악성코드 실행과 은닉을 위한 다중 압축 연구

이정훈* · 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

A Study of Multiple Compression for Malicious Code Execution and Concealment

Jeong-Hoon Yi* · Dea-Woo Park*

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

E-mail : *yyyjjhh@paran.com · *prof1@paran.com

요 약

최근의 악성코드는 백신에 쉽게 탐지 되지 않기 위해 바이러스를 압축파일로 변조시켜 악성코드 패턴을 지연하는 추세이다. 시중에 나와 있는 수많은 백신엔진 중에서는 압축파일로 변조된 악성코드 패턴 및 검사가 가능한지 알아 봐야한다. 본 논문은 다중 압축 파일로 위장 변조된 은닉된 악성코드의 패턴을 검사하여 검출되는지를 검사 엔진을 통해 모의실험을 한다. 은닉된 악성코드의 행위를 분석하며, 호스트 파일 변조와 시스템 드라이버 파일 감염 및 레지스트리 등록이 되는가를 분석한다. 본 연구를 통해 은닉형 악성코드의 검사와 백신 치료 효과를 강화시켜 악성코드로 인한 피해를 감소하는데 기여할 것이다.

ABSTRACT

Recently, the malicious code is not easily detectable in the vaccine for the virus, malicious code as a compressed file by modulation pattern is the tendency to delay. Among the many antivirus engines on the market a compressed file that can be modulated by malicious code, and test whether the pattern will need to know. We cover a multi-compressed files, malicious code modulated secreted by examining patterns of test engine is being detected is through a computer simulation. Analysis of secreted activities of malicious code and infect the host file tampering with the system driver files and registry, it gets registered is analyzed. this study will contribute hidden malicious code inspection and enhance vaccine efficacy in reducing the damage caused by malicious code.

키워드

Malicious Code, Concealment Technique, Multiple Compression Technique, Vaccine Engine

Ⅰ. 서 론

2009년에는 네트워크와 관련된 악성코드 이슈가 많았다. 그림 1처럼 2009년 7월 7일부터 시작된 7.7 DDoS (Distributed Denial Of Service) 공격 사건은 기존 방식이 아닌, PC를 감염시키는 악성코드를 이용하여 예약된 시간에 타겟 리스트를 공격하는 방식을 사용했고, 정보를 유출하고 하드디스크를 파괴하는 등 해커의 공격이 진화 된 악성코드의 위험성을 일깨워 주었다[1].

또한 전 세계적으로 악명을 떨친 컨피커 웜(Win 32/Conficker.worm)은 윈도우 취약점 및 관리목적의 공유폴더 등의 다양한 공격경로를 활용하여 개인 및 기업 네트워크를 전방위적으로 위협하였다.

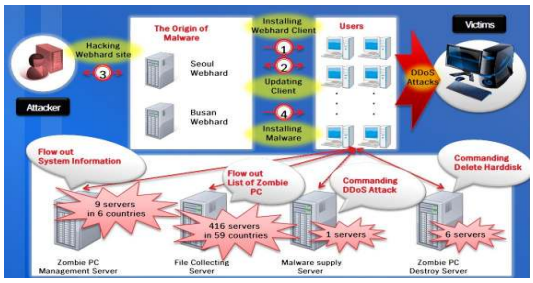

그림 1. 7.7 DDoS 인터넷 공격 분석[2]

2008년에는 워드, 엑셀 등 오피스 프로그램의 취약점이 발견되고 Acrobat Reader(PDF), Flash Player(Flash) 등의 어도비(Adobe)사의 프로그램 취약점들이 위협적인 악성코드로 발전되었다[3].

정상적인 문서에 악성코드를 은닉시킨 후 지인으로 가장하여 국가기관의 공직자 등 특정인들에게 유포시켜 PC에 저장된 중요 자료들을 빼내가는 범죄가 지속적으로 발생하고 있다[4].

