**Доклад 2. Появление кибероружия для ведения кибервойн**

Евгений Касперский, генеральный директор антивирусной «Лаборатории Касперского», отметил: «В недалеком прошлом мы боро­лись с киберпреступниками и интернет-хулиганами, теперь, боюсь, наступает время кибертерроризма, кибероружия и кибервойн». Ил­люстрацией этому являются известные примеры вредоносного про­граммного обеспечения (ВПО) – Stuxnet, Duqu, Flamer, Gauss, кото­рые многие антивирусные компании причисляют к кибероружию».

Впервые в истории компьютерный червь Stuxnet использовал­ся в качестве кибероружия для выведения из строя промышленных объектов.

В конце сентября 2010 года стало известно, что компьютерный червь Stuxnet нанес серьезный урон иранской ядерной программе. Используя уязвимости операционной системы Microsoft Windows и пресловутый «человеческий фактор», Stuxnet успешно поразил 1368 из 5000 центрифуг на заводе по обогащению урана в Натанзе, а также сорвал сроки запуска ядерной АЭС в Бушере. Заказчик этой атаки официально неизвестен. Исполнитель – нерадивый сотрудник компании Siemens, вставивший инфицированный флэш-накопитель в рабочую станцию. Ущерб, нанесенный ядерным объектам Ирана, сопоставим с ущербом от атаки израильских ВВС.

Мировую прессу заполнили мрачные пророчества о наступле­нии эры технологических кибервойн. Кибернетические атаки могут стать идеальными инструментами таких войн – они стремительны, эффективны в своей разрушительности и, как правило, анонимны.

Е. Касперский рассказал о военных целях вируса Stuxnet: «Stuxnet не крадет деньги, не шлет спам и не ворует конфиденци­альную информацию. Этот зловред создан, чтобы контролировать производственные процессы, в буквальном смысле управлять огром­ными производственными мощностями».

Компьютерный червь Stuxnet был обнаружен в июне 2010 года в промышленных системах, управляющих автоматизированными производственными процессами. Это первый известный компью­терный червь, руткит которого действует на уровне логических контроллеров. Поэтому Stuxnet заражает не столько программное обеспечение, сколько аппаратную основу системы, что значительно затрудняет борьбу с ним. Имеются сведения, что 60% всех компью­теров, пораженных этим вирусом, расположены на стратегических объектах атомной промышленности Ирана. Хотя компания Siemens, производившая компьютерное оборудование для иранских заводов, опровергает эту версию.

В прессе было сделано предположение, что Stuxnet представляет собой специализированную военную разработку, возможно израиль­скую, поскольку исходный код вируса содержит завуалированные упоминания слова MYRTUS. Этим словом буквально переводится с иврита имя библейского персонажа, персидской царицы иудейского происхождения Эсфири, которая помогла сорвать план нападения персов на Иудейское царство. Кроме того, в коде однажды встречает­ся никак не объясненная дата 9 мая 1979 г. (19790509) – по странному совпадению, на этот день пришлась казнь известного иранского про­мышленника Хабиба Эльганяна, еврея по национальности.

Данный вирус использует четыре ранее неизвестные уязвимо­сти системы Microsoft Windows, одна из которых «нулевого дня» (zero-day), направленная на распространение при помощи USB-flash ­накопителей.

***0day (англ. zero day) — термин, обозначающий неустранённые уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы.***

***Сам термин означает, что у разработчиков было 0 дней на исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем ПО исправлений ошибки (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от неё).***

Данный червь примечателен тем, что, по сути, он яв­ляется инструментом промышленного шпионажа – он предназначен для получения доступа к системе Siemens WinCC, которая отвечает за сбор данных и оперативное диспетчерское управление крупным производством.

До поры до времени Stuxnet никак себя не проявляет, но в заданный момент времени он может отдать команды, физиче­ски выводящие из строя промышленное оборудование. Ускользать от антивирусных программ ему помогало наличие настоящих цифровых подписей (два действительных сертификата, выпущенных компания­ми Realtek и JMicron).

Исследователь компании Trend Micro Поль Фергюсон (Paul Ferguson) заявил, что с созданием Stuxnet в мире появилось полноцен­ное кибероружие, которое выходит за рамки традиционных деструк­тивных схем (кража номеров кредитных карт и т. д.) и способно при­вести к серьезным авариям на очень опасных промышленных объектах.

Данный вирус стал первым настоящим кибероружием, так как он способен «выйти за пределы цифрового мира» и уничтожить ма­териальные объекты, а не только парализовать интернет-коммуника­ции. Объем вируса составляет примерно 500 КБ кода на ассемблере, С и С++.

В августе 2010 года сотрудниками лаборатории Касперского было выдвинуто предположение, что за созданием этого вируса сто­ят крупные государственные структуры. Руководитель отдела систем безопасности компании Symantec Лоран Эсло предполагает, что над созданием Stuxnet работали как минимум от шести до десяти чело­век на протяжении шести–девяти месяцев. Ориентировочная сумма создания Stuxnet составляет не менее $3 млн.

