2015

Прогноз угроз

McAfee Labs

Кибершпионаж

Частота кибершпионских атак будет по-прежнему увеличиваться.

Сбор разведданных

Постоянные игроки начнут собирать информацию более скрытым способом.

Изощренные киберпреступники перейдут от проведения быстрых атак к сбору разведывательных данных.

Кража денег

Новые игроки будут искать способы кражи денег и дезорганизации противников.

В 2013 году общее количество инцидентов кибершпионажа составило 511, из них 306 инцидентов — с подтвержденным раскрытием данных.[1]

Виды субъектов, занимающихся кибершпионажем.[2]

87 %
Лица, связанные с государством

11 %
Организованная преступность

1 %
Конкуренты

1 %
Бывшие сотрудники

Интернет вещей

Частота атак на устройства «Интернета вещей» будет быстро расти в связи с огромным количеством подключаемых объектов, низкой культурой безопасности и высокой ценностью данных, содержащихся на устройствах «Интернета вещей».

50 млрд устройств

К 2019 году в мире будет более 50 млрд устройств, подключенных к Интернету.[3]

Устройства «Интернета вещей»

Атаки на устройства в «Интернете вещей» уже стали обычным явлением.

- IP-камеры
- Интеллектуальные счетчики
- Медицинские устройства
- Устройства АСУТП

Компания HP недавно опубликовала результаты исследования, содержащие тревожные статистические данные о защищенности устройств в «Интернете вещей». Из 10 протестированных популярных устройств:[4]

70 %
содержали риски безопасности

25
— среднее количество брешей или рисков взлома домашних сетей, обнаруженных на каждом устройстве

80 %
не были защищены паролями достаточной сложности и длины

90 %
собирали по меньшей мере одну разновидность информации личного характера

70 %
предоставляли злоумышленнику возможность выявить действительную учетную запись путем перебора учетных записей

Конфиденциальность

Пока правительства и компании пытаются определить, что же является честным и санкционированным доступом к «персональной информации», конфиденциальность данных остается под угрозой.

110 млн человек

В прошлом году **риску раскрытия данных** в том или ином виде **подверглись** около 110 миллионов американцев, т. е. **примерно 50 % взрослого населения США**.[5]

Пароли

Устаревшие системы на основе ролей и **схемах использования паролей будут демонстрировать свою ненадежность** и проигрывать в противостоянии злоумышленникам.

Нормативные акты

Количество **правил и положений о защите данных** будет увеличиваться медленными, но постоянными темпами.

Биометрические данные

Биометрические данные и идентификаторы в контексте станут важнейшими областями для инноваций, но вместе с тем, пожалуй, и **наилучшими индикаторами присутствия и намерений**.

Программы-вымогатели

Методы распространения, шифрования и выбора целей в программах-вымогателях будут совершенствоваться.

2 млн образцов

Общее количество образцов программ-вымогателей в «зоопарке» McAfee Labs **в III квартале 2014 года превысило 2 миллиона**.

Облачные хранилища данных

Программы-вымогатели будут атаковать конечные точки, подписанные на облачные службы хранения, и пытаться **использовать хранящиеся в облаке учетные данные вошедших в систему пользователей** в том числе с целью заражения резервных копий данных, загружаемых в облако.

Украдено 255 000 $

McAfee Labs стала свидетелем того, как с помощью одного экземпляра программы-вымогателя CryptoLocker **за один месяц было украдено 255 000 долларов США**.

Мобильный сегмент

Мы ожидаем, что программы-вымогатели, **заражающие резервные копии данных в облаке**, распространятся и в мобильном пространстве.

Мобильные устройства

Число атак на мобильные устройства продолжает быстро расти, в то время как новые технологии увеличивают поверхность атаки и мало что делается для пресечения злоупотреблений в магазинах приложений.

Электронные платежи

Внимание киберворов привлечет набирающая популярность технология **беспроводной связи ближнего радиуса действия (near-field communications, NFC) для осуществления цифровых платежей** с мобильных устройств.

Виртуальная валюта

Мы ожидаем увеличения количества программ-вымогателей, нацеленных на мобильные устройства и **требующих выплаты выкупа в виртуальной валюте**.

Вредоносная реклама

Ненадежные магазины мобильных приложений будут одним из основных источников вредоносных программ, распространяемых посредством «вредоносной рекламы».

Наборы для генерирования вредоносных программ для мобильных устройств

Растущий уровень доступности наборов для генерирования вредоносных программ и исходного кода вредоносных программ **облегчит киберпреступникам задачу проведения атак на мобильные устройства**.

Количество образцов вредоносных программ для мобильных устройств в этом квартале выросло на 16 %, а в прошлом году — на 112 %.

16 %
III кв. 2014 г.

112 %
IV кв. 2013 г. — III кв. 2014 г.

Общее количество образцов вредоносных программ для мобильных устройств в III квартале 2014 года превысило 5 миллионов.

Вредоносные программы не только для Windows

Для проведения атак на системы, работающие не под управлением Windows, еще много лет будет использоваться уязвимость Shellshock.

22 487 атакующих IP-адресов

За первые четыре дня после объявления об обнаружении уязвимости **было выявлено 22 487 атакующих IP-адресов, связанных с Shellshock**.[6]

Shellshock

Злоумышленники будут использовать Shellshock для **кражи данных, взятия систем в заложники и ассимилирования спам-ботов**.

Устройства

Данную уязвимость могут содержать такие устройства, как **маршрутизаторы, телевизоры, промышленные контроллеры, системы управления полетом и объекты критически важной инфраструктуры**.

Опасность

В Национальной базе данных уязвимостей (National Vulnerability Database, NVD) серьезность уязвимости Shellshock оценивается в **10 баллов из 10**.[7]

Подробнее о составленном специалистами McAfee Labs прогнозе угроз на 2015 год можно прочитать в «Отчете об угрозах» за ноябрь 2014 года.

Полный текст отчета можно получить по адресу www.mcafee.com/November2014ThreatsReport.

intel Security

McAfee теперь входит в состав Intel Security.

1 Verizon 2014 Data Breach Investigations Report (Отчет компании Verizon о расследовании утечек данных за 2014 г.).
2 Verizon 2014 Data Breach Investigations Report (Отчет компании Verizon о расследовании утечек данных за 2014 г.).
3 McAfee, на основании исследований компаний BI Intelligence, IDC и Intel.
4 HP Internet of Things Research Study (Отчет HP по исследованию на тему «Интернет вещей»).
5 USA Today.
6 Akamai Security.
7 Национальная база данных уязвимостей (США).