

Безопасность бизнес-приложений

Илья Медведовский,
к.т.н., директор Digital Security



Сложные в техническом плане системы

В основном мало изучены, так как не всем доступны и находятся “внутри” КИС



Содержат большое количество уязвимостей на всех уровнях

Редко подвергаются дополнительным вмешательствам по принципу «Работает – НЕ трогай»



Сетевой уровень

Уровень ОС

Уровень СУБД

Серверы приложений

Клиентские приложения

! Все уязвимости, присущие перечисленным уровням, обычно присутствуют в корпоративных приложениях

Сеть

- отсутствие шифрования, перехват трафика, уязвимости протоколов

Операционная система

- уязвимости ОС и сетевых приложений
- излишние права доступа, некорректные настройки

СУБД

- уязвимости
- стандартные пароли, отсутствие парольных политик
- некорректные настройки

Серверы приложений

- полный перечень существующих веб-уязвимостей (XSS, SQL Injection, Auth Bypass, XSRF и др.)
- переполнения буфера
- разграничение полномочий
- прочие недостатки

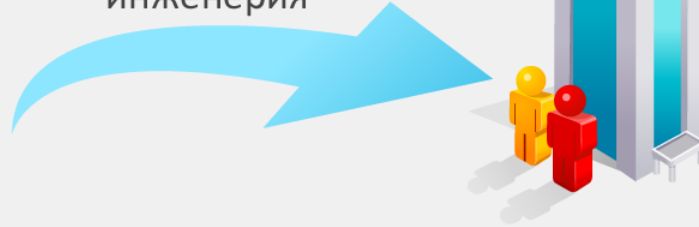
Клиентские приложения

- удаленные уязвимости ПО
- уязвимости ActiveX компонентов
- социальная инженерия

1.



социальная инженерия



Пользователям SAP было отправлено письмо, в котором при помощи социальной инженерии предлагалось перейти по [ссылке](#)

2. Ссылка вела на страницу, вызывающую уязвимый компонент **ActiveX**, входящий в состав клиентского приложения SAP GUI



ActiveX



[click me!!!](#)

3.



интернет



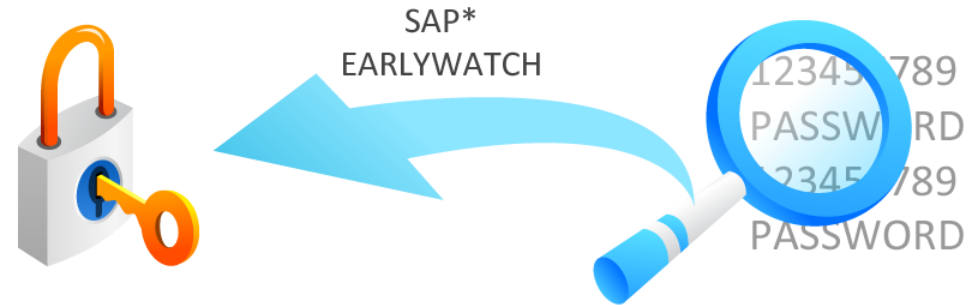
0-day уязвимость переполнения буфера в **ActiveX** компоненте, позволяла получить **удаленный доступ** на рабочую станцию пользователя

1.



С рабочей станции была получена информация о всех SAP системах предприятия (файл `sapgui.ini`)

2. Далее были проверены стандартные пароли к стандартным учетным записям таким как `SAP*` и `EARLYWATCH`



3.



В результате **3 из 10 систем** имели стандартные пароли на доступ к стандартным клиентам (мандантам), которые используются для администрирования, но не содержат бизнес данных

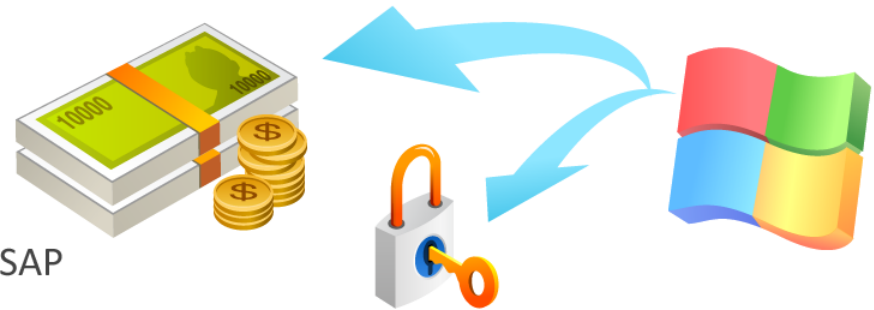
1.



Получив **доступ в SAP** при помощи одной из транзакций, позволяющей выполнять команды ОС, был **получен доступ непосредственно в ОС**

2. Доступ к ОС позволил:

- получить доступ к СУБД и через нее уже ко всем бизнес данным SAP
- включить перехватчик сетевых пакетов (сниффера), что позволило перехватить хэши паролей пользователей на доступ к SAP



3.



Расшифрованные пароли были проверены на доступ к другим SAP системам: в итоге **ещё 5 из 10 систем** оказались под контролем

- Получен доступ к **80% SAP систем** компании из сети Интернет, даже не используя продвинутые методы атак!
- В ходе проникновения были использованы **только уязвимости SAP систем**
- **Сценарий проникновения инвариантен** относительно ПО, оборудования и инфраструктуры компании
- Несмотря на безопасные настройки КИС, успех данного сценария атаки был обусловлен **отсутствием должного внимания к безопасности бизнес приложения SAP**

	SAP		Oracle	
Всего опубликовано	8	14	84	114
Обнаружены Digital Security	5	11	8	12
Опубликованы Digital Security	3	7	5	5

Требуется проводить
детализированный аудит защищенности
бизнес-приложений