UCC서비스 현황과 향후 보안위협

2007. 4. 3

인터넷침해사고대응지원센터 (KISC)

한국정보보호진흥원
Korea Information Security Agency

□ 개 요

인터넷 인프라 환경이 발전하고, 디지털 방식을 이용하는 카메라, 캠코더 등의 사용이 일반화 되어 감에 따라, 사용자들이 직접 동영상, 사진 등을 제작하여 인터넷에 공유하는 경우가 많아지고 있다. 이러한 사용자들이 제작한 Contents (UCC)를 서비스 형태로 제공하는 사이트도 매년 늘고 있으며, 향후에 더욱 증가할 것으로 예상된다.

인터넷을 통하여 타인이 제작한 동영상, 사진 등의 Contents들을 쉽고 빠르게 공유할 수 있는 것은 사용자들에게 큰 편리함과 만족감을 제공해 주지만, 누구나 Contents를 제작하여 많은 사용자들에게 공유할 수 있다는 점을 악용할 경우 UCC가 악성코드 전파 및 해킹을 위한 효과적인 수단으로 이용될 수 있다. 공격자는 사용자들이 많은 관심을 가지고 있는 Contens를 제작, 악성코드를 삽입하여 UCC 사이트에 공유하는 방식으로 해킹을 시도할 것으로 보인다. UCC에 의한 해킹피해 발생을 사전에 예방하기 위하여 OS 및 웹 브라우져와 사용하고 있는 미디어 플레이어들을 최신으로 패치하고, 신뢰할 수 없는 파일은 설치하거나 열어보지 말도록 하며, 백신제품을 설치 및 실시간 감시를 활성화 하도록 한다.

□ UCC 소개 및 현황

o UCC (User Created Content)란?

사용자가 금전적인 이익을 목적으로 하지 않고 제작한 Contents를 의미하며, 디지털 카메라 등 정보통신 분야가 발전함에 따라 일반인의 빠른 정보 생산이 가능해 지면서 최근 급격히 확산되고 있다

o UCC 서비스 현황

UCC는 초기에는 단순히 보고 즐기는 글과 사진 위주의 엔터테인먼트 Contents 형태였다가, 동영상 위주의 Contents로 발전하고 있으며, UCC 서비스 형태로 운영되는 포탈 사이트도 매년 늘어나고 있다.

<사용자가 제작한 동영상 공유사이트 예 "YouTube">

□ UCC와 보안위협

o UCC의 위험성

- 사용자가 제작하는 Contents들이 인터넷을 통하여 다수의 이용자들에게 신속히 공유가 될 수 있다는 점은 큰 편리성을 제공하지만, 한편으로는 해킹을 위하여 제작된 공격코드가 삽입되어 있는 Contents 들이 매우 쉽게 다수의 사용자에게 배포될 수 있다는 위험요소를 안고 있다.
- 또한, UCC는 포털사이트, 커뮤니티 사이트 등 인터넷 서비스 제공자가 책임을 지고 만드는 콘텐츠가 아니며, 누구라도 제작하여 배포할 수 있어 해킹에 악용될 소지가 크다.
- 사진, 동영상 등 UCC에서 이용되는 모든 Contents 들은 악의적인 해커에 의하여 악용될 가능성이 있으며, 이러한 경우 UCC가 악성코드 전파를 위한 매개체 역할을 하게 된다.

※ 참고: UCC를 이용한 해킹피해 사례

. 실제로 악의적인 URL이 삽입되어 있는 동영상이 Myspace, YouTube 등을 통하여 유포되는 피해가 발생함. 또한, 동영상을 볼 수 있도록 하는 코덱 프로그램 설치를 유도하여 스파이웨어를 설치하는 피해사례도 보고됨.

o 예상되는 UCC 해킹공격 유형

UCC를 통하여 발생할 수 있는 공격 및 피해유형은 여러 가지가 있을 수 있으나 대표적으로 예상되는 예를 살펴보면 다음과 같다.

