

**В ОКРУЖНОМ ФЕДЕРАЛЬНОМ СУДЕ США
В ЗАПАДНОМ ОКРУГЕ ШТАТА ПЕНСИЛЬВАНИЯ**

СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ)		
)		
Истец,)	Гражданский иск №	14-0685
)		
против)	ПРИНИМАЕТСЯ В	ПОЛУЧЕНО
)	<i>ОДНОСТОРОННЕМ</i>	27 МАЯ 2014 г.
ЕВГЕНИЯ МИХАЙЛОВИЧА БОГАЧЕВА,)	<i>ПОРЯДКЕ, БЕЗ</i>	СЕКРЕТАРЬ КАНЦЕЛЯРИИ,
и др.)	<i>РАЗГЛАШЕНИЯ</i>	ФЕДЕРАЛЬНЫЙ ОКРУЖНОЙ СУД
)		ЗАПАДНЫЙ ОКРУГ ШТАТА
)		ПЕНСИЛЬВАНИЯ
Ответчики.)		

**ВРЕМЕННЫЙ СУДЕБНЫЙ ЗАПРЕТ И ПРИКАЗ ОБ УСТАНОВЛЕНИИ
ОСНОВАНИЙ**

Правительство США, выступая истцом, подало заявление с просьбой об
(док. № 3)
обеспечении иска в соответствии с томом 18 Свода законов США, §1345 и §2521, на
основании того, что обвиняемые нарушили положения §1343, §1344 и §2511, указанные в
томе 18 Свода законов США. Правительство также подало одностороннее ходатайство с
целью получения временного судебного запрета и приказа об установлении оснований,
(док. № 4)
призванного обосновать отказ в выдаче обеспечительных мер согласно правилу 65(b)
Федеральных гражданско-процессуальных норм и тому 18 Свода законов США,
§1345(a)(1) и §2521.

**УСТАНОВЛЕННЫЕ ФАКТЫ И СДЕЛАННЫЕ СУДОМ ЮРИДИЧЕСКИЕ
ВЫВОДЫ**

Рассмотрев материалы, заявление, доказательства и меморандум, поданные в
поддержку ходатайства правительства о выдаче временного судебного запрета, приказа об
установлении оснований и других мер вспомогательного обеспечения, юридического
меморандума в поддержку иска ("Юридический меморандум"), а также сопроводительное
заявление, суд настоящим констатирует следующие факты и делает нижеуказанные

юридические выводы:

1. Данный суд обладает юрисдикцией по предмету этого дела и имеет достаточное количество оснований полагать, что он будет обладать юрисдикцией над всеми сторонами данного дела. Исковое заявление указывает требование, на основании которого можно применять санкции к обвиняемым согласно тома 18 Свода законов США, §1345 и §2511.

2. Существует достаточное количество оснований полагать, что обвиняемые занимались и, скорее всего, занимаются действиями или поступками, которые являются нарушением тома 18 Свода законов США, §1343, §1344 и §2511. Поэтому вполне вероятно, что решение по настоящему делу будет принято в пользу правительства.

3. Существует достаточное количество оснований полагать, что если приказ данного суда, устанавливающий ограничения и запреты к обвиняемым, не будет принят, обвиняемыми будет нанесен непосредственный и непоправимый вред, вызванный продолжающимися нарушениями §1343, §1344 и §2511 тома 18 Свода законов США. Доказательства, указанные в Юридическом меморандуме и сопроводительном заявлении правительства, указывают на то, что правительство скорее всего получит в суде подтверждение своего утверждения о том, что обвиняемые нарушают нормы §1343, §1344 и §2511, указанные в томе 18 Свода законов США, в следствие того что они:

- a. умышленно заражают вредоносными программами ("вредоносная программа") сотни тысяч компьютеров с целью похищения банковской и другой идентификационной сетевой информации из зараженных компьютеров и использования этих компьютеров в бот-сети "Gameover Zeus" (сеть других зараженных компьютеров,

контролируемая обвиняемыми);

- b. используют вредоносную программу "GameOver Zeus" для перехвата сообщений потерпевших не имея разрешения на это;
- c. используют идентификационные данные, похищенные с помощью вредоносной программы "GameOver Zeus" для получения доступа к банковским счетам потерпевших и мошеннического перевода денежных средств;
- d. умышленно заразили более 100 000 компьютеров в США вредоносной программой "Cryptolocker" - так называемой "программой, требующей выкупа", которая шифрует важные файлы пользователей, а затем требует выкуп за возвращение файлов в читаемую форму.

