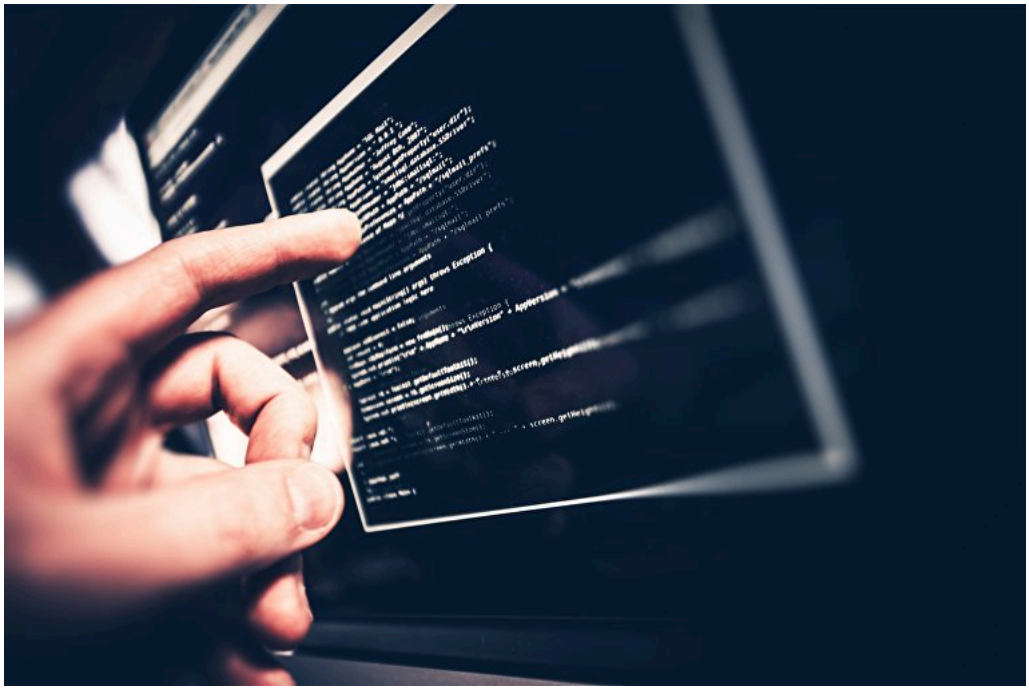
Опубликовано: 23 МАРТА 2017

Охота на русского хакера

Утром 30 декабря, на следующий день после того, как Барак Обама ввел санкции против России за вмешательство в выборы, проходившие в США в 2016 году, Тильманн Вернер (Tillmann Werner) сидел за завтраком в Бонне, что в Германии. Он намазал джем на ломтик ржаного хлеба, налил себе чашку кофе и, устроившись за столом у себя в столовой, стал проверять, что пишут в Twitter.



© FOTOLIA, TOMASZ ZAJDA

Новости о санкциях появились накануне вечером, поэтому Вернер, аналитик фирмы CrowdStrike, работающей в сфере кибербезопасности, все еще уточнял подробности. Открыв по ссылке официальное заявление, Вернер увидел, что Белый дом выбрал в качестве объектов адресных санкций изрядный список русских фамилий и организаций — две спецслужбы, четырех высокопоставленных работников разведки, 35 дипломатов, три компании из сферы информационных технологий и двух хакеров. О деталях говорилось, в основном, расплывчато. Затем Вернер остановился и перестал просматривать текст. Его взгляд привлекло одно имя, числившееся в списке: Евгений Михайлович Богачев.

Дело в том, что Вернер знал о Евгении Богачеве довольно много. Он точно, в технических подробностях знал, как Богачев ухитрялся на протяжении многих лет безнаказанно грабить и держать в страхе мировые финансовые системы. Он знал, каково с ним бороться.

Но Вернер понятия не имел, какую роль мог играть Богачев в хакерских атаках во время избирательной кампании. Богачев не был похож на других, кто попал под санкции — он был грабителем банков. Возможно, самым активным и успешным грабителем в мире. «А он-то почему в этом списке?» — задумался Вернер.

1. Омаха

Война Америки с самым известным российским киберпреступником началась весной 2009 года, когда спецагент Джеймс Крэйг (James Craig), новичок в оперативном отделении ФБР в Омахе, штат Небраска, начал заниматься парой странных электронных краж. Крейг — бывший морской пехотинец с квадратной челюстью — был агентом всего полгода, но начальство все равно подключило его к этому делу из-за его предыдущего опыта — на протяжении многих лет он работал ИТ-специалистом в ФБР. Одним из его прозвищ в колледже было «тихий компьютерщик».

Главным потерпевшим в том деле была дочерняя структура гигантской компании First Data, занимающейся обработкой операций по кредитным картам, которая потеряла в мае того года 450 тысяч долларов. Вскоре после этого произошла кража 100 тысяч долларов со счета клиента банка Омахи First National Bank of Omaha. Как заметил Крейг, странным было то, что кражи, судя по всему, осуществлялись с собственных IP-адресов потерпевших с использованием их логинов и паролей. Проверив их компьютеры, он обнаружил, что они были заражены одной и той же вредоносной программой, которая называется «троян Zeus».

В кругах специалистов по интернет-безопасности, как выяснил Крейг, Zeus был известен. Это вредоносное ПО, появившееся в 2006 году, прославилась среди преступников и экспертов в области безопасности как шедевр — универсальная программа, работающая бесперебойно, четко и эффективно. Его автором был «фантом». Он был известен только в интернете под никами «Славик», lucky12345 и под десятком других имен.

Троян Zeus заражал компьютеры довольно обычным способом. Скажем, через фальшивые электронные письма со ссылками или поддельные уведомления посылочной службы об отгрузке товара, которые обманным путем заставляли получателя скачать файл. Но как только файл оказывался в компьютере, вредоносная программа Zeus давала хакерам возможность делать что угодно. Они могли «перехватывать» сайты и использовать регистратор работы клавиатуры для записи логинов, паролей и пин-кодов. Хакеры могли даже модифицировать страницы регистрации, чтобы запрашивать дополнительную ценную информацию — например, девичью фамилию матери или номер социальной страховки. Этот прием называется атакой «человек в браузере». Пока вы заходите на казалось бы безопасные сайты, вредоносная программа модифицирует страницы до их загрузки, перекачивая ваши данные и данные о состоянии вашего счета. Только при входе с другого компьютера вы понимаете, что

деньги исчезли.