▸ 공격경로

UCC에 해당되는 모든 Contents 유형은 공격에 악용될 위험성이 있으나, 대표적으로 UCC로 많이 공유되고 있는 동영상과 이미지, 플래쉬 파일등이 주요한 공격경로로 악용될 것으로 보인다.

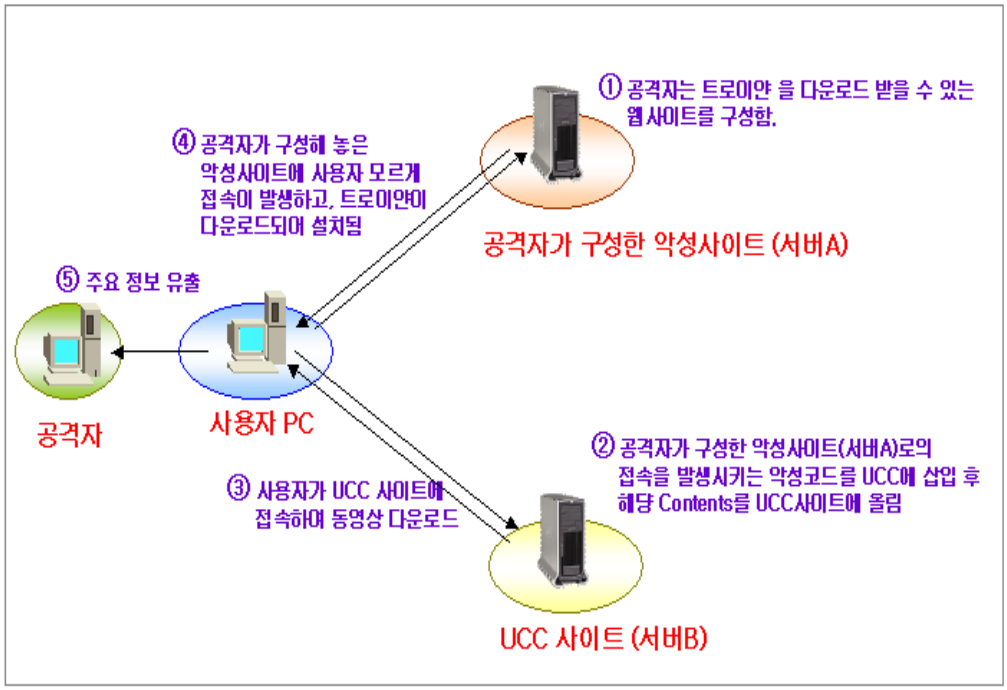
<공격 경로>

* 악성 동영상 파일을 통한 사용자 PC 공격
* 악성 이미지 파일을 통한 사용자 PC 공격
* 악성 플래쉬 파일을 통한 사용자 PC 공격
* 악성 음악/음성 파일을 통한 사용자 PC 공격

▸ 공격 형태 및 기법 예상

트로이얀 등의 악성코드를 설치하기 위한 악성 사이트를 구성해 놓은 후에, UCC를 통하여 해당 사이트로 접속을 유도하는 형태의 공격이 많을 것으로 예상된다. (사용자가 UCC를 봄과 동시에 사용자 모르게 악성사이트로 접속이 발생하여 트로이얀 등의 코드가 설치. 설치 후에는 정보 유출)

대표적인 공격유형 예를 살펴보면 다음과 같다.



① 공격자는 트로이얀 등을 다운로드 받을 수 있는 웹사이트를 구성.
(트로이얀 다운로드 및 설치를 위한 코드를 올려놓음.)

② 동영상,이미지,플래쉬를 제작.
해당 UCC에는 공격자가 구성한 악성사이트 [서버A]로 사용자 모르게 접속을 발생 시키는 악성코드를 삽입함. 완성된 악성Contents를 UCC 공유사이트에 올림.

③④ 일반사용자가 악의적인 스크립트가 삽입되어 있는 동영상을 다운로드하여 열어볼 경우 공격자가 구성해 놓은 악성사이트 (서버A)에 접속이 발생하게 되며, 해당 서버로부터 트로이얀 등의 악성코드가 다운로드 및 설치되게 됨.

