웹 아티팩트

1 캐시

- 웹 사이트 방문 시, 사이트로부터 자동으로 다운받은 컨텐츠
- 컨텐츠 캐시를 통해 재 방문 시 로딩 속도 향상
- 캐시 데이터 (다운받은 데이터)
  - 이미지 파일, 텍스트 파일, 아이콘, HTML 파일, XML 파일, 스크립트 등
- 캐시 인덱스 정보
  - 캐시 데이터 위치, 다운로드 URL, 다운로드 시간, 다운로드 데이터 크기 등

1.1 분석방법

- 다운로드 URL + 다운로드 시간 -> 특정 시간에 해당 사이트 이력
- 다운로드 URL + 키워드 검색 -> 중요 사이트 방문 이력 확인
- HTML 캐시 파일 – 웹 메일 내용 확인
- 웹 브라우저에서 문서 열람 시 열람 파일 그대로 저장 – PDF, HWP 등

2 히스토리

- 사용자가 방문한 웹 사이트 접속 정보 저장
- 월별, 일별 방문 기록을 분류해서 저장
- 히스토리 정보
  - 방문 사이트 URL, 방문 시간, 방문 횟수, 사이트 제목 등
- 저장 형식
  - 직접 접근 – URL 입력창에 직접 주소 입력
  - 간접 접근 – URL 링크를 통해서 접근

2.1 분석방법

- 방문 사이트 URL + 방문 시간 -> 해당 사이트 방문 이력
- 방문 사이트 URL + 방문 횟수 + 키워드 검색 -> 사용자 행위 분석
- GET 방식으로 전달된 인자 값 분석
  - 검색어 추출
  - 아이디, 패스워드 추출
- 검색어 URL 인코딩
  - ex)
  http://search.daum.net/search?w=tot&DA=YZRR&t__nil_searchbox=btn&sug=&sq=&o=&q=%ED%8F%AC%EB%A0%8C%EC%8B%9D

3 쿠키

- 웹 사이트 방문 시 자동으로 사용자 저장장치에 저장되는 텍스트 데이터
- 사용자 기반 서비스 제공
  - 자동 로그인 기능
  - 쇼핑몰 열람한 물건, 장바구니 물건
  - 웹 하드 찜 해놓은 자료, 다운받은 자료
- 쿠키 정보
  - 호스트 사이트, 경로, 수정 시간, 만료 시간, 이름, 값 등

3.1 분석방법

- 호스트, 경로 -> 접속한 사이트, 사용한 서비스
- 수정 시간 -> 마지막 접속 시간
- 이름, 값 -> 로그인 아이디 저장 옵션 활성화 시, 로그인 아이디 획득 가능
- 구글 애널리틱스 정보
  - 어느기기로 , 어느 브라우저로, 연령대까지 기록해주는 기능이다 .
  - 구글에 신청하고 웹페이지에 한줄만추가하면된다..
  - 이런사이트는 쿠키에 좀더유용한정보를 남긴다.

4 다운로드목록

- 사용자가 선택하여 내려 받은 파일 정보 -> 사용자 편의를 위해 저장
- 사용자 의도와 관련 없이 다운로드되는 캐시 데이터와는 구분
- 다운로드 목록 정보
  - 다운로드 파일 저장 경로, 소스 URL, 파일 크기, 다운로드 시간, 다운로드 성공 여부

4.1 분석방법

- 다운로드 URL -> 접속 사이트
- 다운로드 시간 -> 해당 파일의 다운로드 시간
- 다운로드 파일의 경로 -> 파일 내용 확인
- 다운로드 받은 파일이 없을 경우, 저장된 URL을 이용해 다운로드 재시도
  - 대용량메일은인증이없다 .따라서링크만있으면 얼마든지다운받을수있다 .

5 아티팩트 경로

- **인터넷 익스플로러 (IE, Internet Explorer)**

구분	경로
Cache	%UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5**index.dat** %UserProfile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\<Random>\<All Files>
History	%UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5**index.dat** %UserProfile%\AppData\Local\Microsoft\Windows\History\History.IE5\<period>**index.dat**
Cookie	%UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies**index.dat** %UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies\<All Files>
Download	%UserProfile%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory**index.dat** (IE9 ~)
IE v10	**%UserProfilel%\AppData\Local\Microsoft\Windows\WebCache**WebCacheV(01|24).dat

- **사파리 (Safari)**

구분	경로
Cache	%UserProfile%\AppData\Local\Apple Computer\Safari**Cache.db**
History	%UserProfile%\AppData\Roaming\Apple Computer\Safari**History.plist**
Cookie	%UserProfile%\AppData\Roaming\Apple Computer\Safari\Cookies**Cookies.plist**
Download	%UserProfile%\AppData\Roaming\Apple Computer\Safari**Downloads.plist**

- **오페라(Opera)**

구분	경로
Cache	%UserProfile%\AppData\Local\Opera\Opera\cache**dcache4.url**
History	%UserProfile%\AppData\Roaming\Opera\Opera**global_history.dat**
Cookie	%UserProfile%\AppData\Roaming\Opera\Opera**cookies4.dat**
Download	%UserProfile%\AppData\Roaming\Opera\Opera**download.dat**

- **크롬 (Chrome)**

구분	경로
Cache	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Cache\
History	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default**History** %UserProfile%\AppData\Local\Google\Chrome\User Data\Default\History\History Index <year-month>
Cookie	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default**Cookies**
Download	%UserProfile%\AppData\Local\Google\Chrome\User Data\Default**History**

