ИССЛЕДОВАНИЕ ПРИМЕНЯЕМЫХ ГОСУДАРСТВАМИ МЕТОДОВ И ТЕХНИЧЕСКИХ ОСОБЕННОСТЕЙ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Н.В. Евглевская, *к.т.н., Военная академия связи им. Маршала Советского Союза С.М. Буденного, n.evglevskaya@gmail.com;*
Д.А. Остроухов, *Национальный исследовательский университет ИТМО, demid-ostrouhov@yandex.ru;*
С.Н. Ракицкий, *к.в.н., доцент, Военная академия связи им. Маршала Советского Союза С.М. Буденного, s15136@mail.ru.*

УДК 004.056.57

Аннотация. Все большее число правительств по всему миру прибегают к хакерским атакам для облегчения своей правоохранительной и другой деятельности, связанной с безопасностью граждан и государства. В статье рассматриваются методы правительственного взлома. Особое внимание уделено наиболее распространенным в различных странах программным средствам, применяемым при правительственном взломе, их техническим особенностям.

Ключевые слова: правительственный взлом; вредоносное программное обеспечение; бэкдор; эксплойт; оперативно-разыскная деятельность.

RESEARCH OF METHODS AND TECHNICAL FEATURES OF CRIMINAL INTELLIGENCE OPERATIONS USED BY STATES

Natalya Evglevskaya, *candidate of Engineering, The Military Academy of Telecommunications named after Marshal of the Soviet Union S.M. Budyonny.*
Demid Ostroukhov, *ITMO National Research University;*
Stanislav Rakitsky, *candidate of military sciences, associate Professor, The Military Academy of Telecommunications named after Marshal of the Soviet Union S.M. Budyonny.*

Annotation. An increasing number of governments around the world are resorting to hacker attacks to facilitate their law activity related to the security of citizens and state. The article discusses the methods of government hacking. Special attention is paid to the prevailing software tools used in various countries, their technical features.

Keywords: government hacking; malware; backdoor; exploit; intelligence-gathering activities.

Введение

В настоящее время правительство многих стран прибегают к хакерским атакам, что связано с безопасностью граждан и государства. Но многие используют этот потенциал тайно и без четких правовых оснований. В тех случаях, когда правительства стремятся закрепить такие полномочия на законодательной основе, они часто делают это без гарантий и надзора, применимых к подобного рода действиям в соответствии с международным законодательством в области прав человека.

Взлом может представлять собой уникальную и серьезную угрозу конфиденциальности и безопасности данных. Поэтому, даже в тех случаях, когда правительства применяют вышеупомянутые подходы в связи с законной деятельностью, такой как сбор доказательств в рамках уголовного расследования или разведывательных данных, они вряд ли смогут продемонстрировать, что

хакерство, как форма деятельности по обеспечению безопасности, совместимо с международным законодательством в области прав человека. Однако на сегодняшний день не было проведено публичных дебатов о масштабах и характере таких полномочий и их последствий для конфиденциальности и безопасности данных граждан, государства и международного сообщества в целом.

Когда дело доходит до описания методов и тактик, используемых государствами и их правоохранительными органами для правительственного взлома, можно столкнуться с двумя трудностями. Одна из них заключается в том, что методы, которые используют государственные органы, являются государственной тайной и, как следствие, засекречены. Во-вторых, каждое государство имеет разные мотивы, когда дело доходит до инициирования правительственного взлома, и, следовательно, использует разные тактики [1].

Накопление или эксплуатация уязвимостей

В 2017 г. интернет захлестнула настоящая эпидемия файлов с расширением *Wcry* (закодированные файлы). Отсюда и пошло название шифровальщика – *WannaCry*. Атака затронула больницы, предприятия, университеты и многие другие общественно значимые сферы общества. Инцидент с *WannaCry* вызывает особый интерес, так как вредоносное воздействие было украдено у Агентства национальной безопасности (АНБ) Соединенных Штатов Америки. В связи с данным событием актуализировался вопрос: должны ли государства накапливать знания об уязвимостях программного обеспечения (ПО) и программном обеспечении для их использования?

Аргумент в пользу наличия у государств этих запасов такой же, как аргумент, используемый для оправдания накопления традиционного вида оружия, оружия массового поражения. Общая идея заключается в том, что такие запасы необходимы для национальной безопасности: для защиты и продвижения интересов государства. В случае использования уязвимостей для шпионажа, аргумент безопасности можно изменить, проведя аналогию с другими методами шпионажа. Как должно быть очевидно, в той мере, в какой государства имеют право накапливать физическое оружие и заниматься шпионажем в целях своей безопасности, они, по-видимому, также имеют право накапливать программное оружие и знания об уязвимостях.

Очевидный моральный контраргумент может быть построен на следующих основаниях: вред, причиняемый при краже и распространении такого ПО и информации, превышает выгоды, получаемые государствами, имеющими это ПО и информацию. Инцидент с *WannaCry* служит прекрасным примером. В то время, когда АНБ имело кратковременное преимущество, обладая исключительным правом собственности на ПО и информацию, ущерб, нанесенный вымогателями миру, безусловно, превышает это небольшое временное преимущество. Учитывая масштаб ущерба, который может быть нанесен, вред, причиняемый украденным ПО и информацией, как правило, превышает выгоды для государств. Таким образом, накопление такого ПО и знание уязвимостей является морально неправильным.

