PC방 침해사고 예방을 위한 보안 안내서

2016. 11

미래창조과학부

KISA 한국인터넷진흥원

KOREA INTERNET & SECURITY AGENCY

목 차

제 1 장
개 요

제1장 개요

1.1 배경

PC방은 인터넷전용선과 근거리통신망(LAN)으로 연결된 컴퓨터를 설치하고, 게임을 포함하여 교육, 문화, 통신 오락 등 다양한 멀티콘텐츠를 제공하는 업종이다. 또한, 온라인 및 DVD 게임, 정보검색, 사이버증권, 사이버 뱅킹, 온라인 채팅 등 고성능 컴퓨터와 초고속망을 이용한 모든 서비스를 제공한다. '15년 발간된 국세청 통계자료를 기준으로 PC방은 전국 10,644개가 있다.

그러나, PC방은 개방적인 운영환경과 취약한 보안 관리로 인해 사이버 공격의 표적이 되거나 악용되는 사례가 많았다.

'15년 12월에는 전국 약 1천여 개 PC방에서 운영되고 있는 노하드 솔루션의 라이센스 인증 서버를 대상으로 디도스 공격이 발생하여 해당 제품을 사용하는 대부분의 PC방에서 장애가 발생하였으며, PC방 관리에 사용되는 보조 SW를 의도적으로 변조한 후 인터넷 도박 화면 정보를 전송하는 악성코드를 심어 PC방에 제공한 일당이 경찰에 검거된 사례도 있었다. 또한, 기업 APT 해킹 공격으로 탈취된 중요 정보가 해외로 유출되기 전 추적을 회피하기 위한 중간 단계로 PC방 서버가 악용된 사례도 있었다.

이에 본 안내서에서는 PC방과 관련된 침해사고 위협사례를 다루어 그 위험성을 인지하도록 하고, PC방 운영 시 반드시 반영하여야 할 보안 사항을 제공하여 사고예방 및 피해를 최소화 하고자 한다.

1.2 안내서 목적 및 구성

목적	PC방 관련 지속 발생하는 공격의 심각성 인지를 통한 보안 인식제고 및 침해사고 예방
대상	PC방 운영자, 솔루션 및 SW 제공 업체, 인터넷PC문화협회
범위	PC방 관련 침해사고 예방을 위해 지켜야 할 사항
구성	[1장] 개요 1.1 배경 1.2 안내서 목적 및 구성 [2장] 보안 위협 2.1 PC방 소프트웨어 유통 구조 2.2 침해사고 사례 ■ 노하드 솔루션 대상 디도스 공격 사고 ■ PC방 관리 보조SW 변조 사고 ■ 정보 유출 경유지 악용 사고 [3장] 침해사고 예방을 위한 보안 안내 3.1 솔루션 및 SW 제공업체 3.2 PC방 운영자

제 2 장
보안 위협

제2장 보안 위협

2.1 PC방 솔루션 및 소프트웨어 유통 구조

PC방은 운영 솔루션과 관리 프로그램을 통해 서비스를 제공한다. 운영 솔루션의 경우 일반 PC를 이용하는 방식과 중앙 서버에서 운영체제 및 게임SW를 제공하는 노하드 방식으로 구분되며, 전체 PC방 중 약 30% 정도가 노하드 방식을 이용하고 있다.

