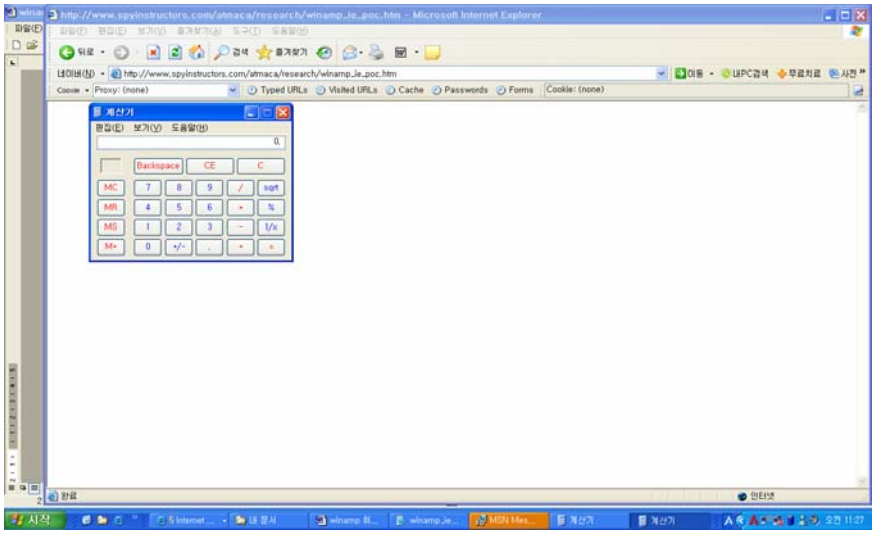
제목: Winamp Application 문제의 현황 및 해결
작성자: 바다란 , 작성일 2006.2.1일 잠시동안

1.개요:

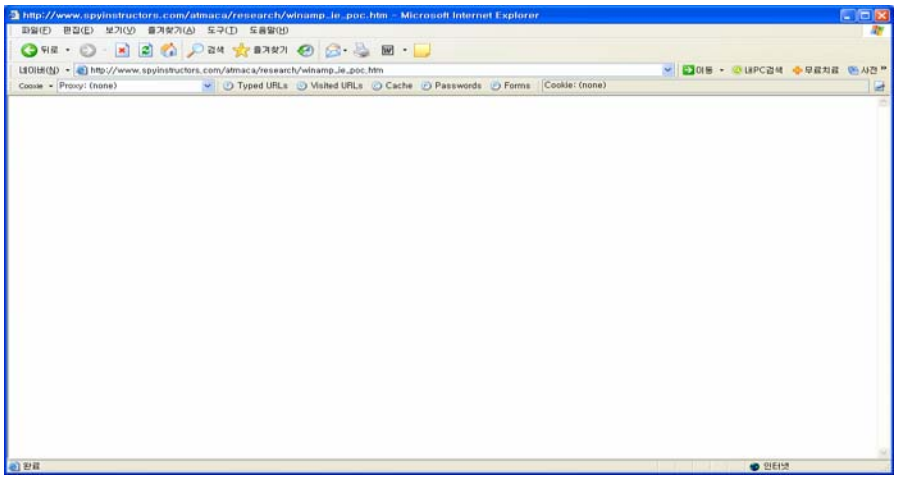
Winamp 문제 발생 버전은 5.12 버전 이하이며 Universal 버전의 exploit이 1.31일 발표된 상황입니다. 1.29일 최초 exploit 발표 이후 Universal exploit이 추가로 발표되어 동일한 공격이지만 향후 활발한 공격이 예상 됩니다.
http://www.frsirt.com/exploits/20060131.winamp_playlist_unc.pm.php
http://www.frsirt.com/exploits/20060129.winamp0day.c.php
(공격 코드에 대한 분석은 특별히 하지 않는다. 관심 있는 분 각자 해보시길)
또한 전 세계적으로 많이 사용되는 미디어 관련 Application이다 보니 국내는 물론 세계적으로도 피해가 예상이 됩니다. 현재 많이 발생 되고 있는 사용자 정보를 빼내어 가는 공격은 물론 사용자 PC를 제어하는 웜 및 Bot 관련 전파에도 다수 이용이 될 수 있으므로 위험한 상황이라 할 수 있다.
최초 문제를 공격하는 exploit은 1.29일 출현 하였으며 문제의 원인은 winamp 프로그램내에서 PLS 파일을 파싱하는 과정에서 문제가 발생 . winamp가 pls 파일을 파싱 할 때 File1 인자에 대해서 문제가 발생함 . pls 및 m3u , cda format은 winamp 상에서 사용자가 작성이 가능한 리스트이다. 만약 pls 파일내의 File 인자에 과도한 길이를 입력할 경우 (대략 1040byte) Overflow가 발생되며 임의의 명령을 실행 시킬 수 있는 것이 발견 되었으며 단일 Exploit 또는 여러 공격을 통합한 공격 유형으로 제작이 되어 근 시일 내에 공격이 이루어 질 것이다.

