В ФЕДЕРАЛЬНЫЙ СУД СОЕДИНЕННЫХ ШТАТОВ

ЗАПАДНОГО ОКРУГА СЕВЕРНОЙ КАРОЛИНЫ

ОТДЕЛЕНИЕ г. ШАРЛОТТ

КОРПОРАЦИЯ MICROSOFT,

Истец,

против

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

Ответчиков.

ПОДАНО В ОПЕЧАТАННОМ ВИДЕ

№ гражданского иска _____

ИСКОВОЕ ЗАЯВЛЕНИЕ

Истцы, КОРПОРАЦИЯ MICROSOFT CORP. («Microsoft»), настоящим подают исковое заявление и утверждают, что НЕУСТАНОВЛЕННЫЕ ЛИЦА №№1-82 («Неустановленные лица» или «Неустановленные ответчики») контролируют всемирную систему объединенных незаконных компьютерных сетей, совокупно известных под названием «Ботнеты Citadel», состоящих из подключенных к сети Интернет компьютеров конечных пользователей, которые Ответчики заразили вредоносными программными средствами. Ответчики использовали Ботнеты Citadel для заражения миллионов компьютеров в сети Интернет, при помощи которых в течение последних полутора лет были украдены миллионы долларов. Ответчики контролируют Ботнеты Citadel через сложную инфраструктуру командования и управления, которая размещена на и эксплуатируется через интернет-домены, указанные в Приложении «А» (далее – «Вредоносные домены»), и IP-адреса, указанные в Приложении «В» к настоящему

Исковому заявлению (далее – «Вредоносные IP-адреса») (совокупно именуемым далее «Вредоносные домены и IP-адреса»), а именно:

ПРЕДМЕТ ИСКОВОГО ТРЕБОВАНИЯ

1. Исковое требование основано на: Законе о компьютерном мошенничестве и злоупотреблении (Свод законов США, раздел 18, § 1030); Законе о контроле над активным распространением навязчивой порнографии и рекламы (CAN-SPAM) (Свод законов США, раздел 15, § 7704); Законе о защите информации, передаваемой через электронные системы связи (Свод законов США, раздел 18, § 2701); нарушении торговой марки в соответствии с Законом о торговых марках (Свод законов США, раздел 15, § 1114), ложном обозначении происхождения в соответствии с Законом о торговых марках (Свод законов США, раздел 15, § 1125(a)); ослаблении торговой марки в соответствии с Законом о торговых марках (Свод законов США, раздел 15, § 1125(c)); Законе о борьбе с организованной преступностью (RICO) (Свод законов США, раздел 18, § 1962(c)); неосновательном обогащении; неправомерном использование компьютера; присвоении имущества по общему праву и причинении зловредности. Компания Microsoft обращается с требованием о принятии обеспечительных мер (запретов) и иных средств правовой защиты по праву справедливости в отношении Ответчиков, а также взыскания с них убытков в связи с созданием, контролированием, обслуживанием и непрекращающимся использованием Ботнетов Citadel, которые нанесли и продолжают наносить компании Microsoft, ее клиентам и населению в целом невозместимый вред.

СТОРОНЫ

2. Истец, корпорация Microsoft Corp., является корпорацией, образованной и осуществляющей свою деятельность в соответствии с законами штата Вашингтон, с местонахождением в городе Редмонд (штат Вашингтон). Компания Microsoft является ведущим поставщиком технологических продуктов и услуг, в частности компьютерных

программ, интернет-услуг, веб-сайтов и сервисов электронной почты.

3. На основании имеющихся сведений и убеждений компания Microsoft заявляет, что Неустановленное лицо №1 является создателем или участником группы, которая создала и обеспечивает поддержку и дальнейшую разработку бот-кода «Citadel» для Ботнетов Citadel. Неустановленное лицо №1 использует псевдоним «Aquabox», и с ним можно связаться по адресам aquabox@jabber.jp, aquabox@jabber.org, и aquabox@lugmen.org.ar.

4. На основании имеющихся сведений и убеждений компания Microsoft заявляет Неустановленные лица №№2-82 используют псевдонимы, указанные в Приложении «С». В соответствии с имеющимися сведениям, Неустановленные лица №№2-82 осуществляют деятельность Ботнетов Citadel. Связь с этими лицами возможно или вероятно может быть установлена при помощи контактной информации, указанной в Приложении «С».

5. На основании имеющихся сведений и убеждений компания Microsoft заявляет, что Неустановленное лицо №1 в качестве создателя и разработчика вредоносного бот-кода, действовало по соглашению с Неустановленными лицами №№2-82, которые приобретали, разрабатывали и (или) оказывали поддержку этому бот-коду и в настоящее время осуществляют или участвовали в осуществлении работы Ботнетов Citadel.

6. Ответчики владеют, осуществляют работу и обслуживание ботнетов Citadel через инфраструктуру командования и управления, которая размещена на и (или) эксплуатируется через Вредоносные домены и IP-адреса. Командная инфраструктура, которая размещена на и эксплуатируется через Вредоносные домены и IP-адреса, поддерживается сторонними компаниями, предоставляющими услуги по регистрации

доменов и веб-хостингу. Эти компании указаны в Приложениях «A» и «B» к настоящему Исковому заявлению.

7. Истцам неизвестны настоящие имена, фамилии и роли Ответчиков, обозначенных в настоящем иске как Неустановленные лица №№1-82, в связи с чем иск в отношении Ответчиков предъявляется с использованием этих вымышленных наименований. Компания Microsoft внесет поправки в Исковое заявление с указанием настоящих имен, фамилий и ролей Ответчиков, как только таковые будут установлены. Компания Microsoft примет должные меры к тому, чтобы определить настоящие имена, роли и контактную информацию Ответчиков и официально вручить Ответчикам судебное извещение.

8. На основании имеющихся сведений и убеждений компания Microsoft заявляет, что каждый из названных вымышленным обозначением Ответчиков несет какого-либо рода ответственность за указанные в настоящем документе события и что заявленный в настоящем документе вред, причиненный компании Microsoft и клиентам компании Microsoft, был непосредственно причинен данными Ответчиками.

9. Действия и бездействие, которые приписываются в настоящем документе Ответчикам, были предприняты каждым из Ответчиков в отдельности, являлись действиями или бездействием, санкционирование, контроль и руководство которыми каждый из Ответчиков либо осуществлял, либо имел возможность осуществлять, и (или) действиями и бездействием, которым каждый из Ответчиков способствовал, в которых принимал участие или иным образом поощрял и за которые каждый из Ответчиков несет ответственность. Каждый Ответчик оказывал пособничество и подстрекательство действиям Ответчиков, указанным ниже, в том смысле, что каждый Ответчик знал об этих

действиях и бездействии, способствовал их совершению и извлекал в полном объеме или частично пользу от их совершения. Каждый Ответчик являлся агентом каждого из остальных Ответчиков и, совершая действия, о которых утверждается ниже, действовал в рамках и масштабах таких отношений представительства и с разрешения и согласия других Ответчиков.

ПОДСУДНОСТЬ И МЕСТО РАССМОТРЕНИЯ

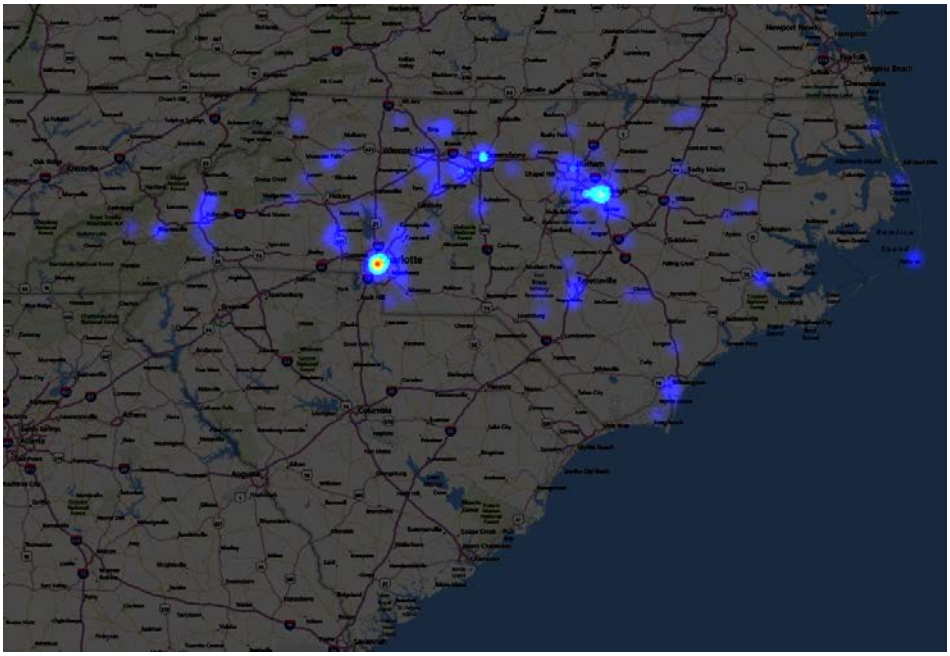
10. Настоящее исковое требование основано на нарушении Ответчиками Федерального закона о компьютерном мошенничестве и злоупотреблении (Свод законов США, раздел 18, § 1030), Закона о контроле над активным распространением навязчивой порнографии и рекламы (CAN-SPAM) (Свод законов США, раздел 15, § 7704), Закона о защите информации, передаваемой через электронные системы связи (Свод законов США, раздел 18, § 2701), Закона о защите торговых марок (Свод законов США, раздел 15, §§ 1114, 1125(a), (c)) и Закона о борьбе с организованной преступностью (RICO) (Свод законов США, раздел 18, § 1962(c)). Таким образом, на основании Свода законов США, раздел 28, § 1331, данное исковое дело находится в подведомственности настоящего Суда. Исковое требование предъявляется также в связи с неправомерным использованием компьютера, неосновательным обогащением, присвоением имущества и причинением зловредности. Соответственно, данное исковое дело находится в подведомственности настоящего Суда на основании Свода законов США, раздел 28, § 1367.

11. Ответчики совершают действия, о которых заявляется в настоящем документе, в отношении штата Северная Каролина и Западного округа Северной Каролины, используют средства совершения преступлений, находящиеся в Северной Каролине и Западном округе Северной Каролины, для осуществления действий, которые

приписываются им в настоящем Исковом заявлении, и занимаются иной деятельностью, пользуясь правом на ведение бизнеса в Северной Каролине и Западном округе Северной Каролины.

12. В частности, Ответчики осуществляют контроль на сетью, состоящей из скомпрометированных пользовательских компьютеров, которая называется «Ботнеты Citadel» и которую Ответчики используют для ведения незаконной деятельности, причиняя тем самым вред компании Microsoft и клиентам Microsoft, а также населению Западного округа Северной Каролины в целом. Ответчики совершили действия в отношении Западного округа Северной Каролины путем направления вредоносного компьютерного кода на компьютеры отдельных пользователей Интернет, находящихся в Западном округе Северной Каролины, и заражения компьютеров этих пользователей вредоносным кодом, что привело к превращению этих компьютеров в часть Ботнетов Citadel. На Рис. 1 отражено географическое расположение инфицированных компьютеров в Западном округе штата Северная Каролина.

