윈도우 악성코드 분석을 통한 탐지 및 대응 기술에 관한 연구

임원규* · 이정현** · 임수진*** · 박원형*** · 국광호***

요 약

오늘날 네트워크의 속도와 인터넷 기술의 발전과 동시에 윈도우 취약점을 통한 악성코드가 많이 발생하고 있다. 악성코드는 여러 감염 형태 및 특성이 있어 바이러스 백신을 이용하여 탐지하기도 어려울 뿐만 아니라 제거하는 것도 쉽지 않다. 본 논문은 윈도우 악성코드의 분류와 특징을 분석하여 프로그램을 이용한 악성코드의 위치를 파악하고 신종 악성코드에 대한 신속한 대응을 위해 스크립트 기술을 제안 한다.

A Study on Detection and Responding Technology through Windows Malware Analysis

Won Gyu Lim* · Jung Hyun Lee** · Su Jin Lim***
Won Hyung Park*** · Kwang Ho Kook***

ABSTRACT

Nowadays, the network's speed and internet technology are progressing rapidly but malwares are occurring frequently through the Window's weak point. Since the malwares have various infection types and characteristics, it is hard to detect them by the virus vaccine and to cure them. This paper analyzes the type and characteristics of the malware and proposes a script technology that can find the location of the malware by the program and respond rapidly to the new kind of malwares.

Key words : Malware, Detection, Script

접수일 : 2010년 1월 20일; 채택일 : 2010년 2월 25일

* 서울산업대학교 IT정책대학원 산업정보시스템전공
** 고려대학교 정보경영공학전문대학원
*** 서울산업대학교 산업정보시스템공학과

1. 서 론

오늘날 네트워크의 속도와 인터넷 기술이 발전함에 따라 윈도우와 인터넷의 취약점을 통해 악성코드가 많이 발생하고 있고 바이러스 백신을 이용한 치료 또한 어렵다. 특히 인터넷을 통해 쇼핑을 하거나 증권을 매매하는 등의 금전적인 거래가 늘어남에 따라 금전적 유출을 목적으로 하는 보안 사고들이 자주 일어나고 있다. 최근 UCC나 소셜네트워크(SNS)와 같은 웹 2.0 서비스를 통해 보다 쉽게 사용자가 흥미를 갖고 접근할 수 있는 다양한 감염 경로로 악성코드가 유포되고 있는 실정이다. 따라서 고도화된 악성코드를 통해 백신 솔루션이 무력화되거나 신종 악성코드가 급속히 확산된다면 악성코드 대응에 대한 대안점을 찾기가 어렵다. 그리고 컴퓨터 사용자들이 악성코드에 대응할 수 있는 유일한 방법은 악성코드의 감염을 예방, 진단 및 제거하는 백신 프로그램을 선택하여 사용하는 것이다. 그러나 새로운 악성코드가 발견된 후, 이에 대한 감염 예방, 대응 및 제거를 위해 백신 프로그램의 엔진이 업데이트되어 나오기까지는 일정 기간이 소요된다.

따라서 컴퓨터 사용자들은 이 기간 동안 감염된 신종 악성코드에 대해 아무런 대책 없이 수동적인 입장으로 있을 수밖에 없게 된다. 또한 컴퓨터 사용자들은 악성코드 감염에 적절히 대응하는 방법과 악성코드에 대한 사전 지식이 부족하여 PC에 치명적인 손실을 입는 경우도 발생할 수 있다.

본 논문은 이러한 최근 현실을 반영 악성코드 대응 기술을 연구하여 PC 사용자 및 기업의 관리자가 능동적으로 악성코드 감염을 미연에 방지하고 감염이 되었을 경우, 적극적인 대처로 악성코드의 확산을 막을 수 있는 기술을 연구한다.

