ТОП-15 УТЕЧЕК
ЗА 2015 ГОД

Александр Антипов,
главный редактор
SecurityLab.ru

В прошлом году в мире информационной безопасности произошло огромное количество масштабных инцидентов. Значительное место среди них занимают взломы с последующими утечками персональных и конфиденциальных данных. Самые заметные случаи, собранные в этом обзоре, показывают: нет такой индустрии или сферы деятельности, которая защищена от утечек.

01

ГРУППА СТРАХОВЫХ КОМПАНИЙ ANTHEM

Злоумышленники первый раз взломали ресурсы страховщиков еще в 2004 году, но об этом стало известно только в 2015-м. Это значит, что в течение 11 лет хакеры имели прямой доступ к персональным данным 80 миллионов клиентов Anthem — к именам, адресам, телефонам, номерам социального страхования, истории трудоустройства.

02

ХАКЕРСКАЯ КОМПАНИЯ HACKING TEAM

Итальянская компания, предлагающая услуги взлома и кибершпионажа, сама оказалась жертвой крупной утечки. Хакеры-конкуренты выложили в интернет огромный архив, содержащий конфиденциальные документы о сотрудничестве Hacking Team со спецслужбами всего мира. Подробный анализ архива позволил обнаружить эксплойты ко многим уязвимостям нулевого дня.

03

САЙТ ДЛЯ СУПРУЖЕСКОЙ ИЗМЕНЫ ASHLEY MADISON

В июле 2015 года хакерская группировка The Impact Team выложила учетные данные 11 млн пользователей сайта Ashley Madison, среди которых оказались известные политики и бизнесмены. Данные, выложенные в открытый доступ, стали использоваться злоумышленниками для вымогательства и других атак. Обиженные канадские пользователи даже попытались отсудить у владельцев Ashley Madison 575 млн долл. компенсации. Некоторые западные СМИ заявляли, что скандальная утечка данных привела к двум самоубийствам.

04

САЙТ ЗНАКОМСТВ ADULT FRIENDFINDER

Вслед за взломом Ashley Madison хакеры атаковали аналогичный сервис «взрослых» знакомств Adult FriendFinder. Данные почти 4 млн пользователей были выложены в открытый доступ.

05

VTECH И HELLO KITTY

Атаки на обе компании объединяет одно существенное событие: хакеры получили доступ к данным детей. Возможно, получение информации о детях не было главной целью атакующих, однако прецедент создан. В ходе атаки «пострадали» данные 14,8 млн клиентов.

03 05 07 09 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 53 55 57 59 61 63 65 67 69 71 73 75 77 79 81 83 85 87 89 91 93 95 97 99 101 103

06

JUNIPER SCREENOS

Очень громкий инцидент, произошедший в декабре. Компания обнаружила бэкдор в ScreenOS, который присутствовал в системе по меньшей мере с 2012 года. Учитывая сектор применения устройств компании, можно предположить, что спецслужбы, внедрившие бэкдор, использовали его для хищения корпоративных и государственных секретов самых крупных компаний в мире.

07

«АВТОВАЗ» И MEGAINDEX

В декабре стало известно об успешной атаке на компанию ALTWeb Group, и как следствие — взлом «АвтоВАЗа». Как заявлял хакер, в его распоряжении оказалось 14 тысяч пар «логин — пароль», а валидность базы составила примерно 60%. Имея доступ ко всей базе клиентов ALTWeb Group, хакер обнаружил еще 250 тысяч пар «логин — хеш пароля» компании MegaIndex, и уже за первые сутки расшифровал 90% из них.

08

МЕНЕДЖЕР ПАРОЛЕЙ LASTPASS

Один из самых популярных менеджеров паролей в июне сообщил об успешной атаке злоумышленников на свои облачные ресурсы. Злоумышленники сумели похитить зашифрованные мастер-пароли, подсказки к этим паролям и имейлы пользователей сервиса.

09

ТЕЛЕКОМ T-MOBILE

Взлом телекоммуникационной компании посредством атаки на подрядчика Experian позволил злоумышленникам заполучить доступ к личным данным 15 млн клиентов оператора связи. Компания Experian также отличилась в 2014 году, позволив хакерам похитить и продать через вьетнамский сервис почти 200 млн записей, содержащих личные данные клиентов.

10

ЛИЧНАЯ ПОЧТА ДИРЕКТОРА ЦРУ

Джон Бреннан стал жертвой атаки трех подростков. Используя методы социальной инженерии, хакеры сумели заполучить доступ к переписке директора ЦРУ. Неправительственный интернет-аккаунт содержал письма с номерами социального страхования и персональными данными более десятка чиновников разведывательной службы, а также правительственный документ о применении жестких техник допроса к лицам, подозреваемых в терроризме.

11

БАЗА ДАННЫХ ИЗБИРАТЕЛЕЙ США

В конце 2015 года личные данные 191 миллиона граждан США были выложены в интернет. Опубликованная в свободном доступе база данных содержит имена, физические и электронные адреса, даты рождения, номера телефонов, а также сведения о принадлежности к политическим партиям избирателей из всех 50 штатов страны и округа Колумбия.

03
05
07
09
11
13
15
17
19
21
23
25
27
29
31
33
35
37
39
41
43
45
47
49
51

12

МЕДИЦИНСКАЯ БАЗА PREMERA

В начале 2015 года здравоохранительная компания Premera рассказала об успешной атаке на ее ресурсы. Личные данные 11 млн клиентов были похищены хакерами. Данные содержали имена, адреса, телефоны, номера социального страхования, банковскую информацию и медицинские данные. В настоящее время Premera обвиняют в преступной халатности, нарушении условий заключенного с клиентами контракта, нарушении Закона о защите прав потребителей штата Вашингтон (Washington Consumer Protection Act) и несвоевременном уведомлении клиентов о киберинциденте. Если суд удовлетворит иски потерпевших, компанию обяжут выплатить весь нанесенный им материальный и моральный ущерб.

13

ПРОФСОЮЗ ПОЛИЦИИ FRATERNAL ORDER OF POLICE

Неизвестные похитили базу крупнейшего объединения полицейских США — архив с конфиденциальной информацией размером 2,5 гигабайта, включая домашние адреса полицейских. Кроме архива, злоумышленники также получили доступ к закрытому форуму, где члены организации обсуждали различные темы, от необходимости более жестких мер в отношении нелегальных мигрантов до критики политики президента США.

14

ВЕБ-КАМЕРЫ ДЛЯ ПРИСМОТРА ЗА ДЕТЬМИ

Поисковая система Shodan открыла раздел, позволяющий посмотреть в миллионы веб-камер. За короткое время работы ресурса в кадр уже попали плантации конопли, задние дворы банков, детские спальни, кухни, гостиные, бассейны, школы и колледжи, лаборатории, магазины. Уязвимость камер заключается в том, что они используют для передачи видео протокол RTSP (Real Time Streaming Protocol) без надлежащей аутентификации. В итоге изображение с этих камер доступно любому, кто к ним подключится.

15

ОТПЕЧАТКИ ПАЛЬЦЕВ ЧИНОВНИКОВ

В начале лета стало известно о хакерской атаке на Управление кадровой службы США (US Office of Personnel Management). Злоумышленники похитили личные данные 21 млн американских госслужащих, а также отпечатки пальцев 5,6 млн человек. В отличие от украденного пароля, человек не может сменить свои отпечатки пальцев, поэтому их похищение открывает широкий простор для совершения преступлений против гражданина на протяжении всей его жизни. Как можно использовать чужие отпечатки? Исследователи из Chaos Computer Club еще осенью 2013 года продемонстрировали, как легко обойти систему биометрической идентификации Touch ID на популярных устройствах компании Apple. Получив чужой отпечаток пальца, немецкие хакеры с помощью несложной техники изготовили искусственный палец и разблокировали iPhone 5s, защищенный с помощью Touch ID.

53
55
57
59
61
63
65
67
69
71
73
75
77
79
81
83
85
87
89
91
93
95
97
99
101
103

Массовые утечки 2015 года заставляют взглянуть под другим углом на безопасность личных данных, поскольку использование этих данных позволяет злоумышленникам продолжить атаку. В этом году мы уже можем наблюдать такие последствия. В частности, в начале года случилась серия успешных атак на российские банки, в том числе «Металлинвестбанк», «Русский международный банк», «Гарант-Инвест». По данным Group-IB, с августа 2015 года по февраль 2016-го хакеры успешно похитили 1,8 млрд рублей со счетов клиентов российских банков. То ли еще будет.