К тому времени, когда Крейг начал свое расследование, Zeus превратился в наиболее эффективную и предпочтительную подпольную цифровую вредоносную программу, став своего рода пакетом приложений Microsoft Office для онлайн-мошенничества. Славик был довольно редким персонажем в мире тех вредоносного ПО — он был настоящим профессионалом. Он регулярно обновлял код трояна Zeus, проводя предварительное тестирование его функций. Его продукт был бесконечно гибким, его варианты были оптимизированы для различных видов атак и целей. Компьютер, зараженный вредоносной программой Zeus, можно было даже включить в бот-сеть из зараженных компьютеров, которыми можно управлять вместе для рассылки спама, атак отказа в обслуживании или рассылки новых фальшивых сообщений и писем для дальнейшего распространения вредоносной программы.

Но незадолго до того, как Крейг принял свое дело в разработку в 2009 году, Славик начал менять тактику. Он начал готовить онлайн — преступников из числа приближенных, обеспечив группу избранных одним из вариантов своей программы под названием Jabber Zeus. Она была снабжена протоколом мгновенного обмена сообщениями Jabber, позволяющим группе поддерживать связь и координировать атаки — как в случае с двумя кражами в Омахе. Вместо того чтобы проводить общие операции по инфицированию компьютерных сетей, они начали выбирать в качестве объектов своих атак исключительно корпоративных бухгалтеров и людей, имеющих доступ к финансовым системам.

Поскольку Славик все больше приобщался к организованной преступности, он резко сократил свой бизнес по розничной торговле вредоносными программами. В 2010 году он объявил в сети о своем «уходе на покой» и затем выпустил то, что аналитики в области безопасности стали называть Zeus 2.1. Это была улучшенная версия его трояна, защищенная ключом шифрования, с помощью которого Славик фактически привязывал каждую копию к конкретному пользователю — с ценником свыше 10 тысяч долларов за копию. Теперь Славик имел дело только с элитой — группой амбициозных преступников.

«Мы понятия не имели, насколько большим было это дело, — говорит Крейг. — Масштабы деятельности этих ребят были феноменальными». К ним начали обращаться другие организации, потерявшие деньги и ставшие жертвами мошеннических операций со счетами. Их было очень много. Крейг понял, что сидя за своим столом в пригороде Омахи, он охотится за хорошо организованным международным преступным сообществом. «Появлялись все новые и новые пострадавшие», — рассказывает Крэйг. По масштабам это дело затмило все другие киберпреступления, которыми ФБР занималось раньше.

2. Jabber Zeus

Первый крупный прорыв Крейга в расследовании этого дела произошел в сентябре 2009 года. С помощью некоторых отраслевых экспертов он идентифицировал сервер в Нью-Йорке, который, судя по всему, играл некую роль в преступном сообществе, использовавшем Zeus. Он получил ордер на обыск, и группа криминалистов ФБР скопировала данные с сервера на жесткий диск, а затем отправила его в Небраску. Когда инженер в Омахе проанализировал результаты, он на мгновенье застыл в изумлении. На жестком диске были записи десятков тысяч строк мгновенных сообщений чатов на русском и украинском языках. Взглянув на Крэйга, инженер сказал: «У тебя теперь есть их Jabber-сервер».

Это были все цифровые операции преступников — «сценарий» всего дела. Фирма Mandiant, работающая в сфере кибербезопасности, отправила в Омаху на несколько месяцев инженера, чтобы помочь расшифровать код программы Jabber Zeus, а ФБР начало направлять туда агентов из других регионов в командировки сроком от одного до трех месяцев. Лингвисты со всей страны энергично взялись за расшифровку записей. «Проблемой был сленг», — говорит Крэйг.

В сообщениях говорилось о сотнях жертв, об их украденных учетных данных, размещенных в разных файлах на английском языке. Крейг и другие агенты начали обзванивать организации, сообщая им, что они стали жертвами кибермошенничества. Он узнал, что некоторые предприятия уже уволили сотрудников, которых они заподозрили в кражах, не понимая, что компьютеры этих людей были заражены вредоносными программами, а их логины — украдены.

Кроме того, дело вышло за пределы виртуального мира. Однажды в 2009 году в Нью-Йорке в местное отделение ФБР пришли три молодые женщины из Казахстана и рассказали странную историю. Женщины приехали в Соединенные Штаты в поисках работы и оказались замешанными в довольно любопытной схеме. Мужчина отвозил их в местный банк и приказывал им заходить внутрь и открывать новый счет. Они должны были объяснять кассиру, что они — студентки, приехавшие в страну на лето. Через несколько дней мужчина приказывал им снова пойти в банк и снять со счета все деньги. Немного денег они оставляли себе, а остальные отдавали ему. Агенты проанализировали полученную информацию и пришли к выводу, что женщины были «денежными мулами»: их работа состояла в том, чтобы обналичивать средства, которые Славик со своими товарищами воровали с настоящих банковских счетов.

К лету 2010 года в Нью-Йорке следователи предупредили руководство банков в регионе и посоветовали обращать внимание на подозрительные выплаты, попросив в этих случаях вызвать агентов ФБР. В результате удалось обнаружить десятки «мулов», снимавших со счетов десятки тысяч долларов. Большинство из них были студентами или вновь прибывшими иммигрантами с Брайтон-Бич. Одна женщина объяснила, что после неудачной попытки устроиться на работу в продуктовый магазин она стала «мулом». Агенту она сказала: «Я могла либо пойти заниматься стриптизом, либо выполнять эту работу». А один мужчина объяснил, что за ним заезжают в 9 утра, до 3 часов он снимает деньги со счетов, а потом проводит остаток дня на пляже. В большинстве случаев суммы, снимаемые со счетов, составляют около девяти тысяч долларов — как раз такие, по которым не требуется составлять отчетность в соответствии с федеральным законом. «Мулы» обычно получали 5%-10% от общей суммы, и еще определенная доля причиталась вербовщику. Остальные деньги отправлялись за границу.

Соединенные Штаты оказались лишь одним из рынков, на которых воцарилось это многонациональное (как вскоре поняли следователи) мошенничество. Представители властных структур проследили похожие методы работы «мулов» в Румынии, Чехии, Великобритании, на Украине и в России. В общей сложности следователи могли бы связать с действиями этой группы кражи на сумму приблизительно 70-80 миллионов долларов, но они полагают, что общая сумма гораздо больше.

Банки подняли шум и потребовали от ФБР положить конец мошенничеству и остановить финансовые потери. За лето агенты Нью-Йорка начали выходить на высокопоставленных вербовщиков и организаторов этой системы в США. В одном из отелей в Милуоки в 11 часов вечера по наводке были задержаны двое молдаван; один подозреваемый в Бостоне пытался скрыться от полицейской облавы в квартире своей подруги, и его пришлось снимать с пожарной лестницы.

Между тем, дело Крейга в Омахе продвинулось, и агенты вышли на более масштабную банду, использовавшую вредоносную программу Jabber

Zeus. ФБР и Министерство юстиции нацелились на территорию на востоке Украины в районе Донецка, где, судя по всему, жили несколько руководителей преступной группировки Jabber Zeus. Алексей Брон, известный в интернете как thehead («главарь»), специализировался на переводе денег группировки по всему миру. Иван Викторович Клепиков, работавший под ником petr0vich, руководил в группировке работой в сфере информационных технологий, в его ведении были веб-хостинг и доменные имена. А Вячеслав Игоревич Пенчуков, известный местный ди-джей, который действовал под ником tank («танк»), управлял всей схемой и в руководстве занимал второе место после Славика. «Организованность этих совсем молодых людей (им было по 20 с чем-то лет) поразила бы любую компанию из списка Fortune 100», — говорит агент ФБР Джеймс Крейг. Участники преступной группировки тратили свои огромные прибыли на дорогие автомобили (Пенчуков имел слабость к престижным BMW и Porsche, а Клепиков предпочитал спортивные седаны Subaru WRX). И в чатах они постоянно обсуждали шикарный отдых в Турции, Крыму, Арабских Эмиратах.

К осени 2010 года ФБР было готово ликвидировать сеть. Когда чиновники в Вашингтоне организовали резонансную пресс-конференцию, Крейг ехал в поезде и 12 часов трясся в вагоне, добираясь через всю Украину в Донецк, где он встретился с агентами украинской службы безопасности, чтобы провести обыск в домах у «танка» и «петровича». Стоя в гостиной дома у «Петровича», украинский агент попросил Крейга показать свой значок ФБР. «Покажи ему, что это не только мы», — настаивал он. Крейг был ошеломлен тем, что он увидел: хакер, одетый в фиолетовый бархатный смокинг, выглядел невозмутимым, когда агенты обыскивали его захламленную квартиру в панельном доме советского образца; его жена стояла на кухне с ребенком на руках и смеялась, разговаривая со следователями. «И это та банда, за которой я гоняюсь?» — удивлялся Крэйг. Обыск продолжался до поздней ночи, и Крейг вернулся в гостиницу в 3 часа ночи. Он уехал в Омаху, забрав с собой почти 20 терабайтов изъятых данных.

Проведя 39 арестов в четырех странах мира, следователям удалось ликвидировать преступную сеть. Но главные игроки скрылись. Один из главных в США вербовщиков «мулов» сбежал на запад, скрываясь буквально из-под носа следователей в Лас-Вегасе и Лос-Анджелесе, после чего все-таки покинул страну, спрятавшись в грузовом контейнере. Но — что более важно — Славик, сам организатор всех преступлений, оставался инкогнито. Следователи предполагали, что он живет в России. И однажды в онлайн-чате они увидели его запись, в которой он сообщал, что женат. Кроме этого никаких сведений у них не было. В тексте официального обвинения его как создателя вредоносных программ Zeus называли, используя его интернет-псевдоним. Крейг даже не знал, как выглядит его главный подозреваемый. «У нас есть тысячи фотографий „танка", „петровича", но фотографий Славика мы ни разу не видели», — говорит Крейг. Вскоре следы преступника исчезли даже в сети. Славик, кем бы он ни был, ушел в тень. И после семи лет преследования киберпреступников, действовавших с помощью троянской программы Jabber Zeus, Крейг начал заниматься другими делами.

3. Игра не закончена

Примерно через год после того, как ФБР уничтожило сеть Jabber Zeus, небольшая группа аналитиков, работающих в сфере кибербезопасности, которые выявляют в сети вредоносные программы и бот-сети, стали замечать, что появилась новая версия вредоносной программы Zeus. Исходный код этой программы был выложен в сеть в 2011 году (может, намеренно, а может, и нет), в результате чего Zeus фактически стал открытым проектом, и после чего появилась масса новых версий. Но та версия, которая бросилось в глаза аналитикам, была совершенно другой. Она была более мощной и более сложной, в частности, в вопросе методов сборки бот-сетей.

До этого в большинстве бот-сетей использовалась веерная система, то есть, хакер программировал один командный сервер для передачи команд непосредственно на зараженные компьютеры, называемые «зомби». Потом армию этих «зомби» можно задействовать для рассылки спама, распространения вредоносных программ или проведения атак отказа в обслуживании на представляющие интерес сайты. Правда, из-за такой веерной системы бот-сети были уязвимыми, и сотрудникам правоохранительных органов или специалистам по безопасности было относительно легко их ликвидировать. Если существовала возможность выбить командный сервер из сети, захватить его или лишить хакера возможности поддерживать с ним связь, то, как правило, можно было и уничтожить бот-сеть.

Однако эта новая версия программы Zeus зависела от традиционных командных серверов и взаимодействия равноценных зомби-машин, из-за чего уничтожить его чрезвычайно трудно. В зараженных компьютерах хранился постоянно обновляемый список других зараженных систем. И если одно устройство обнаруживало, что его связь с командным сервером прервана, оно использовало сеть с равноценными узлами для поиска нового командного сервера.

Сеть, по сути, была разработана с нуля, чтобы обеспечить ей неуязвимость; как только от интернета отключался один командный сервер, владелец бот-сети мог просто создать где-нибудь еще новый сервер и перенаправить сеть с равноценными компьютерами на него. Новая версия программы получила название GameOver Zeus — в честь одного из имен ее файлов gameover2.php. Это название, естественно, стало поводом для черного юмора. Среди экспертов по безопасности ходила такая шутка: «Как только эта гадость заразит ваш компьютер, игра для вашего банковского счета закончена».