2. 분석

자신의 Winamp player가 위험한지 여부를 확인 하기 위해서는 winamp의 버전을 확인 하거나 (5.12 버전 이하) 위험여부 확인 URL을 통해 체크가 가능하다.
http://www.spyinstructors.com/atmaca/research/winamp_ie_poc.htm



URL 실행 시 취약한 버전의 Winamp 사용 시에는 위와 같이 임의의 프로그램 (여기에서는 calc.exe)이 실행이 된다. Winamp를 설치 하지 않은 경우에는 아무런 위해 행위가 발생되지 않는다. 이 공격 코드 자체는 Winamp Application의 취약성을 공격하는 코드 이므로 winamp program이 설치 되지 않은 곳은 아래와 같이 아무런 영향이 없다.



공격코드

http://www.spyinstructors.com/atmaca/research/winamp_ie_poc.htm

위의 URL 코드는 아래와 같다. iframe으로 pls 파일을 브라우저에 실행 하도록 지정이 되어 있으며 pls 확장자와 매핑이 된 실행 프로그램이 있을 경우 해당 프로그램을 실행하게 된다. Pls 확장자는 winamp application과 연동이 되어 있다.

```
<html><body><iframe width="0" height="0" marginwidth="0" marginheight="0" border="0" frameborder="0" src="crafted.pls"></iframe></body></html>
```

위의 악성코드를 포함한 html 파일에서 다운 받도록 하는 crafted.pls 파일의 내용은 playlist 항목의 형식을 그대로 유지하고 있으며 File 인자에 입력이 되는 문자열의 길이가 충분히 길 경우에 Overflow가 발생 되게 된다.

Crafed.pls 파일의 내용

[playlist]

File1=₩₩릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮릮
릮릮
릮릮
릮릮
릮릮
릮릮
릮릮
릮릮
릮릮
릮릮
릮릮릮릮릮릮릮릮릮릮릮릮릮TPSP)?祐?[illegible]?갸┐?M껒悔梢5JM┐?◘>VrHz鰒힛홏↕"奉┘됫꾿壹塊
쳈?| ?└亮9?Iw8?&奉+ 됏E??쫠해L?Ri--?쮍VN}?vA둪┐?젓?뎜D?쬚┐?%>?팦뙊탕 u jV 칁탺
퀒?꿦픎!a?M릮a?┐꿂4[illegible]?릮?Title1=~BOF~

Length1=FFF

NumberOfEntries=1

Version=2

winamp 설치 버전에 대해서는 다음과 같은 문제 발생

본 테스트 환경에서는 일반적으로 구할 수 있는 winamp 5.12 lite 버전 설치

취약버전 실행시에는 다음과 같은 샘플 공격 코드에서 실행하도록 지정한 calc.exe 실행됨

WINAMP Application 설치 PC 상에서의 감염 유형 – 2 가지

- 자동실행 – winamp 확장자가 매칭되어 자동 실행으로 설정이 될 경우 악성코드를 포함한 .pls 파일의 다운로드시 winamp가 자동 실행 되며 overflow 발생되어 winamp를 실행시키는 권한으로 임의의 명령 실행이 가능함 (ex:calc.exe)

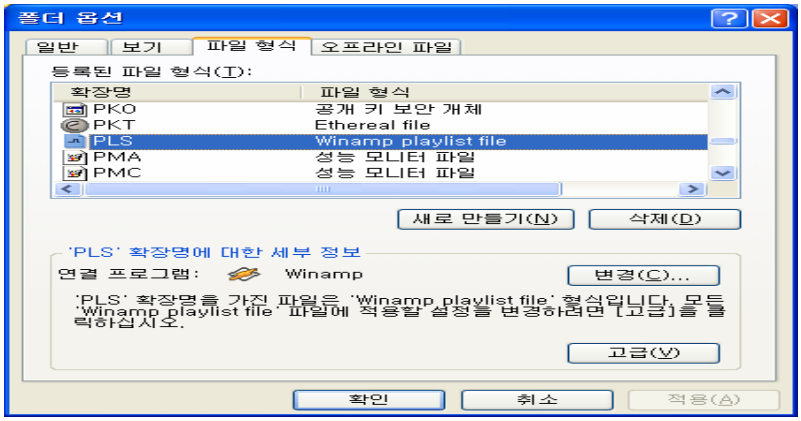
- 임의 실행 – 악성코드를 포함한 .pls 파일을 더블클릭 하거나 열기를 선택 할 경우 winamp가 실행이 되며 이후 임의의 명령 실행이 됨 (ex: calc.exe)

