韓國 컴퓨터情報學會 論文誌
第11卷 第5號, 2006. 11.

2006-11-5-2-11

DLL injection 기법을 이용하는 악성코드의 새로운 치료 방법 연구

박 희 환*, 박 대 우*

A Study on New Treatment Way of a Malicious Code to Use a DLL Injection Technique

Hee-Hwan Park*, Dea-Woo Park*

요 약

개인 정보의 탈취에 필요한 악성코드는 Phishing, Pharming메일, VoIP 서비스를 이용하는 Vishing, 모바일 금융을 위장한 SMiShing 등에 이용되어진다. 악성코드의 삭제나 치료는 앤티바이러스나 스파이웨어 제거 프로그램을 사용한다. 그런데 DLL Injection 기법을 이용하여 기생 동작하는 악성코드는 윈도우 운영체제에서 반드시 실행되어야 하는 프로세스인 lsass.exe, winlogon.exe, csrss.exe와 연계되어 있어 치료가 되지 않는다. 사용자가 바이러스의 치료를 위하여 임의로 프로세스를 강제 종료하려 한다면, 운영체제 시스템 전체가 리부팅이 발생하거나 블루 스크린이 발생한다. 본 논문에서는 치명적인 결과를 발생하는 DLL Injection 기법을 이용하는 악성코드를 치료하는 새로운 치료방법을 제안한다. 새로운 치료를 위한 Thread에 종료함수를 임의로 삽입하고 Thread를 제어하여 DLL의 동작을 종료하고, 종료함수가 가지는 Thread를 다시 Injection 한 후 KILL DLL 클릭하여 삭제한다. 본 논문에서 실험을 한 치료방법과 해결하는 방안은 컴퓨터 바이러스의 대한 획기적인 차원의 연구가 될 것이며 경제와 금융사회의 유비쿼터스 보안을 강화하는 초석이 될 것이다.

Abstract

A Malicious code is used to SMiShing disguised as finance mobile Vishing, using Phishing, Pharming mail, VoIP service etc. to capture of personal information. A Malicious code deletes in Anti-Virus Spyware removal programs, or to cure use. By the way, the Malicious cord which is parasitic as use a DLL Injection technique, and operate are lsass.exe, winlogon.exe, csrss.exe of the window operating system. Be connected to the process that you shall be certainly performed of an exe back, and a treatment does not work. A user forces voluntarily a process, and rebooting occurs, or a blue screen occurs, and Compulsory end, operating system everyone does. Propose a treatment way like a bird curing a bad voice code to use a DLL Injection technique to occur in these fatal results. Click KILL DLL since insert voluntarily an end function to Thread for a new treatment, and Injection did again the Thread which finish an action of DLL, and an end function has as control Thread, and delete. The cornerstone that the treatment way that experimented on at these papers and a plan to solve will become a researcher of the revolutionary dimension that faced of a computer virus, and strengthen economic financial company meeting Ubiquitous Security will become.

▸ Keyword : Computer Virus, Computer Virus Vaccine, DLL injection, Ubiquitous Security, Malicious Software.

• 제1저자 : 박희환, 교신저자 : 박대우(prof1@paran.com)
• 접수일 : 2006.10.20, 심사일 : 2006.11.05, 심사완료일 : 2006.11.12
* 숭실대학교 정보과학대학원 정보보안학과

Ⅰ. 서 론

모바일 환경에서의 금융업무가 급속히 확대되고 있다. 이동단말기에서 금융 전문 칩을 이용하여 은행 간 계좌이체를 하거나 자금 결제를 하고, 증권사이트에 접속하여 실시간으로 주식거래하고 있다. 이와 같은 최근의 모바일 환경은 유비쿼터스(Ubiquitous) 시대로의 금융업무로 변화되어 가고 있다. 따라서 유비쿼터스 시대로의 금융업무를 지원하기 위한 금융업계에서는 시간과 장소와 기기에 제한이 없는 일일 24시간 거래에 따른 안전한 금융지원 및 백업 시스템을 갖추고 있어야 한다[1].

유비쿼터스 시대의 금융업무로의 전환은, 악의적인 공격을 사용하는 해커의 활동에도 변화를 가져왔다. 특히 최근의 악의적인 해커의 사이버 공격방법들은 기존의 공격방법들을 혼합시키는 새로운 변종 공격을 만들어냈다. 트로이목마와 같은 악성코드를 이용하여 개인의 아이디와 패스워드를 추출해 내고, 이 정보를 이용하여 웜이나 DDoS 공격을 사용하여 금융지원 시스템을 집중적으로 공격할 수 있다[2].