2. 관련 연구

2.1 악성코드의 정의

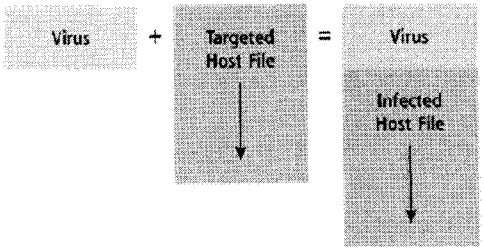
악성코드란 말웨어(Malware) 혹은 악성프로그램(Malicious Software)이라 하며, 악의적인 목적을 위해 작성된 실행 가능한 코드의 통칭으로 자기 복제 능력과 감염 대상 유무에 따라 바이러스, 웜, 트로이 목마 등으로 분류된다[1, 2].

2.2 악성코드 분류

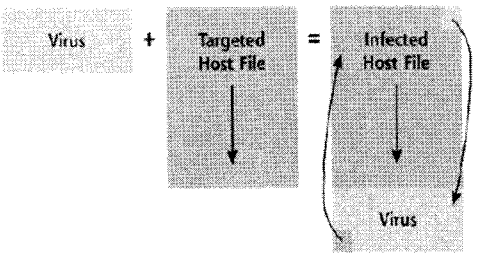
악성코드는 대표적으로 바이러스, 웜, 트로이 목마, 스파이웨어 및 기타 악성코드로 분류된다. 다음으로 악성코드의 분류기준에 따른 대표적인 악성코드를 알아보고자 한다.

2.2.1 바이러스

바이러스는 컴퓨터 시스템의 정상적인 파일을 감염시켜 자신 또는 자신의 변형 코드를 실행프로그램, 시스템 영역 등의 실행 가능한 부분에 복제하는 프로그램이다[1]. 또한 감염대상에 따라 아래 (그림 1), (그림 2)와 같이 전위형 바이러스 및 후위형 바이러스로 대상에 따라 감염 위치가 다르게 위치된다[3].



(그림 1) 전위형 바이러스



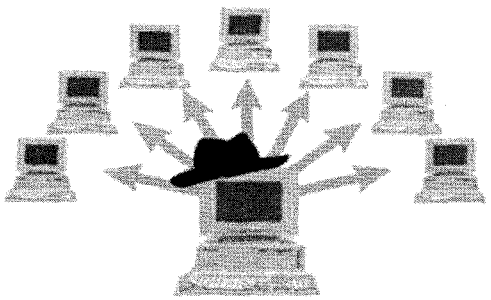
(그림 2) 후위형 바이러스

바이러스는 감염 되고 나서 어디에 상주하느냐에 따라 분류하는 방법이 일반적이며, 부트 바이러스와 파일 바이러스, 부트/파일 바이러스로 나뉜다. 부트 바이러스는 컴퓨터를 켰을 때 초기에 실행되는 프로그램에 감염되어 있다가 바이러스의 위치를 부트영역으로 옮겨 다른 파일로 전염된다. 파일 바이러스는 일반적인 프로그램에 감염되는 컴퓨터 바이러스를 말하는데, 감염된 파일을 실행하지 않으면 전염되거나 확산되는 것을 피할 수 있다. 제작이 쉬운 반면 파일 크기가 변한다거나 감염된 파일을 실행하지 않으면 활동할 수 없다는 특징이 있다[4]. 부트/파일 바이러스는 부트 섹터와 파일 모두에 감염되는 바이러스로 일반 바이러스에 비하면 바이러스 크기가 상당히 큰 특징을 가지고 있으며 파괴적인 바이러스가 대다수를 차지한다[5].

2.2.2 웜

웜은 바이러스와 달리 다른 파일을 감염시키지 않고 자신을 복제하는 능력을 가진 프로그램을 말한다. 일반적으로 '웜 바이러스', '바이러스 웜' 등의 말을 사용하기도 하지만, 사실 정확한 표현은 아니다. '웜'이라는 용어가 사용자에게 생소하기 때문에 악성 프로그램의 대명사인 바이러스와 함께 붙는 것이다.

윈도우를 기반으로 하는 웜은 (그림 3)과 같은 형태로 보통 네트워크를 이용하여 전파 된다.



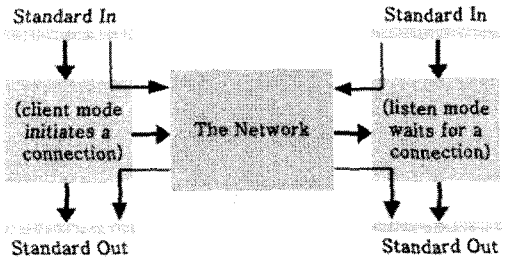
(그림 3) 네트워크를 통한 웜 전파

최초로 발견된 윈도우 기반의 인터넷 웜인 I-Worm/Happy99는 WINSOCK32.DLL을 변형해서 메일을 보낼 때 웜 파일을 첨부하는 형태를 취했으며, 이는 WINSOCK32.DLL이 윈도우에서 인터넷과 관련된 일을 할 때 사용된다는 특성을 이용한 것이다[5].

2.2.3 트로이 목마

트로이 목마는 자기 복사 능력은 없이 고의적인 부작용만 가지고 있는 프로그램으로, 프로그램 제작자의 실수로 포함된 프로그램 버그와는 다르며, 고의로 제작되었다는 점에서 볼 때 바이러스와 같은 악의적인 파괴 프로그램이라 할 수 있다.

트로이 목마는 (그림 4)와 같이 클라이언트 시스템이 감염되면 계정 및 패스워드와 같은 공격 대상 정보를 트로이 목마 서버로 전송하는 역할을 한다.



(그림 4) 트로이 목마를 통한 정보유출

트로이 목마는 일종의 프로그램이므로 컴퓨터 바이러스와 마찬가지로 일반적인 프로그램이 수행하는 모든 일을 할 수 있다. 따라서 트로이 목마 프로그램으로 특정 파일을 지울 수 있으며, 최악의 경우 하드 디스크를 포맷해 버리는 것도 얼마든지 가능하다. 이런 점에서 트로이 목마도 컴퓨터 사용자 입장에서는 컴퓨터 바이러스와 함께 조심해야 할 악의적인 파괴 프로그램이다.

2.2.4 스파이웨어

스파이웨어는 사용자 이름이나 아이피주소, 방

문한 웹사이트 목록, 클릭한 배너 광고 등 사용자 컴퓨터속의 정보를 빼내서 전송하는 프로그램을 말한다. 또한 사생활 침해가능성이 있는 유해가능 프로그램이며, 사용자의 동의 없이 사용자를 속여 설치되어 다음 <표 1>에 해당하는 행위를 수행하는 프로그램이다[3].

〈표 1〉 정보통신망 이용촉진 및 정보보호 등에 관한 법률

① 웹 브라우저의 홈페이지 설정이나 검색 설정을 변경 또는 시스템 설정을 변경하는 행위
② 정상 프로그램의 운영을 방해, 중지 또는 삭제하는 행위
③ 정상 프로그램의 설치를 방해하는 행위
④ 다른 프로그램을 다운로드하여 설치하게 하는 행위
⑤ 운영체계 또는 타 프로그램의 보안설정을 제거하거나 낮게 변경하는 행위
⑥ 사용자가 프로그램을 제거하거나 종료시켜도 당해 프로그램이 제거되거나 종료되지 않는 행위
⑦ 컴퓨터 키보드 입력 내용이나 화면 표시 내용을 수집, 전송하는 행위

2.3 악성코드 분류에 따른 특성

다음 <표 2>는 악성코드 분류 기준에 따라 다음과 같은 특성을 비교하여 분석하였다.

〈표 2〉 악성코드 특성 비교

구 분	주요목적	피해	복제	감염	대책
바이러스	데이터 손실, 삭제	O	O	O	치료
웜	급속 확산, 전파	O	O	X	삭제, 차단
트로이목마	데이터 손실, 유출	O	X	X	삭제
스파이웨어	사용불편 심리적 거부	O	X	X	삭제

대표적인 악성코드 별 특성을 보면, 바이러스를 제외한 악성코드들은 파일의 형태가 독립적으로 존재하도록 생성되기 때문에 방역을 위해서 해당 파일을 삭제하거나 원복하면 된다. 하지만, 바이러스는 윈도우의 정상파일을 대상으로 위·변조하기 때문에 치료를 위해서는 반드시 복원 및 복구를 하여야 한다.

