제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

개선된 악성 코드 분류지침 및 명명법에 관한 연구

곽효승*, 김판구*
*조선대학교 전자계산학과
e-mail:{robotsc, pkkim}@mina.chosun.ac.kr

A Study on the Advanced Classification and Naming Convention of Malicious Code

Hyo-Seung Kwak*, Pan-Koo Kim*
*Dept of Computer Science, Chosun University

요 약

국내외 각 백신업체별로 악성 코드의 분류 체계가 마련되어 있지만 각각의 백신업체별로 분류 체계가 차이가 있고 또한 도스 운영체제 때부터 사용한 분류 체계를 그대로 사용하여 현재의 악성 코드 분류와는 많은 차이를 보이고 있다. 이러한 백신업체들의 악성 코드 분류를 정확하게 분류하는 방법으로 본 논문에서 새로운 악성 코드 분류지침과 분류지침에 의한 명명법을 제안한다.

본 논문에서 제안한 분류지침을 토대로 안티-바이러스 산업 및 악성 코드 연구를 활성화시키는 정책 수립의 기초 자료로 사용할 수 있으며, 악성 코드 정보의 체계화 · 통합화 · 표준화 등에 기여할 수 있다.

1. 서론

인터넷 사용자의 급증으로 악성 코드(malware) 또한 기하급수적으로 늘어나고 있다. 이러한 악성 코드의 증가로 인하여 악성 코드별 분류와 명명이 필요하게 되었다.

현재 국내외의 백신업체들에서는 분류체계가 각각 마련되어 있다. 그렇지만, 백신업체들의 분류체계가 서로 틀리기 때문에 한 악성 코드에 대해서 여러 개의 분류가 나올 수 있다.

악성 코드 명명법 또한 각 백신업체의 악성 코드 분류체계에 따른 명명법이 있기 때문에 악성 코드의 명명도 각각 다르다.

각 백신업체들의 분류체계와 명명법은 예전의 도스 운영체제 때부터 사용하던 분류체계와 명명법을 사용하고 있다. 그래서, 현재의 악성 코드로 나타나는 것에 대해 악성 코드를 분류하기가 어렵다.

이러한 문제를 해결하기 위한 새로운 악성 코드의 분류지침을 제안하고, 이 분류지침에 의한 악성 코드 명명법을 제시하고자 한다.[1)]

본 논문의 구성은 2장에서 국내외 악성 코드 분류에 대해서 알아보고 3장에서는 백신업체들의 악성 코드 명명법을 알아본다. 4장에서의 새로운 악성 코드 분류지침과 악성 코드 명명법을 제안하고, 5장에서는 결론을 맺는다.

본 연구는 2002년도 한국정보보호진흥원 지원으로 수행되었음.

2. 국내외 악성 코드 분류

2.1 안철수연구소 악성 코드 분류

악성 코드의 종류는 [표 1]과 같이 악성 코드의 정의를 중심으로 대 분류로 나눈다. 이 대 분류에 의해 유형을 나눈다. 이 유형들은 대 분류에 중복되어서 표현된다.

[표 1] 악성 코드 분류 - 안철수연구소

종 류	유형
바이러스	윈도우파일, 도스파일, 부트, 부트/파일, 스크립트, 팜, 리눅스, 매크로
트로이목마	윈도우파일, 도스파일, 백도어, 스크립트
웜	윈도우파일, 도스파일, 스크립트, 매크로
가짜(Hoax)	가짜
조 크	조크
기 타	보안상 위험

2.2 (주)하우리 악성 코드 분류

악성 코드의 종류를 [표 2]와 같이 대 분류가 있고, 대 분류와는 상관없이 악성 코드가 수행되어 나

타나는 증상에 의한 분류로 나누어 분류하고 있다.

[표 2] 악성 코드 분류 - (주)하우리

대 분 류	증상에 따른 분류
매크로	하드포맷, 파일생성, 파일삭제, 파일감염, 메일발송, 정보유출, 화면출력, 시스템 정보 변경, 플래쉬 메모리 및 하드디스크 손상, 네트웍/시스템속도저하, 특정음 출력, 파일손상, 홈페이지 주소 변경, 하드디스크손상, 시스템비정상작동, FAT 파괴, CMOS 삭제, 섹터 삭제, 홈페이지 변경, 내용상 기제, 레지스트리 변경, 파일 파괴, 기본 메모리 감소,특정 포트 오픈, 메시지 박스 출력, 프로세스 종료, 윈도우 종료, 메시지 전송, 파일삭제 및 하드포맷, 감염 외 증상 없음, 확산 외 특별한 증상 없음, 특정 파일 겹쳐쓰기, 증상없음 등
스크립트	
도스	
가짜	
부트	
도스용 트로이 목마	
윈도우 트로이 목마	
윈도우 파일	
윈도우조크	
IIS 웜	
기타	