이때 개인 정보를 탈취하기 위한 방법으로 불법적인 금융위장 사이트로의 사회공학적인 접속을 하게 만드는 피싱(Phishing)[3]과 파밍(Pharming)[3]메일, 또한 VoIP 서비스[4]로 불특정 다수에게 전화를 걸어 개인의 중요한 금융정보를 빼내는 비싱(Vishing), 모바일 금융을 위장한 문자메시지를 이용한 스미싱(SMiShing) 등의 기법을 이용하고 있다. 특히 최근의 모바일 환경에서의 악성모바일 코드[5]들의 출현도 빈번해지고 있다.

해커의 개인 정보의 탈취에는 필수적으로 악성코드가 사용되어지고 있다. 그런데 이러한 악성코드는 윈도우 운영체제에서 감염된 상태로 존재하면서, 해커의 공격의 명령에 따라 중요 정보를 해커에게 전달한다[6].

유비쿼터스 보안을 위해서, 이런 경우 악성코드가 발견되면 앤티바이러스나 스파이웨어 제거와 같은 보안제품으로 악성코드를 삭제하거나 치료하는데 사용한다.

기존의 바이러스 스캔 프로그램이나 스파이웨어 스캔닝 프로그램을 이용하여, 바이러스나 악성코드를 검색하고 검색과 동시에 하거나, 검색한 후 바이러스 백신 프로그램을 이용하여 치료한다.

하지만 악성코드를 치료하는 백신 프로그램으로 치료를 한 후에도, 실제 시스템의 내부에는 계속 치료되지 않고 존재하는 악성 바이러스 코드가 있다. 즉 악성코드의 백신 치료 상태 후의 결과보고에서도 악성코드는 계속 존재하면서, '재부팅 시에 삭제됩니다, 액세스가 거부 되었습니다'라는 메시지를 남긴다. 이러한 경우 실제로 PC의 내부에서는 악성코드가 치료되지 않은 경우이다.

보안 제품은 응용 프로그램이기 때문에 시스템 프로그램으로 위장된 악성코드는 응용 프로그램으로써 제어권한을 가질 수 없다.

즉 악성코드에 감염된 시스템을 사용자 혹은 관리자가 적절한 조치를 취하지 못하는 상황이 되는 것이다. 이런 경우 기존의 백신 프로그램으로 치료가 되지 않아 강제로 치료를 하여야만 한다. 강제적 치료를 수행할 경우에 운영체제 시스템이 온전히 구동되기 위해서는 몇 가지 반드시 실행되어야 하는 프로세스 몇 가지가 있다.

예를 들면 lsass.exe(Winlogon 서비스에 필요한 인증 프로세스), winlogon.exe(사용자의 로그인/로그오프를 담당하는 프로세스), csrss.exe(Client/Server Runtime SubSystem : 윈도우 콘솔을 관장하고 쓰레드를 생성/삭제하며 16bit 가상 MS-DOS 모드를 지원)및 기타 서비스 프로세스이다[7][8].

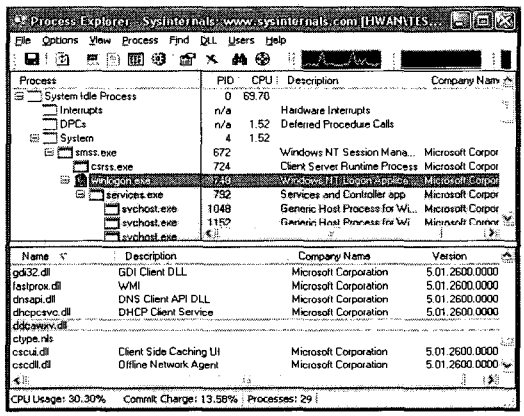

그림 1. DLL Injection 기법으로 실행된 악성코드
Fig. 1 The Malicious Code that was Performed to DLL Injection Techniques.

이러한 프로세스는 실제 윈도우 운영체제의 관리자 권한을 가진 사용자라 하더라도 시스템 상에서 제어할 수 없는 경우가 있다. 즉 사용자가 임의로 위와 같은 프로세스를 강제 종료와 같이 제어하려한다면, 윈도우 운영체제 시스템 전체가 리부팅이 발생하거나 블루 스크린이 발생한다.