4. Существует достаточное количество оснований полагать, что продолжение таких действий могут нанести непоправимый ущерб как физическим лицам, так и компаниям, находящимся на территории США. Кроме того, существует также достаточное количество оснований полагать, что обвиняемые будут продолжать принимать участие в указанных противоправных действиях, если они не будут немедленно остановлены на основании приказа, выданного данным судом.

5. На основании доказательств, изложенных в Юридическом меморандуме и сопроводительном заявлении правительства, а также других улик, существует вероятность того, что правительство сможет доказать следующее: обвиняемые выполняют действия, которые нарушают законодательство США и причиняют вред членам сообщества, и обвиняемые продолжают совершать свои незаконные действия, не взирая на наличие четких признаков нанесения ими вреда членам сообщества.

6. Существуют достаточные основания полагать, что предоставление обвиняемым предварительного уведомления об этом иске приведет к непосредственной и непоправимой помехе для возможности получения эффективного окончательного постановления данного суда. На основании доказательств, изложенных в Юридическом меморандуме и сопроводительном заявлении правительства, существует достаточное количество оснований полагать, что если обвиняемые будут заранее предупреждены об этом иске, они перенесут свои серверы и/или инфраструктуру управления и контроля, изменят кодировку своих вредоносных программ или осуществят иные меры, призванные затруднить или сорвать запланированное правительством противодействие (в случае предварительного ознакомления с действиями правительства).

7. Запрос правительства о предоставлении обеспечительных мер *в одностороннем порядке* не является результатом какого-либо отсутствия обоснованности в действиях правительства. Наоборот, он основан на сути незаконного поведения обвиняемых. Поэтому, в соответствии с федеральным гражданско-процессуальным кодексом ст. 65(b), наличие веских оснований и интересы правосудия требуют того, чтобы данный приказ был предоставлен без предварительного уведомления обвиняемых и, соответственно, чтобы правительство было освобождено от обязанности предоставить обвиняемым предварительное уведомление о заявлении правительства.

8. Правительство продемонстрировало наличие веских оснований полагать, что обвиняемые направляли свою противозаконную деятельность на физических лиц и компании, расположенные в западном округе штата Пенсильвания, так как, среди всего прочего, они заразили вредоносными программами "Gameover Zeus" и "Cryptolocker" многие компьютеры в данном районе и использовали идентификационную информацию,

похищенную вредоносной программой "Gameover Zeus" для получения несанкционированного доступа к банковским счетам потерпевших, находящихся в данном округе.

9. Правительство продемонстрировало наличие веских оснований полагать, что для немедленного прекращения наносимого обвиняемыми ущерба необходимо прекратить заражение компьютеров программами "Gameover Zeus" и "Cryptolocker" обвиняемыми и коммуникацию с существующими компьютерами, зараженными программами "Gameover Zeus" и "Cryptolocker".

10. Правительство продемонстрировало наличие веских оснований полагать, что обвиняемые использовали и будут в дальнейшем использовать адреса доменов, которые указаны в Приложении "А", для совершения правонарушений, указанных в §1343, §1344 и §2521 том 18 Свода законов США, при использовании вредоносной программы "Gameover Zeus". Существует достаточное количество оснований полагать, что для немедленного прекращения противозаконной деятельности обвиняемых и предотвращения нанесения дальнейшего ущерба физическим лицам и компаниям, находящимся на территории США, необходимо немедленно для каждого текущего и потенциального домена обвиняемых (которые указаны в Приложении "А") выполнить следующие действия: 1) сделать его недоступным для обвиняемых; и 2) перенаправить его на следующие адреса серверов: `nsl.kratosdns.net` и `ns2.kratosdns.net`.