Однако, государствам просто необходимо обезопасить свое ПО и информацию, используемую в качестве оружия. Точно так же, как государство обязано гарантировать, что его традиционное вооружение не может быть использовано в преступных или террористических целях, государство обязано гарантировать, что его ПО и информация об уязвимостях не будут украдены. Таким образом, государствам приемлемо иметь кибероружие, как и обычное оружие.

Компьютерная сеть, формирующая нервную систему современного мира, слишком важна для всех, чтобы подвергать ее риску ради относительно незначительных и краткосрочных выгод, которые могли бы получить государства, создающие вредоносные программы и накапливающие уязвимости [2].

Социальные риски, связанные с уязвимостями в информационных системах и применяемыми средствами защиты, можно увидеть, проведя параллель с балансом рисков с биологическим оружием и государственными программами по укреплению и охране здоровья населения.

В микробиологии в случае обнаружения патогенного микроорганизма, опасных инфекций, требуется время для разработки вакцины. А после разработки вакцины требуется время для проведения вакцинации населения. То же самое применительно и по отношению к уязвимостям ПО: требуется время для разработки исправлений, а также время для развертывания исправления после его разработки. Программа вакцинации никогда не может быть универсальной точно так же, как данный патч никогда не может быть установлен на каждом уязвимом сетевом компьютере на планете.

Также возможно взять патогенный микроорганизм и «превратить» его в оружие, например, расширив диапазон температур, при которых он остается жизнеспособным, или просто создав «бомбы» для доставки, способные быстро распространить его по определенной территории. А уже вакцинированное население не уязвимо к биологическому оружию.

Предполагается, что наши правительственные учреждения должны защищать нас. Они знают, что эти уязвимости опасны. Хотим ли мы, чтобы они отложили создание программ вакцинации только для того, чтобы иметь запас эффективного оружия для использования в будущем?

Что, если бы Минздрав России в дополнение к своей текущей деятельности по сохранению здоровья и долголетия граждан, отвечал за разработку и накопление биологического оружия для использования против различных категорий граждан? Лучше или хуже, когда одно и то же агентство несет ответственность как за защиту нашего общества, так и за сохранение его уязвимости? Что должно произойти, если какая-либо часть государства или независимый исследователь обнаружит особенно опасный микроб – следует ли проинформировать Минздрав? Должен ли государственный орган, обнаруживший такой микроб, рассматривать возможность сохранения его в секрете, чтобы оно могло использовать его против людей, которых оно считает «плохими», хотя остальная часть населения также уязвима? Какой стимул у независимого исследователя, заботящегося о безопасности, делиться таким пугающим открытием с Минздравом, если он знает, что министерство может принять решение использовать опасную информацию в негативных целях, а не для защиты здоровья населения?

Что, если бы государство активно создавало биологическое оружие, разрабатывая способы его более широкого распространения или создавая эффективные средства его доставки?

Эти виды оружия не могут быть применены без определенного риска их распространения, вот почему биологическое оружие было запрещено международной конвенцией. Тот, кто подвергся воздействию микроба, может культивировать его и производить больше. Тот, кто подвергся воздействию вредоносного ПО, может создать копию, проверить ее, модифицировать и повторно развернуть. Должны ли мы мириться с такого рода деятельностью государств, отвечающих за общественную безопасность? К сожалению, этот вопрос на данный момент на международной арене обсуждается недостаточно

активно, несмотря на тот факт, что несколько государств накапливают уязвимости и используют их против информационных систем в общедоступной сети [3].

Вредоносное программное обеспечение

В общих чертах, вирусные программы – это вредоносные программы, которые каким-либо образом вредят или делают нечто нежелательное в аппаратном и ПО легальных пользователей. Большинство людей знают о вирусах, троянах, программах, крадущих информацию, и даже программах, которые шифруют данные и требуют деньги за их восстановление. За последние несколько лет стали широко известны вирусы, использующиеся для слежения, или шпионские программы. Это программы, которые устанавливают на компьютер не киберпреступники, а государственные органы безопасности или полиция. Они дают им доступ к коммуникациям пользователя в сети и, поскольку жизнь сейчас в большой степени проходит в интернете, то там государство в основном и занимается слежкой.

Вредоносные шпионские программы могут иметь широкий спектр возможностей. Например, поскольку мобильные телефоны теперь все реже используются для телефонных звонков, а все больше для общения в интернете, наблюдается рост количества шпионских программ для, так называемого, «полицейского перехвата». Если на телефон тайно установлена подобная программа, то она позволяет следить за перемещениями пользователя через *Global Positioning System GPS*, просматривать список контактов, читать *SMS*-сообщения, записывать телефонные разговоры, видеть переписки в социальных сетях и многое др. [4].

Внедрение вредоносного ПО состоит из нескольких этапов: доставка, эксплуатация, исполнение и отчетность.

Первый этап. Доставка. Уполномоченный государственный орган должен сначала доставить свое вредоносное ПО до цели, как правило в сообщении, отправляемом подозреваемому. Сообщение включает описание, предназначенное для того, чтобы принудить жертву перейти по ссылке, которая перенаправляет ее веб-браузер на веб-сайт или контент, контролируемый правоохранительными органами. Этот тип доставки вредоносных программ, получивший название «фишинг» в области компьютерной безопасности, нацелен на конкретных лиц.