Рис. 1 ***Географическое расположение компьютеров Ботнета Citadel в Западном округе штата Северная Каролина***



13. Ответчики предприняли вышеуказанные действия, осознавая, что такие действия причинят вред компьютерам пользователей, находящимся в Северной Каролине, и тем самым нанесли ущерб компании Microsoft, ее клиентам и иным лицам в Северной Каролине и других регионах Соединенных Штатах Америки. Таким образом, этот Суд обладает персональной юрисдикцией над Ответчиками.

14. В соответствии с Сводом законов США, раздел 28, § 1391(b), должным местом рассмотрения является настоящий судебный округ. Значительная часть событий или бездействия, которые дают основания для иска Microsoft, а также значительная часть собственности, которую затрагивает иск Microsoft, располагаются в данном судебном округе. Этот судебный округ обладает надлежащей подсудностью в соответствии со Сводом законов США, раздел 28, § 1391(c), поскольку Ответчики подпадают под персональную юрисдикцию в этом судебном округе.

15. Истец Microsoft напрямую пострадал в результате действий, о которых заявляется в настоящем документе, и предъявляет данный иск от своего имени.

ОБСТОЯТЕЛЬСТВА ДЕЛА

Продукты, услуги и репутация компании Microsoft

16. Истец Microsoft® является поставщиком операционной системы Windows®, браузера Internet Explorer® и сервисов электронной почты и мгновенного обмена сообщениями Outlook,® Hotmail®, Windows Live® и MSN®, а также широкого ряда другого программного обеспечения и услуг. Компания Microsoft вкладывает значительные ресурсы в разработку продуктов и услуг высокого качества. Благодаря высокому качеству и эффективности продуктов и услуг компании Microsoft, а также значительным ресурсами, которые Microsoft затрачивает на продвижение этих продуктов и услуг, компания

заработала серьезную репутацию у своих клиентов, создав сильный бренд и превратив название Microsoft и названия своих продуктов и услуг в мощные и известные во всем мире символы, признанные в своей торговой категории. Компании Microsoft принадлежат зарегистрированные торговые марки, отражающие качество продуктов и услуг компании и ее бренда, в том числе Microsoft®, Windows®, Internet Explorer® и другие. Точные копии регистрационных документов торговых марок компании Microsoft содержатся в Приложении «D».

17. Управлением, контролированием, обслуживанием и расширением Ботнетов Citadel Ответчики нанесли и продолжают наносить каждому Истцу, его клиентам, его участникам и населению в целом серьезный и невозместимый вред.

Компьютерные «Ботнеты»

18. В целом, «ботнет» – это ряд индивидуальных компьютеров, на которых запущено программное обеспечение, позволяющее осуществлять общение между этими компьютерами, а также централизованное или децентрализованное общение с другими компьютерами, предоставляющими команды. Ботнет состоит из множества (иногда миллионов) компьютеров конечных пользователей, зараженных вредоносными программными средствами («вредоносное ПО» или «Троян»). Отдельные компьютеры в бот-сети часто принадлежат пользователям, которые, не осознавая этого, загрузили или были заражены таким программным обеспечением, которое превращает компьютер в часть ботнета. Компьютер конечного пользователь может стать частью ботнета, если пользователь непреднамеренно взаимодействует с вредоносной рекламой на сайте, открывает вредоносное приложение к электронному письму или загружает вредоносные программные средства. В каждом из таких случаев на компьютер пользователя

устанавливается программный код, в результате исполнения которого компьютер становится частью ботнета и получает возможность отправлять и получать сообщения, код и команды от других компьютеров в ботнете.

19. Преступные организации и отдельные киберпреступники нередко создают, контролируют, обслуживают и множат ботнеты с целью осуществления неправомерных действий, нарушающих права других лиц. Ботнеты привлекают их тем, что позволяют осуществлять широкий спектр противозаконных действий, устойчивы к попыткам обезвреживания и дают возможность скрыть личность контролирующих их злоумышленников. Без ведома конечного пользователя владельцы ботнета используют зараженный компьютер для самых различных незаконных целей. Компьютер в ботнете может быть использован, например:

a. для хищения учетной информации и данных, мошенничества, компьютерного проникновения и иных неправомерных действий;
b. для анонимной массовой рассылки нежелательных сообщений электронной почты без ведома и согласия отдельного пользователя, которому принадлежит инфицированный компьютер;
c. для распространения дополнительных вредоносных программных средств для заражения других компьютеров, которые также становятся частью ботнета;
d. в качестве «прокси» или для ретрансляции сообщений, исходящих от других компьютеров, с целью маскировки и сокрытия реального источника этих сообщений.

Ботнеты являются крайне эффективным общим средством контроля над огромным

количеством компьютеров и выполнения любых внутренних действий по отношению к содержанию этих компьютеров или внешних действий по отношению к любому компьютеру в сети Интернет.

20. Компания Microsoft предъявляет настоящее исковое требование для того, чтобы заставить Ответчиков прекратить контролировать, обслуживать и расширять Ботнеты Citadel, которые наносят вред компании Microsoft, ее клиентам и населению в целом. Ответчики контролируют, обслуживают и множат Ботнеты Citadel через сложную инфраструктуру командования и управления, которая размещена на и эксплуатируется через Вредоносные домены и IP-адреса, описанные в настоящем документе и указанные в Приложениях «A» и «B».

«Ботнеты Citadel»

21. Ботнеты Citadel главным образом осуществляют кражу информации об учетных записях на веб-сайтах, в частности на сайтах интернет-банкинга. Основная цель Ботнетов Citadel – заразить компьютеры конечных пользователей с тем, чтобы: (1) осуществить хищение учетных данных пользователей в Интернете, в том числе учетных данных в системах интернет-банкинга; (2) осуществить доступ к учетным записям клиентов при помощи украденных данных; (3) похитить информацию из учетной записи клиента на сайте и осуществить хищение средств с банковских и финансовых счетов клиента. Кроме того, создатели вредоносного кода Ботнетов Citadel осуществляют взаимодействие в рамках общей операции по созданию, распространению и осуществлению деятельности Ботнетов Citadel. Ущерб, причиняемый в результате компании Microsoft, ее конечным пользователям-клиентам, финансовым учреждениям, государственным органам и населению в целом является результатом одной глобальной

преступной операции, в рамках которой осуществляется контроль, управление и обслуживание Ботнетов Citadel.

Ответчики взаимодействуют в рамках общей операции по созданию, контролированию и обслуживанию Ботнетов Citadel

22. Ботнеты Citadel – это семейство объединенных бот-сетей, известных в Интернете под названием ботнеты «Citadel». Программный код и инфраструктура, на основе которых построены ботнеты «Citadel» сходны с теми, которые использовались при создании их предшественника – ботнета Zeus. Ответчик Неустановленное лицо №1 – создатель и разработчик кода Citadel, конкретная личность которого в настоящее время неизвестна, – анонимно действует в сети Интернет уже несколько лет. Неустановленное лицо №1 предлагает на продажу в Интернете бот-код Citadel в виде «Конструкторского пакета», который позволяет другим лицам, в том числе другим Ответчикам, с легкостью настроить, эксплуатировать, обслуживать и множить ботнеты с целью заражения компьютеров конечных пользователей, хищения денежных средств, рассылки нежелательных сообщений электронной почты и совершения иных вредоносных деяний. В зависимости от уровня сложности конкретной версии, а также уровня поддержки и индивидуализации, стоимость кода может составлять от 2 тыс. 400 долларов США и более (в случае более полной и персонализированной версии). Такой пакет содержит программное обеспечение, при помощи которого другие Ответчики могут генерировать исполняемый кода ботнета, файлы конфигурации и файлы веб-сервера, которые они развертывают на командных серверах.

23. Бот-код «Citadel» впервые появился приблизительно в январе 2012 года. Со временем код «Citadel» претерпел преобразования, стал более утонченным, в том числе обрел функции, направленные на противодействие попыткам анализа и обезвреживания

ботнета.

24. Неустановленное лицо №1 предоставляет обширное послепродажное обслуживание другим Ответчикам. При помощи инструмента управлениям отношениями с клиентами, который называется «Citadel CRM» и предоставляется через сеть Интернет Неустановленным лицом №1, Неустановленные лица №2-82 общаются с Неустановленным лицом №1 и друг с другом на предмет обновлений кода Citadel, решения технических проблем и лучших способов запуска, поддержания и защиты своих ботнетов Citadel. При помощи Citadel CRM другие Ответчики могут сообщать о проблемах, вносить предложения о новых функциях и голосовать за них, а также обмениваться идеями и практическими рекомендациями с другими операторами ботнетов Citadel. При помощи Citadel CRM Неустановленное лицо №1 обращается за идеями о новых функциях или предлагает новые функции, а Неустановленные лица №№2-82 могут голосовать за ту функцию или функции, внедрение которых Неустановленным лицом №1 они хотели бы видеть. Они также могут называть сумму, которую они готовы заплатить Неустановленному лицу №1, чтобы мотивировать это лицо на выполнение работы. Неустановленные лица №№ 1-82 активно сотрудничают в ежедневном процессе разработки и управления Citadel.

25. Например, при помощи Citadel CRM 13 января 2013 года Неустановленное лицо №1 предложило новую функцию и обратилось с просьбой к Неустановленным лицам №№2-82 высказаться в связи с этой функцией. Предлагаемая функция оснащает бот Citadel собственным антивирусом, который позволяет ему очистить компьютер конечного пользователя от конкурирующих вредоносных программы и рекламного ПО. Операторы ботнетов Citadel таким образом рассчитывают на то, что обнаружение конечным

пользователем вируса на своем компьютере станет менее вероятным и, значит, пользователь не станет тщательно чистить компьютер, а также на то, что таким образом будет удалено ПО, которое может помешать работе бота Citadel на компьютере. В сообщении автор просит Неустановленных лиц №№2-82 проголосовать, считают ли они эту функцию полезной или нет, и предлагает им назвать цену, которую они готовы заплатить за внедрение такой доработки. Ниже на рисунке представлен снимок экрана Citadel CRM, на котором изображено указанное выше общение:

26. Неустановленное лицо №1 быстро добавляет новый функционал и исправляет «баги». В сжатые сроки им были выпущены многочисленные версии, предлагающие операторам ботнетов Citadel последние обновления. Скорость появления обновлений свидетельствует об интенсивности и больших масштабах работы, которая

проводится с целю превращения Citadel в серьезный инструмент киберпреступности, а также о высоком уровне взаимодействия между разработчиками и клиентами Citadel. В первые шесть месяцев существования Citadel Неустановленное лицо №1 выпустило пять версий Конструкторского пакета.

27. Неустановленное лицо №1 является разработчиком Citadel. Он разработал и ввел Citadel в коммерческий оборот путем: (1) проектирования и разработки бот-кода Citadel и всех модулей, дающих боту Citadel возможность осуществлять хищение; (2) создания Конструкторского пакета, приобретение которого дает клиентам возможность быстрого генерирования ботов и файлов конфигурации, являющихся основными средствами совершения финансовой кражи; (3) продажи Конструкторских пакетов в интернет-магазине Citadel другим преступникам, а также оказания послепродажной поддержки и сервиса клиентами в форме исправления «багов», представления новых функций и часто обновляемых новых версий Citadel; (4) предложения сотрудничать и работать по найму для добавления новых функций.

