메일필터링을 통한 E-mail 보안

CERTCC-KR

이현우, lotus@certcc.or.kr
백원민, 100@sunoo.com
하도윤, dyha@certcc.or.kr
김상철, ksch@certcc.or.kr

[목 차]

1. 개요

Firewall이 널리 보급되면서 서버의 보안 취약점에 대한 공격은 효과적으로 방어할 수 있게 되었다. 반면, E-mail 첨부파일, HTML이 내장된 E-mail 등을 이용한 공격은 아직 효과적인 대응방법이 없다. 특히, 이러한 공격은 대부분의 사이트에서 제공하는 서비스(E-mail, HTTPD 등)를 이용한 공격이기 때문에 더욱 탐지하거나 차단하기가 쉽지 않다. 최근의 인터넷 웜 공격은 이러한 취약점을 이용한 것으로 99년 Melissa 바이러스를 기점으로하여 급속히 증가하고 있다.

본 고에서는 E-mail과 관련된 보안 취약성에 대하여 알아보고 이에 대한 대응방법을 소개한다. 메일 서버 차원에서 각 조직의 메일 보안정책을 구현할 수 있도록 도와주는 Procmail 등과 같은 도구의 사용 및 기능에 대하여 설명한다.

※ 본 문서는 악성프로그램 예방지침의 참고자료로 작성된 자료이다.

악성프로그램 예방지침 : http://www.certcc.or.kr/paper/tr2000/2000-08/tr2000-08.htm

Top

2. E-mail를 이용한 공격방법

2.1 액티브 컨텐츠 공격

메일 열람시 HTML 기능이 있는 E-mail 클라이언트나 웹 브라우저를 사용하는 이용자를 대상으로 하는 공격기법이다. 주로 "자바스크립트"나 "비주얼베이직스크립트"등과 같은 HTML 또는 E-mail 클라이언트의 스크립팅 기능을 이용하여 피해자의 컴퓨터에서 정보를 유출하거나 악성 프로그램을 실행시킨다.

이러한 공격의 간단한 예로는 사용자가 메시지를 열어볼 때 음란사이트나 광고사이트를 보여주도록 하거나 또는 시스템을 마비시키는 서비스거부공격 공격 형태를 보여준다. 최근에 발견되는 VBS 웜을 예로 들수 있다.

※ AnnaKournikova : http://www.certcc.or.kr/cvirc/Alert/61/AnnaKournikova.html

이런 공격은 E-mail 클라이언트 프로그램의 버그나 시스템의 버그를 이용하는 것이 아니기 때문에 보안 패치로써 해결하지 못한다. 무었보다 E-mail 클라이언트의 스크립팅 기능을 사용하지 않도록 설정하는 것이 중요하다. 다음은 Outlook에서 스크립팅 기능을 제거하는 방법이다.

또 다른 방법으로는 메일서버에서 메일이 저장될 때 이러한 스크립트 태그를 다른 이름으로 바꾸어 자장하는 방법이 있다. 이렇게 함으로서 사용자가 메일을 읽을때는 메일 클라이언트는 스크립트를 해석하지 못하게된다.

2.2 버퍼오버플로우 공격

일반적인 버퍼오버플로우 공격과 마찮가지로 E-mail 서버 또는 클라이언트의 취약성을 이용하여 다양한 공격을 수행할 수 있다. 현재 메일서버로 많이 사용하고 있는 sendmail은 취약성이 많이 보완되어 왔으나, 메일 클라언트에서는 아직 많은 보안문제들이 발견되고 있다. Outlook Express, Netscape Mail 등에서 발견된 버퍼오버플로우 취약성은 공격자가 조작된 E-mail을 보내 피해자의 컴퓨터에서 임의의 명령을 실행하거나 트로이잔 같은 악성 프로그램을 심을 수 있도록 한다.

※ MS Outlook BufferOverflow : http://www.certcc.or.kr/advisory/ka2000/ka2000-025.txt

이러한 취약성은 메일서버 또는 메일클라이언트의 보안패치를 적용함으로서 해결할 수 있다. 또한 메일서버에서 조작된 E-mail 헤더나 첨부 헤더를 탐지하여 수정함으로서 메일 클라이언트 공격을 예방할 수 있다.

