악성 프로그램의 기법 분석 및 동향(IV)

황규범, 박현철*, 조시행, 안철수

안철수연구소

Analysis Malicious Code Scheme and Current Status(IV)

Kyu-beom Hwang, Hyuncheol Park*, Sihaeng Cho, Charles Ahn

Ahnlab, Inc.

요 약

본 논문에서는 컴퓨터 바이러스(이하 바이러스) 및 웜 그리고 트로이목마 등 악성코드의 명명법 차이를 설명하고, 2001년 10월부터 2002년 10월까지, 주요 악성 코드의 기법을 분석하고 전반적인 바이러스 발견 동향 및 향후 전망에 대해 기술하고 향후 악성코드 대응 방법에 관한 연구 방향을 제시하고 논문을 맺는다.

I. 서론

최근에는 저렴한 비용으로 사용이 가능한 ADSL 서비스 외에 신축 아파트의 초고속 인터넷 서비스의 기본 설치 등으로 인하여 어느 때보다 인터넷의 사용이 보편화되었다.

그리고 2002년 들어, 무선인터넷에 대한 관심과 무선 인터넷 상용 서비스가 나타나 저렴한 비용으로 때와 장소를 가리지 않고, 인터넷에 접속해 채팅, 게임 외에 인터넷 뱅킹, 사이버 증권 투자 등을 할 수 있게 되었다.

이러한 발전 속에서, 악성코드들은 기존보다 더 빠른 확산을 보이고 있다.

감염 경로로 지난해까지는 주로 네트워크 환경 혹은 메일 등이 이용되었으나 올해는 메신저 서비스 이용자의 증가로 인해, 악성코드가 조직 내로 침투할 수 있는 새로운 침투 경로로서 메신저가 부각되고 있다.

과거의 웜들은 메일 클라이언트의 주소록을 이용하거나, 사용자의 인터넷 웹 캐시 파일에서 주소를 추출하여 사용하므로 주소록을 사용하지 않는 경우나, 웹 메일을 사용하는 경우 감염 확산이 어려웠다. 그러나, 메신저의 경우 또래집단간 혹은 업무집단 내에서 많이 사용하고 있고, 메신저의 주소록을 이용하여 나를 가장하여 다른 사람에게 악성코드를 전달하므로 확산 가능성이 높다.

본 논문의 구성은 제 2장에서 악성코드 명명법을 설명하고 제 3장에서는 1998년부터 2002년 10월까지 국내에 발견된 바이러스들을 포함하는 악성 코드의 기법 특징을 분석하고, 4장에서는 최근에 나타나는 주요 악성 코드의 동향을 기술하며, 5장에서는 악성 코드에 대한 대응 방법에 대하여 기술하고 제 6장에서는 결론을 기술한다.

II. 명명 방법 차이

악성코드명을 명명하는 정책은 각 백신회사들이 모두 다르다. 이로 인하여 동일한 바이러스를 서로 다른 바이러스로 오인하는 경우도 있어 본 장에서 명명법을 간단히 정리한다.

악성코드의 명명은 여러 가지 방법이 있으나, 대표적으로 악성코드에 존재하는 문자열이나 특징적인 증상을 이용하는 경우가 많다.

확산이 큰 악성 코드의 경우 사용자의 혼란을 줄이기 위하여 이름을 통일하는 경우도 많으나 지역 차와 시차 등으로 그렇지 못한 경우도 간간이 발생하여, 사용자에 혼란을 초래하기도 한다.

명명 원칙은 비슷하나 그 표현 방법이 달라, 전혀 다른 악성코드로 오해하는 경우도 있다.

국내에서 주로 접할 수 있는 이름은 안철수연구소, 하우리, 시만텍, 트렌드마이크로 등에서 만들어진 이름들로 일반적으로 플랫폼, 이름, 분류 등으로 구성되어 있다. 또한 주요 악성코드는 백신사들간에 이름을 통일하여 사용하므로 거의 비슷한 이름들이 사용된다.

표 1. 명명 방법 차이

백신	이름	표준 양식
안철수연구소	Win32/Appix.worm Win32/Bootstap.worm	접두어/이름.접미어 분류/이름.접미어
하우리	I-Worm.Win32.Appix Win32.Bootstap	접두어.분류.이름 접두어.이름
시만택	W32.Appix.C.Worm,	접두어.이름.분류
트렌드 마이크로	WORM_BOOSTAP	분류_이름

[표 1]은 각 백신사간 명명법 차이를 보여주는 것으로 같은 악성코드 이름을 다소 다르게 표현하기도 하고 다른 이름을 사용하기도 한다. 이름이 Bootstap에서 Appix로 변경되어진 사례이다.

보통 [표 2]와 같이 플랫폼 내지 악성코드가 활동할 수 있는 환경을 표현하는 접두어, 바이러스를 제외한 웜이나 트로이목마 등의 악성코드 분류명을 표현하는 분류이름, 특별한 변환 형태나 손상 여부를 표현하는 접미어 등으로 구성하고 있다고 볼 수 있다.

표 2 명명법 주요 구성

	표현 단어
접두어	Win32(W32) Win95(W95) WinNT(WNT) Win2K(W2K) VBS JS HTML Script XM, X97M, WM, W97M
분류어	worm trojan joke WORM TROJ JOKE
파일 형태	demaged image eml html vbs
최종접미어	@mm @m

명명법은 다소 다르나 위의 표현 단어들을 각각 대체시키면 크게 어려움 없이, 각 백신사의 이름을 이해할 수 있을 것으로 보인다.[1]

III. 기법 특징

이 장에서의 단계 구분은 국내에 발견된 바이러스나 웜을 중심으로, 서버가 아닌 PC클라이언트 상에서 나타나는 악성코드를 연도별 구분을 하고 2001년 10월부터 다수 발생한 악성코드의 기법 변화를 분석한다.[2]

주요 특징으로 악성코드 제작에 고급언어의 사용이 일반화 되었다는 점과 이메일을 통한 확산, 네트워크 공유 환경을 통한 확산 외에 MSN메신저, P2P 자료 공유 등을 통한 확산이 증가하고 있다.

표 3은 1988년부터 2002년 10월까지 주요 기법 동향을 정리한 것이다.

표 3. 1988~2002년 악성코드 주요 기법 동향

연도	주요 기법 동향
1988	부트 바이러스 출현
1989	파일 바이러스 출현
1990	부트/파일 바이러스 출현
1991	연길형 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 실행점볶분명화기법
	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
	네트워크 공유를 이용한 악성코드
2002	취약점을 이용한 악성코드
	메신저를 이용한 악성코드 확산

1. 네트워크 공유를 이용한 악성 코드

2001월 9월 11일, 미국 뉴욕에 있는 무역센터 테러로 인하여 많은 사람이 희생되자, 미국은 아프카니스탄의 빈 라덴을 축출하기 위한 전쟁을 벌이고, 이 시점(10월 23일)에 반전 및 빈 라덴 지지 성향의 바이러스가 국내에서 처음으로 발견되었다.

이 바이러스의 특징은 ICQ사이트에서 가져온 사용자 이메일주소로 메일을 발송하며, 공유된 네트워크로 확산 가능하고, 아웃룩의 취약점을 이용하고 있어 일부 버전에서는 읽기 만해도 감염되며 메일 이름을 다양하게 선택한다.

아울러 감염 확산을 위하여 감염된 시스템의 C 드라이브 전체가 BinLaden이란 이름으로 공유 설정이 되므로, 제2, 제3의 바이러스에 감염될 수도 있다.

바이러스는 1/1365의 확률로 윈도우 화면을 아래와 같은 화면을 출력한다.

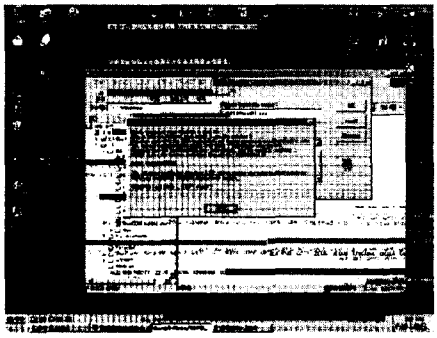

그림 1 AntiWar의 증상

2. 취약점을 이용한 악성코드

코드레드와 님다의 경우 IIS 서버의 버퍼 유니코드 처리 오류를 이용한 오버플로우 공격을 통하여 제이권을 얻는 취약점이 이용되었으며 공격은 지금까지도 시도되고 있다.

2002년 1월에 발견된 JS/Spida는 SQL 서버에 SA(System Administrator)의 암호가 설정되지 않은 경우에 1433포트로 SA로 로그인을 할 수 있는 취약점을 이용한 것으로 동년 5월 21일이후 급속히 확산되었다. 메일을 발송하기위한 프로그램들을 포함하고 있어 SQL서버의 정보가 유출되며, SA 암호가 임의로 설정된다.[3]

2001년 님다 이후, MIME에 멀티미디어 스트림을 가장한 실행형 악성코드를 첨부하여 아웃룩에서 자동으로 실행되게 하는 방법은 일반적인 전파 방법이다.

2002년 4월 발견된 클레즈.H(Win32/Klez.H)의 경우 클레즈 웜이 발전한 형태로 시스템간 복제뿐만 아니라 일반 실행 파일에 감염되는 엘컨(Win32/Elkern) 바이리스를 포함하고 있어 메일 및 네트워크 환경에서 감염이 이루어지고 과거의 이떠한 바이리스보다 빠른 감염 속도를 보였다.

클레즈의 경우 메일 제목과 발신자를 위장하며, 제목도 매우 다양하게 나타나며, 백신업체의 업데이트 파일임을 가장하기도 한다.

현재까지 전세계적으로 광범위하게 확산되고 있으며 실행중인 백신을 강제로 종료시켜, 제거에 어려움이 있었으나, 국내에서는 각 백신사의 적절한 대응으로 피해를 줄일 수 있었다.[4][5]

2002년 9월에 발견된 슬래피(Linux/Slapper.worm)는 리눅스 아파치 서버의 Open-SSL 취약점을 이용하여 소스 형태로 전파되고 시스템에서 자동으로 gcc를 이용하여 컴파일하게 하는 새로운 방법을 이용하였으며 국내에는 Open-SSL을 쓰는 경우가 적어 피해가 적었지만, 그만큼 보안 수준이 낮다는 오명을 얻기도 했다.[6]

슬래피는 바이리스 제작자들이 윈도우뿐만 아니라 리눅스에도 관심을 가지고 있음을 보여준 사례이다.

최근의 악성코드의 공격 기법은 OS 및 애플리케이션의 취약점을 이용한 경우가 많아, 어느때보다도 패치에 대한 정보 습득과 적용이 중요하다.

3. 메신저를 이용한 악성코드 확산

2001년 중반까지는 ICQ, mIRC등이 많이 사용되었으나 MSN메신저가 OS와 인터넷 익스플로러에 포함되면서 사용자가 폭발적으로 증가하여 지금은 메신저 유저의 상당수를 차지한다.

MSN메신저를 통해 확산되는 악성코드는 2001년을 이후로 꾸준이 나타나고 있고, 2002년에 들어와 악성코드 확산이 눈에띄게 증가했다.

MSN 메신저는 기본적으로 메시지 전송외에 파일을 전송할 수 있으며, 이는 사용자의 책임하에 실행하게 되이, 부주의한 사용으로 인한 피해가 발생한다.

2002년 2월 JS/Exploit.Mssenger의 경우 대화상대자에게 URL이 담긴 메시지를 발송하며, 해당 URL은 악의적 사이트로 안내할 수 있어, 제2 제3의 공격이 가능함을 보여주었다.[7]

7월에 발견된 Win32/Supova.worm 의 경우 [그림 2]와 같이 파일 형태로 전송되며 파일명을 몇가지로 변경하여 사용자를 속인다.