Ответчики вместе осуществляют деятельность Ботнетов Citadel

28. На основании имеющихся сведений и убеждений компания Microsoft заявляет, что общий код и характеристики ботнетов Citadel, а также данные, касающиеся конкретной деятельности Ответчиков, позволяют говорить о том, что Ботнеты Citadel контролируются определенным числом Ответчиков, действующих по соглашению друг с другом. В соответствии с имеющимися сведениями, Неустановленное лицо №1 – создатель и поставщик бот-кода – взаимодействует с покупателями, разработчиками и иными продавцами кода Ботнета Citadel на постоянной согласованной основе с целью осуществления контроля, управления, распространения и обслуживания Ботнетов Citadel.

По имеющимся сведениям, вредоносные программные средства, которые Ответчики устанавливают на машинах пользователей, обладают общим кодом и характеристиками и со временем претерпели изменения и сейчас более сильно напоминают друг друга.

29. Неустановленные лица №№2-82 приобрели код Ботнета Citadel и по соглашению с создателем кода запускают и осуществляют деятельность Ботнетов Citadel. Каждое из Неустановленных лиц №№2-82 принимало участие в преступном предприятии Citadel посредством совершения следующих действий: (1) приобретения и использования Конструкторского пакета Citadel с целью генерирования ботов и файлов конфигурации для контроля над ботами; (2) развертывания ботов под именем одной или нескольких бот-сетей; (3) создания командной инфраструктуры, состоящей из подключенных к сети Интернет серверных компьютеров для коммуникации с запущенными ботами; (4) использования одного или нескольких способов заражения компьютеров конечных пользователей Citadel; (5) использование ботов Citadel на зараженных компьютерах конечных пользователей по всему миру для хищения информации, касающейся безопасности, и информации о финансовых счетах; (6) использования ботов Citadel для хищения денежных средств непосредственно с финансовых счетов ничего не подозревающих пользователей по всему миру; (7) нанесения вреда находящемуся в собственности и лицензируемому Microsoft программному обеспечению, включая Windows и Internet Explorer через искажение поведения этих программ и превращения их в преступный инструмент; (8) эксплуатации известных брендов и торговых марок Microsoft с целью введения клиентов Microsoft в заблуждение и, как следствие, нанесения серьезного ущерба брендам, торговым маркам, репутации и доверию к компании Microsoft; (9) использования ботов Citadel для незаконной рассылки нежелательных

электронных сообщений; (10) использования ботов Citadel для вторичного заражения компьютеров такими программами, как программа-вымогатель «Reveton», которая требует оплаты за разблокирование компьютера жертвы; (11) использования ботов Citadel для организации распределенных атак типа «отказ в обслуживании» на финансовые и иные учреждения.

30. Неустановленное лицо №1 – ответчик-создатель кода ботнета – взаимодействует с Ответчиками-операторами ботнетов на постоянной согласованной основе с целью осуществления контроля, управления, распространения и обслуживания Ботнетов Citadel. Неустановленное лицо №1 постоянно предоставляет Неустановленным лицам №№2-82 обновления и инструкции, касающиеся развертывания и работы ботнетов Citadel.

Преступное предприятие Citadel

31. Неустановленное лицо №1 является разработчиком Citadel, вводит Citadel в коммерческий оборот и оказывает поддержку Конструкторским пакетам Citadel. Он постоянно сотрудничает с и оказывает поддержку Неустановленным лицам №№2-82, которые приобрели Конструкторский пакет и которые с его помощью создали и запустили один или более ботнетов Citadel. В свою очередь Неустановленные лица №№2-82 постоянно осуществляют обратную связь с Неустановленным лицом №1 по вопросам усовершенствования базы исходного кода Citadel.

32. В соответствии с имеющимися сведениями, Неустановленные лица №№1-82 составляют группу людей, объединенных общей целью совершения определенных действий в составе постоянно действующей организации, при этом различные участники объединения действуют в качестве его постоянных составляющих частей. У предприятия

Ответчиков есть назначение, при этом между лицами, имеющими отношение к предприятию, существуют взаимоотношения, и предприятие обладает достаточным сроком существования для того, чтобы эти участники имели возможность реализовывать назначение предприятия. В соответствии с имеющимися сведениями, Ответчики №№1-82 вступили в сговор с целью создания и создали предприятие для совместного действия (далее – «Преступное предприятие Citadel») с общей целью разработки и проведения глобальной ботнет-операции по краже учетных данных, как подробно описано в настоящем документе.

33. Преступное предприятие Citadel существует по крайней мере с января 2012 года, когда Неустановленное лицо №1 представило общественности единый консолидированный ботнет по хищению учетных данных. Другие Ответчики, обозначенные как Неустановленные лица №№2-82, вступили в Преступное предприятие Citadel и стали принимать в нем участие в разное время после этой даты.

34. С этого момента Преступное предприятие Citadel начало последовательную и активную реализацию назначения своей деятельности – разработку и проведение глобальной ботнет-операции по хищению учетных данных – и продолжит таковую реализацию, если средства судебной защиты, с просьбой о которых обращается компания Microsoft, не будут предоставлены.

35. Как назначение Преступного предприятия Citadel, так и взаимоотношения между Ответчиками подтверждаются: (1) появлением ботнета Citadel; (2) последующим развитием и работой ботнета Citadel; (3) соответствующими взаимосвязанными ролями Ответчиков в продаже, работе и извлечении прибыли из Ботнетов Citadel в процессе достижения общих финансовых интересов Ответчиков.

36. В соответствии с имеющимися сведениями, Ответчики вступили в сговор с целью осуществления и участия в деятельности Преступного предприятия Citadel и осуществили и приняли участие в такой деятельности через совершение ряда организованных преступных действий («рэкетирской деятельности»), как описано в настоящем документе. Каждое предикатное действие связано и осуществляется с целью реализации незаконного назначения, объединяющего участников Преступного предприятия Citadel. Эти действия продолжаются и не прекратятся, если настоящий Суд не удовлетворит просьбу компании Microsoft о предоставлении временного судебного запрета.

37. В соответствии с имеющимися сведениями, Ответчики вступили в сговор и сознательно и с намерением совершить мошенничество использовали поддельное устройство доступа в виде ключа продукта Windows XP для установки и активации нелицензионной копии Windows XP с целью создания необходимого программного обеспечения Citadel, работу на котором осуществляют Ответчики.

38. Как подробно указывается в настоящем документе, Ответчики использовали поддельный код доступа для установки и активации многочисленных нелицензионных копий Windows XP с целью создания общей среды программирования, чтобы другие Ответчики могли изготовлять и компилировать необходимые программные средства Citadel для использования в ботнете Citadel и реализации их общей финансовой цели получения несанкционированных устройств доступа, как описано ниже.

39. В соответствии с имеющимися сведениями, Ответчики вступили в сговор и сознательно и с намерением совершить мошенничество продали и распространили тысячи устройств несанкционированного доступа в виде украденных паролей, номеров

банковских счетов и других учетных данных через Ботнеты Citadel, созданные и управляемые Ответчиками.

40. Как подробно указывается в настоящем документе, Ответчики использовали Ботнеты Citadel для хищения, перехвата и получения данной информации об устройствах доступа у десятков тысяч лиц при помощи ложных веб-страниц, а затем использовали эти устройства несанкционированного доступа, полученные с помощью мошенничества, для хищения миллионов долларов со счетов этих лиц.

41. В соответствии с имеющимися сведениями, Ответчики также вступили в сговор и сознательно и с намерением совершить мошенничество вступили во владение и продолжают владеть тысячами таких устройств несанкционированного доступа, полученных с помощью мошенничества, как описано в настоящем документе.

42. В соответствии с имеющимися сведениями, Ответчики вступили в сговор и сознательно и с намерением совершить мошенничество осуществили транзакции с похищенными устройствами несанкционированного доступа для получения миллионов долларов с банковских счетов отдельных лиц.

43. В соответствии с имеющимися сведениями, Ответчики вступили в сговор с целью осуществления и осуществили мошеннический план в отношении десятков финансовых учреждений, предоставив участникам Преступного предприятия Citadel возможность ложно выступать в качестве конкретных клиентов банка и дав им тем самым возможность получить доступ к и осуществить хищение денежных средств со счетов этих клиентов.

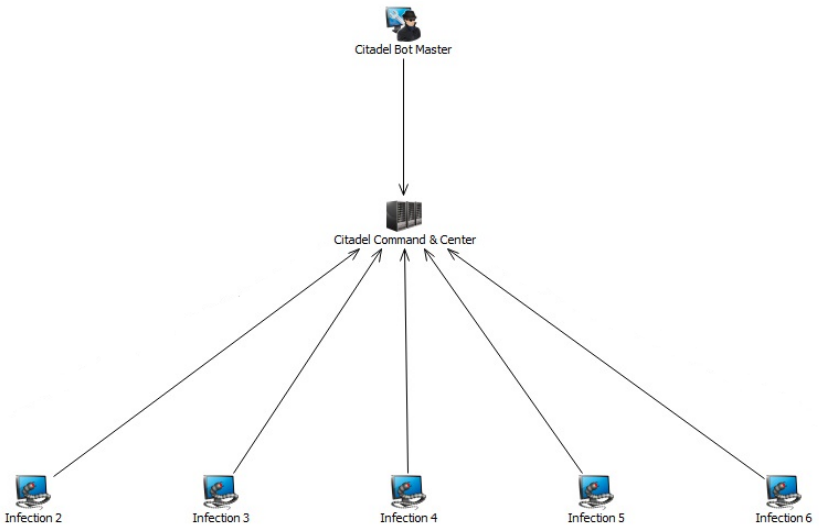
44. Каждое из вышеуказанных незаконных действий было осуществлено при помощи Палаты автоматизированных расчетов между штатами (ACH) и (или) банковских

переводов между штатами США и (или) международных банковских переводов, затронув тем самым торговлю между штатами и (или) внешнюю торговлю США.

Структура Ботнетов Citadel

45. Архитектура ботнетов Citadel состоит из двух уровней. Низшей уровень называется «Инфицированным уровнем» и состоит из ботов, работающих на зараженных компьютерах пользователей. Второй уровень – «Командный». Через него оператор ботнета осуществляет коммуникацию с ботами и управление ими. Многоуровневую архитектуру ботнетов Citadel можно представить следующим образом:

Рис. 1.



1. <u>Инфицированный уровень Citadel</u>

46. По имеющимся оценкам, Инфицированный уровень включает от двух до пяти миллионов зараженных компьютеров, которые без ведома их владельцев находятся под контролем оператора ботнета Citadel. Это – компьютеры конечных пользователей, которые находятся в офисах, квартирах, школах, библиотеках и интернет-кафе по всему миру. Такие компьютеры обычно называются «ботами» Citadel. Ответчики направляют

свои действия на владельцев этих компьютеров и похищают у них информацию о финансовых счетах и иные персональные данные. Ответчики умышленно разместили боты Citadel на инфицированные компьютеры на всей территории Соединенных Штатов Америки, включая Западный округ штата Северная Каролина.