Следующим инцидентом, который также можно классифициро­вать как эпизод кибервойны, стало обнаружение в сентябре 2011 года троянца Duqu, целью которого было похищение конфиденциальной информации с промышленных объектов (кибершпионаж). Такое странное название, *Duqu*, троянец получил благодаря расширению создаваемых им файлов, ~DQ. В ходе детального исследования тро­янца Duqu было выявлено наличие ряда общих черт со Stuxnet и установлено, что обе вредоносные программы были созданы на еди­ной платформе, получившей название Tilded.

Впервые это вредоносное ПО было обнаружено в компьютер­ных системах европейских предприятий. Информация, которую ищет *Duqu*, касается прежде всего документов с описанием ИТ-инфраструктуры предприятия. Вероятно, эти данные нужны зло­умышленникам для осуществления последующих атак уже с целью установления контроля над разного типа промышленными система­ми. Как говорилось выше, *Duqu* является родственным червю Stuxnet и содержит части кода, идентичные «атомному» родственнику. Спе­циалисты делают предположение, что с Duqu работала та же команда, представители которой разрабатывали *Stuxnet*.

Дополнительный анализ червя провели представители компа­нии *McAfee*, сообщившие, что Duqu также «работает» и в Африке, и на Среднем Востоке, а не только в Европе. Как только червь попадает в систему, сразу устанавливается кейлоггер, записывающий все дей­ствия пользователя, а также происходит поиск дополнительной си­стемной информации. Червь может копировать список запущенных в системе процессов, информацию об аккаунте пользователя, а также информацию о домене. Делает он и скриншоты, записывает сетевую информацию, а также «исследует» файлы на всех доступных дисках, включая съемные и сетевые.

По данным компании *Symantec*, червь работает в системе 36 дней с момента запуска, а потом самоуничтожается.

Продвинутый компьютерный вирус Flame был обнаружен экс­пертами «Лаборатории Касперского» в мае 2012 года в ходе рассле­дования, инициированного Международным союзом электросвязи (ITU). Компьютерный вирус Flame собирал разведданные и гото­вился для проведения кибератак, направленных на замедление про­граммы Ирана по созданию собственного ядерного оружия.

Flame состоит из пакета модулей, который, будучи полностью развернутым, занимает около 20 МБ. В этой связи он является труд­но поддающейся анализу вредоносной программой. Большой размер вирусу придают множество включенных в него библиотек, например, для сжатия (ZLib, libbz2, PPMD) и работы с базами данных (sqlite3). Кроме того, Flame включает в себя виртуальную машину LUA.

В функционале Flame многое напоминает промышленное дело­вое ПО. После установки трояна он создает базу данных Mini SQL (mSQL) с формализованным описанием всего хранящегося на пора­женном хосте. Скриншоты, отправляемые в зашифрованном виде на управляющие серверы, Flame снимает только с интерфейсов процес­сов, перечисленных в специальном списке. Помимо него существует «черный список» процессов, скриншоты окон которых делать не надо. В первую очередь в него входят антивирусы. Среди других функций трояна – сетевой сниффер, аудиошпион, поиск соседних устройств по Bluetooth, распространение через общие папки, запуск HTTP-сервера и т. п. Функциональность Flame может быть расширена путем под­грузки дополнительных модулей, которых известно около 20.

Судя по всему, основная задача Flame – кибершпионаж. Пос­ле своего внедрения в систему Flame способен проводить комплекс действий, например, перехват сетевого трафика, снятие скриншотов, запись аудиоразговоров, перехват клавиатуры и т. п. Все похищенные данные доступны для операторов трояна через командные серверы. По команде с сервера Flame может полностью удалить следы своего пребывания на компьютере.

Программа Flame, о которой эксперты российской «Лаборато­рии Касперского» говорят, как о «возможно, самом сложном вирусе в истории», а в прессе называют «самым опасным кибероружием», собирала данные о местоположении иранских правительственных компьютерных сетей, а также занималась мониторингом активности в них, отсылая своим создателям массивные потоки секретных ма­териалов в рамках подготовки к масштабным кибератакам против Ирана.

На первый взгляд, программа Flame не имела ничего общего с исследованными ранее образцами Stuxnet и Duqu. Однако результа­ты последнего исследования доказывают, что разработчики платформ Tilded и Flame сотрудничали, а Stuxnet содержит в своем ресурсе компонент на платформе Flame.

Один из бывших высокопоставленных сотрудников американ­ской разведки заявил на условиях анонимности: «Вирусы Flame и Stuxnet являются элементами более масштабной атаки, которая все еще продолжается сегодня. Похищение секретной информации у Ирана с помощью вируса является очередным, но не последним ша­гом в этом направлении». Об этом сообщала газета Washington Post со ссылкой на анонимные источники среди западных чиновников.