2.3 트로이잔 목마 공격

트로이잔 목마를 이용한 공격은 일반 사용자가 트로이잔 프로그램을 실행시켜 해당 시스템에 접근할 수 있는 백도어를 만들게 하거나 또는 시스템에 피해를 주게 한다. 이러한 공격의 예로는 분산 서비스 공격을 수행하는 Win/Trinoo 트로이잔, 패스워드와 같은 정보를 수집하는 스파이형 트로이잔, 그리고 시스템 자원을 사용하는 트로이잔에 이르기 까지 매우 다양하다.

이러한 공격이 성공하기 위해서는 피해자가 트로이잔을 실행시키도록 유도해야 되는데 이때 "사회공학 기법(Social engineering)"이 사용된다. "Loveletter", "annakournikova.jpg" 와 같은 이름은 사용자로 하여금 첨부파일을 실행시키도록 유도한다. 특히, 시스템 관리자를 사칭하여 첨부된 프로그램을 실행시키도록 하는 메일 메시지를 받았을 때는 반듯이 관리자에게 확인을 한 뒤 실행시켜야 한다.

특히, 윈도우 시스템은 디폴트로 파일이름의 확장자를 숨기도록 설정되어 있어, 공격자는 다음과 같은 파일명을 사용하여 트로이잔 실행파일이나 스크립트 파일의 확장자를 숨길 수 있다.

xxx.txt.vbs - txt 파일로 가장한 비주얼베이직 실행 스크립트

xxx.jpg.scr – jpg 그림파일로 가장한 스크린세이버 실행파일

xxx.mpg.dll – 동영상 파일로 가장한 dll 실행 파일

xxx.txt.exe – txt 파일로 가장한 실행 파일

이러한 공격을 당하지 않기 위해서는 메일을 통해 수신한 프로그램을 실행시키지 않아야 한다. 메일 첨부파일을 바로 더블 클릭하는 것은 매우 위험한 습관이다. 하지만 최근에는 이러한 사용자 주의를 우회할 수 있는 공격도 있다. E-mail 클라이언트의 버그 또는 잘못된 설계로 인하여 사용자의 간섭없이도 자동으로 트로이잔을 실행시킬수 있는 공격방법이 공개되어 있다.

이러한 공격을 예방하는 방법으로 메일서버에서 실행가능한 첨부파일 이름을 실행되지 못하는 이름으로 바꾸는 방법이 있다(예, exploit.exe를 exploit.defanged-exe 등으로 바꾸어 메일클라이언트에서 실행되지 않도록 한다). 또 다른 방법으로는 메일 첨부파일을 조작하여 첨부파일로 보이지 않도록 바꾸는 것이다. 사용자가 반듯이 첨부파일을 얻기 위해서는 시스템 관리자에게 연락하여야 한다. 이는 시스템관리자가 첨부파일을 점검할 수 있는 기회를 제공한다. 다음은 bugtraq, 뉴스그룹, 그리고 백신업체의 권고문에서 나오는 트로이잔 목마의 확장자와 파일이름 들이다.

*.asd	*.chm	*.dll	*.ocx	*.hlp
*.hta	*.js	*.pif	*.scr	*.shb
*.shs	*.vb	*.vbe	*.vbs	*.wsf
*.wsh	IBMls.exe	anti_cih.exe	aol4free.com	avp_updates.exe
*.[a-z][a-z][a-z0-9].[a-z0-9]+ (to catch "double-extension" attachments)				
babylonia.exe	badass.exe	buhh.exe	chocolate.exe	compu_ma.exe
happy99.exe	i-watch-u.exe	ie0199.exe	jesus.exe	list.doc
lovers.exe	navidad.exe	path.xls	photos17.exe	picture.exe
pretty park.exe	prettypark.exe	qi_test.exe	seicho_no_ie.exe	serialz.hlp
setup.exe	story.doc	suppl.doc	surprise!.exe	x-mas.exe
y2kcount.exe	yahoo.exe	zipped_files.exe		

트로이잔 공격의 또 다른 채널은 매크로 기능을 제공하는 프로그램의 데이터 파일을 이용할 수 있다. 최근의 워드프로세서, 스프레드쉬트, 데이터베이스 등은 이를 지원한다. 이러한 첨부파일을 열때는 항상 백신프로그램을 통하여 먼저 바이러스 감염여부를 확인하도록 해야 한다. 그리고 이러한 기능을 지원하는 프로그램에서 매크로를 자동으로 실행하는 모드를 제거해야 한다.

