ЦРУ везде и всюду

Олег Демидов

Олег Демидов

УТЕЧКА: ЗНАЧЕНИЕ, МАСШТАБЫ И НОВЫЙ ВЗГЛЯД НА ЦРУ

7 марта на сайте проекта *Wikileaks* был опубликован массив данных под названием Year Zero, который, по словам администраторов проекта, является лишь первой частью более обширного массива, названного ими *Vault 7* («Убежище 7»). Утверждается, что вся эта документация изначально была подготовлена ЦРУ и представляет собой «базу знаний» ведомства о его программах по взлому электронных платформ и устройств, интернет-сервисов, перехвату содержимого онлайн-коммуникаций и осуществлению целевых операций в киберпространстве. Всего опубликованный массив насчитывает 8761 документ, включая 7818 веб-страниц и 943 приложенных файла, которые в сумме представляют собой структурированную библиотеку электронных документов с описанием уязвимостей в программном обеспечении (ПО), а также средств эксплуатации таких уязвимостей. Речь идет о разнообразных инструментах: эксплойтах, троянах, вирусах и компьютерных червях, руткитах, а также средствах обхода антивирусных продуктов, обманных систем (ханипотов) и иных систем защиты информации. В список целей ЦРУ входят десктопные и мобильные ОС (*Windows, iOS, Android*), низкоуровневые прошивки пользовательских устройств, сетевое оборудование для массового рынка (роутеры *Cisco*), программные прошивки устройств «умного телевидения» (*Samsung*) и систем автотранспорта, антивирусное программное обеспечение (ПО) и многие другие ниши ИТ-продукции для конечных пользователей.

Утечка является одной из крупнейших в истории ЦРУ и спецслужб вообще, и по объему раскрытых документов сразу же превзошла серию публикаций программ тайной электронной слежки и создания киберарсенала АНБ, начатую Эдвардом Сноуденом летом 2013 года. До этого достоянием общественности становились лишь отдельные кибероперации ЦРУ. В их числе разработка средств кибершпионажа и саботажа для замедления ядерной программы Ирана с 2005 по начало 2010-х гг. (включая печально известный компьютерный червь *Stuxnet*, внедрение которого в автоматизированные системы управления технологическим процессом (АСУ ТП) на производственном комплексе в г. Натанз в

2009–2010 гг. привело к выводу из строя каскада центрифуг для обогащения урана). Кроме того, в феврале 2017 г. *Wikileaks* публиковала документы, согласно которым в 2012 г. ЦРУ вело агентурную и электронную слежку за лидерами президентской избирательной кампании во Франции. То есть в принципе наличие у ЦРУ собственных киберсредств для целевых операций и программ их применения – не новость, однако масштаб таких программ до публикаций *Vault 7* никто не представлял.

При этом перед нами до сих пор лишь вершина айсберга – *Wikileaks* заявили, что опубликовали лишь первую часть утекшего архива (*Year Zero*), охватывающего документы за 2013–2016 год. Утверждается, что «база знаний» составляет лишь порядка 1% от общего объема информации по программам создания киберсредств ЦРУ, которыми уже располагают активисты. То есть речь может идти о многих сотнях тысяч документов, особенно если учесть, что то же АНБ начало разработку своих нынешних программ еще в начале 2000-х гг., и ЦРУ вряд ли сильно отстает от своих коллег. Общий объем массива самих средств вредоносного ПО ЦРУ оценивается в несколько сотен млн строк кода – для сравнения, код поискового движка *Google*, одного из крупнейших проектов в истории программирования, насчитывает порядка 2 млрд. строк.

Wikileaks приняли решение не публиковать файлы и документы, содержащие сам компьютерный код разработанного ЦРУ вредоносного ПО. Это разумно, так как публикация таких средств в открытом доступе мгновенно позволит пополнить ими свои арсеналы зарубежным спецслужбам и компьютерным преступникам по всему миру[1]. В этом смысле и перед ЦРУ, и перед *Wikileaks* сейчас стоит единственная общая задача – предотвратить распол-

---

[1] Похожие ситуации уже имели место. Например, в 2016 г. неизвестная хакерская группа *Shadow Brokers* опубликовала в Сети часть архива уязвимостей нулевого дня и вредоносного ПО. По словам представителей хакеров, этот инструментарий был изначально разработан военными из Агентства национальной безопасности (АНБ) США для собственных кибероперацией, а позднее использовался якобы связанной с АНБ хакерской группой *Equation Group*, у которой его и похитили *Shadow Brokers.* Так или иначе, после открытой публикации первой части архива и выставления на аукцион нескольких других массивов данных доступ к ним получили не только специалисты по информационной безопасности (ИБ) и представители компаний, чья продукция была целью вредоносного ПО (*Cisco, Fortinet, Juniper*), но и компьютерные преступники.

зание средств из киберарсенала ЦРУ по международному рынку компьютерной преступности.

Впрочем, значительная часть «базы знаний» содержит не готовые образцы вредоносного ПО или детальное описание уязвимостей, а скорее концепции, черновые наброски подходов к преодолению защиты и построению векторов атаки на те или иные ИТ-продукты и решения. Вообще, модель организации данных о киберарсенале спецслужбы достаточно любопытна: она представляет собой вики-массив электронных документов и файловых приложений, которые могут пополнять, редактировать и комментировать зарегистрированные пользователи системы.

Сообщество пользователей превышает 5 тыс. чел. и включает в себя штатных сотрудников ЦРУ и представителей компаний-подрядчиков (по некоторым оценкам, 10-12 структур), работающих со спецслужбой в рамках проектов по развитию киберсредств. Движок базы знаний также основан на ПО *Confluence*, разработанном частной компанией *Atlassian*. По мере обновления данных по тем или иным проектам формируются разные версии соответствующих вики-страниц – в общей сложности массив включает 1136 предыдущих версий отдельных страниц.

В итоге все это выглядит похоже на базу знаний какой-нибудь ИТ-корпорации, чем на архив документов спецслужбы в стереотипном представлении с нечитаемыми машинно сканами документов, грифами «секретно» и десятками подписей ответственных сотрудников. Разведка как бюрократическая машина тоже модернизируется, причем не только по формату, но и по стилю коммуникаций, который напоминает общение в хакерском сообществе и частных компаниях. Страницы с описаниями средств эксплуатации уязвимостей насыщены интернет-мемами, комментаторы зачастую позволяют себе весьма неформальную лексику, описывая грубые ошибки в коде систем, которые удалось взломать, и так далее. Для обмена идеями перспективных разработок с 2009 г. организован внутренний формат «Симпозиума по сетевым технологиям, инжинирингу, исследованиям и развитию» с иронической аббревиатурой *NERDS* (от англ. *nerd* – компьютерный фрик, «задрот»). Названия ряда техник атак и проектов по разработке вредонос-

ного ПО несут отсылки к популярным персонажам компьютерных игр и кинематографа.

Представители *Wikileaks* утверждают, что утечка произошла как раз вследствие действий инсайдера – зарегистрированного пользователя «базы знаний», который может быть как штатным сотрудником ЦРУ, так и представителем компании-подрядчика. Примечательно, что за последние годы крупнейшие утечки данных о программах развития киберсредств спецслужб США, прежде всего АНБ, происходили именно на стороне частных подрядчиков. Два наиболее громких эпизода – разоблачения Эдварда Сноудена и действия Гарольда Мартина III, скопировавшего огромный архив документов и кода «кибероружия» АНБ в 2016 г. Оба на момент утечек были сотрудниками *Booz Allen Hamilton*, достаточно известного подрядчика Минобороны и спецслужб США.

