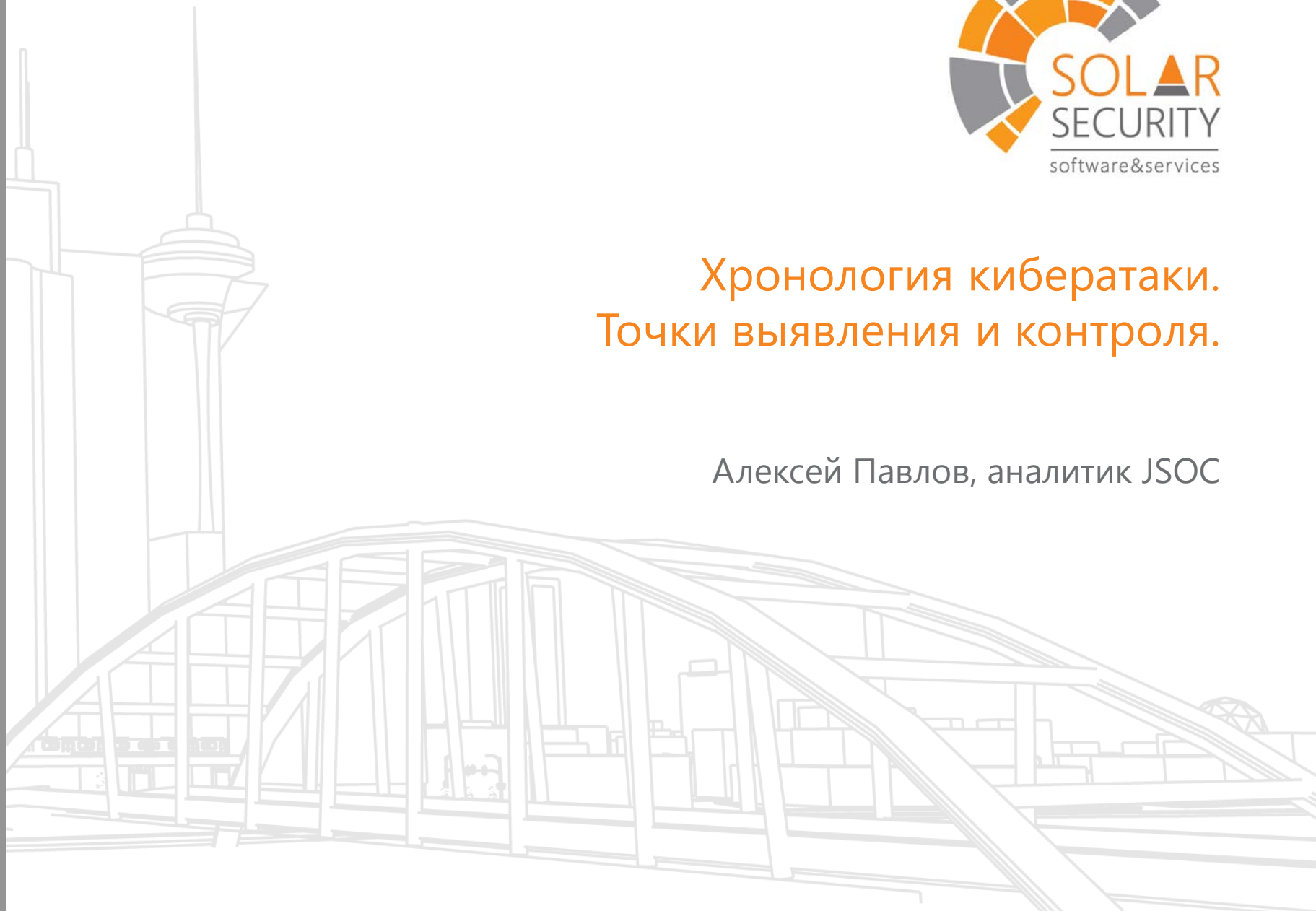


SOLAR SECURITY
software&services

Хронология кибератаки. Точки выявления и контроля.

Алексей Павлов, аналитик JSOC

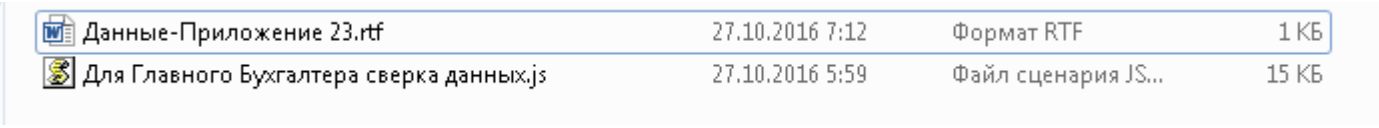
Признаки успешной схемы

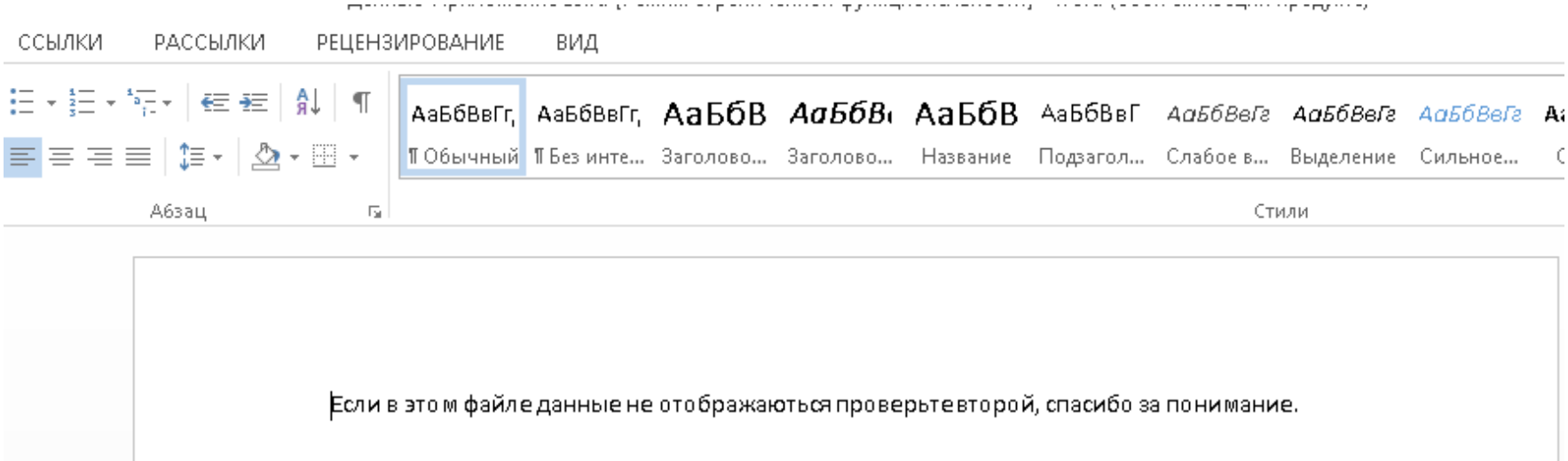
- Масштабируемость
- Универсальность
- Легкая монетизация
- Оригинальность

Развитие атаки

- Проникновение в инфраструктуру
- Расширение сферы влияния
- Получение доступа к ключевым системам (ERP, CRM, АБС, процессинг)
- Хищение информации, вывод денежных средств

