제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

소빅 웜을 통한 웜 발전동향

박재우, 김원호
국가보안기술연구소

요 약

2003년 초, 소빅 웜이 발견되었다. 이후 계속적인 변종이 발견되었으며, win32.sobig.F는 많은 피해를 야기하였다. 또한 간단하게 수정된 변종 웜들(넷스카이 웜과 베이글 웜의 경쟁적인 변종 웜)의 출현으로 심각한 피해가 예상된다. 본 논문에서는 소빅 웜과 변종 웜들을 분석하고 이를 중심으로 향후 발생할 악성코드의 발전 동향을 미리 예측하여 1.25 인터넷 대란과 같은 사고를 예방하고자 한다.

Worm evolution trend through Sobig worm variant

JaeWoo Park, WonHo Kim
National Security Research Institute

ABSTRACT

In early 2003, a worm called Sobig was found. Later, many of its variations were found, and win32.Sobig.F caused the most serious problems. This kind of simply modified worms (including those caused by the "war" between Netsky vs. Beagle Worm) will be expected to cause many more problems. In this paper, we analyze the Sobig Worm and its variations. We, further, design a method that can expect future directions of modifications. We believe this will prevent serious loss such as we experienced on Jan 25.

1. 서 론

웜[1]은 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램을 말하며, 네트워크를 통해 연결된 다른 컴퓨터에 침투해 감염시킨다. 웜은 단순히 자기 복사 및 전파 기능을 가진 프로그램으로 결과적으로 막대한 시스템 과부하를 일으킨다는 점에서 바이러스를 능가하는 피해를 야기한다. 웜은 확산 속도가 바이러스에 비해 빨라 단시간 내에 네트워크에 치명타를 입힐 수 있다.

웜이 처음 알려진 것은 1988년 11월 발생한 '모리스 웜(morris worm)'[2]사건으로, 유닉스 시스템을 통해 전파되는 프로그램이 퍼지면서 수천 대의 서버 시스템이 정하는 등 혼란이 일어났다. 2003년 1월 초에 소빅 웜이 발견된 이후로 계속적인 변종이 발견되어 미국과 캐나다의 철도, 항공망에 상당한 타격을 가한 것으로 확인되었다.

소빅 웜의 경우 제작자가 동일인으로 추정이 되며 그 동안 얻은 지식을 바탕으로 웜의 기능을 계속 확장 및 버그를 수정하여 배포하는 것으로 보인다. 현재 또다른 강력한 변종을 제작하고 있을지 모르며 이에 대해 보안 전문가들이 이메일을 대량으로 발송하는 소빅 웜의 변종이 소빅.F가 마지막으로 끝나지 않을 것이라고 경고하고 있다. 소빅 웜은 감염된 PC에 스팸메일을 무작위로 대량 살포하는 동작을 실행시키도록 고안돼 있어 소빅 웜에 감염된 수만 대 PC의 사용자들은 자신도 모르는 사이에 추적 불가능한 이메일을 발송하도록 악용될 수 있다[3]. 본 고에서는 소빅 웜을 통해 향후 웜의 발전 동향을 알아보고자 한다.

2. 소빅 웜의 공통적인 특색[4]

지금까지 발견된 소빅 웜 변종은 다음과 같은 공통적인 특징을 가지고 있다.

■ 메일 주소 획득

로컬 컴퓨터를 검색하여 DBX, HLP, MHT, WAB, HTML, HTM, TXT, EML 확장명을 가지는 파일을 찾아 메일주소를 추출하는 방법을 사용하고 있다.

■ 웜 실행 압축

소빅 웜은 TELOCK 실행압축방식을 사용하여 웜의 자체 크기를 최소화하고 백신 제작자의 웜 분석을 어렵게 하기 위해 사용한다.

■ 자체 SMTP 전송

일반적인 웜은 릴레이 서버를 미리 지정하여 전송을 하는 방법을 취하기 때문에 이 서버에 대해 접속이 차단될 경우 확산이 어려운 결함이 있지만, 소빅 웜에서는 자체적인 메일 전송 기능을 통해 더욱 확산이 빠르게 가능하였다.

■ 악성코드 다운 및 실행

소빅 웜의 모든 변종이 가지고 있는 기능으로 윈도우 WIN32 API 인 UrlDownloadToCacheFileA 함수를 이용하여 제작자가 미리 서버 리스트를 지정해 둔 서버에 접속하여 제작자의 명령이 담긴 파일을 전송 받은 후, 제작자의 명령대로 지정된 파일을 다운받아 CreateProcess 함수를 호출하여 프로세스를 생성한다.