왜냐하면 이러한 신종 악성코드는 DLL Injection 기법을 이용하기 때문이다. 그림 1.에서 DLL Injection 기법은 시스템이 온전히 구동되기 위해서는 반드시 실행되어야 하는 프로세스에 연계되어 있어, 강제적으로 악성코드를 치료하려면 DB서버와 같은 중요 컴퓨터 시스템의 운영체제에 치명적인 영향을 미칠 수 있다.

개인 사용자뿐만 아니라 특히 인터넷 쇼핑몰이나 금융 지원 시스템 관련 서버에서 이러한 현상이 발생한다면 사회적, 경제적인 손실뿐만 아니라, 대규모의 금융공황 상태와 같은 큰 문제가 발생 할 수 있다. 이러한 피해를 입은 경우 컴퓨터 범죄수사를 수사하고 재판 증거로 채택하는 컴퓨터 포렌식(Computer Forensic)의 경우에도 디지털 증거의 무결성 확보를 위한 여러 가지 문제점[9]을 발생시킬 수 있다.

따라서 본 논문에서는 이러한 치명적인 시스템의 다운이나, 리부팅과 디지털 증거의 무결성 확보를 위한 여러 가지 문제점과 같은 악영향으로부터 중요한 컴퓨터 시스템의 자원을 보호하기 위하여 DLL injection 기법을 이용하는 악성코드를 분석하고, 새로운 치료 방법을 제안하고, 제안 방법을 구현하여, 악성코드가 치료됨을 증명한다.

이 연구 방법의 결과는 신종 컴퓨터 바이러스의 대한 획기적인 차원의 연구가 될 것이며, 경제와 금융사회의 정보보안을 강화하기 위한 백신 분석과 치료방법에 대한 문제점을 제시하고 해결하는 방안을 제시하였다.

II. 관련 연구

2.1. DLL Injection의 의미

일반적인 악성코드는 자신을 실행파일로 하여 자기 독립적으로 실행된다. 즉 악성코드를 만든 제작자의 의도대로 자체적인 기능을 보유하여 의도된 행동을 수행한다.

DLL Injection은 정상적이 파일에 기생하여 실행되는 형태 혹은 정상적이 파일에 기생하는 기법을 이용하여 자신을 은폐하기 위한 수단을 강구한다.

2.2. DLL injection 악성코드

1) DLL injection의 악성코드의 이름

악성코드 파일 이름은 jhbn.exe이다. 바이러스를 분류하는 회사에 따라서 악성코드의 이름은 다르게 불린다.

Trojan.Virtumod(VirusChaser 백신 프로그램)[10]

Win-Trojan/Virtumod. 544788(V3 백신 프로그램)[11]

Trojan.Vundo(Norton 백신 프로그램)[12]

- 파일 크기 : 51,725 Bytes

2.3. DLL injection 감염경로

DLL Injection 악성코드의 주요 감염 경로는 다음과 같다.

1) 해킹으로 인한 변조된 웹사이트 접속 시 사용자 PC에 유입된다.
2) ActiveX Controller에 의해 설치된다.
3) 또 다른 악성코드에 의해 생성되거나 다운로드 및 설치된다.

2.4. DLL injection 감염증상

DLL injection 기법을 이용하는 악성코드는 그림 2.와 같이 감염되어 시행되는 과정을 기술하면 아래와 같다.

1) 악성코드가 실행되면 자신을 시스템 폴더에 *.dll형태 파일을 생성하고 파일은 삭제된다.

- %System%\ddcyw.dll (파일명은 Random한 이름을 가짐.)

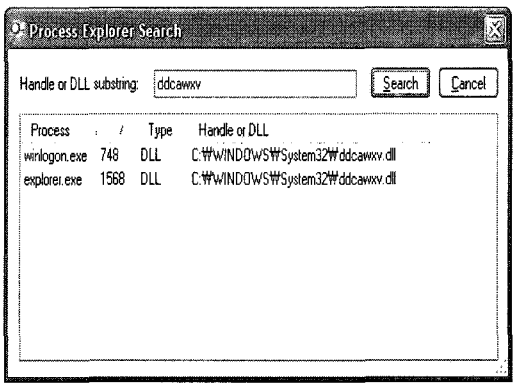

그림 2. DLL Injection 파일 찾기
Fig 2. Find a DLL Injection File.