В массиве содержатся данные о виртуальной и физической инфраструктуре ЦРУ, используемой для организации и координации деятельности по перехвату данных в Сети и других форматах разведдеятельности с использованием информационных технологий. Например, европейский «филиал» Центра киберразведки, действующий на площадке консульства США во Франкфурте-на-Майне (ФРГ), выполняет роль базы для координации кибероперацій ЦРУ в Европе, Африке и на Ближнем Востоке. Кроме того, опубликованные материалы содержат информацию и о внутренней организационной схеме ЦРУ, которая включает разветвленную структуру технических подразделений, специализирующихся на разработке средств эксплуатации уязвимостей по отдельным направлениям платформ и ИТ-продуктов. Эта информация позволяет по-новому взглянуть на подход спецслужбы к организации деятельности по электронной слежке и целевым кибероперациям, а также оценить ее место среди приоритетов ведомства. Работа ЦРУ по развитию собственного киберпотенциала сконцентрирована в рамках одного из пяти управлений – Управления цифровых инноваций (*Directorate of Digital Innovation*). Его внутренняя организация пока известна лишь частично, но ключевой его структурой является Центр кибернетической разведки (*Center of Cyber Intelligence*), в компетенцию которого очевидно и входило развитие опубликованной «базы знаний» ведомства по киберсред-

ствам и непосредственная разработка последних. Деятельность Центра киберразведки разбита по трем ключевым направлениям (группам): Группе компьютерных операций (*Computer Operations Group, COG*), Группе физического доступа (*Physical Access Group, PAG*) и Группе инженерно-технических разработок (*Engineering Development Group, EDG*). Именно инженерно-техническая группа занималась разработкой, тестированием и сопровождением ПО, содержащегося в опубликованном *Wikileaks* массиве. Об остальных двух группах и их деятельности из опубликованных документов известно немного.

Наконец, конкретные направления и ниши разработки ПО распределялись между двумя подгруппами и их девятью отделами в составе Группы инженерно-технических разработок. Так, отдел мобильных устройств (*Mobile Devices Branch, MDB*) собирал уязвимости и разрабатывал средства их эксплуатации (эксплойты) для смартфонов, в основном фокусируясь на уязвимостях на уровне мобильных операционных систем (*iOS, Android*). Отдел автоматизированных программных имплантов (*Automated Implant Branch, AIB*) создавал вредоносное ПО, позволяющее эксплуатировать (использовать) уязвимости в десктопных продуктах – например, персональных компьютерах и ноутбуках под управлением операционной системы (ОС) *Windows*, а также устройств линейки *MacBook* от *Apple*. В свою очередь, отдел сетевых устройств (*Network Devices Branch, NDB*) отвечал за разработку техник и средств сетевых атак на веб-серверы и иную инфраструктуру Интернета. Проекты отдела встраиваемых систем (*Embedded Devices Branch, EDB*) включали в себя разработку средств эксплуатации уязвимостей в ПО различных «умных» устройств[2]. Например, отдел EDB работал над взломом «умных»

2 Встраиваемые системы являются одним из ключевых архитектурных элементов в «умных» устройствах. По сути, встраиваемая система представляет собой специализированный мини-компьютер – микропроцессорную систему управления, контроля и мониторинга, она работает, будучи встроена непосредственно в то устройство, которым управляет. Встраиваемые системы уже давно активно использовались в ряде областей, таких как телекоммуникационное оборудование, банкоматы и платежные терминалы, станки и производственное оборудование с числовым программным управлением (ЧПУ) проч. В настоящее время область применения встраиваемых систем радикально расширяется – во многом из-за развития индустрии и рыночных

телевизоров *Samsung F8000* и концепцией эксплуатации уязвимостей в ПО «умного» транспорта.

Столь разветвленная структура и глубокая нишевая специализация подразделений Центра киберразведки говорит о том, что в ЦРУ выстроена полноценная система «разделения труда», которая обеспечена техническими, финансовыми и человеческими ресурсами для того, чтобы одновременно развивать киберсредства для большинства крупнейших ниш продукции для конечных пользователей. В этом одно из коренных отличий программ спецслужбы от частных хакерских групп, включая группировки-источники постоянные источники повышенной угрозы (*Advance persistent threats, APTs*): частные игроки, даже самые продвинутые и опасные, сфокусированы на одной или нескольких смежных группах целей из-за ресурсных ограничений. Программы ЦРУ накрывают зонтиком едва ли не все ключевые для них ниши.

Другое отличие – в том, что государственные игроки никуда не спешат. Машинерия киберразведки ЦРУ явно выстраивалась долгие годы и будет работать еще дольше; спецслужба может позволит себе годами следить за разработками производителей и ждать, пока те допустят ошибки в коде и таким образом создадут новые уязвимости в своих продуктах – в отличие от частных группировок, действующих в рамках конкретных проектов, ограниченных по ресурсам и срокам.

Ресурсная база ЦРУ конкретно в части программ киберразведки пока неизвестна, но из организационной схемы ведомства ясно, что это направление стало одним из его ключевых приоритетов. А общий объем ресурсов ЦРУ весьма значителен. В 2014 г. усилиями Эдварда Сноудена были рассекречены данные о бюджете и количестве сотрудников ЦРУ: в 2013 г. финансирование ве-

---

продуктов Интернета Вещей, а также рынка мобильных устройств. Так, встраиваемые системы являются ключевыми аппаратными компонентами смартфонов и других гаджетов, всевозможной офисной технике и умной бытовой электронике (стиральные машины, микроволновые печи и прочие кухонные приборы с подключением к Сети). Встраиваемые системы необходимы для работы «умных» автомобилей и любого умного транспорта, в том числе в современных электроприводах двигателей; давно используются в авионике, GPS-приемниках и проч. Наконец, еще одной обширной сферой применения встраиваемых систем является современное медицинское оборудование, в том числе подключаемое к сетям связи.

домства превышало 4,8 млрд долл. США, а персонал – 21 тыс. чел. Если исходить из того, что «базу знаний» по программам киберразведки используют более 5 тыс. чел. (подрядчиков из них вряд ли большинство), то на разработку киберсредств может быть направлено до четверти всех ресурсов спецслужбы. Это ставит ЦРУ в один ряд с военными коллегами из АНБ и Киберкомандования и делает претендентом на статус оператора крупнейшей в мире программы разработки государственного киберарсенала.

Параллели и различия между программами АНБ и ЦРУ – один из самых интересных вопросов в нынешней истории. Но чтобы попытаться ответить на него, необходимо хотя бы вкратце обрисовать основные проекты разведслужбы по созданию киберпотенциала для целевых операций.

КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ЦРУ

Атаки на мобильные устройства. Одним из наиболее масштабных и опасных проектов ЦРУ, судя по *Vault 7*, является разработка средств обхода защиты, удаленного контроля и тайного сбора данных с мобильных устройств пользователей (планшеты, смартфоны).

Основными целями спецслужбы стали мобильные ОС *Android* от *Google* и *iOS* от *Apple*, которые в сумме занимают 98% глобального рынка ОС для мобильных устройств (порядка 85% у *Android* и 13% у *iOS*). Эти операционные системы сегодня используют примерно 2 млрд пользователей смартфонов, планшетов и других мобильных устройств практически в каждой стране мира. Каждой из этих ОС в документах ЦРУ посвящен отдельный каталог документов, которые содержат наборы уязвимостей в этих системах, описания техник атак и готовых образцов вредоносного ПО для эксплуатации выявленных уязвимостей. В этой работе был задействован отдел мобильных устройств (*MDB*). Каталог техник атаки на смартфоны с использованием уязвимостей в ОС *Android* содержит более 25 пунктов; для устройств на iOS разработано 14 техник атаки.

