온라인 광고배너를 통한 악성코드 유포대응 보안 가이드

2016. 10

미래창조과학부

KISA 한국인터넷진흥원

목 차

제1장 개요 ····· 1

1.1 배경 ····· 2

1.2 가이드 목적 및 구성 ····· 3

제2장 보안 위협 ····· 4

2.1 온라인 광고 구조 ····· 5

2.2 온라인 광고를 악용한 악성코드 유포 ····· 8

제3장 온라인 광고배너 악성코드 유포대응 방안 ····· 11

3.1 미디어렙사 및 매체사 ····· 12

3.2 이용자 ····· 17

제 1 장
개 요

제1장 개요

1.1 배경

멀버타이징(Malvertising)은 악성 소프트웨어를 뜻하는 멀웨어(Malware)와 광고(Advertising)의 합성어로 온라인 광고[1]를 통해 악성코드를 유포시키는 행위를 말한다. 멀버타이징 기법은 공격자 측면에서 악성코드를 대량 유포하는데 두 가지 장점이 존재한다. 첫째, 정상적인 온라인 광고 네트워크나 웹사이트에 악성코드 유포 광고를 삽입하는데, 온라인 광고는 방문자의 관심을 주목할 만한 주제나 방문자가 많은 사이트에 게시되기 때문에 악성코드 유포를 위한 최적의 환경 조건을 제공한다. 둘째, 온라인 광고는 수많은 정상적으로 운영 중인 웹사이트와 서로 연동되기 때문에 공격자가 각각의 웹사이트를 직접적으로 해킹하지 않아도 악성코드를 손쉽게 대량 유포할 수 있다.

최근 멀버타이징 기법을 이용한 악성코드 유포 공격이 이슈화되고 있다. 그 이유는 온라인 광고 배너를 운영하는 광고 서버가 보안에 취약한 상태로 노출되어 운영되고 있는 것이 가장 큰 원인이다. 온라인 광고 서버는 미디어렙사 및 매체사에서 운영하고 있고, 보안 투자가 어려운 영세 · 소규모 기업의 경우 공격자의 타겟이 될 수 있다. 만약 단 한 곳의 광고 서버가 해킹되면 광고계약을 맺은 다수의 웹사이트에서 동시 다발적으로 악성코드 유포가 가능해지기 때문에 대규모 침해사고 피해가 발생할 수 있다.

1) 온라인 광고 : 광고주가 자신 또는 재화 등에 관한 사항을 정보통신망을 통하여 이용자, 그 밖의 다른 사람에게 널리 알리거나 제시하는 행위 또는 그 정보를 말함

이에 본 가이드에서는 온라인 광고 서버를 통해 발생하는 침해사고 위협사례를 다루어 그 위험성을 인지하도록 하고, 온라인 광고 서버 운영시 반영하여야 할 사항을 제공하여 사고예방 및 피해를 최소화 하고자 한다.

1.2 가이드 목적 및 구성

목적	온라인 광고배너를 악용하는 멀버타이징 공격기법의 심각성 인지를 통한 보안 인식제고 및 침해사고 예방
대상	미디어렙사, 매체사, 일반 이용자
범위	온라인 광고배너를 통한 악성코드 감염 예방을 위해 지켜야 할 사항
구성	[1장] 개요 1.1 배경 1.2 가이드 목적 및 구성 [2장] 보안 위협 2.1 온라인 광고 구조 2.2 온라인 광고를 악용한 악성코드 유포 [3장] 온라인 광고배너 악성코드 유포대응 방안 3.1 미디어렙사 및 매체사 3.2 이용자

제 2 장
보안 위협

제2장 보안 위협

2.1 온라인 광고 구조

온라인 광고는 다뤄야할 데이터가 많고 광고주의 요구사항 등 데이터의 수정이 빈번하므로 수동 관리에 어려움이 발생한다. 따라서 보다 쉽게 광고를 등록, 관리하고 송출하기 위해 광고 서버(AD Server)를 사용한다. 또한, 광고 상품을 노출 영역별로 일일이 서버와 연동하는 번거로운 작업 부하를 줄이기 위해 광고 네트워크(AD Network) 서비스를 사용한다. 광고 네트워크를 이용하게 되면, 광고주는 다양한 매체에 광고하는 것이 편리해지고 효율적인 거래가 이루어지게 된다.

