КИБЕР АТАКИ. МИРОВЫЕ АТАКИ ЗА 2018 ГОД

Екатерина ПОЛУЯНОВ

Технический Университет Молдовы

Аннотация: *С каждым годом мир все больше становится «цифровым» и опасность кибератак увеличивается. Растет и наносимый ими вред. А так как ситуация сама собой не исправится, то можно смело утверждать, что специалисты по информационной безопасности всегда будут востребованы.*

Ключевые слова: *Ботнеты, Эксплойты, Бэкдоры, Компьютерные вирусы, Кибератаки.*

Введение

К вредоносным программам относят любое программное обеспечение, которые несанкционированно проникающее в компьютерное оборудование. Такие продукты как правило используются для нарушения работы компьютера, хищения личных данных и т.д., чтобы в дальнейшем извлечь из этого выгоду, как правило финансовую.

К примеру, злоумышленник получает контроль над управлением компьютером, крадет конфиденциальную или личную информацию и в дальнейшем шантажирует «жертву». Вторая цель не преследует получения материальной выгоды. Использование вредоносного программного обеспечения может быть проявлением желания его создателя утвердиться в своих умениях через обычное хулиганство или шутку.

1. Цели атак

Атаки вредоносных программ распространяются практически на всех пользователей Интернета. Немало от вредоносов страдают предприятия и различные компании и организации, например, гостиницы, сети ресторанов. Атакам вредоносов подвергаются не только компьютеры жертв, но и веб-сайты. У них воруют информацию о клиентах и пользователях, включая данные банковских карт, что грозит потерей финансов, баз данных, корпоративной информации. Интерес представляют личные данные, информация об электронных и банковских счетах, электронная почта, пароли доступа к социальным сетям.

Самые опасные и сложные вредоносные программы создаются на заказ государственными спецслужбами или связанными с ними группами киберпреступников. Такие вредоносы имеют ярко выраженную специфику и направлены на конкретную жертву или группу жертв. Они направлены на сбор и кражу секретных данных или прямое вредительство.

2. Топ-атак за 2018 год

Самой крупной, по масштабам причиненного ущерба, кибер-атакой в 2018 году был взлом **криптовалютной биржи Coincheck**, в результате которого было украдено больше полумиллиарда долларов. Хакеров так и не нашли, несмотря на то, что следы похищенной криптовалюты были найдены на других криптовалютных биржах, где есть строгие правила верификации пользователей, KYC и AML правила.

Если говорить про вирусы похожие на WannaCry и в том числе по его масштабам и причиненному, то что-то крайне отдаленное случилось в компании **Boeing**. В документе, подписанном главным инженером Boeing Commercial Airplane Майклом Вандервелом, говорится, что вирус может перекинуться на программное обеспечение самолетов, а также производственные системы. Он призвал коллег к осторожности, отметив, что вирус "метастазирует". При этом на странице Boeing в твиттере говорится, что СМИ преувеличили масштабы кибервзлома. Подробности кибератаки, в том числе предполагаемое использование вируса WannaCry или подобного ему, в Boeing пока раскрывать отказались.

Что же касается кражи личных данных, то самым, пожалуй, громким случаем была кража личных данных клиентов сети отелей Marriott. Одна из крупнейших в мире сетей отелей, **компания Marriott International**, сообщила об утечке данных 500 млн клиентов. Это крупнейших взлом с 2013 г., когда в распоряжении киберпреступников оказались данные 3 млрд пользователей Yahoo!. В руках злоумышленников оказались сочетания имени, номера телефона, номера паспорта, адреса электронной почты, почтового адреса, даты рождения и пола не менее 327 млн человек. В Marriott не исключают,

что киберпреступники могли завладеть данными о банковских картах, которые хранятся в зашифрованном виде. Там также отмечают, что доступной оказалась информация Starwood Preferred Guest (SPG), а именно данные об аккаунте, дате рождения, поле, времени прибытия и отбытия, резервации и предпочтениях.

Личные данные около 3 млн пользователей **Facebook**, использовавших приложение с психологическими тестами, находились в свободном доступе в течение четырех лет, сообщало издание New Scientist со ссылкой на собственное расследование. Данные собирались с помощью проекта Кембриджского университета — приложения myPersonality. Оно было запущено в 2007 г. и предлагало пользователям пройти психологические тесты и быстро получить результаты. При этом определенное число пользователей соглашалось делиться своими личными данными из профилей Facebook.Результаты психологических тестов использовали академики университета Кембриджа, которые потом хранили эти данные на сайте с "недостаточными мерами предосторожности" в течение четырех лет, говорится в расследовании. На протяжении этих лет доступ к данным пользователей хакеры могли получить "без особых трудностей", отмечает издание.

3. Правил сетевой безопасности.

1. Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.

2. Храните номер карточки и ПИН–коды в тайне. Запомните и сотрите/заклейте CVC-код.

3. Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

4. Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.

5. Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.

6. Проверяйте запросы персональных данных из каких-либо деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.

7. Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию.

Вывод

В заключении хочется сказать, что с момент массового распространения интернета, борьба между хакерами и специалистами по безопасности с каждым годом приобретала все большие и большие масштабы, и вряд ли когда-нибудь закончится. Так как свои методы совершенствует каждая из сторон.

Источники:

1. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf
2. *https://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%E0%F2%E0%EA%E0/*