3. 문제 해결

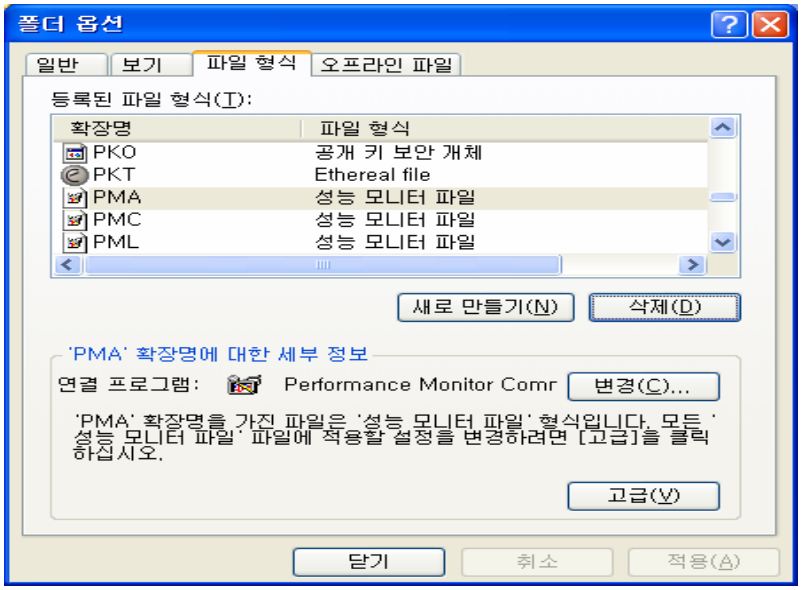
문제 해결 방식은 간단하다. 첫 번째로 Winamp application 의 제거 혹은 5.12 버전 이상인 5.13 버전으로의 업데이트가 있으며 두 번째로는 현재 PLS 확장자의 Parsing에서 발생되는 문제이므로 해당하는 확장자와 연결된 프로그램 항목을 제거하면 기본 문제는 사라지게 된다.

Winamp application 5.13 버전의 다운로드 :
http://www.winamp.com/player/

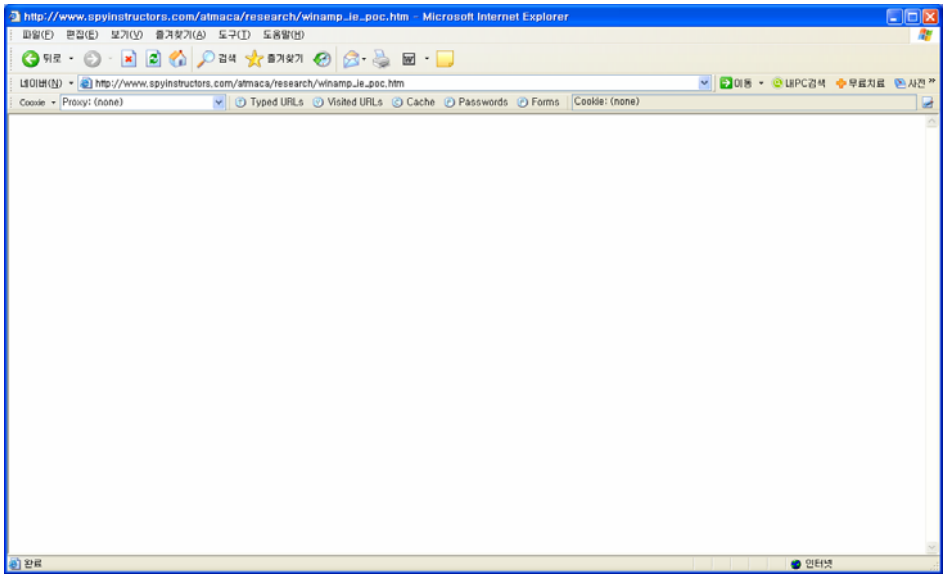
winamp 문제의 임시해결
탐색기 -> 도구 -> 파일형식 -> PLS 찾기 후 제거



제거 이후



제거 이후 실행 되지 않음



확장명에 대한 제거 이후에 pls 확장자에 대한 실행 명령만 제거할 경우 명령 실행이 되지 않음. 해당 실행 명령 제거는 winamp와의 연결정보 제거 이므로 그다지 영향이 크지 않으면서 문제 해결 할 수 있다.

