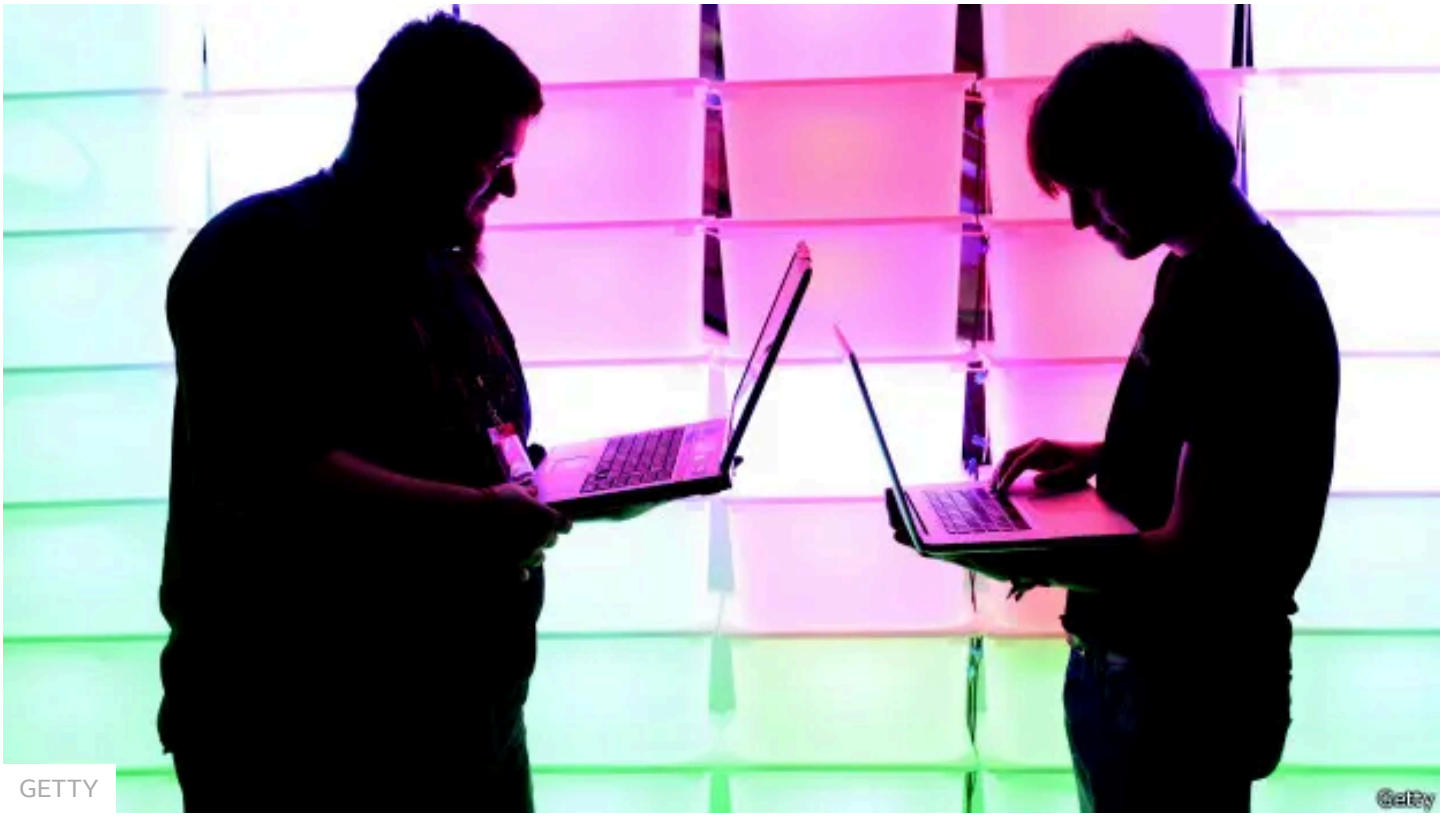
Евгений Богачев: хакер, которого ищет ФБР



GETTY

Программа Cryptolocker распространялась через электронную почту

Владимир Козловский

Русская служба Би-би-си, Нью-Йорк

4 июня 2014

На данный момент против 30-летнего россиянина Евгения Михайловича Богачева и его сообщников, обвиняемых в мошенничестве, похищении личных данных и отмывании денег, заведены в США три дела, одно гражданское в Пенсильвании и два уголовных, в Пенсильвании и Небраске.