2.4 쉘 스크립트 공격

유닉스와 같은 시스템은 사용상의 편리와 확장을 위해 쉘 스크립트를 제공한다. 어떤 메일 프로그램은 메일 메시지를 처리할 때 내장된 쉘 명령을 지원하는데, 이를 잘못 사용하게 되면, 공격자는 조작된 메일헤더를 포함한 메일을 보내 해당 시스템에서 특정 명령이 수행되도록 할 수 있다. 이는 메일헤더를 검사하여 이러한 조작된 부분을 탐지할 수 있다.

Top

3. Procmail을 통한 E-mail 보안

"Procmail"은 강력한 메일 프로세서로 메일 메시지의 헤더와 본문에서 특정 정보를 찾아 정의된 규칙에 따라 적절한 조치를 수행하는 프로그램이다. procmail의 설치, 설정 등과 관련된 자세한 내용은 다음 링크를 참조 바란다.

·관련 한글문서 : http://trade.chonbuk.ac.kr/~leesl/procmail/index.html

·procmail 최신버전 : http://www.procmail.org/

procmail 설치하기

a. procmail 최신버전(procmail-3.15.1) 다운로드

- http://www.procmail.org/

b. 압축을 풀고 압축을 푼 디렉토리로 이동

```
# tar -xvf procmail-3.15.1.tar.gz
# cd procmail-3.15.1
```

c. procmail 설치

```
# make install 또는
# make install-suid
```

※ 보안을 위해서는 make install-suid를 하는 것이 바람직

3.1 Sanitizer 설치

다음 사이트에서 제공되는 "sanitizer"라는 procmail ruleset은 앞서 설명한 E-mail을 이용한 모든 공격에 효과적으로 대응할 수 있도록 해준다. "sanitizer" 파일을 윈도우 시스템에서 다운로드 받을 경우에는 각라인에서 DOS 시스템의 "end-of-line" 문자를 제거해 줘야 한다. 잘 모르면 유닉스에서 다운로드 받아 수정하지 않고 그대로 사용하면 된다.

·Procmail 보안 홈페이지

ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-security.html

·sanitizer 다운로드 URL

http://www.impsec.org/email-tools/procmail-sanitizer.tar.gz

ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-sanitizer.tar.gz

위 사이트중 한군데서 다운로드 받은 파일의 압축을 풀면, 관련 설명 문서들과 sanitizer 설정파일인 "html-trap.procmail", 그리고 필터링해야될 파일 목록이 있는 "poisoned-files" 파일이 생기게 된다.

자동으로 모든 사용자의 E-mail에 대하여 필터링하기 위해서는 다음과 같이 "Sanitizer" 룰셋을 설치하면 된다.

o Sanitizer 설치를 위한 요구사항

- procmail이 설치되어 있어야 한다.

- sendmail을 이용할 경우 Local Delivery Agent로 procmail을 사용하도록 설정되어 있어야 하는데 이는 /etc/sendmail.cf 파일에서 다음과 같이 설정하면 된다.

```
Mlocal, P=/usr/bin/procmail, F=lsDFMAw5:/|@qSPfhn9, S=10/30, R=20/40, A=procmail -Y -a $h -d $u
```

- perl이 설치되어 있어야 한다.

o 유닉스 시스템에서의 "sanitizer" 설치

- 소유자와 그룹이 root인 /etc/procmail 디렉토리를 755(rwxr-xr-x) 권한으로 설정
- 위의 ftp 사이트에서 sanitizer 룰셋을 다운받아 위 디렉토리에 저장하고 소유자와 그룹은 root로 그리고 권한은 644(rw-r--r--)로 설정한다.
- 설정 방법에 따라 룰셋을 설정한다.