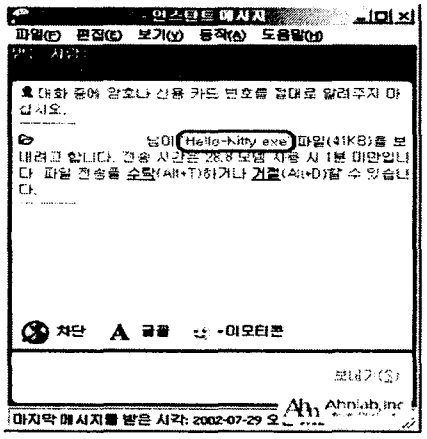

그림 2 Supova웜이 전송된 모습

10월에 급속히 확산된 Win32/BR2002.worm의 경우도 [그림 3]같은 메시지를 전송한다. BR2002의 경우도 트로이목마를 포함하고 있는데, 향후 백오리피스와 같은 원격제어 툴도 포함될 수 있으며, 해당 시스템의 권한 설정을 무력화할 수 있는 프로그램등이 포함될 수 있을 것으로 보인다.

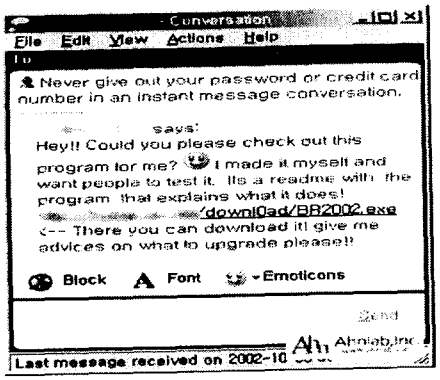

그림 3. BR2002 웜이 전송된 모습

메신저의 경우 사용자에게 실행 선택 권한이 있어, 주의만 한다면 충분히 막을 수 있으며, 지인(知人)으로부터 파일이 전송되고 메시지 제목이 위장된다면 매우 빠른 확산 속도를 가질 것으로 예측되어 더욱더 관심과 주의가 필요하다.

일반적으로 백신은 악성코드가 실행 혹은 저장될 때 차단하므로, 알려진 바이러스의 전송 및 실행을 차단하는 것은 어렵지 않다.

IV. 주요 동향

최근에는 발견되는 악성코드의 개체가 감소하였고, 직접적인 자료 피해나 유출과 같은 심각한 증상을 가지는 악성코드의 수가 감소하여, 전체적인 피해는 감소한 것으로 보인다.

2002년의 특징은 클레즈H에서 보았듯이 악성코드가 발전하여, 웜의 특징을 가진 복잡한 형태의 바이러스가 나타나고, 확산속도도 기존의 악성코드에 비해 매우 빠르다는 특징을 가진다. 하나의 바이러스가 또 다른 바이러스를 가지고 있고, 인터넷 익스플로러의 리모트 쓰레드로 동작하여 공유된 파일을 감염시키므로, 네트워크 환경을 이용하는 기업이나 학교의 피해가 크다는 특징을 갖는다.

발생하는 악성코드의 주요 유형은 윈도우 웜과, 윈도우 바이러스가 주종을 이루고 있으며, 스크립트와 매크로 바이러스도 꾸준히 나타나고 있다.

2002년에는 네트워크 외에 MSN 메신저가 악성코드의 주요 확산경로 역할을 하고 있고, 닷넷 프레임워크에서 동작하는 바이러스가 소개되었으며, 64비트 윈도우XP가 발표되어 새로운 유형의 악성코드가 다수 출현할 것으로 보인다.

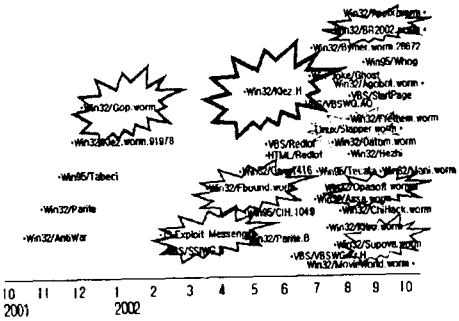

그림 4. 주요 악성코드 발견동향

[그림 4]는 2001년 10월부터 2002년 10월까지의 바이러스와 웜의 발견 동향으로, 넘다 이후에는 별다른 특이한 바이러스가 나타나지 않다가 2002년 4월 클레즈 바이러스의 피해가 컸으며, 7월 이후 악성코드의 발견이 크게 증가하고 있음을 알 수 있다.