⑤ 악성코드 감염에 의하여, 사용자PC의 중요정보가 공격자에게로 유출됨.

공격자는 공격을 수행하기 위하여 동영상 URL스크립트 삽입기능, 플레이어 취약점, Codec을 가장한 악성코드 유포, 플래쉬의 액션스크립트 기능, 이미지 렌더링 취약점 등을 악용할 가능성이 높다.

<공격 기법 예>

* 동영상에 URL 스크립트 삽입
* 동영상 플레이어 취약점등 악용
* 이미지 렌더링 취약점 등 악용
* Codec 등을 가장한 악성코드 유포
* 플래쉬 액션스크립트 기능 악용

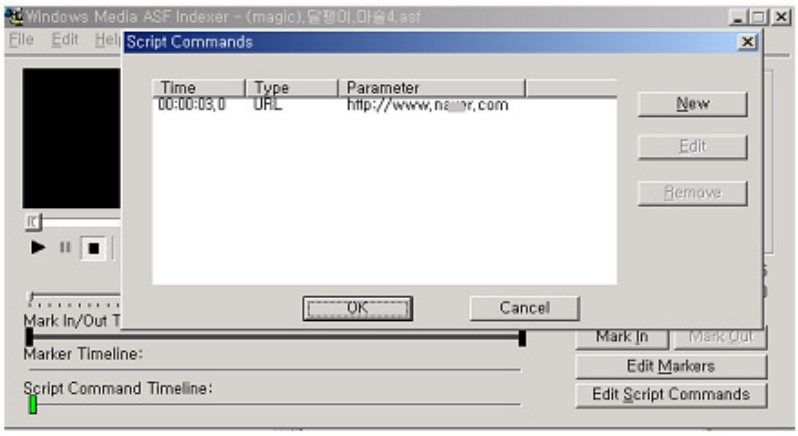
【공격 기법 별 상세】

☞ 동영상에 URL스크립트를 삽입하는 기법

공격자는, 악성사이트(트로이얀 다운로드 사이트)로의 접속을 유도하기 위하여 동영상에 URL스크립트를 삽입할 수 있다.

➡ Windows Media Player ASF 파일에 URL 삽입하는 예

Media 도구를 이용하여 동영상에 URL스크립트를 삽입하는 경우의 예이다. 아래와 같은 조작을 통하여 동영상이 시작 된 후, 사용자가 정의한 시간에 사용자가 정의한 특정사이트로의 접속을 발생시킬 수 있다.

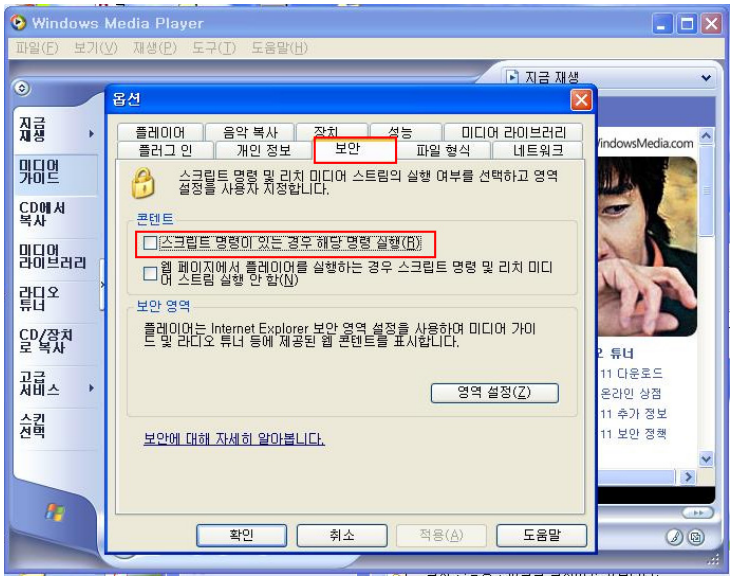


※참고: 최근의 Windows Media Player 버전에서는 아래와 같이 보안옵션을 통하여 URL 스크립트 기능을 사용하지 않을 수 있도록 선택메뉴를 제공함 (기본설정 값은 OFF 임).