인터넷 익스플로러에 감염되는 스파이웨어의 경우, 윈도우 시스템에 영향을 끼치지는 않지만, PC를 사용하는 목적이 대부분 인터넷을 사용하는 것이므로 스파이웨어에 감염시 사용자가 특히 많은 불편을 끼치게 된다. 최근에는 사용자 몰래 설치되는 스파이웨어 보다는 언인스톨(Uninstall)이 제공되는 유해가능프로그램이 사용자에게 불편을 주고 있다[1].

3. 윈도우 악성코드 특징 분석

3.1 윈도우 악성코드 복사본 생성

악성코드는 윈도우 폴더 또는 시스템 폴더에 복사본을 생성한다. 대부분의 악성코드 및 의심 파일들이 해당 폴더에 복사본을 생성하는 이유는 시

〈표 3〉 윈도우 악성코드 감염 폴더 위치[3]

폴더위치	예시
%SystemRoot%	C:\Windows, C:\WINNT
%SystemRoot%\System32	C:\Windows\System32, C:\WINNT\System32
%SystemRoot%\System32\drivers	C:\Windows\System32\drivers, C:\WINNT\System32\drivers
%USERPROFILE%\Local Settings\Temp	C:\Documents and Settings\계정\Local Settings\Temp
%PROGRAMFILES%\Common Files	C:\Program Files\Common Files\Common Files
%PROGRAMFILES%\Common Files\System	C:\Program Files\Common Files\Common Files\System
System Root 폴더	C:\, D:\, USB Stick 등

스템 파일과 유사한 이름으로 파일을 생성해 시스템 파일이 많아 좀처럼 악성코드를 찾아내기 어렵게 하기 위함이다.

<표 3>과 같이 악성코드 감염 파일은 주로 윈도우 폴더와 프로그램 폴더에 주로 위치한다. 또한 악성코드를 찾을 경우에는 최근에 생성된 파일을 기준으로 정렬하여 찾는다. 하지만 모든 악성코드의 생성된 날짜가 최근으로 표시되지 않으므로 주의해야 한다. 악성코드 파일 유형은 다음과 같이 EXE, COM, DLL, SYS, DAT, BMP, BAT, PIF 확장자를 가지고 있다.

3.2 자동실행을 위한 레지스트리 위변조

악성코드가 윈도우 폴더 또는 시스템 폴더에 복사본을 생성하더라도 해당 파일을 실행해야 악성코드가 동작되게 된다. 따라서 악성코드가 실행되기 위해서는 레지스트리의 자동 실행되는 값을 위변조 함으로써 시스템 재시작시 자동으로 실행하게 한다.

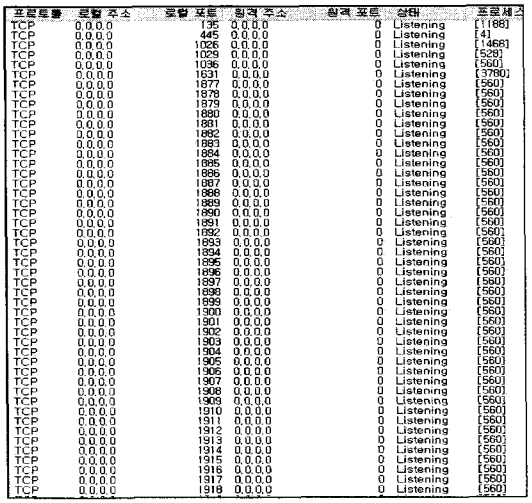
위 <표 4>와 같이 악성코드는 시작 프로그램에 추가하기 위해 레지스트리를 변경한다. 또한 winlogon을 위변조하여 PC의 부팅시 동작 하게 한다.

