악성 프로그램의 기법 분석 및 동향(III)

황규범*, 조시행, 안철수

안철수연구소

Analysis Maclious Code Scheme and Current Status(III)

Kyu-beom Hwang*, Sihaeng Cho, Charles Ahn

Ahnlab, Inc.

요 약

본 논문에서는 컴퓨터 바이러스(이하 바이러스) 및 웜 그리고 트로이목마와 같은 악성 코드의 정의와 개념에 대해 기술하고, 2000년 11월부터 2001년 10월까지, 바이러스를 중심으로 한 악성 코드의 주요 기법을 분석하고 전반적인 바이러스 발견 동향 및 향후 전망에 대해 기술하고 향후 악성코드 대응 방법에 관한 연구 방향을 제시하고 논문을 맺는다.

I. 서론

최근에는 인터넷의 사용이 보편화되어, 때와 장소를 가리지 않고, 인터넷에 접속해 채팅이나 게임등을 즐기고 있는 사람도 많이 있다.

이전의 컴퓨터 악성코드들은 사용자가 자신의 컴퓨터에 감염된 파일을 다른 사람에게 전달하는 과정에서 악성코드가 전파되는 수동적인 양상을 보였으나 최근에는 보다 능동적으로 공유 폴더를 찾아 감염을 확산시키거나 사용자가 편지를 보낼 때 사용자 몰래 웜이나 바이러스를 첨부시켜 보내거나 혹은 사용자 모르게 사용자의 메일링 리스트에 있는 사람들에게 메일을 보내고, 더 나아가 누가 내 이름을 사칭하여 다른 사람들에게 메일을 발송하는등으로 발전하고 있어 그 피해는 점점 더 심각해지고 있다고 할 수 있다.

본 논문의 구성은 제 2장에서 바이러스 및 악성코드의 정의 및 구성 요소에 대하여 기술하고, 제 3장에서는 1998년부터 2001년 10월까지 국내에 발견된 바이러스들을 포하하는 악성 코드의 기법 특징을 분석하고, 제 4장에서는 최근 악성 코드의 주요 동향을 기술하며, 제 5장에서는 악성 코드에 대한 대응 방법에 대하여 기술하고 제 6장에서는 결론을 기술한다.

II. 악성 코드의 정의 및 구성

본장에서는 악성코드의 정의와 주요 구성 요소에 대해 기술한다.

1. 악성 코드의 정의

악성 코드는 일반적으로 제작자가 의도적으로 사용자에게 피해를 주고자 만든 모든 악의의 목적을 가진 프로그램 및 수행 가능한 매크로, 스크립트등 실행 가능한 형태의 모든 유형을 포함하여 정의한다.[2]

최근에는 심리적 위협을 주는 프로그램이나 메일 문서등도 악성코드 범주에 포함하고 있다.

본 고에서는 악성코드 이름은 구분을 위하여 이탤릭체와 밑줄을 사용한다.

2. 악성 코드의 구성

악성 코드의 주요 유형은 바이러스, 웜 그리고 트로이목마로 구성하고 있으며, 혹스(Hoax, 일명 가짜 바이러스), 조크(심리적 불안만 초래함)등이 포함되고 있다.

1) 컴퓨터 바이러스

바이러스는 1984년 Fred Cohen의 학위 논문, "Computer Viruses - Theory and Experiments"에서 새로운 보안 위협으로 소개가 되었으며 바이러스 정의는 다음과 같다.[1]

> We define a computer 'virus' as a program that *can 'infect' other programs by modifying them to include a possibly evolved copy of itself.* With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows.

바이러스는 감염 대상 프로그램(코드)에 자신(바이러스)의 코드 및 변형 코드를 감염시키며, 네트워크 및 컴퓨터 시스템에서 확산된다.

