Криптографические плагины для браузеров

Смирнов Павел
Зам. начальника отдела разработок, к.т.н.
ООО «КРИПТО-ПРО»

План

- Криптография в браузере для облачных сервисов
- Функции криптографического плагина
  - Целевая
  - Защитная
- Что работает не так
- Как это исправить

Дорога в облака

Все там будем.

Применение криптографических плагинов

Где применяются

- Электронные торговые площадки
- Порталы государственных услуг
- Интернет-банкинг

Для чего применяются

- Аутентификация пользователя
- Создание/проверка ЭП
- Зашифрование/расшифрование

Веб – недоверенная среда

- JavaScript выполняется в «песочнице», но…
- Плагин – проход в стене песочницы

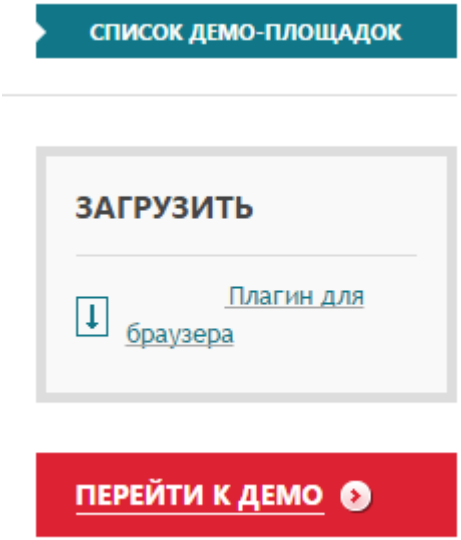
От чего должен защищать плагин

Угрозы:

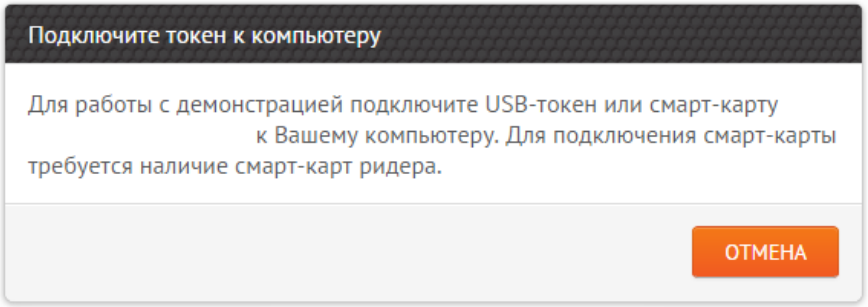
- Блокировка токена/смарткарты
- Чтение локальных файлов
- Чтение сертификатов пользователя
- Использование закрытого ключа
  - Подпись, расшифрование

Кого исследовали

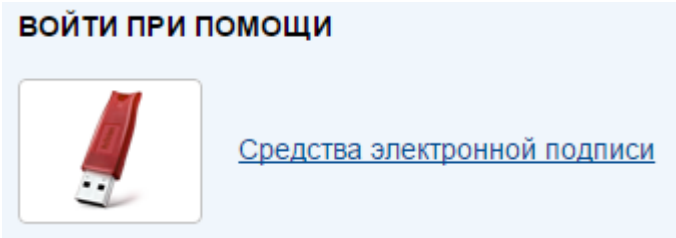
Вендор №1



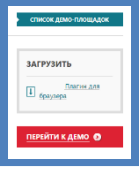
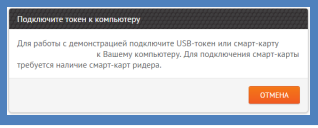
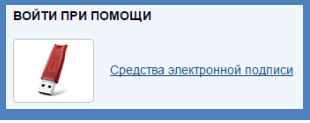
Вендор №2



Вендор №3



Что плохого обнаружили

Угроза	Вендор №1	Вендор №2	Вендор №3
			
Блокирока токена/смарткарты	Да	Да	Да
Чтение локальных файлов	Нет	При ПИН-коде по умолчанию	Нет
Чтение сертификатов пользователя	Да	Да	Да
Подписание документов	При запомненном ПИН-коде или по умолчанию	При ПИН-коде по умолчанию	При запомненном ПИН-коде или по умолчанию

Как закрыть уязвимости

Запускаться только на ограниченном наборе сайтов

Годится для плагинов ограниченного распространения

или

Задавать вопрос пользователю

Менее удобно для пользователя, но можно предусмотреть список «доверенных» сайтов

Как жить без плагинов

Курс на веб без плагинов

- Chrome полностью отключит NPAPI в сентябре 2015 года

В угоду безопасности?

- Число векторов атак уменьшается
- Возможность взаимодействия с нативным кодом остаётся

Chrome Extension + Native Messaging

- Предварительная версия КриптоПро ЭЦП Browser plug-in доступна
- Описанные угрозы остаются

СПАСИБО ЗА ВНИМАНИЕ!

КРИПТО-ПРО – ключевое слово в защите информации

http://www.cryptopro.ru
Тел./факс:
info@cryptopro.ru
+7 (495) 995-48-20
spv@cryptopro.ru