〈표 4〉 윈도우 악성코드 레지스트리를 변경[3]

Key	변경 내용
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Name 등록
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Name 등록
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService	Name 등록
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce	Name 등록
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Name 등록
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx	Name 등록
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Name 등록
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Name 등록
HKLM\SYSTEM\CurrentControlSet\Services	Service 등록
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	"Userinit" = "C:\WINDOWS\system32\userinit.exe" 변경
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	"Shell" = "Explorer.exe" 변경

3.3 네트워크 연결을 통한 감염

네트워크 연결을 통한 감염은 특정 TCP 또는 UDP 포트를 이용하여 감염되거나 감염시킨다. (그림 5)는 IRCBot 계열 웜에 감염된 PC의 네트워크 상황을 보여 준다. 아래 (그림 5)와 같이 감염이 되면, 특히 135, 445포트와 같이 공유와 관련된 포트가 오픈되고 그 이후에 자신의 모든 포트를 오픈하여 다른 컴퓨터로 감염을 시키기 위한 준비를 한다.



(그림 5) 감염PC에서의 네트워크 명령어 실행

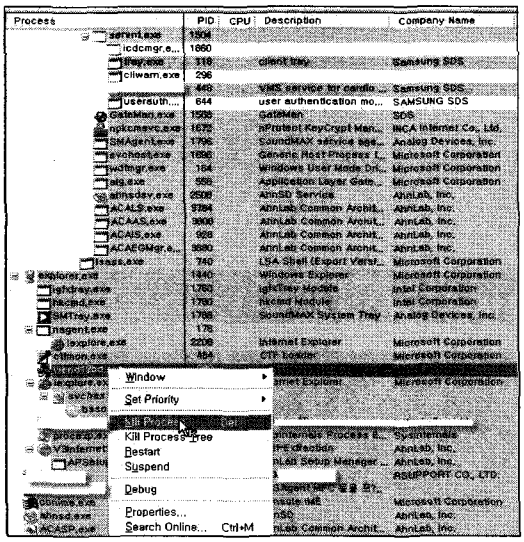
네트워크로 감염되거나 감염시키는 IRCBot 계열 웜은 감염시 자기 자신의 네트워크 포트 전체를 스스로 열고, 특히 공유 포트인 SMB 계열의

135, 445포트를 이용하여 같은 네트워크 세그먼트 대역을 랜덤하게 스캐닝 한다.

4. 윈도우 악성코드 탐지/대응 도구

4.1 Process Explorer

Process Explorer는 악성코드로 의심되는 파일이 스레드로 인젝션되어 있는지 확인하고, 의심되는 프로세스를 확인하기 위한 도구이다. Process Explorer는 대부분의 CERT들과 백신업체의 엔지니어들이 악성코드 대응시 많이 사용하고 있으며, Mircosoft에서 무료로 제공하며 윈도우 시스템에 가장 최적화 되어 있다[6].



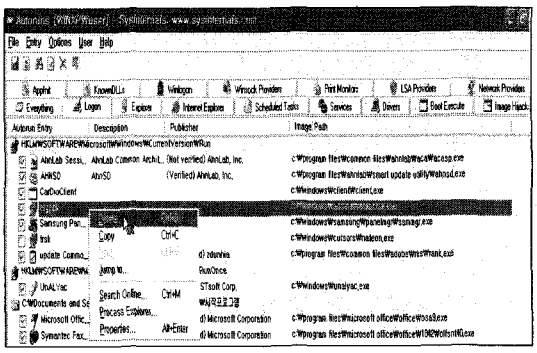
(그림 6) Process Explorer 악성코드 탐지 및 제거

Process Explorer를 이용하여 악성코드를 탐지하려면 (그림 6)과 같이 Description 및 Company name 항목이 없는 부분을 찾는다. 대부분의 악성코드가 해당 항목을 넣지 않기 때문에 가장 우선적으로 확인해 보고 의심해야 한다. 또한 프로세스 상에서 동작중인 의심 항목을 제거하기 전에, 악성코드의 위치를 찾아내 파일을 삭제하거나 이름 변경을 해야 한다. 위치를 찾기 위해서는 마우스를 의심 프로세스에 갖다 대면, 파일의 경로가 보여 진다. 그 후 악성코드가 위치한 폴더로 이동하여 해당 파일의 이름을 변경 하거나 삭제하는 등의 처리가 필요하다.