■ 웜 자동 실행 기능

윈도우에 다음과 같이 일반적으로 많이 쓰이는 레지스트리 등록 부분과 사용자 프로필 시작 메뉴에 등록하여 리부팅 시에도 지속적인 웜의 활동이 가능하게 한다.

- HK_CU\Software\Microsoft\Windows\CurrentVersion\Run
- HK_LM\Software\Microsoft\Windows\CurrentVersion\Run
- Windows\AllUsers\Start Menu\Programs\StartUp
- Documents and Settings\All Users\Start Menu\Programs\Startup

■ 웜 중복 실행 및 복사 방지

제작자는 웜의 중복 실행으로 인한 시스템

속도 저하를 방지하고 웜의 확산을 효과적으로 하기 위해 MUTEX와 EVENT를 생성시켜 중복된 웜 이름의 프로세스 생성을 막는 기능을 사용한다.

소빅 웜은 2003년 1월 초에 발견된 이후 2003년 8월 중순까지 6종이 발견되었다. 이 기간동안 제작자는 기존의 버그를 수정하고 새로운 기능을 추가하여 변종을 제작·시험하면서 기능 향상을 꾀하였다.

3. WIN32.Sobig.F 웜 변종의 특징[5][6]

2003년 여름에 발견된 Sobig.F 웜은 지금까지 발견된 것 중 6번째 버전으로 가장 큰 피해를 입혔다. 이 웜 변종은 다음과 같은 특징을 가진다.

■ NTP 프로토콜을 이용한 시간 동기화

일반적으로 웜 감염자의 컴퓨터 내부 시간은 다를 수가 있으며 지역에 따라 역시 다르다. 공개된 표준 시간 서버에 접속하여 시간 동기화를 통해 정확한 시간 계산 및 동작이 가능하였으며 기존의 웜/바이러스와 가장 큰 차이점이다.

■ 서버 리스트를 통한 악성코드 다운 및 실행

변종 모두가 지니고 있는 특성으로, 처리 방식은 조금씩 다르다. 초기 변종에서는 웜 본체에 특정 서버의 주소와 다운받을 파일명을 내장하였다. 따라서 백신 개발자가 웜에 대한 분석이 끝난 즉시 해당 파일 및 서버 차단이 가능하여 피해를 줄일 수 있었다. 6번째 버전에서는 서버 리스트를 통해 접속하여 제 3의 사이트에서 다운 받는 방식을 사용하여 추적이 어렵고 제작자가 의도한 효과가 극대화 될 수 있도록 하였다.

■ 발신자 주소 조작

이전의 웜과는 다른 특성으로 정확한 감염자를 판별하기가 어렵다. 일반 백신 제품군에서는 발신자 주소를 바탕으로 감염 여부를 통보해주는 방법을 취하는데 이러한 웜의 특성으로 인해 오히려 백신 제품군이 스팸에 이용되고 시스템에 과부하를 가져오는 현상을 가져왔다.

■ 자체 웜 확산 중지

2번째 버전 이후에 나타나는 공통적인 특성으로 특정 날짜가 되면 자가 소멸하여 계속적인 증식을 막는다.

■ 제작자와 통신 채널 오픈

웜 제작자 또는 다른 감염된 컴퓨터로부터 명령을 받으면 해당 파일을 다운받게 하는 기능으로 다운받는 파일이나 접속을 추적하기가 상당히 어렵다. 또한, 자체 웜 업데이트 기능도 있다.

■ 메일 주소 수집

웜이 메일 주소를 수집하는 DBX, HLP, MHT, WAB, HTML, HTM, TXT, EML 파일들은 사용자가 쓰는 주소록과 기타 웹 사용 시 발생되는 파일로서 사용자가 접속한 사이트나 불특정 대상을 목적으로 한다.