2. Командный уровень Citadel

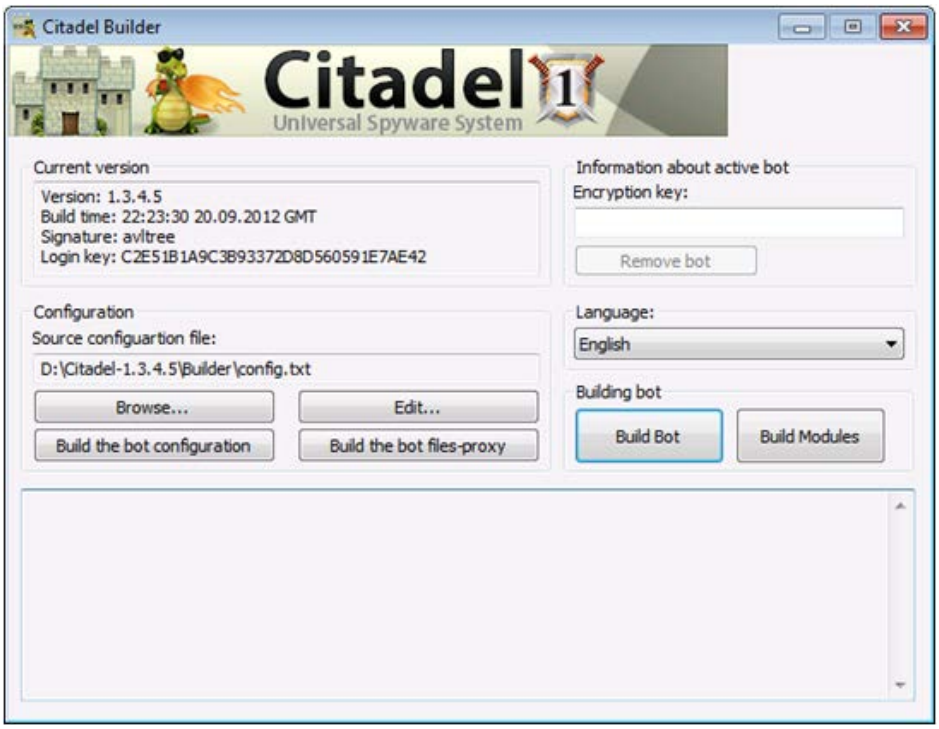
47. Второй уровень архитектуры ботнета Citadel называется «Командным уровнем». В него входят специализированные компьютеры, также подключенные к сети Интернет, на которых работает специализированное программное обеспечение. Ответчики покупают или берут в аренду эти серверы и с их помощью направляют команды, которые позволяют контролировать зараженные компьютеры в Инфицированном уровне и получать информацию от зараженных компьютеров.

48. Вредоносные программные средства Citadel, которые работают на зараженных Citadel компьютерах конечных пользователей – ботах, – заставляют их периодически, приблизительно каждые 20 минут, связываться через Интернет с одним или несколькими командными серверами. Боты загружают с этих серверов обновления и инструкции и загружают на них информацию. Обновляя инструкции, размещенные на командных серверах, операторы ботнета Citadel имеют возможность связываться с и осуществлять контроль над зараженными Citadel компьютерами конечных пользователей. Серверы командного уровня включают серверы на доменных именах и IP-адресах, указанных в Приложениях «A» и «B» к настоящему документу.

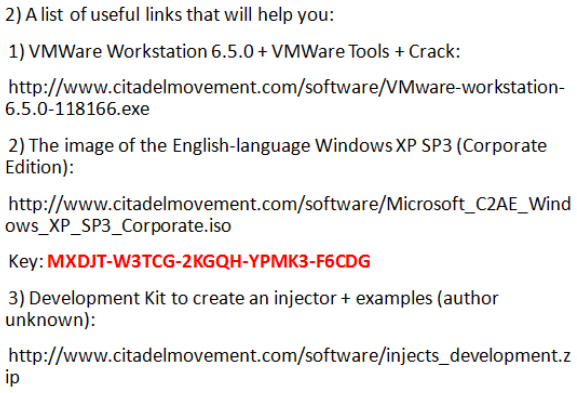
Ответчики используют Вредоносные домены и IP-адреса для заражения и контроля над компьютерами конечных пользователей и хищения у жертв информации и денежных средств

1. Создание бот-кода Citadel и файла конфигурации

49. Чтобы создать ботнет Citadel Неустановленные лица №№2-82 и другие лица сначала приобретают Конструкторский пакет у Неустановленного лица №1. Конструкторский (базовый) пакет – это программное приложение, которое предлагает покупателю ряд опций, определяющих конфигурацию кода ботнета Citadel. После определения параметров конфигурации покупатель может нажать кнопку «Сборка бота», и Конструкторский пакет создает исполняемый код ботнета, а также файлы конфигурации, которые оператор ботнета размещает на командных серверах. На языке Citadel под «ботом» понимается модуль, который загружается на компьютер конечного пользователя, чтобы заразить и контролировать его. Файл конфигурации – это текстовый файл, в котором содержатся параметры, используемые ботом для управления своей текущей работой, такие как домены, в которым следует подключаться. На рисунке ниже представлен снимок экрана Конструкторского пакета Citadel.



50. Неустановленное лицо №1 призывает своих клиентов собирать бот-код на компьютерах с Windows XP. Таким образом сборка всех ботов Citadel происходит в общей среде, что облегчает Неустановленному лицу №1 тестирование Конструкторских пакетов Citadel. С целью предоставления своим клиентам доступа к Windows XP, не требующего оплаты такого доступа в пользу компании Microsoft, Неустановленное лицо №1 предоставляет пиратскую версию Windows XP и пиратский ключ продукта Windows XP. Ниже на рисунке представлена отрывок из руководства пользователя Конструкторского пакета Citadel. В нем для клиентов Citadel указывается путь для получения версии Windows XP и указывается (красным цветом) пиратский ключ продукта к этой копии Windows XP.


2) A list of useful links that will help you:

1) VMWare Workstation 6.5.0 + VMWare Tools + Crack:

http://www.citadelmovement.com/software/VMware-workstation-6.5.0-118166.exe

2) The image of the English-language Windows XP SP3 (Corporate Edition):

http://www.citadelmovement.com/software/Microsoft_C2AE_Windows_XP_SP3_Corporate.iso

Key: MXDJT-W3TCG-2KGQH-YPMK3-F6CDG

3) Development Kit to create an injector + examples (author unknown):

http://www.citadelmovement.com/software/injects_development.zip

2. Создание командной инфраструктуры Citadel

51. Помимо кода и файлов конфигурации, которые создаются с помощью Конструкторского пакета Citadel, оператору ботнета Citadel необходимо создать в сети Интернет командную инфраструктуру. Такая инфраструктура создается путем создания учетных записей в компаниях веб-хостинга, то есть компаниях, предоставляющих места для связи компьютеров с сетью Интернет через соединения высокой пропускной способности. В качестве командной инфраструктуры своих ботнетов оператор ботнета

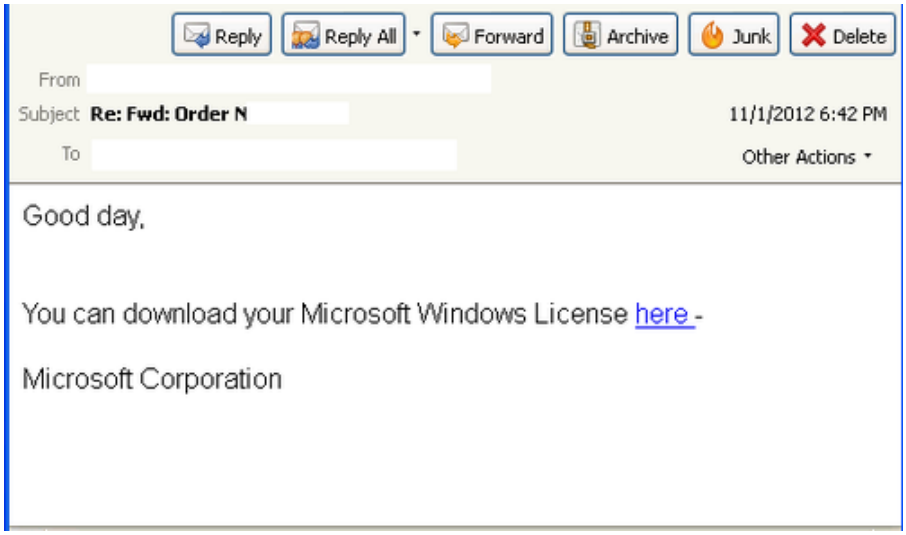
Citadel может использовать сотни компьютеров, подключенных через различные веб-узлы по всему миру. Наиболее уязвимыми точками архитектуры ботнета Citadel являются доменные имена и IP-адреса командных серверов, поскольку их можно обнаружить и определить их местонахождения; при этом, если они отключены от Интернета, связь ботнетов с зараженными компьютерами конечных пользователей будет прервана (то есть соединение между компьютерами Инфицированного и Командного уровней будет нарушено) и деятельность ботнета обезврежена.

3. Размножение ботнетов Citadel и управление ими

52. После создания бот-кода Citadel, файла конфигурации и командной инфраструктуры Ответчик начинает заражать компьютеры конечных пользователей, превращая их в боты Citadel. Для этих целей Ответчики используют несколько методов. Как правило, заражение компьютеров пользователей происходит с использованием программного средства, которое называется «Загрузчик троянов». Оператор ботнета размещает загрузчик троянов на сайт, который он либо создал сам, либо взломал.

53. Затем Ответчики, как правило, заманивают пользователей Интернета на эти серверы. В качестве одного из методов Ответчики направляют пользователям сети Интернет нежелательные электронные сообщения (спам), включающие ссылки на доменные имена и IP-адреса серверов, содержащих вредоносные программные средства. Содержание письма вводит пользователей сети Интернет в заблуждение, и они нажимают на ссылки, в результате чего без их ведома или согласия на компьютере происходит установка вредоносных программных средства. На рисунке ниже приведен пример такого спама. Здесь видно, что операторы ботнетов Citadel неправомерно используют торговые марки известных компаний и организаций, таких как Microsoft и NACHA, а также

финансовых и других учреждений, с целью обмануть получателя и убедить его, что спам пришел из легитимного источника.



54. После подключения конечного пользователя к веб-сайту, на котором располагается загрузчик Citadel, высоко специализированное программное обеспечение, располагающееся на этом сайте и известное под названием «эксплойт-пакет» (exploit pack), начинает проверку компьютера пользователя на наличие уязвимостей, которые могут быть присущи, например, устаревшей операционной системе без исправлений. В случае обнаружения уязвимости, «эксплойт» устанавливает троян на компьютер пользователя. В результате на компьютере пользователя происходит установка бота Citadel. С этого момента компьютер пользователя и операционная система Microsoft Windows, установленная на компьютере, находятся под тайным контролем оператора ботнета Citadel. Программное обеспечение и компьютер используются для осуществления вредоносной деятельности, которая описывается ниже.

