



## ИСТОРИИ

# Славик, Смелый и другие Даниил Туровский — о самых известных российских хакерах

09:06, 13 июля 2015 · Источник: Meduza

Фото: Изображение: labs.bitdefender.com.

[Ссылка на материал](#)

Это PDF-версия материала, опубликованного на «Медузе». Вы можете отправить этот файл в любом мессенджере или по электронной почте вашим близким в России, особенно тем, кто не умеет обходить блокировки. Вы можете также распечатать этот текст и показать его тем, кто не пользуется интернетом.

«Медуза» признана «нежелательной» организацией на территории РФ, поэтому, пожалуйста, будьте осторожны и делитесь нашими материалами только с теми, кому доверяете.

Подробнее о «нежелательном» статусе.

Самый удобный способ читать «Медузу» без VPN — это скачать наше приложение. Оно работает в России, несмотря на блокировку, и это абсолютно безопасно. Версия для iOS и для Android. Приложение на Android также можно скачать по прямой ссылке.

Устанавливайте приложение не только себе, но и близким!

В конце июня в немецком Бонне начался суд на Сергеем Максимовым — «хакером Хэллом». По мнению следствия, он ответственен за взломы почты и блогов российских оппозиционеров, в том числе Алексея Навального. Процесс идет на фоне широкой дискуссии в американских СМИ, посвященной русским хакерам, которых считают самыми опасными, богатыми и технически подкованными в мире. Весной Newsweek посвятил русским хакерам один из своих номеров; Хиллари Клинтон заявляла, что «правительство России прямо или косвенно финансировало хакерские атаки» на государственные структуры США. Специальный корреспондент «Медузы» **Даниил Туровский** рассказывает о наиболее заметных российских хакерах и группировках.

---

## Евгений Богачев

Один из самых разыскиваемых ФБР хакеров. За любую информацию, которая поможет его арестовать, США обещают вознаграждение до трех миллионов долларов.

Евгений Богачев известен под псевдонимами Slavik и Lucky12345; по информации американских спецслужб,

он участвовал в «широкомасштабном вымогательстве», а также «незаконно заражал компьютеры вирусом под названием Zeus („Зевс“»). Вирус использовался для получения номеров банковских счетов, паролей, личных идентификационных номеров — и последующего воровства денег.



Объявление о розыске Евгения Богачева

Скриншот: fbi.gov

Участники группировки, которой руководил Богачев, рассылали письма, которые приводили на сайты, зараженные вирусом. В 2011 году группировка разработала новую модификацию вируса под названием «Gameover Zeus» (GOZ, «Игра окончена»). Этот вирус, по данным ФБР, заразил порядка миллиона

компьютеров и принес создателям более ста миллионов долларов.

По данным мониторинговой команды Dell SecureWorks Counter Threat Unit, «Игра окончена» — самый мощный банковский троян последних лет; в 2013-м на его долю приходилось 38% активности всех банковских троянов в мире. Вирус способен незаметно копировать номера банковских карт, пароли, личные идентификационные номера и другую конфиденциальную информацию.

Спецслужбы США считают, что Богачев находится в Анапе. Отмечается, что он любит выходить на яхте в Черное море.

## **APT28**

С 2007 года некая российская группировка хакеров занимается масштабным кибершпионажем — собирает информацию о системах безопасности мировых оборонных структур, работе правительств стран восточной Европы. Исследование, посвященное этой группировке, в 2014 году выпустила американская компания FireEye, специализирующаяся на разработке средств защиты от кибератак. Компания считает, что кибершпионажем занимается группировка APT28 — сокращенно от Advanced Persistent Threat («Целенаправленная устойчивая угроза»).

По данным экспертов, хакеры используют два основных метода распространения вредоносных программ. Во-первых, это регистрация доменного имени, максимально похожего на доменное имя интересующей хакеров структуры (этот метод использовали для атаки на сайты НАТО, ОБСЕ, правительств Мексики, Венгрии, Польши). Во-вторых, фишинг — рассылка фальшивых электронных писем от известных интернет-сервисов, содержащих вредоносные ссылки (применялся в отношении сотрудников Еврокомиссии, НАТО и ООН).