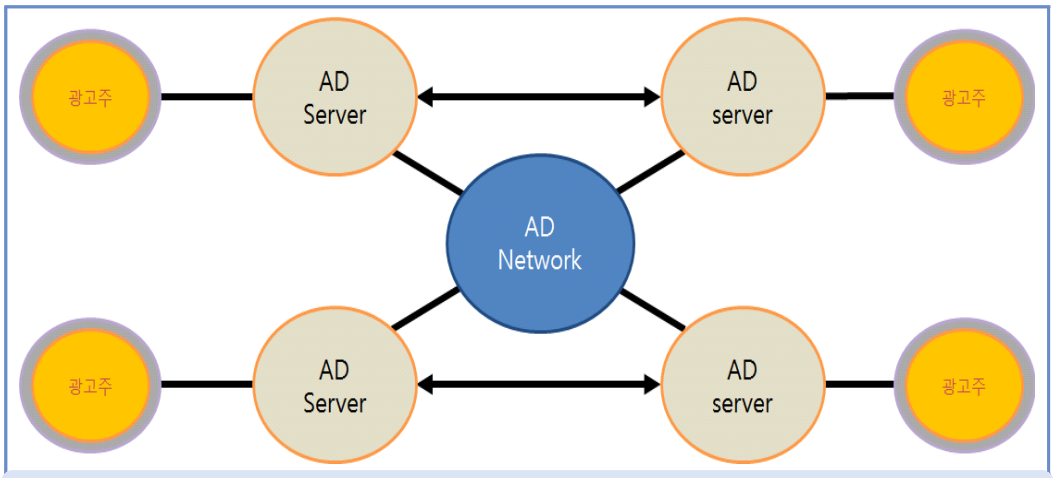

그림 2-1 광고 서버 및 광고 네트워크 연동

광고 네트워크로 인해 광고의 송출은 편리해졌으나, 항상 고정적인 트래픽을 보유하는 것이 아니기 때문에, 사회적인 이슈로 매체의 트래픽이 증가하게 되면 매체에 고정적으로 광고금액을 집행하던 광고를 제외하고는 증가된 트래픽에 대해서는 추가

이익을 볼 수 없게 된다. 따라서, 다양한 각각의 광고 네트워크들을 서로 제휴하여 해당 문제점을 상호 보완하기 위한 광고 익스체인지(AD Exchange)라는 플랫폼을 사용한다. 광고 익스체인지는 양사 간의 유연한 거래를 위해 제휴된 곳의 자원들을 파악하게 되며, 이로 인해 매체사의 여유 자원을 통해 광고주들의 광고를 추가 집행하여 광고의 거래를 가능하게 한다.

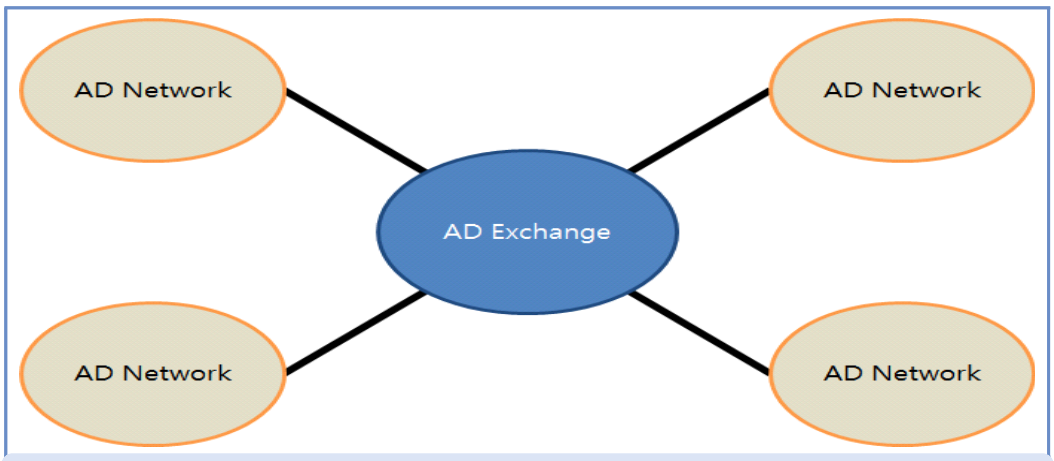

그림 2-2 광고 네트워크 및 광고 익스체인지 연동

온라인 광고의 주요 구성은 광고주, 광고 대행사, 미디어렙사, 매체사, 이용자로 구분할 수 있다.