(그림 6)과 같이 Process Explorer를 통해 탐지된 의심 프로세스를 강제로 제거하기 위해서는 우측 마우스 클릭 후 Kill Process 항목을 클릭하여 처리한다. 하지만, 간혹 다른 모듈에 삽입되어 동작될 수 있기 때문에 강제 닫힘 기능을 사용하더라도 프로세스가 다시 살아나는 경우가 있다. 따라서 해당 프로세스를 강제로 닫기 전에 앞서 밝힌 바와 같이 동작 프로세스의 의심파일의 위치를 찾아내어 처리해야 한다.

4.2 AutoRuns

악성코드로 의심되는 파일이 시스템 시작 프로그램으로 등록되어 있는지 확인하는 도구이다. 특히 레지스트리를 손쉽게 관리 할 수 있고 각 항목별로 조정이 가능하며 레지스트리에 등록되는 모든 악성코드에 대한 대응 및 방역이 가능한 도구이다[6].



(그림 7) AutoRuns 악성코드 탐지 및 제거

(그림 7)은 AutoRuns를 이용하여 시작 프로그

램에 삽입되어 있는 의심 악성코드를 탐지하고 제거 하는 과정을 보여 준다.

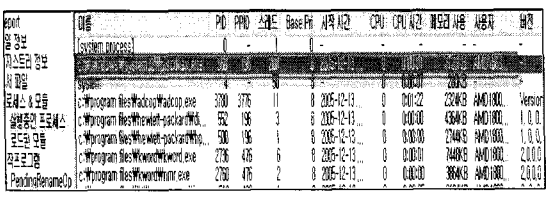
AutoRuns를 이용하여 악성코드를 탐지하려면 위 (그림 7)과 같이 Publisher나 Description 항목이 없는 부분을 찾는다. 대부분의 악성코드가 해당 항목을 넣지 않기 때문에 가장 우선적으로 확인해 보고 의심해야 한다. 또한 시작 프로그램에 등록된 의심 항목을 제거하기 전에, image Path를 확인하여 악성코드의 위치를 찾아내 파일을 삭제하거나 이름 변경을 해야 한다. (그림 7)과 같이 AutoRuns를 통해 탐지된 의심 프로세스를 강제로 제거하기 위해서는 우측 마우스 클릭 후 Delete 항목을 클릭하여 처리한다.

본 장에서 다룬 2가지 도구를 통해 악성코드를 탐지하고 제거하는 것이 가능하지만 신속히 악성코드를 탐지 및 제거하기 위해서 자동화된 도구를 이용하지 않으면 안되며 또한 악성코드 확산을 조기에 방지하기 어렵다.

5. 자동화된 윈도우 악성코드 대응 도구

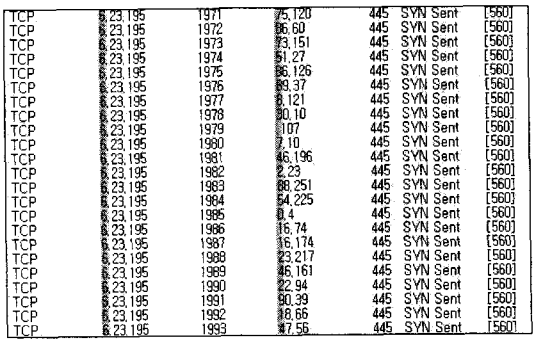
5.1 악성코드 사례 분석

아래 (그림 8)과 같은 증상을 갖는 악성코드 감염 PC가 발견되고 네트워크 트래픽이 과부하 및 네트워크 장비가 다운되는 현상이 발생 하였다고 하자.



