


Know Thy Limits

Возможности систем обнаружения веб-сайтов, реализующих атаки Drive-by-Download

Андрей Петухов, Александр Раздобаров
факультет ВМиК МГУ им. Ломоносова

Контекст

- Ненаправленные атаки vs направленные атаки
- Атаки класса Drive-by-Download
- Задачи злоумышленника
  - ✓ максимизировать поток посетителей на сайт
  - ✓ максимизировать “пробив”
  - ✓ максимизировать время жизни сайта (или ВПО на сайте)

Задача обнаружения DbD

- Установить факт проведения сайтом атаки Drive-by
- Кому интересно?
  - ✓ поставщикам решений по End-point защите
  - ✓ поисковым системам
  - ✓ владельцам сайтов
- Вопрос: насколько хорошо они это делают?
- Вопрос: насколько просто им противодействовать?
- Мотивация: заявления об эффективности wepawet

Цель и постановка задачи

- Исследование ограничений средств обнаружения вредоносных сайтов, реализующих атаки DbD
- Предположения:
  - ✓ эксплойт, реализующий атаку, не поддается обнаружению методами статического сигнатурного анализа большинством AB
  - ✓ атаки обнаруживается какими-то AB методами динамического анализа
    - часть посетителей сайта с AB не подвержены атаке
    - злоумышленник ведет борьбу за остальных посетителей сайта, уязвимых к атаке
  - ✓ ВПО и распространяющий его код реализуют методы противодействия обнаружению

Методы противодействия

- Фильтрация HTTP-запросов
- Цель: не допустить на сайт “светозарных джеддаев”
- Методы
  - ✓ по IP (условно и безусловно, incl. Tor Exit Nodes, проверка адреса DNS-сервера)
  - ✓ по заголовку HTTP referrer
  - ✓ по HTTP-cookie, flash cookie
  - ✓ по заголовкам управления кешированием (ETag/If-Match, Expires/If-Modified-Since)
  - ✓ локальное хранилище в браузере (localStorage)

Методы противодействия

- Фингерпринтинг поведения
- Цель: не допустить на сайт нечеловеков
- CAPTCHA не предлагать!
- Методы
  - ✓ отлов DOM-событий из JavaScript (особенно, возникающих при визуализации)
  - ✓ всплывающая реклама
  - ✓ CSS history hack
  - ✓ закачка ресурсов (связанные картинки, тот же favicon.ico, css, js)

Методы противодействия

- Фингерпринтинг ПО
- Цель: не допустить клиентов, не подверженных атаке
- Методы
  - ✓ определение типа по различию в интерпертации Javascript
  - ✓ определение версии по поддержке HTML5, CSS3
  - ✓ если не коррелирует с UA - от ворот поворот!
  - ✓ еще больше можно получить из flash и java-апплетов

Методы противодействия

- Обфускация и привязка кода к окружению
- Цель: затруднить оффлайн анализ Javascript-кода
- Методы
  - ✓ обфускация (jjencode)
  - ✓ шифрование, ключом которого является переменная браузера, зависящая от окружения (document.location, document.referer, cookie, заголовки от сервера)
  - ✓ $=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.

Результаты

- Среда для генерации страниц, реализующих “обвязку” для атаки Drive-by-Download
  - ✓ среда реализована на Node.JS + MongoDB
- Ни одна из протестированных систем обнаружения вредоносных сайтов не дошла до атаки (FAIL!)
  - ✓ нам даже не пришлось включать фильтрацию по IP
  - ✓ самый “отсеивающий” метод противодействия - фингерпринтинг поведения
- Готовы протестировать вашу систему (NDA included!)

Спасибо за внимание

- Email: petand@lvk.cs.msu.su
- Web log: http://andrepetukhov.wordpress.com/
- Tel: +7 (495) 932-88-58