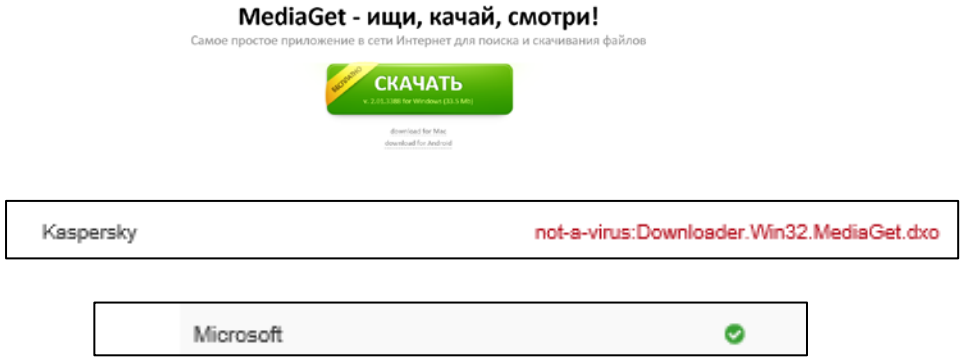
Точка входа в инфраструктуру





Точка входа в инфраструктуру

- 14 May 2016 17:23:44 MSK Запуск MediaGet (-zapiska-obrazets.exe)
- 14 May 2016 17:44:14 MSK Последний логин пользователя
- 15 May 2016 03:07:57 MSK Запуск процесса vuupc.exe
- 15 May 2016 03:08:02 MSK Инцидент
- 15 May 2016 03:26:00 MSK Оповещение аналитика по телефону
- 15 May 2016 03:32:48 MSK Оповещение от 1-й линии в сторону Заказчика
- 15 May 2016 03:55:00 MSK подключение машины к ArcSight



ProcessName
C:\Users\[redacted]\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\UPDI94DB\-zapiska-obrazets.exe
C:\Users\[redacted]\AppData\Local\Temp\SkinAppSetup.exe
C:\Users\[redacted]\AppData\Local\Temp\Oursurfing.exe
C:\Users\[redacted]\AppData\Local\Temp\Bundle.exe
C:\Users\[redacted]\AppData\Local\Temp\gamesdesktop.exe
C:\Users\[redacted]~1\AppData\Local\Temp\js-B4OR6.tmp\gamesdesktop.tmp
C:\Users\[redacted]\AppData\Local\Temp\qweee.exe
C:\Users\[redacted]\AppData\Local\Temp\jobitdownloader_installcube.exe
C:\Users\[redacted]\AppData\Local\Temp\vuupc.exe
C:\Users\[redacted]\AppData\Local\Temp\jdmstartsearch.exe
C:\Users\[redacted]\AppData\Local\Temp\loadmoney.exe
C:\Users\[redacted]\AppData\Local\Temp\mailruhomesearchvbm.exe

Точка входа в инфраструктуру
Меры

- Антивирусы, анти-спам
- Контроль рабочих станций ключевых сотрудников
- Security awareness
- IPS, песочницы, UTM, NGFW, WAF
- Использование репутационных баз

Шаг второй:
Обустройство. Типовые шаги

- 22.08.2016 19:35-19:50 Непредвиденное завершение работы операционной системы 4-х серверов, вызванное критической ошибкой (Crush)
- Анализируемые данные:
  - Логи контроллеров домена
  - Локальные логи серверов
  - Логи ДНС
- Сложности:
  - Локальный Security log очищен
  - Нет сетевых событий – отсутствует сегментация сети

АНАЛИЗ

- Анализ MFT и USN – нет данных. Частая дефрагментация
- Анализ доменных логов – аутентификация доменного администратора
- Анализ system event log:
  - 11.08.2016 14:58:31 EventID 7045 – в системе установлена служба it_helpdesk (исходное имя psexecsvc)
  - Количество запусков с момента установки – 45.
- Анализ текущего состояния файловой системы:
  - 11.08.2016 15:21:33 – Замена легитимной библиотеки Windows/System32/Sens.dll
  - 11.08.2016 15:39-45 - Создание Windows/tvnserver.exe и Windows/screenhooks32.dll (компонент Tight VNC), Windows/System32/stor32.dll – keyloger и users.exe+negative.dll - отправка данных по DNS-туннелю.
  - 11.08.2016 15:48:19 - Создание C:/Users/<compromised user>/AppData/LocalLow/NTUSER.DAT – запись работы кейлоггера
- Анализ DNS:
  - 11.08.2016 - 22.08.2016 успешные попытки резолва доменный имен вида dfsfqerewewzxc.<malware_site1>.eu, sdfjhk5lkjsd8as23jfdgjhdka.<malware_site2>.net.
  - Доменов - 5, хостинг – 1.