위에서 언급한 특징 중 가장 큰 특징은 웜이 사용하는 서버 리스트는 웜 본체에 XOR 비트 연산을 통하여 하드 코딩되어있다는 점이다. 따라서 일반 문자열 분석기법으로는 웜 분석이 어려우며 실행 시 메모리 덤프를 통해서만 분석이 가능하다. 이 서버 리스트에 있는 컴퓨터는 미국, 캐나다, 한국에 있었으며 주로 ADSL 을 사용하는 일반 컴퓨터로, 이 컴퓨터 사용자들은 자신의 컴퓨터 감염 사실도 모른 체, 웜의 확산에 도움이 되는 역할을 한 것으로 보인다. 이미 제작자는 Sobig.C 변형에서 www.geocities.com의 세 군데 폴더에서 암호화된 파일을 다운받아 실행하는 방법을 사용한 적이 있었는데, 이 때 백신업체에서는 웜 샘플을 분석하여 웜이 특정

파일을 다운받는 사이트에서 해당 파일을 분석한 뒤 해당 사이트에 요청을 하여 파일 삭제 및 서버 폐쇄를 요구함으로써 피해를 줄일 수 있었다.

그 후, 제작자는 6번째 웜에서 배포된 웜 본체에 서버리스트를 포함시켰고, 이 리스트를 참조하여 별도의 인증과정을 거쳐 파일 또는 새로운 명령을 다운받아 실행하도록 구조를 변경하였다. 이에 대하여, 백신업체 및 보안 업체에서는 해당 호스트의 접속 및 공개된 NTP 서버와의 접속을 모두 차단하는 대응을 통해 피해를 줄일 수 있었다. 만약 웜 간에 서버리스트를 교환하는 방식을 도입하였다면 더 큰 위험이 있을 것으로 판단된다.

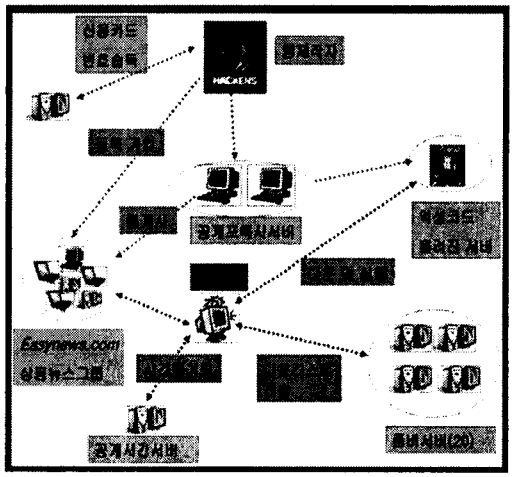
4. TELOCK 압축방식

소빅 웜에서 사용하고 있는 TELOCK는 TMG 라는 해커 그룹에서 제작한 EXE, OCX, DLL등의 실행파일을 압축하는 방식이다. TMG 그룹에서는 자기들이 제작한 크랙 프로그램의 용량을 줄이고 패치, 변조, 디버깅, 역어셈블러를 피하기 위한 용도로 사용하였다. TELOCK는 다음과 같은 특징을 가진다.

- 실행 파일의 .RELOC 부분을 완전히 제거하여 실행 파일의 크기를 감소시킬 수 있다.
- 패치, 디버깅, 역어셈블러, 압축해제 등의 방법을 피할 수 있다.
- 윈도우 환경에서 쉽게 사용할 수 있다.
- 파일 형식인 PE(Portable Executable)부분을 최적화 시키며 체크섬, 배열 등을 바꿀 수 있다.
- 공개 버전과 개인 버전, 베타버전 등 다양한 버전의 형식이 존재하며 압축 방식이 전부 달라서 해독이 어렵다.
- 소프트아이스와 같은 디버깅 도구 동작 및 추적을 탐지하면 프로그램 실행을 중지시키는 동작을 하여 추적 불가능하게 만든다.
- 다형성 암호 체계로 해독을 어렵게 만든다.
- EP(Entry Point) 부분을 사용자 정의로 지정이 가능하다.

5. 웜 배포 추적

소빅 웜이 배포된 경로를 추측해보면 다음과 같은 추론이 가능하다.



(그림 1) 소빅 웜의 배포 추적

웜 제작자는 익명성을 획득하기 위해 다양한 방법을 사용하였다. 웜 제작자는 타인의 신용카드 번호를 습득하고 자신의 아이피를 숨기기 위해 훔친 신용카드를 이용하여 상용성인뉴스그룹에 가입하고 공개 프록시 서버를 통해 웜이 첨부된 글을 뉴스그룹에 게재한 것으로 파악되었다.[7][8]. 일반 뉴스그룹 사용자의 호기심을 자극하여 악성코드가 올려진 서버로부터 웜을 다운받아 실행되어 확산된 것으로 추정된다.