2002년에 들어와 피해를 준 악성코드는 JS/Exploit-Messenger, Win32/Fbound.worm, Win32/Klez.H, Win32/Supova.worm, Linux/Slapper.worm, Win32/Opasoft.worm, Win32/BR2002, 등이 있으며 점차 피해가 확산될 것으로 최근에는 Win32/Parite.B의 감염 피해가 크다.

2002년 7월 이후 웜의 출현이 잦아지고 있으나 자료 유출이나 자료 파괴와 같은 직접적인 피해 증상이 없는 경우가 많아, 사용자들의 경각심 덕분에 악성코드로 인한 피해가 줄어든 것으로 보인다.

향후, MSN 메신저를 통한 악성코드 확산 및 P2P 자료 공유 소프트웨어를 통한 확산이 일반화될 것으로 보여 주의가 요구된다.

V. 대응방법

최근에는 악성코드의 발전으로 인하여 개인이 대응하기에는 어려움이 많다. 따라서 최신의 백신을 이용하여야 하고, 취약점이 있는 시스템을 보완하며, 불필요한 네트워크 권한을 삭제하는 등의 관리가 필요하게 되었다.

백신을 사용함에 있어 중요한 것은 최신 엔진으로 정기적인 업데이트를 수행해야 한다는 점이고, 백신은 일반적으로 발견 후 조치이므로 처음 발견 후 일정시간이 지나야 백신이 발표된다. 따라서 신속한 대응을 위해서는 정부나 백신회사에서 제공하는 정보를 이용하여 자신이 할 수 있는 적극적인 조치를 취할 수 있어야 한다.

또한, MSN 메신저와 같이 잘 알고 있는 사람과의 친분을 기반으로 하는 네트워크로 악성코드가 유입될 경우 급속히 확산될 가능성이 높고 매우 큰 피해가 우려된다. 메신저를 통해 파일이 전

송될 경우 수신 여부를 묻게 되는데, 보낸 사람에게 파일 전송 여부를 확인한 후 수신하는 것이 좋다.

메일의 경우에는 [그림 5]와 같이 메일의 등록정보를 확인하여 문서파일임에도 파일 형식이 다르게 나타나는 등 이상한 점이 발견되면 열어보지 않아야 하며, 백신을 이용하여 점검하는 것이 좋다.

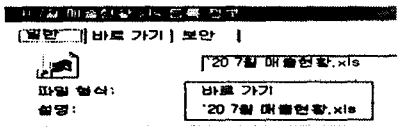

그림 5. 감염된 XLS문서의 등록정보

그림 6은 정상적인 경우로, 위의 경우와 달리 원래 문서의 확장자(.xls)가 엑셀 문서임을 보여주고 있다.

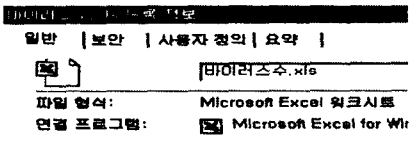

그림 6. 정상 XLS 문서의 등록정보

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. 일반적인 시스템에서는 두 번째 확장자가 생략되며, 이런 점은 리브레터 때부터 이용되어왔다.

이중 확장자로 인한 피해를 줄이기 위해서는 [그림 7]과 같이 탐색기의 폴더 옵션에서 "알려진 파일 형식의 파일 확장명 숨기기" 기능을 제거하여 숨김 파일을 볼 수 있도록 함으로써 악성코드에 의해 생성된 파일들을 확인할 수 있도록 하는 것이 좋다.

