백신프로그램 분석을 통한 개발전략(기업분석 중심으로)

박경원*

*숭실대학교 SW특성화대학원

A Development Stragy for Analysis of Vaccine Program

Kyeong-won Park*

* Graduate of Soong-sil University

E-mail : kwpark85@naver.com

요 약

최근 해킹 등의 보안문제로 인해 많은 기업들이 다양한 백신프로그램을 개발하고 있다. 그러나 이러한 프로그램들은 해킹의 방법이 다양화되어 가고 있기 때문에 모든 문제를 해결하는데 어려움이 있다. 본 논문에서는 기업에서 제공하고 있는 백신프로그램의 분석을 통해 향후 백신프로그램 개발 방향을 제시하고자 한다.

ABSTRACT

Recently, many corporatiions have developed various vaccine programs because we are faced with security problems. However, these programs have difficulty dealing with all problems related with security. Because hackers try to intrude by so many methods. This paper includes objects of next generation development for analyzing vaccine programs.

키워드

백신프로그램, 백신, 보안, 해킹

Ⅰ. 서 론

최근 해킹이나 악성코드 등의 보안과 관련된 많은 문제가 발생하고 있다. 이로 인하여, 많은 사람들이 컴퓨터 시스템을 사용하는데 많은 문제가 발생하고 있어 불편함을 호소하고 있다. 현재, 대부분의 기업들은 이러한 문제를 해결하기 위해서 다양한 백신프로그램을 지속적으로 개발하고 있다. 그러나, 현재 개인이나 기업에게 제공되고 있는 대부분의 프로그램들은 해킹의 방법이 점점 다양화되어 가고 있어 현재 발생하고 있는 모든 해킹에 대한 대응책을 마련하는데 어려움을 겪고 있다. 따라서, 본 논문에서는 기업에서 제공하고 있는 백신프로그램 기능에 대해서 분석하고 이를 통해 이전보다 개선된 백신프로그램 개발 전략을 제시하고자 한다.

Ⅱ. 본 론

서론에서는 백신프로그램에 대한 전반적인 현황에 대해 언급하였다. 본론에서는 현재 대중적으로 이용하고 있는 안랩에서 제공하는 V3 Lite 프로그램, 이스트소프트에서 제공하는 알약 프로그램 및 네이버에서 제공하는 네이버 백신에 대해서 언급하기로 한다.

(1) V3 Lite

V3 Lite는 국내기업인 안랩에서 제공하고 있는 컴퓨터 바이러스 검사프로그램이다. 현재 국내에서 가장 많이 사용하고 있는 백신 프로그램이다. 이 프로그램에 대한 기능은 다음과 같다.

- 실시간 검사/빠른 검사로 바이러스, 웜 등 악성코드 진단 및 치료
- ASD 클라우드 진단을 통한 신·변종 악성코드 검사

· 의심스러운 웹 사이트 접속 차단 등 웹 보안 기능

(2) 알약

알약은 이스트소프트사에서 제공하고 있는 통합 백신프로그램이다. 다른 백신 프로그램에 비해서 상대적으로 가볍다는 점이 특징이다. 또한, 프로그램을 쉽게 사용할 수 있도록 설계되었기 때문에 많은 사람들이 이용하고 있다. 알약의 주요기능은 다음과 같다.

· 바이러스와 악성코드에 대한 검사 및 치료
· 실시간 감시
· 신종 악성코드에 대한 탐지
· 자동 업데이트
· 이동장치검사
· 악성봇 사전 방역
· 게임모드 지원
· 악성코드 감염 의심 알림
· PC 최적화 및 관리
· 보안 업데이트
· 호스트 파일 보호
· 알약 알림 서비스

(3) 네이버 백신

네이버 백신은 네이버에서 제공하는 백신프로그램으로 악성코드 및 스파이웨어, 바이러스, 웜, 해킹 등의 외부적 위험 요소로 부터 다양한 기능을 통해 사용자의 PC를 보호하고 치료하는 목적으로 만들어진 프로그램이다. 다른 백신프로그램과는 다르게 Windows XP에 대한 보안기능과 32비트 버전과 64비트 버전에 대해 최적화된 기능을 제공한다. 네이버 백신의 특징은 아래와 같다.

· 더욱 빠르고 가벼워진 검사
· 안정적인 엔진 제공
· 다양한 검사와 치료 방법
· 실시간 감시 및 DB 업데이트
· 클릭 한번으로 PC 최적화하기
· 시스템 최적화
· ActiveX 컨트롤, 툴바 정리
· 시작 프로그램, 설치 프로그램 관리

III. 분석결과

본론에서는 국내에서 제공하고 있는 백신프로그램에서 제공하는 기능에 대해서 분석하였다. V3 Lite, 알약, 네이버 백신은 악성코드 등에 대한 실시간 방지 서비스, 시스템에 설치되어 있는 프로그램에 대한 관리 기능 및 실시간 업데이트 기능을 제공하고 있다는 점을 확인할 수 있다. 그러나, V3 Lite에서는 웹사이트 차단 기능을 제공하고, 알약에서는 게임을 할 때 발생할 수 있는 악성코드 보호를 제공하며 네이버 백신에서는 설치 프로그램 관리 및 Windows XP에 대한 시스템 보호기능을 제공한다. 현재 제공하고 있는 백신프로그램을 분석해 볼 때, 프로그램 마다 제공하는 기능이 다소 차이가 있지만 대체적으로 악성코드 침입 방지 기능 및 프로그램 보호 기능을 제공하고 있다고 볼 수 있다.

IV. 결 론

우리는 지금까지 백신 프로그램에 대해 분석해 보았다. 그러나, 업데이트 기능은 일정한 주기에 의해 이루어지기 때문에 신종 악성코드나 바이러스 등에 대처하는데 어려움이 따르고 있다. 따라서, 이러한 문제를 해결하기 위해서는 개발자(혹은 개발업체)가 주기적인 업데이트 방식 대신에 실시간 업데이트 형식의 서비스를 사용자에게 제공해야 한다.

아직까지 국내에서는 인터넷을 하면서 발생하는 대포적인 악성코드인 애드웨어를 치료할 수 있는 소프트웨어가 제대로 개발되지 않았다. 추후에는 애드웨어를 치료할 수 있는 기능까지 추가해서 인터넷을 사용하는데 불편함이 없도록 하는 것이 중요할 것이다.

참고문헌

[1] http://www.ahnlab.com/kr/site/product/productView.do?prodSeq=8
[2] http://alyac.altools.co.kr/Public/Alyac/AlyacPub.aspx
[3] http://software.naver.com/software