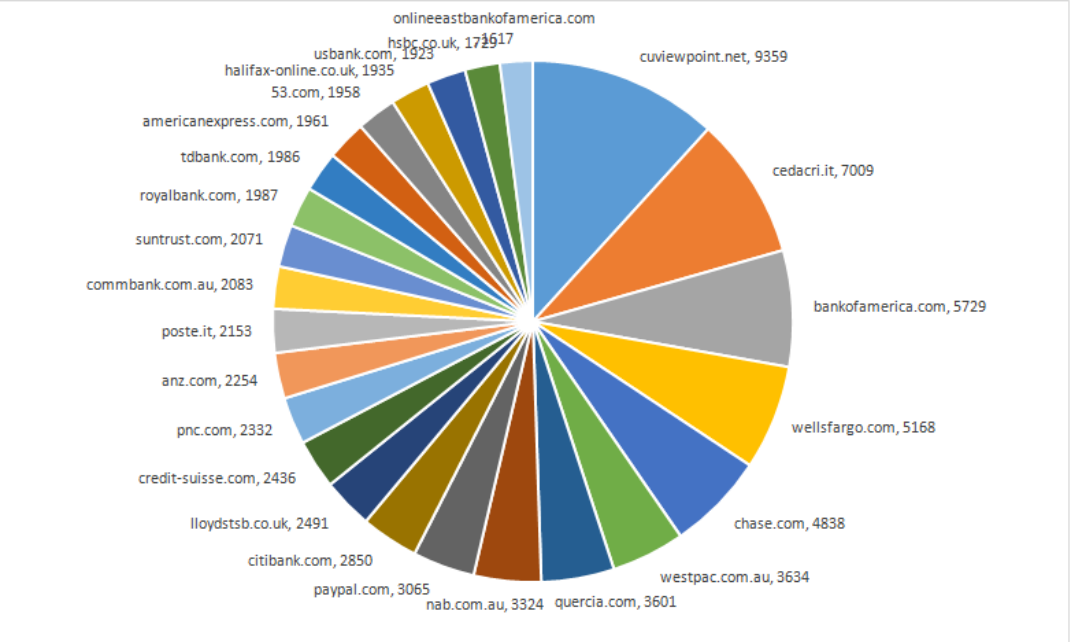
55. После установки бот Citadel связывается с одним или несколькими (до пяти) командными компьютерами в сети Интернет. Эти компьютеры называются «базовыми

доменами», поскольку представляют собой первые домены, контакт с которыми пытается осуществить бот Citadel. Они включены в первоначальный исполняемый файл бота, который генерируется Конструкторским пакетом Citadel. Изучив тысячи ботов Citadel, компания Microsoft составила список этих базовых доменов.

56. Установив контакт с одним из этих базовых доменов, бот Citadel устанавливает с него шифрованный файл конфигурации. В файлах конфигурации Citadel содержится различная информация, которая позволяет управлять работой бота на компьютере пользователя. Путем внесения изменений в файлы конфигурации операторы Citadel могут управлять работой зараженных пользовательских компьютеров.

57. В файлах конфигурации Citadel содержится различная информация, которую бот использует в ежедневном хищении денежных средств. Эта информация включает список обозначенных для атак финансовых учреждений. На зараженном пользовательском компьютере бот Citadel отслеживает все соединения пользователя с Интернетом, ожидая того момента, когда пользователь установит соединение с одним из указанных в списке финансовых учреждений. В этот момент бот начинает атаку на учетные записи пользователя с использованием описанных ниже разнообразных приемов.

58. Из рисунка ниже видно, сколько раз каждая из организаций, входящих в 25 финансовых учреждений, наиболее часто подвергающихся атакам Citadel, была указана в перехваченном файле конфигурации из группы нескольких файлов конфигурации, изученных компанией Microsoft. Среди американских финансовых учреждений, наиболее часто становившихся мишенью Citadel, можно назвать Bank of America, Wells Fargo, Chase, Citibank, American Express и U.S. Bank. Штаб-квартира Bank of America находится в городе Шарлотт (штат Северная Каролина).



59. Файл конфигурации Citadel также содержит список командных серверов Citadel для осуществления связи. Бот обращается к командным компьютерам, чтобы загрузить обновленные файлы конфигурации, обновленное ПО и новые модули атак. Кроме того, на эти командные компьютеры бот передает похищенную у пользователя информацию. Замена командных серверов, связь с которыми осуществляют запущенные боты, на новые проводится каждые шесть-восемь недель, что делает инфраструктуру ботнета трудноуловимой.

60. Кроме того, файл конфигурации Citadel содержит информацию, которая не позволяет боту атаковать конечных пользователей или финансовые учреждения на территории России и Украины. Согласно повсеместному убеждению, создатели Citadel включили эту информацию с тем, чтобы ботнеты Citadel не работали в странах, где сами создатели ведут свои операции, позволяя им тем самым оградить себя от преследования местных правоохранительных органов.

4. Защитные механизмы Ботнетов Citadel

61. Компания Microsoft обращается к суду с просьбой о предоставлении средств правовой защиты в том числе и тому, что ботнеты Citadel обладают определенными механизмами защиты, которые позволяют им противостоять мерам технической борьбы с ними. Первый такой механизм – возможность быстрого перехода на совершенно новую командную инфраструктуру в случае выявления операторами Citadel атаки на инфраструктуру ботнета. Поскольку боты обращаются к командным серверам для получения нового файла конфигурации каждые 20 минут и поскольку операторы ботнета могут запустить новые файлы конфигурации по всему миру фактически мгновенно, в случае выявления атаки на существующую командную инфраструктуру операторы имеют возможность быстро перевести боты на новую командную площадку.

62. В качестве дополнительного механизма защиты бот Citadel, запущенный на компьютере конечного пользователя, не дает этому компьютеру устанавливать соединение с сайтами, связанными с антивирусным ПО. Если пользователь пытается установить соединение с сайтом для загрузки антивирусного ПО, Citadel блокирует это соединение. Выявив попытку соединения с антивирусным сайтом, бот Citadel перехватывает контроль над браузером пользователя и перенаправляет браузер. Таким образом, антивирусная программа на компьютере пользователя не получает обновлений и жертва не в состоянии посетить антивирусные или иные сайты компьютерной безопасности, чтобы загрузить инструмент для удаления вируса или получить консультацию по устранению последствий.

B. Ответчики используют Citadel для хищения денежных средств

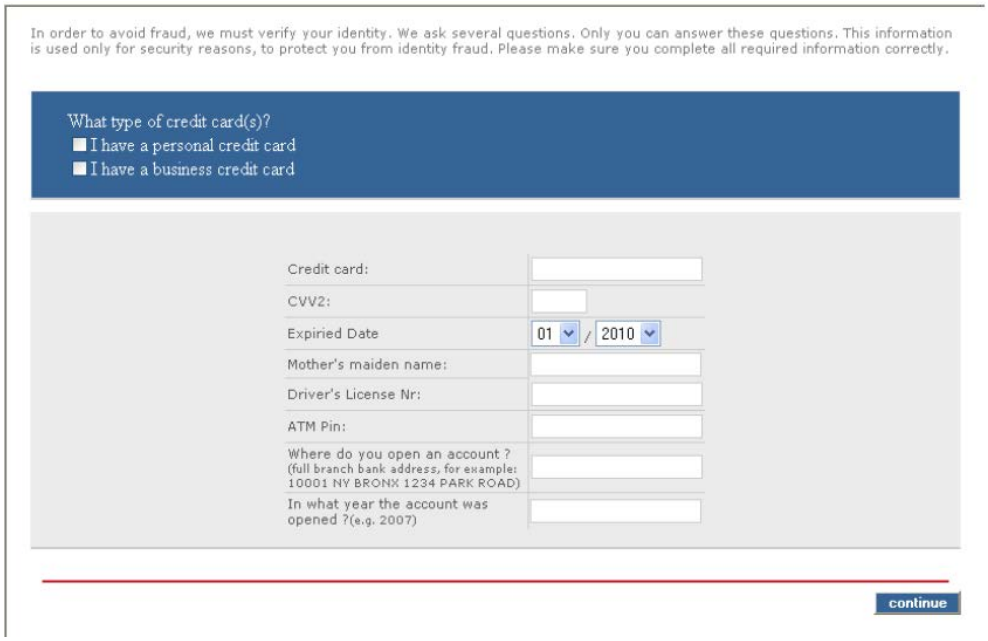
63. Как только ботнет Citadel готов к работе, Ответчики переходят с следующему этапу: хищению денег с финансовых счетов владельцев зараженных пользовательских компьютеров. Атака Citadel начинается с того момента, когда бот Citadel,

действующий на инфицированном компьютере пользователя, определяет, что пользователь устанавливает связь с веб-сайтом финансового учреждения. Определив, что пользователь пытается установить соединение с нужным финансовым сайтом, бот может действовать несколько способами. Во-первых, он может осуществить перехват нажатий клавиш в ходе доступа пользователя к своим финансовым счетам. Бот может записать информацию, представленную на сайте, и даже получить снимки экрана или видео страниц учетной записи пользователя. Затем бот Citadel передает все эту информацию на командный сервер, после чего оператор ботнета может использовать ее для хищения со счетов пользователя или осуществления с похищенной информацией иных противоправных действий.

64. Одним из вариантов этой базовой атаки является использование запущенным на зараженном компьютере пользователя ботом Citadel приема для извлечения у пользователя более конфиденциальной информации. Этот прием называется «веб-инжект». При осуществлении «веб-инжекта» бот Citadel изменяет внешний вид веб-страниц финансового учреждения в браузере конечного пользователя. Бот Citadel, по сути, берет под контроль браузер пользователя и не дает браузеру представить точное воспроизведение сайта, соединение с которым установил пользователь. Вместо этого, бот вынуждает браузер подменить то, что видит пользователь. Это происходит благодаря «ижекту» (встраиванию) дополнительного кода в код веб-сайта, обрабатываемого браузером для выведения в отображаемый формат.

65. Например, если настоящий сайт запрашивает только имя пользователя и пароль, через «веб-инжект» бот может расширить этот запрос и включить в него дополнительную информацию, в том числе номер социального страхования, дату

рождения, девичью фамилию матери и иную подобную информацию, которая обычно используется в ответах на секретные вопросы (для восстановления пароля и т. п.). Citadel может эксплуатировать подобным образом различные браузеры, включая Microsoft Internet Explorer, Google Chrome и Mozilla Firefox. Ниже на рисунке представлены два снимка экрана с примером «веб-инжекта» Citadel. В данном случае оператор бот Citadel пытался получить у жертвы информацию о счете кредитной карты и иную персональную информацию, которая также может использоваться в преступных целях.



66. Ниже на рисунке изображена консоль Citadel, которую оператор ботнета использовал для организации и отображения похищенной информации о кредитных картах и персональной информации (конфиденциальная информация скрыта).