Насколько можно было сказать, программу GameOver Zeus контролировала группа элитных хакеров — и ее руководителем был Славик. Он появился снова, став гораздо сильнее, чем когда-либо. Новую преступную группировку Славика стали называть «бизнес-клубом» (Business Club). В сентябре 2011 года в сообщении, распространенном среди членов группировки (в котором им представили новый набор онлайн-инструментов для организации денежных переводов и «мулов»), прозвучали теплые слова приветствия в адрес новых избранников Славика: «Мы желаем вам всем успешной и плодотворной работы».

Основной задачей группы Business Club (как и группировки Jabber Zeus) было ограбление банков, что она и делала с еще более циничной изобретательностью, чем ее предшественница. Схема была многоплановой: во-первых, вредоносная программа GameOver Zeus похищала банковские учетные данные пользователя, перехватывая их, как только кто-нибудь входил с зараженного компьютера в личный кабинет. Затем члены группировки Business Club снимали деньги со счета в банке и переводили их за рубеж на другие счета, которые они контролировали. После завершения кражи, группа осуществляла с помощью своей мощной бот-сети DDoS-атаку на эти финансовые учреждения, чтобы отвлечь сотрудников банка. А также чтобы клиенты банка не смогли понять, что все деньги с их счетов сняты, пока эти средства не будут переведены в другой банк. Шестого ноября 2012 года ФБР наблюдало за тем, как с помощью программы GameOver было украдено (в рамках одной транзакции) 6,9 миллиона долларов, затем проведена DDoS-атака, в результате которой компьютерная система банка была парализована в течение нескольких дней.

В отличие от предыдущей группировки Jabber Zeus, более продвинутая сеть, использовавшая программу GameOver, сосредоточилась на кражах с чужих банковских счетов шести- и семизначных сумм, на фоне чего могло показаться, что кражи из банка в Бруклине совершались дедовскими методами. Теперь преступники использовали взаимосвязанную глобальную банковскую систему против ее же самой, скрывая свои огромные

кражи среди потоков триллионов долларов в рамках законной торговли, ежедневно бурлящих по всему миру. В частности, следователи выявили два региона в дальневосточном Китае, недалеко от российского города Владивосток, из которых «мулы» переводили огромные суммы похищенных денег на счета группировки Business Club. Следователи поняли, что стратегия этой преступной группировки представляет собой эволюционный скачок в сфере организованной преступности. Грабители банков больше не оставляли следов на территории США. Теперь они могли сделать все дистанционно, не вторгаясь в сферу действия законов США. «А это единственное, что необходимо, чтобы действовать безнаказанно», — говорит бывший высокопоставленный сотрудник ФБР Лев Таддео (Leo Taddeo).

4. Остановить утечку денег

Целью преступной группировки были не только банки. Преступники также осуществляли атаки на счета нефинансовых предприятий, больших и малых, некоммерческих организаций и даже физических лиц. В октябре 2013 года группа Славика начала внедрять вирус-вымогатель CryptoLocker — вредоносную программу, шифрующую файлы на зараженном компьютере и вынуждающую владельца заплатить небольшую плату, скажем, 300-500 долларов, чтобы разблокировать файлы. Этот вирус быстро стал любимым инструментом группировки киберпреступников — отчасти потому, что он помогал превратить балласт в прибыль. Проблема при создании широкой бот-сети, предназначенной для масштабного мошенничестве в финансовой сфере, оказывается, состоит в том, что большинство «зомби-компьютеров» не подключаются к солидным корпоративным счетам. Славик и его соратники оказались в ситуации, когда десятки тысяч «зомби-машин» почти всегда простаивали. Хотя с помощью программы-вымогателя особых денег украсть не получается, она позволяет преступникам извлекать выгоду, используя эти зараженные компьютеры, которые в других случаях бесполезны.

Принцип действия вирусов-вымогателей известен примерно с 1990-х годов, но в программе CryptoLocker он является основным. В используемой преступниками из Business Club программе-вымогателе, попадающей в компьютер жертвы, как правило, под видом скромного вложения в электронное письмо, использовалось устойчивое шифрование, и жертвы были вынуждены платить биткоинами. Это было неловко и неудобно, но многие уступали. В ноябре 2013 года руководство отдела полиции в Суонси, штат Массачусетс, не скрывая раздражения, выложило почти 750 долларов, чтобы вернуть «к жизни» один из своих компьютеров. Вирус «настолько сложный и эффективный, что вам приходится покупать эти биткоины, о которых мы никогда не слышали», рассказал в интервью местной газете лейтенант полиции из Суонси Грегори Райан (Gregory Ryan).

В следующем месяце специалисты фирмы Dell SecureWorks, работающей в сфере безопасности, подсчитали, что в том году вирусом CryptoLocker во всем мире было заражено около 250 тысяч машин. Один из аналитиков отследил 771 вынужденный выкуп, благодаря которым группа Славика получила чистую прибыль на общую сумму 1,1 миллиона долларов. «Он был одним из первых, кто понял, как отчаянно люди будут пытаться вернуть доступ к своим файлам, — говорит о Славике Бретт Стоун-Гросс (Brett Stone-Gross), бывший в то время аналитиком компании Dell SecureWorks. — Он не заламывал цену, но заработал много денег и придумал новый вид онлайн-преступлений».

По мере того, как сеть GameOver продолжала набирать силу, ее операторы продолжали добавлять в свой арсенал новые способы получения доходов — сдавая свою сеть в аренду другим преступникам, чтобы те распространяли вредоносные программы и спам. Или осуществляли такие мошеннические проекты, как клик-фрод, когда «зомби-машины» заставляют приносить доход с помощью щелчка мышью по объявлениям на фальшивых сайтах.

Расходы, которые приходилось нести банкам, предприятиям и частным лицам, компьютерные системы которых были заражены программой GameOver, с каждой неделей росли. Из-за краж компания могла запросто лишиться годовой прибыли или еще больших сумм. В США список жертв был разнообразным — от регионального банка в Северной Флориде до племени американских индейцев в штате Вашингтон. Поскольку вредоносная программа массово проникала в компьютерные системы в частном секторе, она все чаще становилась объектом особого внимания специалистов в области обеспечения личной кибербезопасности. Затраченные суммы были ошеломляющими. «Я не думаю, что кто-то имеет представление об общих масштабах — на фоне одной кражи пяти миллионов долларов сотни мелких краж кажутся несущественными, — объясняет специалист по безопасности из голландской фирмы Fox-IT Майкл Сэнди (Michael Sandee). — Когда банк подвергается массированным атакам — по 100 транзакций в неделю — вы перестаете обращать внимание на конкретные вредоносные программы и отдельные атаки. Вам просто нужно остановить утечку средств».