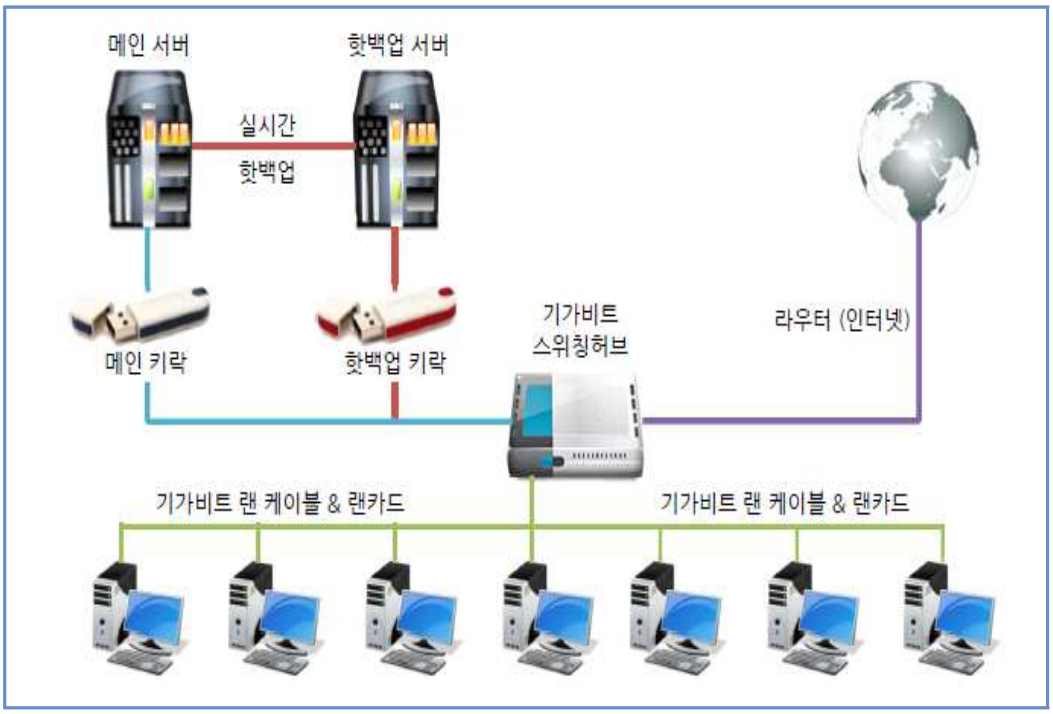

그림 2-1 노하드 시스템 개념도

관리 프로그램은 PC방에 있는 개별 PC를 중앙에서 쉽게 통합 관리하기 위해 사용되며, 최근에는 백신 및 유해사이트 차단 기능이 추가되는 등 많은 기능을 지원한다.

구 분	설 명	종 류	비 고
운영 솔루션	일반 PC를 이용하는 방식과 중앙서버에서 운영체제 및 게임SW를 제공받는 노하드 방식으로 구분	납품업체 : 케니소프트, 지매니져, 슈퍼피방	노하드 방식은 전체 PC방 중 약30% 사용
관리 프로그램	PC방에 있는 개별 PC를 중앙에서 쉽게 통합 관리 (요금 정산 등)하기 위해 사용	SW명 : 네티모, 피카라이브, 게토, 넷커맨더	관리 프로그램을 쉽게 사용하기 위한 보조SW을 사용중

표 2-1 PC방 운영 솔루션과 관리 프로그램 현황

운영 솔루션과 관리 솔루션은 프랜차이즈 특성에 따라 선택되어지며, 전국 각 대리점을 통해 초기 도입이 이루어진다. PC방 운영자들은 프랜차이즈를 통해 도입된 관리 프로그램 외에도 효율적인 관리를 위해 다양한 보조 SW를 추가로 사용하고 있다. PC방 고객들이 주문하는 식품 및 결재를 관리하는 프로그램들이 대표적이다. 보조 SW는 개인이 개발하여 블로그 또는 개인 홈페이지를 통해 배포되는 것이 일반적인 형태이다.