본 논문은 최근 악성코드 동향과 피해사례를 통하여 악성코드 피해를 조사하고, 은닉형 악성코드와 다중 압축형 악성코드 검사를 하고, 악성코드 진단 및 치료 프로그램을 사용하여 모의실험을 실시하고, 호스트 파일 변조, 시스템 드라이버 파일 감염, 레지스트리 등록에 관한 은닉 악성코드 행위 분석을 한다.

II. 관련연구

2.1. 최근 악성코드 발생 동향

2010년 3월 KISA에서 탐지하여 대응한 악성코드 유포 및 경유사이트는 371건으로 전월 대비 93.2% (192→371건) 증가하였다. 악성코드 유포 및 경유지로 악용된 사이트를 기관별로 분류하면 기타(개인)(46.4%), 기업(42.0%), 비영리(7.3%) 홈페이지 순이었으며, 국외 유포지 사이트 탐지 증가로 기타 부분이 증가하였으며, 국내 경유지의 경우는 기업으로 분류된 co.kr, com 도메인이 악성코드 경유사이트로 많이 악용 되었다. 해커가 일반 이용자의 접속이 많은 기업 사이트를 주로 악성코드 경유사이트로 악용하고 있다

2010년 최근 MS IE 신규 취약점을 이용한 스팸메일 전파가 확인 되어, DDoS 공격 등 불법적 행위를 수행하는 악성코드 변종이 지속적인 것으로 파악된다[5].

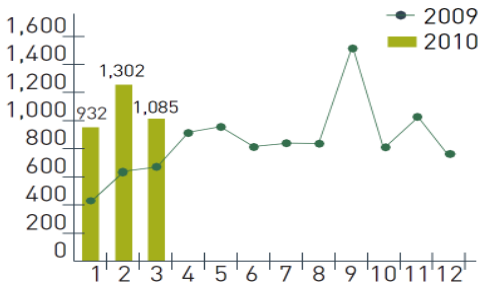

그림 2. 월별 침해사고 통계

그림 2는 2010년 월별 침해사고 통계를 2009년 월별 침해사고와 비교한 그래프이다.

2.2. 악성코드 피해사례

■ 사회적인 이슈를 악용한 악성코드의 유포

- 2008년 3월 "이명박 대통령 순방일정" 이라는 제목의 해킹메일 피해가 확인되었다. 해당 메일의 첨부 파일 "대통령 출국일정.xls"에는 Excel 프로그램의 취약점을 공격하는 코드가 삽입되어 있다. 이미 패치 된 Excel 사용자가 해당 파일을 열어볼 경우 악성코드에 감염되며, 감염 후에는 키보드 입력유출, 사용자 화면유출, 공격자 원격로그온 등의 피해가 발생한다. 이와 마찬가지로 2009년에도 마이클 잭슨 사망, 오바마 美대통령 당선, 前대통령들의 연이은 서거 등 국내□외적으로 사회적인 이슈가 많이 발생하여 인구에 회자되었다[9].

■ 악성코드 대량생산을 위한 자동화된 도구의 이용

- 2008년 넷봇(NetBot)을 이용하여 DDoS 에이전트를 손쉽게 제작할 수 있는 도구가 개발되고, 2009년 "풍운"이라는 DDoS 공격도구가 인터넷에 공개되어 분산서비스거부공격에 악용되었다. 이 두 가지 도구는 사용자 인터페이스(UI)를 제공하여 손쉽게 이용할 수 있는 기회를 제공하였고 기존의 악성코드 제작을 위해 소요되는 시간을 단축시켜 대량 생산을 가능하도록 환경을 조성 하였다. 변종 악성코드의 출현 주기가 짧아져 이에 대한 대응시간의 지연을 초래하였다.