표 2-1 주요 온라인 광고 구성

구 분	설 명
광고주	매체사를 통한 온라인 광고 요청
광고 대행사	광고주가 요청한 온라인 광고 제작
미디어렙사	매체사로부터 광고 권한을 구입해 온라인 광고 게시
매체사	온라인 광고를 게시할 수 있는 대형 포털, 커뮤니티 등
이용자	웹사이트를 통한 온라인 광고 이용

온라인 광고가 제공되는 형태는 크게 두 가지이다. 첫째, 미디어렙사가 매체사의 온라인 광고 권한을 매입하고 광고대행사가 요청한 광고를 홍보한다. 둘째, 매체사가 직접 광고 대행사가 요청한 광고를 홍보한다. 미디어렙사는 광고 기회 및 효율이 높은 광고 상품을 팔기 위해서 다양한 매체사의 온라인 광고 권한을 갖고 있다. 이러한 구조를 통해 광고주는 하나의 미디어렙사만 계약하면 다양한 매체사에 상품을 광고할 수 있다.

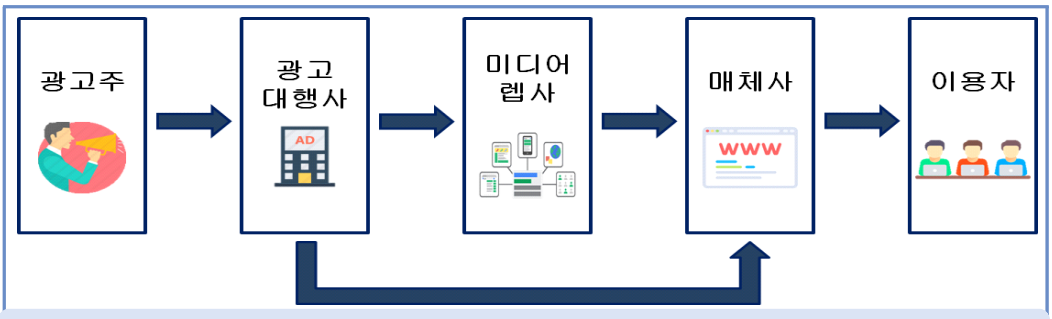

그림 2-3 온라인 광고 제공형태

미디어렙사가 매체사의 광고 권한을 매입할 경우 매체사 웹사이트 특정 부분에 광고 스크립트를 삽입할 수 있는 권한을 얻게 된다. 미디어렙사는 광고 대행사가 요청한 광고 콘텐츠를 매체사 웹사이트에 광고 스크립트로 삽입하고 온라인 광고가 이용자에게 게시된다. 미디어렙사는 광고 효과를 높이기 위해 다양한 매체에 접속한 이용자의 쿠키정보를 기반으로 적합한 광고를 실시간으로 변경하면서 게시한다. 이때, 온라인 광고 서버는 이용자에 적합한 광고 판단, 매체사 웹사이트의 광고 스크립트 실시간 변경, 광고 효과 분석, 광고 비용 측정 등 온라인 광고의 전반적인 역할을 수행한다.

공격자는 악성코드 유포를 위해서 온라인 광고 서버를 해킹해 정상적인 광고에 악성코드 유포 링크를 삽입하거나, 악성코드를 유포하는 위장 광고 사이트를 정상적인 절차에 따라 온라인 광고에 등록하는 방법을 사용한다. 공격이 성공할 경우 불특정 다수를 대상으로 악성코드가 유포되는 막대한 침해사고 피해가 발생하기 때문에 온라인 광고 서버와 온라인 광고 콘텐츠의 보안 조치에 각별한 주의를 기울여야 한다.