- **파이어폭스 (Firefox)**

구분	경로
Cache	%UserProfile%\AppData\Local\Mozilla\Firefox\Profiles\<Random>\Cache*.*
History	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default**places.sqlite**
Cookie	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default**cookies.sqlit**
Download	%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\<Random>.default**download.sqlite**

6 아티팩트 분석

6.1 시점이 특정되는 경우

- 시점을 기준으로 캐시, 히스토리, 쿠키, 다운로드 목록에 대한 통합 타임라인 분석

6.2 시점이 특정되지 않은 경우

- 웹 브라우저로 다운받은 PE 파일 검색
- 이상 패턴 검색 (a.jpg, b.gif, 1322.jpg, 2499.jpg 등)
  - 악성코드의 이름 또는 버전을 관리하기 위해 숫자로 저장한다.
- 악성 사이트 접속 여부
  - 시스템 프로파일(%SystemRoot%₩System32₩config₩systemprofile₩) 분석

6.3 악성 URL 목록 및 URL 점검

- 최신이 아닌 한달정도가 지난정보이다.
- Automater, http://www.tekdefense.com/automater/
  - 입력기능 – 도메인명, IP 주소, MD4 해시값
  - 출력기능 – HTML, CSV, TXT
  - 쿼리 사이트 지정 – 지정한 사이트만 쿼리 (sites.xml 참고)
  - 다중 질의 지원 – URL이 나열된 TXT 파일 입력 가능

7 액티브X

- 웹 상에서 컨텐츠를 다운로드하기 위한 프레임워크 (IE 상에서만 실행됨)
- 웹 서비스만으로 부족한 부분을 클라이언트에 프로그램 설치로 보완
- 사용자의 동의를 유도하여 악성 프로그램 설치

7.1 다운로드경로설정

- 키 : HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Internet Settings
- 값 : ActiveXCache

7.2 기본다운로드 경로

- %SystemRoot%₩Downloaded Program Files

8 자바 애플릿

- 웹 브라우저를 통해 실행되는 자바 기반의 애플리케이션
- 애플릿을 다운받아 클라이언트에서 실행 -> 자바 가상머신 설치 필요
- 자바는 액티브액스 보다 흔적이 하나 더 남음
  - jar
  - index파일

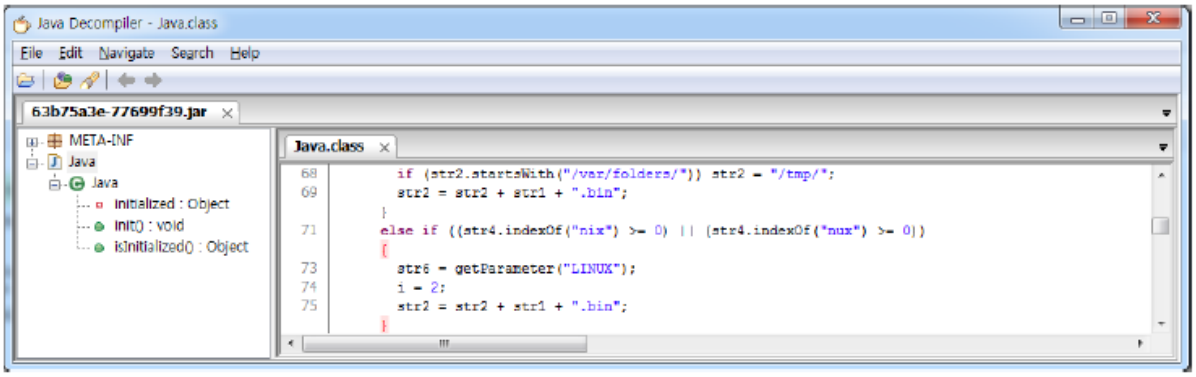
8.1 취약점

- 자바 애플릿(JAR)을 통해 다운로드, 실행 -> 악성코드 실행, JRE 취약점 악용
- 자바 애플릿이 실행되면 JAR 파일, IDX 파일이 캐시 폴더에 저장
  - %UserProfile%₩AppData₩LocalLow₩Sun₩Java₩Deployment₩Cache₩##

8.2 JAR 파일

- 다운로드되면서 랜덤한 이름으로 변환되어 저장
- JAR 압축 해제 -> 디컴파일을 통해 분석 가능

- **자바 애플릿(JAR) 파일**



8.3 IDX 파일

- 다운받은 JAR 파일과 동일한 경로에 '.idx' 형태로 저장
- 다운받은 경로(IP 주소 혹은 도메인명), HTTP 헤더, 다운로드 시간 확인 가능
- 분석도구 : Java_IDX_Parser – Brian Baskin
  - https://github.com/Rurik/Java_IDX_Parser

- **자바 IDX 파일**

```
[*] Section 2 (Download History) found:
URL: http://207.58.245.179:80/tY77np5Yyi
IP: 207.58.245.179
<null>: HTTP/1.1 200 OK
content-length: 32768
last-modified: Tue, 03 Apr 2012 00:25:21 GMT
content-type: text/plain; charset=UTF-8
date: Tue, 03 Apr 2012 00:32:31 GMT
server: Apache/2.2.17 (Fedora)
```

9 기타

- 북마크
- 시작페이지/화면구성
- 세션(탭) 저장 정보
- 자동완성(폼, 데이터, ID, 패스워드) 정보
- 파비콘 정보