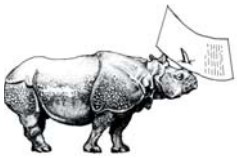

Олег Демидов, Максим Симоненко

ПОЖАР В КИБЕРПРОСТРАНСТВЕ

В конце мая 2012 г. Иран заявил о том, что его нефтяные компании подверглись интенсивным кибератакам. По инициативе Международного союза электросвязи (МСЭ) для расследования этих инцидентов была привлечена российская *Лаборатория Касперского*. Первые технические отчеты об инциденте были опубликованы в понедельник 28 мая того же года. Представители *Лаборатории Касперского* установили, что для осуществления атаки был использован беспрецедентный по сложности *супервирус*, который получил в базе вредоносных программ название *Flame* (англ. *пламя*). Впоследствии оказалось, что венгерская Лаборатория криптографии и системной безопасности (CrySyS) Будапештского университета технологии и экономики с начала мая 2012 г. занималась исследованием вируса, очень похожего на *Flame*, если не идентичного ему.

Первые версии вируса были обнаружены американской компанией *Webroot community* в конце 2007 г. на территории Европы. В следующем году вирус был обнаружен в ОАЭ. Вирусу пришлось проделать длинный технологический и временной путь, чтобы достичь Ирана весной 2010 г. в том виде, в котором его можно было наблюдать в 2012 г. На момент обнаружения в начале мая 2012 г. *Flame* находился на пике своего развития и вошел в фазу максимального распространения. К середине месяца *Flame* распространился по всему ближневосточному региону, так что установить непосредственную цель его создателей стало весьма затруднительно. При создании вируса использовались передовые технологии проникновения в компьютерные системы, но вместе с тем в нем отсутствуют какие-либо эффективные механизмы наведения на конкретную цель. Это позволяет говорить о том, что география распространения *Flame* не отображает спектр и местонахождение конечных объектов, поражение которых являлось его основной задачей.

В равной степени необоснованно выглядит повсеместное использование ярлыка *кибероружия* в отношении *Flame*. Сменщика *Stuxnet* и *Duqu* в галерее главных мировых *киберстрашилок* можно характеризовать по-разному, например, по аналогии с недавним открытием биологов, как *макровирус*, но использование понятия *кибероружие* принципиально искажает суть, назначение программы. В задачи выявленных и описанных модулей не входит выведение из строя компьютерных систем и, тем более, высокоизбирательное физическое поражение объектов критической инфраструктуры, под которое был спроектирован *Stuxnet. Flame* представляет собой эталонное средство ведения затяжного и многоуровневого кибершпионажа. В исследованиях и официальных документах большинства стран с развитым сектором ИКТ кибершпионаж всегда классифицируется отдельно от актов политически мотивированной агрессии в киберпространстве, гипотетических кибервойн

и киберконфликтов, то есть всех тех действий, которые могут осуществляться при помощи *оружия на основе программного кода.*

Навязчивое позиционирование *Flame* в качестве кибероружия, впрочем, кажется отнюдь не случайным — в подаче вируса под таким углом присутствует скрытый логический переход. Согласно последнему, *Flame* внедрялся в сети не в рамках отдельной операции, а скорее как часть стратегии использования обширного киберинструментария, совмещающего средства добычи информации с применением программ, способных наносить непосредственный физический ущерб инфраструктуре. В качестве такой стратегии в первую очередь неявно подразумеваются действия неких субъектов, направленные на торможение ядерной программы Ирана. Действительно, трудно отделаться от впечатления о *комплементарности Flame* и *Stuxnet* — изощренного инструмента выкачивания разнородных данных о любых интересующих объектах и, с другой стороны, хирургически точного орудия их поражения. Проблема, однако, заключается в том, что принимать целеобусловленную связь *Stuxnet* и *Flame* невозможно и контрпродуктивно, а значит, невозможно утвердительно говорить о *Flame* как о кибероружии. Ведь непосредственно кибершпионаж, несмотря на всю свою деструктивную природу, никакого ущерба инфраструктуре не наносит. *Flame* правомерно сравнивать скорее с оптическим прицелом на спайперской винтовке — оказаться в его фокусе весьма неприятно, но убивает все-таки пуля, а не оптика. А в случае с Flame прицел и винтовка существуют вроде как отдельно, и доказать, что они используются совместно, практически невозможно.