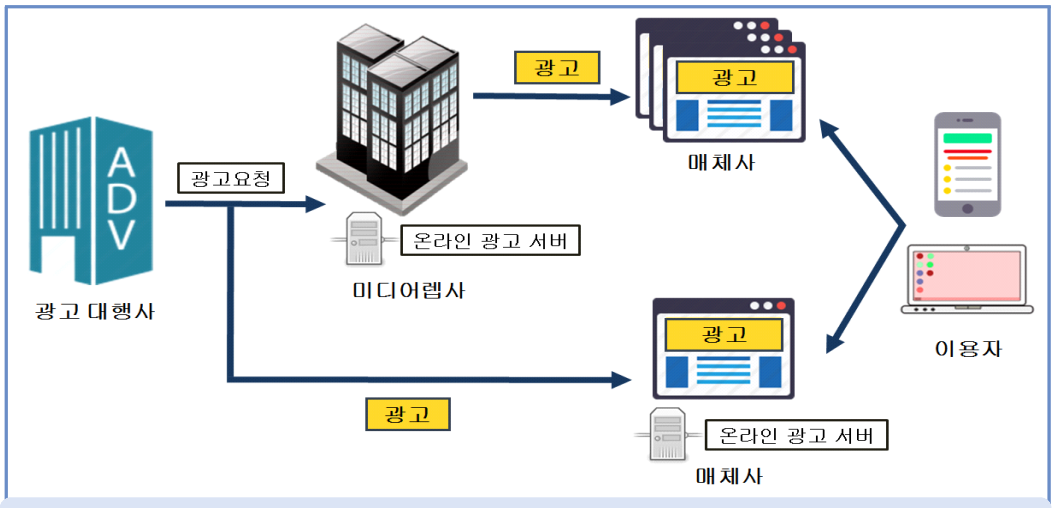

그림 2-4 온라인 광고 등록 개요도

2.2 온라인 광고를 악용한 악성코드 유포

멀버타이징은 온라인 광고 시스템의 특성을 악용해 불특정 다수에게 악성코드를 유포하는 공격기법을 말한다. 올해 해외의 경우 뉴욕타임즈, BBC 등 뉴스 웹사이트의 광고를 통한 악성코드 유포가 있었고, 국내의 경우 대형 커뮤니티 사이트의 광고배너를 통한 악성코드 유포 사례가 있었다.

멀버타이징을 통한 악성코드 유포 방법은 온라인 광고 서버 해킹과 애드웨어[2]를 이용한 두 가지 방법이 있다. 첫째, 온라인 광고 서버 해킹방법은 다음과 같다. 우선 공격자는 보안이 취약한 온라인 광고 서버를 해킹하여 매체를 통해 전송되는 온라인 광고에 악성코드를 삽입한다. 다음으로 운영체제와 응용 프로그램(웹브라우저, 플래시 플레이어, 자바 등)의 보안 조치가 취약한 PC 이용자가 매체에 접속할 경우 악성코드에 자동으로 감염된다. 악성코드가 삽입된 온라인 광고는 다수의 매체를 통해 동시 다발적으로 유포되기 때문에 침해사고 피해가 기하급수적으로 증가하게 된다.

그림 2-5 광고 서버 해킹을 통한 악성코드 유포

둘째, 애드웨어를 이용한 악성코드 유포 방법은 다음과 같다. 우선 공격자는 악성코드 유포지 링크가 삽입된 위장 광고 사이트를 정상적인 절차를 통해 온라인 광고 업체에 등록하고, 온라인 광고 업체는 위장 광고를 온라인에 게시한다. SW 다운로드 사이트는 애드웨어를 이용자에게 배포하고 애드웨어를 통해 이용자는 위장 광고 사이트에 접속 후 악성코드에 감염된다.

2) 애드웨어(Adware) : 특정 소프트웨어를 실행할 때 또는 설치 후 자동적으로 광고가 표시되는 프로그램

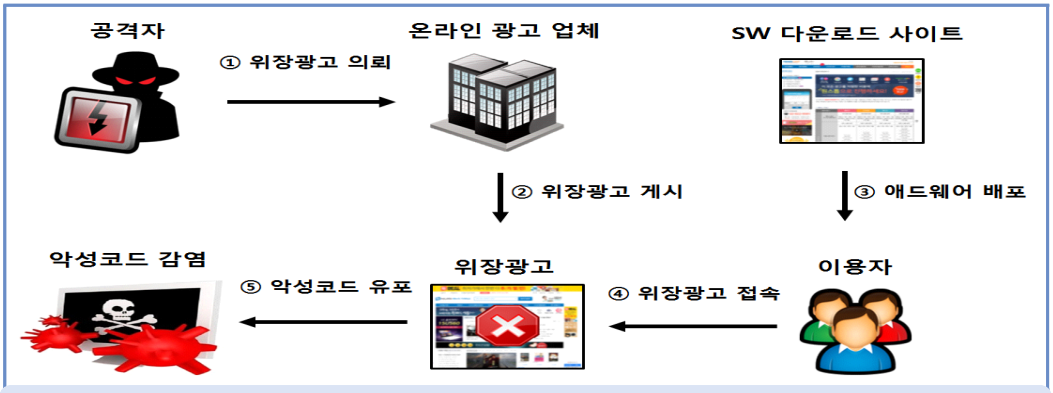

그림 2-6 위장 광고를 통한 악성코드 유포

공격자가 삽입하는 악성링크는 아이프레임(iframe)[3] 태그 등을 사용하여 이용자의 눈에는 보이지 않는 크기의 악성링크를 삽입하거나, 난독화된 주소(URL)를 사용해 위장 광고 사이트로 접속시키기 때문에 온라인 광고의 링크를 추적해 악성행위 여부를 검사해야 한다.

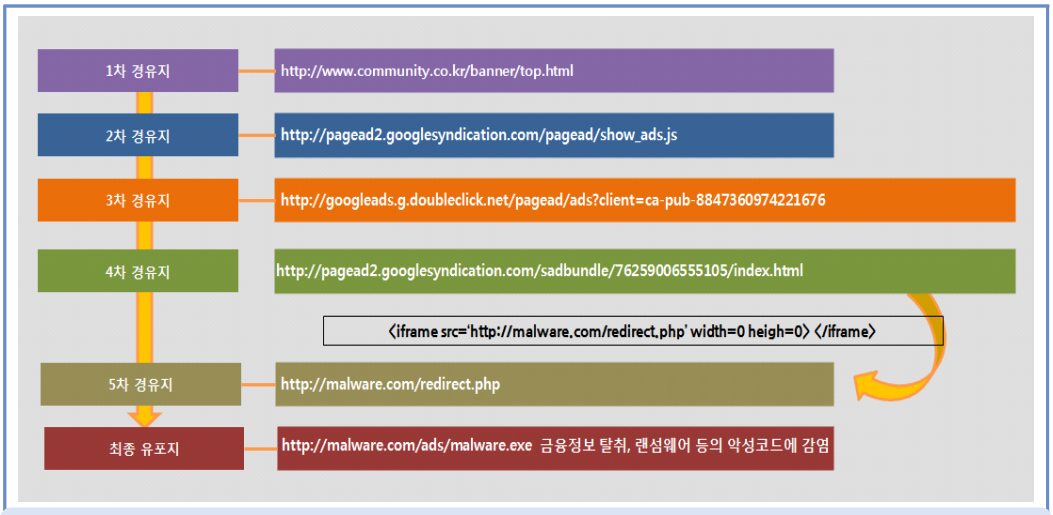

그림 2-7 악성 스크립트 삽입 구조

3) 아이프레임(iframe) : 웹문서 중간에 다른 웹문서나 텍스트 파일과 같은 내용을 원하는 크기로 불러들여 보여주는 태그

제 3 장
온라인 광고배너 악성코드 유포대응 방안

제3장 온라인 광고배너 악성코드 유포대응 방안

3.1 미디어렙사 및 매체사

공격자의 멀버타이징 기법으로부터 안전한 온라인 광고를 제공하기 위해 온라인 광고 서버 운영 시 적절한 보안 조치가 필요하다. 보안 관리 영역은 크게 온라인 광고 신규 계약 점검, 광고 서버의 기술적 점검 및 관리적 점검 영역으로 나누었다.

관련된 점검 사항은 다음과 같다.

【 온라인 광고 신규 계약 점검 】

❍ 광고 의뢰주의 신뢰성 평가

공격자는 온라인 광고 서버를 직접 해킹하는 방법 이외에 악성 링크가 삽입된 위장 광고를 정상적인 방법으로 등록할 수도 있기 때문에 신규 계약 접수를 의뢰하는 광고주의 재무 상태나 업종 등이 신뢰할 수 있는지 평가하여야 한다.

❍ 계약 정보의 허위여부 확인

신규로 생성한 도메인은 신뢰성을 검증할 기간이 짧고, 악성코드를 유포하기 위한 목적으로 생성했을 가능성이 있기 때문에 광고를 요청한 도메인, 이메일 주소 등 계약 정보에 허위 내용이 포함되어 있는지 확인하여야 한다.

【 광고 서버의 기술적 점검 】

❍ 광고 페이지 링크・파일의 악성여부 점검 및 지속 모니터링

광고 링크는 해당 도메인이 정상적으로 등록되어 사용되는지, .swf 파일 등을 포함하여 모든 파일에 대해 악성 여부를 점검하고 지속적으로 모니터링을 수행하여야 한다.