※ 만약 게이트웨이로 사용되는 sendmail relay에서 필터링을 하고자 할 경우에는 다음 사이트를 참고하여 /etc/sendmail.cf 파일을 수정하고 /etc/procmail/filter.rc 파일을 만들어야 한다.

http://www.impsec.org/email-tools/procmail-on-gateway.txt

※ Outgoing 메일에 대한 필터링은 다음 사이트를 참고하여 /etc/sedmail.cf 파일을 수정하고 /etc/procmail/outgoing.rc 파일을 만들어야 한다.

http://trade.chonbuk.ac.kr/~leesl/procmail/outgoing_mail_filter.html

Top

3.2 Sanitizer 설정방법

sanitizer는 환경변수와 설정에 따라 통제되는데, 이는 "/etc/procmailrc" 이라는 파일을 통해 이루어진다.

다음은 기본적인 /etc/procmailrc 파일의 예이다.

```
PATH="/usr/bin:$PATH:/usr/local/bin"
SHELL=/bin/sh
POISONED_EXECUTABLES=/etc/procmail/poisoned
SECURITY_NOTIFY="postmaster, security-dude"
SECURITY_NOTIFY_VERBOSE="virus-checker"
SECURITY_NOTIFY_SENDER=/etc/procmail/local-email-security-policy.txt
SECRET="CHANGE THIS"
# this file must already exist, with proper permissions (rw--w--w-):
SECURITY_QUARANTINE=/var/spool/mail/quarantine
POISONED_SCORE=25
SCORE_HISTORY=/var/log/macro-scanner-scores
DROPPRIVS=YES
LOGFILE=$HOME/procmail.log
# Finished setting up, now run the sanitizer...
INCLUDERC=/etc/procmail/html-trap.procmail
# Reset some things to avoid leaking info to
# the users...
POISONED_EXECUTABLES=
SECURITY_NOTIFY=
SECURITY_NOTIFY_VERBOSE=
SECURITY_NOTIFY_SENDER=
SECURITY_QUARANTINE=
SECRET=
```

만약 이미 /etc/procmailrc 파일을 이용하고 있다면, 위 내용을 추가하면된다. 다음은 etc/procmailrc 파일에서 사용되는 각각의 환경변수에 대한 설명이다. 위 예에 포함되지 않는 것도 설명한다.

o MANGLE_EXTENSIONS

앞서 설명한 것 처럼 각 기관의 메일정책에 따라 첨부파일의 확장자 이름을 제한하는 방법중의 하나이다. 만약 첨부된 파일의 확장자가 ".exe"일 경우, ".mangled-exe"로 바꾸어 주는 역할을 한다. 이는 다음과 같은 보안상의 효과를 가져온다.

※ 첨부된 파일의 확장자를 다른 이름으로 바꿈으로서 클라이언트에서 이를 실행(더블클릭)했을 때 실행되지 않도록 하는 것이다. 이럴경우, 사용자가 첨부된 파일을 실행시키기 위해서는 먼저 파일을 저장한 다음에 이름을 바꾸고 실행시켜야 되기 때문에 백신이 바이러스를 검사할 기회를 갖게되는 것이다.

※ 자동실행되는 악성 코드일 경우에는 이름을 바꿈으로서 첨부된 코드를 찾지 못하도록 하여 공격을 방지할 수 있다.

Sanitizer는 다음과 같이 디폴트로 위험한 확장자에 대하여 MANGLE_EXTENSIONS 환경변수를 설정하고 있기 때문에 특별히 따로 설정할 필요가 없으나, 만약 각 기관의 메일정책에 따라 변경할 경우 또는 디폴트 설정이 불편한 경우에는 다음 라인을 수정하여 procmailrc 파일에 추가하면 된다. 단 "INCLUDERC=/etc/procmail/html-trap.procmail" 가 있는 라인 이전에 설정하여야 한다.