탐색기 -> 도구 -> 파일 연결 -> PLS 확장자 제거 이외에 Registry 항목에서의 제거는 더욱 간단하다.

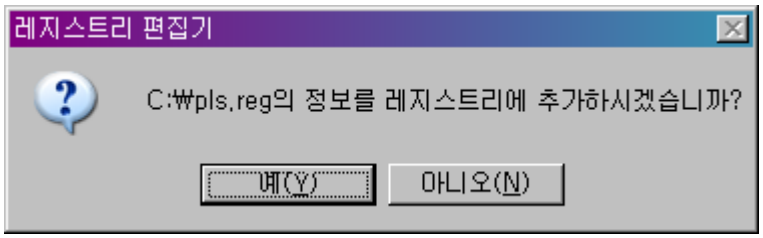
레지스트리 내용

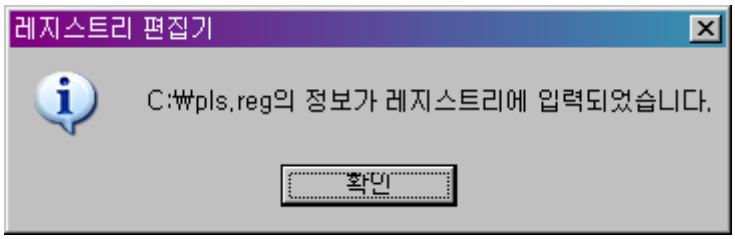
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT₩.pls]

@=""

위의 내용을 pls.reg로 저장한 후 실행 하기만 하면 된다.





원래 레지스트리 파일의 내용

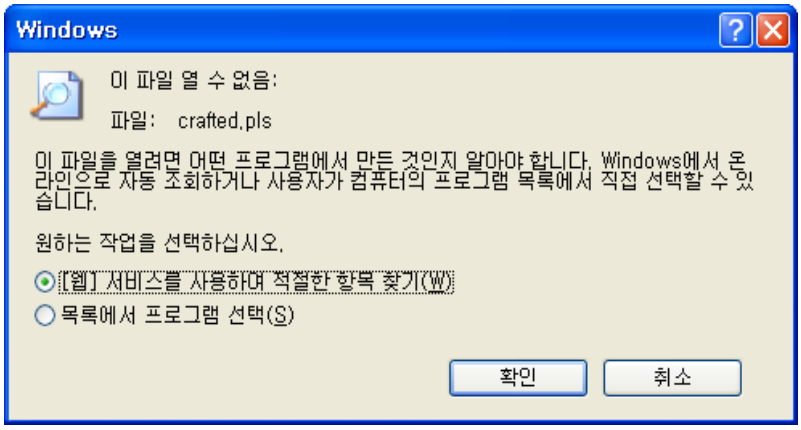
[HKEY_CLASSES_ROOT₩.pls]

@="Winamp.PlayList"

"Content Type"="audio/scpls"

"Winamp_Back"=""

레지스트리의 갱신 이후에는 확장자와 연결된 프로그램 항목이 없으므로 pls 파일이 다운로드 된다 하여도 실행이 되지 않는다. 다만 아래와 같이 다운로드만 확인이 되고 파일의 오픈도 되지 않는다. Winamp가 있다고 하여도 pls 확장자는 오픈 되지 않는다.



4. 결론

사용자 단위에 영향을 미칠 수 있으므로 간단하고 급하게 작성을 하였다. PLS 확장자를 사용하지 못한다는 것은 사용자가 작성하는 playlist 항목을 이용하지 못한다는 것과 동일한 결과를 가져 올 수 있다. 따라서 Winamp 이용 시에 .pls 파일을 읽지 못해 작성해 놓은 .pls 파일을 이용하지 못할 수 있는 부수적인 문제가 있다. 그러나 큰 문제를 해결 하기 위해서는 다음과 같은 간단한 해결책으로 문제를 해결 할 수 있다.

Winamp application의 업데이트
http://www.winamp.com/player/
또는 pls.reg 파일의 실행 (아래의 내용을 copy 하여 pls.reg로 저장 후 더블클릭만 하면 됨)

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT₩.pls]
@=""
```