최근의 컴퓨터 바이러스들은 프로그램 중간에 함수를 가로채는 방식인 실행점불분명화기법(EPO, Entry Point Obscuring Scheme)과 다형성 기법을 사용하고 있으며, 스크립트를 이용한 바이러스가 꾸준히 나타나고 있으며, 고급언어로 작성되어 다양한 부작용을 가진 바이러스들도 나타나고 있다.[6]

대표적으로 국내에 처음 발견된 *뇌(Brain)*, 많은 피해를 준 *CIH(Win95/CIH)*, 메일을 통해 널리 확산되었던 *러브레터(VBS/Love Letter)*, 매크로 문서에 감염되는 *라루(XM/Laroux)*등이 있고 네트워크 공유 환경을 통해 광범위하게 확산되는 *펀러브(Win32/FunLove.4099)* 그리고 최근에 발견되어 확산된 *님다(Win32/Nimda)*등이 있다.

2) 웜

웜은 기억 장소에 코드 형태로 존재하거나 혹은 실행 파일로 존재하며 작동시 파일이나 코드 자체가 다른 시스템으로 감염된다.

1988년 널리 퍼져 피해를 준, 모리스웜을 시작으로 초기에는 유닉스 시스템에서만 감염되는 것으로 인식되어 왔으나, 1999년부터 윈도우 시스템에서도 널리 확산되고 있으며 최근까지 많은 피해를 주고 있다.

대표적으로 국내외에 처음으로 발견 확산된 *I-Worm/Happy99*, 컴퓨터의 파일을 삭제하여 문제가 되었던 *I-Worm/ExploreZip*, 암호키해독을 목적으로 분산시스템을 구현한 *I-Worm/Wininit* 그리고 최근에 중요 문서 유출이라는 치명적인 부작용을 가지며 널리 확산된 *Win32/Sircam.worm*등이 있다.

3) 트로이목마

트로이목마는 포괄적으로 정의하여 악의의 기능을 포함하는 프로그램이나 악의의 목적에 적극적으로 활용되는 프로그램등을 의미한다.

최근에는 인터넷 게임방과 같은 공유PC환경에서 키로그 프로그램 혹은 시스템 원격제어 서버등이 설치되어 있는 경우가 많아 피해가 우려된다.

대표적으로 시스템 원격제어에 활용되는 *백오리피스2000(Win-Trojan/Back Orifice.2000)*와 *넷버스(Win-Trojan/Netbus)*등이 있다.

4) 혹스(Hoax)

혹스는 주로 이메일을 통하여 다른 사람에게 거짓 정보 즉 루머를 유포하는 것으로 사용자에게 심리적인 위협이나 불안감을 조장한다.

혹스는 현재 대부분 백신에서는 진단 기능을 제공하지 않으나 해당 정보는 백신사 홈페이지를 통해 제공하고 있다.

5) 조크

조크는 심리적인 위협이나 불안감을 조장하는 프로그램으로써, 물질적인 피해는 없으나 백신에서 진단/삭제한다.

대표적으로 하드디스크를 포맷하는 화면을 보여주는 *Win-Joke/Format Game*이나 공포스런 얼굴을 작업중에 갑자기 나타나게 하여 놀라게 하는 고스트(*Win-Joke/Ghost*)등이 있다.

6) 유해 프로그램

유해 프로그램은 물질적, 정신적 피해는 없으나 사회 정의에 반하는 프로그램중 트로이목마와 조크로 분류하는데 어려움이 있는 경우로, 주민등록번호생성기, 신용카드번호생성기등과 같이 악의적으로 이용될 경우 다른 사람의 프라이버시를 침해하여 사회적 문제를 야기할 수 있어 백신에서는 진단하여 삭제 처리한다.

대표적 주민번호생성기(*Win-Trojan/Jumin*)이 있다.

III. 기법 특징

본 고의 단계 구분은 국내에 발견된 바이러스나 웜을 중심으로 하며, 서버가 아닌 PC클라이언트 상에서 나타나는 악성코드를 중심으로 연도별 구분을 하고 2000년 11월부터 다수 발생한 인터넷

웜, 스크립트 바이러스 그리고 윈도우 바이러스를 중심으로 기법 변화를 분석한다.

주요 특징으로 악성코드 제작에 고급언어가 사용되는 경우가 많아졌다라는 점과 이메일을 통한 확산, 네트워크 공유 환경을 통한 확산이 증가했다는 점이다.

표 1은 1988년부터 2001년 10월까지 주요 기법 동향을 정리한 것이다.

