컴퓨터 바이러스 유형에 따른 백신 프로그램의 성능분석

박득배*, 장인태*, 송영준**, 안재형*
*충북대학교 정보통신공학과
**충북대학교 BITRC
e-mail:songyjorg@dreamwiz.com

The Performance Analysis of Vaccine Programs According to Computer Virus Classes

Deuk-Bae Park*, In-Tae Jang*, Young-Jun Song**, Jae-Hyeong Ahn*
*Dept. of Electrical & Computer Engineering, Chunbuk National University
**BITRC, Chungbuk National University

요 약

본 논문은 초고속 인터넷 시대에 자주 출몰하는 컴퓨터 바이러스 및 악성코드의 특징을 분석하고, 이에 대응하는 국내외 사용 백신 프로그램들의 성능을 비교 분석하여 미래에 출현할 악성 바이러스에 대한 최상의 대처법을 제안하였다. 국내외에서 가장 많이 사용되는 상용 백신 프로그램의 특정 바이러스 및 악성코드를 침투시켜 대응 여부를 조사하고, 백신 프로그램의 DB(데이터베이스) 업데이트 주기, 대응 바이러스 목록 분석 등을 시행하여 특정 바이러스 및 악성코드에 대한 효율적인 대응책을 제시하였다.

1. 서론

인터넷 인프라의 급속한 발전과 인터넷 보급률의 확대에 따라 PC의 보안을 위협하는 악성 프로그램이 갈수록 다양화되고 있고 악성 프로그램에 의한 피해는 기하급수적으로 증가하고 있다. 인터넷 인프라 기술의 발전이 오히려 개인 정보보호에 큰 피해를 주고 있다. 즉 고성능 컴퓨터가 인터넷의 특정 좀비 컴퓨터로 이용되거나 웜에 감염되어 또 다른 전염 대상 PC를 찾을 때 네트워크 인프라의 고속화에 따라 피해 상황도 확산되고 있다.

특히 교통, 금융, 에너지 그리고 국가 시스템 망에 대한 보안이 더욱 중요해 지고 있다. 국가 정보 네트워크 인프라는 경제 및 사회 전반적으로 사용되는 망이기 때문에 어떤 위협으로부터도 안전하게 보호되어야 하고 운영되어야 한다. 만약 국가망이 위협을 받을 경우 시회와 경제에 큰 혼란이 온다[1].

악성 프로그램은 그 종류에 따라서 다양한 형태가 존재하지만, 다른 프로그램 또는 운영체제에 접근하여 코드를 변경시키거나 정보를 유출하는 동작, 비정상적인 네트워크 패킷을 송수신하는 동작 또한 보안 프로그램으로부터 자신의 존재를 숨기기 위한 은닉 행위와 같은 일반적인 프로그램과는 다른 이상 행동을 수행한다는 공통적인 특징을 가지고 있다.

이처럼 현재 다양한 바이러스 및 악성코드들이 보안을 위협하고 있다. 이러한 위협으로부터 보호할 수 있는 가장 최적의 방법은 여러 가지 방법이 있지만 가장 중요한 것은 백신 프로그램이 효율적으로 대응해야 한다. 각각의 백신 프로그램의 차이점과 DB(데이터베이스)의 업데이트 주기 및 악성코드와의 상관관계를 잘 분석하여 적절하게 대응을 해야 한다[2]. 이러한 분석만 잘 이루어진다면 특정 악성코드가 발생하였을 때 PC사용자들이 더욱 효과적으로 백신 프로그램을 통해 대응할 수 있다[3].

본 논문에서는 여러 악성코드의 동향 및 유형을 분석해 보았고 샘플 악성코드로 백신 프로그램의 상관관계를 분석하였고 여러 백신 프로그램의 DB 업데이트 주기를 분석해 보았다.

본 논문은 제 1장은 연구의 필요성을 기술하고, 연구의 범위를 설정 하였다. 제 2장에서는 바이러스 및 백신 소프트웨어의 일반적인 이론을 제 3장은 바이러스 유형에 따른 백신 프로그램 성능비교를 제시하였다. 제 4장에서는 제안 방법을 구현, 실험하여 백신별 DB 업데이트 주기 및 업데이트 내역을 연구하였다. 제 5장은 결론 및 앞으로 개선되어야 할 점과 향후 연구 과제를 중심으로 기술하였다.

2. 관련연구

2.1 최근 유행하는 악성코드 TOP 10

최근 유행하는 악성 코드 Top 10은 <표 1>과 같이 사용자 PC에서 탐지된 악성코드를 기반으로 산출한 통계를 보여준다[4]. 카테고리는 Adware, spyware, Trojan, Worm의 4개 부분으로서, 감염자수가 많은 악성코드들로부터 순차적으로 정리하였다.