Дела были открыты в разное время, но обнародованы разом в начале июня, когда ФБР и спецслужбы еще десятка стран доложили о том, что общими усилиями наконец

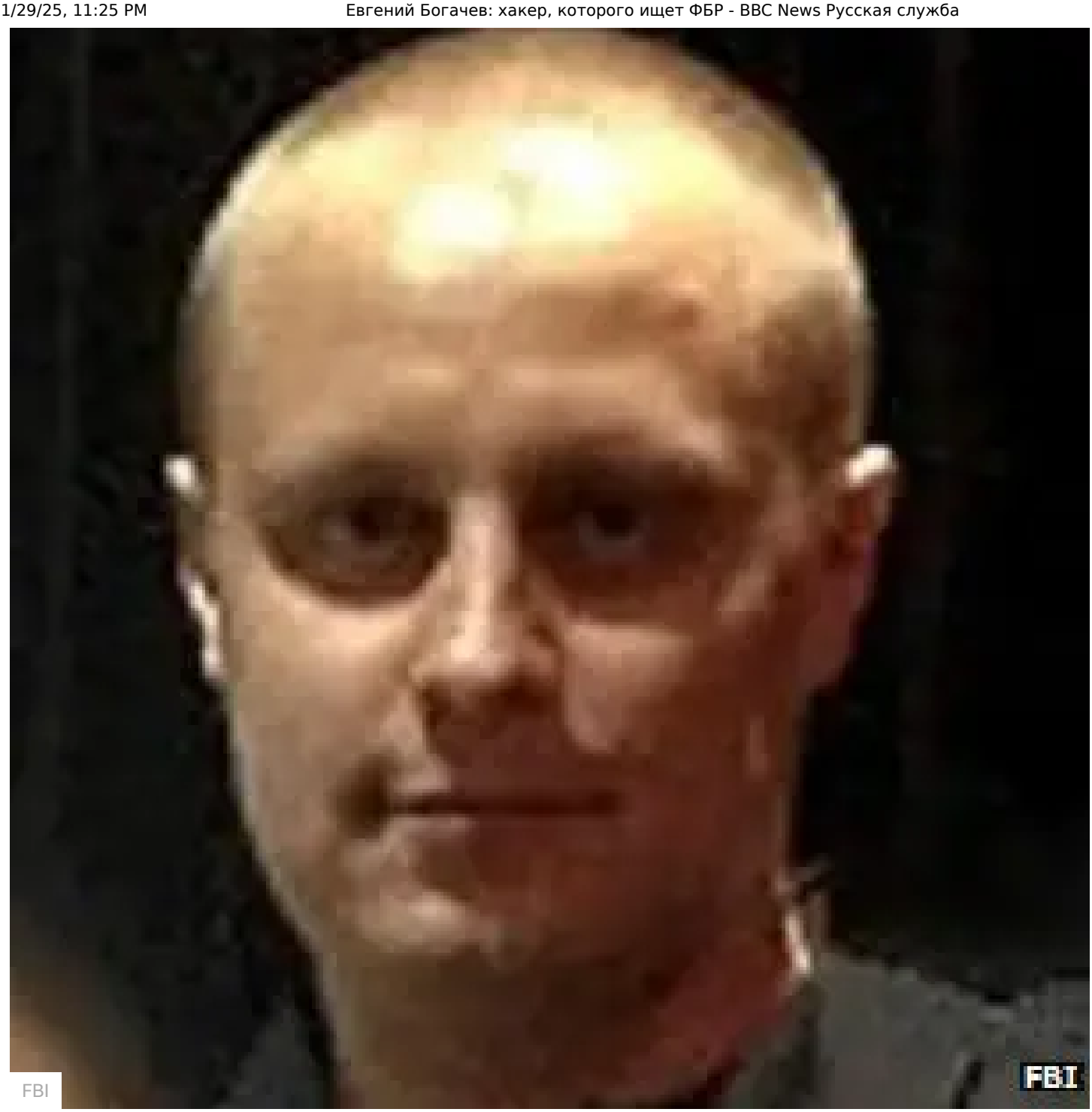
сумели в большой степени обезвредить ботнет GameOver Zeus (GOZ) и распространявшуюся с его помощью вредоносную программу Cryptolocker.

Оба были созданы и использовались в незаконных целях преступной группой, возглавляюшейся Богачевым (ники Slavik, Pollingsoon и Lucky12345), который проживает в Анапе.

Его точный адрес указан в 9-страничном гражданском иске, который власти США возбудили в Западном округе Пенсильвании против Богачева и четырех его сообщников, пока известных следователям лишь под никами Temp Special, Ded, Chingiz 911 и Mr. Kykypyky и проживающими в России и на Украине.

Как утверждают истцы, ответчики пользовались ботнетом GOZ для совершения мошеннических операций и незаконного перехвата чужих электронных сообщений.

Зловредные боты



FBI

Евгений Богачев официально объявлен в розыск ФБР

Ботнет – это группа компьютеров, в которые мошенники тайно запускают зловредные программы с тем, чтобы те выполняли их команды без ведома своих законных владельцев. Зомбированные такие образом компьютеры используются для рассылки спама, внедрения зловредных программ, хищения данных и мошеннических операций.

Как говорится в иске, сообщники Богачева обслуживали под его началом ботнет GOZ. В числе прочего, ботнет выведывал у пострадавших банковские реквизиты, пароли и другую конфиденциальную информацию, а потом переводил деньги с их банковских счетов сообщникам преступной группы.

Например, индейское племя, проживающее в штате Вашингтон, лишилось таким

образом более 277 тысяч долларов, а один флоридский банк – почти 7 млн. долларов.

Троянский конь

GOZ является усовершенствованным вариантом трояна Zeus, который впервые появился в 2007 году. GOZ распространяется с сентября 2011 года и с тех пор причинил убытки, превышающие 100 млн. долларов.

Считается, что преступная группа Богачева заразила от 500 тысяч до миллиона компьютеров по всему миру.

Программа Cryptolocker заражает с помощью ботнета чужие компьютеры и кодирует содержащиеся в них файлы. Потом на экране монитора выскакивает требование в течение 72 часов заплатить кибермошенникам выкуп. В противном случае файлы потерявшего навсегда останутся запертыми сложным кодом, расшифровать который, как говорится в исковом заявлении, практически невозможно.

AFP

GOZ является усовершенствованным вариантом трояна Zeus, который впервые появился в 2007 году

"Преступники по сути дела требовали выкупа за захваченные ими частные имейлы, бизнес-планы, детские домашние задания или семейные фотографии, содержавщиеся в компьютере жертвы", - сказала замминистра юстиции Лесли Колдвелл.

В случае частных лиц затребованный выкуп редко превышает 750 долларов. Другое дело компании, у которых требуют гораздо большие суммы.

Некоторые компании отказываются платить выкуп. Так, одна страховая компания в Питтсбурге использовала дублирующие файлы вместо тех, которые ей намертво закодировала Cryptolocker. Но пока она ликвидировала ущерб, ей пришлось отправить сотрудников по домам и простаивать. Она оценивает свой ущерб в 70 тысяч долларов.

Cryptolocker закодировала оперативно-следственные материалы и фотографии преступников, которые содержались в базе данных полиции массачусетского городка Суонси. Полиция отделалась выкупом в 750 долларов, переведя его шантажистам в онлайновой валюте биткойн, которая позволяет замаскировать получателя денег.

Конец Зевса

Программа орудует с сентября прошлого года и успела заразить более 234 тысяч компьютеров. За первые два месяца ее пребывания в интернете вымогатели получили с ее помощью более 27 млн. долларов.

Раньше всего уголовное дело против Богачева было возбуждено в Небраске. Главным обвиняемым числился Lucky12345, поскольку тогда власти еще не знали, что под этим ником скрывается Богачев, который сейчас уже внесен в главный список киберпреступников, разыскиваемых ФБР.

Возглавлявший следственную бригаду сотрудник ФБР Джеймс Крейг характеризовал Богачева как "кодировщика, который разрабатывал новые коды для взлома банковских систем".

По словам Крейга, кроме Богачева, по этому делу была привлечена целая группа его сообщников, в которую входил, например, гражданин Украины Вячеслав Игоревич Пенчуков, пользовавшийся ником tank и якобы ведавший краденными банковскими реквизитами и "мулами", то есть лицами, на чей счет переводились похищенные деньги.

Разветвленная сеть

31 июля 2009 года сотрудник ФБР допросил некую Рене Мичелли, числившуюся владелицей корпорации Pandora Services LLC, которой были перечислены 29 839 долларов, похищенные с банковского счета компании Doll Distributing. Мичелли сообщила, что искала работу с помощью интернета и устроилась в российскую компанию программного обеспечения под названием "1С".

REUTERS

ФБР провело пресс-конференцию, на которой рассказала о ходе дела

Ее попросили зарегистрировать корпорацию и открыть ей банковский счет. Работодатель объяснил, что в ее обязанности входит получение денежных переводов и перечисление их в иностранные банки.

Другим богачевским "мулом" работала Хайди Нельсон, которая сообщила ФБР, что была уволена в начале 2009 года и пыталась трудоустроиться через интернет. С ней связался человек, представившийся заместителем начальника отдела кадров одной российской компании. По его словам, Нельсон будет должна работать с клиентами в США, периодически получать денежные переводы и потом отправлять деньги в Россию.

Другим фигурантом этого дела был проживавший на Украине Иван Викторович Клепиков, он же petrOvich в интернете. ФБР называет его "системным администратором, ведавшим техническими аспектами преступной схемы".

Жителем Украины был и Алексей Дмитриевич Брон, он же thehead и якобы "финансовый менеджер преступной операции". Считается, что он ведал переводом денег через онлайновую систему Webmoney.

Обвинямый Алексей Тихонов проживал в России и был известен в сети как kusanagi. Он якобы занимался разработкой новых кодов для взлома банковских закромов.

Евген Кулибаба проживал в Великобритании, пользовался ником jonni, якобы находил новых "мулов" и отмывал деньги мошенников в Англии, где он сейчас находится под стражей.

Юрий Коваленко жил там же и тоже арестован британской полицией. Он был известен под ником jtkO и якобы поставлял "мулов" Кулибабе.

В России проживал обвиняемый, который значится в судебных документах как Aqua, пользовался таким же ником и тоже ведал "мулами".

Наконец, по делу проходил житель Украины, пользовавшийся ником Mricq. ФБР характеризует его как разработчика кодов, применявшихся для проникновения в банковские системы.

Давнее дело ФБР

По словам фэбээровца Крейга, Богачев и его сообщники "заражали тысячи бизнес-компьютеров программами, которые похищали пароли, номера счетов и другую информацию, необходимую для того, чтобы войти в онлайновые банковские счета и затем использовать похищеннную информацию для кражи миллионов долларов".

Как можно понять из судебного документа за подписью следователя Крейга, который увлекательно описывает попытки выяснить имя человека, скрывающегося под ником Lucky12345, 14 августа 2013 года некий интернет-провайдер предоставил ФБР данные о счете на имя Евгения Богачева и его телефонный номер.

Информация провайдера включала адреса компьютеров, с которыми связывался Богачев, и время этих соединений. Дальнейшее было делом техники.

Как явствует из судебных докуменов, ФБР завербовало некоего осведомителя, хорошо знакомого с деятельностью Богачева, и идентифицировало ряд вебсайтов типа Visitcoastweekend, на которых Богачев общался со своими сообщниками.

"GameOver Zeus является самым изощренным ботнетом, который когда-либо пытались нейтрализовать ФБР и наши союзники", - замечает замдиректора этого ведомства Роберт Андерсон.

"Богачев – это поистине преступник XXI века, который совершает по всему миру киберпреступления одним нажатием на клавишу", - заявил на пресс-конференции в Вашингтоне замминистра юстиции США Джеймс Коул.