Более сложная тактика правоохранительных органов заключается в следующем. Идентифицируется оператор интернет-ресурса, подвергается захвату его инфраструктура, но в тоже время интернет-ресурс продолжает работу с добавленным вредоносным кодом. Когда подозреваемые взаимодействуют с веб-сайтом при определенных условиях запуска – например, посещая его при входе в систему или переходя на определенные веб-страницы – вредоносное ПО доставляется до подозреваемого. Таким образом, в отличие от фишинговой атаки, этот тип атаки нацелен на любых лиц, которые ведут себя определенным образом.

Второй этап. Эксплуатация. В начале реализации данного этапа правоохранительным органами известно следующее. ПО поступает из различных источников, не всем разработчикам можно доверять. Как следствие, ПО обычно выполняется с ограниченными разрешениями: оно может получать доступ только к определенным данным и функциональным возможностям на устройстве. Веб-браузеры и мобильные устройства устанавливают особенно строгие правила безопасности, требуя, чтобы ПО было написано на определенных языках и предоставляло доступ только к определенным возможностям. Веб-браузеры, например, обычно запускают только ПО, написанное на языке *JavaScript*, и предоставляют этому ПО доступ только к сохраненным данным, связанным с

источником ПО. Некоторые функции, такие как включение веб-камеры устройства и *GPS*, доступны только с согласия пользователя. Другие возможности устройства, такие как чтение данных из сторонних приложений, полностью запрещены. Вводя эти ограничения, службы безопасности устройства одновременно соответствуют ожиданиям пользователя в отношении безопасности и конфиденциальности и информируют о них.

Взлом правоохранительными органами обязательно подрывает барьеры безопасности, чтобы предоставить следователям доступ к необходимым им данным и функциям. Разработчики вредоносных программ выявляют или приобретают уязвимости в приложениях, которые позволяют им обходить защиту устройств. Конкретная уязвимость в системе безопасности устройства, которую использует государство, и то, как оно использует эту уязвимость, зависят от множества факторов, включая информацию, которую ищут следователи, и конфигурацию ПО, используемого подозреваемыми.

Третий этап. Исполнение. Как только правоохранительные органы обходят средства защиты, их ПО запускается. Простой экземпляр вредоносного ПО может отметить время запуска ПО, собрать информацию об ОС и процессоре, а затем отправить сетевой запрос, содержащий *IP*-адрес устройства.

Более изощренные вредоносные программы могут извлекать дополнительную идентифицирующую информацию через ОС устройства. Такими данными могут быть: имя компьютера и уникальный идентификатор, который производитель компьютера присвоил его сетевой карте и др.

Четвертый этап. Отчетность. Наконец, когда ПО правоохранительных органов запустилось на устройстве подозреваемого, оно обращается посредством сети интернет к правоохранительным органам, инициировавшим применение данного ПО, чтобы сообщить информацию о расследовании. Для решения этой задачи подходит любой сервер, контролируемый государством.

Перечисленные четыре этапа: доставка, эксплуатация, исполнение и отчетность, являются основополагающими для функционирования правительственного вредоносного ПО. И каждый шаг потенциально может привести к непредвиденным последствиям, включая угрозы безопасности и конфиденциальности данных граждан [5].

Бэкдоры

Современное шифрование не только защищает информацию от злоумышленников, оно также не позволяет правоохранительным органам ознакомиться с данными граждан. Даже, когда правоохранительные органы получают разрешение на данные действия со стороны суда, это не помогает им расшифровывать данные граждан. Такое ограничение находится в центре продолжающихся дебатов о надлежащей роли шифрования в обществе, которые впервые начались в 1990-х гг.

Сторонники правоохранительных органов утверждают, что шифрование представляет фундаментальную угрозу общественной безопасности, поскольку санкционированные судом расследования не могут быть проведены. Защитники конфиденциальности и представители бизнеса подчеркивают важность шифрования для обеспечения личной неприкосновенности, защиты деловых операций и ограничения власти правоохранительных органов. В попытке удовлетворить обе потребности, правоохранительные органы настаивали на использовании специальных «бэкдоров» в зашифрованных системах, то есть специального метода дешифрования, который может использоваться

правоохранительными органами только при выполнении санкционированных судом оперативно-разыскных действий.

В основе этих социально-политических дебатов лежит технический вопрос: возможно ли создать надежную систему шифрования с «бэкдором», который могут использовать только правоохранительные органы? За последние 30 лет был достигнут незначительный прогресс в ответе на этот вопрос. Большинство предлагаемых конструкций систем шифрования с «бэкдорами» предоставляют государству ключи шифрования, которые могут расшифровать все, в надежде, что никто не воспользуется ключами не по назначению. Подавляющее большинство исследователей и активистов согласны с тем, что этот подход по своей сути ошибочен, так как существует слишком много способов злоупотребления ключами шифрования.

Прогресс в решении этого технического вопроса застопорился, поскольку требования к желаемым системам так и не были полностью определены. Иными словами, на самом деле есть два вопроса, маскирующихся под один: (1) какие свойства должны обеспечивать системы шифрования с «бэкдорами» правоохранительных органов? и (2) возможно ли построить системы, которые обеспечивают эти свойства? Редко можно увидеть четкий и связный ответ на первый вопрос и консенсуса нет. Это затрудняет переход ко второму вопросу.