Среди разработок под *Android* – 8 эксплойтов (средств эксплуатации уязвимостей), позволяющих осуществлять удаленный до-

ступ к устройству после заражения; два из них нацелены на продукцию *Samsung* (смартфоны *Samsung Galaxy, Nexus* и планшеты *Samsung Tab*). Большинство разработок (15) основаны на технике атаки с повышением привилегий в системе: после изначальной доставки вредоносного кода в систему контролирующий его через Сеть злоумышленник может преодолевать различные слои защиты устройства и в конечном счете получить почти неограниченный контроль над ним (*root access*). При этом становятся доступны возможности удаленного управления камерой устройства, микрофоном, файлами и данными, хранящимися в системе, записи действий пользователя с клавиатурой (кейлоггинг), съема данных геолокации, записи переписки и разговоров, блокировки обновлений системы, самостоятельной установки и удаления приложений и проч. Три эксплойта адаптированы под заражение системы через уязвимости в мобильных браузерах (*Chrome, Opera,* мобильный браузер *Samsung*). Для реализации такой атаки пользователь должен перейти на скомпрометированный либо фишинговый сайт, с которого эксплойт незаметно загружается в систему и заражает ее. Сходные возможности предлагают эксплойты для устройств на *iOS* (*iPhone*). Однако полностью скомпрометировать защиту устройств *iPhone* позволяет лишь один эксплойт. Остальные эксплойты ЦРУ представляют собой техники атаки для преодоления отдельных средств и уровней защиты в программной платформе *iOS*. Так, некоторые вредоносные программы позволяют обходить «песочницу» (*sandbox*) – программную функцию в *iOS*, которая блокирует прямой доступ приложения к самой операционной системе.

По оценкам экспертов, в сумме применение таких эксплойтов позволяет практически полностью взломать защиту тех версий мобильных ОС, под которые они разработаны. Однако из архива данных *Vault 7* складывается впечатление, что ЦРУ несколько отстает в написании средств эксплуатации уязвимостей от развития и обновления самих ОС. Так, эксплойты для *iPhone* и планшетов *iPad* не адаптированы для *iOS 10* – более новой версией мобильной ОС от *Apple*, которая на сегодня установлена почти у 80% пользователей соответствующих устройств.

Вообще положение с уязвимостями достаточно интересно. С одной стороны, только в разработках для компрометации мо-

бильных устройств использовано до нескольких десятков так называемых уязвимостей нулевого дня (*zero-days*) в мобильных ОС. Особая опасность таких уязвимостей в том, что они неизвестны вендору (производителю) соответствующего продукта и отраслевому сообществу – а значит, они еще не закрыты, для них не разработаны исправления (патчи), которые устраняют угрозу атаки. Отсюда и понятие «нулевого дня». Однако в то же время быстрое обновление версий мобильных ОС на рынке во многом сводит на нет успехи ЦРУ в выявлении уязвимостей нулевого дня и разработке использующих их средств для версий ОС прошлого поколения. Так, сразу после публикации *Vault 7* представитель *Apple* сообщил СМИ, что все ключевые уязвимости, выявленные ЦРУ в *iOS*, уже устранены компанией. Отсюда может следовать двоякий вывод – либо ЦРУ и вправду пока не успевает за рынком, либо в *Vault 7* просто не отражены последние наработки спецслужбы: по оценкам экспертов, база знаний отражает ситуацию с развитием проектов «мобильного» отдела полтора-два года назад. С тех пор ЦРУ вполне могло существенно продвинуться и в поиске уязвимостей в новых версиях мобильных ОС, и в разработке средств атак на них.

Интересен и тот факт, что именно по направлению компрометации защиты мобильных устройств ЦРУ наиболее тесно сотрудничало с другими спецслужбами и частными подрядчиками. Так, многие уязвимости (в том числе *zero-days*) и основанные на них эксплойты, судя по пометкам в документах проекта, были разработаны совместно с АНБ и британским Центром правительственной связи (*GCHQ*, давний партнер АНБ по развитию программ массового перехвата электронных данных), либо выкуплены у неназванных частных партнеров. Это немедленно послужило поводом для обвинений в том, что ЦРУ тратит средства госбюджета на коллекционирование и сохранение уязвимостей в продуктах американских ИТ-компаний вместо того, чтобы раскрывать и ликвидировать их.

Особую тревогу у пользователей вызвали сообщения том, что эксплойты ЦРУ позволяют взламывать защиту приложений на мобильных устройствах и свободно перехватывать переписку из защищенных мессенджеров. Представители *Wikileaks* несколько

неточно осветили этот момент в своем анализе, заявив, что разработки ЦРУ позволяют «обходить криптографическую защиту» и собирать данные из защищенных сервисов и мессенджеров, включая *WhatsApp, Signal, Telegram, Weibo, Confide* и *Cloackman* за счет «взлома» устройств, на которых установлены такие сервисы. Это не совсем так. Инструменты ЦРУ действительно позволяют собирать данные переписки, которую пользователь ведет в защищенных мессенджерах – но их криптографическая защита при этом остается нетронутой. Вместо этого в тех случаях, когда внедрение эксплойта дает злоумышленнику удаленный доступ к устройству, для чтения переписки используются возможности других его приложений. Например, активируется функция снимков экрана устройства (скриншотов) в тот момент, когда пользователь запускает приложение-мессенджер и ведет в нем переписку. Сохраненные скриншоты со снимками текста переписки отсылаются на сервер, который контролируют агенты ЦРУ. Аналогично, если пользователь сохраняет полученные через мессенджер фото и другие файлы в файловом хранилище смартфона, эти данные также пересылаются ЦРУ – не из мессенджера, а из файлового хранилища взломанного устройства. Такие методы сбора данных после установления контроля над устройством довольно похожи на программы того же АНБ (*XKeyScore* и *PRISM*), ранее раскрытые Сноуденом. При этом ЦРУ не создало инструментов, которые бы позволяли преодолевать криптографическую защиту самих мессенджеров и расшифровывать данные из них напрямую. Скомпрометированы в данном случае операционные системы самих устройств, а не сторонние защищенные приложения.

АТАКИ НА ДЕСКТОПНЫЕ УСТРОЙСТВА И СЕТЕВОЕ ОБОРУДОВАНИЕ

По аналогии с разработкой средств атак на мобильные ОС, ЦРУ создало отдельную подборку уязвимостей и линейку эксплойтов для взлома операционных систем и других программных платформ десктопных (настольных) устройств. Основной целью в этом сегменте стала ОС Windows, а главным разработчиком - отдел автоматизированных имплантов (AIB). Сотрудникам спец-

службы удалось выявить достаточно обширный перечень уязвимостей в ОС от *Microsoft*, включая ряд уязвимостей нулевого дня, и создать серию техник атаки и образцов вредоносного ПО для их эксплуатации. Часть из таких эксплойтов может быть внедрена в систему удаленно – через содержащий вредоносный код файл, направленный фишинговым электронным письмом, или при входе на скомпрометированный сайт в Интернете. Однако существенная часть средств предполагает локальное внедрение в систему – то есть через внешний носитель. Это важный для ЦРУ функционал, так как целевые операции ведомства зачастую требуют доступа к системам и инфраструктуре, которая находятся на защищенных объектах и надежно изолированы от сети. Так, в линейку средств ЦРУ входят вирусы для передачи информации с компьютеров под управлением *Windows*, физически изолированных от сети (air-gapped systems). Одним из таких инструментов является *HammerDrill v2.0*: средство, которое внедряется в *Nero* – популярное ПО для записи информации на оптические диски (*CD* и *DVD*) и затем передается с компьютера на компьютер вместе с диском, на которое записано. Попадая на компьютер под управлением *Windows*, *HammerDrill* заражает его вредоносной программой-трояном и может собирать с системы необходимые данные. Другие направления разработки включают средства для заражения программой-трояном внешних *USB*-носителей (флэшек), которые также при попадании в систему под *Windows* запускают вредоносный код и собирают из системы необходимые данные. Некоторые инструменты используют достаточно нестандартные техники для тайного сбора данных из систем под управлением *Windows*. Так, средство *Brutal Kangaroo* («Жестокий кенгуру») записывает данные в скрытую область жесткого диска системы – *NTFS*, стандартную файловую систему на устройствах под *Windows*. Еще один модуль вредоносного ПО – *PICTOGRAM* («Пиктограмма») сохраняет скопированную из системы информацию с помощью стеганографии – т.е. сокрытия данных внутри уже существующего на устройстве файла изображения (фото, картинка). Кроме того, отдельный каталог средств атаки на ПК под управлением ОС *Windows* был разработан отделом встраиваемых систем (*EDB*).