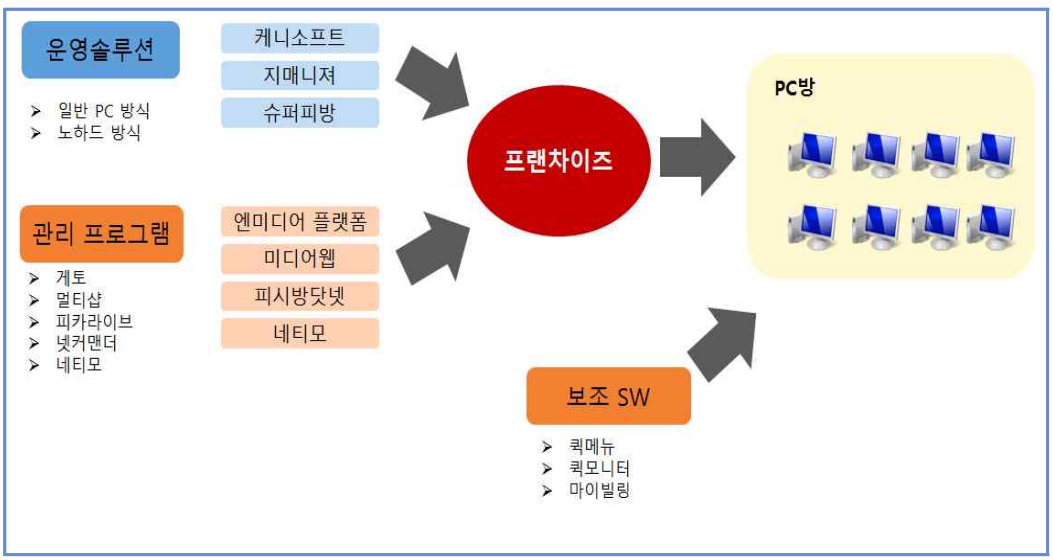

그림 2-2 PC방 솔루션 및 관리 프로그램 유통 구조

2.2 침해사고 사례

■ 노하드 솔루션 대상 디도스 공격 사고

PC방 관련 침해사고 중 가장 최근에 발생한 대표적인 사례는 디도스 공격이다.

올해 초, PC방에서 사용되는 노하드 솔루션 중 특정 A社 제품이 정상 작동하지 않아 해당 솔루션을 사용하고 있던 전국 상당수 PC방이 영업을 중단하는 사고가 발생했다. 당시, PC방 매장 내에 있는 PC들이 정상적인 부팅이 되지 않는 문제가 지속되었으며 사고 발생 후 PC방 커뮤니티 등에서는 A社 제품을 사용 중인 PC방 업주들의 불만이 폭발적으로 증가하였다.

사고 당시, 노하드 솔루션이 정상 작동하지 않은 이유는 크게 2가지였다.

첫 번째 장애 원인은 노하드 솔루션에서 사용되는 인증 서버를 대상으로 발생한 디도스 공격이었다. 노하드 솔루션은 그 특성상 개별 PC들이 정상 작동하기 위해 해외(중국)에 위치한 중앙 인증서버를 통해 인증 과정을 거쳐야 한다. 사고 발생 시점에 해당 솔루션을 개발하고 판매하는 중국 본사를 통해 확인한 결과, 인증 서버를 대상으로 디도스 공격이 발생하여 정상적인 인증이 이루어지지 않고 있었음이 확인되었다.

최근 디도스 공격이 점차 대규모화 되어 가고 있고, 중국에 위치한 인증 서버 대상 디도스 공격을 신속히 막기는 어려우므로, 일정기간 인증 없이도 사용할 수 있는 기간 라이센스를 활용하는 방안을 고려할 필요가 있다.