■ 악성코드 정보의 인터넷 공유

- 2009년 11월 아이폰 악성코드가 한달 사이에 3종이 발생한 것도 한때 최초 아이폰 악성코드의 소스코드가 공개 되었던 것에 기인한 것으로 판단된다. 인터넷 전화감청 바이러스(SkypeTrojan)도 공개된 적이 있어 향후 인터넷 상의 무수한 악성코드 정보를 활용한 변종 발생 가능성이 높아졌다.

■ ActiveX 취약점을 악용한 악성코드 전파

- 2009년 7월 MS社에서 비디오 스트리밍 ActiveX 관련 취약점에 대한 보안공지를 발표하였다. 해당 취약점은 Data속성에 입력된 gif 파일의 크기를 처리하는 과정에서 버퍼오버플로가 발생하는 것으로 취약한 ActiveX 호출 스크립트로 구성되어있는 웹 사이트와 악성코드를 원격 시스템에 업로드하고 해당 페이지를 유명 웹 사이트 혹은 게시판에 iframe을 이용하여 삽입한다. 피해자가 해당 페이지에 접속할 시 취약한 msvidctl.dll은 쉘코드를 실행시키고 원격지에서 악성코드를 다운로드 및 실행하는 방식으로 전파된다.

III. 은닉 악성코드 검사와 실행

3.1. 은닉형 악성코드

2009년에 발견된 스팸 봇은 은폐기법과 자기보호가 고도화 되었다. 또한 시스템 파일을 감염시켜 존재하기 때문에 진단과 치료가 더욱 더 힘들다. 은폐기법과 자기보호 고도화와 관련하여 특이한 악성코드가 많다. TDSS와 TDL3로 불리어지는

해당 악성코드가 있다. 이 악성코드는 부트 바이러스나 MBR Rootkit처럼 사용 하지 않는 디스크 영역에 자신의 코드를 숨겨두고 활동한다. 일반적으로 이 영역은 확인 할 수 없기 때문에 악성코드는 찾기가 더 힘들다[6]. 특히 이미지파일을 이용한 은닉형 악성코드인 gif, jpg 등 일반적인 이미지 파일은 파일 첫 부분에 헤더가 위치하고 나머지 부분에 데이터가 위치한다. 따라서 데이터가 위치하는 정상적인 이미지파일의 마지막 부분에 악성코드를 삽입하면 이미지 파일의 손상 없이 악성코드 은닉이 가능하다[7].

3.2. 다중 압축(위장)형 악성코드

실행 압축 기법을 이용하면 보다 작은 크기의 저장 공간을 점유하면서 원래의 실행 파일과 같은 기능을 하는 또 다른 실행 파일을 만들 수 있다. 최근의 많은 악성 코드들은 실행 압축 기법을 이용하여 파일 크기를 줄여 악성 코드들의 전파 속도를 빠르게 하고 있다. 실행 압축은 ZIP, RAR과 같이 데이터를 하나로 묶어 놓은 압축과 달리 대상이 실행할 수 있는 파일을 압축하는 것으로 압축을 해제하는 과정 없이 바로 프로그램을 실행할 수 있다. 또한 WildList의 자료에 따라 92% 이상의 악성 코드가 실행 압축 혹은 암호화되어 있다고 조사 되었고, 많은 악성 코드들이 실행 압축 기술과 함께 암호화 기법을 사용하여 분석을 더욱 어렵게 만들고 있다[8].

3.3. 악성코드 실험 환경

악성코드 실험을 아래와 같이 실험 환경을 구성하였다.

■ 시스템
- CPU : Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz
- OS : Microsoft Windows XP Professional
- RAM : 512MB
- HDD : 40GB

■ 백신프로그램
- V3, Kaspersky, Norton

3.4. 악성코드 모의실험

악성코드 샘플 142개(50MB)을 V3, Kaspersky, Norton을 이용하여 모의실험을 하였다.