Нужно отметить, что системы под управлением *Windows* стали главной, но все же не единственной целью программ ЦРУ по взлому десктопных устройств. Для настольной продукции *Apple* (*MacBook*) был разработан руткит (вредоносное ПО, позволяющее злоумышленнику дистанционно контролировать систему на уровне программного ядра) под названием *QuarkMatter*. После внедрения в систему с помощью эксплойта это ПО переписывает низкоуровневую программную прошивку *EFI* на устройствах *MacBook*, давая автору атаки контроль над системой. Поскольку прошивка *EFI* находится ниже по уровню, чем сама ОС *MAC*, такое вредоносное ПО крайне трудно обнаружить и самостоятельно удалить из системы.

Эксплуатация уязвимостей в ОС различных устройств (ПК и сетевого оборудования) осуществлялась и в рамках другого проекта инженерно-технической группы: *HIVE*. Проект реализован в виде вики-каталога вредоносного ПО, который содержит специализированные и при необходимости обновляемые программные закладки (*implants*) для различных ОС и программных платформ, в том числе *Windows, OS X, Solaris, MikroTik* (используется в маршрутизаторах) и *Linux*. Закладки в данном случае представляют собой скрытно внедряемые в систему программы, либо преобразованные фрагменты кода исходной программы, которые позволяют осуществлять несанкционированный доступ к ресурсам системы, изменяя свойства ее защиты. То есть, внедряя программные закладки за счет эксплуатации найденных в перечисленных ОС уязвимостей, ЦРУ в дальнейшем могло осуществлять удаленный контроль через сеть над устройствами. В рамках *HIVE* описывается специальная служебная сетевая инфраструктура, которая позволяет агенту удаленно взаимодействовать с внедренными в устройства закладками, и таким образом осуществлять дистанционный контроль устройств, снимать с них нужные данные и т.д. Такая инфраструктура включает в себя виртуальные серверы, развернутые в сети ЦРУ: *Listening Post (LP)/Command and Control (C2)*. Эта инфраструктура способна поддерживать ряд доменных имен, каждое из которого выделено для взаимодействия с той или иной закладкой. Запросы к таким доменным именам перенаправляются на какого-либо публичного коммерческого провайдера

виртуальных частных серверов (*VPS*). На такой открытый сервер и направляется трафик от внедренной в систему закладки через защищенный протокол *HTTPS*. Далее такой трафик еще дважды перенаправляется на различные промежуточные серверы в Сети с помощью технологий *VPN* (виртуальная частная сеть) – и наконец обрабатывается на одном таких серверов.

АТАКИ НА «УМНЫЕ» ТЕЛЕВИЗОРЫ

Много шума в СМИ наделал и проект Отдела встраиваемых систем (*EDB*) ЦРУ *Weeping Angel* («Плачущий ангел») по взлому с целью скрытого сбора данных «умных» телевизоров *Samsung* серии *F8000*, подключаемых к Интернету. В массиве документов *Year Zero* присутствует раздел этого проекта, включающий 7 страниц и историю из 18 правок. Любопытно, что проект ЦРУ осуществляло не в одиночку, а вместе с британской контрразведкой *MI5*: в июне 2014 г. представители технических подразделений спецслужб провели совместный семинар, на котором обсуждался ход проекта, задачи на будущее и фиксировались достигнутые результаты. Вкратце, они таковы: для моделей серии *F8000*, использующих программные прошивки определенных версий (1111, 1112 и 1116) был реализован ряд возможностей по удаленному сбору данных и введению в заблуждение пользователей устройств. После того, как разработанные ЦРУ средства внедрялись в систему, при выключении устройства владельцем активировался режим, имитирующий отключение системы (*fake-off mode*). Отключался экран и светодиодные индикаторы на передней панели устройства, что создавало у пользователя впечатление, что его телевизор действительно выключен. При этом микрофон, которым оснащены *LED*-телевизоры *Samsung F8000,* напротив, включался и записывал аудиоданные – а именно, используя встроенную систему распознания голоса, разговоры людей рядом с устрйоством. Записанные данные затем сохранялись (в объеме до 700 мегабайт) и отправлялись на сервер, контролируемый спецслужбой. Таким образом, «умные ТВ» Samsung фактически исполняли функцию устройств для тайной прослушки собственных пользователей.

Выполнение телевизором таких функций обеспечивалось за счет внедрения в его ПО специального кода – компактной программы, имитирующей функции командного интерпретатора (*TinyShell*), которая взаимодействовала с программной прошивкой устройства и позволяла осуществлять удаленное выполнение команд и передачу файлов (например, записанного на микрофон аудио). Речь не идет о вирусе или компьютерном черве – лишь о средстве удаленного исполнения команд на устройстве.

Проект немедленно вызвал зловещие ассоциации с телекранами из оруэлловского «1984». Однако в действительности ЦРУ и их британским коллегам удалось достичь лишь частичного успеха в его реализации. В том же отчете с июньского семинара с *MI5* приводится обширный список проблем и нерешенных задач. Первая и ключевая из них – спецслужбам, по крайней мере на тот момент, не удалось обеспечить возможность внедрения необходимого ПО в программную прошивку телевизоров дистанционно, через Интернет. По сути, единственным способом получить контроль над тем или иным конкретным устройством было внедрение в него программной нагрузки через внешний съемный носитель – например, *USB*-флэшку. Т.е. вместо того, чтобы эксплуатировать глобальную систему аудиопрослушки, распространителем которой выступал бы сам Samsung, ЦРУ пришлось бы организовывать агентурную операцию каждый раз, когда нужно поставить под контроль один конкретный телевизор. Кроме того, идея проекта хромает и из-за ряда мелких технических недоработок. Например, в режиме имитации отключения устройства блокировалось подключение к сетям *Wi-Fi*, не отключались светодиодные индикаторы на задней панели телевизора – в итоге пользователь мог заподозрить, что устройство работает ненормально. Кроме того, разработанное для удаленного исполнения команд ПО не работало с программными прошивками *F8000* после версии 1116, – соответственно, обновление прошивки телевизора сводило на нет всю проделанную работу.

ЦРУ пыталось решить эти проблемы – так, в документах имеется информация о том, что разработанное спецслужбой ПО может блокировать обновление прошивки телевизоров. Ставилась задача доработать режим имитации отключения и, конечно, обе-

спечить возможность дистанционного внедрения в телевизоры ПО для удаленного исполнения команд. Еще одной задачей было обеспечить возможность передачи записываемого с ТВ аудиотрафика через Интернет в режиме стриминга, т.е. в реальном времени, вместо того, чтобы получать из хранилища устройства ранее записанные аудиофайлы. Наконец, по аналогии со сбором аудиоинформации через микрофон планировалось реализовать функцию сбора данных (скриншотов) через встроенную камеру умного телевизора. Но о том, удалось ли решить эти задачи, ничего не известно – обновления данных о «Плачущем ангеле» заканчиваются файлом о семинаре 2014 г.

В общем и целом, на оруэлловскую антиутопию этот проект явно не тянет. Кроме того, ЦРУ отнюдь не является пионером идеи взломать устройства «умного телевидения». В марте 2013 г. на знаменитой хакерской конференции *BlackHat* исследователи Аарон Граттафиори и Джош Явор рассказали об обнаруженных ими уязвимостях безопасности в системах «умных телевизоров» – причем именно производства *Samsung*. Возможности эксплуатации этих уязвимостей по большей части совпадают с тем, чего пытались достичь ЦРУ и *MI5*. Это не означает, что отраслевые специалисты «подарили» ЦРУ идею проекта – просто уже к 2013 г. проблемы с безопасностью и уязвимости умных телевизоров были уже достаточно широко известны как ИТ-отрасли, так, видимо и спецслужбам.