Однако можно определить минимальные свойства, которыми должны обладать зашифрованные системы:

Доступ правоохранительных органов к конфиденциальным данным граждан возможен только при наличии разрешения суда. Зашифрованный контент по умолчанию должен оставаться полностью защищенным. Правоохранительные органы – и только правоохранительные органы – должны иметь возможность использовать ключи шифрования, если соответствующее разрешение выдано соответствующим судом.

Выявляемость злоупотреблений. Огромная проблема с существующими предложениями заключается в том, что злоупотребления могут происходить скрытно; конкретный работник правоохранительных органов может использовать ключи шифрования в своих целях и никто никогда не узнает об этом.

Системы должны требовать создания общедоступного следа прежде, чем можно будет использовать «бэкдор». Этот след позволит аудиторам поднимать тревогу при обнаружении неправомерного использования.

Глобальная политика выдачи разрешений судами. Как общество, нам необходимо договориться о том, как должны выглядеть эти разрешения. Например, возможно, мы хотим ограничить выдачу разрешений конкретными лицами. Возможно, мы хотим, чтобы разрешения можно было использовать только в течение коротких периодов времени. Определив некоторую глобальную политику выдачи разрешений, мы можем ограничить разрушительные возможности суда или правоохранительных органов.

Криптографическое обеспечение. (Теоретически) легко написать закон, который требует, чтобы система обладала указанными выше свойствами. К сожалению, в первую очередь необходимо позаботиться о предотвращении злоупотреблений системой со стороны лиц, которые не уважают закон. Таким образом, необходимо разработать технические системы, которые обеспечивают соблюдение всех этих свойств, используя что-то более надежное, чем закон, например математику. Другими словами, необходимо, чтобы математика, используемая для построения системы, делала ключи шифрования непригодными для использования, если судебное разрешение не соответствует политике разрешения или не был создан контрольный журнал.

Развертывание «бэкдора» правоохранительных органов без этих минимальных свойств защиты от злоупотреблений, несомненно, является прямым путем к катастрофе. Прежде чем начать обсуждение того, как внедрять «бэкдоры», крайне важно согласовать минимальные свойства защиты от злоупотреблений для такой системы [6].

***Pegasus* (*NSO Group*, Израиль)**

Pegasus – шпионская программа, которую можно незаметно установить на мобильные телефоны и другие устройства, работающие под управлением некоторых версий мобильных операционных систем (ОС) *iOS* и *Android*. Разработчиком *Pegasus* является израильская компания *NSO Group*. Компания заявляет, что предоставляет «уполномоченным правительствам технологии, которые помогают им бороться с терроризмом и преступностью», она также опубликовала фрагменты условий применения программы, требующих от клиентов использовать *Pegasus* только в целях уголовной и национальной безопасности. *NSO Group* также утверждает, что соблюдает права человека [7].

Атака очень проста в осуществлении. Она начинается, когда злоумышленник отправляет *URL* веб-сайта (через *SMS*, электронную почту, социальные сети или любое другое сообщение) идентифицированной цели. Пользователю нужно выполнить только одно действие – нажать на ссылку. Как только пользователь нажимает на ссылку, ПО незаметно выполняет серию эксплойтов против устройства жертвы для удаленного взлома устройства компании *Apple*, чтобы можно было установить пакеты шпионского ПО. Единственным признаком того, что что-то произошло, будет закрытие браузера после перехода по ссылке.

Для достижения цели программа-шпион после взлома телефона пользователя не загружает вредоносные версии этих приложений на устройство жертвы с целью захвата данных, а компрометирует исходные приложения, уже установленные на устройстве. Сюда входят предустановленные приложения, такие как *Facetime* и *Calendar*, а также приложения из официального *App Store*.

Пользователь, зараженный этим шпионским ПО, находится под полным наблюдением злоумышленника, поскольку в дополнение к перечисленным выше приложениям, он также следит за:

- телефонными звонками;
- журналами вызовов;
- *SMS*-сообщениями, которые отправляет или получает жертва;
- аудио- и видеосвязью, которая (по словам основателя *NSO Group*) превращает телефон в «портативную рацию».

Доступ к указанному контенту может быть использован для получения дальнейшего доступа к другим учетным записям жертвы, принадлежащим цели, таким как банковские услуги, электронная почта и другие сервисы, которыми она может пользоваться на устройстве или вне его [8].

***FinSpy* (*FinFisher*) (*Vilicius Holding GmbH*, Германия)**

FinSpy – коммерческая шпионская программа, которой пользуются силовые структуры и государственные органы разных стран. Впервые она попала на радары исследователей в 2011 г., когда на *Wikileaks* появились связанные с ней документы. В 2014 г. исходный код зловреда выложили в интернет, однако на этом его история не закончилась: разработчики переписали *FinSpy* и он до сих пор продолжает заражать устройства по всему миру.

FinSpy не ограничивается одним методом заражения. Имеется сразу три пути, которые шпионская программа использует, чтобы проникнуть на компьютеры с ОС *Windows* [9].