* 기본적인 윈도우 시스템 폴더(%System%)

-Windows 9X/ME: C:\Windows\SYSTEM

-Windows NT/2000: C:\Winnt\System32

-Windows XP: C:\Windows\System32

2) 생성된 *.dll은 아래와 같은 특정 프로세스에 자신을 인젝션 하여 실행 파일에 기생하여 실행되어 진다.

- %System%\winlogon.exe
- %System%iexplorer.exe

3) 아래와 같은 레지스트리 경로에 키 값을 생성하여, 윈

도우가 시작 시마다 자신이 실행될 수 있도록 한다.

레지스트리 경로 : HEKY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\임의dll파일이름

4) 자신이 온전히 실행되기 위하여 감염된 시스템에 다음과 같은 악의적인 행위를 한다.

- 레지스트리 값을 생성 (윈도우에 의한 자동 시작)한다.
- 악성코드가 등록한 레지스트리 값의 존재 여부를 실시간 확인한다.

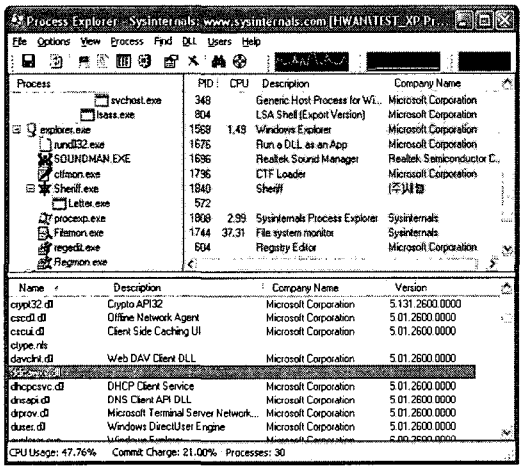

그림 3. 특정 프로세스에 기생하여 실행

Fig 3. Parasitic to a Specific Process, and Perform.

- 그림 3.처럼 만약 삭제되면 운영 프로그램에 기생하여 다시 악성 프로그램을 프로그램을 생성한다.
- winlogon.exe에 dll형태로 인젝션 하는 것처럼 동일한 방식으로 explorer.exe에도 그림 4.와 같이 인젝션 되어 동작한다(이 기법은 사용자에 의해 악성코드를 실행 할 수 있는 효과가 있다.).

2.5. DLL injection 기존 치료 방법

1) 직접 치료 방법

기존 프로세스에 대한 제어가 가능한 툴이 다양하게 존재한다.

iexplorer.exe

explorer.exe

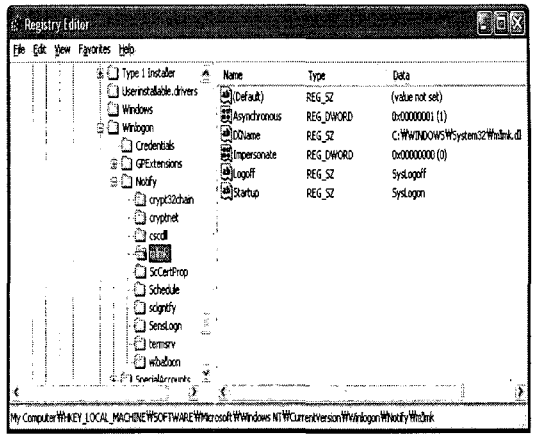

그림 4. 레지스트리 편집기 확인

Fig 4. Registry Editor Confirmation.

위와 같은 프로세스 경우에는 해당 실행 파일에 *.dll파일이 injection되어 동작하고 있다면 먼저 실행 파일을 종료 후에 *.dll파일만 삭제하면 된다.

2) 툴을 이용하는 방법

프로세스 뷰어라는 툴[13]은 하나의 프로세스가 이용하는 dll 파일 정보 등 열람이 가능하다. 다음은 DLL injection 기능의 바이러스 분석에 사용된 툴을 그림 5.에서 소개한다.