В ходе расследования, инициированного Международным сою­зом электросвязи и проводимого «Лабораторией Касперского» в на­чале июля 2012 года, была найдена вредоносная программа SPE (mi­ni Flame).

Вредоносная программа miniFlame/SPE представляет собой небольшой по размеру полнофункциональный шпионский модуль, предназначенный для кражи информации и непосредственного до­ступа к зараженной системе. В отличие от Flame, которая использо­валась для крупномасштабных шпионских операций с заражением тысяч пользователей, miniFlame/SPE – инструмент для хирургиче­ски точных атак.

Вирус miniFlame действительно основан на платформе Flame, но реализован в виде независимого модуля, способного функциони­ровать как самостоятельно, без наличия в системе основных модулей Flame, так и в качестве компонента, управляемого Flame.

Вирус miniFlame/SPE является инструментом точечных атак и, вероятно, использовался исключительно против конкретных объ­ектов, представляющих для атакующих наибольший интерес и зна­чение. Вирус miniFlame не является широко распространенной вре­доносной программой. Вероятнее всего, она развертывается лишь на очень небольшом числе компьютеров жертв «высокого ранга». Основное назначение miniFlame – выполнять функции бэкдора на зараженных системах, обеспечивая возможность непосредственного управления ими со стороны атакующих.

Глава Киберштаба США при Пентагоне, генерал Кит Александер (Keith Alexander), выступая в Конгрессе, публично заявил, что за последние несколько лет угроза кибервойн растет стремительными темпами.

По словам замминистра обороны США, новая стратегия кибер­безопасности США основывается на следующих пяти принципах:

«Первый из этих принципов заключается в том, что мы должны признать киберпространство тем, чем оно уже стало, – новой зоной во­енных действий. Точно так же, как сушу, море, воздушное и космическое пространство, мы должны рассматривать киберпространство как сферу наших действий, которую мы будем защищать и на которую распро­страним свою военную доктрину. Вот что побудило нас создать объеди­ненное Киберкомандование в составе Стратегического командования.

Второй принцип, о котором я уже упоминал, – оборона должна быть активной. Она должна включать две общепринятые линии пас­сивной обороны – собственно, это обычная гигиена: вовремя ставить заплаты, обновлять свои антивирусные программы, совершенство­вать средства защиты. Нужна также вторая линия обороны, которую применяют частные компании: детекторы вторжения, программы мо­ниторинга безопасности. Все эти средства, вероятно, помогут вам от­разить примерно 80% нападений. Оставшиеся 20% – это очень грубая оценка – изощренные атаки, которые невозможно предотвратить или остановить посредством латания дыр. Необходим гораздо более ак­тивный арсенал. Нужны инструменты, которые способны определять и блокировать вредоносный код. Нужны программы, которые будут выявлять и преследовать внутри вашей собственной сети вторгшиеся в нее зловредные элементы. Когда вы нашли их, вы должны иметь возможность заблокировать их общение с внешней сетью. Иными словами, это больше похоже на маневренную войну, чем на линию Мажино.

Третий принцип стратегии кибербезопасности – это защита гражданской инфраструктуры.

Четвертый – США и их союзники должны принять меры кол­лективной обороны.

Наконец, пятый принцип – США должны оставаться на передо­вых рубежах в разработке программного продукта».

Президент США Барак Обама подписал указ, согласно которо­му инфраструктурные компании и спецслужбы будут обмениваться информацией о киберугрозах, а также будут разработаны националь­ные стандарты кибербезопасности.

Киберкомандование объявило 12 марта 2013 года, что перед ли­цом новых угроз, связанных с киберпреступностью, Пентагон создаст 40 групп (несколько тысяч гражданских лиц и военнослужащих), которые будут заниматься подготовкой возможных превентивных кибератак для защиты американских стратегических интересов.

По словам экспертов по безопасности Южной Кореи, Север­ная Корея уже давно активно готовится к ведению войны в кибер­пространстве, имея в своем распоряжении подразделение из 3 ты­сяч элитных хакеров, которыми управляет сам лидер страны Ким Чен Ын. В Северной Корее государство воспитывает специалистов в области кибератак для проведения боевых операций. Сейчас они способны проводить масштабные операции, включая DDoS-атаки и взлом хорошо защищенных сетей.



В Великобритании Центр правительственной связи (GCHQ) и Министерство обороны разрабатывают возможность запуска кибер­атак против враждебных государств и террористов. В рамках данной стратегии два независимых подразделения внутри Оборонной груп­пы киберопераций (DCOG) будут разрабатывать методы ответных реакций на враждебные действия, угрожающие информационной безопасности Великобритании.

В настоящее время некоторые государства заявили о необхо­димости формирования совместной политики по противостоянию кибернетическим угрозам. Однако, по мнению ряда экспертов, это представляется весьма сомнительным, поскольку слишком вели­ки соблазны, предлагаемые высокими технологиями: анонимность, безопасность (для атакующего), беспрецедентное соотношение «стои­мость/эффективность».