Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2649 14.03.2017, 13:54
4

Что не так с очередной утечкой WikiLeaks

Прошла неделя с момента публикации 7 марта на сайте WikiLeaks более восьми тысяч документов, которые свидетельствуют, что ЦРУ США использует и, более того, производит хакерские инструменты. В первых комментариях журналисты называли Vault 7 – такое имя получил разоблачающий хакеров ЦРУ архив – не иначе как равным по масштабу сливам Бредли Мэннинга в 2010 году и Эдварда Сноудена в 2013-м. Но, спустя несколько дней, энтузиазм спал и даже сменился на критику. SmartBabr разбирался почему.

Хуже некуда

Тотальной слежкой за жителями всего мира через смартфоны и сети связи уже никого не удивишь: WikiLeaks и его информаторы хорошо потрудились, чтобы развеять у людей всякие иллюзии о частной жизни в эпоху интернета.

На тему тотальной слежки исчерпывающе высказался, конечно, Эдвард Сноуден. АНБ следит за миллиардом человек? Следит за правительствами 35 стран и перехватывает звонки на любых переговорах? Спецслужбы США незаконно проникают в компьютерные сети операторов связи других стран? На все эти вопросы ответ положительный. И он никого не пугает и даже не удивляет.

Впрочем, может ли вообще что-то удивлять после сливов Бредли (Челси) Мэннинга видеозаписей расстрела американскими военными мирных жителей в Багдаде и публикации WikiLeaks архива сводок о методах войны США в Афганистане? Вряд ли.

Во всяком случае в отношении Центрального разведывательного управления США иллюзий никто точно не питал. Поэтому и документы со схемами взлома широкого спектра массовых компьютерных сервисов – Skype, сетей Wi-Fi, коммерческих антивирусных программ – не стали ни для кого откровением.

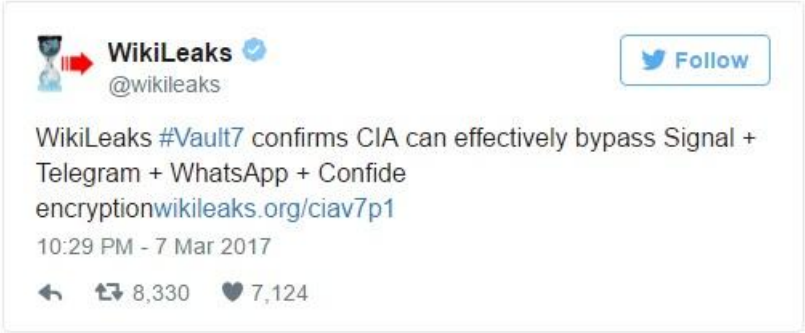
– Используют хакерские инструменты? Ну ок. Мы не спецагенты, и не преступники, чтобы их опасаться.
Именно такая реакция возникает у большинства людей в ответ на рассказы о методах спецслужб. Вполне логично.

Ближе к телу

В WikiLeaks, безусловно, понимали, что архив Vault 7 – подробный, сугубо технический каталог инструментов и инструкций ЦРУ – не обладает взрывной силой. Но по каким-то причинам организации было важно обратить на него внимание всего мира. Для этого был придуман хороший ход: показать, что дело касается каждого и сделать акцент на брендах.

«Дырявыми» фактически названы продукты Apple, Android от Google, телевизоры Samsung, Skype и другие сервисы Microsoft. В отчете и заголовках также фигурировали мессенджеры, использующие end-to-end шифрование – Signal, Telegram, WhatsApp – последний оплот анонимности.

Приведенный выше твит многие издания восприняли буквально: ЦРУ может прочесть зашифрованные сообщения. Чуть позже журналисты прошерстили выложенный архив и выяснили, что документы в нем только подтверждают силу шифрования. «Если вы используете эти мессенджеры, то давайте проясним: ничто в документах WikiLeaks не говорит, что ЦРУ может



дискредитировать их», – написало издание Wired.

Позже свое пояснение дали в Telegram: спецслужбы действительно могут получать доступ к передаваемой в этих мессенджерах информации, но только через уязвимости (проще говоря, дыры в защите) операционных систем, таких как iOs и Android, и внутренней прошивки смартфонов. End-to-end шифрование по-прежнему им не по зубам.

Суровая реальность

Fig. 1.1: **Mesh Network Deployed Across Numerous Devices**

С опровержением наличия «дыр» в iOs и Android никто не выступил. Значит ли это, что Apple и Google сознательно не латали бреши в защите своих продуктов? В документах WikiLeaks об этом ничего не сказано, но, скорее всего, нет. Уязвимости есть абсолютно во всех больших интернет-сервисах, они возникают из-за несогласованной разработки и по другим причинам.

Под уязвимости хакеры пишут эксплойты, с помощью которых получают контроль над устройством. «Белые» хакеры ищут уязвимости и добровольно сообщают о них компаниями, «серые» – продают на специальных биржах: либо другим хакерам, либо компаниям.

Так вот в документах WikiLeaks содержится информация о сотнях уязвимостей «нулевого дня» – то есть действующих, до сих пор неисправленных, – а также о программах, эти уязвимости эксплуатирующих. И это, по мнению WikiLeaks, является самым страшным: дыры в безопасности надо не копить, а латать, чтобы они не навредили всему миру.

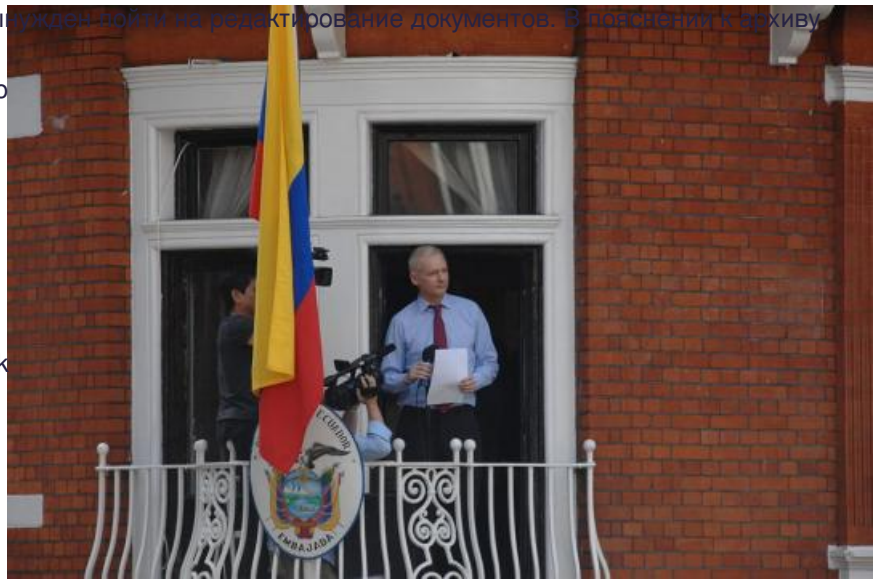
> *«Как только кибероружие "освобождается", оно способно распространиться по всему миру за считанные секунды и его могут использовать соперничающие государства, кибер-мошенники и подростки-хакеры»*, – сказано в пресс-релизе WikiLeaks.

То, что «выйти на свободу» кибероружию не так уж сложно, подтверждает сам факт утечки. WikiLeaks не назвала источник слива, но указала, что документы незаконно распространялись среди бывших правительственных хакеров и подрядчиков США, один из которых предоставил организации части своего архива. То есть инструменты из отчета – уже достояние хакеров, и прямо сейчас кто-то может использовать их для кражи информации или незаконной слежки.

Имеет ли ЦРУ полномочия быть поставщиком продуктов для подпольного рынка хакерских услуг? Это надо обсуждать, уверены в WikiLeaks, и здесь с ней никто не спорит.

Продолжение следует

Еще один интересный момент. С архивом Vault 7 WikiLeaks пришлось пойти на не очень типичное для себя действие. Основатель организации Джулиан Ассанж всегда выступал за прозрачность и транспарентность данных. После утечек 2010 года, посвященных войне в Афганистане, он много критиковал журналистов за то, что они давали читателям переработанные данные и убирали имена участников событий. Аргументы о защите тайны частной жизни жертв не принимались.



В случае с Vault 7 Ассанж сам был вынужден дойти на редактирование документов. В пояснении к архиву WikiLeaks отмечается, что многие из опубликованных документов частично отредактированы волонтерами организации, чтобы избежать раскрытия фактического кода и средств взлома для хакеров.

Критики указывают на еще одно слабое место этой публикации WikiLeaks. Как отмечает The New York Times, утечка отличается от слива Эдварда Сноудена тем, что в ней нет конкретных примеров использования указанных средств против реальных целей. С одной стороны, это плюс: так как может ограничить ущерб от утечки для национальной безопасности. С другой стороны, минус: пострадавшие не подключатся к борьбе за наказание хакеров.

Впрочем, вполне возможно, что примеры использования хакерского арсенала ЦРУ еще всплывут на поверхность. WikiLeaks начала публикацию подтверждений слежки за канцлером германии Ангелы Меркель, а Россия уже призвала спецслужбы США дать ответ на материалы организации по ЦРУ.

Да и все-таки значение Vault 7 не сводится только к разоблачению хакеров-разведчиков. Основная цель – достучаться до технологических компаний, указать на их слабые места и побудить исправить.

Правда, и здесь вышла небольшая заминка: 11 марта, спустя четыре дня после публикации архива, Google и Microsoft сообщили Forbes, что до сих пор никто из WikiLeaks с ними не связался. При этом ранее Google отчиталась о закрытии брешей в Android, а Microsoft, только позже, заявила, что опубликованная Wikileaks информация об уязвимостях в его продуктах устарела. Но работа с архивом идет, и это главное.

Автор: Полина Чехова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2649 14.03.2017, 13:54
4
URL: https://babr24.com/?IDE=272053 Bytes: 7917 / 6992 Версия для печати

Автор текста: **Полина Чехова**,
журналист.

На сайте опубликовано **494**
текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта