Digital Security

Клиент банка под атакой

© 2009, Digital Security

Интернет-банкинг

- Практически все банки предоставляют услуги по интернет-банкингу
- Существуют различные аспекты безопасности интернет-банкинга
- Рассмотрим безопасность ПО, поставляемого банками клиенту

© 2002—2009, Digital Security

Специфика модели нарушителя

С точки зрения злоумышленника, пользователь интернет-банкинга является более простой и удобной целью атаки, чем сам банк:

- Пользователь защищен слабее банка
- Пользователей гораздо больше, чем банков
- У одного пользователя может быть клиентское ПО от разных банков

© 2002—2009, Digital Security

Безопасность пользователей банк-клиентов

Безопасность пользователя зависит, от:

1. сохранности ЭЦП и пароля
2. сложности подделки ЭЦП и подбора пароля
3. безопасности рабочей станции
4. безопасности канала передачи
5. безопасности клиентского ПО банк-клиента

© 2002—2009, Digital Security

Особенности клиентского ПО

- Многие банки не пишут свое собственное ПО, а используют решения сторонних производителей
- Это ПО может скачать **любой желающий**; достаточно зайти в раздел демо-версии на сайте разработчика

© 2002—2009, Digital Security

Уязвимости ПО банк-клиентов

Доступ к HDD клиента на чтение и запись

- Суть уязвимости — наличие функций, которые сохраняют или читают файлы, при этом вызов функций ничем не ограничен
- Эти функции можно запустить удаленно, обращаясь к определенным ActiveX-компонентам

© 2002—2009, Digital Security

Уязвимости ПО банк-клиентов

Переполнение буфера

- Банк клиенты, как и любое другое ПО, подвержены уязвимостям переполнения буфера
- В простейшем варианте уязвимость приводит к отказу в обслуживании
- Если возможно выполнение произвольного кода, то можно:
  - получить удаленный административный доступ к системе
  - добавить учетную запись
  - загрузить троянскую программу
  - украсть ключи и другую критичную информацию

© 2002—2009, Digital Security

Реализация атаки

- Перечисленные уязвимости возможно реализовать удаленно, передав жертве ссылку на злонамеренный сайт
- Можно передать ссылку на доверенный сайт, предварительно обнаружив на нем XSS-уязвимость, с помощью которой вызов будет перенаправлен на злонамеренный сайт
- По различным оценкам порядка 80-90% сайтов подвержено XSS, **в том числе и сайты большинства банков**

© 2002—2009, Digital Security

Результат атаки

Данные уязвимости позволяют атакующим проникнуть на машину с установленным банк-клиентом и:

- загрузить специализированный троян или клавиатурного шпиона, что бы узнать логин и пароль
- найти ключи на жестком диске или дискете
- если ключи на устройстве USB-Token, то можно перехватить вызов функции подписи и подменить документ

Уязвимость банк-клиента — ключ к проникновению во внутреннюю корпоративную сеть компании

© 2002—2009, Digital Security

Результаты исследований

1. Были проанализированы 3 банк-клиента зарубежных производителей, используемых в ряде европейских банков
2. В 2-х была обнаружена уязвимость доступа к дискам
3. В 3-х — переполнение буфера (из них в 2-х возможность выполнения произвольного кода)
4. Подобные уязвимости были обнаружены и западными исследователями в других зарубежных продуктах, например: **danske bank ActiveX buffer overflow**

© 2002—2009, Digital Security

Защита с точки зрения разработчика

- Закрытие уязвимостей в ПО
  - необходимо помнить про такие классические ошибки, как переполнение буфера
  - необходимо ограничить доступ к функциям, которые позволяют получить доступ к файловой системе
  - необходимо ограничить доступ к функциям работы с реестром
- Сторонний аудит безопасности приложений

© 2002—2009, Digital Security

Защита с точки зрения клиента

- Безопасные настройки браузера
- Запуск браузера от непривилегированной учетной записи
- Дополнительные средства защиты от фишинг-атак и XSS
- Не переходить на непроверенные ссылки

© 2002—2009, Digital Security