РАЗРАБОТКА КОНЦЕПЦИИ АТАК НА «УМНЫЙ» ТРАНСПОРТ

Другой проект отдела встраиваемых систем (*EDB*), который был отмечен в анализе утечек *Wikileaks* и цитируется СМИ – поиск возможностей и разработка концепций программного обеспечения для взлома систем умного транспорта, включая автомобили. На сайте *Wikileaks* отмечается, что появление у спецслужбы подобных инструментов может быть использована для организации «практически неотслеживаемых покушений» путем взлома умных автомобилей и провоцирования автокатастроф. В самом массиве данных ЦРУ присутствует документ 2014 г. – протокол встречи отдела *EDB*, в котором приводится список «перспектив-

ных направлений работы» подразделения. В перечне среди прочего фигурирует разработка средств для эксплуатации устройств Интернета Вещей, а также систем транспорта и операционной системы *QNX*. *QNX* это коммерческая распределенная ОС для рынка встраиваемых систем, разработанная канадской компанией *Quantum Software Systems*; в 2010 г. приобретенная разработчиком защищенных средств коммуникации *BlackBerry*. В настоящее время она используется в ряде отраслей, включая *3D*-навигацию и развлекательные мультимедийные системы. Но в последнее время *BlackBerry* продвигает *QNX* прежде всего в нише управления различными системами умного автотранспорта. В настоящее время основанные на *QNX* мультимедийные системы используются примерно в 60 млн автомобилей производства *Ford, Fiat* и *Maserati*. В октябре 2016 г. *Blackberry* расширила сотрудничество с *Ford*, подписав соглашение, согласно которому разработка *Ford SYNC* – информационно-развлекательной системы нового поколения в автомобилях *Ford* будет вестись на базе *QNX*.

Таким образом, ЦРУ действительно рассматривало возможности эксплуатации систем умного автотранспорта, ориентируюсь на поиск уязвимостей в ключевых программных платформах в этой нише. Потенциальные возможности в этой сфере огромны, т.к. современные автомобили до предела насыщены информационными технологиями и системами обмена данными на различных уровнях от тех же систем развлечения и предоставления информации водителю до систем, передающих телематические данные и непосредственно контролирующих работу ключевых узлов автомобиля, включая фары, тормоза, рулевое управления и сам двигатель. Даже если не говорить о нише беспилотных авто и наиболее прорывных проектов с точки зрения компьютеризации систем управления (*Tesla*), достаточно упомянуть, что ПО легковых авто последнего поколения по данным того же *Ford* составляет до 150 млн строк кода – больше, чем в магистральных авиалайнерах. В столь сложных системах неизбежно находятся уязвимости, позволяющие построить вектор атаки, особенно если их неотъемлемой функцией является беспроводная передача данных через *Wi-Fi* и *Bluetooth*. Как и в случае с «умными телевизорами», ЦРУ не первым обратило внимание на возможности

взлома умных авто. В последние два-три года взлом различных компонентов «умных авто» стал одним из популярных упражнений для специалистов по информационной безопасности. Одним из наиболее ярких примеров можно назвать взлом систем управления 2014 *Jeep Cherokee*, который успешно провели в 2015 г. ИБ-исследователи Чарли Миллер и Крис Валасек. За счет эксплуатации уязвимости в информационно-развлекательной и навигационной системе Uconnect экспертам в конечном счете получить контроль над управляющими системами автомобиля, что позволило удаленно поворачивать руль, кратковременно блокировать тормоза и заглушить двигатель. По итогам тестового взлома производитель (*Fiat Chrysler*) вынужден был отозвать 1,4 млн авто для устранения уязвимостей. Вопиющим случай оказался еще и потому, что за счет уязвимости в системе Uconnect исследователи получили возможность удаленного доступа к тысячам других использующих ее транспортных средств.

Однако и в этом случае огромные потенциальные возможности не были реализованы ЦРУ, если судить по опубликованной части массива *Vault 7*. Документ *EDB* по сути представляет собой стенограмму «мозгового штурма» с намеченными направлениями будущей работы. В нем отсутствуют списки конкретных уязвимостей в ПО «умных авто», для которых предлагается разработать средства эксплуатации. Тем более не упоминаются сами такие средства и какие-либо проработанные векторы атак. Даже сама постановка задачи с «невидимыми покушениями» является домыслом аналитиков *Wikileaks*, в чем те честно признаются. Опять же, мы имеем дело с неполным набором данных и информация может поменяться по мере дальнейшей публикации утечек. Но пока все указывает на то, что к 2014 г. ЦРУ только стало задумываться о развитии средств проведения целевых операций за счет вторжения в информационные системы умного транспорта. Как и в случае с «умными телевизорами», ход мысли спецслужбы пока запаздывает по отношению к развитию дискуссии в частной отрасли ИБ. Вместе с тем, это никак не устраняет проблему на будущее – разведслужба несомненно создаст действующие инструменты для кибероперацией с умным транспортом, это лишь вопрос

времени. В этом смысле аналитики *Wikileaks* имеют полное право нагнетать тревогу – несмотря на усилия исследователей, угроза эксплуатации ИТ-инфраструктуры умного транспорта в кибероперациях спецслужб пока явно недооценена его производителями и пользователями.

ОБХОД СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

Отдельным направлением работы спецслужбы стало создание целой линейки средств вредоносного ПО для компрометации и обхода самых распространенных антивирусных решений для конечных пользователей и корпоративных клиентов. Каталог с описанием таких средств для 21 антивирусного продукта, включая таких отраслевых лидеров как *Comodo, Avast, Kaspersky, AVG, ESET, Symantec, Microsoft Security Essentials* (встроенный антивирус для Windows) и проч. представлен в документе *Personal Security Products* (Персональные продукты для обеспечения безопасности). Документы с техническим описанием средств эксплуатации уязвимостей конкретных антивирусов, за исключением *Avast*, имеют секретный статус и пока не опубликованы *Wikileaks*. Однако подробное описание разработанным ведомством подходов к эксплуатации уязвимостей антивирусной защиты доступно в отдельных приложениях и охватывает продукты *F-Secure, Avira, AVG,* Лаборатории Касперского и *Comodo*. Используемые техники и средства эксплуатации уязвимостей в антивирусном ПО достаточно разнообразны и продвинуты, но не во всех случаях гарантируют их авторам гарантированный обход всех средств антивирусной защиты от того или иного производителя. Например, для обхода защиты продуктов Лаборатории Касперского эксплуатируется ошибка в обработке обращений самого антивируса к одной из динамически подключаемых библиотек (*DLL*) в ОС *Windows*. В результате злоумышленник может подменить исходную библиотеку собственной, к которой и будет обращаться рабочий процесс антивируса – таким образом, антивирусная защита будет преодолена и открыта возможность для атаки на систему. Однако такая уязвимость присутствует только в предыдущих версиях антиви-

русного ПО Лаборатории Касперского, которые адаптированы для работы с *OS Windows XP* и *Windows 7*. То есть сегодня эта уязвимость по большому счету неактуальна и скорее имеет для базы знаний ЦРУ архивную ценность. Для обхода защиты других антивирусных средств (*F-Secure, Avira*) используются две уязвимости в функционировании их эвристических алгоритмов обнаружения и классификации потенциальных вредоносных программ. Частичный обход защиты антивируса *Comodo* возможен за счет размещения вредоносного кода в разделе «Корзина» для удаленных файлов, который не анализируется антивирусом. При этом использование этой уязвимости лишь открывает путь для незаметной доставки на устройство вредоносного кода, но не отключает антивирус и не дает беспрепятственно установить полный контроль над системой.