Многие пытались. В период с 2011 по 2013 годы аналитики в области кибербезопасности и различные фирмы трижды пытались пресечь деятельность сети, распространявщей GameOver Zeus. Три европейских аналитика в сфере безопасности объединились и весной 2012 года предприняли первый штурм. Славик легко отбил их атаку. Тогда, в марте 2012 года, отдел Microsoft по кибербезопасности обратился в суд с гражданским иском против сети, в надежде на то, что Служба маршалов США организует обыски в центрах обработки данных в штатах Иллинойс и Пенсильвания, где находились командные серверы, распространявшие вредоносную программу Zeus, и начнет судебный процесс в отношении 39 лиц, предположительно связанных с сетями Zeus (Славик был в списке первым). Но план Microsoft подорвать деятельность распространителей GameOver реализовать не удалось. Зато Славик получил информацию о том, что известно следователям о его сети, и смог скорректировать свою тактику.

5. Наступление

Люди, ведущие борьбу с бот-сетями — это маленькая группа амбициозных инженеров и аналитиков, называющих себя «интернет-дворниками», которые работают, чтобы обеспечить бесперебойную работу сетей в интернете. Одним из членов этой группы является высокий, худощавый немец Тильманн Вернер — аналитик фирмы CrowdStrike, работающей в сфере кибербезопасности — который прославился благодаря своему особому таланту и энтузиазмом. В феврале 2013 года он перехватил управление бот-сетью Kelihos (печально известной тем, что она распространяла вредоносные программы, построенные на спаме о продаже «Виагры»), прямо на сцене во время презентации на крупнейшей конференции по кибербезопасности. Но он знал, что Kelihos — это не GameOver Zeus. Вернер наблюдал за программой GameOver с момента ее создания, поражаясь ее эффективности и стойкости.

В 2012 году он объединился со Стоуном-Гроссом, который всего несколько месяцев назад окончил аспирантуру и жил в Калифорнии, а также с несколькими другими аналитиками, чтобы наметить план и попытаться атаковать GameOver. Работая на двух континентах, в основном в свободное время, эти люди разработали план атаки через онлайн-чат. Они тщательно изучили предыдущий опыт европейских специалистов, выяснив, когда их попытки были неудачными, и целый год готовили свой штурм.

В январе 2013 года они были готовы — запаслись пиццей, предполагая, что им придется вести длительную осаду сети Славика. (Когда вы идете с боем на бот-сеть, говорит Вернер, «у вас есть только один выстрел. Вы либо попадете в цель, либо промахнетесь). Их план состоял в том, чтобы перераспределить работу сети GameOver с равноправными узлами, централизовать ее, а затем перенаправить трафик на новый сервер,

находящийся под их управлением — то есть, сделать то, что называется «нейтрализацией». Этим они надеялись нарушить связь бот-сети со Славиком. И поначалу все шло хорошо. Славик не проявлял никаких признаков борьбы, а Вернер со Стоун-Гроссом наблюдали, как с каждым часом к их «системе нейтрализации» подключается все больше и больше зараженных компьютеров.

В самый разгар своей работы аналитики перехватили управление сетью Славика на 99%, но они упустили из виду важную особенность, которая обеспечивала устойчивость структуры GameOver. Несколько инфицированных компьютеров по-прежнему тайно поддерживали связь с командными серверами Славика. «Мы не учли, что есть второй уровень управления», — говорит Стоун-Гросс. К началу второй недели работы Славику удалось продавить обновленное ПО для всей своей сети и восстановить свой контроль над ней. Аналитики с нарастающим ужасом наблюдали, как в интернете распространяются новая версия GameOver, и пиринговая сеть Славика начинает восстанавливаться. «Мы сразу же поняли, что случилось — мы совершенно не обратили внимания на другой канал связи», — говорит Вернер.

Хитрый план, на подготовку которого ушло девять месяцев, провалился. Славик победил. Во время провокационного онлайн-чата со специалистами польской службой безопасности он злорадствовал по поводу того, что все попытки захватить его сеть оказались тщетными. «Не думаю, что он считает возможным провал его бот-сети», — говорил Вернер. Приунывшие аналитики были готовы предпринять новую попытку. Но им была нужна помощь — из Питтсбурга.

6. Питтсбург

За последние десять лет из отделения ФБР в Питтсбурге звучат самые серьезные государственные обвинения в киберпреступности — в немалой степени благодаря руководителю местного отдела по борьбе с киберпреступностью, бывшему продавцу мебели по имени Кит Мулярски (Keith Mularski).

Импульсивный и общительный агент Мулярски, который вырос недалеко от Питтсбурга, стал чем-то вроде знаменитости среди специалистов по кибербезопасности. Он пришел работать в ФБР в конце 1990-х годов и первые семь лет провел в бюро в Вашингтоне, округ Колумбия, занимаясь делами, связанными со шпионажем и терроризмом. Радуясь возможности вернуться домой в Питтсбург, он в 2005 году стал участником новой программы по обеспечению кибербезопасности, несмотря на то, что не особо разбирался в компьютерах. Мулярски проходил обучение прямо на рабочем месте в ходе двухлетнего секретного расследования, целью которого было выявить в недрах интернет-форума DarkMarket лиц, похищавших личные данные. Действуя под ником Мастер Сплинтер (навеянным сериалом для подростков «Черепашки-ниндзя»), Мулярски ухитрился стать администратором форума DarkMarket и оказаться в центре растущего в сети преступного сообщества. В этой ипостаси он даже чатился со Славиком и «рецензировал» раннюю версию вредоносной программы Zeus. Благодаря его доступу к DarkMarket следователям, в конечном итоге, удалось арестовать 60 человек на трех континентах.

