учитывая издержки, которые они несут при переходе на иную марку продуктов, и восприятие ими рисков. (там же, ¶ 76)

Microsoft выделяет значительные вычислительные и человеческие ресурсы на борьбу с ZeroAccess и другим вредоносным ПО и помощь заказчикам в определении того, заражен ли их компьютер, и если так, в его очистке. (там же, ¶ 77) Помимо выделения ресурсов на помощь конечным пользователям в борьбе с ZeroAccess, Microsoft также приходится расходовать средства на мониторинг своей платформы интернет-рекламы на предмет мошеннического трафика и щелчков, отфильтровывая их по возможности до того, как они нанесут вред, и выплачивая компенсации рекламодателям, если мошенничество было обнаружено позднее. (там же, ¶ 77) Указанные мероприятия требуют глубокого технического расследования и дорогостоящих действий по расчету и возмещению ущерба, нанесенного рекламодателям Microsoft. (там же, ¶ 77)

Неправомерная установка программного обеспечения ботнета ZeroAccess и другого вредоносного ПО на компьютеры пользователей наносит ущерб Microsoft и ее заказчикам. (там же, ¶ 78) Установка программного обеспечения ботнета путем введения пользователя в заблуждение является вмешательством и повреждением операционной

системы Microsoft Windows, выполненным без разрешения Microsoft. (там же, ¶ 78) Операционная система Windows лицензируется Microsoft для использования своими заказчиками. (там же, ¶ 78)

3. ZeroAccess наносит ущерб рекламной платформе Microsoft и заказчикам, которые ее используют

a. ZeroAccess вынуждает рекламодателей платформы Microsoft оплачивать мошеннические щелчки

Деятельность ZeroAccess также негативно сказывается на рекламодателях, использующих платформу Microsoft, других рекламодателей и владельцев веб-сайтов, которые законным образом приобретают у таких поставщиков, как Bing Ads, средства повышения целевого трафика своего веб-сайта. (там же, ¶ 79) Рекламодатели (лица, создающие рекламные объявления для своей компании) размещают рекламу на определенных веб-страницах или связывают свои объявления с определенными ключевыми словами поисковой системы, так, что конечный пользователь, выполняющий поиск по нужным ключевым словам, может посетить веб-сайт рекламодателя. (там же, ¶ 79) ZeroAccess и подобное ему вредоносное ПО существенно искажают эти взаимоотношения. Выполняя не запрошенные пользователем щелчки и посещения веб-страниц, ZeroAccess повышает трафик веб-сайта рекламодателя, но этот трафик никак не способствует повышению продаж. (там же, ¶ 79) Рекламодатель оплачивает услуги рекламной сети по количеству щелчков, но фактически платит за трафик, который не имеет практический пользы. (там же, ¶ 79) Microsoft приходится непрерывно отслеживать мошеннические щелчки и возмещать их стоимость, что создает дополнительные издержки и подрывает отношения с заказчиками.

b. ZeroAccess вмешивается в выдачу результатов рекламодателей в платформе Microsoft

Рекламодатели Bing оплачивают размещение рекламы в поисковых результатах Bing. (там же, ¶ 80) Однако, ZeroAccess изменяет результаты, представляемые на компьютере пользователя. (там же, ¶ 80) Рекламодатель не оплачивает лишний щелчок Bing, потому что щелчка по его ссылке не было, но вред рекламодателю тем не менее наносится: его объявление из-за отсутствия щелчков понижается в релевантности (поскольку ZeroAccess уводит пользователей от ожидаемых результатов выдачи Bing). (там же, ¶ 80) В результате рекламодателям Microsoft становится сложнее увидеть свои объявления в выдаче по поисковым запросам в будущем. (там же, ¶ 80) Это форма нанесения ущерба репутации. (там же, ¶ 80) Имеется существенный риск того, что рекламодатели отнесут эти проблемы на счет поисковой системы Bing или платформы Bing Ads, чем будет нанесен значительный вред этим торговым маркам и брендам. (там же, ¶ 81)

G. Блокировка связи между зараженными компьютерами и IP-адресами и доменами контроля мошенничества — ЕДИНСТВЕННЫЙ способ воздействия на ZeroAccess

В структуру ботнета ZeroAccess заложена устойчивость к техническим средствам борьбы с ним, что не позволяет легко прекратить наносимый им ущерб. (там же, ¶ 82) Особенно ярким свидетельством этого является одноранговая топология (отсутствие центра контроля, который можно было бы отключить), основное назначение которой — противодействие мерам, направленным на прекращение ущерба, наносимого ботнетом, и обеспечение его роста. (там же, ¶ 82) Далее, Ответчики запрограммировали ZeroAccess на отключение обычных средств безопасности Windows при заражении компьютера, а сами

файлы вредоносного ПО зашифрованы. (там же, ¶ 82) Эти меры исключают использование обычных технических средств борьбы с угрозой.

Однако, действия ботнета могут быть нарушены путем прекращения связи между зараженными ZeroAccess компьютерами и IP-адресами контроля мошенничества и доменами контроля мошенничества, перечисленными в приложении А, от которых такие зараженные компьютеры получают указания по выполнению перехвата браузера и мошенничества со щелчками. (там же, ¶ 83)

Поэтапные запросы на фильтрацию трафика к IP-адресам и доменам контроля мошенничества, неформальное разрешение спора или уведомление Ответчиков до фильтрации трафика были бы недостаточны для прекращения вреда. (там же, ¶ 84) Операторы ботнета ZeroAccess немедленно предприняли бы меры по защите ботнета, если бы знали о действиях со стороны Microsoft. К примеру, они могли бы ввести в использование новые IP-адреса и указать зараженным компьютерам использовать их для получения дальнейших инструкций. (там же, ¶ 84)

Известны прецеденты, когда аналитики безопасности или правительственные агентства пытались прекратить вред, наносимый ботнетами, при этом позволяя операторам ботнета получить соответствующее уведомление. (там же, ¶ 85) В таких случаях операторы ботнета немедленно переводили инфраструктуру ботнета в новые, неустановленные участки сети Интернет, и принимали иные меры, позволяющие ботнету продолжать функционировать и приводящие к уничтожению или сокрытию свидетельств его работы. (там же, ¶ 85) Так, когда крупная поставщик услуг безопасности попытался нейтрализовать ZeroAccess, киберпреступники, управляющие ZeroAccess, быстро распространили обновление, позволившее ботнету продолжить свою работу. (там же, ¶ 85)

Учитывая архитектуру ботнета ZeroAccess и использование IP-адресов контроля мошенничества для связи с зараженными компьютерами и управления ими, операторы ZeroAccess, в случае получения ими уведомления о грядущем отключении этих IP-адресов, распространят на зараженные компьютеры новый список, состоящий из других IP-адресов контроля, и уничтожат свидетельства работы ботнета и нужные улики на зараженных компьютерах пользователей. (там же, ¶ 86)

Единственный способ прекратить вред, наносимый Microsoft, ее заказчикам и обществу — пресечь распространение компьютерами, расположенными по IP-адресам контроля мошенничества, инструкций компьютерам, зараженным ZeroAccess, и перенаправить соответствующие домены контроля мошенничества на безопасные серверы. Эта мера позволит в значительной степени нарушить текущее управление компьютерами, зараженными ZeroAccess, и поставщики услуг Интернета, у которых обслуживаются пользователи зараженных компьютеров, смогут уведомить тех о факте заражения и содействовать в восстановлении нормальной работы компьютеров, тем самым выводя компьютеры из состава ботнета ZeroAccess. (там же, ¶ 82)

III. ЮРИДИЧЕСКИЕ ДОВОДЫ

Microsoft испрашивает односторонний ВЗСП и предварительный судебный запрет в рамках федеральных правил гражданского судопроизводства 65(b), закона Ленхема, 15 U.S.C. § 1116(a), закона о вынесении судебных приказов, 28 U.S.C. § 1651 и общей правомочности суда для прекращения вреда, сохранения статус-кво и обеспечения сохранности свидетельств деятельности Ответчиков на время рассмотрения этого дела. Ниже приводятся доводы в пользу обоснованности меры, испрашиваемой Microsoft.

