Confidential

RUSSIA

The circulation of this report has been strictly limited to the members of the *Trialogue* Club International.

This issue is for your personal use only.

Published monthly in Russian and in English by *Trialogue Company Ltd.*

Issue № 9, vol.2. September 2012.

5 сентября 2012 г.

Олег Демидов, Максим Симоненко сообщают из Москвы:

ПОЖАР В КИБЕРПРОСТРАНСТВЕ

АННОТАЦИЯ

Отсчет истории Flame начинается отнюдь не с Ирана. Первые версии вируса - или, точнее, его прототипа - были обнаружены американской компанией Webroot Community в конце 2007 г. на территории Европы. В следующем году вирус был обнаружен в ОАЭ. На момент обнаружения в начале мая 2012 г. Flame находился на пике своего развития и вошел в фазу максимального распространения. К июню 2012 г. область поражения вирусом Flame разрослась до масштабов всего ближневосточного региона. Flame внедрялся в сети не в рамках изолированной операции, а скорее как часть стратегии использования обширного киберинструментария, совмещающего средства добычи информации с применением программ, способных наносить непосредственный физический ущерб инфраструктуре. Встает вопрос 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 на уровне аксиомы невозможно и контрпродуктивно - а значит, невозможно утвердительно говорить о Flame как о кибероружии.

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

Как появился ***Flame***?

Отсчет истории ***Flame*** начинается отнюдь не с Ирана. Первые версии вируса - или, точнее, его *прототипа* - 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 достигнуть Ирана весной 2010 г. уже практически в том виде, в котором его выявили специалисты *Лаборатории Касперского* в 2012 г. На момент обнаружения в начале мая 2012 г. ***Flame*** находился на пике своего развития и вошел в фазу максимального распространения. К июню 2012 г. область поражения вирусом ***Flame*** разрослась до масштабов всего ближневосточного региона, так что установить непосредственную цель вирусописателей весьма затруднительно. При создании вируса использовались передовые технологии для его проникновения в компьютерные системы, но, вместе с тем, в нем отсутствуют какие-либо эффективные механизмы наведения на конкретную цель. Все это позволяет говорить о том, что нынешняя география распространения ***Flame*** не отображает спектр и местонахождение конечных объектов, поражение которых было основной целью вируса.

В равной степени необоснованным 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 прицельно спроектирован ***Stuxnet***. ***Flame*** представляет собой эталонное средство ведения затяжного и многоуровневого кибершпионажа. В исследованиях и официальных документах большинства стран с развитым сектором информационных технологий кибершпионаж, как правило, 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 кода*.

Кибероружие?

Навязчивое позиционирование ***Flame*** в качестве кибероружия, впрочем, кажется отнюдь не случайным – в подаче вируса под таким углом присутствует скрытая логика. ***Flame*** внедрялся в сети не в рамках изолированной 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 на уровне аксиомы 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., 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 ими под сомнение. С ***Flame*** для них все пока не так очевидно. Поэтому попытка отвлечь внимание от вопроса, кем создан новый макровирус, может быть достаточной для того, чтобы раздувать шумиху вокруг уже слабоактуальной 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 было приостановлено на этом объекте иранской ядерной программы в конце 2009 – начале 2010 гг. 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 вся история с SCADA-системами ***Siemens*** тянется еще от версии, которую в статье ***The New York Times*** предпочитают не упоминать вообще - про то, что главной целью супервируса являлась первая иранская АЭС в Бушере. Словом, статья американского издания, предлагая ценные, хотя и неочевидные ответы по поводу ***Stuxnet***, ставит лишь новые вопросы в отношении нынешнего шпионского супервируса.

Как он работает?

В публикациях СМИ и экспертной среде ***Flame*** признан 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, 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 был один заказчик.

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 высокотехнологичный вирус.