ПРЕДВАРИТЕЛЬНЫЕ ВЫВОДЫ

- ✓ Данный сервер не из первых зараженных машин в инфраструктуре
- ✓ Канал попадания вредоноса – скомпрометированная УЗ доменного администратора
- ✓ Инструмент - psexec

ПОИСК


Индикаторы компрометации
Мониторинг ДНС запросов от хостов
Сбор информации: Следы присутствия вредоноса
PowerShell-скрипт: поиск исполняемых файлов
PowerShell-скрипт: Сбор System event log с хостов – поиск запуска службы
Антивирус: поиск по базе MD5 psexecsvc
PowerShell-скрипт: поиск модифицированных веток реестра

ПОСЛЕДСТВИЯ

- Временные нарушения в работе ключевых приложений
- Взломан файл PS.xls с паролями на сервера ERP, CRM, хранящийся на зараженной машине
- Многочисленные успешные попытки входа в БД приложений, CRM с УЗ администратора с скомпрометированных машин
- Общий объем DNS-трафика на управляющий центр > 1 Гб

Обустройство. Типовые шаги
Меры

Базовые

- Антивирус, контроль приложений (черный список)
- Запрет (ограничение) локального администратора для сотрудников
- Запрет, либо контроль RAT, TOR на прокси
- Сегментация сети

Дополнительные

- Контроль базовых сценариев (сеть, брутфорсы)
- Использование репутационных баз
- Application white listing
- Контроль съемных носителей
- Физическая изоляция сегментов

Шаг третий:
Контроль над целевыми хостами, учетками

- ✓ Заражение машины сотрудника ИБ
- ✓Доступ до сервера сканера защищенности
- ✓Запуск сканирования в ночное время
- ✓Выявление уязвимостей межсегментных МСЭ
- ✓Проникновение в критичный сегмент с хоста сканера защищенности

Контроль над целевыми хостами, учетками
Меры

- Мониторинг доменных активностей
- Контроль целостности ключевых машин
- Контроль съемных носителей
- Application white listing
- Профили критичных машин, ключевых учетных записей

Шаг Четвертый:
Поход за информацией, деньгами

- Аутентификации в нерабочее время
- Использование технологических УЗ
- Нестандартные механизмы подключения к БД
- Запуск утилит на серверах
- .....

Шаг Четвертый:
Как бывает……

Login
{\«lastName\":null,\,\"email\":\"******@MAIL.RU\",\"userId\":****,\"login\":\"
*****@MAIL.RU\",\"firstName\":\"Константин\“,\"address\": 2.95.*.*}

modify_order_bonus ":"{\"bonusAvailable\":18.0,\"bonus\":20000}" reason: **ERROR**

modify_order_bonus ":"{\"bonusAvailable\":18.0,\"bonus\":10000}" reason: **ERROR**

modify_order_bonus ":"{\"bonusAvailable\":18.0,\"bonus\":5000}" reason: **ERROR**

modify_order_bonus ":"{\"bonusAvailable\":18.0,\"bonus\":1000}" reason: **ERROR**

modify_order_bonus ":"{\"bonusAvailable\":18.0,\"bonus\":-20000}" reason: **SUCCESS**

-20 000 < 18.0

Поход за информацией, деньгами
Меры

- Выявление аномалий в аутентификации, соединениях
- Application white listing+контроль запуска процессов
- Исключение (по возможности) машин из домена + /etc/hosts
- Контроль изменений ключевых полей БД, нестандартных механизмов подключения

Спасибо!
Вопросы?

Павлов Алексей
av.pavlov@solarsecurity.ru
+7 (916) 178 98 90

Эффективность-реализуемость мер