(그림 8) 웜으로 의심되는 악성코드 탐지

앞서 확인한 악성코드 대응 및 분석 도구인 Process Explorer 및 AutoRuns 도구를 이용하여 문제가 발생된 PC에서 다음의 의심 파일 및 시작 프로그램에 등록된 레지스트리 경로 및 값을 얻는다.



(그림 9) 웜으로 의심되는 네트워크 과부하

위 (그림 8), (그림 9)를 통해 확인한 의심파일 위치는 다음과 같다.

① 프로세스에서 동작되는 의심 프로세스는 Plscdksx.exe이며 C:\winnt\system32에 위치 한다.

② 해당 파일의 실행을 위해서 다음의 시작 프로그램이 등록되어 있다.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\'systemprocess'C:\winnt\system32\plscdksx.exe

의심 파일 위치를 통해 대응 원리에 맞게 다음과 같이 스크립트를 제작하였다.

5.2 자동화된 스크립트 제작

<표 6>과 같은 웜의 경우 파일의 탐지가 불가능하게 되어 있는 경우가 많아 의심 파일이 숨김 속성으로 되어 있는 경우가 많다. 따라서 스크립트 작성시 SetfileAttributes 명령의 NORMAL 옵션으로 속성을 해제해 주어야 한다. 웜의 의심파일의 경우 의심 파일 삭제로 방역 처리가 가능하나 다른 DLL과 인젝션 되어 있는 경우가 많아 실제 Delete 명령으로 파일을 삭제하면, 삭제할 수 없다고 오류 메시지가 발생할 가능성이 많다. 따라서 방역 처리는 파일 이름을 변경 후 재생성되

지 않도록 파일 이름으로 디렉토리를 생성한다. 또한 부팅 후 의심파일이 시작되지 않도록 레지스트리의 시작 프로그램 값을 삭제하여야 악성코드 처리가 완료 된다. 실제 구현하여 적용한 결과 수작업으로 대응한 것보다 평균 1분30초 이상의 빠른 방역이 가능하였다.

〈표 6〉 악성코드 대응 도구 개발 코드

```
SetCompressor LZMA // 실행압축종류를 설정
Name 'KillWorm' // 스크립트 파일명을 지정
OutFile 'KillWorm.exe'
// 컴파일 후 생성되는 파일명 지정
SilentInstall silent
// 설치 과정은 숨김으로 설정
Section
  SetOutPath $TEMP
  File '.\kill.exe'
// kill.exe를 Temp 디렉토리에 둔다
  nsExec :: ExecToStack/TIMEOUT=10000
  '"$TEMP\kill.exe" -f Plscdksx.exe'
    Pop $0
  StrCmp $0 '0' 0 exit
// Plscdksx 프로세스를 Kill 프로그램으로 죽인다.
  만약 plscdksx 프로세스가 동작되지 않으면
  다음으로 넘어간다
SetFileAttributes $SYSDIR\Plscdksx.exe
NORMAL
// Systemroot 아래에 있는 Plscdksx.exe파일의
  숨김 속성을 해제한다.
  Rename $SYSDIR\ Plscdksx.exe $SYSDIR\
  Plscdksx.bak
// Plscdksx.exe 파일의 확장자 이름을 변경한다
  CreateDirectory '$SYSDIR\Plscdksx.exe'
// Plscdksx.exe 이름으로 디렉토리를 생성한다.
DeleteRegValue HKLM 'SOFTWARE\Microsoft\
Windows\CurrentVersion\Run' 'system process'
// 자동 시작으로 설정되어 있는 레지스트리 값을
  삭제한다
exit :
SectionEnd
// 프로그램을 마친다.
```