Главный вывод по этому направлению работы формулируют сами сотрудники ЦРУ в своих примечаниях к техническому описанию средств эксплуатации уязвимостей: дело не в блестящем уровне созданных спецслужбой эксплойтов, а в обилии грубых и местами курьезных ошибок в коде самих антивирусных средств. И даже с учетом этого в ряде случаев ведомству удалось выявить уязвимости и разработать средства их эксплуатации лишь для старых и уже в основном неактуальных версий антивирусного ПО. Однако «в пользу» ЦРУ свидетельствует тот факт, что те или иные уязвимости удалось выявить в продуктах практически всех крупнейших компаний антивирусной отрасли.

ПРОТИВОДЕЙСТВИЕ РАССЛЕДОВАНИЮ КОМПЬЮТЕРНЫХ АТАК

Помимо разработки средств обхода и эксплуатации антивирусной защиты устройств пользователей, сотрудники ЦРУ уделили серьезное внимание мерам противодействия расследованию совершаемых ими атак и иных операций. В базе данных ведомства содержится блок детальных инструкций по техникам написания кода вредоносного ПО и осуществления компьютерных атак таким образом, чтобы не оставлять «цифровых отпечатков», которые бы компрометировали саму спецслужбу, а также прави-

тельство США и «организации-партнеров» при расследовании инцидентов. При этом ставится задача затруднить расследования не только для компаний, специализирующихся на такой деятельности, но и для крупнейших разработчиков и производителей продукции, которая входит в список целей операций ЦРУ (в том числе *Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens*), а также антивирусных компаний. Одним из источников рекомендаций по написанию вредоносного ПО служит документ-мануал «Правильные и неправильные методы проведения специальных мероприятий» («*Tradecraft DO's and DON'Ts*»). Весьма интересный документ «Требования к криптографии Управления сетевых операций» содержит подробные инструкции по применению сотрудниками ЦРУ средств криптографической защиты информации при организации сетевых атак, удаленном управлении вредоносным ПО на зараженных системах. Отдельные документы содержат инструкции и требования к передаче агентами через сети связи собранных в ходе операции данных и отправке сообщений, а также непосредственно внедрению в информационные системы вредоносного ПО и осуществлению длительного контроля над скомпрометированными устройствами.

НАКОПЛЕНИЕ И ИСПОЛЬЗОВАНИЕ ЧУЖИХ РАЗРАБОТОК ВРЕДОНОСНОГО ПО

В дополнение к разработке собственного вредоносного ПО ЦРУ активно изучало чужие разработки и стремилась заимствовать и адаптировать их для решения свих задач. В рамках Отдела удаленной разработки (*RDB*) действовала отдельная группа *UMBRAGE*, в задачи которой создание репозитория (пополняемой базы данных) образцов вредоносного кода, добытого ЦРУ на черном рынке, полученного в ходе собственных расследований чужих кибероперацийлибо предоставленного коллегами из АНБ и других спецслужб, а также из частного сектора. В опубликованной *Wikileaks* версии репозитория содержатся данные о нескольких десятках образцов вредоносного ПО и техниках осуществления компьютерных атак. Согласно краткому описанию в шапке самого документа, поддер-

жание такой базы данных с точки зрения спецслужбы могло нести двойную пользу. Во-первых, «полуфабрикатные» образцы чужого вредоносного кода могут быть быстро и с небольшими ресурсозатратами доработаны для решения ЦРУ точечных задач вместо разработки с нуля многофункциональных собственных инструментов. То есть речь идет о банальной оптимизации использования ресурсов по принципу «зачем изобретать свое, если можно взять чужое». Во-вторых, применение заимствованных у киберпреступников и, возможно, зарубежных хакерских группировок паттернов вредоносного ПО и техник компьютерных атак опять же помогает решит задачу запутывания расследования инцидентов и уничтожения своих «цифровых отпечатков».

Собранные в репозитории группы *UMBRAGE* средства и их компоненты достаточно разнообразны и включают в себя кейлоггеры (программы, записывающие действия пользователя с клавиатурой), сборщики паролей, модули для перехвата изображения и звука с вебкамер персональных устройств, средства уничтожения информации на диске, повышения привилегий, обхода антивирусов и проч. Стоит также отметить, что объектом внимания спецслужбы стали кибероперации отдельных группировок, предположительно связанных с их военными коллегами из АНБ. Так, отдельный файл посвящен анализу ошибок, которые привели к раскрытию деятельности *Equation Group* – группировке-источнику повышенной угрозы (*APT*), которая в течение 14 лет с 2001 по 2015 гг. атаковала при помощи крайне передовых средств вредоносного ПО правительственные и корпоративные цели как минимум в 42 странах, оставаясь незамеченной. В конечном счете деятельность Equation Group была раскрыта Лабораторией Касперского благодаря ряду допущенных членами группировки ошибок в техниках атак и «заметании следов» – и теперь ЦРУ пытается предусмотреть эти ошибки.

МАСКИРОВКА АГЕНТУРНЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНОГО ПО

Наконец, важный для понимания методов целевых операций ЦРУ проект – *Fine Dining*, еще один инструментарий техник атак. При-

мечателен он тем, что содержит 24 «обманных» программ, которые позволяют агенту ЦРУ внедрять в систему вредоносное ПО прямо при свидетелях. Эти приложения визуально маскируют процесс работы агента с устройством, в результате у непосвященного наблюдателя эта деятельность не вызовет подозрений: средства *Fine Dining* позволяют маскировать процесс внедрения вредоносного ПО под запуск агентом видеоплеера, работу с презентацией в *PowerPoint*, компьютерную игру и даже запуск антивирусного сканера (Антивирус Касперского, *McAfee, Sophos*). Разработка столь изощренного инструментария показывает, насколько большую роль в программах киберразведки ЦРУ играет агентурная работа – и в то же время, насколько возможности спецслужбы ограничены необходимостью внедрять в системы вредоносное ПО не удаленно, через сеть, а через прямой физический доступ. Для сравнения, ничего подобного в киберарсенале АНБ за 4 года разоблачений не нашлось – и это логично, т.к. военные работают в рамках концепции радиоэлектронной разведки (*signals intelligence, SIGINT*) и развивают технологии удаленных атак на системы. Для ЦРУ же основным форматом исторически являлась именно агентурная разведка (*human intelligence, HUMINT*). В этом смысле весь гигантский киберарсенал ведомства, включая ПО и инфраструктуру для удаленных операций в Сети, по большому счету остается продвинутым технологическим приложением к полевой работе агентов – хотя документы *Vault 7* и позволяют говорить о технологически обусловленном синтезе *SIGINT* и *HUMINT*.

НЕКОТОРЫЕ ВЫВОДЫ И НАБЛЮДЕНИЯ

Любые обобщения в отношении нынешней утечки и программ развития киберсредств ЦРУ следует считать промежуточными и неполными, пока не опубликованы остальные имеющиеся в распоряжении *Wikileaks* данные. С этой оговоркой уместно обозначить несколько моментов.

1. Систематическая и развернутая в индустриальном масштабе деятельность ЦРУ по развитию собственного арсенала киберс-

редств для целевых разведопераций создает достаточно серьезную постоянную угрозу как для пользователей, так и для вендоров продукции и решений в широком диапазоне ниш ИТ-рынка. Прежде всего речь идет о продукции для конечных пользователей. Наиболее тревожной ситуация выглядит для ниши ОС, как для настольных, так и для мобильных устройств. За счет концентрации ресурсов на сборе уязвимостей и создании средств их эксплуатации для двух мобильных ОС, в сумме занимающих почти весь глобальный рынок, ЦРУ обладает эффективными средствами атак на мобильные устройства абсолютного большинства пользователей в мире. При этом возможность комбинации большого числа различных техник и эксплойтов делает задачу защиты от таких атак нетривиальной. «Запаздывание» групп разработчиков ЦРУ по сравнению с работой вендоров по закрытию уязвимостей и обновлению версий ОС и прошивок их устройств не снимает проблему: судя по всему, передовые разработки спецслужбы за последние пару лет просто не попали в массив данных утечки. Сложившаяся ситуация ставит перед крупнейшими вендорами ОС, а также самих мобильных и десктопных устройств (*Apple, Google, Microsoft, Samsung* и др.) задачу по выработке консолидированной стратегии повышения уровня защиты ОС и разработки новых архитектурных решений и стандартов для нейтрализации системной угрозы со стороны государственных программ электронной разведки.