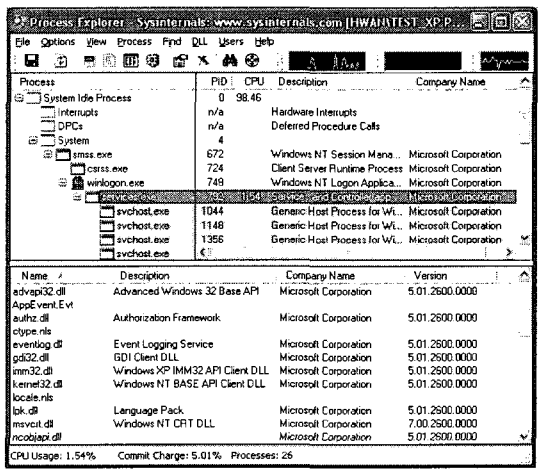

그림 5. Process Explorer 정보 보기

Fig 5. Process Explorer Information Example.

사용된 툴 이름은 Process Explorer v10.2[123]이다. Process Explorer v10.2는 시스템에 모든 프로세스 정보를 보여준다.

그림 6.에서 File Monitor는 실시간 파일의 I/O를 감시한다.

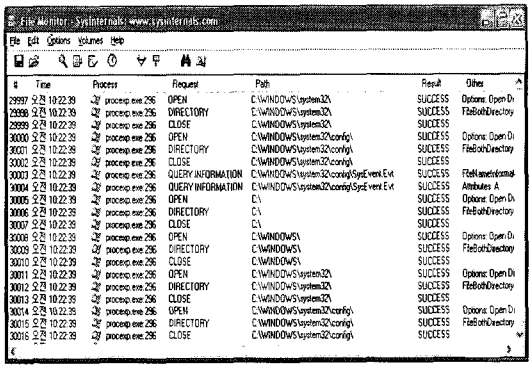

그림 6. File Monitor 감시
Fig 6. File Monitor Watch.

추가적으로 제어 또한 가능하여 해당 목록 파일을 그림 7.처럼 unload 할 수도 있다. 악성코드가 이용하는 winlogon.exe 프로세스에 인젝션 되어 있는 dll파일을 unload시 다른 프로세스와는 다른 현상이 나타난다.

실제 iexplorer.exe에 인젝션 되어 있는 dll파일은 툴로써 쉽게 unload 할 수 있었다.

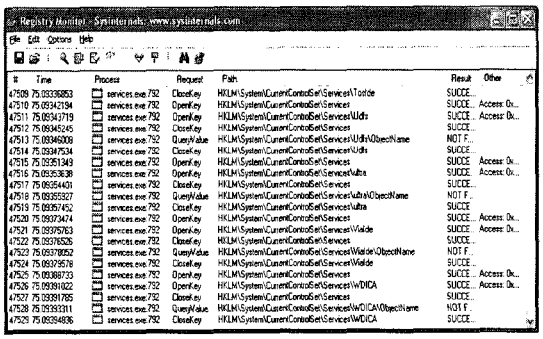

그림 7. DLL Injection 기능 파일
Fig 7. File Functional DLL Injection.

그러나 winlogon.exe를 툴로 제어하려 하면 다시 말해서 악성코드인 dll 파일을 unload시도하면 시스템이 리부팅 되거나 그림 8.처럼 블루 스크린 현상이 발생한다.

만약 인터넷 쇼핑몰이나 금융 지원 시스템 관련 서버에서 이러한 현상이 발생한다면 경제적인 손실뿐만 아니라, 업무가 마비되는 현상을 일으켜 파급적인 피해를 초래 할 수 있다.

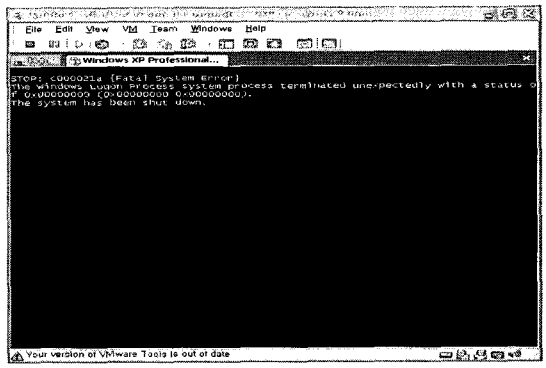

그림 8. 블루 스크린 현상 발생
Fig 8. The Blue Screen Phenomenon Occurrence.

III. DLL injection 악성코드의 분석 및 새로운 치료 방법 연구

3.1. DLL injection 악성코드의 증상

DLL Injection 기능의 악성코드가 감염되는 주요 감염 경로는 다음과 같다.

1) 아래와 같은 레지스트리 값을 0.5초단위로 지속적으로 write한다.

HEKY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\임의 dll파일이름

2) 파일을 제어하려하면 아래와 같이 블루스크린이 발생하면서 리부팅 된다.

3.2. DLL injection 악성코드의 감염피해 분석

DLL Injection 기능의 악성코드는 자신이 생성한 값을 실시간으로 지속적 write 한다. 따라서 윈도우 운영체제의 CPU 점유율이 증가하고 또 다른 악성코드에 대한 다운로드를 시도하기 때문에 트래픽이 유발된다.

3.3. DLL injection 악성코드의 새로운 치료 방법

중요한 것은 윈도우 운영체제의 시스템 파일을 종료하지 않고 dll파일만 제어해야만 한다. 이를 위해선 그림 9.처럼 실행파일이 생성한 핸들에 의해 발생된 Thread에 종료 함수를 임의로 삽입하고 Thread를 제어하여 DLL의 동작을 종료한다. 여기서 단지 Dll의 행위만 종료된 상태이기

때문에 DLL를 unload하는 경우 시스템 파일이 종료되지 않는다.

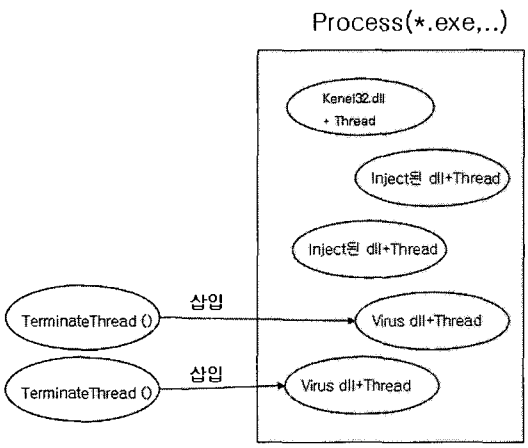

그림 9. Thread에 종료함수를 삽입
Fig. 9 Insertion by an End Function to Thread.

3.4. 기존 치료 방식과 제안한 치료 방식

기존 방식은 Injection되어 진 DLL을 제어하기 위하여 해당 실행 파일을 종료하고 unload 했었다.

하지만 제안된 방식은 실행 파일을 종료하지 않고도 제어가 가능하다는 것을 보여준다.

즉 추가적인 동작을 하도록 Thread에 종료함수를 삽입하여 DLL 일의 동작만 종료하고 실행파일은 지속적으로 동작함을 유도하였다.

IV. DLL injection 악성코드의 치료

감염증상을 나타내면 바이러스 스캔 프로그램을 작동시킨다. 바이러스 증상과 코드를 분석하여 바이러스의 침해 과정을 정의하고 이름을 붙인다. 바이러스 치료를 위해 감염된 Injection 악성코드가 사용하는 Thread를 캡처하여 삽입할 수 있는 프로그램을 설계 및 악성코드의 치료를 구현 하였다.

4.1. DLL injection 악성코드의 수동 치료 절차

바이러스가 winlogon에 injected 될 시에 Thread를 생성하게 된다. 바이러스는 자신이 Injection되어진 실행 파일을 이용하여 팝업창 활성화 등 행위를 시도한다. 이때 생성되는 Thread는 kernel32.dll를 Hooking하여 호출되는 함수를 통해 정보를 알 수 있다.

dll이 unload를 하기 위해서는 단순히 dll 카운터 값을 0으로 만들어 줌으로써 unload를 할 수 있다.

하지만 윈도우 운영체제 시스템 상에서 어떠한 행동을 하고 있는데 dll을 메모리상에서 내리는 것은 오류가 났다고 판단하기 때문에 해당 프로세스를 재시작 하게 된다. 이를 방지하기 위하여 종료 함수를 가진 dll 쓰레드를 임의 삽입한다.

4.2. DLL injection 악성코드의 치료 프로그램 작성

Injection 되어진 프로세스를 클릭하면 사용되는 DLL 파일들을 보여준다.

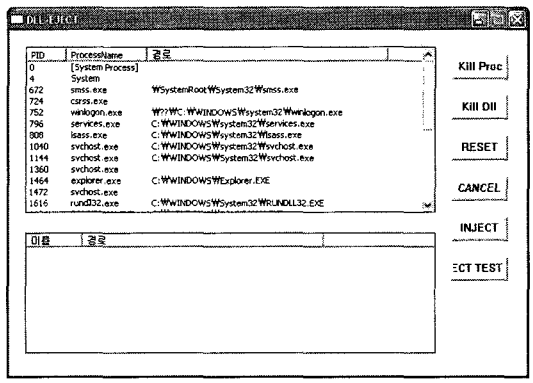

그림 10. Dll injection 악성코드의 치료 프로그램
Fig. 10 Treatment Program of a Malicious Code Dll injection.