연도	주요 기법 동향
1988	부트 바이러스 출현
1989	파일 바이러스 출현
1990	부트/파일 바이러스 출현
1991	연결형 바이러스 출현
1992	외국 바이러스의 국내 변형
1993	간단한 다형성 암호화 바이러스 출현
1994	국산 암호화 바이러스 전성기
1995	다형성 바이러스 본격화
1996	매크로 바이러스 출현
	윈도우 바이러스 출현
1997	다형성 바이러스 기술적 발전
	윈도95/NT 바이러스의 출현
1998	원격제어 트로이목마 출현
1999	정보 유출 가능성을 가진 매크로 바이러스
	Win95/CIH에 의한 대규모 피해
	인터넷을 통한 웜의 확산
2000	윈도우 바이러스의 실행점불분명화기법
	VBA를 이용하는 스크립트 바이러스 출현
	DLL함수를 가로채는 윈도우 바이러스
	첨부 파일명을 변경하는 웜의 등장
2001	고급언어를 작성된 바이러스
	메일서비스를 이용하여 감염 확산
	중요 문서를 유출하는 웜의 등장
	타인명의도용 메일 발송 바이러스 등장

표 1. 1988~2001년 악성코드 주요 기법 동향

1. 첨부 파일명을 변경하는 웜

일반적으로 첨부 파일 형태로 확산되는 웜은 HAPPY99.EXE, ZIPPED_FILE.EXE, 등과 같이 파일명이 고정되어 있어 "HAPPY99.EXE로 첨부된 실행 파일은 삭제"등의 조치를 취할 수 있었다. 그러나 2000년 11월에 회오리로 유명한 *하이브리스(I-Worm/Hybris)*의 경우 첨부 파일명을 무작위로 명명하여 사용자들의 주의를 피해갔다.

또한 나비다드 웜의 경우에는 일반 사용자들이 첨부 파일에 대한 경각심이 높아짐에 따라서, 기존의 메일중에 첨부 파일이 있는 메일만 그 첨부 파일의 내용을 바꾸어 다시 발송한다. 이런 경우 메일의 내용에 첨부 파일이 있어 참조하라는 문구가 있는 경우가 많아 대부분 의심없이 실행하게 되었으며, 이로 인해 널리 확산되었다.

2. 고급언어로 작성된 바이러스

바이러스의 경우에는 다른 프로그램을 감염시켜 기생하므로 어셈블리를 사용하여 작은 크기로 작성하는 것이 일반적이었다.

그러나 최근에 확산된 *님다*의 경우 어셈블리가 아닌 C언어로 작성된 것으로 추정되고 있으며, 고급언어를 사용함에 따라, 다양한 외부 제작 라이브러리를 이용하여 메일을 통한 확산 및 네트워크를 통한 확상 기능이 어렵지 않게 구현된 것으로 추정하고 있다.

현재까지도 감염률이 높은 *CIH*의 경우 1KB정도의 크기였고, 기업이나 학교등과 같은 조직에서 높은 감염 및 확산률을 보이는 *펀러브*는 약 4KB 정도이며 이들 바이러스들은 어셈블리로 제작되었으며 감염방법이 *님다*처럼 다양하지 못하다.

3. 메일서비스를 이용한 감염 확산

과거에는 스크립트를 이용하거나 소켓라이브러리의 함수를 가로채 메일을 보내는 기법들이 사용되었으나 최근에는 MAPI(Microsoft Mail API)를 사용하여 SMTP(Simple Mail Transfer Protocol)를 악성 코드내에 직접 구현한 사례가 나타나고 있다.[7]

메일 서비스를 이용하여 악성코드를 확산시키는 경우 첨부 파일을 첨부하여 사용자의 관심을 통한 실수를 유발시켜 감염을 확산시키는 방법에서 러브레터와 같이 심리적인 유혹을 통하는 방법, 서캠과 같이 조언을 구하는 듯한 메일과 사용자가 호기심을 가질만한 문서에 웜을 붙여 첨부하는등 지능적으로 발전하고 있다.

그림 1은 메일을 보내는 방법의 변화가 주요 악성코드명을 기록한 것이다.