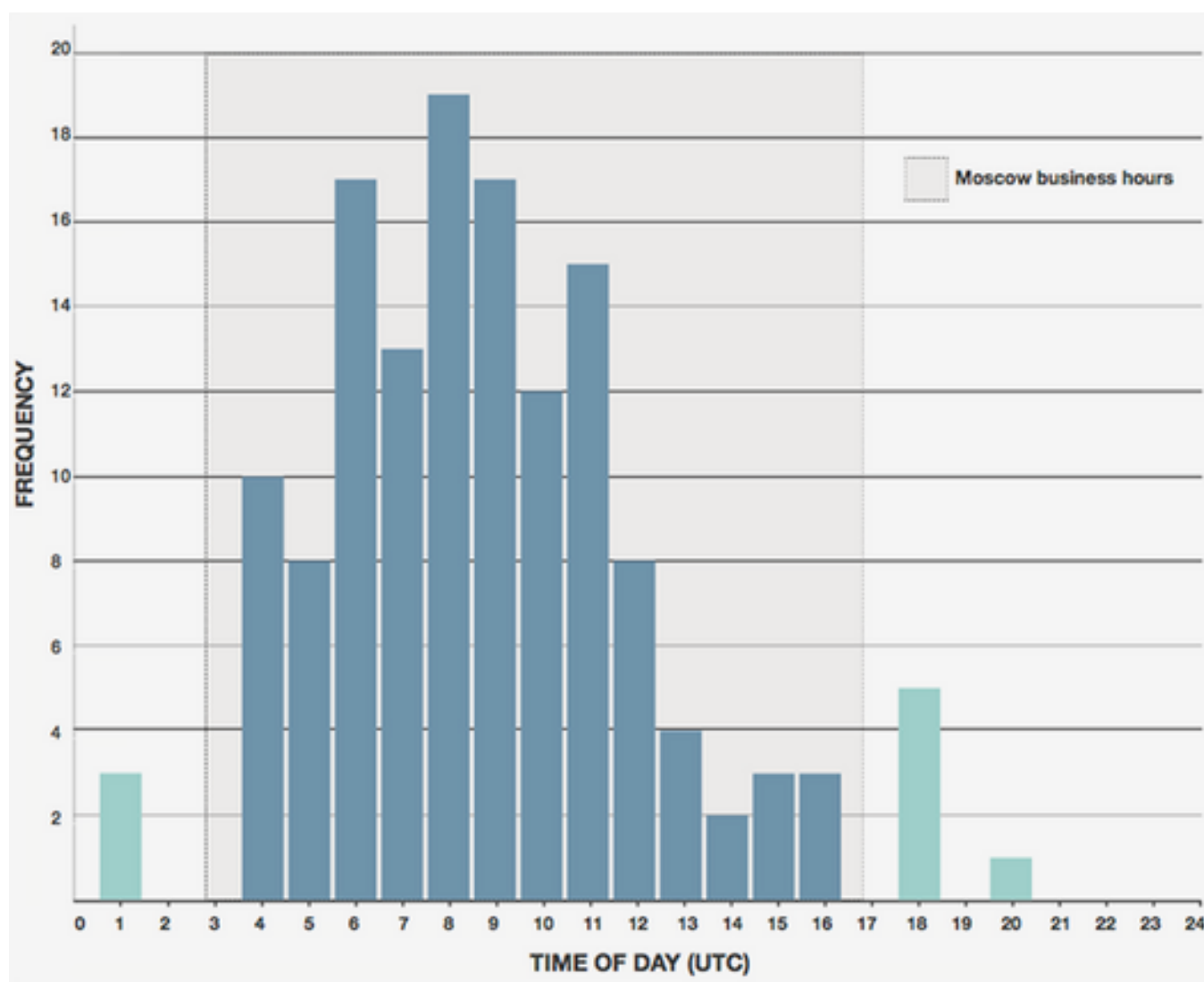


График разработки вредоносных программ APT28

Инфографика: [FireEye](#)

У АРТ28 — широкий круг интересов: от подразделений норвежской армии до террористических группировок Северного Кавказа и «Хизб ут-Тахрир» (в России организация признана террористической). По мнению специалистов компании FireEye, такая информация может понадобиться только какому-нибудь правительству. В пользу того, что в группировке работают россияне, говорит статистика: 96% вирусов были написаны в рабочие дни (с понедельника по пятницу) с восьми утра до шести вечера по московскому времени. Кроме того, в программном коде многих вирусов от АРТ28 осталась информация о том, что при программировании раскладка клавиатуры была переключена с русского на английский.

## Неизвестные против США

В 2014 году (месяц не сообщался) неизвестным российским хакерам удалось получить доступ к электронной корреспонденции президента США Барака Обамы и переписке сотрудников Госдепартамента, писала The New York Times. Информация не была секретной, но в ней содержались сведения о готовящихся встречах и дипломатическая переписка.