В последующие годы начальник отдела ФБР в Питтсбурге решил активно содействовать борьбе с киберпреступностью — с учетом ее растущего значения. К 2014 году агенты ФБР из отдела Мулярски вместе с другим отрядом, прикомандированным к малоизвестной питтсбургской организации под названием «Национальный криминалистический и учебный союз в сфере кибербезопасности», вели судебные процессы по некоторым из самых серьезных дел по линии Министерства юстиции. Двое из агентов из числа подчиненных Мулярски, Эллиотт Питерсон (Elliott Peterson) и Стивен Лэмпо (Steven Lampo), занимались розыском хакеров, причастных к распространению GameOver Zeus, в то время как их коллеги расследовали дело, которое в итоге позволило предъявить обвинение пяти китайским военным хакерам, которые проникли в компьютерные системы американских корпораций Westinghouse, US Steel и других компаний, действуя в интересах китайской промышленности.

ФБР занималось расследованием деятельности распространителей GameOver уже около года, когда Вернер и Стоун-Гросс предложили объединить усилия с отделом в Питтсбурге с тем, чтобы уничтожить бот-сеть Славика. Если бы они обратились с таким предложением к какой-нибудь другой структуре в правоохранительных органах, ответ, возможно, был бы другим. Сотрудничество властей с представителями этой сферы было относительно редким явлением; было известно, что федералы обычно расследовали дела, связанные с киберпреступлениями, выуживая у специалистов отрасли все, что можно, но информацией с ними не делились. Но команда в Питтсбурге была не как все и имела опыт взаимодействия, и агенты ФБР знали, что эти два аналитика — лучшие в своей области. «И мы ухватились за такую возможность», — говорит Мулярски.

Обе стороны понимали, что для того, чтобы разобраться с бот-сетью, им следует работать на трех фронтах. Во-первых, они должны были выяснить раз и навсегда, кто руководит сетью GameOver (то, что следователи называют «авторством»), и начать уголовное преследование; даже после кражи миллионов долларов, ни ФБР, ни специалисты в сфере безопасности не знали даже имен членов группировки Business Club. Во-вторых, им надо разрушить цифровую инфраструктуру самой сети GameOver — той, в которую проникли Вернер и Стоун-Гросс. И в-третьих, им нужно было вывести из строя физическую инфраструктуру бот-сети, собрав все судебные решения, поручения и другие исполнительные документы, а также заручиться поддержкой других стран, чтобы захватить ее серверы в разных частях планеты. И после того, как все это будет сделано, им понадобились бы партнеры в частном секторе, которые были бы готовы использовать обновления ПО и патчи безопасности для восстановления зараженных компьютеров в тот момент, когда хорошие парни перехватят управление бот-сетью. Не предприняв какого-либо из этих шагов, они, скорее всего, как и до этого, не смогли бы ликвидировать GameOver Zeus.

При этом отдел, возглавляемый Мулярски, начал создавать международное партнерство, делая то, чего власти США никогда не делали. Он заручился поддержкой Национального криминального агентства Великобритании, должностных лиц в Швейцарии, Нидерландов, Украины, Люксембурга и десятка других стран, а также экспертов по безопасности из Microsoft, CrowdStrike, McAfee, Dell SecureWorks и других компаний.

Во-первых, чтобы помочь выяснить личность Славика и заставить разведслужбы заняться преступниками из Business Club, ФБР объединило свои действия с голландской компанией Fox-IT, известной своим опытом в киберкриминалистике. Голландские аналитики приступили к работе по отслеживанию старых логинов и адресов электронной почты, имеющих отношение к группировке Славика, чтобы получить представление о том, как она работала.

Как оказалось, Business Club представлял собой свободный союз, в который входило около 50 преступников, каждый из которых заплатил вступительный взнос, чтобы получить доступ к усовершенствованной панели управления сетью GameOver. Управление сетью осуществлялось через два защищенных паролем британских сайта —Visitcoastweekend.com и Work.businessclub.so, на которых велся подробный учет, был раздел с часто задаваемыми вопросами и ответами, а также предусматривалась «билетная» система решения технических вопросов. Когда следователи получили законное право проникать в сервер группы Business Club, они нашли очень подробный журнал, в котором отслеживались различные текущие махинации группы. «Во всем был виден профессионализм», — рассказывает Майкл Сэнди из компании Fox-IT. В том, что касалось определения конкретных сроков транзакций между финансовыми учреждениями, говорит он, «они, похоже, ориентировались лучше, чем банки».

7. Шпионские программы

Однажды после нескольких месяцев розыскной работы следователи получили от источника в компании Fox-IT наводку — адрес электронной почты, который мог бы их заинтересовать. Это была одна из многих подобных наводок, которые они получили. «У нас было много улик и сведений, — говорит Мулярски. — Но эта привела нас к кое-чему очень важному. Команде удалось отследить связь этого электронного адреса с британским сервером, которым Славик пользовался для управления веб-сайтами группы Business Club. В результате дальнейшей следственной работы и благодаря дополнительным судебным постановлениям власти, в конечном итоге, вышли на российские социальные сети, где адрес электронной почты был привязан к конкретному имени. Владельцем адреса был Евгений Михайлович Богачев. Сначала следователям это имя ни о чем не говорило. Потребовалось еще несколько недель работы, чтобы понять, что оно на самом деле принадлежит «фантому», который изобрел вредоносную программу Zeus и создал группу Business Club.

Оказалось, что Славику 30 лет, и он вел вполне безбедную жизнь в Анапе, российском курортном городе на берегу Черного моря. Судя по фотографиям в интернете, он любит кататься на катере с женой. У супругов есть маленькая дочь. На одной из фотографий Богачев позирует в пижаме леопардовой расцветки, в темных очках и с большим котом на руках. Следственная бригада пришла к выводу, что он написал первую версию программы Zeus, когда ему было всего 22 года.

Но это было не самым поразительным открытием, сделанным голландскими следователями. Продолжая свою аналитическую работу, они заметили, что кто-то из руководства сети GameOver регулярно ищет в десятках тысяч бот-сетей зараженных компьютеров в некоторых странах такую информацию, как адреса электронной почты, принадлежащие офицерам грузинской разведки или руководителям элитных турецких полицейских подразделений, или документы с грифом «Секретно», содержащим секретную информацию Украины. Этот неизвестный также искал секретные материалы, связанные с сирийским конфликтом и торговлей российским оружием. В какой-то момент взорвалась лампочка. «Это команды шпионских команд», — говорит Сэнди.