В ходе операции под кодовым обозначением "Tovar" с ФБР сотрудничали спецслужбы Украины, Канады, Франции, Люксембурга, Голландии и Великобритании. Украинцы, например, 7 мая изъяли компьютеры, управлявшие ботнетом в Киеве и Донецке.

По словам Колдвелл, к субботе вирус Cryptlocker больше не функционировал, а ботнет GOZ был сильно поврежден.

Коул сообщил, что США обсуждали с Россией вопрос о выдаче Богачева, но эксперты отмечают, что Москва резко возражает против судов над своими гражданами за границей, особенно в последнее время. Поэтому оглашение предъявленнных Богачеву обвинений, скорее всего, лишь предостережет его против опрометчивых выездов за границу.

Читайте также

США обвинили хакера из России в кибермошенничестве

Выходцы из бывшего СССР в поле зрения властей США

Шпионский скандал: Китай требует разъяснений у США

Главное

«Люди не осознают масштабов»: что потеряет Украина от заморозки Трампом программ USAID

3 часа назад

Пентагон лишил охраны и допуска к секретам генерала Милли, назвавшего Трампа фашистом

3 часа назад

Требование репараций или выдачи Асада? Чем закончились первые переговоры России с новыми властями Сирии

29 января 2025

Не пропустите

Олигарх против Левиафана: почему Илон Маск решил «вернуть Европе былое величие»

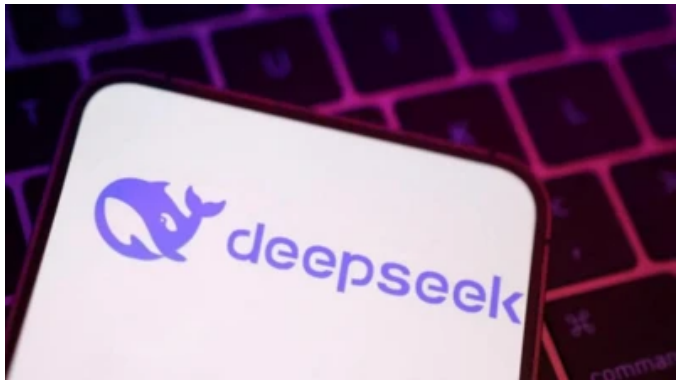
29 января 2025

Может ли ситуация на фронте выйти из-под контроля? Объясняет «Военное время»

29 января 2025

«Исходя из возможностей». Почему Россия так сильно отстает в космосе от США и Китая

28 января 2025



«Момент „Спутника"». Как китайский чатбот DeepSeek встряхнул западную индустрию искусственного интеллекта и чем это ей грозит

28 января 2025

Между перезагрузкой и санкциями. Чего ждать Грузии от Трампа

28 января 2025

Как Абрамович сэкономил на налогах, «арендуя» свои яхты: расследование Би-би-си

«Большой ребенок». Как жил и погиб обвиненный в проведении «туров для геев» Андрей Котов

27 января 2025

Пережившие Холокост: Европа забывает уроки Аушвица

27 января 2025

Самое популярное

1 Требование репараций или выдачи Асада? Чем закончились первые переговоры России с новыми властями Сирии

2 Первые шаги Трампа на посту президента: от заморозки международной помощи до рейдов против нелегальных мигрантов

3 Второй с начала года массированный удар дронов по России. Главное

6 Премьер-министр Сербии ушел в отставку. Причиной стали протесты из-за гибели людей на вокзале

7 В грунте астероида Бенну найдены «кирпичики жизни»

8 Дональд Трамп примет Биньямина Нетаньяху в Белом доме. Это его первый иностранный гость

4 **Участник беспорядков на Капитолии застрелен полицейским через несколько дней после помилования**

5 **Трамп подписал указы о запрете политики разнообразия и инклюзивности и о двух гендерах в армии США**

9 **Роман Абрамович, возможно, должен Великобритании миллиард фунтов стерлингов неуплаченных налогов — расследование Би-би-си**

10 **Колумбия вывезла депортированных из США мигрантов на своих самолетах и без наручников. Это и есть компромисс с Трампом?**