2. ИТ-отрасль США, за исключением узкого круга специализированных подрядчиков спецслужб, не выглядит вовлеченной в те или иные формы сотрудничества с ЦРУ. В массиве данных *Vault 7* нет данных о взаимодействии ИТ-вендоров и разработчиков со разведслужбой. Речь идет лишь о том, что ЦРУ методично и целенаправленно собирала информацию об уязвимостях в продукции различных компаний и разрабатывала разнообразные средства эксплуатации этих уязвимостей – самостоятельно и при содействии других спецслужб и подрядчиков. В этом смысле нынешний сюжет несколько отличается от истории программ АНБ. Во-первых, после публикации данных, добытых Эдвардом Сноуденом в 2013 г., на крупнейшие американские ИТ-корпорации и их сервисы (*Yahoo, Google, Facebook YouTube, Skype, Apple*) пали подозрения в сотрудни-

честве с АНБ в рамках глобальной программы *Prism*, позволявшей спецслужбе перехватывать колоссальные объемы данных пользователей за счет прямого доступа к корпоративным серверам, где эти данные хранились и обрабатывались. Отраслевые гиганты резко отрицали свое сотрудничество с АНБ, однако окончательную истину в этой ситуации вряд ли удастся установить. Во-вторых, в рамках программы *Bullrun*, нацеленной на компрометацию средств криптографической защиты данных, АНБ подкупала и принуждала разработчиков таких средств внедрять в свои решения для массового рынка бэкдоры (*backdoor* – в данном случае программные средства, позволяющие третьей стороне получать доступ к содержимому зашифрованных коммуникаций между двумя сторонами, в том числе системы депонирования (передачи) ключей шифрования). То есть в той или иной степени частный ИТ-сектор США оказался вовлечен во взаимодействие с АНБ – сегодня в ситуации с ЦРУ таких фактов пока не наблюдается.

3. Несмотря на весь свой масштаб и технологическую изощренность, созданный ЦРУ киберарсенал не является инструментом массового неизбирательного перехвата и сбора данных (*bulk data interception*). Формула, которая отражает назначение раскрытых программ ЦРУ: «глобальный инструментарий для точечных целевых операций». В части кибероперацій перед разведслужбой никогда не стояла задача подлинно массового сбора данных – не в смысле фактического объема добываемых сведений, а в смысле избирательности применения средств их сбора и постановки задач. Здесь снова нужно подчеркнуть, что несмотря на активное развитие ЦРУ средств дистанционной электронной разведки (*SIGINT*), основной парадигмой его деятельности по-прежнему остаются целевые агентурные операции (*HUMINT*). В соответствии с требованиями времени киберарсенал служит высокотехнологичным и жизненно необходимым приложением к ним – но не наоборот, по крайней мере пока что.

Избирательный характер операций и сбора данных – ключевое отличие между программами развития киберсредств ЦРУ и АНБ. Амбиции военных простираются дальше: грубо говоря, в рамках раскрытых Сноуденом программ АНБ стремилось создать инстру-

ментарий, позволяющий перехватывать обмен данными в рамках если не всего Интернета, то каких-то его существенных сегментов. Именно поэтому проекты АНБ предполагали не только сбор данных с устройств конечных пользователей, но и, прежде всего, доступ к инфраструктурным узлам, где концентрируются огромные массивы интернет-трафика и других данных: серверы, облачные хранилища и дата-центры крупнейших интернет-компаний, крупнейшие узлы телекоммуникационной инфраструктуры, включая даже магистральные волоконно-оптические линии связи. В эту же логику укладывается и работа по компрометации ключевых средств шифрования трафика в Сети в рамках программы Bullrun. В такой парадигме целевые операции против конкретных лиц и систем – второстепенная задача. Более того, логика работы с большими данными (*big data*) подобного масштаба может предполагать в корне иной алгоритм организации задач: сначала осуществляется перехват массивов «сырых» данных, и уже по итогам его аналитической обработки идентифицируются конкретные цели и объекты дальнейших (например, контртеррористических) операций.

Для сравнения, лучшим примером подхода ЦРУ к кибероперациям до сих пор можно считать *Stuxnet*: под узкую, специфическую задачу с нуля был создается масштабный арсенал высокоизбирательных средств, гарантирующих поражение высокозащищенной цели. Опять же, не случайным выглядит отсутствие в базе знаний ЦРУ проектов по взлому инфраструктуры, на которой концентрируются большие объемы данных (те же облачные сервисы, дата-центры, серверы крупнейших сервис-провайдеров и проч.). Большинство проектов ЦРУ сконцентрировано на устройствах и системах, с которыми взаимодействуют конечные пользователи. Также существенные ресурсы направлены на разработку средств преодоления устройств, изолированных от Сети (*air-gapped*), в том числе использующих довольно устаревшие, почти «винтажные» внешние носители (*CD/DVD*). Это идеально соответствует профилю целей операций кибершпионажа ЦРУ в том же Иране: научно-исследовательские учреждения и правительственные объекты со строгим режимом безопасности, ученые, работающие с секретными данными, и проч. В рамках такой парадигмы, напротив, неизбирательный сбор больших данных из сети по принципу

«делаем, потому что можем» в общем неактуален. Поэтому рядовому пользователю не стоит особенно бояться, что конкретно его устройство взломает, а данные из него похитит ЦРУ. Правда, если это действительно случилось, это может значить, что этот пользователь – объект целевой операции, и тогда у него проблемы.

4. Нынешние утечки подтверждают, что военные структуры (Киберкомандование и АНБ) являются далеко не единственными в США государственными игроками США в области разработки комплексного киберарсенала для проактивных операций. Членами Разведывательного сообщества США являются 16 разведывательных и информационно-аналитических правительственных структур: 8 гражданских и 8 военных. К первым относятся информационно-аналитическое управление Министерства внутренней безопасности, информационное управление Госдепартамента, управление разведки и безопасности в ядерной сфере Министерства энергетики, управление разведки и борьбы с терроризмом Минфина, ФБР в структуре Минюста. Остальные 8 членов – различные структуры Минобороны США, включая АНБ и Киберкомандование. То есть только в США насчитывается 16 государственных игроков в сфере разведки, и у каждого из них есть или разрабатываются те или иные программы и средства для работы в Сети – хотя по объемам финансирования и масштаб АНБ и ЦРУ должны далеко превосходить остальных коллег.

Кроме того, американская ситуация служит индикатором международных тенденций в области развития госпрограмм электронной разведки. Наличие арсенала средств для кибероперaций и тайного сбора данных в Сети становится не только приоритетной задачей государственного уровня, но и ключевым активом в смысле удержания и расширения аппаратных полномочий и борьбы за бюджет на уровне отдельных силовых ведомств, подчас конкурирующих друг с другом. В более широком смысле раскрытие утечки ЦРУ подводит черту под очевидным фактом состоявшейся вепонизации киберпространства. Государства по всему миру применяют проактивные киберсредства в постоянном и необходимом режиме, зачастую не делая принципиальных различий между целями на своей территории и за рубежом. В этих условиях

наивно полагать, что гражданские и военные спецслужбы России, Китая, Израиля, государств ЕС и вообще любой другой страны не развивают собственные средства тайного сбора данных и программы кибероперацией или готовы от них отказаться.