2.3 Wildlist 악성 코드 분류

WildList, Supplemental List, Frequency List로 구성되어 악성 코드 분류를 하고 있다. Wild List와 Supplemental List에서는 "+, -, *"를 표시하고 있다. "+"는 그 달의 새로이 보고된 악성 코드의 이름 앞에 붙인다. "-"는 그 달의 WildList로부터 Supplemental List로 내려온 악성 코드 이름 앞에 붙인다. "*"는 WildList와 Supplemental List에서 자주 나타나는 악성 코드 명 앞에 붙인다.

The WildList는 많은 협력자들, 최소한 두 명의 협력자에 의해 통보되고, 일정 지역이 아닌 전 지역에 걸쳐 발견된 악성 코드 명 목록이다.

Supplemental List는 특정 지역에서 자주 발생하지만 다른 지역에서 발견하기 힘든 악성 코드 명이고, The WildList로부터 이동한 악성 코드 명 목록이다.

Frequency List는 각 악성 코드에 대하여 상당히 많은 협력자들에 의해 보고, 저장되어진 The WildList이다.

2.4 Trend Micro 악성 코드 분류

[표 3]과 같이 Payload와 Type으로 악성 코드를 분류하였다.

Payload는 악성 코드가 시스템에 미치는 영향 또는 악성 코드로 인한 피해를 산출하기 위한 종류이다.

Type은 악성 코드의 형태이다. 즉, 운영체제 또는 파일의 종류 등에 의한 분류이다.

[표 3] 바이러스 분류 - Trend Micro

Payload	Type
Corrupts Hard Disk	ActiveX Control
	Backdoor
Creates Files	Batch File
	Boot
Deletes Files	Elf Executable
	File Infector
Displays Graphics	Html
	IRC Script
Displays Message	Java Applet
	Java Script
Formats Hard Disk	Joke
	Macro
Generates Sound	Shell Script
	Trojan
Hangs System	VB Script
	Visio 5
Modifies Files	VXD
	Worm
Others	Others

3. 국내외 악성 코드의 명명법

3.1 안철수연구소 악성 코드 명명법

악성 코드의 명명은 내부 문자열의 특징적인 증상을 기본원칙으로 한다. 변형 악성 코드의 경우 B, C 등을 덧붙여 사용한다. 악성 코드의 변형이 심할 경우 II, III등을 사용한다.

[표 4]는 안철수 연구소의 악성 코드 명명 방법을 표현한 것이다.

[표 4] 안철수연구소 악성 코드 명명법

접 두 어/	이 름	접 미 어
Win32/	Goner	worm

3.2 (주)하우리 악성 코드 명명법

"형태(Type).이름(Name).변형정도(A, B, ...).크기(Size)"의 형태로 악성 코드를 명명한다.

[표 5]는 (주)하우리의 악성 코드를 명명 방법을 표현한 것이다.

[표 5] (주)하우리 악성 코드 명명법

분 류	접 두 어	이 름
I-Warm/	Win32	Goner

3.3 (주)시만텍 악성 코드 명명법

"접두사.이름.접미사"의 형태로 악성 코드를 명명한다. 접두사는 악성 코드의 특성을 표현하고, 접미사는 악성 코드의 형태를 표현한다.

[표 6] (주)시만텍 악성 코드 명명법

접 두 어	이 름	변 형	접 미 어
W32	Goner	A	@MM

3.4 CARO 악성 코드 명명법

CARO(Computer Anti-virus Research Organization)는 유럽을 중심으로 한 안티 바이러스 단체이다. 이 단체에서는 1991년 악성 코드 명명규칙을 제정하였다. 악성 코드의 명명은 "Family_Name, Group_Name, Major_Varient, Minor_Varient" 으로 이루어져 있으며 각 부분은 '.'으로 구분한다.

4. 새로운 악성 코드 분류 및 명명법

2장의 악성 코드 분류 방법과 3장의 악성 코드 명명법을 살펴보았다. 여기서 악성 코드 분류는 악성 코드를 쉽게 분류할 수 없고 또한 한 악성 코드가 여러 곳에 중복 될 수 있는 문제점이 발생했다.

이러한 문제점을 해결하기 위해서 본 논문에서는 각 업체들의 악성 코드 분류지침을 바탕으로 새로운 악성 코드 분류지침을 제안하고, 분류지침에 의한 명명법을 제시한다.

