운영체제 지원 종료에 따른 사회적인 보안 위협에 대한 벤더와 정부의 역할에 대한 연구

김인만*, 오태원*
*고려대학교 컴퓨터정보통신대학원
e-mail : Imk5419@naver.com, taewon@korea.ac.kr

A case study of responsibility of vendor and government as Operating System End-of-Life

InMan Kim*, Taewon Oh*
* Dept. of Computer & Information Technology, Korea University

요 약

최근 벤더의 운영체제 지원 종료에 따른 보안 문제와 그로 인한 개인 정보 침해등 피해가 발생되어 전세계적으로 문제가 대두되고 있다. 세계 각국이 벤더와 연장 지원 계약을 하는 등 발빠른 대처를 하고 있으나, 근본적인 문제의 해결은 아직 미흡한 실정이다. 이를 위해 사용자, 벤더 그리고 정부가 운영체제 지원종료로 인한 사회적 문제에 대한 인식이 필요하며, 특히 운영체제를 생산 및 공급하며 지원의 의무를 가지는 벤더와 사회의 안전에 대한 책임을 갖는 정부의 역할에 대해 연구하였다.

1. 서론

최근 운영체제(Operation System, 이하 OS) 생애주기(Life-Cycle)에 따라 벤더의 지원 종료에 따른 보안 문제가 전세계적으로 대두되고 있다.

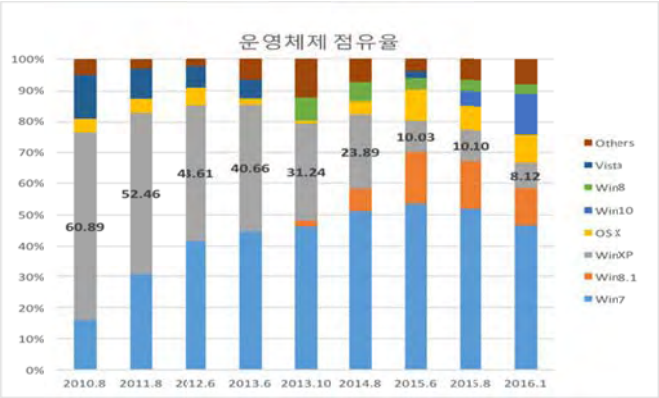
OS 는 모든 형태의 컴퓨터에 필수적으로 설치되어 있으며, 일반 데스트톱 PC, 랩탑 등에 사용되는 클라이언트 OS 와 기업용 서버 OS, 스마트폰이나 테블릿 등에 사용되는 모바일 OS, 특수 기기(가전, 자동차, 항공기 등)에 사용되는 임베디드(Embedded) OS 로 나눌 수 있다. 이러한 OS 를 생산 및 공급하는 벤더는 제품 출시부터 일정 기간 동안 주기적으로 OS 취약점의 보안 패치, 발견된 버그 수정 및 성능 향상 등에 필요한 업데이트를 자동 또는 수동제공하고 있다. 하지만 지원 종료 이후에는 어떠한 수정 업데이트를 제공하지 않아 지원이 종료된 OS 는 바이러스나 스파이웨어, 악성코드, 해킹등 보안 위협에 노출되어 이로 인한 사용자의 직접적인 금전적인 피해 및 개인정보 유출, 좀비 PC 감염 등에 의한 사회혼란과 피해의 발생과 같은 위험이 높아진다.

따라서 OS 지원 종료에 따른 사회적인 문제를 야기하는 위협에 대해 살펴보고, 이에 대응할 수 있는 사용자, 벤더, 정부의 역할에 대해서 연구해 보고자 한다.

2. 지원 종료된 운영체제 사용현황

OS 지원 종료에 대한 위협이 대두되기 시작한 것은 2014 년도 Microsoft(이하 MS)사의 클라이언트 OS 인 Windows XP 와 서버 OS 인 Windows 2003 Server 제품군에 대한 기술 지원 종료를 선언하면서 시작되었다. 이로 인해 국가정보원, 미래창조과학부, 방송통신위원회, 행정자치부에서 2015 년도에 발간한 정보 보호 백서 10 대 위협에 오르기도 했다[1].

MS 사는 OS 에 대한 지원을 그동안 기본 5 년에 추가적으로 5 년을 연장해 10 년 동안 유지하여왔다. 하지만 Windows XP 경우 다른 OS 의 비해 완성도가 높게 만들어 졌고, 다양한 분야에 광범위하게 사용됨에 따라서 총 13 년 간의 서비스를 지원해 왔다.



<표 1> 운영체제 점유율 (2010.8~2016.1)
출처 : StatCounter

<표 1>처럼 Windows XP 는 OS 점유율에서 꾸준히 50%이상을 차지하고 있었으며, 2013 년 이후 에

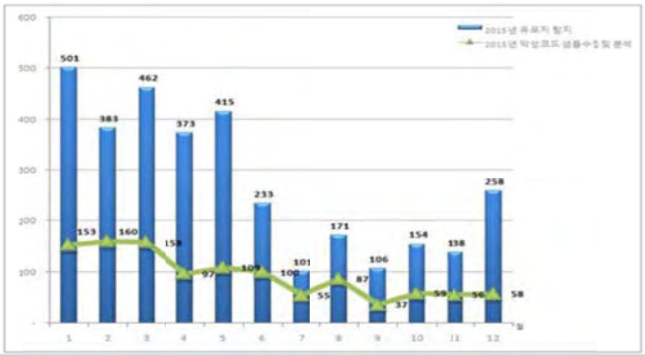
서야 Windows 7 의 점유율이 Windows XP 의 점유율을 넘어섰다. 하지만 Windows XP 지원 종료이후인 2016 년 1 월까지도 8%이상의 점유율을 보여주고 있음을 알 수 있다.

지원 종료 이후에는 더 이상 OS 에 대한 보안 업데이트를 제공하지 않기 때문에 OS 의 취약점을 이용한 악의적인 공격에 의한 위협에 쉽게 노출될 수 있기 때문에 안전한 사용을 위해서 사용자, 기업 및 정부에서는 기존 OS 시스템의 업그레이드 또는 보완장치를 갖추어야 한다. 하지만 OS 업그레이드를 하기 위해서는 많은 비용, 시간과 시스템의 환경변화에 따른 위험부담 등이 필요하기 때문에 사용자에 강요할 수 만은 없는 실정이다.

3. 위협성

OS 벤더는 지원 종료이후 OS 의 어떠한 취약점이 발견되더라도 패치를 배포하지 않기 때문에 이미 지원이 종료된 OS 는 스파이웨어, 악성코드, 해킹등 보안 위협에 그대로 노출될 수 밖에 없다.

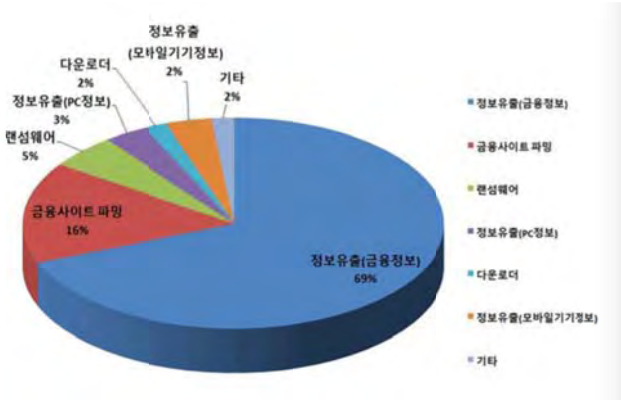
한국 인터넷진흥원(KISA)가 2015 년 12 월에 발표한 월간 악성코드 은닉사이트 탐지 동향 보고서에 의하면 악성코드 유포지 탐지 건수는 138 건에서 258 건으로 전월대비 87% 급속하게 증가했으며, 앞으로도 꾸준히 증가할 것이라고 전망하고 있다.



<표 2> 악성코드 유포지 탐지 건수 (2015.1~2015.12)

이러한 악성 코드들은 OS 와 소프트웨어의 취약점을 이용하여 감염되며, 이 중 69%는 정보유출(금융정보)로 이어져 제 2, 제 3 의 범죄에 사용되어 실제 금전적인 피해로 이어진다[2]. 또한 이러한 악성 코드를 통해 좀비 PC 를 양상하여 여러 가지 사이버 위협이나 사이버 범죄 등 사회적인 문제를 야기할 수 있다.

IT 기업의 경우 OS 의 알려진 취약점으로 인해 기업이 보유한 데이터의 통합성, 가용성, 보안성의 손상, 네트워크를 통한 감염, 사업 연속성 단절과 같은 자산에 대한 직접적인 피해와 함께 신뢰도의 하락과 그에 따른 매출 감소로 이어 질 수 있으며, 이는 기업의 생존에도 크게 영향을 줄 수 있다.



<표 3> 악성코드 유형별 비율

4. 대응사례

가장 큰 문제가 발생할 가능성이 있는 부분은 바로 금융권이다. 전 세계의 현금인출기(이하 ATM) 중 약 95%에 Windows XP 가 설치 사용되고 있고, 국내의 경우 전국 ATM 의 94%가 Windows XP 또는 그보다 더 오래된 OS 를 사용 중이다. 또한 금융권 업무용으로 사용하는 PC 의 24%(약 16 만대)가 Windows XP 를 사용 중이다. ATM 이나 금융권의 PC 는 악의적인 공격으로 인하여 은행과 고객에게 직접적으로 금전 피해를 발생 시킬 수 있기 때문에 새로운 OS 업그레이드와 인터넷이 연결되지 않는 별도의 통신망을 사용하여 해커의 공격을 원천 차단해야 한다[3].

정부는 Windows XP 의 지원 종료에 따른 보안 위협에 대응하기 위해 악성코드 모니터링과 전용 백신을 제작 및 보급을 담당하는 비상 대응반과 행정기관 Windows XP 대응 종합 상황실을 운영하고 있지만, 국가적으로 근본적인 Windows OS 지원 종료에 대한 대책이 마련하지 않는다면, 5 년, 10 년 후에 위와 같은 위협을 되풀이 될 것이다[4]. 미국, 호주, 영국의 경우에는 Windows XP 의 지원 종료 이후에도 금융기기의 안전을 위해서 OS 가 업그레이드 되기 전까지 MS 사와 기술 지원 계약을 체결하였다[5][6][7]. 영국 정부는 별도 계약을 통해 공공부문의 지원을 2015 년 5 월까지 연장하였으나, 추가 지원 이후 2015 년 7 월 CNR Search 에 따르면 영국 지방의회의 31%는 여전히 지원 종료된 Windows XP 를 사용하고 있다고 한다[8]. 독일의 경우에는 오픈소스 기반 자체 OS 인 Linux 로 전환하였으며, 우분투의 보급을 촉진하고 있다. 일본의 경우 1,320 백만 이상의 PC 가 Windows XP 를 사용하고 있어 지원 종료로 인해 바이러스, 해킹에 대한 위협이 노출되어 있다. 기업용 PC 중 약 723 만 대가 Windows XP 기반으로 구동되고 있으며, 상위 버전의 Windows OS 의 전환이 느리게 진행되고 있다. 이에 일본 정부는 지역 상공 회의소와 협력을 통해서 소규모 기업의 OS 전환을 촉진하기 위한 세미나를 개최하고, 신규 PC 구매 비용을 유예해주는 인센티브 제공하는 동시에 PC 제조사들은 PC 의 가격 할인을 통해서 판매를 촉진하고 있다. 또한 Windows XP 를 PC 2 대중 1 대를 사

용하는 중국의 경우 정부 차원의 기술 지원 연장을 MS 사에 요청했지만 거절되자 우분투 기반의 OS 를 개발하여 보급을 확산 시키고 있다.

5. 해결방안

일반적으로 지원이 종료된 OS 에 대한 업그레이드 또는 장비 교체를 권하고 있지만, 일반 사용자의 경우에는 업그레이드에 대한 추가적인 비용과 시간이 필요한데다가 보안의식의 부재로 새로운 기기로 바꾸기 전까지는 OS 의 업그레이드를 하지 않는다. 또한 IT 기업에서는 OS 업그레이드 비용부담, 직원교육, 어플리케이션의 호환성에 대한 수정-테스팅 등과 같이 추가적인 시간과 노력이 필요하다. 지원이 종료된 OS 에 대한 업그레이드는 정부 차원의 법령이나 이를 실행하지 않을 경우에 대한 제재가 있지 않은 상태로 자율 권고사항이기 때문에 보안에 미흡한 기업들은 업그레이드를 미루고 있다.

그렇지만 앞서 언급된 한 것처럼 OS 의 취약점에 대한 공격이 많은 사회적인 문제를와 추가적인 사이버 범죄로 인해서 사용자의 피해를 야기시킬 수 있다. 이러한 사회적인 문제의 해결에는 사용자, 벤더 그리고 정부의 책임 공유가 필요하다.

사용자들은 자신의 기기에 악성코드 감염, 해킹등 피해에 대비하여 OS 에 대한 보안 업데이트의 주기적인 설치가 필요하며, 악성코드 감염을 방지하기 위한 노력을 기울여야 한다. 벤더는 OS 의 지원 종료의 발표 이후에 지속적이고 적극적인 홍보를 통해서 사용자 또는 기업이 지원 종료에 대한 위협을 인지할 수 있도록 노력하여야 하며 정부와 기업 요청시에 추가적인 지원과 이에 대한 협조를 적극적이로 임해야 할 것이다. 정부는 자국내의 사용자와 기업의 기술 지원 종료된 OS 에 대한 지속적인 모니터링과 위협에 대한 가이드 라인을 제공할 의무를 가지면서, 지원 종료된 OS 업그레이드 비용을 추가적인 지원 또는 세금 감면과 같은 정책을 통해 기업 측면에서 업그레이드에 대한 비용 절감을 할 수 있도록 도와야 한다. 또한 법이나 제도적인 방침을 마련하여 사용자와 기업이 지원이 종료된 OS 에 대하여 책임을 가지고 지원하도록 하여야 한다. 실제로 2014 년 MS 사의 Windows XP 지원 종료 당시 영국 정부는 Windows XP 를 계속 사용하여 PC 보안을 지키지 않은 기업에게 최고 50 만 파운드의 벌금을 부과하겠다고 밝힌 바 있다.

6. 결론

OS 지원 종료에 대한 대응이 적절치 않았을 경우 발생하는 문제와 피해에 대한 책임은 사용자, 벤더, 정부 모두에 있다고 할 수 있다.

이에 필요한 첫번째는 OS 지원 종료로 인한 문제가 발생하고 또는 발생할 수 있고, 그에 따른 피해가 발생한다는 사실에 대한 사회적인 인식과 문제를 해결하고 피해를 방지하기 위해 사회적인 제도와 이를 실행하기 위한 비용의 지출에 대한 사회적 합의이다.

두번째로 벤더에서 규정하는 OS 의 생애주기(Life-Cycle)가 아닌 최종 사용자까지 지원을 하도록 하는 등의 선제적인 제도적 장치와 사용자를 추적-관리 할 수 있도록 개인정보침해를 하지 않는 범위에 한하여, 합법적인 방법을 통해 벤더에서 판매 및 사용자 정보를 정부가 확보할 수 있어야 한다

세번째로 정부는 OS 지원 종료에 의한 문제 및 피해에 대한 모니터링 뿐만 아니라 앞서 말한 사회적 합의에 의해 사용자와 벤더를 지원하고 협력하여야 한다. 필요에 따라서는 법적, 제도적 제재가 필요할 수도 있다.

7. 향후 연구 계획

스마트폰, 테블릿, PC, 서버, IoT, 무인자동차를 포함 한 OS 를 사용하는 모든 디바이스에 대한 대응책이 필요하다. 특히 안드로이드 OS 를 사용하는 스마트폰에 대한 위협이 현실로 다가오고 있어 그에 대한 연구가 시급하다.

참고문헌

[1] 국가정보원, 미래창조과학부, 방송통신위원회, 행정자치부 “국가정보보호백서 2015”, 2015
[2] 한국인터넷진흥원, “월간 악성코드 은닉사이트 탐지 동향보고서”, 2015.12
[3] 금융위원회, “윈도우 XP 기술지원 종료에 따른 금융회사 대응 현황,” 2014. 3. 26.
[4] 전자신문, “윈도 XP 지원종료 후속대책 마련에 분주,” 2014. 4. 8.
[5] 전자신문, “170 만대 ATM 위험, XP 종료 앞두고 美·英 은행 MS 에 SOS,” 2014. 3. 23.
[6] 이투데이, “윈도우 XP 지원 종료, 영국·독일·일본·중국 등 나라별 업데이트 대처법은?,” 2014. 4. 3.
[7] Sydney Morning Herald, “Doomsday approaches for Windows XP users,” 2014.3.19
[8] CRN research, “Local authorities still running unsupported Windows XP”, 2015.7.23 (http://www.computing.co.uk/ctg/news/2418923/local-authorities-still-running-unsupported-windows-xp)