아래와 같은 URL 스크립트 비활성화 메뉴가 없을 경우, Windows

Media Player에 대한 패치(KB828026)를 실시하여 피해를 예방해야 함.

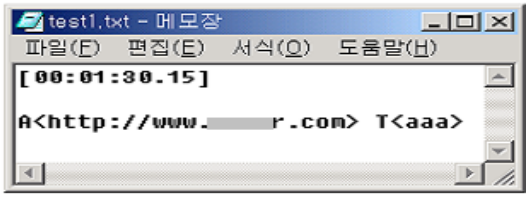
< URL스크립트 비활성 메뉴 예 ["도구" → "보안"] >



➡ QuickTime MOV 파일에 URL스크립트를 삽입하는 예

QuickTime은 컴퓨터에서 디지털미디어를 재생할 수 있는 Apple사의 소프트웨어이다. QuickTime의 HREF Track 기능을 이용하면 동영상에 URL을 삽입할 수 있다.

i) 특정사이트 접속을 위한 스크립트 작성



ii) 동영상에 URL 스크립트를 삽입

※참고: 최신버전으로 업데이트를 할 경우 피해예방이 가능

☞ 미디어 플레이어, 이미치 처리 취약점등을 공격에 악용

동영상 플레이어, 이미지처리엔진 등에 취약점이 존재할 경우, 해당 취약점을 공격에 악용할 수 있다. 공격에 이용될 수 있는 취약점을 살펴보면 다음과 같다.

<Microsoft Windows Media Palyer 취약점/ MS 이미지처리 취약점 예>

패치 번호	내 용
[MS06-078]	Windows Media Format 원격코드 실행 취약점
[MS06-026]	WMF 그래픽 렌더링 처리문제로 인한 원격 코드 실행 취약점
[MS06-024]	Windows Media Player의 비트맵 파일을 처리 취약점
[MS06-022]	ART 이미지 렌더링 취약점
[MS06-006]	Windows Media Player 플러그인의 취약점으로인한 원격 코드 실행 문제점
[MS06-005]	Windows Media Player의 원격 코드 실행 취약점
[MS06-001]	WMF 그래픽 렌더링 처리문제로 인한 원격 코드 실행 취약점
[MS05-009]	Windows Media Player 원격 PNG 이미지 포맷 버퍼 오버플러우 취약점

<QuickTime 취약점 예>

번 호	내 용
CVE-ID: CVE-2007-0711	▣ 취약대상 제품: Windows Vista/XP/2000 ▣ 취약 내용: 나쁜 의도로 제작된 3GP 파일을 보는 경우 애플리케이션이 작동을 멈추거나 임의의 코드가 실행될 수 있음. QuickTime에서 3GP 비디오파일을 사용하는 중 인티저 오버플로우가 발생함. 사용자에게 악성비디오를 보내 사용자가 파일을 열 경우 오버플로우를 야기함으로서 애플리케이션의 중단과 임의코드 실행을 유발함.
CVE-ID: CVE-2007-0712	▣ 취약대상 제품: Mac OS X v10.3.9 상위 버젼, Windows Vista/XP/2000 ▣ 취약 내용: 나쁜 의도로 제작된 MIDI 파일을 보는 경우 애플리케이션이 작동을 멈추거나 임의의 코드가 실행될 수 있음. QuickTime에서 MIDI 파일을 사용하는 중 버퍼 오버플로우가 발생함. 사용자에게 악성 MIDI 파일을 보내 사용자가 파일을 열 경우 오버플로우를 야기함으로서 애플리케이션의 중단과 임의 코드 실행을 유발함.
CVE-ID: CVE-2007-0713	▣ 취약대상 제품: Mac OS X v10.3.9 상위 버젼, Windows Vista/XP/2000 ▣ 취약 내용: 나쁜 의도로 제작된 Quicktime 파일을 보는 경우 애플리케이션이 작동을 멈추거나 임의의 코드가 실행될 수 있음 QuickTime에서 QuickTime 파일을 사용하는 중 버퍼 오버플로우가 발생합니다. 사용자에게 악성 비디오 파일을 보내 사용자가 파일을 액세스 할 경우 오버플로우를 야기함으로서 애플리케이션의 중단과 임의 코드 실행을 유발함.
CVE-ID:	▣ 취약대상 제품:

CVE-2007-0714	Mac OS X v10.3.9 and later, Windows Vista/XP/2000 ▣ 취약 내용: 나쁜 의도로 제작된 Quicktime 파일을 보는 경우 애플리케이션이 작동을 멈추거나 임의의 코드가 실행될 수 있음. QuickTime에서 비디오 파일의 UDTA 사용 중 인티저 오버플로우가 발생함. 사용자에게 악성 비디오 파일을 보내 사용자가 파일을 액세스 할 경우 오버플로우를 야기함으로서 애플리케이션의 중단과 임의코드 실행을 유발함

<기 타>

소프트웨어 명	내 용
곰플레이어	스택오버플로우로 인한 원격코드실행 취약점. 비정상적인 URI 를 포함하는 ASX 파일처리 시 발생 ※ 취약점 해결을 위하여 2.1.1버전으로 업데이트 필요.
WinAmp	버퍼 오버플로우 취약점 ※ 취약점 해결을 위하여 Winamp 5.3.1 버전으로 업데이트 필요.

☞ Codec등을 가장한 악성코드 유포

동영상을 보려는 사용자에게 위장된 Codec 프로그램을 설치하도록 유도하는 방식. 해당 Codec은 악성코드 이거나, 악성코드가 삽입되어 있어, 해당 프로그램 설치 시 사용자가 감염되는 유형이다.

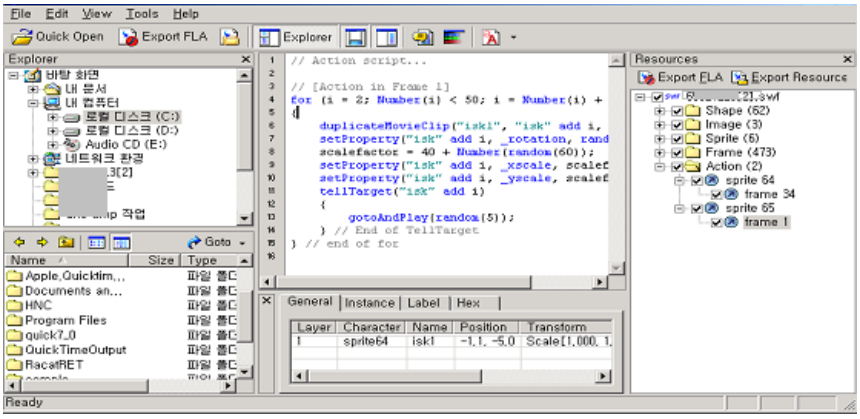
☞ 악성 플래쉬 파일을 이용한 공격 기법

프래쉬는 GIF 기반 애니메이션의 한계점을 극복하기 위하여 만들어진 에니메이션 저작도구 및 플레이어로써, 사운드 추가, 강력한 프로그램 환경인 액션 스크립트 기능추가 등 계속적으로 기능이 개선되어가고 있다. 플래쉬로 제작된 파일은 용량이 작고 웹 브라우져에서 이용이 가능하며, 기타 다양한 잇점으로 인하여 사용자가 크게 증가 및 웹 Contents 제작에 반드시 필요한 도구가 되었다. 플래쉬에는 액션 스크립트라고 하는 강력한 프로그램 밍 기능이 있는데, 이러한 기능은 공격자에 의하여 악용될 소지가 있다.