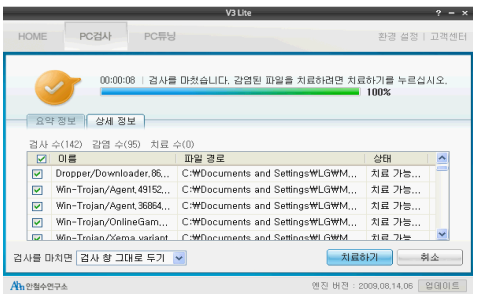

그림 3. V3 악성코드 모의실험

그림 4. Kaspersky 악성코드 모의실험

그림 5. Norton 악성코드 모의실험

그림 3과 같이 V3는 악성코드 142개중 95개가 발견 되었고, 그림 4와 같이 Kaspersky는 악성코드 142개중 133개가 발견 되었다. 또한 그림 5처럼 Norton은 악성코드 142개중 68개가 발견 되었으며, Kaspersky(94%) > V3(67%) > Norton(48%)의 악성코드 발견율 결과가 나왔다.

Ⅳ. 은닉 악성코드 행위 분석

4.1. 호스트 파일 변조

악성코드에 의한 호스트(hosts) 파일에 대한 변조는 대부분 Blackhole 라우팅 기법으로 알려진 안티 바이러스 및 보안 관련 홈페이지나 호스트에 대한 접근을 차단시킨다. hosts 파일 변조는 시그니쳐 진단을 회피할 목적으로 생성 된 것으로 본다.

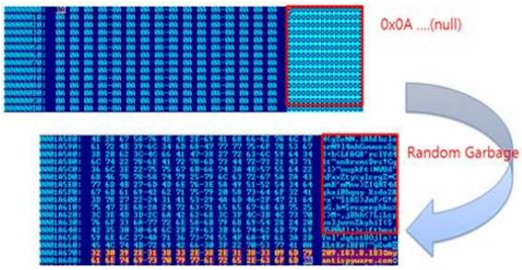

그림 6. 변조된 hosts 파일 형태[10]

그림 6처럼 hosts 파일시작은 0x0A 값으로 채

워진 형태 (텍스트 편집기에서는 null 보임)이다. 이 크기는 일정하지 않다. garbage data 역시 생성 될 때 마다 random 하기 때문에 변조된 hosts 파일은 시그니쳐 진단으로는 1:1 진단밖에 되지 않는다. 변조된 hosts 파일을 만들어내는 악성코드는 IRCBot으로, 자신을 유저모드(user mode)로 은폐하여 동작을 한다. 그리고 자신의 중요한 코드 대부분은 Explorer.exe 와 같은 윈도우 중요 프로세스에 인젝션 한 후 동작을 한다.

4.2. 시스템 드라이버 파일 감염

윈도우 시스템 드라이버 파일을 감염 시키는 악성코드가 cdrom.sys 파일을 대상으로 감염시켰다. 지금까지 대상이 되었던 시스템 드라이버 파일은 Ntfs.sys, Ndis.sys, Agp440.sys, Cdrom.sys 이다. 감염된 파일의 외형은 그림 7과 같다.

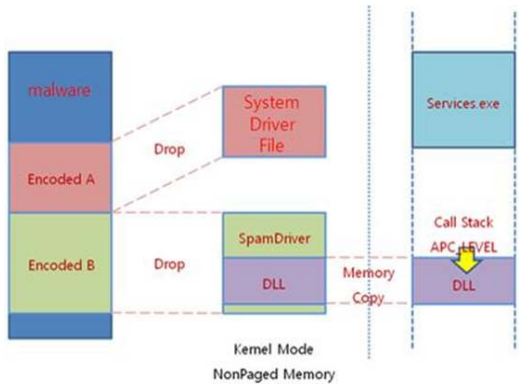

그림 7. 감염된 드라이버 파일 구조와 실행[10]

정상 드라이버 파일은 악성코드의 마지막 섹션에 암호화 되어 저장된다. 악성코드가 로드 될 때 이 부분을 복호화 하여 정상 드라이버 파일을 메모리에 로드 하면서 동작 한다. 이때 정상 드라이버와 스팸 메일을 보내는 다른 모듈도 함께 동작하도록 되어 있다. 파일 상으로는 존재 하지 않고 Services.exe 에 코드를 삽입하여 동작 하도록 한다.