파일이 난독화 되어 있거나 의심스러운 내용이 포함되어 있는지 확인하여 파일이 변조 되었는지 점검하여야 하며, 광고 페이지 내에 아이프레임(iframe) 또는 리다이렉션 페이지에 포함된 주소(URL)가 정상적으로 사용되고 있는지 점검하여야 한다.

❍ 네트워크 보안

침입차단시스템, 침입탐지시스템 등 네트워크의 안전성을 제고할 수 있는 정보보호시스템을 설치·운영하고, 네트워크 모니터링 도구를 이용하여 광고 서버 및 연계되는 시스템에 대해 트래픽을 24시간 모니터링 해야 한다.

ACL(Access Control List) 등의 접근제어 기능을 적용할 수 있는 설비를 사용하고 외부에서는 직접 접속할 수 없도록 네트워크를 구성해야 한다.

❍ 서버 보안

서버에 대한 접속로그, 설정 변경 로그는 최소한 3개월 이상 유지・관리하여야 한다. 인가된 자만 시스템에 접속할 수 있도록 설정하고, 불필요한 프로토콜 및 서비스는 제거하도록 한다.

설정파일 및 주요 데이터는 복호화 되지 않도록 일방향 암호화하여 저장・백업을 해두어야 한다. 주요 보안패치는 시스템에 주기적으로 적용・기록 관리하여야 한다.

❍ 정보보호시스템 보안

이상징후 탐지를 알리는 경고 기능을 설정하여 운영하고, 정보보호시스템 보안기능(비정상 트래픽 차단 등)의 정상 작동 여부를 월 1회 이상 점검하여야 한다.

❍ 취약점 점검 및 조치

광고, 웹 서버 등 운영되고 있는 시스템은 연 1회 이상 취약점 진단을 실시하고, 발견된 취약점은 제거 또는 보완하여 공격자의 침입이 가능한 경로를 미리 차단하는 것이 필요하다.

【 광고 서버의 관리적 점검 】

❍ 시스템 운영・관리

사내 보안정책을 통해 모든 시스템의 운영체제와 자바, 플래시 플레이어 등의 응용 프로그램은 최신 버전의 상태로 유지하고, 백신 프로그램을 설치하여 정기적으로 검사하여야 한다.

퇴사나 인사이동에 따른 담당자의 계정과 권한 설정을 점검・관리하고, 관리자 및 개발자 PC의 비밀번호는 복잡도(2조합 10글자 또는 3조합 8글자) 만족 및 일정주기로 비밀번호를 변경하여야 한다.

❍ 안전한 광고 서버 구축·관리

광고 서버와 연관된 홈페이지를 운영 하고 있다면 근본적으로 홈페이지 개발 시점부터 보안의식 및 시큐어 코딩으로 홈페이지를 구축하고 주기적인 취약점 점검·패치를 적용하여 침해사고가 발생되지 않도록 사전에 방지해야 한다.

❍ 보안 전담부서 구축 및 보안교육 실시

보안 전담 부서 및 담당자를 지정하여 운영 중인 시스템을 점검·관리하고, 사내 내부 직원 대상으로 정보보호 인식제고를 위해 정기적으로 보안교육을 실시하여야 한다.

❍ 침해사고 대응체계 수립

보안정책에 의해 정의된 체계적인 보안 운영지침과 절차를 수립하여 준수하고, 침해사고 발생 시 즉각 대처할 수 있는 비상연락체계를 마련하여야 한다.

❍ 경영진의 사회적 책임성

광고 서버를 운영하는 경영진 또는 보안담당자는 광고 서버가 공격자로부터 해킹을 당해 악성코드가 유포되는 매개체로 악용됨과 동시에 이용자 PC의 악성코드 감염 및 금전적 2차 피해가 발생되지 않도록 사회적 책임을 가지고 사전적인 점검 및 예방 등에 노력을 기울여야 한다.

❍ 웹보안 강화 서비스 이용

한국인터넷진흥원에서는 중소·영세기업 대상으로 해킹예방을 위한 웹보안 강화 서비스(웹취약점 점검[4], 웹보안도구[5])를 제공하고 있으므로 이를 이용하여 침해사고를 예방할 수 있다.