В этом контексте любопытна статья *The New York Times* от 1 июня 2012 г.[1], в которой разоблачается санкционированная лично Бараком Обамой грандиозная спецоперация США *Олимпийские игры* по осуществлению серии атак на атомную инфраструктуру Ирана, частью которых якобы стал *Stuxnet*. При всех сенсационных откровениях по поводу *Stuxnet* авторы практически полностью обходят стороной тему *Flame*, хотя сам выход столь подробного материала едва ли случайно столь точно совпал с шумихой вокруг нового супервируса. Попытка лаконично закрыть тему *Flame* ремаркой о том, что его появление не имеет никакого отношения к антииранскому *крестовому походу* США в киберпространстве — и, соответственно, к *Stuxnet*, — оставляет вопросы. Дело в том, что наиболее ценная для NYT целевая аудитория — иранское руководство и экспертное сообщество, не вынесет из статьи ничего принципиально нового по поводу *Stuxnet*. Американо-израильское авторство *Stuxnet* и *Duqu* едва ли ставилось гражданскими и военными экспертами под сомнение. С *Flame* для них все пока не так очевидно, поэтому попытка отвлечь внимание от вопроса, кем создан новый макровирус, могла выглядеть достаточно оправданной, для того чтобы раздувать шумиху вокруг менее актуальной на сегодня угрозы *Stuxnet* за счет громких разоблачений руководства США.

Кроме того, среди захватывающих историй о засекреченной программе *Олимпийских игр* в статье *The New York Times* присутствуют ссылки на факты, которые либо не могут быть проверены при помощи открытых источников, либо в определенной степени противоречат ранее приводившимся фактам о *Stuxnet*. Во-первых, авторы статьи утверждают, что осенью 2010 г., практически сразу после обнаружения *Stuxnet*, вирус поразил от одной до пяти тысяч центрифуг на обогатительных мощностях в Натанзе. Но в начале декабря 2010 г. МАГАТЭ опубликовало отчет о том, что порядка тысячи центрифуг были приостановлены на этом объекте иранской ядерной программы уже в конце 2009 — начале 2010 г. Больше никакой информации о новых остановленных центрифугах не поступало. Во-вторых, в открытых источниках отсутствуют данные, которые бы подтверждали, что центрифугами в Натанзе управляют SCADA производства *Siemens*. Этот момент важен, так как сюжет с SCADA-системами *Siemens* отсылает нас к версии, которую в статье *The New York Times* предпочитают не упоминать, и согласно которой главной целью супервируса была первая иранская АЭС в Бушере. Словом, статья американского издания, предлагая ценные, хотя и неочевидные ответы по поводу *Stuxnet*, ставит лишь новые вопросы в отношении нового шпионского супервируса.

В публикациях СМИ и экспертной среде *Flame* уже стал наиболее комплексной угрозой для информационных систем. И для этого есть основания. Вирус использует последние достижения в области создания вредоносных кодов, а объем вируса, который в совокупности составляет порядка 20 Мб информации и 70 тыс. строк кода, поражает воображение всех специалистов в сфере информационной безопасности. Переходит ли количество в качество? На первый взгляд да. В нем используются современные методы заражения, использующиеся в свое время в *Stuxnet* и *Duqu*: уязвимости в файле автозапуска *autorun.inf*, в файлах типа *.inc*, а также в службе диспетчера очереди печати. Использование этих технологий наталкивает некоторых экспертов на мысль о том, что над разработкой *Flame* и вирусного семейства *Stuxnet* работала одна команда. Но не стоит забывать, что это всего лишь технологии, или кусок кода, который был опубликован в открытом доступе, что позволяет использовать его кому и когда угодно. В добавление ко всему разработчики *Stuxnet* использовали уникальные механизмы маскировки и проникновения вируса — было украдено несколько подлинных цифровых подписей авторитетных производителей компьютерного оборудования, что затрудняло обнаружение вируса антивирусными программами, а также для проникновения в систему использовалась ранее неиспользованная уязвимость нулевого дня. Всего этого нет во *Flame*, в нем используются лишь общедоступные технологии, что может говорить о том, что над *Stuxnet* и *Flame* работали разные команды, хотя не исключено, что действовали они в интересах одного и того же заказчика.