4.3. 레지스트리 등록

Win-Trojan/Autorun.153321은 윈도우의 자동실행 기능을 이용하여 전파하며, 악의적인 행동을 수행하는 트로이 목마이다. 해당 트로이 목마가 실행되면 특정 폴더에 url[1].htm, 윈도우 프로그램 파일 폴더\microsoft shared\msinfo\에 zrpacinr.sys, zrpacinr.dll, zrpacinr.drv, zrpacinr.log등 루트킷 드라이버와 후킹서비스를 생성하는 파일들을 생성하고 레지스트리에 등록하여 윈도우 시작 시 자동으로 실행되게 한다.

Ⅴ. 결 론

악성코드를 이메일이나 그림, 동영상 등에 보이지 않게 은닉하여 해당 자료를 열 때 같이 실행되도록 하는 방법으로 피해자의 정보를 탈취하거나 좀비PC로 만들어 공격에 사용하는 해킹기법은 발견하기 어려운 공격 중 하나이다.

본 논문에서는 최근에 발생하는 악성코드 동향과 악성코드 피해사례 분석을 바탕으로 은닉형 악성코드와 다중 압축형 악성코드를 만들어 시스템에 감염시킨 후 V3, Kaspersky, Norton의 백신 프로그램을 사용하여 모의실험을 하여 감염 사실을 확인하였다. 이러한 악성코드 행위를 분석한 결과 변조된 hosts 파일 형태를 확인하고, 시스템 드라이버 파일 감염은 마지막 섹션에서 이루어지는 것을 확인하고, 루트킷 드라이버와 후킹서비스를 생성하는 파일을 생성하고 윈도우 자동시작 레지스트리에 등록 되는 것을 확인하였다.

향후 연구로는 은닉된 악성코드와 변종된 악성코드에 대한 백신의 검사와 치료기능을 강화하여 악성코드 은닉 여부를 점검하는 백신 프로그램의 기능 향상을 위한 연구가 필요하다.

참고문헌

[1] 안철수연구소 제품기획팀, "안철수연구소 DDoS 공격 방어 사례 -7.7 DDoS 대란 분석 보고서", 안철수연구소, 2009. 07. 16.

[2] Tai M. Chung, "The Need for International Collaboration in Computer Security", ISCR2009 발표자료, 2009. 09. 16.

[3] 김지훈, "진화하는 악성코드 기법, 트위터도 뚫었다", AhnLab 칼럼, 2010. 03. 19.

[4] 양경철, 이수연, 박원형, 박광철, 임종인, "전자우편을 이용한 악성코드 유포방법 분석 및 탐지에 관한 연구", 한국정보보호학회논문지, 제19권 제 1호, 2009. 02.

[5] 한국인터넷진흥원, "인터넷 침해사고 동향 및 분석 월보", http://www.krcert.or.kr, 2010. 03.

[6] ASEC연구원, SiteGuard연구원, "ASEC REPORT", 안철수연구소, Vol. 12, p.10, 2009.

[7] 박일형, 서승우, "이미지 파일을 이용한 악성코드 은닉기법 분석 및 해킹 예방대책에 관한 연구", 대한전자공학회 하계학술대회, pp.235-236, 2009. 07.

[8] 박남열, 김용민, 노봉남, "우회기법을 이용하는 악성코드 행위기반 탐지 방법", 한국정보보호학회논문지, 제 16권 제 3호, pp.17-28, 2006. 06.

[9] 한국인터넷진흥원, "인터넷 침해사고 동향 및 분석 월보", http://www.krcert.or.kr, 2009. 12.

[10] ASEC연구원, "ASEC REPORT", 안철수연구소, Vol. 3, 2010. 04.