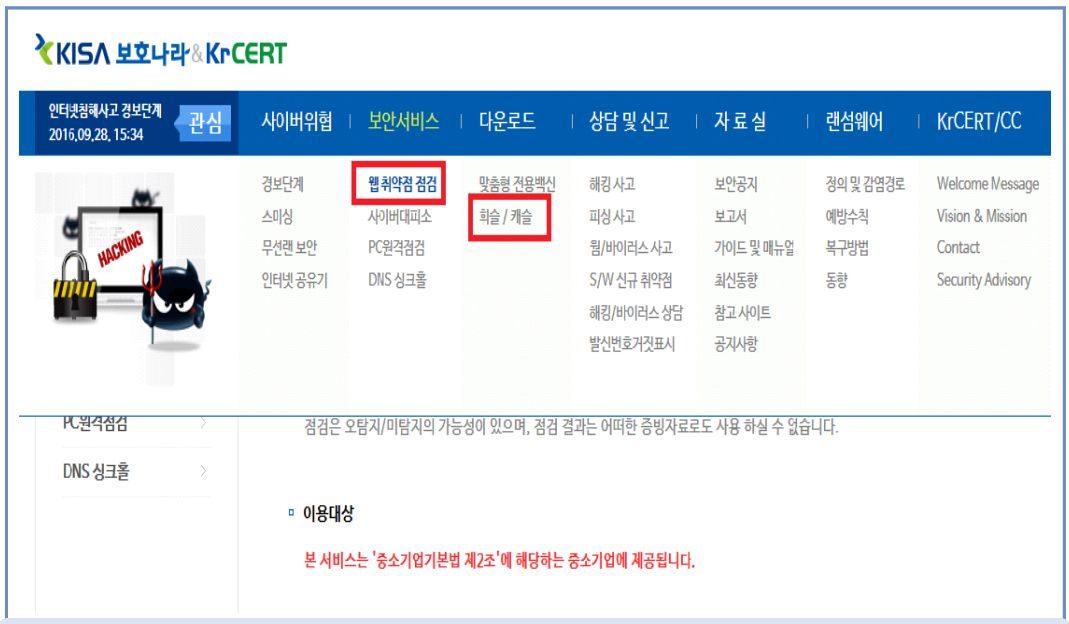

그림 3-1 웹취약점 및 웹보안도구(취슬/캐슬) 신청

4) 웹취약점 점검 : 홈페이지 취약점(개인정보 유출, 설정 오류 등) 원격점검 및 조치안내
5) 웹보안도구 : 웹셸 및 악성코드 탐지를 위한 취슬과 웹 방화벽 프로그램인 캐슬 보급

3.2 이용자

❍ 운영체제와 응용 프로그램의 최신 보안 업데이트 수행

이용자 측면에서 멀버타이징 피해를 예방하기 위해 가장 중요한 부분은 운영체제, 응용 프로그램의 최신 보안 업데이트를 수행하는 것이다. 최신 보안업데이트를 수행 할 경우, 악성코드가 삽입된 광고에 노출되어도 취약점이 존재하지 않아 악성코드에 감염되지 않는다.

이용자는 응용 소프트웨어를 최신으로 유지하기 위해서 주요 백신 제품에 확대 적용된 『SW 원클릭 안심 서비스』이용을 권장한다. 『SW 원클릭 안심 서비스』는 업데이트가 필요한 주요 소프트웨어 대해 안내해주는 서비스로 손쉽게 응용프로그램의 업데이트를 수행 할 수 있다.