Вредоносная программа создает копию исходной главной загрузочной записи и сохраняет ее в другом месте на жестком диске. Кроме того, вредоносная программа записывает 0x2*A*00 байт данных на зараженный жесткий диск. Эти данные позже копируются вредоносным загрузочным кодом. Адрес первого сектора, содержащего эти данные, жестко закодирован в коде начальной загрузки. Вредоносная программа использует адресацию логических блоков (*LBA*) для определения физического местоположения вредоносных данных на жестком диске [10].

FinSpy располагает широкими возможностями для слежки за пользователями. Так, версии зловреда для персонального компьютера могут:

- включать микрофон и записывать или транслировать злоумышленникам все, что он слышит;
- записывать или передавать злоумышленникам в реальном времени все, что пользователь вводит на клавиатуре;
- включать камеру и записывать или транслировать изображение с нее;
- копировать файлы, которые пользователь изменяет, отправляет на печать, получает, удаляет и так далее;
- снимать скриншоты или захватывать участок экрана там, где пользователь кликает мышью;
- воровать письма клиентов из *Thunderbird, Outlook, Apple Mail* и *Icedove*;
- перехватывать контакты, чаты, звонки и файлы в *Skype*.

В дополнение к этому версия *FinSpy* для ОС *Windows* может перехватывать *VoIP*-звонки, перехватывать сертификаты и ключи шифрования для определенных протоколов, а также загружать и запускать утилиты для сбора криминалистических данных. Помимо вышеперечисленного, *Windows*-версия шпиона способна заражать смартфоны.

Мобильные версии *FinSpy* могут прослушивать и записывать звонки – как голосовые, так и *VoIP*, читать *SMS* и следить за активностью пользователя в мессенджерах, таких как *WhatsApp, WeChat, Viber, Skype, Line, Telegram, Signal* и *Threema*. Кроме того, мобильный шпион отправляет злоумышленникам список контактов и звонков жертвы, мероприятия из календаря, информацию о местоположении устройства и многое др. [9].

***Remote Control System* (*RCS*) (*Hacking Team*, Италия)**

Hacking Team, также известная как *HT S.r.l.,* является компанией, расположенной в г. Милан, которая позиционирует себя как первую, предложившую наступательное решение для киберрасследований. Ее флагманский продукт *Remote Control System* (*RCS*), названный «хакерский пакет для правительственного перехвата», представляет собой набор имплантатов удаленного мониторинга (т.е. шпионских программ), продаваемых исключительно правительственным учреждениям по всему миру.

Remote Control System отличает от традиционных решений для наблюдения (например, прослушивания телефонных разговоров) возможность захватывать данные, хранящиеся на компьютере цели, даже если цель никогда не отправляет информацию через интернет. *Remote Control System* также позволяет правительству следить за зашифрованными интернет-коммуникациями объекта, даже если объект подключен к сети, которую правительство не может прослушивать. Возможности

RCS включают в себя копирование файлов с жесткого диска компьютера, запись звонков по *Skype*, мониторинг электронной почты, мгновенных сообщений и паролей, вводимых в веб-браузере. Кроме того, *RCS* может включать веб-камеру и микрофон устройства, чтобы следить за объектом [11].

На рис.1 представлена логическая архитектура прототипа развертывания *RCS Hacking Team*. В определенных случаях может использоваться «распределенная» архитектура.

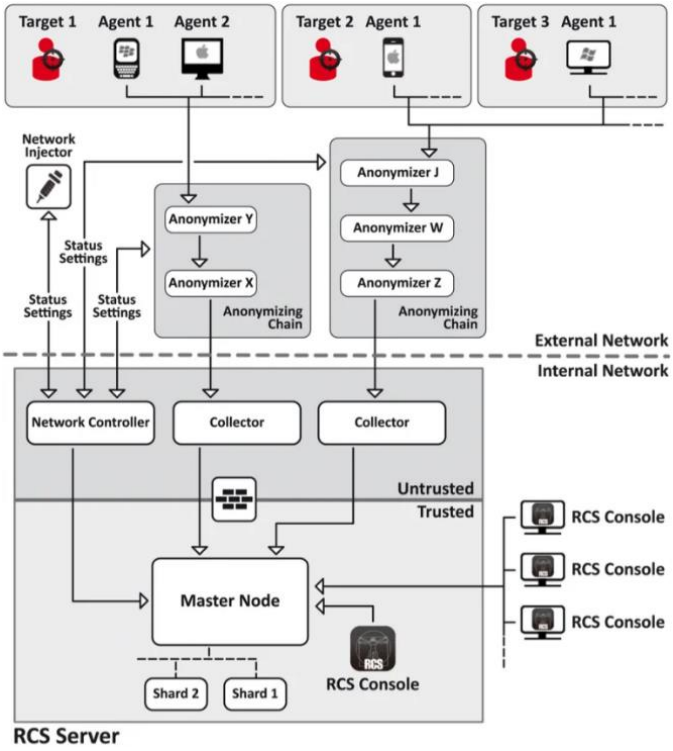

Рисунок 1

Remote Control System имеет ряд определенных ролей, каждая со своими собственными обязанностями и разрешениями в системе.

Системный администратор проходит обучение в *Hacking Team* на «этапе заключения контракта», а также выполняет другие задачи системного администрирования, включая установку и обновление серверов *RCS*, а также сетевых инжекторов.

Администратор создает учетные записи, выполняет операции и назначает цели.

Технический специалист отвечает за создание имплантатов (в документации они называются «агентами») и управление сетевыми инжекторами.

Аналитики обрабатывают выходные данные системы и выполняют интеллектуальный анализ с помощью консоли *RCS* [12].

***Predator* (*Cytrox*, Северная Македония)**

Predator – это шпионское ПО, разработанное компанией *Cytrox* и предназначенное для ОС *Android* и *iOS*. В мае 2022 г. исследователи из группы анализа угроз *Google* (*TAG*) сообщили, что *Predator* объединил пять эксплойтов нулевого дня в один пакет и продал его нескольким субъектам, поддерживаемым правительством, которые использовали его в трех отдельных кампаниях. По словам исследователей, *Predator* тесно сотрудничал с компонентом под названием *Alien*,

который «живет внутри нескольких привилегированных процессов и получает команды от *Predator*».

Анализ шпионского ПО, проведенный *Cisco Talos* в мае 2023 г., показал, что компонент *Alien* шпионского ПО активно реализует низкоуровневую функциональность, необходимую *Predator* для наблюдения за своими целями вместо того, чтобы просто выполнять функции загрузчика для *Predator*, как предполагалось ранее. В примере *Talos Alien* использовал пять уязвимостей, четыре из которых затрагивали *Google Chrome*, а последняя – *Linux* и *Android*, для заражения целевых устройств. После заражения устройства *Predator* получает полный доступ к его микрофону, камере и пользовательским данным, таким как контакты и текстовые сообщения. Кроме того, *Predator* имеет доступ к службам определения местоположения устройства и приложениям для обмена сообщениями, таким как *WhatsApp, Telegram* и *Signal*, что позволяет хакерам перехватывать и фальсифицировать сообщения [13].

***Hermit* (*RCS Lab*, Италия)**

Hermit – это шпионское ПО, разработанное итальянским коммерческим поставщиком шпионских программ *RCS Lab*, которое может быть тайно установлено на мобильные телефоны под управлением *iOS* и *Android.*

Компания *RCS Lab* занимается тем же бизнесом, что и *NSO Group*, которая получила известность благодаря своему шпионскому ПО *Pegasus* и продает шпионский софт правительственным учреждениям. Подобно *Pegasus, Hermit* способен отслеживать звонки, отслеживать местоположение, читать текстовые сообщения, получать доступ к фотографиям, записывать аудио, совершать и перехватывать телефонные звонки и способен получить *root* на устройствах *Android.* Некоторые злоумышленники выдавали себя за оператора мобильной связи жертвы, чтобы обманом заставить жертву загрузить приложение, которое доставит полезную нагрузку. Также вредонос выдавал себя за законное приложение для обмена сообщениями. Хотя приложения, содержащие шпионское ПО, не были доступны в *iOS App Store* или *Google Play Store*, злоумышленники смогли получить сертификаты, разрешающие установку зловреда на любое устройство *iOS*, через корпоративную программу *Apple* для разработчиков. Как только информация о *Hermit* стала достоянием общественности, *Apple* заявила, что отозвала связанные с ней сертификаты, а *Google* заявил, что распространил обновления *Google Play Protect* для всех пользователей [14].

***Regin* (АНБ, США)**

Regin (также известный как *Prax* или *QWERTY*) – это сложное вредоносное ПО и набор инструментов для взлома, используемый Агентством национальной безопасности США и его британским аналогом, Штаб-квартирой правительственных коммуникаций (*GCHQ*). Впервые оно была публично раскрыто «Лабораторией Касперского», «*Symantec*» и «*The Intercept*» в ноябре 2014 г. Вредоносная программа нацелена на конкретных пользователей компьютеров под управлением ОС *Windows* и была связана с агентством по сбору разведывательной информации АНБ США и его британским аналогом *GCHQ*. «The *Intercept*» предоставил образцы *Regin* для скачивания, включая вредоносное ПО, обнаруженное у бельгийского телекоммуникационного провайдера *Belgacom*. «Лаборатория Касперского» заявляет, что впервые узнала о *Regin* весной 2012 г., но некоторые из самых ранних образцов датируются 2003 г. (Имя *Regin* впервые было упомянуто на веб-сайте *VirusTotal* 9 марта 2011 г.) Среди компьютеров, зараженных Regin по всему миру, 28% находились в России, 24% – в Саудовской

Аравии, по 9% – в Мексике и Ирландии и по 5% – в Индии, Афганистане, Иране, Бельгии, Австрии и Пакистане.

Regin использует модульный подход, позволяющий загружать функции, которые точно соответствуют цели, обеспечивая индивидуальную слежку. Конструкция делает его очень подходящим для постоянных, долгосрочных операций массового наблюдения за целями. Этапы развертывания вредоносного ПО *Regin* показаны на рис. 2.

