ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

Материалы тренинга

Угрозы в интернет

- Вирусы
- СПАМ
- Сети
- Мобильные (смартфоны и планшеты)
- Mac OS

Вирусы

- Вирусы, черви, троянские программы

Компьютерный вирус и компьютерный червь — это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро.

Троянские программы — это вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать:

- удаление данных;
- блокирование данных;
- изменение данных;
- копирование данных;
- замедление работы компьютеров и компьютерных сетей

В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению.

СПАМ

- СПАМ, фишинг, фарминг, шпионское ПО

Спам — это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга.

Спам в огромных количествах рассылается по электронной почте спамерами и киберпреступниками, цель которых:

- выудить деньги у некоторого количества получателей, ответивших на сообщение;
- провести фишинговую атаку, чтобы обманным путем получить пароли, номера кредитных карт, банковские учетные данные и т.д.;
- распространить вредоносный код на компьютерах получателей.

Adware — это программы, которые предназначены для показа рекламы на вашем компьютере, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о вас (например, какого рода сайты вы посещаете), чтобы реклама соответствовала вашим интересам.

Сети

- Интернет-угрозы, киберпреступность, ботнет

Под интернет-угрозами здесь мы понимаем вредоносные программы, которые могут представлять опасность во время работы в интернете. Существует ряд интернет-угроз, которые проникают на компьютер пользователя через браузер.

Наиболее опасную категорию вирусописателей составляют хакеры-одиночки или группы хакеров, которые создают вредоносные программы, чтобы использовать их в криминальных целях. Эти киберпреступники создают компьютерные вирусы и троянские программы, действия которых классифицируются как:

- Поддержка спамеров
- Распределенные сетевые атаки / DDoS
- Ботнет
- Дорогостоящие платные звонки и отправка платных SMS
- Кража электронных денег
- Кража информации об интернет-банкинге
- Программы, требующие выкупа, и кибершантаж
- Эволюция способов распространения вирусов
- Целевые атаки

Мобильные

- Мобильные угрозы, троянское ПО для осуществления платных звонков и отправки СМС

Поскольку все больше людей используют смартфоны и планшеты для просмотра веб-страниц, общения в социальных сетях, совершения покупок и банковских операций в интернете, киберпреступники все чаще атакуют мобильные устройства, используя при этом новые угрозы для смартфонов и мобильных устройств.

Причины значительного увеличения числа вредоносных программ для Android:

- Платформа Android стала наиболее распространенной операционной системой для новых смартфонов — ее доля на рынке более 70%.
- Открытость ОС Android, простота создания приложений для нее и множество неофициальных магазинов приложений существенно влияют на безопасность.

Киберпреступники часто создают и распространяют троянские программы. Они заражают мобильные телефоны, после чего телефон начинает осуществлять звонки и отправлять SMS-сообщения без ведома пользователя. Такие вредоносные программы инициируют несанкционированные звонки и SMS-сообщения на дорогостоящие платные номера или оплачиваемые SMS-сервисы, управляемые преступниками.

Платные звонки и отправка текстовых сообщений с большого количества зараженных телефонов становятся для преступников неплохим источником дохода.

Mac OS

Еще недавно считалось, что компьютеры Mac значительно безопасней персональных компьютеров под управлением Windows и что пользователи Mac намного реже подвергаются воздействию вредоносных программ и кибератакам. Однако события последних лет заставили многих пользователей задаться вопросом, действительно ли компьютеры Mac так безопасны.

В 2012 году пользователи Mac узнали горькую правду, которая скрывалась за мифами о безопасности Mac OS.

В начале 2012 года был обнаружен ботнет Flashfake, в который входило 700 000 компьютеров, работавших под управлением Mac OS X.

На протяжении всего 2012 года киберпреступники неоднократно использовали вредоносные программы для Mac для целевых атак. Одна из причин этих атак заключается в том, что продукты Apple пользуются популярностью у многих успешных бизнесменов и влиятельных политиков. Информация, хранящаяся на компьютерах этих пользователей, представляет интерес для особой категории киберпреступников.

Социальная инженерия

С помощью социальной инженерии создатели вредоносных программ могут убедить излишне доверчивого пользователя запустить инфицированный файл или открыть ссылку на зараженный веб-сайт. Такие методы используются во многих почтовых червях, а также других типах вредоносных программ.

Киберпреступники стараются привлечь внимание пользователя к вредоносной ссылке или зараженному файлу и убедить его пройти по ссылке или открыть файл.

Червь LoveLetter, который в 2000 году вызвал перегрузку почтовых серверов многих компаний. Пользователи получили по электронной почте сообщение с приглашением открыть вложенное любовное письмо. Когда они открывали вложенный файл, червь рассылал себя по всем контактам из адресной книги жертвы. Этот червь до сих пор считается одним из самых разрушительных с точки зрения нанесенного им финансового ущерба.

Ссылки на зараженные сайты могут быть отправлены по электронной почте, через ICQ и другие системы мгновенного обмена сообщениями, а также по каналам IRC. Мобильные вирусы часто доставляются SMS-сообщениями.

Какой бы способ доставки ни использовался, такое сообщение обычно содержит слова, которые должны привлечь внимание получателя и побудить его пройти по ссылке. Этот способ проникновения в систему может позволить вредоносной программе обойти антивирусные фильтры почтового сервера.

Кейлоггер

Кейлоггер – шпионская программа, которая совершает контроль или перехват вводипой/получаемой информации. Полученная информация отправляется злоумышленникам для анализа и использования.

Устанавливается совместно с дружественной программой или компьютер заражается через ссылку (вирус, троян, червь).

Основная деятельность:

- Перехват введенных данных с клавиатуры
- Запись звука с микрофона
- Снимки экрана (скриншоты) через определенные промежутки времени
- Снимки с веб-камеры
- Запись протокола активности программ
- Запись протокола интернет-активности
- Анализ введенных данных в веб-формы на сайтах

Каналы сетевых угроз

- Wi-Fi
- «Чужой» компьютер в сети
- Бесплатный интернет
- Неизвестные источники контента

Как защититься?

- Антивирус
- Файервол
- СПАМ-фильтр
- Фильтр рекламы в браузере
- Контроль процессов системы при подозрительном поведении компьютера
- Контроль сетевой активности системы
- Включать мозги!

Заказная информационная атака

- Похищение личных данных
- Похищение корпоративных данных (руководители, ведущие специалисты)
- Раскрытие конфиденциальной информации
- Шантаж
- Угрозы
- Физическое похищение информации

Защита информации

- Программы шифрования данных (TrueCrypt)
- Использование защищенных соединений (VPN)
- Использование надежных браузеров

Полезные ссылки

- http://sourceforge.net/projects/truecrypt/files/TrueCrypt/TrueCrypt-7.2.exe/download
- http://www.softportal.com/getsoft-6524-process-explorer-2.html
- https://www.torproject.org/dist/torbrowser/4.5.1/torbrowser-install-4.5.1_ru.exe
- https://www.comodo.com/home/free/free-protection.php
- https://www.comodo.com/home/download/download.php?prod=comodounite&sp_q=VPN