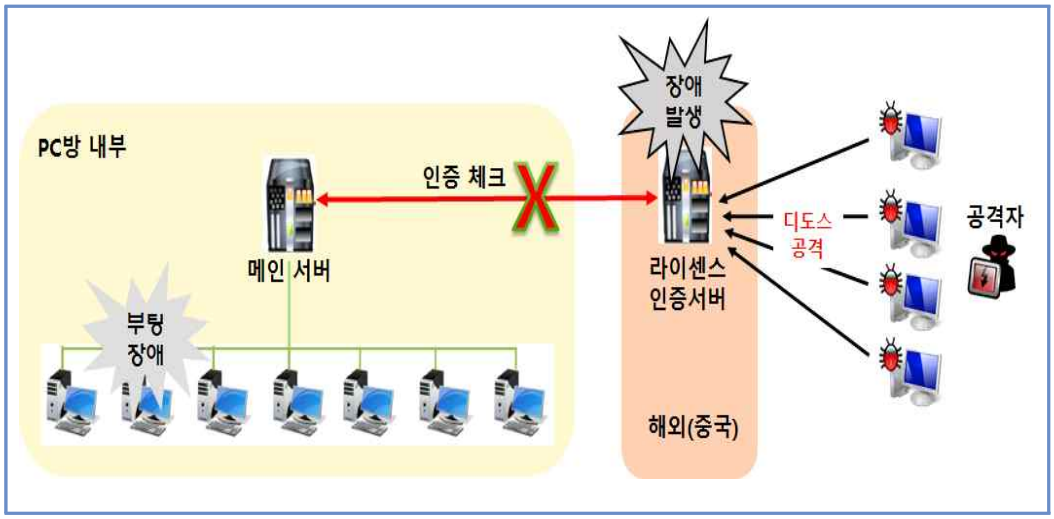

그림 2-3 노하드 인증 서버 대상 디도스 공격 개요

두 번째 장애 원인은 PC방내에 존재하는 노하드 솔루션 메인 서버를 대상으로 발생된 취약점 공격이었다. 디도스 공격으로 인한 장애가 지속되자 A社 제품을 납품하는 국내 업체는 일정기간 인증 없이도 사용할 수 있는 기간 라이센스를 구입하여 PC방에 제공하였다.

그 후 일시적으로 장애가 해결되는 듯 하였으나 또 다시 다른 이유로 장애가 발생하였다. 개별 PC방마다 존재하는 노하드 솔루션 메인 서버의 특정 포트를 대상으로 발생된 취약점 공격이 원인이었다.

당시 발생된 취약점 공격은 특정 포트를 대상으로 비정상적인 요청을 보내어 서버의 정상적인 동작을 중지시키는 일종의 도스 공격이었다.

A社 제품의 국내 납품업체는 메인 서버에 간단한 방화벽을 설치함으로써 취약점 공격을 방어할 수 있었다. 방화벽을 통해 외부에서 메인 서버로 요청되는 패킷을 전체 차단한 것이었다.

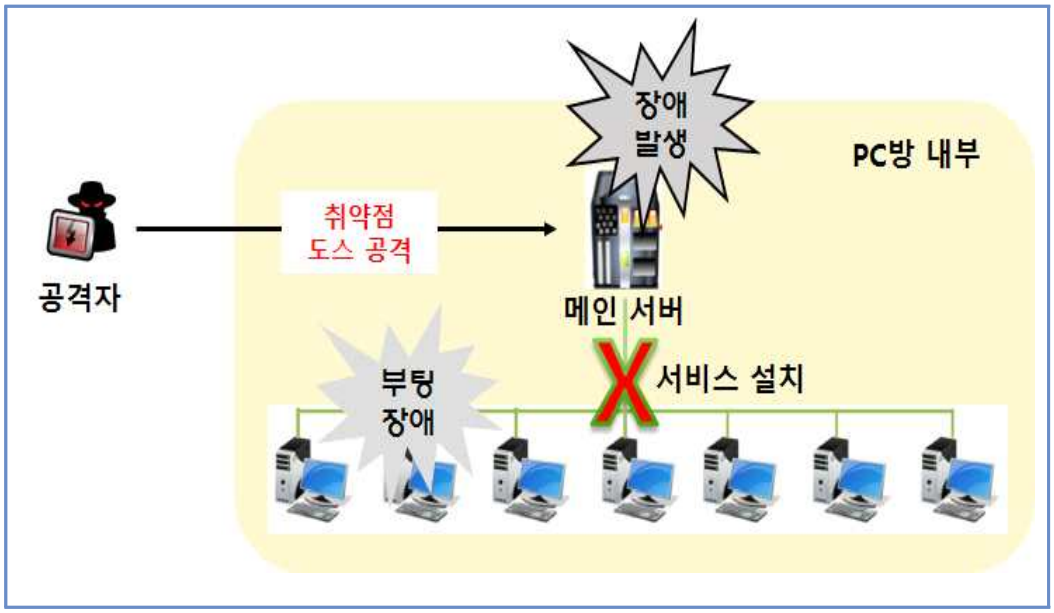

그림 2-4 노하드 메인서버 대상 취약점 공격 개요

PC방 내부에 있는 노하드 솔루션 메인 서버의 경우 라이센스 인증을 제외하고는 외부 네트워크와 통신할 필요가 없으므로 방화벽을 활용하여 접근을 제한하는 등의 보안 조치만으로도 취약점 공격에 대응할 수 있다.

■ PC방 관리용 보조 SW 변조 사고

PC방에서 사용되는 관리용 보조 SW에 악성코드 기능이 심겨져 오랜 기간 배포되어 온 사실이 경찰 수사를 통해 확인되었다. PC방의 경우 개별 PC를 중앙에서 쉽게 통합 관리(요금 정산 등)하기 위해 다양한 중앙 관리 프로그램을 사용하고 있으며, 이러한 프로그램의 기능 향상을 위해 다양한 보조 SW를 추가로 사용한다.

위 사고의 경우, 악의적인 의도에 의해 특정 보조 SW 내부에 상대방의 게임화면을 실시간으로 훔쳐 볼 수 있는 악성 기능이 심겨져서 배포된 사례이다. 즉, 사용자가 PC방에서 포커류의 게임을 실행하면 자동적으로 상대방에게 게임 화면이 전송되어 사기도박 피해를 입게 되는 것이다.

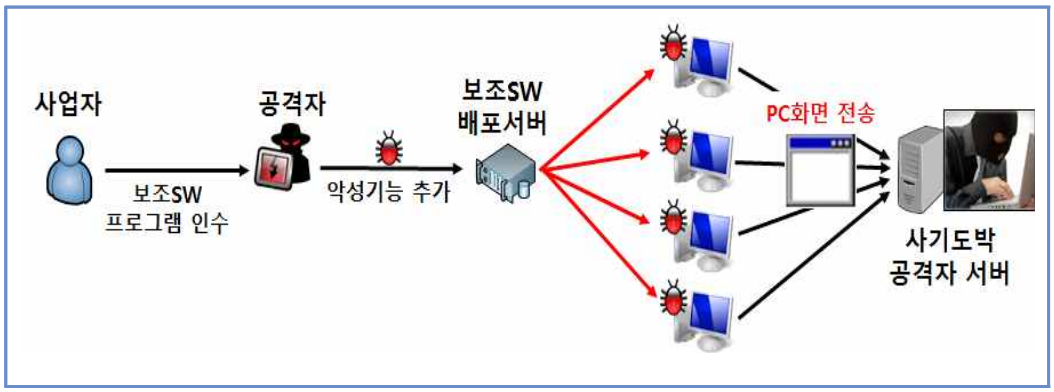

그림 2-5 PC방 중앙관리 보조SW 변조 사고 개요

경찰 수사 결과, 사기도박 행위자들은 정상 사업자로부터 보조SW 프로그램을 인수한 후 의도적으로 내부에 악성 기능을 추가하여 PC방에 납품한 것으로 확인되었다. 이 사고처럼, 의도적으로 SW를 변조할 경우 PC방 운영자들이 문제점을 인지하기는 매우 어려우므로, 보조SW 사용에 있어 많은 주의가 필요하다.

■ 정보 유출 경유지 악용 사고

과거에는 PC방 매장 내에 있는 PC들이 악성코드에 감염되어 침해사고에 악용된 사례가 많았다. 그 후, 개별 PC에 백신을 설치하고 정기적으로 운영체제를 초기화 하는 등의 노력으로 인해 PC가 악용되는 사례는 점차 감소되어 왔다.

그러나 최근에는 PC방에서 운영되는 다양한 관리용 서버들이 침해사고에 악용되고 있다. 특히, 해커는 개인정보와 같은 기업의 중요 정보를 외부로 유출시키기 위해 여러 중간 경유지를 사용하는데, 이때 PC방에서 사용되는 서버를 이용하는 사례가 발견되었다. PC방 서버의 경우 접속기록 등 로그 관리가 체계적으로 이루어지지 않기 때문에 추적이 어렵다는 점을 해커가 악용하는 것이다.

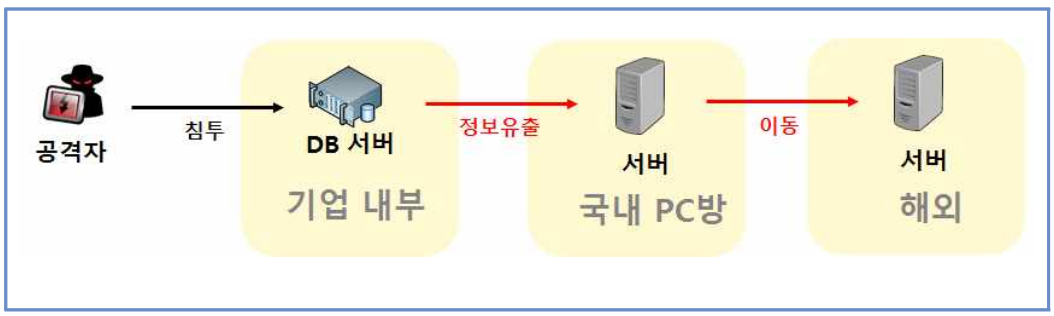

그림 2-6 PC방 서버를 이용한 정보유출

PC방에서 운영되는 관리용 서버의 경우 관리자만 접근을 허용하는 접근제어 정책이 반드시 필요하다. 또한, 관리용 서버 자체가 악성코드에 감염되지 않도록 OS 최신버전을 설치하고 정기적으로 백신 검사를 수행하는 등의 노력도 반드시 필요하다.

제 3 장
침해사고 예방을 위한 보안 안내

제3장 침해사고 예방을 위한 보안 안내

3.1 솔루션 및 SW 제공 업체

솔루션 및 SW 제공업체의 경우에는 제품을 개발하는 단계와 PC방에 실제 구축하는 단계에서 침해사고 예방을 위한 관리지침을 명확히 준수하는 것이 필요하다.

필수적으로 준수해야 하는 관리지침은 아래와 같다.

❍ 네트워크 보안 관리지침 준수

서버가 PC방 내부적으로만 사용되며 외부와 통신할 필요가 없을 경우에는 서버의 IP가 외부 인터넷에 노출되지 않도록 구축하는 것이 중요하다. 만일, 서버의 인증 및 업데이트를 위해 외부 인터넷과 통신할 필요가 있을 경우에는 통신이 필요한 특정 IP에 한정하여 접근하도록 설정하는 것이 중요하다.

위와 같이 네트워크를 설정하기 위해서는 방화벽을 통해 IP 접근을 제한하거나, 인터넷 노출이 전혀 필요 없는 경우 사설 IP 대역으로 서버 환경을 구성할 수 있다.

❍ SW 개발 환경에 대한 보안

SW의 경우 자사에서 개발되어 각 PC방으로 배포되는 형태이므로 개발 환경 단계에서 악의적인 코드가 삽입되지 않도록 보안을 유지하는 것이 중요하다. 이를 위해서는 서버 관리자 계정을 안전하게 관리하고, 관리자 페이지에 대한 접근제어 정책을 적용하는 것이 무엇보다 중요하며, 개발을 위해 필요한 소프트웨어에 대한 보안 업데이트를 최신으로 유지하는 것이 필요하다.

❍ 침해사고 신고

정보통신망 이용촉진 및 정보보호 등에 관한 법률
제48조의3(침해사고의 신고 등) ① 다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생하면 즉시 그 사실을 미래창조과학부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 본다. 1. 정보통신서비스 제공자 2. 집적정보통신시설 사업자 ② 미래창조과학부장관이나 한국인터넷진흥원은 제1항에 따라 침해사고의 신고를 받거나 침해사고를 알게 되면 제48조의2제1항 각 호에 따른 필요한 조치를 하여야 한다.

솔루션을 사용하는 PC방을 대상으로 디도스 공격이 발생하거나, 개발한 SW에 악성기능이 추가되는 등 침해사고가 확인될 경우, 한국인터넷진흥원 보호나라 & KrCERT 홈페이지(www.boho.or.kr)를 통해 신고해야하며 대응·조치를 위한 기술지원을 받을 수 있다.

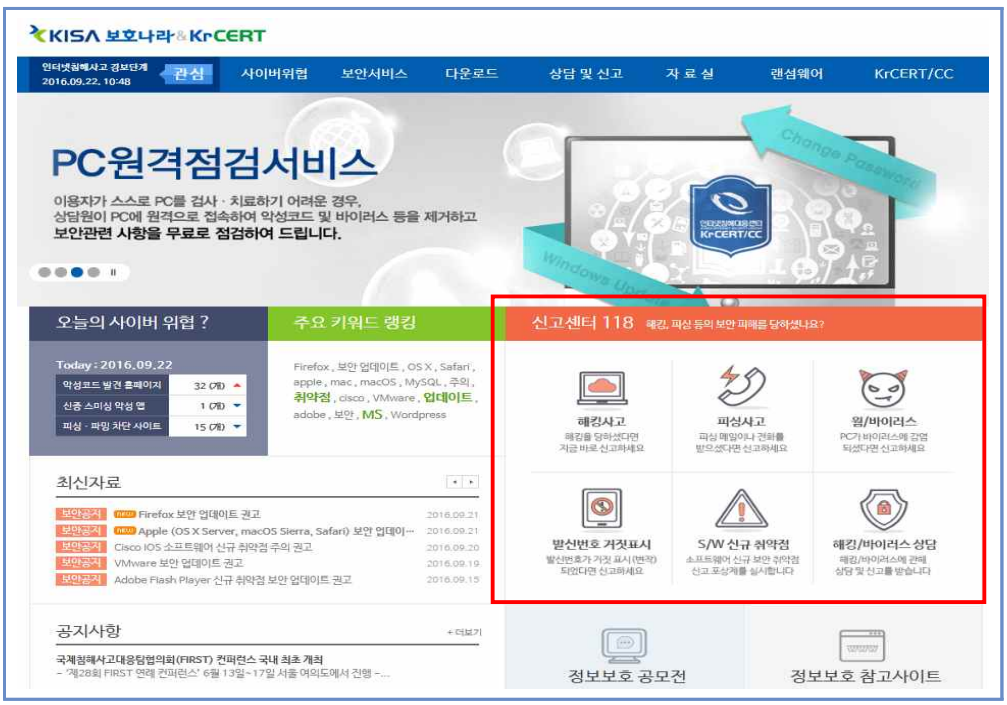

그림 3-1 한국인터넷진흥원 해킹사고 신고

3.2 PC방 운영자

❍ 보안장비(방화벽 등) 운영

방화벽은 가장 기본적이고 필수적인 보안장비이다. PC방에서 운영하는 서버가 외부 인터넷에 노출될 경우 해커의 공격 대상이 될 수 있으며, 방화벽을 통해 특정 서비스만 접근을 허용하는 정책을 적용함으로써 많은 피해를 예방할 수 있다. 또한, 외부에서 PC방 내부로의 접근을 시도한 이력을 기록할 수 있어 향후 침해사고 발생 시 대응하는데 많은 도움이 된다.

특히, 최근 자주 발생하고 있는 노하드 솔루션 서버 대상 디도스(or 도스) 공격 피해를 최소화하기 위해서는 외부에서 불필요하게 솔루션 서버에 접근하는 것을 방화벽을 통해 모두 차단하도록 설정해야 한다.

❍ 운영체제와 응용 프로그램의 최신 보안 업데이트 수행

PC방 운영자는 PC방 관리를 위해 사용하는 중앙 PC 또는 서버에 대한 운영체제, 응용 프로그램의 최신 보안 업데이트를 정기적으로 수행해야 한다. 최신 보안업데이트를 수행 할 경우, 외부에서 공격 시도가 발생하여도 취약점이 존재하지 않아 악성코드에 감염되지 않는다.

PC방 운영자는 응용 소프트웨어를 최신으로 유지하기 위해서 주요 백신 제품에 확대 적용된 『SW 원클릭 안심 서비스』 이용을 권장한다. 『SW 원클릭 안심 서비스』는 업데이트가 필요한 주요 소프트웨어에 대해 안내해주는 서비스로 손쉽게 응용프로그램의 업데이트를 수행할 수 있다.