67. Еще одна версия этой атаки – отображение ботом Citadel полностью поддельного веб-сайта финансового учреждения, с которым пользователь пытается установить соединение. С этой целью бот сначала завладевает браузером пользователя и не дает ему установить соединение с настоящим сайтом финансового учреждения. Затем он обращается к командному серверу, загружает шаблон сайта финансового учреждения и отображает его пользователю или устанавливает соединение пользователя с поддельным сайтом. Пользователь, полагая, что он находится на настоящем сайте, выполняет обычные действия. Однако, когда пользователь вводит на поддельном сайте свою настоящую информацию доступа к учетной записи, например, имя пользователя и пароль, оператор ботнета может осуществить доступ к учетным записям пользователя на настоящем сайте.

Измененные сведения учетной записи с настоящего сайта могут быть представлены пользователю, который смотрит на поддельный сайт, чтобы обман не раскрылся, пока хищение на закончено полностью. Для выполнения хищения оператор ботнета может внести изменения в транзакции, осуществленные на реальном сайте, например, путем изменения суммы выведенных денежных средств и изменения информации, касающейся того, куда денежные средства должны быть направлены. Операторы ботнета многократно осуществляют несанкционированное использование торговых марок финансовых учреждений на этих поддельных сайтах интернет-банкинга с целью запутать своих жертв и ввести их в заблуждение. Из-за этого пользователю фактически невозможно определить, что он подвергается атаке.

68. Боты Citadel дают оператору ботнета возможность удаленного доступа и управления зараженным компьютером через Интернет. Оператор ботнета может установить соединение между компьютером пользователя и банком пользователя и при помощи похищенных ранее у пользователя регистрационных данных вывести все денежные средства с его банковских счетов. Вредоносное программное средство специально разработано таким образом, чтобы предоставлять Ответчикам возможность при осуществлении этой вредоносной деятельности скрывать ее следы от конечного пользователя, компании Microsoft, финансовых учреждений и других сайтов-жертв до того момента, когда возвращать контроль за средствами или похищенной информацией пользователям и владельцам этих сайтов уже поздно. Чтобы конечный пользователь оставался в неведении относительно действий, совершаемых удаленно с его компьютером, у бота Citadel, в частности, есть команда отключения звуков (например, «кликов» и сигналов предупреждения), которые компьютер пользователя мог бы издавать при

удаленном управлении.

69. Помимо хищения с финансовых счетов инфицированного пользователя, при заражении Citadel компьютер становится более подверженным заражению другими видами вредоносных программных средств, которые также разработаны с целью хищения денежных средств у конечного пользователя.

C. Ответчики используют компьютеры конечных пользователей для атаки на другие компьютеры в сети Интернет

70. В некоторых версия Citadel предлагается модуль, предназначенный для включения зараженного компьютера в список для осуществления определенного вида атаки, известной под названием распределенная атака типа «отказ в обслуживании» (DDoS-атака). При DDoS-атаке тысячи инфицированных пользовательских компьютеров, подключенных к сети Интернет, по команде оператора ботнета одновременно и непрерывно пытаются установить соединение с целевым сайтом. При этом доступ обычных клиентов к сайту оказывается невозможен. Такие атаки часто используются с целью вымогательства денег у компаний и по соображениям мести. Операторы ботов Citadel также специально рассчитывают DDoS-атаки на финансовые учреждениям по времени, чтобы отвлечь внимание банка от происходящего или произошедшего хищения.

D. Повреждение компьютеров и программного обеспечения Microsoft

71. Само заражение Citadel причиняет вред компании Microsoft и ее клиентам путем повреждения компьютеров клиентов и программного обеспечения, установленного на их компьютерах по лицензии Microsoft. При заражении компьютера конечного пользователя вредоносное программное средства вносит изменения на самом глубоком и чувствительном уровне операционной системы. При заражении компьютера жертвы

исполняемый файл Citadel отключает брандмауэр Windows, удаляет Microsoft Security Essentials и добавляет новых пользователей или расширяет привилегии текущих пользователей. Кроме того, он осуществляет фундаментальные изменения на уровне Реестра Windows. Клиентам Microsoft, чьи компьютеры заражены вредоносным программным средством, причиняется вред этими изменениями Windows, которые искажают обычные утвержденные параметры и функции операционной системы пользователя, дестабилизируют ее и насильно привлекают компьютеры пользователей в ботнет.

72. После того как Citadel заражает, вносит изменения и начинает контролировать операционную систему Windows и браузер Internet Explorer, они перестают функционировать в обычном порядке и становятся орудием обмана и хищения, нацеленным на владельца зараженного компьютера. При этом на них все равно остаются торговые марки Microsoft Windows и Internet Explorer. Безусловно, таким образом предполагается вводить в заблуждение клиентов Microsoft, что и происходит. При этом бренду и торговым маркам Microsoft наносится чрезвычайный ущерб. Клиенты, как правило, не имеют представления о том, что их компьютеры заражены и стали частью ботнета Citadel. Даже если клиентам известно о заражении, им часто не хватает технических ресурсов и навыков для решения проблемы, в результате чего их компьютеры используются в неправомерных целях неопределенно долго. Даже при наличии профессиональной помощи очищение зараженного пользовательского компьютера может быть крайне сложным процессом, отнимающим много времени и нервов.

1. Citadel наносит значительный вред компании Microsoft

73. Компания Microsoft как поставщик операционной системы Windows® и веб-

браузера Internet Explorer® должна внедрять средства защиты с целью предотвращения хищения учетных данных ботнетами Citadel у клиентов, использующих программное обеспечение Microsoft. Кроме того, компания Microsoft выделяет значительные компьютерно-технические и человеческие ресурсы для борьбы с вирусами, распространяемыми Citadel, а также помощи клиентам в оценке зараженности компьютеров и при необходимости их очистке. Недовольство клиентов, вызванное необходимостью решать проблему Ботнета Citadel на своем компьютере, несправедливым образом уменьшает их уважение к Windows и Microsoft и порочит репутацию и престиж компании Microsoft.

2. Ботнеты Citadel наносят значительный вред третьим лицам и населению

74. Citadel наносит вред многочисленным финансовым учреждениям, интересы которых представляют отраслевые группы FS-ISAC (Центр анализа и обмена информацией между финансовыми службами) и Ассоциация американских банкиров, а также организации NACHA, осуществляющей руководство Палатой автоматизированных расчетов между штатами (ACH), компании Microsoft и ее индивидуальным клиентам, информация и денежные средства которых оказываются похищены.

ТРЕБОВАНИЯ О ЗАЩИТЕ ПРАВ

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №1
Нарушение Закона о мошенничестве с использованием компьютеров и злоупотреблении ими, Свод законов США, раздел 18, § 1030

75. Microsoft еще раз заявляет и включает путем отсылки все заявления, содержащиеся в абзацах с 1 по 74.

76. Ответчики (1) сознательно и намеренно осуществили доступ к защищенной операционной системе, программным средствам и компьютерам Microsoft; (2) сознательно

и умышленно осуществили доступ к защищенным компьютерам клиентов Microsoft; (3) осуществили доступ к указанным защищенным компьютерам без наличия полномочия или в масштабах, превышающих границы любого полномочия, и сознательно способствовали передаче программы, информации, кода и команд, в результате чего умышленно без полномочия причинили ущерб защищенным компьютерам (Свод законов США, раздел 18, § 1030(a)(5)(A)) и умышленно без полномочия осуществили доступ к защищенным компьютерам, в результате чего причинили ущерб и убытки (Свод законов США, раздел 18, § 1030(a)(5)(C)).

77. Действия ответчиков причинили убытки компании Microsoft, составившие в течение одного года по крайней мере 5 тыс. долларов США.

78. Компании Microsoft понесла убытки в результате действий Ответчиков.

79. Microsoft обращается с требованием о принятии обеспечительных мер и взыскании реальных убытков и штрафных санкций в соответствии со Сводом законов США, раздел 18, §1030(g) в размере, который будет установлен в ходе судебного процесса.

80. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №2
Нарушение Закона о контроле над активным распространением незапрашиваемой порнографии и рекламы (CAN-SPAM), Свод законов США, раздел 15, § 7704

81. Microsoft еще раз заявляет и включает путем отсылки все заявления, содержащиеся в абзацах с 1 по 80.

82. Компания Microsoft предоставляет услуги доступа к сети Интернет.

Microsoft дает пользователям возможность осуществлять доступ к контенту, в том числе оригинальному, электронной почте и другим интернет-услугам.

83. Ответчики инициировали передачу по электронной почте массового спама, представляющего собой коммерческие электронные сообщения, через компьютеры, используемые во внешней торговле и коммуникациях и торговле и коммуникациях между штатами, на тысячи и миллионы компьютеров, которые также используются во внешней торговле и коммуникациях и торговле и коммуникациях между штатами и являются «защищенным компьютерам», согласно определению в Своде законов США, раздел 18, § 1030(e)(2)(B).

84. Посредством рассылки сообщений Ответчики инициировали передачу на защищенные компьютеры коммерческих сообщений электронной почты, которые содержали ложные по существу или вводящие в заблуждение сведения о заголовках, в нарушение Свода законов США, раздел 15, § 7704(a)(1).

85. Ответчики инициировали передачу на защищенные компьютеры коммерческих сообщений электронной почты, обладая реальными или подразумеваемыми в достаточной мере знаниями о том, что темы сообщений с большой вероятностью могут ввести получателей в заблуждение относительно содержания или предмета сообщения, в нарушение Свода законов США, раздел 15, § 7704(a)(2).

86. Ответчики передали на защищенные компьютеры коммерческие сообщения электронной почты, которые не содержали действующего обратного адреса электронной почты или иных интернет-механизмов, позволяющих получателю связаться с Ответчиками и сообщить о своем желании отказаться от получения сообщений от Ответчиков в дальнейшем, в нарушение Свода законов США, раздел 15, § 7704(a)(3).

87. Ответчики инициировали передачу на защищенные компьютеры коммерческих сообщений электронной почты, которые не имели: (a) четкого и видимого указания на то, что сообщение носит рекламный характер или является предложением услуг; (b) четкого и видимого уведомления о праве отказаться от получения сообщений в будущем; (c) действующего фактического адреса отправителя, в нарушение Свода законов США, раздел 15, § 7704(a)(5).

88. Нежелательная массовая рассылка сообщений электронной почты осуществлялась Ответчиками в рамках систематической схемы, которая не включала в себя явное указания обратного адреса электронной почты, посредством которого получатели могли бы направить отправителю ответ с просьбой в будущем больше не направлять коммерческие электронные сообщения получателю.

89. Действиями Ответчиков компании Microsoft был непосредственно нанесен ущерб в размере, который будет установлен в ходе судебного процесса.

90. Согласно Своду законов США, раздел 15, § 7706(g)(1)(B), Microsoft имеет право либо на возмещение фактических убытков, либо на возмещение, предусмотренное законодательными актами (в зависимости от того, какая сумма больше).

91. В соответствии с имеющими сведениями, действия Ответчиков были умышленными и сознательными, что дает компании Microsoft право на получение увеличенного возмещения убытков, согласно Своду законов США, раздел 15, § 7706(g)(3)(C).

92. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до

тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №3
Нарушение закона о защите информации, передаваемой через электронные системы связи , Свод законов США, раздел 18, § 2701

93. Microsoft повторяет и включает путем отсылки все обвинения, содержащиеся в разделах с 1 по 92.

94. Лицензионная операционная система Windows и программа Internet Explorer компании Microsoft, а также компьютеры клиентов Microsoft, на которых работает это программное обеспечение, представляют собой средства, через которые пользователям и клиентам Microsoft предоставляется услуга электронной коммуникации.

95. Ответчики сознательно и умышленно осуществили доступ к операционной системе Windows, программе Internet Explorer и компьютерам, на которых они работают, без наличия полномочия или в масштабах, превышающих границы любого полномочия, предоставленного компанией Microsoft или любой другой стороной.

96. Благодаря этому несанкционированному доступу, Ответчики имели доступ, получили, изменили и (или) препятствовали законному, санкционированному доступу к телеграфным и электронным сообщениям, в числе прочего к электронными сообщениями, которые на тот момент еще находились в электронном хранении в операционной системе Windows и программе Internet Explorer компании Microsoft, а также в компьютерах, на которых работает это программное обеспечение.

97. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

98. Действиями Ответчиков компании Microsoft был непосредственно нанесен и

все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №4

Нарушение торговой марки, предусмотренное Законом о защите торговых марок – Свод законов США, раздел 15, § 1114 *и далее.*

99. Microsoft повторяет и включает путем отсылки все обвинения, содержащиеся в разделах с 1 по 98.

100. Ответчики использовали торговые марки Microsoft в торговле между штатами.

101. Ботнеты Citadel генерируют и используют контрафактные копии торговых марок Microsoft в поддельных нелицензированных версиях операционной системы Windows, программы Internet Explorer и (или) в поддельных веб-сайтах и спам-сообщениях, в том числе через программные средства, действующие с Командных серверов или через Командные серверы, расположенные на Вредоносных доменах и IP-адресах. Ответчики таким образом могут вызвать путаницу, ошибку или обман в отношении происхождения, поддержки и санкционирования поддельных и нелицензионных версий операционной системы Windows, программы Internet Explorer, поддельных веб-сайтов и спам-сообщений, а также материалов, предлагаемых через поддельные веб-сайты и спам-сообщения.

102. Ложно используя торговые марки финансовых учреждений Microsoft в связи с нежелательной почтой и поддельными веб-сайтами, Ответчики вызвали и могут вызвать путаницу, ошибку или обман в отношении происхождения, поддержки и санкционирования сообщений электронной почты и поддельных веб-сайтов, которые

генерируются и распространяются Ботнетами Citadel. Ответчики таким образом вызвали и могут вызвать путаницу, ошибку или обман в отношении происхождения, поддержки и санкционирования занятий, действий, продуктов и услуг, осуществляемых или предлагаемых Ответчиками и Ботнетами Citadel.

103. Вследствие своего неправомерного поведения Ответчики несут ответственность перед компанией Microsoft за нарушение этого положения Закона о защите торговых марок.

104. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

105. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

106. Неправомерное и несанкционированное использование Ответчиками торговых марок Microsoft для продвижения, рекламирования или продажи продуктов и услуг представляет собой нарушение торговой марки, согласно Своду законов США, раздел 15, § 1114 *и далее*.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №5

Ложное обозначение происхождения, предусмотренное Законом о защите торговых марок – Свод законов США, раздел 15 § 1125(a)

107. Microsoft повторяет и включает путем отсылки все обвинения, содержащиеся в разделах с 1 по 106.

108. Торговые марки Microsoft являются отличительными знаками, которые

ассоциируются с компанией Microsoft и определяют уникальность ее организаций, продуктов и услуг.

109. Посредством Ботнетов Citadel Ответчики осуществляют несанкционированное использование торговых марок Microsoft. Ботнеты Citadel генерируют и используют контрафактные копии торговых марок Microsoft в поддельных нелицензированных версиях операционной системы Windows, программы Internet Explorer и (или) в поддельных веб-сайтах и спам-сообщениях, в том числе через программные средства, действующие с Командных серверов или через Командные серверы, расположенные на Вредоносных доменах и IP-адресах. Ответчики таким образом могут вызвать путаницу, ошибку или обман в отношении происхождения, поддержки и санкционирования поддельных веб-сайтов и спам-сообщений, а также материалов, предлагаемых через поддельные веб-сайты и спам-сообщения.

110. Ложно используя торговые марки Microsoft в связи с поддельными и нелицензионными версиями операционной системы Windows, программы Internet Explorer и (или) спам-сообщениями и поддельными веб-сайтами, Ответчики могут вызвать путаницу, ошибку или обман в отношении происхождения, поддержки и санкционирования поддельных и нелицензионных версий операционной системы Windows, программы Internet Explorer и (или) сообщений электронной почты и поддельных веб-сайтов, которые генерируются и распространяются Ботнетами Citadel. Ответчики таким образом могут вызвать путаницу, ошибку или обман в отношении происхождения, поддержки и санкционирования занятий, действий, продуктов и услуг, осуществляемых или предлагаемых Ответчиками и Ботнетами Citadel.

111. Вследствие своего неправомерного поведения Ответчики несут

ответственность перед компанией Microsoft за нарушение Закона о защите торговых марок, Свод законов США, раздел 15, § 1125(a).

112. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

113. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №6

Ослабление торговой марки, предусмотренное Законом о защите торговых марок – Свод законов США, раздел 15, § 1125(c)

114. Microsoft повторяет и включает путем отсылки все обвинения, содержащиеся в разделах с 1 по 113.

115. Торговые марки Microsoft являются отличительными знаками, которые ассоциируется с компанией Microsoft и определяют уникальность ее организаций, продуктов и услуг.

116. Ботнеты Citadel осуществляют несанкционированное использование торговых марок Microsoft. Вероятно, что через размывание и опорочивание этими действиями Ответчики могут привести к ослаблению торговых марок Microsoft.

117. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

118. Действиями Ответчиков компании Microsoft был непосредственно нанесен и

все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №7
Нарушения Закона о борьбе с организованной преступностью (RICO) – Свод законов США, раздел 18, § 1962(c)

119. Microsoft повторяет и включает путем отсылки все обвинения, содержащиеся в разделах с 1 по 118.

120. Начиная в январе 2012 года или ранее и на момент подачи настоящего Искового заявления Ответчики, Неустановленные лица №№1-82, имели и действительно имеют отношение к Преступному предприятию Citadel и осуществляют деятельность этого предприятия через ряд организованных преступных действий («рэкетирской деятельности»), при этом такое осуществление и действия затрагивают внешнюю торговлю и торговлю между штатами США. В различные числа после января 2012 года или по сей день, на момент подачи настоящего Искового заявления, Ответчики – Неустановленные лица №№2-82 – действительно установили отношения с Преступным предприятием Citadel, а также осуществляют деятельность и принимают участие в деятельности этого предприятия через ряд организованных преступных действий («рэкетирской деятельности»), которые затрагивают внешнюю торговлю и торговлю между штатами США. Ответчики осуществили незаконный ряд организованных преступных действий («рэкетирской деятельности»), в том числе тысячи предикатных актов мошенничества и связанной с ним деятельности в отношении устройств доступа, Свод законов США, раздел 18, § 1029, мошенничества с использованием электронных средств сообщения, Свод законов США, раздел 18, § 1343, и мошенничества в банковской

сфере, Свод законов США, раздел 18, § 1344.

121. Участники Преступного предприятия Citadel объединены общей целью разработки и проведения глобальной ботнет-операции по краже учетных данных, как подробно описано выше.

122. Ответчики сознательно и с намерением совершить мошенничество использовали поддельное устройство доступа в виде ключа продукта Windows XP для установки и активации нелицензированной копии Windows XP с целью создания необходимого программного обеспечения Citadel, работу на котором осуществляют Ответчики. Как подробно указывается выше, Ответчики использовали поддельный код доступа для установки и активации многочисленных нелицензионных копий Windows XP с целью создания общей среды программирования, чтобы другие Ответчики могли изготовлять и компилировать необходимые программные средства Citadel для использование в ботнете Citadel и реализации их общей финансовой цели получения несанкционированных устройств доступа, в нарушение Свода законов США, раздел 18, § 1029(a)(1).

123. Ответчики сознательно и с намерением совершить мошенничество продали и распространили тысячи устройств несанкционированного доступа в виде украденных паролей, номеров банковских счетов и других учетных данных через Ботнеты Citadel, созданные и управляемые Ответчиками. Как подробно указывается в настоящем документе, Ответчики использовали Ботнеты Citadel для хищения, перехвата и получения данной информации об устройствах доступа у десятков тысяч лиц при помощи ложных веб-страниц, а затем использовали эти устройства несанкционированного доступа, полученные с помощью мошенничества, для хищения миллионов долларов со счетов этих

лиц, в нарушение Свода законов США, раздел 18, § 1029(a)(2).

124. Ответчики также сознательно и с намерением совершить мошенничество вступили во владение и продолжают владеть тысячами устройств несанкционированного доступа, полученных с помощью мошенничества, как описано выше, в нарушение Свода законов США, раздел 18, § 1029(a)(3).

125. Ответчики также сознательно и с намерением совершить мошенничество осуществили транзакции с украденными устройствами несанкционированного доступа для получения миллионов долларов с банковских счетов отдельных лиц, в нарушение Свода законов США, раздел 18, § 1029(a)(7).

126. Также, как подробно указывается выше, Ответчики осуществили мошеннический план в отношении десятков финансовых учреждений, предоставив участникам Преступного предприятия Citadel возможность ложно выступать в качестве конкретных клиентов банка и дав им тем самым возможность получить доступ к и похитить денежные средства со счетов этих клиентов, в нарушение Свода законов США, раздел 18, § 1344.

127. Каждое из нарушений Свода законов США, раздел 18, §1029(a) и Свода законов США, раздел 18, § 1344, описанных выше, было осуществлено с использованием интернет-коммуникаций, «передаваемых посредством электронных средств сообщения... в торговле между штатами или внешней торговле», в нарушение Свода законов США, раздел 18, § 1343.

128. Действия Ответчиков причинили и по-прежнему причиняют прямой вред компании Microsoft. Однако компания Microsoft не понесла убытков в связи с заявленным рядом организованных преступных действий («рэкетирской деятельности»).

129. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №8
Сговор с целью нарушения Закона о борьбе с организованной преступностью (RICO) – Свод законов США, раздел 18, § 1962(d)

130. Microsoft еще раз заявляет и включает путем отсылки все заявления, содержащиеся в абзацах с 1 по 129.

131. Начиная в январе 2012 года или ранее и на момент подачи настоящего Искового заявления Ответчики – Неустановленные лица №№1-82 – вступали в сговор по установлению отношений с Преступным предприятием Citadel и осуществлению деятельности этого предприятия через ряд организованных преступных действий («рэкетирской деятельности»), при этом такое осуществление и действия затрагивают внешнюю торговлю и торговлю между штатами США. Ответчики также вступили в сговор с целью осуществления незаконного ряда организованных преступных действий («рэкетирской деятельности»), в том числе тысячи предикатных актов мошенничества и связанной с ним деятельности в отношении устройств доступа, Свод законов США, раздел 18, § 1029, мошенничества с использованием электронных средств сообщения, Свод законов США, раздел 18, § 1343, и мошенничества в банковской сфере, Свод законов США, раздел 18, § 1344.