4.1 악성 코드 분류지침

새로운 악성 코드들의 분류는 각각 악성 프로그램 정의, 운영체제, 감염영역(부위), 감염 경로, 악성 프로그램 증상 등의 5가지의 분류 형태로 악성 코드 분류 지침을 제안한다.

4.1.1 악성 프로그램의 정의에 의한 분류

악성 코드 형태에 의한 분류로 악성 프로그램이 다른 프로그램에 기생하는지, 또는 다른 시스템에 자기 복제를 하는지 등을 바탕으로 악성 프로그램을 정의하였다.

[표 7]은 악성 프로그램 정의에 의한 분류를 표현한 것이다.

[표 7] 악성 프로그램 정의에 의한 분류

대분류	정 의
바이러스	바이러스의 가장 큰 특성은 복제와 감염이라고 말할 수 있다.
웜 (인터넷 웜)	인터넷(또는 네트워크)을 통하여 시스템에서 시스템으로 자기복제를 하는 프로그램을 의미한다.
트로이목마(백도어)	트로이 목마 프로그램은 유틸리티 프로그램 내에 악의의 기능을 가지는 코드를 내장한다.
가짜 (Hoax)	Hoax 는 전자메일로 다른 사람에게 거짓 정보 즉 루머를 유포를 의미한다.
조크 (Joke)	조크는 트로이목마와 달리 악의적인 목적을 가지지 않고 사용자에게 심리적인 위협 혹은 불안을 조장하는 프로그램을 말한다.

4.1.2 운영체제에 의한 분류

컴퓨터를 운영하는데 여러 가지의 운영체제가 있다. 이 운영체제들에는 각각 다른 형태의 악성 코드들이 활동을 한다. 그러므로 각 운영체제별로 분류한다.

[표 8]은 악성 코드들이 어떤 운영체제에서 감염되는지에 따라서 분류한 것이다.

[표 8] 운영체제에 의한 분류

대분류	정 의
도 스	MS-DOS 기반에서 활동하는 일반적인 부트, 파일, 부트/파일 바이러스 또는 트로이 목마류
윈도우	MS 윈도우 기반에서 활동하는 바이러스 및 악성 프로그램들로 다음과 같이 윈도우 버전별로 구분될 수 있다.
Linux	리눅스 운영체제의 보안상 취약점을 이용하여 실행되는 악성 프로그램들
Unix	유닉스 운영체제의 보안상 취약점을 이용하여 실행되는 웜 종류들
Palm	Palm 운영체제에서 활동하는 트로이 목마 또는 단순한 겹쳐쓰기 바이러스
FreeBSD	아파치 웹서버의 취약점을 이용하여 전파되는 웜

4.1.3 감염영역(부위)에 의한 분류

악성 코드가 악성 행위가 실행되는 형태에 따라 악성 코드를 분류할 수 있다. 이 형태는 악성 코드가 감염되는 영역이 각각 다르므로, 각 영역별로 분류한다.

[표 9]은 악성 코드가 활동하는 영역에 따라서 분류한 것이다.

[표 9] 감염 영역(부위)에 따른 분류

대분류	정 의
파일 바이러스	일반적으로 실행 가능한 프로그램 파일에 감염, 윈도우에서는 다양한 형태의 실행 파일이 존재하므로 감염되는 파일 종류도 여러 가지임
부트 바이러스	부트 영역(주부트 섹터, 도스 부트섹터)에 감염되는 바이러스
부트/파일 바이러스	부트 영역과 파일을 동시에 감염시키는 바이러스
매크로 바이러스	MS 오피스의 매크로 기능을 이용하여 문서파일을 감염시키는 바이러스
스크립트 바이러스	자바 스크립트 및 비주얼베이직 스크립트로 작성된 웜 또는 바이러스

4.1.4 감염 경로에 의한 분류

윈도우에서 악성 코드가 발생하기 전에는 파일의 실행에 의해서만 악성 모드가 감염되었다. 그렇지만, 현재는 다양한 경로를 통하여 악성 코드가 전파되고 있다. 이렇게 다양한 형태로 전파되는 악성 코드들에 대하여 악성 코드에 의한 감염 경로를 분류로 분류한다.

[표 10]은 악성 프로그램이 감염되는 경로에 따라

서 분류한 것이다.