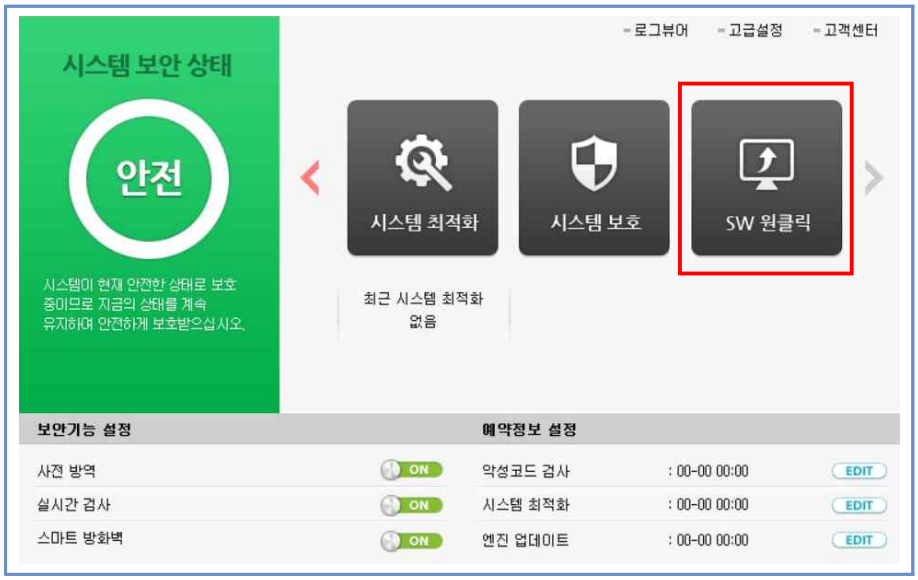

그림 3-2 SW 원클릭 안심 서비스

❍ 백신 프로그램 설치 및 정기적인 점검 실시

악성코드로부터 PC 또는 서버를 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.

PC방 관리를 위해 사용하는 SW의 악성행위를 확인하거나, 디도스 공격 등 침해사고가 확인될 경우, 한국인터넷진흥원 보호나라 & KrCERT 홈페이지(www.boho.or.kr)를 통해 신고해야하며 대응·조치를 위한 기술지원을 받을 수 있다.

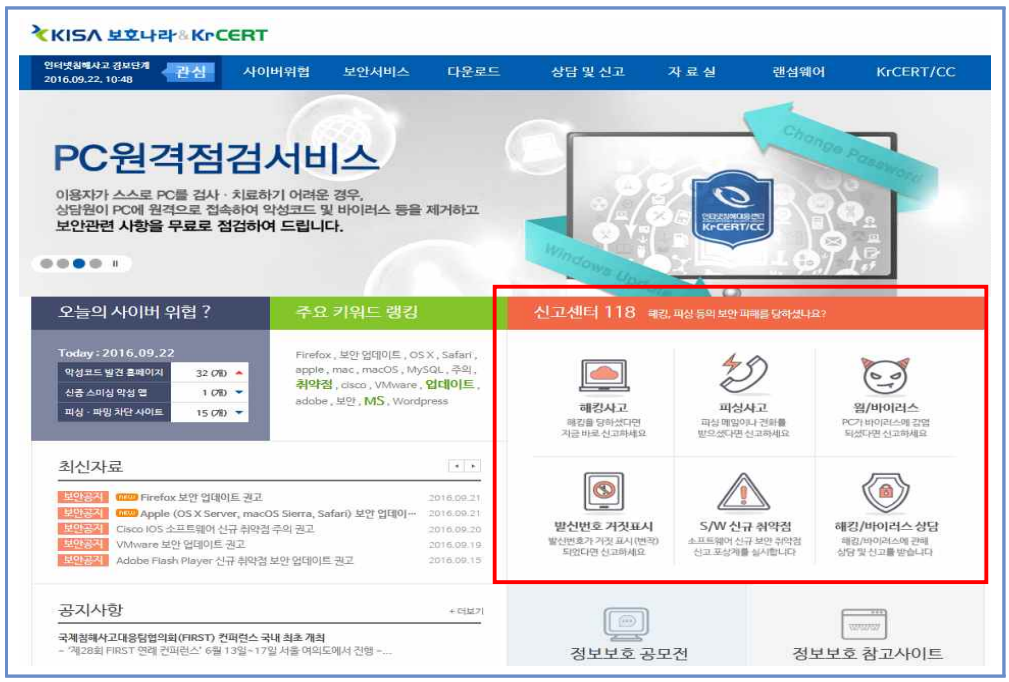

그림 3-3 한국인터넷진흥원 해킹사고 신고