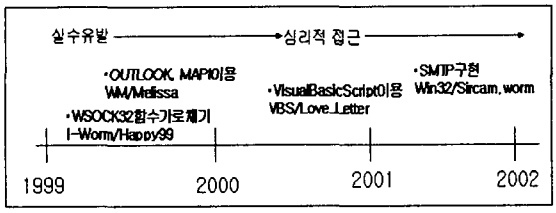

그림 1. 메일전파 악성코드의 주요 발전사

1) WSOCK32.DLL 함수 가로채기

윈도우기반의 인터넷 웜은 메일을 보내기 위하

여 그림 2와 같이 소켓라이브러리의 Send()함수를 가로채서 사용자가 메일을 보낼 때 자신이 자동으로 첨부될 수 있도록 하는 기법으로 1999년 2월 처음 발견되어 신년축하 불꽃 놀이를 보여주는 증상을 가진 *Happy99*와 회오리 화면으로 유명한 *하이브리스*가 대표적이다.[3]

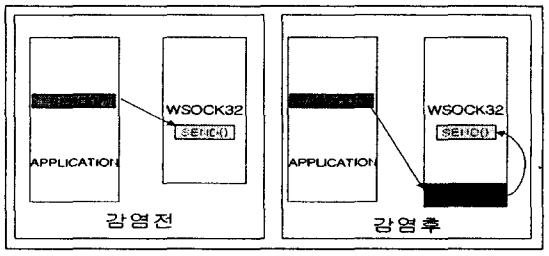

그림 2. Send()함수를 가로챈 형태

이 경우 웜이 능동적으로 메일을 보낼 수 없으므로 자동적인 확산 증상은 없었으나 지인(知人)으로부터 발송되는 메일에 웜을 첨부하여 별다른 의심없이 열어보게 되고, *Happy99*의 경우 즐거움을 주는 증상을 가지고 있어 일부 사람들은 보낸 사람을 고맙게 생각하며 반복해서 여러번 실행하고, 다른 사람에게 직접 디스크로 전해주는 등의 방법으로 확산된 웃지못할 경우도 있었다.

2) 스크립트 이용한 방법

이 기법은 오피스 제품군에 포함된 VBA, 비주얼베이직스크립트 그리고 자바스크립트등에서 아웃룩을 이용하여 메일을 발송하는 방법으로 그림 3와 같이 몇줄의 코드를 이용하면 메일을 발송할 수 있다..

```
set out=WScript.CreateObject ("Outlook.Application")
set mapi=out>GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists (ctrlists)
x=1
regv=regedit.RegRead ("HKEY_CURRENT_USER₩Software₩Microsoft₩WAB₩"&a)
if (regv="") then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv) ) then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries (x)
regad=""
regad=regedit.RegRead ("HKEY_CURRENT_USER₩Software₩Microsoft₩WAB₩"&malead)
```

그림 3. 러브레터의 메일발송 코드일부

그림 4는 악성코드가 포함된 메일을 메일클라이언트인 아웃룩을 이용하여 메일을 보내는 경우로 1999년 4월, 미국을 중심으로 큰 문제가 되었던 *멜리사(W97M/Melissa)*를 시작으로 2000년 5월 "ILoveYou"라는 이름의 메일이 전세계적으로 다량 유포된 러브레터에서 적용된 방법으로 최근에 발견되는 스크립트형 바이러스나 웜은 일반적으로 이 기법을 사용하고 있다고 볼 수 있다.

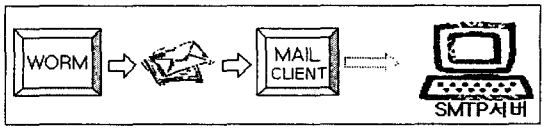

그림 4. 웜이 메일을 보내는 절차

국내에는 아웃룩보다 아웃룩익스프레스를 쓰는 경우가 많아 이 기법에 의한 피해는 다소 적은 편이다..

4) SMTP를 구현

지난 7월에 발견되어 지금까지도 크게 문제시되고 있는 *서캠(Win32/Sircam.worm)*의 경우 기존의 웜이나 바이러스들보다는 한단계 발전한 양상을 보여준다. 기존의 확산 기법은 웜이나 바이러스는 스스로 메일을 보낼수 없었다.

그러나 *서캠*에서는 SMTP를 구현한 라이브러리를 사용하고 있으며 이런 방법으로 미리 지정한 SMTP서버를 이용하여 사용자가 접속했던 사이트의 이메일 주소를 참조하여 불특정 다수에게 메일을 보낸다. 기존의 기법들은 경우 메일 클라이언트가 사용중이 아니거나, 설치되지 않은 경우, 혹은 웹 메일만을 이용하는 경우 사실상 감염이 확산되지 않았으나 *서캠*은 이러한 문제점을 모두 극복했다고 할 수 있다. *서캠*은 현재 델파이로 제작된 것으로 추정하고 있다.

이 기법은 그림 5와 같이 웜이 메일을 보낼 때 스스로 메일을 SMTP서버로 직접 발송하여 다른 사람에게 메일이 발송되도록 하였다. 이런 경우 메일 발송 기록이 남지않으므로 메일 유출 여부 및 유출지를 확인할 수 없어 더 치명적이다.

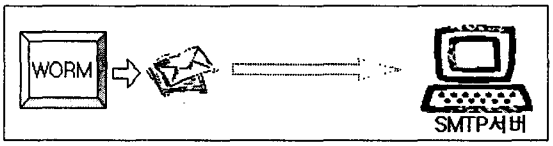

그림 5. 서캠의 메일보내는 절차

5) 타인명의도용 메일 발송 바이러스 등장

지난 9월에 발견된 *님다(Win32/Nimda)*의 경우 *퍼러브*와 *서캠*의 특징을 모두 가지고 있다. 가장 문제시 되는 부분은 서버의 홈페이지 관련 파일들이 *님다*에 감염될 경우 해당 홈페이지를 접속하는 사용자도 감염되게 된다는 점과 다른사람의 이메일주소를 도용하여 메일을 보낸다는 점이다.

*서캠*은 수신자주소만을 인터넷 캐시파일에서 찾아서 참조하는데, *님다*의 경우 발신자주소도 인터넷 캐시파일에서 참조하게 되므로 불특정 다수의 프라이버시가 침해될 수도 있으며, 기관의 경우 바이러스를 유포했다는 오해와 함께, 신뢰 문제가 발생할 수도 있다.

실제로 몇몇 백신사의 고객상담 이메일 주소 혹은 분석 담당자의 이메일 주소로 해당사 고객에게 메일이 발송되어 곤혹을 치룬 사례도 있다.[10]

IV. 주요 동향

최근 발생하는 악성코드의 주요 유형은 스크립트 바이러스, 윈도우 바이러스, 그리고 스크립트 및 윈도우 웜등이다.

2001년에는 Palm상에서 감염되는 바이러스가 발생하였으며 리눅스에서 작동한 웜이나 바이러스 등도 소개되고 있다. 이들은 아직 피해가 적고 널리 확산된 경우가 없어 아직은 크게 문제되지 않는다.[8][9]

그림 6은 최근 3년간 윈도우 기반의 바이러스 및 웜에 대한 발견 동향이다. 2001년이후 악성코드의 수는 줄었으나 피해 규모는 오히려 계속적으로 증가하고 있으며, *CIH*를 제외하면 큰 피해는 주로 2000년 말부터 2001년에 집중되어 있다.

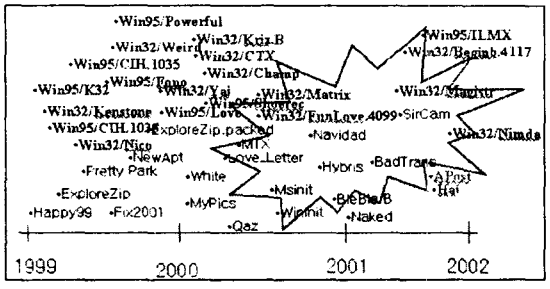

그림 6. 윈도우 바이러스 및 웜 발견 동향

윈도우 바이러스의 경우 2001년에 들어와서 눈에띄게 개체수가 줄었으나 *님다*, *퍼러브*, *CIH*, *Weird*등이 널리 확산되어 피해가 계속적으로 발생하고 있다.

웜의 경우 최근 3개년동안 그 개체 수가 적음에도 불구하고 널리 확산 되었으며 *서캠*과 같이 중요 문서 자료를 유출하는등의 부작용을 포함하기까지 발전하였다. 널리 확산되고 있는 주요 개체로는 *서캠*, *Wininit* 등이 있다.

최근의 주요 이슈를 보면 개인간 혹은 조직간 신뢰의 문제가 발생하는 경우가 나타나고 있다.

서캠 웜의 경우 불특정인에게 중요 문서를 유출시키는 위험을 가지고 있었고, *님다*의 경우 발신자 이름을 바꿈으로써, 최악의 경우 백신 회사나 공인기관이 바이러스를 유포했다는등의 오해를 살 수 있어 주의가 요구된다.

V. 대응방법

최근에는 인터넷 홈페이지를 통해서 감염되거나 이메일에 첨부된 멀티미디어스트림으로 위장하는 등 교묘해지고 있어 기본적으로 백신을 사용하지 않으면 악성 코드에 대한 대응이 어렵다.

백신을 사용함에 있어 중요한 것은 최신 엔진 업데이트를 수행해야 한다는 점이고, 백신은 일반적으로 발견후 조치이므로 처음 발견후 일정시간 후에 백신이 발표된다. 따라서 신속한 대응을 위해서는 정부나 백신회사에게 제공하는 정보를 이용하여 자신이 할 수 있는 적극적인 조치를 취할 수 있어야 한다.

특히, 메일의 경우 그림 7과 같이 첨부된 파일에 대한 등록정보를 보아, 문서 파일인데 파일 형식에 다른 정보가 나타나는등 이상점이 발견되면 열어보지 않아야 하며, 백신을 이용하여 점검한다.

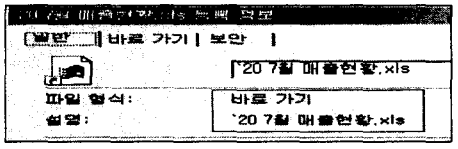

그림 7. 감염된 XLS문서의 등록정보

그림 8은 정상적인 경우로, 위의 경우와 달리 원래 문서의 확장자(.xls)가 엑셀 문서임을 보여주고 있다.

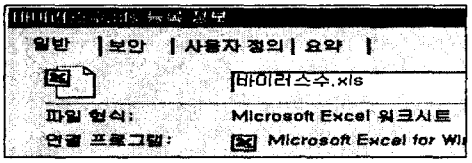

그림 8. 정상 XLS 문서의 등록정보

앞에서의 차이는 이중 확장자 사용에 기인 것이다. 그림 7의 경우에는 실제 파일 명은"'20 7월 매출현황.xls.lnk" 이고 그림 8의 경우에는 "바이러스수.xls" 이다. 이런 기법은 이미 러브레터 때부터 이용되었다.

일반적으로 웜의 경우, 메일을 통하는 경우 일정한 양식을 가지는 메일로 확산됨으로 이를 아웃

룩의 "메시지규칙"등을 이용하여 메일 수신을 방지할 수 있으며, 감염되었다 하더라도, 웜 파일을 찾아 삭제하고, 레지스트리 정보를 수정하면 제거될 수 있다.[4]

그림 9는 아웃룩에서 메시지 규칙을 이용하여 서캠을 방지한 것이다.

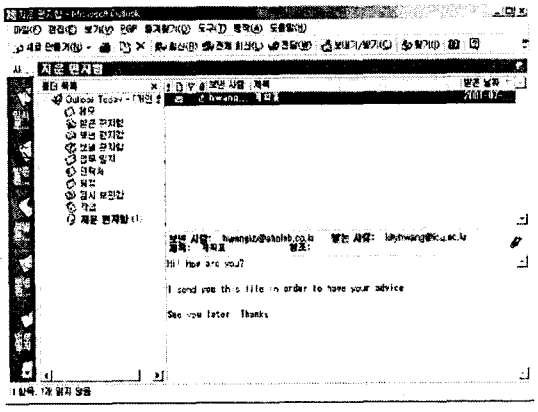

그림 9. 아웃룩의 메시지 규칙을 이용

VI 결론

본 논문에서는 바이러스, 트로이목마, 웜 그리고 조크와 혹스 및 유해 프로그램을 포함하는 악성코드의 변화된 개념을 기술하였고 과거 십수년간 국내에 발견된 바이러스를 중심으로한 악성코드들의 기술 동향을 요약하고 2000년 10월부터 2001년 10월까지의 악성코드의 주요 기법 변화와 주요 동향을 분석하고 그에 대한 대응 방법을 제시하였다.