[표 10] 감염 경로에 의한 분류

대 분 류	정 의
파일실행	감염된 파일을 실행 시 감염되지 않는 다른 파일을 감염
다운로드 (FTP, 메신저)	대상을 다운로드 받고 사용자가 파일을 실행하면 감염
네트워크 (공유폴더)	랜덤 한 IP 대역을 스캐닝하여 읽기/쓰기 공유된 폴더나 드라이브 파일을 감염 또는 웜, 바이러스가 복사되는 방법
보안 취약성	IIS 웹 서버 취약성과 같이 특정 응용 프로그램이나 OS의 취약성을 이용하는 방법
메 일	MAPI 또는 SMTP 기능으로 메일을 통하여 전파되는 방법
부 팅	부팅에 의하여 기본 메모리가 바이러스에 감염

4.1.5 악성 프로그램 증상에 의한 분류

각 악성 코드들은 다양한 형태의 증상을 나타내고 있다. 이러한 형태의 증상들은 최근 들어 새롭게 발생하는 것들도 있고 예전부터 나타난 증상들이 있다. 이에 악성 코드들의 증상들을 중심으로 분류한다.

[표 11]은 악성 프로그램이 시스템에 어떤 형태의 증상을 나타내도록 하는지에 의한 분이다.

[표 11] 악성 프로그램 증상에 의한 분류

대분류	정 의
하드디스크관련	하드와 관련된 악성 프로그램의 증상을 보이는 것.
파일관련	바이러스가 특정 파일 또는 파일에 관련된 삭제, 겹쳐쓰기, 삭제 등의 증상을 보이는 것.
시스템관련	레지스트리 키 값을 변경에 의한 시스템 정보를 변경, 시스템의 FAT 파괴, CMOS의 내용을 변경에 의한 부팅 시 에러, 시스템 마비 등의 악성 프로그램에 의한 시스템 관련 증상.
네트워크관련	메일을 발송, 정보 유출, 네트워크 속도가 저하, 다른 PC로 메시지를 전송, 특정 포트 Open.
특이증상	메시지의 화면에 출력, 특정 음 출력 등.

4.2 악성 코드의 명명법

본 논문에서 제안한 악성 코드의 분류지침을 기반으로 하여 제시하는 전체적인 악성 코드의 명명 규칙은 크게 5부분으로 이루어져 있으며 각 부분은 '_'로 구분한다. 또한 두 가지 이상 항목은 '/'로 구분하여 연속 기입한다. 각각의 이름들은 쉽게 그 악성 코드의 정보를 파악할 수 있도록 명명한다.

[표 12]는 악성 코드의 명명방법을 표현한 것이다.

[표 12]는 악성 코드 명명법

정의에 의한 분류	운영체제에 의한 분류	감염영역에 의한 분류	감염경로에 의한 분류	증상에 의한 분류	악성 코드 이름
Worm	Win	File	Mail	HDisk	CHI

5. 결론

본 논문에서는 기존의 악성 코드의 분류지침 및 명명법을 보완하여 새로운 악성 코드의 분류지침 및 명명법을 제안하였다.

기존 백신업체들의 분류지침에서의 한 가지 형태로 분류지침을 제정하여 그 분류지침에 의해 표현하기에는 많은 모호한 악성 코드들이 발생했다. 이러한 악성 코드들을 본 논문에서 제안한 악성 코드 분류지침에 의해 분류를 하면 보다 쉽고 정확한 분류를 할 수 있다.

본 논문에서 제안한 분류지침을 토대로 안티-바이러스 산업 및 악성 코드 연구를 활성화시키는 정책 수립의 기초 자료로 사용할 수 있으며, 악성 코드 정보의 체계화·통합화·표준화 등에 기여할 수 있다.

참고문헌

[1] Evgeny Kasperksy, Vadim Bogdanov, "Virus Analysis 1", Virus Bulletin, April 1993, Pages 12~13.

[2] F.Fernandez, "Heuristic Engine", The 11th International Virus Bulletin Conference, 2001

[3] Yoshiteru Ishida "The Immune System as a Prototype of Autonomous Decentralized System : An Overview" Proceedings of the 3rd Int'l Symposium on Autonomous Decentralized Systems(ISADS'97), 1997, Pages 85~92.

[4] Sara Hedberg, "Combating Computer Viruses: IBM's New Computer Immune System", IEEE Parallel & Distributed Technology, 1996 Summer.

[5] Vesselin Bontchev, "Future Trends in Virus Writing", Virus Bulletin.

[6] http://www.ahnlab.com

[7] http://www.antivirus.com

[8] http://www.hauri.co.kr

[9] http://www.symantec.com

[10] http://www.zdnet.co.kr/biztech

[11] http://www.trendmicro.co.kr/

[12] http://www.virusbtn.com

[13] http://www.cyber.com/products/vfind/misc/vfind.html

[14] http://www.thewildlist.com/

[15] http://www.wildlist.org/