Программа GameOver была не просто частью сложного вредоносного программного обеспечения, которым пользовались преступники; она была еще и сложным современным средством сбора секретной информации. И насколько (в меру своих возможностей) смогли определить следователи, Богачев был единственным членом группы Business Club, кто знал об этой особенности бот-сети. Похоже, он проводил секретные операции прямо под носом у самых успешных в мире грабителей банков. Агентам ФБР и команде аналитиков из компании Fox-IT не удалось найти конкретных доказательств связи между Богачевым и российскими государственными структурами, но некоторые лица, судя по всему, давали Славику конкретные термины и параметры для поиска в его огромной сети «компьютеров-зомби». Оказалось, что Богачев был русским агентом.

В марте 2014 года следователи могли даже наблюдать, как международный кризис разыгрывается «вживую» внутри снежного шара преступной бот-сети Богачева. Через несколько недель после Олимпиады в Сочи российские войска захватили украинский полуостров Крым и начали действовать с целью дестабилизации на восточной границе Украины. Действуя в соответствии с российской кампанией, Богачев перенаправил часть своей бот-сети на поиск важной в политическом плане информации о зараженных украинских компьютерах — тщательно просматривая секретные сведения, которые могли бы помочь русским предугадать следующие действия своих противников.

Группе следователей удалось создать предварительную теорию и реконструировать историю того, как Богачев постигал азы шпионского ремесла. Несомненная связь с госструктурами помогает объяснить, почему Богачев мог управлять крупной преступной организацией столь безнаказанно, но она проливает новый свет и на некоторые вехи в истории существования сети Zeus. История системы, которую Славик использовал, чтобы запрашивать секретную информацию, начинается приблизительно тогда, когда в 2010 году он инсценировал свой «уход на покой» и сделал доступ к своим программам гораздо более эксклюзивным. Не исключено, что в том году Славик в какой-то момент попал в поле зрения российских спецслужб, и в обмен на разрешение безнаказанно заниматься мошенничеством (разумеется, за пределами России) власти выдвинули определенные требования. Чтобы выполнять эти требования с максимальной эффективностью и в условиях строжайшей секретности, Славик ввел более жесткий контроль над деятельностью своей преступной сети.

Ввиду того, что были обнаружены признаки вероятных связей Богачева с разведслужбами, пришлось пойти на некоторые хитрости при проведении операции по ликвидации сети GameOver — особенно когда встал вопрос о возможности привлечения к сотрудничеству России. Иначе план мог провалиться. Теперь, когда следователи сосредоточили свое внимание на Богачеве, присяжные могли бы, наконец, обвинить его в том, что он был закулисным организатором и руководителем сети распространения GameOver Zeus.

Американские прокуроры всячески старались собрать в гражданских судах документы, необходимые для того чтобы захватить и разрушить эту сеть. «Когда мы на самом деле действовали, у нас работало девять человек — а всего их у нас только 55», — говорит представитель федеральной прокуратуры в Питтсбурге Майкл Комбер (Michael Comber).

На протяжении нескольких месяцев следователи методично ходили к интернет-провайдерам, прося у них разрешения воспользоваться имеющимися прокси-серверами сети GameOver и уверяя, что настал самый подходящий момент для нейтрализации этих серверов и лишения Славика возможности ими управлять. Между тем, Министерство внутренней безопасности, исследовательский центр университета Карнеги-Меллон, а также ряд компаний, занимающихся разработкой антивирусных программ, выразили готовность помочь клиентам получить доступ к их зараженным компьютерам. По мере того, как чиновники координироывли свои действия в Великобритании, США и других странах, между континентами поводились еженедельные селекторные совещания.

К концу весны 2014 года, когда пророссийские силы вели боевые действия на Украине, группа специалистов во главе с США приготовилась к началу штурма сети GameOver. Они уже больше года разрабатывали план уничтожения сети, тщательно анализируя вредоносное ПО, тайно читая сообщения преступников в чатах, пытаясь понять психологию группы, и отслеживая физическую инфраструктуру серверов, обеспечивающую распространение сети по всему миру. На тот момент аналитики знали вредоносную программу лучше, чем сам автор, говорит Эллиотт Питерсон, один из ведущих агентов ФБР, участвовавших расследовании. Мулярски вспоминает, что следователи проверяли все важнейшие модули. Мы можем это делать в соответствии и с уголовным, и гражданским законодательством. Мы можем это сделать и технически», — говорит он. Взаимодействуя с десятками и поддерживая связь с более чем 70 интернет-провайдерами, а также с десятком других правоохранительных органов (начиная Канадой и заканчивая Соединенным Королевством, Японией и Италией), следственная группа была готова начать атаку на преступную сеть в пятницу, 30 мая.

8. Ликвидация

За неделю до атаки началась безумная спешка. Когда Вернер и Стоун-Гросс прибыли в Питтсбург, Петерсон привел их к себе домой, где его дети таращили глаза на Вернера и, разинув рот, слушали его немецкий акцент. За ужином, попивая крафтовое пиво Fathead, они еще раз оценивали предстоящие действия. Они изрядно отставали от плана — код, над которым работал Вернер, еще не был готов, и над ним еще надо было еще долго сидеть. В оставшиеся дни недели и Вернер, и Стоун-Гросс в спешке его дописывали, пока другая группа собирала последние судебные предписания. Другие работали со специальной группой, созданной из представителей двух десятков стран, компаний и консультантов, помогавших в подготовке ликвидации сети GameOver Zeus. Белый дом ознакомили с планом действий, и он ждал результатов. Но казалось, что все трещит по швам.

Например, следователи уже несколько месяцев знали, что бот-сеть GameOver контролируется сервером, находящимся в Канаде. Но потом, за несколько дней до «штурма», они обнаружили, что есть еще один командный сервер на Украине. Осознав это, они очень разволновались. «Если ты даже не в курсе, что существует второй сервер, как ты можешь быть уверенным, что нет еще и третьего», — спрашивал Вернер.