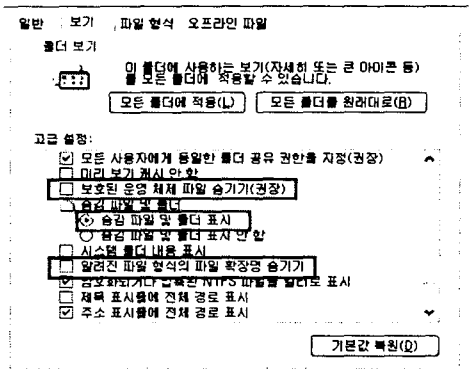

그림 7 탐색기의 폴더 옵션

최근에는 메일의 제목을 계속 변경하여 감염 메일을 발송하는 웜들이 많이 확산되어, 모르는 사람으로부터 전송되었거나 제목이 특이한 경우 주의를 요한다.

VI 결론

본 논문에서는 악성코드들의 명명원칙과 과거 십 수년간 국내에 발견된 바이러스를 중심으로 한 악성코드들의 기술 동향을 요약하고 2001년 10월부터 2002년 10월까지의 악성코드의 주요 기법 변화와 주요 동향을 분석하였으며, 그에 대한 대응 방법을 제시하였다.

최근에는 고급 언어로 작성된 악성코드들이 일반화되었고, 다양한 프로그래밍 기법들이 많이 소개되어 과거와 달리 메일을 보내거나 네트워크 자원에 접속하는 방법을 구현하는 것이 어렵지 않다. 따라서 중요 악성코드에 대한 정보를 수시로 열람하면서 대응 능력을 키우는 것이 보다 중요한 시기라고 할 수 있다.

전체적으로 2002년에는 악성 코드의 개체수가 많이 감소하였고 클레즈 외에는 큰 피해를 준 경우가 없으나 7월 이후 꾸준히 증가하고 있어 주의가 요망된다.

또한 예전에는 클라이언트가 주요 공격 목표였으나 IIS서버에서 SQL서버 및 OpenSSL을 공격하는등 취약점을 이용한 공격 방법이 많이 나타나고 있어, 취약점이 확인되면 바로 보안 패치를 수행하여 취약점을 보완해야 한다.

최근 인터넷의 일반화로 바이러스의 제작, 유포가 국경을 초월하여 여러 나라에서 동시 다발적으로 피해가 발생하고 있고, 복잡한 방법으로 은폐하는 경우도 있어 주의가 필요하며, 지금은 다소 소강상태이지만 지속적인 관심과 투자가 필요할 것으로 보인다.

앞으로의 연구 과제로, 악성코드에 대응하기 위한 전문 인력 양성과 일반 사용자들이 쉽게 이해할 수 있는 교육 자료 및 교육 커리큘럼, 교육 방법에 대한 연구가 필요할 것이며, 원천 기술을 보유한 몇 안되는 국가로써 국가 경쟁력 확보를 위한 지속적인 관심이 필요하다.

참고문헌

[1] 황규범, "컴퓨터 바이러스 분석", 아주대학교 정보통신대학원, 강의자료.

[2] 황규범, 김광조, 안철수, "악성 프로그램의 기법 분석 및 동향(III)", 한국통신정보보호학회 종합학술대회(CISC'2001) 논문집, 2001.

[3] 전자신문 2002년 5월 22일 기사, "SQL 서버 감염시키는 트로이목마 국내 확산"

[4] 디지털 타임즈, 2002년 4월 19일 기사, "메일 열기만해도 감염되는 클레즈H 바이리스 경보"

[5] 디지털 타임즈, 2002년 9월 4일 기사, "8월

바이러스 출몰순위 클레즈 변종 1위"
[6], 전자신문, 2002년 10월 10일 기사 - "슬래퍼 바이러스 국내 서버 피해 미미, 원인은 수준 낮은 탓"
[7] 조선일보, 2002년 2월 7일 기사 - "인터넷 메신저도 '웜' 표적"
[8] 중앙일보, 2002년 1월 10일기사 - "'한자 e-메일 조심하세요' 중국산 바이러스 확산"
[9] 전자신문, 2002년 10월 14일 기사, - "중국 컴퓨터 80%가 바이러스 감염"