5. ЦРУ, как и АНБ ранее, не удалось сломать ключевой элемент системы безопасности и доверия с Сети – современные стандарты криптографической защиты информации. Причем ЦРУ, в отличие от их военных коллег с программой *Bullrun*, и не особо пытались – среди всех ставших известными направлений деятельности ведомства работа по компрометации протоколов и реализаций ключевых стандартов шифрования не представлена. Теоретически самая страшная угроза, которую могли бы нести раскрытые проекты ЦРУ – разработка средств, позволяющих гарантированно взламывать криптографическую защиту в реализациях ключевых протоколов и стандартов (*AES, RSA, TLS/SSL*) и таким образом разрушать существующие экосистемы безопасности как крупнейших ИТ-вендоров, так и Интернета в целом. Но исходя из уже раскрытой *Wikileaks* части данных, ЦРУ даже не ставило перед собой в явном виде такую задачу. Для пользователя, чье устройство стало целью атаки, а данные похищены, разница в том, была ли при этом взломана криптографическая защита используемых им сервисов, или нет, может быть неочевидна. На самом деле она принципиальна: даже самые отработанные и передовые методы атак с эксплуатацией уязвимостей в архитектуре ПО конкретных моделей и продуктов ИТ-рынка требуют доставки вредоносного ПО на устройство. Для этого приходится выстраивать некую более-менее специфическую, а в многих случаях и индивидуальную схему, вектор атаки, чтобы обеспечить применение эксплойта на том или ином конкретном устройстве. Например, спровоцировать пользователя перейти на зараженный интернет-ресурс или запустить на своем устройстве скачанный из Сети или пришедший по электронной почте исполняемый файл с вредоносным ПО. Для поддержания эффективности подобных техник и векторов атак необходимо разрабатывать массивную и громоздкую линейку эксплойтов и постоянно пополнять базу уязвимостей под конкретные версии ОС и программных прошивок, новых версий

и модификаций ПО для всех семейств и серий устройств и сервисов, которые рассматриваются в качестве потенциальных целей. Именно этим и занимается ЦРУ, судя по данным из *Vault 7*, чем объясняется возможная высокая ресурсоемкость его проектов.

Реальное преодоление криптографической защиты ключевых протоколов и реализаций алгоритмов шифрования, используемых в современных сервисах и продуктах открыло бы перед ЦРУ куда более широкие возможности. Строго говоря, у ведомства отпала бы необходимость разрабатывать, поддерживать и обновлять весь тот огромный бестиарий вредоносного ПО, который представлен в его «базе знаний». Имея возможность гарантированного взлома криптографической защиты в реализациях, например, *AES*, ЦРУ могло бы разместить средства перехвата интернет-трафика на сетях связи и просто расшифровывать почти любые потоки данных, передаваемых пользователями тех же мессенджеров, не утруждая себя задачей доставки эксплойтов и средств удаленного контроля на то или иное конкретное устройство, с которого передаются данные. Подобные возможности пыталось проработать АНБ в рамках упомянутой программы *Bullrun* еще с начала 2000-х гг. в рамках добровольно-принудительного сотрудничества с разработчиками средств защиты информации. Кроме того, в АНБ работали над поиском фундаментальных инженерных решений, позволяющих взламывать шифрование таких протоколов как *TLS/SSL, HTTPS, SSH*. Успех на втором направлении означал бы фактическое разрушение экосистемы доверия, на основе которой и функционирует Интернет. Но этот ключевой рубеж пока остается не взятым ни АНБ, ни ЦРУ, судя по данным из *Vault 7*.

6. На основе уже раскрытых данных можно сказать, что ЦРУ уступает АНБ по степени «продвинутости» и технологическому уровню своих разработок. Несмотря на обилие выявленных уязвимостей в мобильных и десктопных ОС, антивирусных продуктах и иных системах, разработку большого количества достаточно серьезных эксплойтов, закладок и других средств, раскрытый арсенал ЦРУ не содержит ни принципиально новых техник атак, ни по-настоящему прорывных образцов вредоносного кода. В свое время (2005-2010 гг.) разведслужба, предположительно вместе с

Киберкомандованием США и Моссадом, создала целое семейство уникальных, не имевших аналогов вредоносных программ для целевых операций кибершпионажа и киберсаботажа на Ближнем Востоке (тот же *Stuxnet*, а также *Flame, DuQu, Gauss* и проч.). Концепции и сам код этого вредоносного ПО вызвали мощное эхо в индустрии киберпреступности и среди околоправительственных хакерских группировок, неоднократно подвергались переработке, модернизации, использовались и до сих пор используются самыми разными акторами. Ничего подобного по уровню в нынешней базе знаний пока найти не удалось. Кроме того, в документах утечки нет описания инструментов, которые бы в полной мере подпадали под условное понятие «кибероружия»: например, средств эксплуатации уязвимостей в АСУ ТП критических важных объектов и стратегических оборонных инфраструктур. Впрочем, с учетом наличия у ЦРУ солидного прошлого опыта таких разработок скорее говорит о неполноте данных в опубликованном массиве документов, чем о том, что подобные проекты были свернуты.

7. Нынешние утечки могут стать катализатором давно необходимых подвижек и изменений по крайней мере в двух областях. Одна из них – согласование и внедрение стандартов и механизмов безопасности в тех нишах, где они по различным причинам отсутствуют. Например, речь идет об Интернете Вещей, устройства которого сегодня массово эксплуатируются для организации беспрецедентно масштабных сетевых атак, которые уже угрожают устойчивости ключевых сервисов Интернета, включая глобальную *DNS*. Еще одна область, где стандартизация безопасности серьезно отстает от развития самой технологии – умный транспорт, который как раз попал в прицел ЦРУ. Наконец, подвижки необходимы и в таких областях, как внедрение обязательного шифрования данных на нижних уровнях сетей производственных объектов (уровень обмена данными между АСУ ТП). Угроза со стороны государственных спецслужб может стать для заинтересованных сторон в каждой из этих ниш (вендоры, операторы, интеграторы, национальные регуляторы и пользователи) необходимым стимулом к ускоренной разработке и внедрению углубленных стандартов и архитектурных принципов безопасности.

Вторая область, в которой остро необходим прогресс – выработка международного режима ответственного поведения в киберпространстве, в том числе в части разумного ограничения государственных кибероперaций. С учетом последних событий, надежд на то, что этот вопрос решат между собой сами государства, откровенно мало. Принимаемые на международных площадках доклады и меры доверия пока по большей части остаются декларациями о намерениях, а бюджеты программ спецслужб на создание военизированного киберпотенциала на многие порядки превышают расходы на продвижение дипломатических инициатив по регулированию поведения в киберпространстве. Ситуацию может изменить альянс глобальных ИТ-вендоров и инженерного сообщества, чьим бизнес-интересам и принципам деятельности напрямую угрожают государственные программы кибероперaций. Именно эти игроки в состоянии сформулировать такие нормы и стандарты обмена информацией, атрибуции кибератак, ограничения распространения вепонизированного кода и проч., которые сами смогут реально выполнять, будучи глобальными разработчиками и провайдерами технологий и инфраструктуры. В этом смысле, российские, китайские и американские вендоры, разработчики и сетевые инженеры могут оказаться в одной лодке, даже пока их правительства скованы взаимным недоверием и гонкой цифровых вооружений. Частных игроков между собой объединяют интересы бизнеса, а с сетевыми инженерами их сближает необходимость поддержания единства и открытости Интернета, без которой невозможно существование глобального трансграничного ИТ-рынка. Дополнительную поддержку им могут оказать сами проекты гражданского активизма, включая *Wikileaks*. Последняя вскоре после публикации *Year Zero* уже пошла на сотрудничество с частными компаниями, чья продукция стала целью киберинструментов ЦРУ, предложив передать им данные вредоносного кода программ спецслужбы для скорейшего закрытия уязвимостей в их продуктах. Возможно, конструкция «ИТ-компании – инженеры – гражданские активисты» сможет ответить на вызов вепонизации киберпространства оперативнее, чем правительства – или по крайней мере заставит последних ускорить свою работу в этом направлении.