В четверг Стоун-Гросс внимательно обговорил с десятком с лишним интернет-провайдеров процедуры, которым они должны следовать, когда начнется атака. В последнюю минуту один ключевой интернет-провайдер отказался участвовать, опасаясь, что это может вызвать гнев Славика. Затем, в пятницу утром, Вернер со Стоун-Гроссом приехали в свой офис на берегу реки Мононгахелы и узнали, что один из их партнеров, компания McAfee, заранее опубликовала в своем блоге объявление об атаке на бот-сеть под названием «Для Zeus and Cryptolocker „игра закончена"»

После отчаянных звонков с требованием убрать пост, штурм, наконец, начался. Канадские и украинские власти заблокировали командные серверы GameOver, отключив их по очереди от интернета. А Вернер и Стоун-Гросс начали перенаправлять «компьютеры-зомби» в тщательно подготовленные «нейтрализаторы», чтобы поглотить вредный трафик, блокируя тем самым доступ группы Business Club к своим собственным системам. В течение нескольких часов атака не давала результатов, и аналитики пытались понять, где в своем коде они допустили ошибку.

К часу ночи в их «нейтрализаторе» было всего около ста зараженных компьютеров, что было крайне мало, учитывая размеры бот-сети, разросшейся до этого до полумиллиона машин. В конференц-зале за спинами у Вернера и Стоун-Гросса стояла столпа чиновников, буквально заглядывавших через плечо, пока аналитики отлаживали код. «Не хочу на вас давить, но было бы здорово, если бы вы смогли сделать так, чтобы программа заработала», — сказал в какой-то момент Мулярски.

Наконец, к вечеру по питтсбургскому времени трафик, направленный в «нейтрализатор», активизировался. На другом конце планеты Богачев вышел в сеть. Атака помешала его отдыху в конце недели. Возможно, он поначалу об этом не думал, учитывая, что он легко выдерживал и другие попытки перехватить управление его бот-сетью. «Прямо сейчас он прощупывает почву. Он не знает, что мы уже сделали», — вспоминает свои слова Питерсон. В ту ночь Богачев еще раз приготовился к битве — к борьбе за контроль над своей сетью. Он ее протестировал, перенаправил трафик на новые серверы и вычислил, как команда из Питтсбурга будет его атаковать. «Это был рукопашный кибербой, — вспоминает федеральный прокурор Питтсбурга Дэвид Хиктон (David Hickton). — Зрелище было потрясающим».

Членам команды удалось незаметно для Богачева отслеживать каналы его связи и отключить его турецкий прокси-сервер. Затем они наблюдали, как он пытается вернуться в интернет с помощью сервиса анонимизации Tor, отчаявшись получить какую-либо информацию о своих потерях. Наконец, после многочасовых неудачных боев Славик замолчал. Как оказалось, атака была гораздо серьезнее, чем он думал. Питтсбургская команда не выходила из сети всю ночь. «Он, должно быть, понял, что это работают правоохранительные органы. Это не просто атака обычного аналитика», — говорит Стоун-Гросс.

К ночи с субботы на воскресенье, пробыв в сети почти 60 часов, питтсбургская команда поняла, что они победили. В понедельник, второго июня, ФБР и Министерство юстиции сообщили о ликвидации сети и предъявили Богачеву обвинение по 14 пунктам.

В течение последовавших недель Славик и аналитики время от времени возобновляли битвы — Славик предпринял одну контратаку в тот момент, когда Вернер и Стоун-Гросс выступали на конференции в Монреале, но в итоге их дуэт одержал победу. Удивительно, но через два с лишним года успех в основном остается в силе. Бот-сеть так и не была восстановлена, хотя около пяти тысяч компьютеров по всему миру по-прежнему заражено вредоносной программой Zeus. А партнеры в сфере безопасности по-прежнему обслуживают «сервер-нейтрализатор», который поглощает трафик с зараженных компьютеров.

Примерно через год после штурма так называемые мошеннические действия на территории США с целью кражи с банковских счетов почти прекратились. Аналитики и следователи долго считали, что за тем шквалом преступлений, которые специалистам отрасли пришлось пережить в период с 2012 по 2014 годы, должно быть, стоят десятки преступных групп. Но почти ко всем кражам причастна лишь небольшая группа высококвалифицированных преступников — так называемая группировка Business Club. «К этому привыкаешь и слышишь, что они повсюду,- говорит Питерсон. — А на самом деле это очень маленькая сеть, и уничтожить ее гораздо легче, чем кажется».

9. Что было потом

В 2015 году Госдепартамент назначил за поимку Богачева награду в три миллиона долларов — самую большую сумму, которую предлагали власти США за киберпреступника. Но он остается на свободе. По данным американских разведывательных источников, власти на самом деле не считают, что Богачев принимал участие в хакерских атаках, которые Россия предпринимала, чтобы повлиять на выборы в США. Скорее всего, администрация Обамы включила его в санкционный список, чтобы оказать давление на российские власти. Есть надежда, что русские могут выдать Богачева Соединенным Штатам в знак доброй воли, поскольку бот-сеть, благодаря которой он был для них настолько полезным, заблокирована. Или, может быть, кто-то, проанализировав ситуацию более внимательно, решит, что они хотят получить в награду три миллиона долларов и дадут ФБР наводку.

Однако неприятная правда состоит в том, что Богачев и другие российские киберпреступники находятся довольно далеко, и Америке их не достать. По-прежнему остаются большие вопросы в отношении расследования случая с GameOver. Как и имеющие отношение к этому делу вопросы о явных связях Богачева с российскими спецслужбами и об общей сумме его хищений, которую чиновники могут назвать лишь округленно с точностью до 100 миллионов долларов. Все они служат предвестниками тех проблем, с которыми столкнутся аналитики, изучающие хакерские атаки во время избирательной кампании. К счастью, у агентов, занимающихся этим делом, есть опыт, который может быть для них полезным. По имеющейся информации, расследованием взлома почтовых серверов демократов занимается отдел ФБР из Питтсбурга.

А пока отдел, возглавляемый Mularski, и специалисты в сфере кибербезопасности также занялись новыми угрозами. Те приемы и методы, которыми пользовались преступники и которые были в новинку, когда Богачев помогал их внедрять, сейчас стали обычным делом.

Распространение программ-вымогателей активизируется. И сегодня бот-сети (особенно Mirai, червь, образованная сломанными или скомпрометированными устройствами вроде интернет-вещей), еще более опасны, чем то, что создавал Богачев.

Никто не знает, что сам Богачев может придумать в следующий раз. В Питтсбург продолжают регулярно поступать наводки о его местонахождении. Но никаких прямых признаков того, что он появился вновь, нет. По крайней мере, пока.

Гарретт Графф (Garrett Graff)

ИноСМИ.Ru