6. 결 론

본 논문은 다양한 증상을 보이는 악성코드의 특성을 파악하며 최적화된 대응 도구를 통해 악성코드 감염 상황을 분석하여 사전 방역을 위해 스크립트를 이용하는 악성코드 대응 기술을 확인 하였다. 악성코드의 예방을 위해 바이러스 백신 프로그램 등을 사용하기도 하지만, 신종 악성코드의 네트워크를 통한 급속한 확산이 발생할 때 대응을 위해 어떻게 분석하고 방역 처리를 하는지에 대해 연구하였다. 스크립트 기반 설치 프로그램은 대응을 위해 악성코드의 감염 현황 및 특성에 맞게 쉽게 스크립트를 작성하여 대응할 수 있는 장점이 있다. 또한 윈도우의 파일 및 레지스트리 값 생성, 삭제 및 변경이 가능하여 악성코드의 감염 현상에 대한 모든 부분의 방역 처리가 가능하다.

하지만 스크립트를 이용하여 개인 사용자 및 기업 관리자가 대응하기에는 악성코드의 분석 후 스크립트를 사용하여 컴파일 해야 하기 때문에 시간이 오히려 많이 걸리고 시행착오가 있을 수 있다. 따라서 사용자가 쉽고 빠르게 대응하기 위해서는 별도로 사전 방역을 할 수 있는 유저인터페이스를 구성하는 프로그램이 필요하다.

앞서 언급한 것과 같이 악성코드 감염의 특징은 정형화 되어 있다는 것이다. 이 정형화된 패턴을 이용하여 유저 인터페이스를 제공하는 이화된 대응 프로그램을 제작하여 사용자에게 제공하여야 할 것이다.

참 고 문 헌

[1] 표준번호 TTAS.KO-12.0010/R1, 악성코드 감염 예방을 위한 지침, 한국정보통신기술협회, 2006.

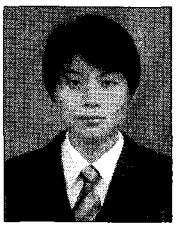
[2] 안철수연구소, 개인정보보호수칙 10계명, http://home.ahnlab.com, 2008.

[3] 정관식, 악성코드대응교육, 조선대학교 CERT 교육자료, 2008.

[4] 장영준, 빛자루 PC 백과 악성코드 증가와 조기 대응의 필요성, 안철수연구소, 2007.

[5] 윤여창, 컴퓨터바이러스의 현황과 대책, 우석대학교 전산정보학부 전산통계학과, 2003.

[6] Mark Russinovich, Sysinternals Process Utilities, http://www.sysinternals.com, 2008.

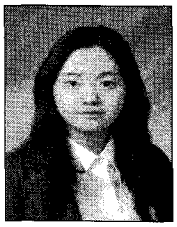


임 원 규

2008년 서울산업대학교 산업정보시스템공학과(학사)
현재 서울산업대학교 IT정책대학원 석사과정(산업정보시스템전공)

이 정 현

2002년 중앙대학교 정보산업대학원 석사(정보보호 및 인터넷)
현재 고려대학교 정보경영공학전문대학원(박사과정)

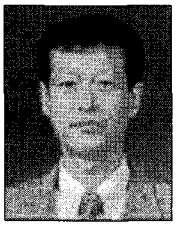


임 수 진

2006년 서울산업대학교 산업정보시스템공학과 입학
현재 서울산업대학교 산업정보시스템공학과 네트워크 보안 Lab 연구원

박 원 형

2002년 서울산업대학교 산업정보시스템공학과 (공학사)
2005년 서울산업대학교 정보산업공학과(공학석사)
2009년 경기대학교 정보보호학과 이학박사 (정보보호전공)
현재 서울산업대학교 산업정보시스템공학과 겸임교수



국 광 호

1979년 서울대학교 공과대학 (공학사)
1981년 서울대학교 대학원 공학 (석사)
1984년 청주대학교 산업공학과 전임강사
1989년 Georgia Institute of Technology, U.S.A (공학박사)
1993년 한국전자통신연구원 선임연구원
현재 서울산업대학교 산업정보 시스템공학과 교수