11. Существуют достаточные основания полагать, что обвиняемые использовали и будут в дальнейшем использовать адреса доменов, которые указаны в Приложении "В" для совершения правонарушений, изложенных в §1343 тома 18 Свода законов США при использовании блокирующей вредоносной программы "Cryptolocker". Существуют

достаточные основания полагать, что для немедленного прекращения противозаконной деятельности обвиняемых и предотвращения нанесения дальнейшего ущерба физическим лицам и компаниям, находящимся на территории США, каждый из текущих и потенциальных доменов обвиняемых, которые указаны в Приложении В, необходимо немедленно сделать недоступным.

12. Существуют достаточные основания полагать, что обвиняемые использовали и будут в дальнейшем использовать адреса в доменной группе ".ru", указанные в Приложении "С", для совершения правонарушений указанных в §1343, §1344 и §2521 тома 18 Свода законов США при использовании вредоносной программы "Gameover Zeus" и правонарушений, указанных в §1343 тома 18 Свода законов США при использовании вредоносной программы "Cryptolocker". Существует достаточное количество оснований полагать, что для немедленного прекращения противозаконной деятельности обвиняемых и предотвращения нанесения дальнейшего ущерба физическим лицам и компаниям, находящимся на территории США, каждый из текущих и потенциальных доменов обвиняемых в зоне ".ru", которые указаны в Приложении "С", необходимо немедленно сделать недоступными.

13. Существуют достаточные основания для выдачи разрешения на вручение поданных в данном деле документов, с которых данным судом был снят гриф секретности, а также любых открытых приказов суда, принятых в ответ на такие документы, как указано ниже, учитывая существующие обстоятельства и необходимость быстрых действий. Нижеуказанные способы вручения документов, обеспечивающие соблюдение должных процедур, соответствуют требованиям федерального гражданско-процессуального кодекса ст. 4(f)(3) и обоснованно считаются достаточными для предоставления обвиняемым

уведомления:

- a. С помощью курьерской почты, отправленной на домашний адрес обвиняемого г-на Богачева в г. Анапа, Российская Федерация; и
- b. С помощью электронной почты, отправленной на электронный адрес, который используется обвиняемым г-ном Богачевым и обвиняемым, использующим псевдоним Chingiz 911, как указано в "Заявлении специального агента Питерсона";
- c. С помощью электронной почты, отправленной на электронные адреса, указанные регистрационными субъектами всех действующих доменных адресов на Интернете, которые используются обвиняемыми в настоящее время для осуществления контроля за программами вредоносного программного обеспечения, известными под названиями "Gameover Zeus" и "Cryptolocker"; и
- d. С помощью публикации на Интернете, на веб-сайтах Департамента юстиции и Федерального бюро расследований.

Истец обязан быстро подать подтверждение о вручении документов через электронную систему подачи материалов для обеспечения выполнения требований параграфа 13.

ВРЕМЕННЫЙ СУДЕБНЫЙ ЗАПРЕТ И ПРИКАЗ ОБ УСТАНОВЛЕНИИ ОСНОВАНИЙ

В СВЯЗИ С ВЫШЕИЗЛОЖЕННЫМ ИЗДАЕТСЯ ПРИКАЗ о том, что обвиняемым, их представителям и иным лицам, которые активно сотрудничают или действуют с ними, временно запрещается использовать вредоносные программы или коды, призванные выполнять какие-либо махинации с использованием электронных средств, банковские махинации, или участвовать в несанкционированном перехвате электронной связи и, в частности, запрещается управлять, контролировать или осуществлять связь с программными обеспечениями, известными под названием "Cryptolocker" и "GameOver Zeus" (другое название - "Peer to Peer Zeus"), на любых компьютерах, не являющимися собственностью обвиняемых.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что правительство должно установить сервер(ы) на замену и другую компьютерную инфраструктуру, как указано в Юридическом меморандуме правительства, которые, действуя совместно с указанными ниже обеспечительными мерами, заменят инфраструктуру обвиняемых по управлению и контролю за бот-сетью "GameOver Zeus" и прервут связи обвиняемых с зараженными компьютерами, находящимися в бот-сети "GameOver Zeus". В соответствии с приказом данного суда о фиксации подключений и запросов, правительство уполномочено собирать информацию о подключениях, маршрутизации, адресации и обмене сигналами ("DRAS"), поступающую с зараженных компьютеров, подключенных к инфраструктуре, создаваемой в соответствии с данным приказом. Правительство обязано обеспечить, чтобы никакое электронное содержание или другая информация, не относящаяся к DRAS, не собирались с компьютеров потерпевших лиц, подключенных к инфраструктуре устанавливаемой в соответствии с данным приказом.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что Регистраторы доменных имен, указанные в Приложении "Е", должны предпринять нижеуказанные действия в отношении любых доменов, которые указаны в Приложении "А" и которые в настоящее время являются зарегистрированными: (док. № 6-5)