공격자는 플래시 제작 시에 악성코드를 설치하기 위한 악성사이트의 URL을 액션 스크립트 내에 삽입하므로써, 플래쉬 실행 시 사용자 모르게 악성코드 설치를 위한 사이트로 접속하게 할 수 있다. 또한, 이미 제작되어진 플래쉬 파일을 역 컴파일하여

악성사이트로 접속이 발생하도록 변조하는 것도 가능하다.

<일반 플래쉬 파일 액션 스크립트어의 역 컴파일 예시>



□ 사고예방을 위한 방안

현재, 미디어 소프트웨어들의 패치적용 필요성에 대한 일반인들의 인식은 매우 낮다. UCC로 인한 해킹피해를 사전예방하기 위해서는 미디어 소프트웨어들에 대한 최신패치를 적용하는 것이 중요하므로, 반드시 현재의 패치현황을 점검하고, 필요할 경우 신속히 업데이트 하도록 한다.

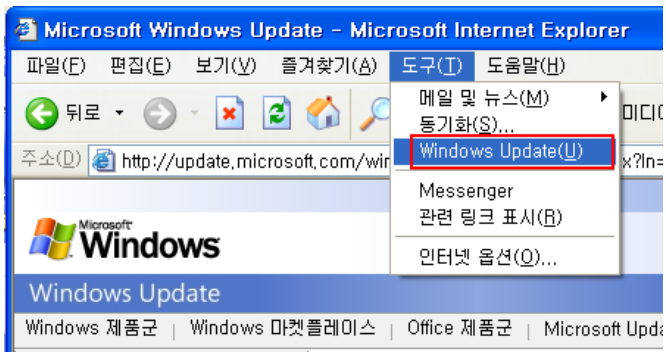
또한, 악성코드가 코덱 등의 프로그램으로 위장되어 배포될 수 있으므로, 신뢰할 수 없는 프로그램은 가능한 설치하지 않도록 한다.

사용자는 PC에 백신제품을 설치하고, 최신으로 패턴을 업데이트 하며, 실시간 감시기능이 활성화되어 있는지 점검할 필요가 있다.

- ▸ 미디어소프트 웨어에 대한 패치현황 점검 및 최신버전으로 업데이트
- ▸ OS 최신 패치 적용
- ▸ 백신 설치 및 최신 패턴으로 업데이트. 실시간 감시 기능 활성화
- ▸ 신뢰할 수 없는 프로그램은 설치하거나 열어보지 말기

※ Quicktime 취약점 업데이트 예
"시작" 클릭 → "모든 프로그램" 클릭 → "Apple Software Update" 실행

※ Windows OS 및 Windows Media Player 취약점 업데이트 예
"시작" 클릭 → "모든 프로그램" 클릭 → "Internet Explorer" 실행
→ "도구 (상단)" 클릭 → "Windows Update" 클릭



□ 결 론

UCC를 이용한 악성코드 감염 및 해킹피해 발생 위험성은 최근 UCC의 이용 확산과 비례하여 높아지고 있으므로 주의와 관심이 필요하다. UCC는 동영상 및 이미지, 프래쉬 파일 외에도 그 범위가 매우 넓으며, 이러한 모든 유형의 Contents가 공격에 악용될 소지가 있다. 최근 인터넷에는 신뢰할 수 없는 수많은 미디어 파일들이 넘쳐나고 있으며, 대부분의 이용자들이 아무런 주의없이 미디어 파일을 접하고 있으므로 위험성은 더 커질 수 있을 것으로 보인다.

향후에, Third-Party 미디어 관련 도구를 공격하는 사례도 증가할 것으로 예상되므로, 이러한 소프트웨어에 대한 패치관리에도 관심이 필요하다.

사용자PC가 일단 악성코드에 감염되게 되면 PC내의 모든 중요한 정보가 공격자에게 유출될 수 있으므로, OS 및 미디어 도구에 대한 패치실시, 백신설치 등을 통하여 UCC로 인한 피해발생을 사전 예방할 필요가 있다.