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. Компьютерный вирус также проявлял повышенный интерес в формате ***AutoCAD***. Но весь этот функционал был уже реализован и ранее, только теперь все это собрано в одном месте и сборка различных комбинаций модулей автоматизирована. Такой взгляд на проблему позволяет предположить, что создателем супервируса могла

выступить даже группа *ленивых хакеров*, желающих повысить производительность труда за счет максимальной автоматизации и интеграции своих *бизнес-процессов*. Такое упрощение реализации кибератак может привести к лавинообразному росту популярности подобного средства разрешения проблем.

Сходная ситуация уже имела место в сфере DDoS-атак. До тех пор, пока для создания ботнетов требовались значительные технологические знания и финансовые ресурсы, DDoS-атаки не были широко распространены. Теперь же, когда сформировался развитый рынок аренды ботнетов по относительно недорогим 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.

Перспективы борьбы с вирусом

Вне зависимости от степени 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 *макровирусы* все больше начинают походить на пресловутый кубик Рубика – поворота одной грани, установки одного нового модуля достаточно для того, чтобы продолжать 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***, ***Titan Rain*** и другими высококлассными видами противозаконной активности, преследовавшими цель кибершпионажа в течение предыдущих лет.

В результате мы имеем *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.

Российские подходы

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 все же следует признать Конвенцию Совета Европы «О киберпреступности». И, наконец, об определении политико-дипломатического и международно-правового статуса киберпространства в контексте военной и национальной безопасности. Для Москвы вопрос состоит, прежде всего, в том, удастся ли сдвинуть процесс с мертвой точки раньше, чем новый макровирус изберет целью уже не иранские, а российские сети.

В условиях пробуксовки внешнеполитических инициатив российские власти наконец стали уделять внимание мерам в области обеспечения безопасности критической информационной инфраструктуры. В июле 2012 г. на сайте Совета безопасности РФ был опубликован фактически первый открытый документ в этой сфере - *Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации*. Рост внимания к защите критической инфраструктуры от киберугроз наблюдается и в Минобороны РФ. Сюжеты с ближневосточными *макровирусами*, безусловно, не сыграли ключевую роль в этих процессах, но, как представляется, все же внесли в них определенный вклад – особенно если говорить о ***Stuxnet***. Параллельно, российские власти меняют тактику в части продвижения инициатив по строительству глобального режима безопасности киберпространства. На помощь российскому МИД явился Евгений Касперский, чья компания - *Лаборатория Касперского* – ныне является одним из флагманов антивирусной индустрии и активно упрочивает свои позиции на мировом рынке с каждым годом. Именно *Лаборатории Касперского* удалось обнаружить резонансные вирусы на Ближнем Востоке за последние месяцы, включая ***Flame*** и ***Mahdi***, а до этого провести наиболее подробный анализ кода ***Stuxnet*** и ***Duqu***. Сам же господин Касперский с начала 2012 г. весьма активно озвучивает идею создания *кибер-МАГАТЭ* – межправительственного органа, ответственного за предупреждение создания и применения государствами и аффилированными с ними акторами программ, подобных ближневосточным супервирусам. Риторика господина Касперского явно укладывается в линию официальных инициатив РФ и, по некоторым предположениям, призвана фактически продвигать их на неправительственном уровне – от лица одного из наиболее уважаемых в отрасли экспертов. Проблема, которую призваны разрешить российские проекты, объективно существует – что наглядно подтверждает и ситуация с ***Flame***.

Авторы – научные сотрудники ПИР-Центра.

Редактор – Ирина Миронова.

(c) Международный клуб *Триалог*: trialogue@pircenter.org;
Centre russe d'etudes politiques: crep@pircenter.org
Москва – Женева, Сентябрь ***2012***

Вниманию членов Международного Клуба Триалог!