1. Предпринять все соответствующие меры, чтобы переадресовать указанные домены на заменяющее сервера, созданные на основании данного приказа, включая изменение полномочных серверов доменных имен для доменов ns1.kratosdns.net и ns2.kratosdns.net.

2. Предпринять все соответствующие меры для того, чтобы как можно быстрее распространить вышеизложенные изменения в системе доменных имен;

3. Предотвратить какую-либо дальнейшую модификацию или передачу указанных доменов без получения предварительного разрешения со стороны данного суда;

4. Предотвратить передачу любых сообщений, предупреждений или уведомлений любого рода для обвиняемых, или представителей обвиняемых, и предотвратить раскрытия данного приказа до тех пор, пока настоящий приказ больше не будет являться закрытым (за исключением действий, необходимых для исполнения настоящего приказа);

5. Предоставить соответствующую помощь в вопросе исполнения положений настоящего приказа и воздерживаться от выполнения каких-либо действий, которые могут сорвать выполнение данного приказа.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что Регистраторы доменных имен, указанные в Приложении "Е", должны предпринять нижеуказанные действия в отношении любых доменов, которые указаны в Приложении "А" и которые в настоящее

время не зарегистрированы: (док. № 6-5)

1. Предпринять все соответствующие меры для переадресации указанных доменов на заменяющий(е) сервер(а), созданные на основании данного приказа, включая изменение полномочных серверов доменных имен для доменов ns1.kratosdns.net и ns2.kratosdns.net;
2. Предпринять все соответствующие меры для скорейшего распространения вышеизложенных изменений в системе доменных имен;
3. Предотвратить какую-либо дальнейшую модификацию или передачу указанных доменов без получения предварительного разрешения со стороны данного суда;
4. Предотвратить передачу любых сообщений, предупреждений или уведомлений любого рода для обвиняемых, или представителей обвиняемых, и предотвратить раскрытия данного приказа до тех пор, пока настоящий приказ больше не будет являться закрытым (за исключением тех действий, необходимых для исполнения настоящего приказа);
5. Предоставить соответствующее содействие в вопросе исполнения положений настоящего приказа и воздерживаться от выполнения каких-либо действий, которые могут сорвать выполнение данного приказа.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что Регистраторы доменных имен, указанные в Приложении "Е", должны предпринять нижеуказанные действия в отношении любых доменов, которые указаны в Приложении "В" и которые в настоящее время зарегистрированы: (док. № 6-5)

1. Принять все соответствующие меры для того, чтобы указанные адреса доменов были неопределяемыми в системе доменных имен;

2. Предпринять все соответствующие меры для скорейшего распространения вышеизложенных изменений в системе доменных имен;
3. Предотвратить какую-либо дальнейшую модификацию или передачу указанных доменов без получения предварительного разрешения со стороны данного суда;
4. Предотвратить передачу любых сообщений, предупреждений или уведомлений любого рода обвиняемым, или представителям обвиняемых, и предотвращать раскрытие данного приказа до тех пор, пока настоящий приказ больше не будет закрытым (за исключением действий, необходимых для исполнения настоящего приказа).
5. Предоставить соответствующее содействие в вопросе исполнения положений настоящего приказа и воздерживаться от выполнения каких-либо действий, которые могут сорвать выполнение данного приказа.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что Регистраторы доменных имен, указанные в Приложении "Е", должны предпринять нижеуказанные действия в отношении любых доменов, которые указаны в Приложении "В" и которые в настоящее время не зарегистрированы: (док. № 6-5)