Injection 목록 확인한다.
일련의 Thread을 삽입한다.
Thread를 종료한다.
DLL unload를 실시한다.

4.3. DLL injection 악성코드의 치료

그림 11.에서 악성코드가 생성한 DLL파일을 다시 클릭하고 종료함수가 가지는 Thread를 다시 Injection 한다. 이 후 KILL DLL 클릭 시 삭제가 된다.

4.4. 악성코드 치료 후 존재 유무의 확인

바이러스 스캔 프로그램을 작동시켜서 프로그램으로 구현된 악성코드의 종료 프로그램을 작동시켜 그림 12.처럼 감염 증상이 없이 깨끗이 제거됨을 확인하였다.

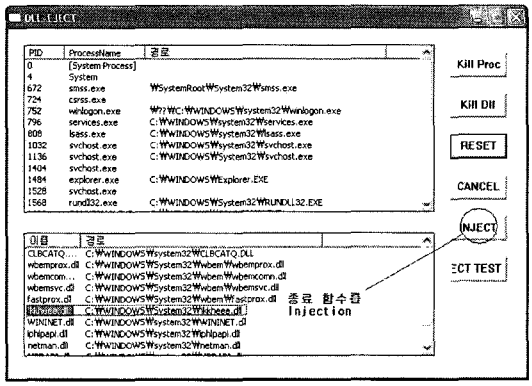

그림 11. DLL injection 악성코드 치료(1)
Fig. 11 code treatment Malicious DLL Injection(1).

운영체제에서 Process Explorer v 10.2를 이용하여 DLL파일을 가지는 Thread가 삭제됨을 확인 하였다. 따라서 DLL Injection 악성코드는 치료되어 결과보고에 나타낸다.

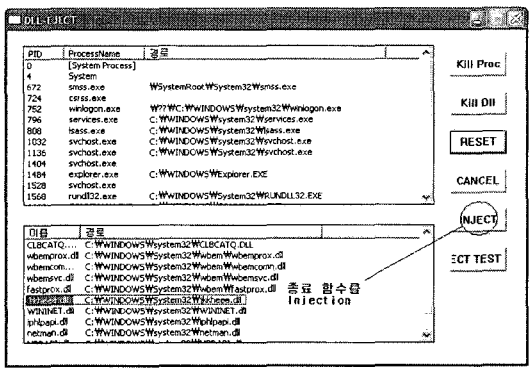

그림 12. DLL injection 악성코드 치료(2)
Fig. 12 code treatment Nasty DLL Injection(2).

V. 결론

개인 정보의 탈취를 위해 불법적인 금융위장 사이트로의 사회공학적인 접속을 하게 만드는 피싱과 파밍 메일, 비싱, 스미싱 등의 기법을 이용하고 있다. 개인 정보의 탈취에는 필수적으로 악성코드가 사용되어지고 있다.

악성코드가 발견되면 앤티바이러스나 스파이웨어 제거를 위한 보안제품으로 악성코드를 치료한 후에도, 실제 시스템의 내부에는 계속 치료되지 않고 존재하는 악성 바이러스 코드가 있다.

이런 경우 기존의 백신 프로그램으로 치료가 되지 않아 강제로 치료를 하여야만 하는데, 이 경우 강제적 lsass.exe, winlogon.exe, csrss.exe 및 기타 서비스 프로세스는 실제 윈도우 운영체제의 관리자의 권한을 가진 사용자라 하더라도 시스템 상에서 제어할 수 없는 경우가 있다. 만약 임의로 위의 프로세스를 강제 종료한다면 윈도우 운영체제 시스템 전체가 리부팅이 발생하거나 블루 스크린이 발생 한다.

이러한 신종 악성코드는 DLL Injection 기법을 이용하기 때문이다. 이 기법은 반드시 실행되어야 하는 프로세스에 연계되어 있어, 강제적으로 악성코드를 치료하려면 DB 서버와 같은 중요 컴퓨터 시스템의 운영체제에 치명적인 영향을 미칠 수 있다.