Осенью 2012 г. в серии «Библиотека ПИР-Центра» выходит монография члена Экспертно-Консультативного совета ПИР-Центра, заместителя министра обороны Российской Федерации А.И. Антонова «Контроль над вооружениями: история, состояние, перспективы»

По вопросам получения книги обращайтесь к Ирине Мироновой.
*Тел.: +7 (495) 987-**19-15***
*Факс: +7 (495) 987-**19-14***
Email: editor@pircenter.org

Выдержки из документа «Международный Клуб Триалог. Условия и правила членства».

3. Права членов Клуба

3.1. Индивидуальные члены Клуба имеют право:
*3.1.3. Получать 1 экземпляр бюллетеня эксклюзивной аналитики **Russia Confidential** по электронной почте, на выбранном языке (русском или английском). По правилам Клуба, передача бюллетеня третьим лицам не допускается.*
[…]
3.2. Корпоративные члены Клуба имеют право:
*3.2.3. Получать 2 экземпляра бюллетеня эксклюзивной аналитики **Russia Confidential** по электронной почте, на выбранном языке (русском или английском) либо на обоих языках одновременно, передавать этот бюллетень другим представителям корпоративного члена Клуба. По правилам Клуба, передача бюллетеня третьим лицам, не являющимся членами Клуба, не допускается.*
[…]

4. Обязанности членов Клуба

4.1. Все срочные члены Клуба обязаны:
*4.1.6. Не передавать полученные материалы бюллетеня **Russia Confidential**, а также пароли доступа на клубную часть сайта ПИР-Центра физическим и юридическим лицам, не являющимся членами Клуба.*
[…]

6. Russia Confidential

*6.1. Бюллетень эксклюзивной аналитики **Russia Confidential** выпускается ООО «Триалог» по заказу ПИР-Центра исключительно для личного пользования членов Клуба.*
*6.2. Бюллетень содержит сжатую эксклюзивную аналитику по вопросам международной безопасности, внешней и внутренней политики России и государств СНГ, подготовленную штатными и приглашенными экспертами ПИР-Центра специально для **Russia Confidential**.*
6.3. В течение не менее 30 дней со дня выхода материалы бюллетеня являются конфиденциальными и не могут цитироваться и передаваться лицам, не являющимся членами Клуба.
6.4. По прошествии не менее чем 30 дней ООО «Триалог» может снять эксклюзивный и конфиденциальный статус с материала, после чего в этих случаях он публикуется в других изданиях ПИР-Центра и может быть использован для цитирования членами Клуба.
6.5. Бюллетень распространяется по электронным адресам членов Клуба 1 раз в месяц по русском или английском языке, по выбору члена Клуба.
6.6. По запросу члена Клуба, он может также получить бумажную версию бюллетеня на выбранном им языке.

Уважаемые члены Международного клуба Триалог,

Мы приветствуем и ценим, когда действующие члены Клуба рекомендуют членство в Клубе или участие в наших заседаниях другим лицам. Помимо того, что такая рекомендация автоматически открывает двери для членства в Клубе, она также ***вознаграждается нами одним из двух способов.*** *Ниже представлены условия вознаграждения. Надеюсь, наше предложение Вас заинтересует.*

С уважением, 

Д.В.Поликанов
Председатель Международного клуба Триалог

Вознаграждения за рекомендацию членства в Международном клубе *Триалог* другим лицам

Вариант 1 – Скидка на членство в следующем периоде	
5%	за 1 нового индивидуального члена
10%	за 1 нового корпоративного члена
10%	за 2 новых индивидуальных членов
15%	за 3 новых индивидуальных членов
20%	за 4 и более новых индивидуальных членов
20%	за 2 новых корпоративных членов
30%	за 3 новых корпоративных членов
35%	за 4 и более новых корпоративных членов

Вариант 2 – Единовременное возмещение в наличной форме	
100 USD	за 1 нового корпоративного члена
200 USD	за 2 новых корпоративных членов
300 USD	за 3 новых корпоративных членов
500 USD	за 4 и более новых корпоративных членов