<표 1> 감염된 악성코드 TOP 10

순위	악성코드	카테고리	감염자수
1	V.ADV.Admoke	Adware	55,195
2	S.SPY.Lineag-GLG	Spyware	46,529
3	V.DWN.디.39.xx	Trojan	33,490
4	V.TRJ.Patched.imm	Trojan	27,240
5	A.ADV.BHO.IESerch	Adware	26,463
6	S.SPY.OnlineGame	Spyware	21,728
7	V.WOM.Conficker	Worm	21,642
8	Trojan.Generic.4667513	Trojan	20,078
9	S.SPY.OnlineGame-H	Spyware	19,099
10	Trojan.Generic.4758434	Trojan	14,837

<표 2>는 2010년 카테고리별 악성코드 유형을 분석한 것으로 가장 높은 비율을 차지한 트로이목마(Trojan)는 보안이 취약한 웹사이트에서 유포된 경우가 많이 발견되었고, 현재 가장 많이 사용되는 운영체제인 윈도우에서 동작하는 악성코드는 윈도우 바이러스, 웜(Worm), 트로이목마(Trojan), 백도어(Backdoor)등이 있다.

<표 2> 2010년 악성코드 유형

순위	악성코드 유형	비율	비고
1	트로이목마	37%	
2	애드웨어	28%	
3	스파이웨어	26%	
4	웜	6%	
5	백도어	3%	

2.2 백신 소프트웨어 분석

국내외 백신 프로그램 업체 중 대표적인 안철수 연구소, 하우리, NHN, McAfree 등의 백신 프로그램들을 분석하여 <표 3>과 같이 각 백신 프로그램의 주요 치료 및 예방 기능이 정리된다. 또한 각 백신 프로그램의 업데이트 주기, 업데이트 방법은 <표 4>와 같이 비교 분석된다. 각 백신의 업데이트 주기는 때에 따라 수시로 업데이트하게 되어 있고, 그 기간은 보통 계약기간 내에 하게끔 된다. 또한 업데이트 방법은 각 백신마다 다른 방법을 취하고 있는 것을 보여준다. 주로 바이러스 정의에 의한 업데이트 방법을 취하나 최근에는 인공지능의 스마트 업데이트로 발전하고 있다.

<표 3> 국내, 해외 백신 프로그램의 특징

백신 소프트웨어	주요 치료 및 예방 기능	제조사
V3 제품군	PC 바이러스 예방, e-mail 매신저 바이러스 예방	안철수 연구소
ViRobot 제품군	유해 Spyware, Adware 진단 및 제거	하우리
바이러스 체이서	강력한 실시간 감시 비 패턴 기방 바이러스 탐지	SGA
네이버 백신	강력한 멀티 엔진 제공	NHN
AVAST	안티 바이러스, 행동 감시 인공지능 감시	알웰 소프트웨어
노턴 바이러스	바이러스, 스파이웨어, 봇넷, 루트켓 차단	Symantec
Anti-virus+	안티바이러스, 안티피싱, 양방향 방화벽 보호	McAfee
Anti-Virus 2010+	고급 개인정보유출 방지, 제로데이공격 사전방어	Kaspersky

<표 4> 백신 프로그램들의 특징 비교

백신명	업데이트주기	업데이트 기간	업데이트방법
V3 365 클리닉	때에 따라 수시	계약기간 내	스마트 업데이트
ViRobot Desktop 5.0	때에 따라 수시	계약기간 내	expert 업데이트
Virus Chaser 6.0	때에 따라 수시	계약기간 내	패턴 업데이트
Naver 백신	때에 따라 수시	평 생	엔진자동 업데이트
Avast Internet Security	때에 따라 수시	계약기간 내	스마트 바이러스 정의 패턴 업데이트
Norton Anti-Virus 2010	때에 따라 수시	계약기간 내	바이러스 정의 업데이트
McAfee Anti-Virus 2010	때에 따라 수시	계약기간 내	바이러스 정의 업데이트
Kaspersky Anti-Virus 2011	때에 따라 수시	계약기간 내	최신 DB 업데이트

3. 바이러스 유형에 따른 백신프로그램 성능비교

최근 많은 이슈가 되고 있는 북특정한 악성 코드를 대상으로 백신 프로그램의 성능을 시험한 결과 <표 5>와

같이 각각의 백신마다 차이가 있었다. 이는 바이러스 백신마다 중요하게 감지하는 악성코드 유형이 다르다는 점을 알 수 있다.

<표 5> 백신 프로그램들의 악성코드 감지결과

	Mega Run	Crack	Setup	Build	Botez	java2
V3	O	X	X	O	O	X
ViRobot	O	O	X	O	O	O
Symantec	O	O	O	X	X	O
MS Security Essential	X	O	O			O

주요 백신 프로그램의 엔진을 살펴보면 V3는 국내 백신 업체 중 유일하게 자체엔진을 사용하고 ViRobot은 자체엔진과 BitDepender 듀얼 엔진을 사용, 알약은 Bit Depender 엔진을 사용하고 있다. 외산 백신업체들은 모두 자기 자체 엔진을 사용하고 있다.

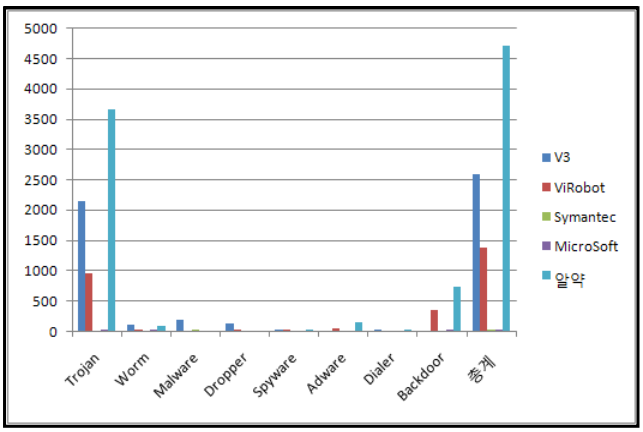
4. 시뮬레이션 결과

본 실험은 바이러스 및 악성코드 출현 시 여러 백신 프로그램들의 엔진 업데이트 주기를 알기 위해 4대의 VMware(가상머신)을 설치하여 각각의 머신에 V3, ViRobot, Symantec, MicroSoft, 알약 백신 프로그램을 설치하여 시간대 별로 업데이트를 실행하였다.

1시 이후 매 시간 마다 업데이트를 실행시켜 각 백신 프로그램의 DB 업데이트 및 주기를 파악 하였다. <표 6>은 DB 업데이트 내역을 수치로 정리한 표이며 이를 그림 1과 같이 그래프로 보여주고 있다. 수치상으론 국내 백신들이 해외 백신들보다 업데이트를 많이 하는 것을 확인할 수가 있다.

<표 6> 백신별 DB 업데이트 내역

	V3	ViRobot	Symantec	MicroSoft	알약
Trojan	2140	952		16	3668
Worm	107	20		3	96
Malware	193		9		
Dropper	128	13			
Spyware	1	3			25
Adware		48			140
Dialer	22				24
Backdoor		349		4	731
총계	2591	1385	9	23	4707



(그림 1) 백신별 DB 업데이트 내역

5. 결론

악성 프로그램은 그 종류에 따라서 다양한 형태가 존재하지만, 다른 프로그램 또는 운영체제에 접근하여 코드를 변경시키거나 정보를 추출하는 동작, 비정상적인 네트워크 패킷을 송수신하는 동작 등은 보안 프로그램으로부터 자신의 존재를 숨기기 위한 은닉 행위와 같은 일반적인 프로그램과는 다른 행동을 수행한다는 공통적인 특성을 가지고 있다.

본 논문에서는 여러 백신 프로그램들의 특징 및 엔진 DB(데이터베이스)의 업데이트 주기를 살펴보았다. 각각의 백신 프로그램들은 엔진 업데이트 시점이 모두 다르고 바이러스를 검출해내는 중요도 또한 다르다. 이에 따라 각각의 백신 프로그램 마다 정의한 바이러스가 달라 어떤 백신프로그램이 바이러스를 가장 잘 잡는다고는 볼 수 없지만 사용자들은 주로 하나의 백신 프로그램의 실시간 감시를 활성화하여 사용하고 PC의 바이러스 감염이 의심되면 각 백신 프로그램들의 DB 엔진을 파악하여 엔진의 특성이 다른 백신프로그램을 사용해 이중으로 바이러스를 검사하면 좀 더 완벽하게 차단할 수 있음을 입증하였다.

감사의 글

"이 논문은 2011년 교육과학기술부로부터 지원받아 수행된 연구임" (지역거점연구단육성사업/충북BIT연구중심대학육성사업단)

참고문헌

[1] 조은선, "악성 이동코드와 대응기법", 한국정보과학회지, 제20권, 제 11호, pp.17-23, 2002.

[2] 이성욱, 홍만표, "악성코드의 암호화 및 해독기법", 한국정보과학회지, 제20권, 제11호, pp.37-43, 2002.

[3] 김진, "사이버 침해에 대한 효율적인 대응방안 연구", 인천대학교 정보통신대학원 석사학위논문, pp.72-76, 2010.

[4] 조시행, "최근 악성코드 위협과 대응", 한국정보통신설비학회, 2009.