132. Участники Преступного предприятия Citadel вступили в сговор с общей целью разработки и проведения глобальной ботнет-операции по хищению учетных данных, как подробно описано выше.

133. Действия Ответчиков причинили и по-прежнему причиняют прямой вред

компании Microsoft. Однако компания Microsoft не понесла убытков в связи с заявленным сговором совершить ряд организованных преступных действий («рэкетирской деятельности»).

134. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №9
Неправомерное использование компьютера (Кодекс общих законов штата Северная Каролина § 14-458)

135. Microsoft еще раз заявляет и включает путем отсылки все заявления, содержащиеся в абзацах с 1 по 134.

136. Ответчики осуществили вмешательство, незаконно и без полномочия, в движимое имущество Microsoft и лишили Microsoft владения этим имуществом.

137. Ответчики использовали без полномочия компьютер и (или) компьютерную сеть с намерением удалить, приостановить или иным образом вывести из строя компьютерные данные, компьютерные программы или компьютерное программное обеспечение компьютера или компьютерной сети.

138. Ответчики использовали без полномочия компьютер и (или) компьютерную сеть с намерением вызвать сбой в работе компьютера.

139. Ответчики использовали без полномочия компьютер и (или) компьютерную сеть с намерением изменить или удалить компьютерные данные, компьютерные программы или компьютерное программное обеспечение.

140. Ответчики использовали без полномочия компьютер и (или) компьютерную сеть с намерением причинить материальный ущерб чужому имуществу

141. Действия Ответчиков по управлению Ботнетами Citadel приводят к несанкционированному доступу к операционной системе Windows и программе Interent Explorer компании Microsoft и компьютерам, на которых работает это программное обеспечение, что приводит к несанкционированному вторжению в эти компьютеры, хищению персональной информации, учетных сведений и денежных средств, а также массовой рассылке нежелательной электронной почты на, с и через компьютеры Microsoft.

142. В соответствии с имеющимися сведениями, Ответчики умышленно способствовали такой деятельности и такая деятельность являлась незаконной и несанкционированной.

143. Действия Ответчиков причинили вред компании Microsoft, в том числе в плане времени, финансов и нагрузки на компьютеры Microsoft. Действия Ответчиков повредили деловую репутацию компании Microsoft и уменьшили ценность имущественного права компании Microsoft на ее операционную систему Windows, программу Internet Explorer, компьютеры и программное обеспечение.

144. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

145. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

146. Действия Ответчиков нарушают законы, содержащиеся в Кодексе общих законов штата Северная Каролина §14-458(a)(1), (2), (3) и (4).

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №10
Присвоение имущества

147. Microsoft еще раз повторяет и включает путем отсылки все обвинения, содержащиеся в абзацах с 1 по 146.

148. Ответчики намеренно создали помехи в работе, присвоили себе и осуществили право собственности на движимое имущество Microsoft, без полномочия и основания, изменив состояние данного имущества, и, как следствие, лишив Microsoft возможности владения и пользования своим имуществом.

149. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

150. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №11

Неосновательное обогащение

151. Microsoft еще раз повторяет и включает путем отсылки все обвинения, содержащиеся в абзацах с 1 по 150.

152. Действия Ответчиков, указанные в настоящем Исковом заявлении, составляют неосновательное обогащение Ответчиков за счет компании Microsoft в нарушение общего права.

153. Ответчики без полномочия приобрели доступ к принадлежащим компании

Microsoft и ее клиентам операционной системе Windows и браузеру Interent Explorer компании Microsoft и компьютерам, на которых работает это программное обеспечение.

154. Ответчики без полномочия или лицензии использовали средства, программное обеспечение и компьютеры Microsoft, принадлежащие компании Microsoft, в том числе для рассылки вредоносных программных средств, хищения персональной информации, учетных сведений и денежных средств, поддержки Ботнетов Citadel, нарушения торговых марок Microsoft, массовой рассылки нежелательной электронной почты и обмана пользователей.

155. Действия Ответчиков по управлению Ботнетами Citadel приводят к несанкционированному доступу к операционной системе Windows и браузеру Interent Explorer компании Microsoft и компьютерам, на которых работает это программное обеспечение, к рассылке вредоносных программных средств, хищению персональной информации, учетных сведений и денежных средств, поддержке Ботнетов Citadel, нарушению торговых марок Microsoft, массовой рассылке нежелательной электронной почты и обману пользователей.

156. Ответчики извлекли неосновательную прибыль из несанкционированного и безлицензионного использования принадлежащих Microsoft операционной системы Windows, браузера Internet Explorer, программного обеспечения, компьютеров и (или) интеллектуальной собственности.

157. В соответствии с имеющимися сведениями, Ответчики понимали и осознавали, какую пользу они извлекают из несанкционированного и безлицензионного использования принадлежащих Microsoft операционной системы Windows, браузера Internet Explorer, программного обеспечения, компьютеров и (или) интеллектуальной

собственности.

158. Сохранении Ответчиками прибыли, которую они извлекли из несанкционированного и безлицензионного использования принадлежащих Microsoft операционной системы Windows, браузера Internet Explorer, программного обеспечения, компьютеров и (или) интеллектуальной собственности, не отвечало бы интересам справедливости.

159. Несанкционированное и безлицензионное использование Ответчиками принадлежащих Microsoft операционной системы Windows, браузера Internet Explorer, программного обеспечения, компьютеров и (или) интеллектуальной собственности, нанесло ущерб компании Microsoft.

160. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса. Ответчики также должны вернуть прибыль, полученную незаконным путем.

161. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет.

ТРЕБОВАНИЕ О ЗАЩИТЕ ПРАВ №12
Причинение зловредности

162. Microsoft еще раз повторяет и включает путем отсылки все обвинения, содержащиеся в абзацах с 1 по 161.

163. Ответчики используют свою собственность, собственность компании Microsoft и собственность ее клиентов таким ненадлежащим образом, который нарушает

права собственности Microsoft.

164. В соответствии с имеющимися сведениями, действия Ответчиков были умышленными и необоснованными.

165. Используя программные средства в операционной системе Windows и браузере Internet Explorer компании Microsoft, а также на компьютерах жертв Ответчики умышленно направляют свои зловредные действия против своей собственности и собственности иных лиц, злоупотребляя своей собственностью и собственностью других лиц таким образом, который нарушает права компании Microsoft. Поведение Ответчиков является крайне необоснованным, не несет в себе общественной ценности и, таким образом, представляет собой «зловредность», которая должна быть устранена посредством судебного запрета, требование о котором содержится в настоящем документе.

166. Microsoft обращается с требованием о принятии обеспечительных мер (запрета) и взыскании реальных убытков и штрафных санкций в размере, который будет установлен в ходе судебного процесса.

167. Действиями Ответчиков компании Microsoft был непосредственно нанесен и все еще наносится невозместимый вред, в отношении которого не существует каких-либо соответствующих средств судебной защиты по общему праву и который не прекратится до тех пор, пока на действия Ответчиков не будет наложен запрет и источник вреда не будет устранен.

ПРОСЬБА О СУДЕБНОЙ ЗАЩИТЕ

В СВЯЗИ С ВЫШЕИЗЛОЖЕННЫМ, компания Microsoft обращается к Суду с просьбой.

1. Вынести судебное решение в пользу компании Microsoft и против

Ответчиков.

2. Признать, что действия Ответчиков являются умышленными и что Ответчики действуют со злым умыслом, обманом и притеснением.

3. Вынести предварительный и бессрочный судебные запреты, предписывающие Ответчикам и их должностным лицам, директорам, руководителям, агентам, служащим, сотрудникам и правопреемникам, а также всем физическим и юридическим лицам, действующим по активному соглашению или совместно с ними, прекратить совершать все действия, о которых заявлено в настоящем Исковом заявлении, или причинять вред, о котором заявлено в настоящем Исковом заявлении, а также прекратить оказывать содействие, пособничество и подстрекательство любым физическим или юридическим лицам в совершении или выполнении любых действий, о которых заявлено в настоящем Исковом заявлении, или в причинении вреда, о котором заявлено в настоящем Исковом заявлении.

4. Вынести предварительный и бессрочный судебные запреты, изолирующие и перекрывающие инфраструктуру ботнетов, включая программное обеспечение, которое действует с и через Вредоносные домены и IP-адреса, а также помещающие эту инфраструктуру вне зоны контроля Ответчиков или их представителей и агентов.

5. Вынести судебное решение в пользу компании Microsoft о взыскании фактических убытков в объеме, должны образом компенсирующем компанию Microsoft за действия Ответчиков, о которых заявлено в настоящем Исковом заявлении, и за любой вред, о котором заявлено в настоящем Исковом заявлении, включая, в том числе, проценты и расходы, в размере, который будет установлен в ходе судебного процесса.

6. Вынести судебное решение в пользу компании Microsoft о возвращении

незаконно присвоенной прибыли.

7. Вынести судебное решение в пользу компании Microsoft о взыскании увеличенных убытков, убытков в показательном порядке и убытков, определяемых особыми обстоятельствами дела, в размере, который будет установлен в ходе судебного процесса.

8. Вынести судебное решение в пользу компании Microsoft о возмещении расходов на адвокатские гонорары и юридические услуги.

9. Принять любые другие меры судебной защиты, которые Суд посчитает справедливыми и обоснованными.

Дата: 29 мая 2013

Подпись: _____

Нил Т. Блумфильд
№ в реестре коллегии адвокатов
штата Северная Каролина 37800

Юридическая фирма
Moore & Van Allen PLLC
100 North Tryon Street
Suite 4700
Charlotte, NC 28202-4003
Телефон: +1-704-331-1084
Факс: +1-704-409-5660
Email: neilbloomfield@mvalaw.com

Адвокаты из других фирм:

Габриэль М. Рэмзи
(ходатайство о допуске (*pro hac vice)* на рассмотрении)
Адвокат истца Корпорации Microsoft

Юридическая фирма
Orrick, Herrington & Sutcliffe LLP
1000 Marsh Road
Menlo Park, CA 94025
Телефон: (650) 614-7400
Факс: (650) 614-7401
Email: gramsey@orrick.com

Джеффри Л. Кокс
(ходатайство о допуске (*pro hac vice)* на рассмотрении)
Адвокат истца Корпорации Microsoft

Юридическая фирма
Orrick, Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104-7097
Телефон: (206) 839-4300
Факс: (206) 839-4301
Email: jcox@orrick.com

Джеймс М. Хсиао
(ходатайство о допуске (*pro hac vice)* на рассмотрении)
Адвокат истца Корпорации Microsoft

Юридическая фирма
Orrick, Herrington & Sutcliffe LLP
777 South Figueroa Street
Suite 3200
Los Angeles, CA 90017-5855
Телефон: (213) 612-2449
Факс: (213) 612-2499
Email: jhsiao@orrick.com

Адвокаты истца