A. Односторонний ВЗСП и предварительный судебный запрет, блокирующий IP-адреса контроля мошенничества, с которых ведется управление ботнетом ZeroAccess, является обоснованным

ВЗСП или предварительный судебный запрет принимается, если податель ходатайства покажет, что: (1) имеются все шансы выиграть дело по существу; (2) в случае отказа в предварительной судебной защите будет нанесен непоправимый ущерб; (3) сравнение степени ущерба свидетельствует в пользу принятия запретительной меры; и (4) запретительная мера послужит интересам общества. См. Winter v. Natural Res. Def Council, Inc., 555 U.S. 7, 19-23 (2008); Dennis Melancon, Inc. v. City of New Orleans, 703 F.3d 262, 268 (5th Cir. 2012).

Microsoft имеет все шансы выиграть дело по существу. Вторжение Ответчиков в защищенные компьютеры, мошенничество и вводящее в заблуждение использование брендов Microsoft нарушают закон о компьютерном мошенничестве и злоупотреблении, закон об охране права на электронную связь и закон Ленхема. Кроме того, это вводящее в заблуждение вредоносное мошенническое деяние, нарушающее законы Техаса. Microsoft, ее заказчикам и обществу будет наноситься непоправимый ущерб, если ботнет ZeroAccess продолжит работу в обычном режиме.

Напротив, принятие ВЗСП и предварительного судебного запрета, испрашиваемого Microsoft, не нанесет ущерба никаким законным интересам Ответчиков. Назначение ботнета ZeroAccess состоит в выполнении незаконных действий. Любые третьи стороны (поставщики услуг Интернета, компании хостинга IP-адресов, регистраторы доменов) будут затронуты пренебрежимо малым и кратковременным образом. Кроме того, в пользу принятия запрета свидетельствует общественный интерес, поскольку вред, наносимый ботнетом Microsoft и ее заказчикам, одновременно наносится

многим пользователям компьютеров и компаниям в США. В связи с вышеуказанным, испрашиваемая Microsoft мера является обоснованной.

1. Microsoft имеет все шансы выиграть дело по существу каждого из положений иска

Microsoft имеет все шансы выиграть дело по существу искового заявления, и потому ходатайство о ВЗСП и предварительном судебном запрете должно быть удовлетворено. Иск содержит следующие заявления в части законного и общего права: (1) нарушение закона о компьютерном мошенничестве и злоупотреблении (18 U.S.C. § 1030), (2) нарушение закона об охране права на электронную связь (18 U.S.C. § 2701), (3) нарушение прав на торговую марку в соответствии с законом Ленхема (15 U.S.C. § 1114), (4) обманное раскрытие происхождения в соответствии с законом Ленхема (15 U.S.C. § 1125(a)), (5) подрыв торговой марки в соответствии с законом Ленхема (15 U.S.C. 1125(c)), (6) посягательство на имущество, (7) присвоение имущества и (8) необоснованное обогащение.

a. Ответчики нарушают закон о компьютерном мошенничестве и злоупотреблении

Закон о компьютерном мошенничестве и злоупотреблении («CFAA»), в числе прочего, предусматривает следующий состав преступления:

- умышленный несанкционированный доступ к охраняемому компьютеру,[3] приведший к нанесению ущерба. 18 U.S.C. § 1030(a)(5)(C);

[3] «Охраняемые компьютеры» — это компьютеры, «которые используется в междуштатной или межгосударственной торговле или связи либо способны оказывать влияние на них, в том числе компьютеры, находящиеся за пределами Соединенных Штатов, характер использования которых позволяет им оказывать влияние на междуштатную или межгосударственную торговлю или связь Соединенных Штатов». 18 U.S.C. § 1030(e)(2)(B).

- умышленный несанкционированный или с превышением назначенных полномочий доступ к компьютеру, приведший к получению информации с охраняемого компьютера. (18 U.S.C. § 1030(a)(2)(C));
- умышленная передача программы, информации, кода или команды, приведшая к умышленному несанкционированному нанесению ущерба охраняемому компьютеру. (18 U.S.C. § 1030(a)(5)(A)).

Находящаяся в собственности Microsoft операционная система Windows, компьютеры заказчиков, на которых она работает, и серверы Microsoft рекламной платформы Bing Ads являются «охраняемыми компьютерами» в соответствии с CFAA. Ответчики умышленно осуществляют несанкционированный доступ к находящейся в собственности Microsoft операционной системе и к компьютерам заказчиков Microsoft, обременяя эти компьютеры путем заражения их вредоносных кодом и самовольного выполнения этого кода. Ответчики умышленно осуществляют доступ к серверам Microsoft Bing Ads, генерируя направленный к ним мошеннический трафик сети Интернет.

Умышленный и несанкционированный доступ к охраняемым компьютерам Microsoft и ее заказчиков со стороны ZeroAccess, кроме того, привел к существенному ущербу и потерям, включая издержки по расследованию случаев несанкционированного доступа. Материалы, прилагаемые к настоящему ходатайству, доказывают, что такой несанкционированный доступ нанес ущерб Microsoft и ее заказчикам. Внедрение вредоносного ПО ZeroAccess, выполнение вредоносного кода и являющийся результатом этого перехват действий компьютера пользователя снижает производительность компьютеров Microsoft и ее заказчиков. Microsoft приходится выделять время и ресурсы на борьбу с заражением компьютеров пользователей, вызванным ботнетом ZeroAccess.

Несанкционированный доступ ZeroAccess в точности подпадает под положения закона о компьютерном мошенничестве и злоупотреблении. См. напр. United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (указывается, что CFAA предусматривает «проникновение на компьютер извне») (цитаты из истории принятия опущены); см. также Physicians Interactive v. Lathian Sys., Inc., 1:03-cv-01193, 2003 U.S. Dist. LEXIS 22868, at *26 (E.D. Va. Dec. 5, 2003) (издан ВЗСП и судебный запрет в соответствии с CFAA, где ответчик проник на компьютер и похитил конфиденциальную информацию), частично аннулированный по другим основаниям, как указано в деле ForceX, Inc. v. Tech. Fusion, LLC, 2011 U.S. Dist. LEXIS 69454, at * 12 (E.D. Va. June 27, 2011); Global Policy Partners, LLC v. Yessin, 1:09-cv-00859, 2009 U.S. Dist. LEXIS 112472, *9-13 (E.D. Va. Nov. 24, 2009) (доступ к компьютеру с использованием учетных данных, не принадлежащих ответчику, подпадает под положения CFAA)[4].