1. Принять все соответствующие действия для того, чтобы зарезервировать, заблокировать, или иным образом воспрепятствовать процессу обнаружения адресов указанных доменов;
2. Принять все соответствующие меры для скорейшего распространения вышеизложенных изменений в системе доменных имен (если это необходимо);
3. Предотвратить какую-либо дальнейшую модификацию или передачу указанных доменов без получения предварительного разрешения со стороны данного суда;
4. Предотвратить передачу любых сообщений, предупреждений или

уведомлений любого рода для обвиняемых, или представителей обвиняемых, и предотвратить раскрытия данного приказа до тех пор, пока настоящий приказ больше не будет являться закрытым (за исключением тех действий, необходимых для исполнения настоящего приказа);

5. Предоставить соответствующее содействие в вопросе исполнения положений настоящего приказа и воздерживаться от выполнения каких-либо действий, которые могут сорвать выполнение данного приказа.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что Провайдеры доступа к Интернету, указанные в Приложении "D", должны предпринять соответствующие попытки для выполнения нижеуказанных действий в отношении адресов доменов, которые указаны в Приложении "C": *(док. № 6-4)*

1. Сделать указанные доменные адреса недоступными путем блокирования путей определения адреса этих доменов;
2. Предотвратить передачу любых сообщений, предупреждений или уведомлений любого рода обвиняемым, или представителям обвиняемых, и предотвращать раскрытие данного приказа до тех пор, пока настоящий приказ больше не будет закрытым (за исключением тех действий, необходимых для исполнения настоящего приказа).
3. Не совершать (а также предпринять любые соответствующие шаги для того, чтобы предотвратить совершение) каких-либо действий, направленных на уклонение от выполнения данного приказа обвиняемыми, представителями обвиняемых, или любыми другими лицами; и
4. Предоставить соответствующее содействие в вопросе исполнения положений

настоящего приказа и воздерживаться от выполнения каких-либо действий, которые могут сорвать выполнение данного приказа.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о необходимости вручения копий судебных документов следующим образом:

1. С помощью курьерской почты, отправленной на домашний адрес г-на Евгения Богачева в г. Анапа, Россия;
2. С помощью электронной почты, отправленной на известные электронные адреса обвиняемых Евгения Богачева и "Chingiz 911";
3. С помощью электронной и обычной почты, отправленной на каждый почтовый и электронный адрес, указанный регистрационными субъектами для всех действующих адресов домена программ "Gameover Zeus" и "Cryptolocker"; и
4. С помощью публикации на веб-сайтах Департамента юстиции и Федерального бюро расследований.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что в соответствии с федеральным гражданско-процессуальным кодексом, ст. 65(b), обвиняемые обязаны явиться в данный суд 3 июня 2014 г., в 11:00, чтобы указать причину (если такая существует) того, почему данный суд не должен выдавать обеспечительный запрет (до принятия окончательного решения по поданному против обвиняемых исковому заявлению), который временно запрещает им выполнять действия, указанные в вышеизложенных положениях данного приказа.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что обвиняемые обязаны подать в суд и предоставить в ответ правительству любые письменные свидетельские

показания, объяснения, ходатайства, заключения экспертов или заявления и/или юридические меморандумы до **16:00 2 июня 2014 года через систему электронной подачи материалов**. Правительство имеет право подать в суд ответ или дополнительные объяснения, материалы, письменные свидетельства или заявления и также предоставить их адвокату обвиняемых до **08:00 3 июня 2014 года через систему электронной подачи материалов**.

ИЗДАЕТСЯ ДОПОЛНИТЕЛЬНЫЙ ПРИКАЗ о том, что срок действия данного приказа истекает **3-го** июня 2014 г., в **14:00** (при условии отсутствия дополнительных приказов, изданных данным судом).

Принято сегодня, **28-го** мая 2014 г., в **09:48**.

[подпись]
Судья Артер Дж. Шваб
ФЕДЕРАЛЬНЫЙ ОКРУЖНОЙ СУДЬЯ