6. 향후 웜 발전 동향예측

현재 발견되는 웜이나 악성코드의 동향을 보면 향후에는 다음과 같은 형태의 악성코드가 출현 할 것으로 예상된다.

■ 사용자 정보 수집

사용자의 민감한 정보(제품등록번호, 신용카드번호 등)를 수집하는 기능을 가진 웜이 확산될 것으로 우려된다.

■ 취약성과 결합

취약성이 발표된 이후 보안 패치가 발표되기까지의 공백 기간에 해당 취약점을 이용하는 웜의 출현이 증가할 것으로 보인다. 실제로, 슬래머 웜과 블래스트 웜의 경우, 마이크로소프트 제품군의 취약성을 이용하고 있어 단시간에 많은 시스템을 감염시켜 큰 피해를 가져왔다. 향후에도 이러한 양상은 계속될 것으로 보인다.

■ 다양한 감염매체를 통한 확산

기존의 웜의 경우 실행파일(exe, scr, com 등)의 확장명을 가지고 있어 대부분의 사용자는 실행파일이 첨부된 메일에 대해서 주의를 기울이고 있다. 향후에는 실행파일이 아닌 첨부문서, 예를 들어 self-executing HTML 등을 이용하여 메일을 열어보기만 하여도 감염되는 웜이 출현할 것으로 예상된다. 또한, 웹사이트를 방문하기만 해도 감염되도록 제작되어 웹브라우저를 공격 매체로 삼거나, 공유 폴더, P2P서비스를 이용하는 등 다양한 매체를 이용하여 확산되는 웜이 나타날 것으로 예측된다.

■ 보안프로그램 공격

최근 들어서는 백신, 방화벽과 같은 보안프로그램을 직접적으로 공격하는 악성코드가 많이 발견되고 있다. 이들 악성코드는 주로 프로세스 목록을 참조하여 보안프로그램을 공격하며, 향후에도 이러한 경향이 계속 될 것으로 예상된다.

■ 사회공학 공격 방법을 이용하는 웜

최근, 사회공학적으로 사용자를 속이는 방법을 이용하는 웜의 피해가 많이 증가하고 있다. 전자메일이 보편화 된 현재 많은 사용자를 확보하고 있는 웹사이트의 주소로 위장하여 사용자 정보를 훔치거나 웜 전파의 매개로 삼는 사회공학공격이 향후에도 증가할 것으로 보인다.

7. 결론

본 고에서는 큰 피해를 야기하였던 소빅 웜을 분석하고, 향후 출현할 웜의 특징을 예측해 보았다. 앞으로도 이러한 특징을 갖는 새로운 악성코드가 계속 제작 배포될 것이고 이에 따른 피해도 급증될 것이다. 이에 대응하기 위해서는 기술적 대책의 마련과 함께 사용자의 보안의식도 한층 높아져야 할 것으로 판단된다.

참고문헌

[1] Roger A. Grimes, Malicious Mobile Code August, 2001.

[2] Simon Garfinkel and Gene Spafford , Practical UNIX and Internet Security 2th , April , 1996

[3] Security & Privacy Magazine, IEEE , Volume: 1 Issue: 4 , July-Aug. 2003 Page(s): 58 -59

[4] Bergeron, J.; Debbabi, M.; Erhioui, M.M.; Ktari, B., Enabling Technologies:The making of a spam zombie army. Dissecting the Sobig worms, Infrastructure for Collaborative Enterprises, 1999. (WET ICE '99) Proceedings. IEEE 8th International Workshops on , 16-18 June 1999 Page(s): 184 -189

[5] http://www.f-secure.com/v-descs/sobig_f.shtml
[6] http://home.ahnlab.com/smart2u/virus_detail_1087.html
[7] http://www.vnunet.com/News/1143114
[8] http://www.securityfocus.com/news/6810

박 재 우

1999년 경북대학교 무기재료공학과(공학사)
2001년 경북대학교대학원 컴퓨터과학과(공학석사)
2000년~ 현재 국가보안기술연구소 연구원

김 원 호

2002년 한동대학교 전산전자공학부(공학사)
2004년 포항공과대학교대학원 컴퓨터공학과(공학석사)
2004년 ~ 현재 국가보안기술연구소 연구원