Далее, как обременение серверов Microsoft Bing Ads искусственными щелчками, так и нанесение урона репутации Microsoft среди рекламодателей является ущербом, предусматриваемым CFAA. См. напр. White Buffalo Ventures, LLC v. Univ. of Texas, 420 F.3d 366, 377 (5th Cir. 2005) (указывается, что фактическое свидетельство нарушения работы сервера может быть достаточным основанием для подачи иска о возмещении убытков в рамках CFAA); Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) (CFAA может применяться, если ответчик покажет «наличие любых обоснованных издержек, возникших у любого потерпевшего, в том числе издержки по реагированию на посягательство, по проведению оценки ущерба и по восстановлению данных, программ, систем или информации до состояния, в котором они находились до

[4] Так, в последние годы операторы ботнетов, распространяющие код, используемый для вторжения в компьютеры пользователей, сбора личной информации и нанесения ущерба, признавались виновными и осуждались в соответствии с законом о компьютерном мошенничестве и злоупотреблении. См. Heath Decl., Exs. 12 и 13 (обвинительный акт Jeanson James Ancheta), 15 (вынесение приговора Jeanson James Ancheta).

посягательства, а также упущенная выгода, понесенные издержки или иной ущерб, являющийся следствием прекращения обслуживания») (цитата опущена); America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (несанкционированный доступ ответчика к серверам истца нарушает CFAA); Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (то же). Следовательно, Microsoft имеет все шансы выиграть дело по существу в части заявки о нарушении закона о компьютерном мошенничестве и злоупотреблении.

b. Закон об охране права на электронную связь

Закон об охране права на электронную связь запрещает «умышленный несанкционированный доступ к средствам осуществления электронной связи» и такой доступ с превышением полномочий, используемый для получения, изменения или изъятия из санкционированного доступа электронного сообщения, находящегося в электронном хранилище. 18 U.S.C. § 2701(a). Серверы Microsoft и лицензированная операционная система Windows, браузер Internet Explorer и страницы поисковой система Bing, доступные конечным пользователям, представляют собой средства осуществления электронной связи.

Вредоносное ПО ZeroAccess несанкционированно устанавливается на зараженных компьютерах конечных пользователей и собирает личную информацию без их ведома и согласия, включая поисковые запросы пользователя, ключевые слова и результаты поиска, возвращенные поисковой системой Microsoft Bing. В частности. вредоносное ПО ZeroAccess перехватывает ввод пользователя в строку поиска и текст результата поиска, возвращенный Bing, и использует эту информацию для перенаправления зараженного компьютера пользователя на веб-сайты по выбору Ответчиков. Эти поисковые запросы, ключевые слова и результаты поиска временно сохраняются на компьютере пользователя

в браузере Internet Explorer и веб-странице поисковой системы Bing. Подобное несанкционированное получение сохраненной электронной информации является нарушением закона об охране права на электронную связь. См. e.g. Lopez v. Pena, 2:12-cv-00165, 2013 U.S. Dist. LEXIS 30299, at *7 (N.D. Tex. Mar. 5, 2013) (указывается, что несанкционированный доступ к хранимой электронной коммуникации подпадает под действие ECPA). Следовательно, Microsoft имеет все шансы выиграть дело по существу в части заявки о нарушении закона об охране права на электронную связь.

c. <u>Нарушение Ответчиками закона Ленхема</u>

Статья 1114(1) закона Ленхема запрещает использование репродукции, подделки, копии или «вводящей в заблуждении имитации» зарегистрированного товарного знака при распространении товаров и услуг, где такое использование может привести к замешательству, ошибке или введению в заблуждение. Ботнет ZeroAccess создает и распространяет копии зарегистрированных и широко узнаваемых товарных знаков Microsoft в рамках подложных, искаженных версий браузера под торговым знаком Microsoft Internet Explorer и веб-страниц под торговым знаком Microsoft Bing, а также мошеннических веб-сайтов, снабженных торговыми знаками Microsoft. Эти неправомочные копии товарных знаков Microsoft вводят жертв в заблуждение, в результате чего те относят указанные неблаговидные действия на счет Microsoft. Это явное нарушение закона Ленхема, и Microsoft имеет все шансы выиграть дело по существу. См. напр. Microsoft Corp. v. Software Wholesale Club, Inc., 129 F. Supp. 2d 995, 1006 (S.D. Tex. 2000) (решение в рамках упрощенного делопроизводства, где ответчик использовал вводившие в заблуждение поддельные товарных знаки Microsoft); Choice Hotels Int'l, Inc. v. Patel, 6:12-cv-00023, 2013 U.S. Dist. LEXIS 55345, at *12-14 (S.D. Tex.

Apr. 16, 2013) (рассмотрение понятия путаницы, указание на презумпцию путаницы при использовании идентичных знаков).

Закон Ленхема также запрещает использование товарного знака, обманное раскрытие происхождения, обманное раскрытие фактов или вводящую в заблуждение интерпретацию фактов, которые:

> с высокой долей вероятности могут привести к замешательству, ошибочному выбору, созданию ложного впечатления о наличии связи такого лица с другим лицом, либо о происхождении, спонсировании или одобрении товаров, услуг или коммерческой деятельности такого лица другим лицом.

15 U.S.C. § 1125(a)(1)(A).

Ботнет ZeroAccess вводящим в заблуждение образом связывает широко узнаваемые товарные знаки Microsoft®, Windows®, Internet Explorer® и Bing® с вредоносной деятельностью, выполняемой на компьютерах пользователей посредством ненадлежащего использования операционной системы Microsoft Windows. В частности, на зараженных ZeroAccess компьютерах конечных пользователей выполняется перехват веб-сеансов браузеров Internet Explorer и перехват результатов поиска в системе Bing и перенаправление на другие результаты и веб-сайты, а также наблюдается вызванное ZeroAccess снижение производительности. Рекламодатели Microsoft получают ложное представление о ценности и эффективности рекламных кампаний, проводимых на платформе Bing Ads. Указанные деяния вводят в заблуждение относительно связи Microsoft с наблюдаемой активностью и создают ложное впечатление, что Microsoft является ее источником, в то время как это не так. Это явное нарушение закона Ленхема, § 1125(a), и Microsoft имеет все шансы выиграть дело по существу. Microsoft Corp., 129 F. Supp. 2d at 1006.

Закон Ленхема также предписывает, что владелец известного, узнаваемого товарного знака «имеет право на запретительное решение в отношении другого лица», которое использует такой товарный знак способом, «который с высокой долей вероятности может привести к ослаблению известного товарного знака путем размытия или путем порчи репутации...». 15 U.S.C. § 1125(c)(1). Здесь ботнет ZeroAccess ненадлежащим образом использует узнаваемые товарные знаки Microsoft при совершении вредоносных действий, направленных на заказчиков Microsoft и общество, чем ослабляет эти товарные знаки путем порчи репутации и путем размытия восприятия этих товарных знаков клиентами. Это также явное нарушение закона Ленхема, § 1125(c), и Microsoft имеет все шансы выиграть дело по существу. См. напр. MetroPCS Wireless, Inc. v. Virgin Mobile USA, L.P., 3:08-cv-01658, 2009 U.S. Dist. LEXIS 88527, at * 39 (N.O. Tex. Sept. 25, 2009) («Порча репутации возникает, когда товарный знак связывается с продуктами низкого качества, либо изображается в нездоровом или отталкивающем контексте, результатом чего является ассоциирование обществом недостатка качества или престижа в товарах ответчика с товарами истца»).

d. <u>Присвоение</u>

Присвоение определяется как противоправное распоряжение чужим имуществом, идущее вразрез с правами владельца. Green Int'l Inc. v. Solis, 951 S.W.2d 384, 391 (Tex. 1997). Здесь несанкционированная установка программного обеспечения и последующий контроль лицензированной операционной системы Microsoft Windows, браузера Internet Explorer, страниц поисковой системы Bing и компьютеров потребителей идет вразрез с интересами и наносит ущерб этой собственности. Таким образом, данное деяние является незаконным посягательством и присвоением. См. Sw. Bell Tel. Co. v. Iverson, 3:11-cv-02009, 2012 U.S. Dist. LEXIS 26678, at *2 (N.D. Tex. Feb. 6, 2012) (ссылки на

несанкционированный сбор электронных данных достаточно для заявления о посягательстве и присвоении); см. также Kremen v. Cohen, 337 F.3d 1024, 1034 (9th Cir. 2003) (признано, что проникновение в компьютерную систему и повреждение данных дает основание для заявлении о присвоении); Physicians Interactive, 2003 U.S. Dist. LEXIS 22868, at *26 (издан ВЗСП и судебный запрет, где ответчик проникал в компьютеры и получал проприетарную информацию, решение: «представляется вероятным, что две предполагаемые атаки, прослеженные [Истцом] до Ответчиков, были направлены на манипуляцию с частной собственностью, находящейся в законном обладании Истца.»); Washington v. Riley, 846 P.2d 1365, 1371 (Wash. 1993) («хакерская деятельность» ответчика признана «посягательством на компьютер» в соответствии с законами Вашингтона).

e. <u>Посягательство на имущество</u>

В соответствии с законами Техаса, посягательством называется вмешательство в посессорные интересы, связанные с частной собственностью. См. напр. Carpenter v. Carpenter, 2012 Tex. App. LEXIS 5322, at *11-12 (Tex. App. 2012). Умышленное противоправное деяние, нарушающее на значительный период времени использование собственником своего имущества, является посягательством. Там же у № 11 (цитата опущена). Несанкционированный доступ к компьютерной системе или сети также может являться посягательством. См. напр. Axis Surplus Ins. Co. v. Mitsubishi Caterpillar Forklift America Inc., 2011 U.S. Dist. LEXIS 148243, at * 2-3 (S.D. Tex. Dec. 27, 2011) (рассмотрение значимого вердикта жюри в пользу истца по жалобе на несанкционированный доступ к компьютерной сети истца, в том числе жалоба о посягательстве на имущество); см. также White Buffalo Ventures, 420 F.3d at 377 n.1 (рассмотрение случаев «цифрового посягательства» с той точки зрения, что

несанкционированный доступ к компьютерной системе или сети является посягательством на имущество). Здесь, санкционированное вмешательство ответчиков в серверы Microsoft Bing Ads путем направления к ним мошеннических щелчков наносит ущерб собственности Microsoft и является посягательством на имущество. White Buffalo Ventures, 420 F.3d at 377 n.1; см. также Sw. Bell Tel. Co. v. Iverson, 2012 U.S. Dist. LEXIS 26678, at *2 (рекомендовано отказать, в числе прочего, в отклонении жалобы на посягательство на имущество в деле о сборе данных в сети истца); America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) (лица, рассылавшие спам по электронной почте, совершили посягательство на имущество, когда «вошли в контакт с компьютерной сетью [истца]... и... нанесли ущерб репутации бизнеса [истца] и ценности его посессорных интересов в этой компьютерной сети».).

f. Необоснованное обогащение

Согласно положениям о необоснованном обогащении, лицо может требовать возмещения, если другое лицо получило от него выгоду путем мошенничества, принуждения или неправомерного преимущества. Heldenfels Bros. v. Corpus Christi, 832 S.W.2d 39, 41 (Tex. 1992). Здесь, Ответчики, не имея на то разрешения, получили выгоду от серверов Microsoft, ее сетей, лицензированной операционной системы Windows, браузера Internet Explorer и поисковой системы Bing, а также компьютеров заказчиков Microsoft. Ответчики достигли этого, заразив эти компьютеры и заставив их отправлять перехваченные веб-сеансы браузера Internet Explorer и результаты поисковой системы Bing для использования в мошенничестве со щелчками. Ответчики получали доход от этой деятельности, в том числе путем направления мошеннического трафика к платформе Microsoft Bing Ads. Таким образом, этот доход Ответчиков не может быть признан обоснованным. Microsoft имеет все шансы выиграть дело по существу.

2. ВЗСП и предварительный судебный запрет необходимы для прекращения непоправимого ущерба

Работа ботнета ZeroAccess наносит непоправимый ущерб Microsoft, ее заказчикам и обществу. Никакие денежные компенсации не смогут исправить вред, который непрерывная деятельность ZeroAccess по мошенничеству со щелчками и перехвату браузера наносит Microsoft и ее заказчикам. Федеральные суды при рассмотрении гражданских дел, касающихся ботнетов, заключали, что «прямой и непоправимый ущерб» потребителям со стороны управляющих серверов, шпионского ПО вирусов, троянских программ и фишинговых веб-сайтов, а также действия по настройке, развертыванию и управлению ботнетом являются достаточным основанием для выдачи одностороннего ВЗСП и предварительного судебного запрета. (См. Heath Decl. Ex. 22 (Microsoft Corp. v. Peng Yong et al., Дело № 1:12-cv-1004-GBL (E.D. Va. 2012) (Lee, J.) (односторонний ВЗСП и предварительный судебный запрет с целью блокировки серверов управления); Exs. 18 and 19 (Microsoft v. Piatti, et al., Дело № 1:11-cv-1017 (E.D. Va. 2011) (Cacheris, J.) (то же); Exs. 14 and 15 (Microsoft Corporation v. John Does 1-27, Дело № 1:10-cv-156 (E.D. Va., Brinkema J.) (то же); Exs. 16 and 17 (Microsoft v. John Does 1-11, Дело № 2:11-cv-00222 (W.D. Wa. 2011) (Robart, J.) (то же); Exs. 20 and 21 (Microsoft Corp. et al. v. John Does 1-39 et al., Дело № 12-cv-1335 (E.D.N.Y. 2012) (Johnson, J.) (то же); Exs. 10 & 11 (FTC v. Pricewert LLC et al., Дело № 09-2407 (N.D. Cal. 2009) (Whyte J.) (односторонний ВЗСП и предварительный судебный запрет с целью прекращения обслуживания компании, выполняющей хостинг ботнета). В частности, окружные суды в делах, поданных к рассмотрению Microsoft, признавали непоправимость ущерба, который ботнеты наносят Microsoft, ее заказчикам и пользователям сети Интернет в целом. (Heath Decl. at Exs. 14-22.)

Ботнет ZeroAccess наносит непоправимый ущерб как Microsoft, так и обществу. По этим причинам вынесение одностороннего ВЗСП, направленного на отключение управляющих серверов мошенничества со щелчками и перехвата браузера ZeroAccess, а также приказа о предоставлении обоснования того, что предварительный судебный запрет не должен быть наложен, является обоснованным. Непоправимость ущерба для Microsoft состоит в том, что перехват браузера, снижение производительности зараженного компьютера конечного пользователя и искажение рекламной среды сети Интернет, выполняемые ZeroAccess, воспринимаются пользователями как характеристики продуктов Microsoft — в частности, услуг и продуктов Microsoft Internet Explorer, Bing и Bing Ads. Заказчики Microsoft могут перейти на другие платформы, продукты и услуги, считая, что проблемы в работе компьютера вызваны Microsoft. После такого перехода имеется очень значительный риск того, что заказчик больше не вернется к продуктам Microsoft, особенно с учетом сомнений в их качестве, вызванных ботнетом, и высокой стоимости перехода на другую платформу. По мере роста ботнета и заражения компьютеров новым вредоносным ПО с помощью перехвата браузера ущерб становится кумулятивным. Такой вид нанесения ущерба репутации и пользователю с очевидностью является непоправимым, что и служит основанием для удовлетворения ходатайства. См. напр. Petro Franchise Sys., LLC v. All Am. Props., Inc., 607 F. Supp. 2d 781, 795 (W.D. Tex. 2009) (потеря контроля над репутацией в глазах потребителей является непоправимым ущербом). Ущерб является непоправимым, поскольку потребители в основной массе не обладают техническими знаниями и навыками, необходимыми для исправления зараженного компьютера и содействия прекращению роста ботнета.

В отсутствие испрашиваемых мер заказчики Microsoft будут находиться под постоянной угрозой передачи своих компьютеров под управление серверов Ответчиков,

координирующих мошенничество со щелчками и перехват браузера, а также несанкционированного проникновения и злоупотребления. В долгосрочном периоде вред такого рода составляет непоправимый ущерб, являющийся основанием для вынесения испрашиваемого решения. См. Arminius Schleifmittel GmbH v. Design Indus., Inc., 1:06-cv-00644, 2007 U.S. Dist. LEXIS 10847, at *22 (M.D.N.C. Feb. 15, 2007) (ущерб признан непоправимым, так как действия ответчиков «имеют значительные и непрерывные долгосрочные последствия».)

3. Сравнение степени ущерба прямо свидетельствует в пользу Microsoft

Принятие одностороннего ВЗСП и предварительного судебного запрета не нанесет ущерба никаким законным интересам Ответчиков, поскольку будет представлять собой лишь сохранение статус-кво. Отключение управляющих серверов ZeroAccess позволит временно прекратить распространение ботнета на новые компьютеры и сохранить свидетельства структуры ботнета и его незаконной деятельности. В случае принятия ВЗСП и предварительного судебного запрета Ответчики не понесут ущерба, поскольку IP-адреса контроля мошенничества служат исключительно незаконным целям. Поэтому Ответчики не понесут ущерба при сохранении статус-кво для последующего рассмотрения дела в суде. См. напр. Pesch v. First City Bank of Dallas, 637 F. Supp. 1539, 1543 (N.D. Tex. 1986) (сравнение степени ущерба ясно свидетельствует в пользу запрета, если запрещаемые действия незаконны).

Третьи стороны (поставщики услуг Интернета, компании хостинга, регистраторы доменов) также будут затронуты пренебрежимо малым образом, поскольку испрашиваемая мера направлена только против IP-адресов, используемых ботнетом, и предписывает указанным третьим сторонам предпринять несложные шаги по блокировке

этих IP-адресов и сохранению улик. Шаги, предписанные этим третьим сторонам, являются частью их обычного ведения дел, и в точности такое содействие с их стороны неоднократно запрашивалось ранее в делах о вредоносной деятельности в сети Интернет. Ограниченное сотрудничество со стороны поставщиков услуг Интернета, компаний хостинга и регистраторов доменов необходимо для обеспечения выполнения испрашиваемого приказа и разрешается в соответствии с законом о вынесении судебных приказов, 28 U.S.C. § 1651. И напротив, если ВЗСП и предварительный судебный запрет не будут приняты, ботнет ZeroAccess продолжит наносить непоправимый ущерб Microsoft, ее заказчикам и обществу. Указанный ботнет уже состоит из миллионов скомпрометированных компьютеров пользователей. Ежедневно происходит заражение новых компьютеров, что значительно повышает возможности ботнета по выполнению незаконных действий и приводит к росту вреда, наносимого Microsoft и обществу.

Коротко говоря, поддержание статус-кво путем блокировки доступа к серверам ZeroAccess, используемым Ответчиками для управления мошенничеством со щелчками и перехвата браузера, не нанесет ущерба законным интересам Ответчиков. Microsoft добивается очень адресного сотрудничества со стороны поставщиков услуг Интернета, компаний хостинга и регистраторов домена, направленного на прекращение использования Ответчиками инфраструктуры третьих сторон для совершения незаконных действий. Испрашивая мера имеет пренебрежительно малый эффект на возможные законные интересы других третьих сторон. Если, однако, ботнет продолжит наносить ущерб Microsoft и обществу, пока идет рассмотрение дела, многие законные интересы окажутся под серьезной угрозой.

4. Принятие ВЗСП и предварительного судебного запрета соответствует интересам общества

Сложно переоценить важность принятия ВЗСП и предварительного судебного запрета для защиты интересов общества помимо интересов Microsoft и ее заказчиков. Каждый потребитель, имеющий доступ к платформе электронной почты и сети Интернет, находится под угрозой нанесения ущерба со стороны ботнета ZeroAccess. Аналогично, каждая компания, оказывающая законные услуги по рекламе и оплачивающая законные рекламные объявления в сети Интернет, находится под угрозой мошенничества со щелчками со стороны ZeroAccess. Так, имеется явные доказательства того, что ZeroAccess нацелен на работу не только в сетях Microsoft, но и в сетях таких компаний, как Google, Yahoo! и Apple. Далее, ZeroAccess продвигает веб-сайты, содержащие контрафактное программное обеспечение, в том числе вредоносное ПО, используемое в мошеннических схемах, наносящих ущерб потребителям. Несомненно, что в интересах общества сохранить статус-кво и прекратить действия ботнета ZeroAccess по мошенничеству со щелчками и перехвату браузера на время рассмотрения жалобы Microsoft.

Ряд окружных судов приходил к выводу, что «управляющие серверы ботнета» и незаконная деятельность, выполняемая посредством ботнета, наносят потребителям «прямой и непоправимый ущерб». (См. Heath Decl. Exs. 14-22 (приказы на отключение ботнетов); см. также Physicians Interactive, 2003 U.S. Dist. LEXIS 22868, at *29 («суд обязан пресечь действия предполагаемых хакеров по атаке и краже проприетарной информации [истца].»). Аналогично, в данном случае ВЗСП и предварительный судебный запрет позволяет сохранить и защитить существенные интересы общества. При

отказе в испрашиваемой мере такую защиту не удастся обеспечить, в случае чего преступники, контролирующие ботнет, безнаказанно продолжат свои действия.