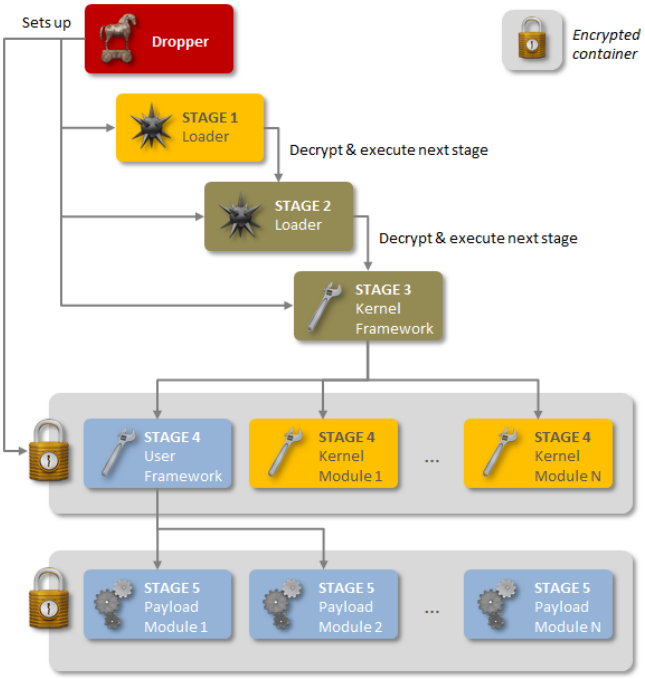

Рисунок 2

Regin работает скрытно и не хранит несколько файлов в зараженной системе; вместо этого он использует свою собственную зашифрованную виртуальную файловую систему (*EVFS*), которая использует вариант шифрования редко используемого шифра *RC*5. *Regin* взаимодействует через интернет, используя *ICMP/ping*, команды, встроенные в *HTTP cookies*, и пользовательские протоколы *TCP* и *UDP*, с сервером управления, который может контролировать операции, загружать дополнительные полезные данные и т.д. [15].

Сравнительный анализ различного вредоносного программного обеспечения

Проведем сравнительный анализ вредоносного ПО, применяемого правоохранительными органами различных стран при осуществлении оперативно-разыскной деятельности. Сравнительный анализ проводится по следующим критериям: страна происхождения, компания-разработчик, целевые устройства и ОС, эксплуатируемые уязвимости, эксплойты, ключевое воздействие, технические возможности, пути заражения.

Pegasus.

Страна происхождения: Израиль.

Компания-разработчик: *NSO Group*.

Целевыми объектами являются устройства с мобильными ОС *Android и iOS*.

Используются уязвимости *iOS CVE*-2016-4655, *CVE*-2016-4656, *CVE*-2016-4657, эксплойты *FORCEDENTRY, Zero-click* и др.

Ключевой особенностью является джейлбрейк *iPhone* или получение *root*-доступа *Android*-устройства.

Среди возможностей: анализ контактов, журналов вызовов, сообщений, фотографий, истории посещенных веб-страниц, настроек, прослушивание зашифрованных аудиопотоков и чтения зашифрованных сообщений, создания скриншотов, регистрации нажатия клавиш, а также сбора информации из приложений, включая, но не ограничиваясь ими, *Facebook, WhatsApp, iMessage, Gmail, Viber, Facebook, Telegram* и *Skype.*

Путей заражения несколько: фишинг, телефонный звонок (вне зависимости от того, будет ли ответ на звонок или нет), сообщения в *iPhone iMessage*, осуществление сетевой атаки.

FinSpy (FinFisher).

Страна происхождения: Германия.

Компания-разработчик: *Vilicius Holding GmbH.*

Целевыми объектами являются устройства с ОС *Windows, macOS* и *Linux* и мобильные устройства с *Android* и *iOS*.

Используются уязвимости в системе безопасности *iTunes* от *Apple* и др.

Ключевой особенность является загрузка и установка троянизированного приложения, выполняющего зловредные функции.

Среди возможностей: прослушивание и запись звонков, чтение *SMS* и слежка за активностью пользователя в мессенджерах, таких как *WhatsApp, WeChat, Viber, Skype, Line, Telegram, Signal* и *Threema*, извлечение списка контактов и звонков, мероприятий из календаря, информации о местоположении устройства и др.

Путей заражения несколько: запуск установщиков легальных приложений, в которых внедрен *FinSpy* (*TeamViewer, VLC Media Player, WinRAR* и др.), проникновение в загрузочную запись *UEFI* и *MBR* и фишинг (например, в *SMS*).

Remote Control System (RCS).

Страна происхождения: Италия.

Компания-разработчик: *Hacking Team.*

Целевыми объектами являются устройства с ОС *Android, BlackBerry, Apple iOS, Linux, Mac OS X, Symbian, Microsoft Windows, Windows Mobile* и *Windows Phone.*

Используется несколько эксплойтов: *Adobe Flash* в документе *Word, RTF*-файл с расширением *DOC* (*CVE*-2010-3333), переполнение целых чисел *Adobe Flash* «*Matrix*3*D*», *CVE*-2013-5331, *CVE*-2013-0633, *CVE*-2012-5054.

Ключевой особенностью является использование технологии прокси-цепочек для анонимизации правоохранительных органов.

Среди возможностей: скрытый сбор электронных писем, текстовых сообщений, историй телефонных звонков и адресных книг, регистрация нажатий клавиш, раскрытие данных истории поиска и создание скриншотов, запись телефонных звонков, активация камеры телефона или компьютера, взлом *GPS* для отслеживания местоположения цели, заражение *UEFI BIOS* прошивки целевого компьютера руткитом, извлечение паролей *Wi-Fi* и др.

Путей заражения несколько: фишинг, открытие документа *Microsoft Word* или просмотр веб-страницы.

Predator.

Страна происхождения: Северная Македония.

Компания-разработчик: *Cytrox.*

Целевыми объектами являются устройства с мобильными ОС *Android* и *iOS*.

Используются следующие уязвимости: *CVE*-2021-37973, *CVE*-2021-37976, *CVE*-2021-38000, *CVE*-2021-38003 в *Chrome* и *CVE*-2021-1048 в *Android.*

Ключевой особенностью является совместная работа с программным компонентом *Alien*, которое настраивает низкоуровневые возможности, необходимые *Predator.*

Основными возможностями являются: получение полного доступа к микрофону, камере и данным пользователя, таким как контакты и текстовые сообщения. *Predator* имеет доступ к службам определения местоположения устройства и приложениям для обмена сообщениями, таким как *WhatsApp, Telegram* и *Signal.* Он также позволяет перехватывать и фальсифицировать сообщения.

Пути заражения неизвестны.

Hermit.

Страна происхождения: Италия.

Компания-разработчик: *RCS Lab*.

Целевыми объектами являются устройства с мобильными ОС *Android* и *iOS*.

Используемые эксплойты и уязвимости неизвестны.

Ключевой особенностью является модульность *Hermit.*

Основными возможностями являются: отслеживание звонков, местоположения, чтение текстовых сообщений, получение доступа к фотографиям, запись аудио, совершение и перехват телефонных звонков, получение *root*-прав на устройствах *Android.*

Известно несколько векторов заражения: фишинг, *SMS*-сообщения, маскировка под сайты и приложения телекоммуникационных компаний или производителей смартфонов.

Regin.

Страна происхождения: США.

Компания-разработчик: АНБ.

Целевыми объектами являются устройства с ОС *Microsoft Windows*, а также *GSM*-операторы.

Используются эксплойты нулевого дня в браузере, веб-эксплойты.

Ключевой особенностью является модульный подход, позволяющий загружать функции, которые точно соответствуют цели, и наличие собственной зашифрованной виртуальной файловой системы (*EVFS*).

Основными возможностями являются: извлечение конфиденциальной информации, такой как электронные письма и документы, а также компрометация операторов связи.

Пути заражения неизвестны.

Заключение

Результаты анализа методов, применяемых государствами для осуществления так называемого правительственного взлома, а также используемое ими ПО, показывает, что рассмотренная государственная деятельность имеет высокую степень деструктивного воздействия на информационные системы, программные продукты, аппаратные и программно-аппаратные устройства.

Применяемые методы требуют высокого уровня профессиональной подготовки всех участников, включенных в данную деятельность. Используемые при этом программные продукты имеют различное происхождение, пути внедрения и функционал. Любая ошибка в осуществлении правительственного взлома может привести к трагическим последствиям.

На основании вышеизложенного, предлагается проведение законодательного регулирования данной деятельности применительно как к Российской Федерации, так и в международном пространстве. Регуляторами в данном случае могут выступать такие международные организации, как Организация Объединенных Наций, Совет Европы, Содружество Независимых Государств, БРИКС и др. С одной стороны можно сказать, что вышеупомянутые действия со стороны правоохранительных органов нарушают права и свободы граждан. Однако стоит также учитывать обязательство правоохранительных органов обеспечивать безопасность граждан и государства. Законодательным органам стран предстоит ставить эти две точки зрения на «чаши весов» и разрабатывать процедуры и законы, обеспечивающие интересы всех сторон общества.

Литература

1. URL https://www.varonis.com/blog/government-hacking-exploits (дата обращения - январь 2024 г.).
2. URL https://aphilosopher.wordpress.com/2017/05/17/the-ethics-of-stockpiling-vulnerabilities (дата обращения - январь 2024 г.).
3. URL https://www.aclu.org/news/privacy-technology/us-government-malware-policy-puts-everyone-risk (дата обращения - январь 2024 г.).
4. URL https://amnesty.org.ru/ru/2015-08-21-MorganMarquis-Boire (дата обращения - январь 2024 г.).
5. Mayer J. Government Hacking // The Yale Law Journal, 2018. – № 3. – С. 570-662.
6. URL https://www.bu.edu/riscs/2021/05/03/abuse-resistant-government-backdoors (дата обращения - январь 2024 г.).
7. URL https://ru.wikipedia.org/wiki/Pegasus_(программное_обеспечение) (дата обращения - январь 2024 г.).
8. URL https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf (дата обращения - январь 2024 г.).
9. URL https://www.kaspersky.ru/blog/finspy-for-windows-macos-linux/31671 (дата обращения - январь 2024 г.).
10. URL https://securityintelligence.com/analysis-of-finfisher-bootkit (дата обращения - январь 2024 г.).
11. URL https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware (дата обращения - январь 2024 г.).
12. URL https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant (дата обращения - январь 2024 г.).
13. URL https://en.wikipedia.org/wiki/Cytrox#Predator (дата обращения - январь 2024 г.).
14. URL https://en.wikipedia.org/wiki/Hermit_(spyware) (дата обращения - январь 2024 г.).
15. URL https://en.wikipedia.org/wiki/Regin_(malware) (дата обращения - январь 2024 г.).