В октябре 2014 года российские (по данным Washington Post) хакеры атаковали сеть Белого дома, которой

пользуются старшие сотрудники президента США. Хакеры не пытались уничтожить данные, но планировали подключиться к другим системам для шпионажа. Атака была отражена.

Весной 2014-го неизвестные хакеры атаковали сети Госдепартамента, весной 2015-го — службы внутренних доходов федерального налогового управления США и Пентагона. Госдепартамент из-за атаки вынужден был отключить электронную почту и сайт. Глава Пентагона Эштон Картер заявил, что хакеры обнаружили уязвимость в одной из старых сетей и через нее получили доступ к основной инфраструктуре, но были «изгнаны таким образом, чтобы свести к минимуму шансы на возвращение». Он утверждал, что была обнаружена связь хакеров с Россией.



Political Undoings / Cuban Moneyball

# Newsweek.

05.15.2015



# CYBERPOWER

THE RUSSIAN HACKERS  
ARE COMING!

Обложка американского журнала Newsweek: «Русские хакеры идут!» 15 мая 2015 года

Один из майских номеров американского журнала Newsweek за 2015 год вышел с обложкой The Russian Hackers are Coming! («Русские хакеры идут!»). «Сегодня киберпространство подобно Европе в 1914 году — накануне Первой мировой. Правительства — точно сомнамбулы. Они не осознают могущества новых технологий», — рассуждал один из героев текста, специалист по кибербезопасности Александр Климбург.

Другой специалист — Джэффри Кар — заявлял в статье, что Россия (наряду с Китаем) является наиболее развитой страной в вопросе ведения кибервойн. По его мнению, именно российские хакеры взломали внутренние сети компании Sony, получив доступ к тысячам электронным писем компании — они угрожали продолжить атаку, если Sony выпустит «Интервью», сатирический фильм о лидере КНДР. Кар приводил и другой яркий пример: во время присоединения Крыма к России вирус BlackEnergy, созданный русскими хакерами, атаковал польские и украинские правительственные организации, сети Еврокомиссии и Европарламента.

## **Владимир Дринкман и Дмитрий Смилянец**

Дринкман и Смилянец — россияне, которых в США называют организаторами «крупнейшей хакерской

схемы, когда-либо раскрытой правоохранительными органами». «Би-Би-Си» считает их дело «одним из самых знаковых в истории киберпреступности».

По данным спецслужб, хакерская группировка Дринкмана (среди фигурантов дела — еще трое россиян и один украинец) похитила в 2005-2012 годах информацию о 160 миллионах кредитных карт США, Канады и Европы, а также проникла во внутренние сети компаний 7-Eleven, Hannaford Brothers, Jet Blue, Visa. Общий ущерб оценивается в 300 миллионов евро.

Владимир Дринкман — 35-летний москвич, который в последние годы жил в Амстердаме. Именно там в июне 2012 года его и задержали — практически случайно; из-за фотографии, которую выложил в сеть другой член группировки Дмитрий Смилянец.



Дмитрий Смилянец, 26 июня 2012 года

Фото: Личная страница «ВКонтакте»

Секретная служба США, давно следящая за Смилянцем (Смелый и ddd1ms, руководитель киберспортивной команды Moscow Five, выступавшей в соревнованиях по Counter Strike и Dota), обнаружила в его фейсбуке снимок, на котором он в толстовке с гербом России позирует на фоне надписи «I Amsterdam» в центре голландской столицы. Спецслужбы обзвонили все отели

в этом районе; в одном из них обнаружился Смилянец. Утром голландская полиция приехала в отель; выяснилось, что Смилянец снял два номера — во втором находился Владимир Дринкман.

Смилянца экстрадировали в США в августе 2013 года. На суде он заявил о своей невиновности. В феврале 2015 года из Нидерландов в США экстрадировали и Дринкмана. Оба ожидают суда.

## **«Анонимный интернационал» (Шалтай-Болтай)**

Группировка хакеров, специализирующаяся на сборе компромата на российских чиновников. Большую часть информации продает заказчикам, остальное выкладывает в открытый доступ в своем блоге (заблокирован на территории России). «Шалтай» публиковал содержимое почтовых ящиков предполагаемых сотрудников Администрации президента, Роскомнадзора и московской мэрии.

По данным «Медузы», в составе группировки — около 12 человек, они живут в разных странах, в том числе, в Таиланде и России («Медуза» встречалась с их руководителем в Бангкоке).





Скриншот твиттера Дмитрия Медведева, 14 августа 2014 года

Самой громкой публичной акцией «Шалтая» по-прежнему остается взлом твиттера премьер-министра России Дмитрия Медведева («Ухожу в отставку. Стыдно за действия правительства. Простите»). «Программисты из „Шалтая“ получили ключи от твиттера премьера, когда выкачали из iCloud электронные копии трех смартфонов Медведева: пароли от соцсети премьер хранил в заметках на айфоне», — рассказывал лидер группировки.

Кроме того, в 2014-2015 годах хакеры публиковали массивы личной и рабочей переписки, якобы принадлежащей бывшему заместителю начальника

управления внутренней политики Администрации президента Тимуру Прокопенко («Медуза» изучала эти сливы здесь и здесь).

## **Anonymous Russia и хакер Хэлл**

Российский филиал международной группировки хакеров-энтузиастов, использующих символику Гая Фокса. В начале 2010-х наносил точечные удары по тем, кто, по их мнению, «уничтожал свободу в российском интернете». Взламывали почтовые ящики активистов молодежных прокремлевских движений, сотрудников Росмолодежи и Администрации президента, сайты региональных отделений «Единой России», атаковали сайт Кремля, публиковали яркие видеообращения к руководству страны (сейчас удалены с ютьюба).

В интервью «Афише» в феврале 2012 года один из участников группировки рассказывал: «Единственное, что все мы разделяем, — это стремление защитить свободу слова в интернете. Нас ударили по сокровенному, отняли наш дом, так что теперь это личная месть». Спустя полгода Госдума приняла поправки в закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

Он получил известность как «закон о черных списках»; имелся в виду «Единый реестр доменных имен, указателей страниц», который составляется экспертами

надзорных органов — Роскомнадзора (детская порнография), ФСКН (наркотики) и Роспотребнадзора (инструкции для самоубийц). Списанием заведует Роскомнадзор.

В августе 2014-го сообщалось, что двух новосибирских хакеров из Anonymous Russia задержали сотрудники ФСБ, но они раскаялись в содеянном и «оказали ФСБ помощь в предотвращении дальнейших компьютерных атак».

В том же интервью «Афише» «Анонимус» говорил, что опубликованные ими почтовые ящики «можно рассмотреть как поддержание равновесия после взлома почты Навального».



Сергей Максимов в зале суда, 24 июня 2015 года

Фото: Вислом Алегасон



Взлом почты Навального взял на себя некий хакер Хэлл, за которым, как считали многие, скрывались российские спецслужбы (почту вскрыли вскоре после того, как сотрудники ФСБ изъяли компьютеры из квартиры оппозиционера). Летом 2015 года в немецком городе Бонн начался суд над Сергеем Максимовым, которого немецкие следователи подозревают во взломах. Навальный заявил, что Максимов — это и есть хакер Хэлл («Медуза» подробно писала об этом процессе).

## Роман Селезнев

За Романом Селезневым секретная служба США охотилась около десяти лет. Они знали, что хакер живет во Владивостоке. По версии следствия, он взламывал компьютеры кассовых автоматов американских магазинов и ресторанов.

За несколько лет Селезнев, по данным спецслужб, украл реквизиты двух миллионов кредиток. Эти данные он продавал в интернете (по некоторым сведениям, сто карточек стоили тысячу с лишним долларов).

На продаже информации Селезнев, предположительно, заработал от 2 до 17 миллионов долларов. В интернете Селезнев был известен под десятками ников, в том числе Track2, 2pac, nCux, Bulba, Roman Ivanoc, bandysli64 и Ruben Samvelich.

Селезнев много путешествовал. В 2011-м он ездил в Марракеш (Марокко) и стал жертвой теракта — террористы взорвали кафе с иностранными туристами. Погибли 16 человек, Селезнев получил тяжелое ранение головы. После этого он вернулся в Россию.



Роман Селезнев с семьей

Фото: AFP / Scanpix

Спецслужбы США продолжали отслеживать его путешествия. В 2014-м они обнаружили его в пятизвездочном отеле на Мальдивах. Местная полиция согласилась помочь спецслужбам его задержать. 5 июля 2014 года его взяли в аэропорту и передали агентам Секретной службы, в тот же день они вылетели на остров Гуам, принадлежащий США. Затем Селезнева перевезли в Сиэтл.

МИД России заявлял, что расценивает его задержание как похищение.

Отец Селезнева, депутат Госдумы от ЛДПР Валерий Селезнев, заявлял: «Он не может быть хакером, потому что он инвалид! Он не мог этого сделать. Для этого необходимо специальное образование, навыки».

Суд над Селезневым начнется 9 мая 2016 года.

---

**Даниил Туровский**

*Москва*