5. Только испрашиваемая односторонняя мера может прекратить непоправимый вред, наносимый Microsoft и обществу

В отсутствие ВЗСП об испрашиваемой мере, вред Microsoft и обществу, в том числе заказчикам Microsoft, продолжит осуществляться в том же объеме, нанося непоправимый ущерб репутации и брендам Microsoft и восприятию ее потребителями. Кроме того, для того, чтобы ВЗСП возымел эффект, он должен быть выпущен в одностороннем порядке, о чем свидетельствуют чрезвычайные обстоятельства. Правило 65 федеральных правил гражданского судопроизводства разрешает вынесение одностороннего ВЗСП, если податель обосновывает прямой и непоправимый ущерб и необходимость исключения уведомления противной стороны. Fed. R. Civ. P. 65(b)(1); см. Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers, Lcal No. 70, 415 U.S. 423, 438-39 (1974) («Односторонний временный запретительный судебный приказ, без сомнения, необходим в определенных случаях...»).

Если принятию ВЗСП будет предшествовать уведомление, Ответчики смогут быстро перевести серверы контроля мошенничества со щелчками и перехвата браузера на новые IP-адреса, прежде чем ВЗСП вступит в силу. Таким образом, уведомление о ВЗСП, несомненно, будет на руку лицам, контролирующим ботнет.

Известно, что односторонние меры допустимы в особых случаях, к которым относится и рассматриваемое дело, где уведомление привело бы к бесполезности испрашиваемой меры. См. напр. Kelly v. Thompson, 2010 U.S. Dist. LEXIS 31800, *3 (W.D. Tex. Mar. 31, 2010) (издан односторонний ВЗСП без уведомления, так как в случае уведомления был бы нанесен непоправимый ущерб); In re Vuitton Et Fils S.A., 606 F.2d 1,

4-5 (2d Cir. 1979) (решением суда) (решено, что уведомление о принятии ВЗСП не является необходимым, если оно «послужит лишь способом избежать дальнейших мер по пресечению деяния»; прошлый опыт показывает, что стоит одному члену преступной организации получить уведомление, как контрабанда переводится к другому, неустановленному лицу, что приводит к продолжению вреда и бесполезности дальнейших судебных действий); Allscripts Misys, LLC v. Am. Digital Networks, LLC, 1:10-cv-00111, 2010 U.S. Dist. LEXIS 4450, at *2 (D. Md. Jan. 20, 2010) (издан односторонний ВЗСП, так как «Ответчик может растратить средства и (или) предпринять шаги, затрудняющие их возвращение...»)[5]

В рассматриваемом случае имеются четкие основания полагать, что операторы ботнета попытаются перевести инфраструктуру при получении уведомления, поскольку именно это они сделали в ответ на попытку обезвреживания ZeroAccess чисто техническими средствами со стороны компании, занимающейся услугами безопасности. Если имеются основания полагать, что операторы ботнета при получении уведомления попытаются избежать обеспечительных мер, переместив управляющие серверы, принятие мер в одностороннем порядке является оправданным. Особенно показательны дела Microsoft Corp. v. John Does 1-27, Microsoft Corp. v. Peng Yong, и Microsoft Corp. v. Piatti, где окружной суд выпустил односторонний ВЗСП для отключения ботнета, признав риск перевода Ответчиками инфраструктуры ботнета и уничтожения улик после получения уведомления. (См. Heath Decl., Exs. 14, 15, 18, 19 и 22.)

[5] См. также Crosby v. Petromed, Inc., 2:09-cv-05055, 2009 U.S. Dist. LEXIS 73419, at *5 (E.D. Wash. Aug. 6, 2009) (издан односторонний ВЗСП, так как «уведомление Ответчиков об этом ходатайстве может привести к дальнейшему нанесению ущерба Истцам...»); AT&T Broadband v. Tech Commc'ns, Inc. 381 F.3d 1309, 1319-1320 (11th Cir. 2004) (выдача одностороннего ордера на обыск с целью изъятия контрабандного оборудования на том основании, что в прошлом ответчики и находившиеся в аналогичном положении лица скрывали улики сразу после получения уведомления); Little Tor Auto Center v. Exxon Co., U.S.A., 822 F. Supp. 141, 143 (S.D.N.Y. 1993) (односторонний ВЗСП обоснован, если контрабанда «может быть уничтожена сразу после получения уведомления»).

Аналогично, в деле FTC v. Pricewert LLC окружной суд выпустил односторонний ВЗСП о приостановке подключения к сети Интернет компании, поддерживающей работу ботнета и выполняющей иные компьютерные преступления, на том основании, что «Будучи уведомлен об этих действиях [истца], Ответчик может переместить хранимый у него вредоносный код и (или) предупредить свою нелегальную клиентуру». (См. Heath Decl., Ex. 10 (FTC v. Price wert LLC et al., Дело № 09-2407) (N.D. Cal., Whyte J.) на с. 3.) Далее, в деле Dell, Inc. v. Belgiumdomains, LLC, 1:07-cv-22674, 2007 U.S. Dist. Lexis 98676, at *4-5 (S.D. Fla. Nov. 21, 2007) суд выпустил односторонний ВЗСП против регистраторов доменов, так как ранее лица, находившиеся в похожей ситуации, скрывали свои деяния и игнорировали приказы суда путем, в числе прочего, использования вымышленных компаний, личных имен и подставных компаний. там же, at *4. В деле Dell суд ясно установил, что если, как и в настоящем деле, преступная схема Ответчиков «имеет электронную природу и может быть быстро и бесследно уничтожена Ответчиками», принятие односторонних мер является обоснованным. там же, at *5-6.

B. Закон о вынесении судебных приказов разрешает суду предписывать третьим сторонам выполнить действия, необходимые для обеспечения испрашиваемой меры

Предлагаемый Microsoft проект приказа предписывает поставщикам услуг Интернета, на инфраструктуру которых полагаются Ответчики, оказать разумное сотрудничество в реализации приказа. Необходимо подчеркнуть, что только эти компании могут фактически отключить инфраструктуру управления мошенничеством со щелчками и перехватом браузера, и потому их сотрудничество является необходимым.[6]

[6] Проект приказа также включает также юридически не обязывающий запрос на добровольное сотрудничество, адресованный компаниям услуг хостинга, у которых Ответчики приобрели IP-адреса и домены, используемые для управления мошенничеством со щелчками и перехватом браузера.

Закон о вынесении судебных приказов предусматривает, что суд может выпустить все приказы, необходимые для отправления правосудия. 28 U.S.C. § 1651(a). Верховный суд постановил, что закон о вынесении судебных приказов разрешает выносить избирательное предписание третьим сторонам, необходимое для выполнения судебного приказа:

> Полномочия, предоставляемые настоящим законом, в определенных случаях распространяются на лиц, которые хоть и не принимали участия в исходном деянии или другой незаконной деятельности, но обладают возможностью воспрепятствовать осуществлению судебного приказа или надлежащему отправлению правосудия, в том числе на тех из них, что не предпринимали никаких действий по воспрепятствованию правосудию.

United States v. New York Tel. Co., 434 U.S. at 174 (цитаты опущены) (приказ телефонной компании содействовать в установке автоматического регистратора звонков разрешен в рамках закона о вынесении судебных приказов); Moore v. Tangipahoa Parish Sch. Bd., 507 Fed. App'x. 389, 396 (5th Cir. 2013) (не опубликовано) («Закон о вынесении судебных приказов дает "федеральному суду полномочия выносить предписания... которые могут потребоваться для обеспечения выполнения приказов, ранее выпущенных этим судом в рамках своей юрисдикции."») (цитата New York Tel. Co., 434 U.S. at 172); см. также In re Application of United States for an Order Authorizing An In-Progress Trace of Wire Commc'ns Over Tel. Facilities, 616 F.2d 1122, 1129 (9th Cir. 1980) (то же; касаемо New York Tel. Co. «суд на основании общих соображений пришел к выводу, что без участия телефонной компании "нет способа выполнить санкционированное судом наблюдение."» 434 U.S. at 172); In re Baldwin-United Corp., 770 F.2d 328, 338-339 (2d Cir. 1985) («Закон о вынесении судебных решений позволяет предписывать сторонам, не участвующим в процессе, совершать действия, необходимые суду для обеспечения выполнения своих решений по делам, относящимся к его юрисдикции»; «Мы не находим, что правило 65 было введено

для ограничения полномочий судов, предоставленных им законом о вынесении судебных приказов для обеспечения обязательности правосудия.»); Dell Inc., 2007 U.S. Dist. LEXIS 98676, at * 16 (закон о вынесении судебных приказом применен совместно с изъятием товарного знака в соответствии с правилом 65 и законом Ленхема).

Предписание этим третьим сторонам оказать разумное содействие в выполнении этого приказа не нарушит надлежащую правовую процедуру, поскольку проект приказа (1) предполагает лишь минимальное сотрудничество третьих сторон в выполнении приказа (запрашиваются действия, которые рутинно совершаются этими сторонами), (2) предполагает минимальную степень вмешательства в нормальную работу третьих сторон, (3) не лишает третьи стороны никаких существенных имущественных интересов и (4) предусматривает компенсацию третьим сторонам за оказанное сотрудничество со стороны Microsoft. Если при выполнении испрашиваемого приказа любой из третьих сторон потребуется довести что-либо до сведения суда, Microsoft немедленно выполнит это. Третьи стороны будет иметь возможность выступить на слушаниях по предварительному судебному запрету, которые должны пройти вскоре после выполнения испрашиваемого приказа. Fed. R. Civ. P. 65(b)(2). Таким образом, предписания третьим сторонам в испрашиваемом приказе избирательны, отвечают надлежащей правовой процедуре и необходимы для обеспечения выполнения принимаемых мер. Более того, Microsoft уже уведомила поставщиков услуг Интернета об этих действиях, ведет с ними сотрудничество и ознакомлена с их мнением относительно положений подаваемого проекта приказа.

C. Microsoft предпримет чрезвычайные меры для доставки уведомления о ВЗСП и слушаниях по предварительному судебному запрету, а также вручения жалобы

Для соблюдения надлежащей правовой процедуры сразу после вступления в силу одностороннего ВЗСП Microsoft предпримет чрезвычайные меры для доставки Ответчикам формального и неформального уведомления о слушаниях по предварительному судебному запрету и для вручения им текста жалобы.

Microsoft представит уведомление по электронной почте, факсу и почте. Microsoft уже известны адреса электронной почты, почтовые адреса и (или) номера факсов, сообщавшиеся Ответчиками, и она намерена запросить дополнительную контактную информацию в соответствии с положениями испрашиваемого ВЗСП. (там же, ¶¶ 7-9, Ex. 1.) Microsoft представит уведомление о слушаниях по предварительному судебному запрету и выполнит вручение жалобы путем немедленной отправки указанных выше состязательных бумаг по адресам электронной почты, номерам факсов и почтовым адресам, которые Ответчики предоставляли компаниям услуг хостинга при размещении управляющего программного обеспечения, доступного по IP-адресам ZeroAccess. (там же, ¶ 10.) Регистрируя IP-адреса, Ответчики согласились воздерживаться от таких злоупотреблений, как те, что рассматриваются в настоящем деле, а также согласились с тем, что уведомления о спорах, касающихся хостинга, могут доставляться им по предоставленным адресам электронной почты, номерам факса и почтовым адресам. (там же, ¶¶ 30-34.)

Microsoft представит Ответчикам уведомление путем публикации. Microsoft уведомит Ответчиков о слушаниях по предварительному судебному запрету и жалобе на их незаконные действия путем публикации этих материалов на централизованном, доступном для публики ресурсе сети Интернет сроком на 6 месяцев. (там же, ¶ 11.)

Microsoft представит Ответчикам уведомление путем личной доставки. Microsoft известны IP-адреса, используемые управляющим программным обеспечением ZeroAccess, и она намеревается в соответствии с ВЗСП запросить у компаний услуг хостинга и регистраторов доменов все имеющиеся физические адреса Ответчиков. Как ожидается, Microsoft сможет получить необходимую контактную информацию Ответчиков в рамках добровольного сотрудничества со стороны компаний услуг хостинга, предусмотренного проектом судебного приказа. В соответствии с правилом 4(e)(2)(A) и 4(f)(3) Microsoft планирует осуществить вручение формального уведомления о слушаниях по предварительному судебному запрету и теста жалобы путем ручной доставки судебной повестки, жалобы Microsoft, настоящего документа и материалов по делу, а также любых изданных судом приказов по всем существующим адресам Ответчиков, которые удастся установить на территории США. (Heath Decl. ¶ 13.)

Microsoft по возможности предоставит уведомление путем личной доставки и в соответствии с конвенциями. Если удастся установить реально существующие физические адреса Ответчиков, Microsoft уведомит Ответчиков и вручит им судебные документы методом личной доставки или в соответствии с Гаагской конвенцией о вручении судебных документов либо иным предусмотренным конвенциями способом. (там же, ¶ 14.)

Уведомление и вручение вышеуказанными способами отвечают надлежащей правовой процедуре, являются уместными, достаточными и разумными для информирования Ответчиков о данном действии, а также являются необходимыми в текущей ситуации. Настоящим Microsoft испрашивает формального одобрения судом приведенных выше альтернативных способов вручения.

Прежде всего, уведомление и вручение по электронной почте, факсу, почте и путем публикации отвечает надлежащей правовой процедуре, поскольку перечисленные средства, в свете обстоятельств, уместны для извещения заинтересованных сторон о ВЗСП, слушаниях о предварительном судебном запрете и судебном процессе. См. Mullane v. Central Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950). Такие методы также допускаются федеральными правилами гражданского судопроизводства 4(f)(3), разрешающими уведомлять ответчиков методами, не запрещенными международными соглашениями. В данном случае Ответчики предположительно находятся в Российской Федерации, которая на настоящий момент приостановила действие Гаагской конвенции, по причине чего выбор применимых способов доставки осуществляется в соответствии с федеральными правилами гражданского судопроизводства и принципами надлежащего осуществления правовой процедуры.[7]

Методы уведомления и вручения, предлагаемые Microsoft, ранее одобрялись в других делах, где фигурировали ответчики из других стран, пытающиеся избежать правосудия. См. напр. Keller Williams Realty, Inc. v. Lapeer, 4:08-cv-01292, 2008 U.S. Dist. LEXIS 58079, at *5 (S.D. Tex. July 31, 2008) (цитируя Rio Props., Inc. v. Rio Int'l. Interlink, 284 F.3d 1007, 1017 (9th Cir. 2002) (одобрено вручение судебного документа ответчику из другой страны по электронной почте); Heath Decl., Ex. 16 (Microsoft Corp. v. John Does 1-

[7] См. http://travel.state.gov/law/judicial/judicial_3831.html (Государственный департамент отмечает, что действие Гаагской конвенции приостановлено в Российской Федерации); RSM Prod. Corp. v. Fridman, 2007 U.S. Dist. LEXIS 58194, *5-6 (S.D.N.Y. 2007) (одобрение вручения ответчику в России судебного документа средствами, не предусмотренными конвенциями, в связи с приостановкой действия Гаагской конвенции); Xcentric Ventures, LLC v. Karsen, Ltd., 2011 U.S. Dist. LEXIS 81698 (D. Ariz. 2011) (то же; одобрено вручение ответчику в России судебного документа по электронной почте в рамках правила 4(f)(3) в связи с приостановкой действия Гаагской конвенции); Henry F. Teichmann, Inc. v. Caspian Flat Glass OJSC, 2013 U.S. Dist. LEXIS 54299, *3 (W.D. Pa. 2013) (Касаемо ответчика в России: «Истец не обязан сначала использовать средства, предусмотренные Гаагской конвенцией, поскольку эти усилия были бы тщетны.»); Arista Records LLC v. Media Servs. LLC, 2008 U.S. Dist. LEXIS 16485 (S.D.N.Y. 2008) (истец не обязан вначале попытаться вручить ответчику в России судебный документ в соответствии Гаагской конвенцией, чтобы иметь возможность выполнить вручение в соответствии с правилом 4(f)(3)).

27, Дело № 1:10-cv-156 (E.D. Va. 2010, Brinkema J.)); Smith v. Islamic Emirate of Afghanistan, 1:01-cv-10132, 1:01-cv-10144, 2001 U.S. Dist. LEXIS 21712 (S.D.N.Y. Dec. 26, 2001) (одобрено вручение судебного документа Усама бен Ладену и организации «Аль-Каида» путем публикации); FMAC Loan Receivables v. Dagra, 228 F.R.D. 531, 535-36 (E.D. Va. 2005) (признание частого использования судами правила 4(f)(3) для международного вручения судебных документов нетрадиционными средствами); BP Prods. North Am., Inc. v Dagra, 236 F.R.D. 270, 271-73 (E.D. Va. 2006) (одобрение уведомления методом публикации); AllscriptsMisys, LLC v. Am. Digital Networks, LLC, 2010 U.S. Dist. LEXIS 4450, at *3 (D. Md. Jan. 20, 2010) (вынесен односторонний ВЗСП и судебный приказ с указанием, что «уведомление о настоящем приказе и временном запретительном судебном приказе может быть доставлено по телефону, электронным средствам связи, по почте или курьерской службой.»).

Такой способ доставки особенно обоснован в случаях, подобных рассматриваемому, где речь идет о преступлениях в сети Интернет, совершаемых ответчиками в других государствах и наносящих прямой и непоправимый ущерб. Как было недавно отмечено Девятым округом:

> [Ответчик] не имел ни офиса, ни помещения; у него имелся только компьютерный терминал. Если какой-то метод связи и подходит для вручения [Ответчику] уведомления, то это со всей определенностью электронная почта — метод связи, который [сам Ответчик] использует и предпочитает. Кроме того, электронная почта является единственным разрешенным судом методом, который позволяет немедленно и напрямую связаться с [Ответчиком]... Так, электронная почта может оказаться единственным средством вручения судебного документа международному нарушителю закона, играющему в прятки с федеральным судом.

Rio Props., Inc., 284 F.3d at 1018; см. также Williams-Sonoma, Inc. v. Friendfinder, Inc., 3:06-cv-06572, 2007 U.S. Dist. LEXIS 31299, at *5-6 (N.D. Cal. Apr. 17, 2007) (вручение по электронной почте соответствует Гаагской конвенции и является обоснованным в делах,

где фигурирует неблаговидное использование технологий сети Интернет международными ответчиками). В рассматриваемом деле адреса электронной почты, предоставленные ответчиками компаниям услуг хостинга и регистрации доменов при приобретении услуг, в дальнейшем использовавшихся для обеспечения работы ботнета, могут выступать наиболее достоверной контактной информацией и средством уведомления и вручения. Более того, Ответчики осведомлены о возможности получения по этим каналам связи уведомления об обнаружении использования приобретенных ими услуг хостинга и регистрации доменов для обеспечения работы ботнета, поскольку таковы положения соответствующих договоров, заключенных Ответчиками. See Nat'l Equip. Rental, Ltd. v. Szukhent, 375 U.S. 311, 315-16 (1964) («Определено... что стороны договора могут заранее согласиться на рассматривать дело в выбранном суде, разрешить вручение уведомления противной стороной или вовсе не предусматривать вручения уведомлений.»). По этим причинам уведомление и вручение документов по электронной почте и методом публикации в данном случае обоснованы и необходимы.[8]

По всем вышеупомянутым причинам Microsoft ходатайствует перед судом о вынесении испрашиваемого судебного приказа и приказа о предоставлении обоснования того, что предварительный судебный запрет не должен быть наложен, а также приказа, подтверждающего, что предложенные настоящим средства уведомления о слушаниях по предварительному судебному запрету и вручения судебных документов отвечают федеральному правилу гражданского судопроизводства 4(f)(3), удовлетворяют

[8] Кроме того, если физические адреса, предоставленные Ответчиками компаниям услуг хостинга, окажется ложными, и местонахождение Ответчиков будет неизвестно, Гаагская конвенция в любом случае не сможет быть применена, и придется все равно прибегнуть к альтернативным способам вручения, как то электронной почте и публикации. См. BP Prods. N. Am., Inc., 236 F.R.D. at 271 («Гаагская конвенция неприменима в случаях, когда неизвестен адрес зарубежной стороны, которой нужно вручить документ.»)

принципам надлежащего осуществления правовой процедуры и уместны для оповещения Ответчиков о данных действиях.

IV. ЗАКЛЮЧЕНИЕ

По приведенным выше основаниям Microsoft ходатайствует о вынесении судом ВЗСП и приказа о предоставлении обоснования касаемо предварительного судебного запрета. Microsoft также ходатайствует о разрешении судом использования альтернативных способов доставки уведомления о слушании по предварительному судебному запрету и текста жалобы.

Дата: 25 ноября 2013 г.

Ходатайствующие

FISH & RICHARDSON P.C.

В лице: _____
David M. Hoffman
Texas Bar No. 24046084
hoffman@fr.com

William Thomas Jacks
Texas Bar No. 10452000
jacks@fr.com

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

В лице юридической службы:

ORRICK, HERRINGTON & SUTCLIFFE LLP

Gabriel M. Ramsey
(Заявление pro hac vice в стадии рассмотрения)
gramsey@orrick.com

Jeffrey L. Cox
(Заявление pro hac vice в стадии рассмотрения)
jcox@orrick.com

Jacob M. Heath
(Заявление pro hac vice в стадии рассмотрения)
jheath@orrick.com

Robert L. Uriarte
(Заявление pro hac vice в стадии рассмотрения)
ruriarte@orrick.com

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

Юридическая поддержка истца
КОРПОРАЦИЯ MICROSOFT

OHSUSA:755155926.12