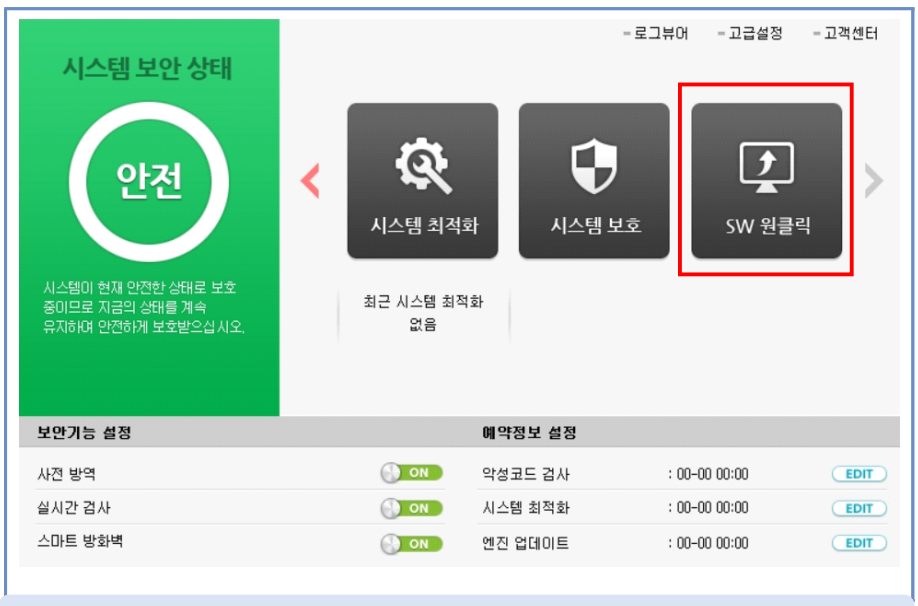

그림 3-2 SW 원클릭 안심 서비스

❍ 백신 프로그램 설치 및 정기적인 점검 실시

온라인 광고를 이용해 유포되는 악성코드로부터 PC를 안전하게 지키기 위해서 주요 보안업체에서 제공하는 백신을 설치해야 한다. 백신의 실시간 검사기능을 통해서 악성코드 감염을 예방할 수 있고 정기적인 검사를 통해서 감염된 PC를 치료할 수 있다.

❍ 파일 다운로드 주의

토렌트, 블로그, 유틸리티 등의 웹사이트에서 파일 다운로드 시 정상 파일을 위장한 악성코드 감염에 주의해야 한다. 공격자는 이용자가 필요로 하는 소프트웨어를 대상으로 악성코드가 포함된 소프트웨어를 배포하려고 하므로 주의가 필요하다.

❍ 온라인 악성 광고차단 기능설정 및 소프트웨어 사용

선택사항으로 필요시 추가적인 방법은 브라우저의 온라인 광고 차단 기능을 사용하는 것이다. 브라우저의 설정 및 광고차단 확장 프로그램을 이용해 온라인 광고를 차단할 수 있다. 인터넷 익스플로러 브라우저의 경우, 【설정 > 인터넷 옵션 > 개인 정보】의 팝업 차단 사용 설정을 통해 온라인 광고를 차단할 수 있다.

크롬 브라우저의 경우, 크롬 웹 스토어에서 제공하는 광고차단 확장 프로그램을 이용해 온라인 광고를 차단할 수 있다.

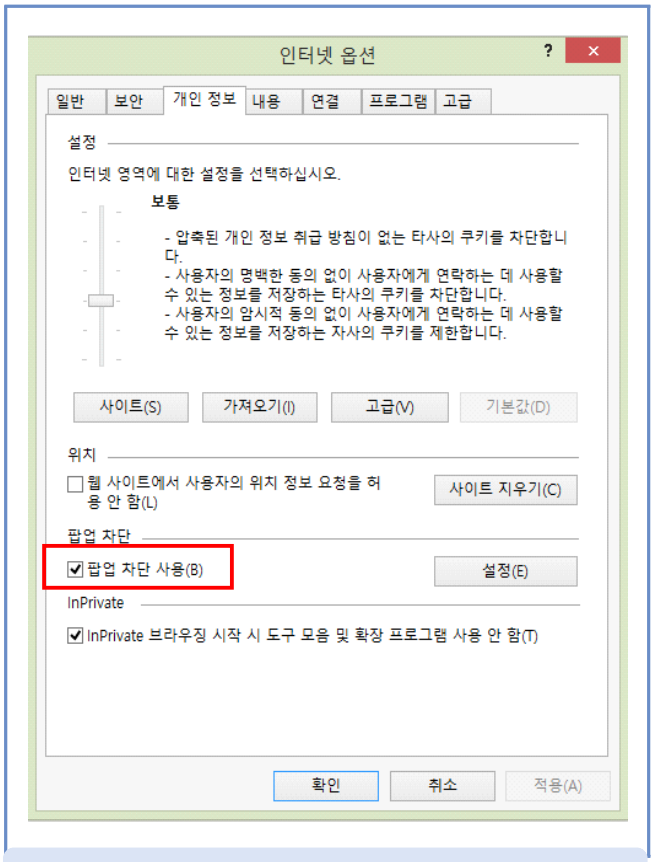

그림 3-3 인터넷 익스플로러 광고차단 설정

그림 3-4 크롬 온라인 광고차단 확장 프로그램

❍ 온라인 악성광고 신고

공격자를 통해 삽입된 악성코드의 피해확산을 최소화하기 위해서 온라인 광고의 악성행위를 확인한 경우, 한국인터넷진흥원 보호나라 & KrCERT 홈페이지(www.boho.or.kr)를 통해 신고 및 기술지원을 받을 수 있다.

그림 3-5 한국인터넷진흥원 해킹사고 신고