본 논문에서는 이러한 치명적인 시스템의 다운이나, 리부팅과 같은 악영향으로부터 중요한 컴퓨터 시스템의 자원을 보호하기 위하여 DLL injection 기법을 이용하는 악성코드의 증상을 분석하고, CPU 점유율이 증가, 트래픽이 유발과 같은 감염피해 분석을 한다.

새로운 치료를 위한 Thread에 종료함수를 임의로 삽입하고 Thread를 제어하여 DLL의 동작을 종료하고, 종료함수를 가진 dll 쓰레드를 임의 삽입한다. 악성코드가 생성한 DLL파일을 다시 클릭하고 종료함수가 가지는 Thread를 다시 Injection 한 후 KILL DLL 클릭 시 삭제가 된다.

본 논문에서 제안된 실험을 통해 특정 프로세스에 Injection 되어져 실행되는 dll 악성코드에 대한 새로운 치료 방법을 제안하고 치료를 실험하여 성공하였다.

새로운 치료 방법에 관한 연구 결과는 신종 컴퓨터 바이러스의 대한 획기적인 차원의 연구가 될 것이며, 경제와 금융사회의 정보보안을 강화하기 위한 백신 분석과 치료방법에 대한 문제점을 제시하고 해결하는 방안을 제시하였다.

향후 연구로는 본 논문연구에서의 치료 중 특이한 케이스가 발견된 경우에 대한 연구이다. 즉 Thread를 제어하여 추가적인 행위를 유도하고 유도된 행위가 자신이 갖는 Thread를 종료 하는 것이다. 이러한 방법은 허용된 쓰레드를 그대로 이용한다는 장점을 바탕으로 서비스를 재시작할 필요가 없다. 그러나 정확한 Thread 정보가 확보 되지 않으면 오히려 블루 스크린을 발생하는 등의 단점 또한 확인되었다. 따라서 이 특이한 경우에 대한 향후 연구를 통해 새로운 바이러스의 치료와 연구에 대한 완전하고 안정된 시스템을 보장하는 백신의 탄생을 기대한다.

참고문헌

[1] Brain Carreier. "File System Forensics Analysis." Addison-Wesley. 2005.

[2] 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11. 30.

[3] TTA. 정보통신용어사전. http://word.tta.or.kr/index.jsp. 2006.10.

[4] 박대우, 윤석현. "VoIP 서비스의 도청 공격과 보안에 관한 연구." 한국컴퓨터정보학회논문지, 제11권 제4호, pp1-10, 2006. 9. 30.

[5] 로저 그라임스, 완성현 역. "Malicious Mobile Code Virus Protection for Windows". 2001. 12.

[6] Peter Szor. "COMPUTER VIRUS RESEARCH AND DEFENSE." Addison-Wesley, May 2005.

[7] 이호동. Windows 시스템 실행파일의 구조와 원리 Chapter 6. 2006.

[8] 정덕영. Windows 구조와 원리. Chapter 10. Paging, 공유 메모리와 공유 모듈. 2005

[9] Adelstein, F. "Live forensics: Diagnosing your system without killing it first". Communications of the ACM. V.49, N.2, 63-66. 2006.

[10] 보안정보 바이러스, http://www.viruschaser.com/main/security/VCInfo_Ls.jsp?page=2&noticeType=A&stype=&scon=. 2006.11.

[11] 보안위협 DB 검색, 최신 보안위협 정보. http://info.ahnlab.com/securityinfo/virus_search.jsp?svccode=aa1001&contentscode=ad001. 2006.11.

[12] Symantec.com, Search Results. http://searchg.symantec.com/search?q=vundo&charset=utf-8&proxystylesheet=symc_en_US&client=symc_en_US&hitsceil=100&site=symc_en_US&output=xml_no_dtd&context=ent. 2006.11.

[13] Process View, Process Explorer, www.sysinternals.com. 2006.11.

저 자 소 개

박 희 환

1998년 관동대학교 컴퓨터 공학과 졸업 (공학학사)

2006년 숭실대학원 정보과학대학원 정보보안학과 (석사과정)

2004년 (주)뉴-테크 웨이브 바이러스 분석 대응팀 연구원

〈관심분야〉 컴퓨터 바이러스, Cracking, 네트워크 보안, 컴퓨터 포렌식

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

〈관심분야〉 유비쿼터스 보안, 네트워크 보안, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality