

스파이웨어의 위험성에 대한 연구

* 성상현

* SK텔레콤

* ssh1116@sktelecom.com

A Study on the Risks of Spywares

* Sanghyun Sung

* SK Telecom

요 약

스파이웨어는 바이러스, 웜과 더불어 개인의 정보시스템에 대한 최대의 위협으로 등장하고 있다. 바이러스, 웜에 대한 탐지 및 대응은 정보시스템 사용자의 대다수가 인식하고 있거나 사용 중인 바이러스 백신 프로그램에 의하여 처리가 가능하지만, 스파이웨어의 경우는 아직 침투경로, 피해유형 및 대응 방안에 대한 인식과 처리가 제대로 이루어지지 못하고 있는 상황이다. 또한, 기존의 바이러스 백신 및 유사 프로그램으로 스파이웨어에 대한 기술적 대응이 불가능한 경우가 대부분이며, 침해형태가 개인 정보 유출로 직결되는 것이어서 더 큰 문제를 안고 있다. 본 논문에서는 먼저 스파이웨어에 대한 기본 개념을 파악하기 위하여, 스파이웨어의 정의를 조사하였다. 또한, 스파이웨어와 관련된 최신 확산 현황을 통해 스파이웨어가 장기적으로 어느 정도의 사회적 문제로 대두될지를 짚어보았다. 마지막 단계로는 스파이웨어에 대한 위협과 보안통제를 조사하였다. 본 논문에서 제시한 내용을 통해 정보시스템의 개인 사용자들은 스파이웨어의 침투 경로 및 침해 내역을 파악하여 이에 대한 개인 차원의 대응을 할 수 있을 것이며, 기업 및 기관의 책임자는 조직내부의 스파이웨어 확산 및 침해에 대응하기 위한 관리적, 기술적 차원의 대응책을 수립할 수 있을 것이다.

1. 스파이웨어의 정의

스파이웨어는 개인 또는 조직에 대한 정보를 그들 스스로 동의하거나 식별하지 못하는 상태에서 수집하도록 지원해주는 소프트웨어를 의미한다 (SearchCRM). 스파이웨어는 컴퓨터 바이러스나 또는 새로운 프로그램 설치의 결과로서 컴퓨터에 잠입할 수 있다. 만약 그 사용자가 어떠한 데이터가 수집되고 있으며 그것이 누구와 함께 공유되고 있는지 등을 충분히 이해하고 있다면, 즉 사용자가 그 사실을 알고 있는 상태에서 설치된 데이터 수집 프로그램은, 정확히 말하자면 스파이웨어가 아니다 (Webopedia). 스파이웨어는 애드웨어, 브라우저 하이재커, 브라우저 플러그인, 키로거 등이 존재한다.

애드웨어(Ad-ware)에는 다음과 같은 프로그램이 속한다. 123Messenger, 123Search, 2020Search, A Better Internet, ACXInstall, AdBreak, AdGoblin, Adult Chat Dialer, Adult-Links, Aornum, ApropoSMedia, ASpam, Aureate, BargainBuddy, BDE, BlazeFind, BonziBuddy, BookedSpace, BrowserAid, BrowserToolbar, Bulla, Clearsearch, ClearStream, Accelerator, Click Till U Win, ClickTheButton.

브라우저 하이재커(Browser Hijacker)에는 다음과 같은 프로그램이 속한다. 2nd-thought, ActualNames, CoolWebSearch, GoFlip, Httper, IETray, iGetNet, ILookup, Ineb Helper, ISTbar, LoadFonts, Masterbar, NavExcel, PRW, Realphx, SafeSearch, Seach Assistant, Searchex, ShopNav, SmartBrowser, Stop Popup Ads Now, Surfairy, Tellafriend, Whazit, Winshow.

브라우저 플러그인(Browser Plugin)에는 다음과 같은 프로그램이 속한다. Alexa Toolbar, Comet Cursor, EasyBar, Fastseeker, FavoriteMan, HotBar, Huntbar, IBIS Toolbar, Internet Marketing Toolbar Pro, Mirar, MySearch, Show Bar, UCmore, W97M_SPY.A, Web Behavior.

키로거(Key Logger)에는 다음과 같은 프로그램이 속한다. 2Spy!, 3rdEye, AB System Spy, Absolute Keylogger, AceSpy, Actions Monitor, Activity Logger, Activity Monitor 2002, Advanced Keylogger, Apophis, AppsTraka, Ardamax Keylogger, AtomicLog, Belkin PCSpy, BizDefender, Black Box, Boss EveryWare, Call Online Two, Catch Cheat Spy, Chat Watch, Chota, COM, Com Policy, Computer Snooper, ComputerSpy.

2. 스파이웨어 전파 현황

최근에는 합법을 가장한 전파 유형도 많이 발생하고 있다. 스파이웨어는 EULA (End User Licensing Agreements)에 대한 사용자의 부주의를 통해서 쉽게 전파되는 경우가 많다. 사용자는 새로 구매하거나 또는 인터넷에서 다운로드받은 무료 소프트웨어 설치할 경우 화면에 나타나는 EULA문구를 세부적으로 읽어보지 않는 경우다. EULA에 동의하진 않는 물음에 단순히 동의(Agree)에 체크를 하고 알 수 없는 모듈들을 다운로드 받고 설치하게 되는 것이다 (Choney, 2004). 이 부분에 대한 법률적 해석은 쉬운 문제가 아니다. 법률적으로는 의사표시에 있어 내심의 의사와 표시의 행위가 서로 일치하지 않거나 의사형성과정에 결함이 있다면, 그 정