С другой стороны, качество функциональной составляющей вируса не столь очевидно. *Flame* достигает своей громоздкости в первую очередь за счет подключения дополнительных модулей, которые напоминают скорее стандартный *хакерский набор*, чем передовое кибероружие. *Flame* способен собрать любую информацию о компьютере-жертве через перехват сетевого трафика, сбор информации о системе, захват скриншотов определенных процессов и даже запись аудио-разговоров. Но весь этот функционал был уже реализован ранее, только теперь все это собрано в одном месте и сборка различных комбинаций модулей автоматизирована. Такой взгляд на проблему позволяет предположить, что создателем такого супервируса могла выступить даже высококвалифицированная группа *ленивых хакеров*, желающих повысить производительность труда за счет максимальной автоматизации и интеграции своих *бизнес-процессов*. Такое технологическое решение в отношении создания средств кибершпионажа может привести к лавинообразному росту популярности подобных вредоносных продуктов, пусть и менее высокого класса. Сходная ситуация уже имела место в сегменте DDoS-атак. До тех пор, пока для создания ботнетов требовались значительные технологические компетенции и финансовые ресурсы, DDoS-атаки не были широко распространены. Теперь же, когда сформировался развитый рынок аренды ботнетов по доступным ценам, этот вид атак становится очень популярным. Нечто подобное может произойти в сфере вирусописания, когда, для того чтобы достичь своих деструктивных целей в киберпространстве, достаточно будет собрать вирус как конструктор из почти универсальных деталей и модулей.

Впрочем, вне зависимости от технологической новизны решений, которые создатели *Flame* заложили в свое детище, перспективы борьбы с супервирусом оставляют довольно грустное впечатление. Основные уязвимости уже латаются, ведущие лаборатории приступили к анализу кода, копии вируса по полученной команде самоудаляются с пораженных систем. Но многомодульные *вирусы* все больше начинают походить на пресловутый кубик Рубика — поворота одной грани, установки одного нового модуля достаточно для того, чтобы программа продолжала функционировать, используя новые уязвимости, список которых никогда не будет исчерпан. Кроме того, международная практика противодействия киберугрозам почти не знает успешных примеров *превентивной* борьбы с созданием и распространением вирусов столь серьезного уровня. Как правило, высококлассные шпионские программы могут успешно функционировать, годами оставаясь незамеченными, а выявляются едва ли не случайно и на той стадии, когда оценить полный объем ущерба и отследить путь вируса уже почти невозможно. При этом

в абсолютном большинстве случаев их обнаруживают частные лаборатории или национальные органы безопасности и правопорядка, никак не связанные с международными структурами. Так было в случаях с *Shady RAT, Moonlight Maze, Titan Rain* и другими высококлассными инструментами кибершпионажа в течение предыдущих лет. В результате налицо выраженный дисбаланс трансграничной природы современных киберугроз и, с другой стороны, преимущественно национальных механизмов поддержания безопасности в Сети. В руках у международного сообщества пока отнюдь не *щит*, способный отражать удары анонимного *кибермеча*, а скорее *пинцет и нитки*, которыми худо-бедно латается нанесенный ущерб.

Между тем вектор, в котором надлежит прикладывать усилия для исправления ситуации, достаточно очевиден и в целом корректно отражен в недавних международно-правовых инициативах РФ, включая концепцию Конвенции об обеспечении международной информационной безопасности. Речь идет, во-первых, о вынесении в политико-дипломатическую плоскость самого понятия *политически мотивированного враждебного поведения в киберпространстве*. Во-вторых, о формировании подлинно глобального режима сотрудничества в области противодействия киберугрозам, прообразом, хотя и не полноценным фундаментом которого можно считать Конвенцию Совета Европы «*О киберпреступности*». Наконец, необходимо четко определить международно-правовой статус киберпространства в контексте национальной и международной безопасности. Для Москвы вопрос заключается в том, удастся ли сдвинуть процесс с мертвой точки раньше, чем новый макровирус изберет целью уже не иранские, а российские сети. Времени не так много.

Примечания

[1] Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York Times. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all (последнее посещение — 17 августа 2012 г.).