최근에는 고급 언어로 작성된 바이러스들이 나타나고 있으며, 이들 바이러스들은 고급언어의 장점을 충분히 이용하여, 메일 및 공유 폴더를 이용하여 감염, 확산 방법이 일반화 되어 가고 있다.

2001년에는 악성 코드의 개체수가 많이 감소하였으나 *서캠*, *님다*, *머지스트르*등의 악성코드에 의한 피해가 크며 구종인 *CIH*, *퍼러브* 그리고 *Wininit*등도 그 피해가 계속되고 있다.

최근에는 서버의 공격이 강화되고 있어, 취약점 점검 및 보안을 포함하는 개념의 백신 제작 필요성이 대두되었다.

국내에서도 지속적으로 바이러스 제작을 시도하는 사람이 있으며 현재 실행점불분명화기법까지 적용된 바이러스가 이미 소개되었으며 이후 새로운 위협을 다가 올 가능성도 있다.

최근 인터넷의 일반화로 바이러스의 제작, 유포가 국경을 초월하여 여러 나라에서 동시 다발적으로 피해가 발생하고 있다. 따라서 이러한 피해를 예방하기 위해서는 정부, 언론 그리고 개발업체간 공조체제가 중요하다. 또한 지속으로 컴퓨터 이용자에게 바이러스 예방 교육과 예방을 위한 솔루션이 기본적으로 도입되어야 하며, 사용자도 보다 적극적인 대응과 주의가 요망되며 학계에서도 악성코드 대응 기술 연구, 개발에 관심을 가져야 할 것이다.

앞으로의 연구 과제는 웜이나 바이러스를 분석하기 위한 테스트 환경의 구축과 고급언어로 작성된 프로그램을 어셈블리 수준에서 분석할 수 있는 방법, 그리고 스크립트 바이러스에 대한 체계적인 대응 기술에 관한 것으로 최초 발견시와 진단 엔진 제작 완료시간간 차이를 최소화하기위한 업무 간소화 및 효율화에 대한 연구가 필요하다..

참고문헌

[1] F. Cohen, "Computer Viruses: Theory and Experiments", Computers & security, Vol. 6, pp. 22-35, February 1987.

[2] 황규범, 김광조, 안철수, "악성 프로그램의 기법 분석 및 동향(I)", 한국통신정보보호학회 종합학술대회(CISC'99) 논문집, 1999.

[3] 황규범, 김광조, 안철수, "악성 프로그램의 기법 분석 및 동향(II)", 한국통신정보보호학회 종합학술대회(CISC'2000) 논문집, 2000.

[4] 황규범, "메일클라이언트를 이용한 악성코드 유입 대응", EN-TM2001-02, 안철수연구소.

[5] 황규범, "현실로 다가온 정보전", EN-TM2001-03, 안철수연구소.

[6] 황규범, "최근 바이러스 기법 동향", 기무사 교육 강의자료, 2001.8.

[7] 황규범, 차민석, 최진영, "지겨운 'Hi! How are you?' 웜 때문에 인간관계 망친다", Sepcial Report, PCLINE 9월호, pp.332, 2001.

[8] John Stojanovski, Scott Molenkamp, "Palm OS: Problems And Potential Solution", Proc. of International Virus Bulletin Conference 2001, pp.135-145, 2001.

[9] Jakub Kaminski, "Not So Quiet On The Linux Front : Linux Malware II", Proc. of International Virus Bulletin Conference 2001, pp.147-167, 2001.

[10] 황규범, "님다 - 나를 누가 사칭하는데....", EN-TM2001-05, 안철수연구소.