※ 디폴트 MANGLE_EXTENSIONS 설정 :

```
MANGLE_EXTENSIONS='html?|exe|com|cmd|bat|pif|sc[rt]|lnk|dll|ocx|do[ct]|xl[swt]|p[po]
t|rtf|vb[se]
?|hta|p[lm]|sh[bs]|hlp|chm|eml|ws[cfh]|ad[ep]|jse?|md[abew]|ms[ip]
|reg|asd|cil|pps|asx|wm[szd]'
```

* 주 : MANGLE_EXTENSIONS은 한 라인에 모든 확장자를 기입하여야 하며, 포맷이 틀릴 경우, 큰 문제가 발생할 수 있다. 포맷을 위에서처럼 확장자간에 "|" 문자를 이용하여 구분해 주면 된다.

또한 기관의 특성에 따라 보안레벨을 정의하여 구현할 수도 있다. 예를 들어 자신의 도메인내에서 오고가는 메일에 대해서는 엑셀파일과 워드 파일의 확장자를 그대로 보존하고자 할 경우에는 다음과 같이 할 수 있다.

/etc/procmailrc 파일에서 "INCLUDERC=/etc/procmail/html-trap.procmail" 라인 전에 다음과 같은 규칙을 설정한다.

```
:0

* ^From:.*<[a-z0-9]+@mydomain.com>

* ^To:.*<[a-z0-9]+@mydomain.com>

{

MANGLE_EXTENSIONS='html?|exe|com|cmd|bat|pif|sc[rt]|lnk|dll|ocx|dot|xl[wt]|p[po]
t|rtf|vb[se]
?|hta|p[lm]|sh[bs]|hlp|chm|eml|ws[cfh]|ad[ep]|jse?|md[abew]|ms[ip]
|reg|asd|cil|pps|asx|wm[szd]'

}
```

o POISONED_EXECUTABLES

바이러스가 주로 이용하는 파일이름의 목록을 가진 파일이름을 정의해 준다. 디폴트로 /etc/procmailrc 디렉토리에 "poisoned" 라는 이름의 파일을 지정하고 있으므로 poisoned 파일을 해당 디렉토리에 카피하면 된다. 현재는 MANGLE_EXTENSIONS에 나온 확장자에 대해서만 파일이름을 검사하도록 되어 있으나 다음버전에서 개선될 것이라고 한다. 디폴트로 필터링하는 파일이름은 1장에서 설명한 바와 같다. 특정 파일이름을 사용하는 바이러스나 웜이 나타날 때 마다 POISONED_EXECUTABLES에 의해 설정된 파일을 업데이트해 줌으로서 악성프로그램으로부터의 공격에 보다 적절히 대응할 수 있는 기능을 제공한다.

```
POISONED_EXECUTABLES=/etc/procmail/poisoned
```

o DISABLE_MACRO_CHECK

Microsoft Office의 위험한 매크로에 대한 검사기능을 제거한다. sanitizer는 Word documents, Excel spreadsheets, PowerPoint presentations 등의 첨부파일을 검사하여 위험한 VBA 매크로(보안 설정을 변경기키거나, 레지스트리를 변경하는 등의 매크로)를 찾아내는 기능이 있다. 만약 이러한 기능을 사용하지 않으려면 다음과 같이 DISABLE_MACRO_CHECK 값을 임의의 값으로 설정하면 된다.

DISABLE_MACRO_CHECK=YES

만약 위 기능을 이용하려면 다음과 같은 추가적인 도구를 설치하여야 한다.

※ metamail package의 일부인 mimencode

※ mktemp

리눅스에서는 대부분 배포판에 포함되어 있으나 다른 종류의 유닉스에서는 소스를 다운받아 컴파일하고 설치해야 한다.

Top

o POISONED_SCORE

sanitizer는 위험한 매크로 코드의 모든 부분을 탐지할 때마다 이를 카운트하여, 일정 수준이 되면 해당 문서를 감염□다고 판단한다. 디폴트로 25로 설정되어 있으나 대부분의 매크로 바이러스는 100이상의 수치를 갖는다. 따라서 80 - 100 정도의 값을 갖도록 하는 것이 바람직 하다.

POISONED_SCORE=100

o SCORE_HISTORY

POISONED_SCORE 값이 적절히 설정되었는지 알아보기 위해 매크로 검사 결과를 기록할 수 있다. 다음과 같이 SCORE_HISTORY를 설정하면 된다. 해당 파일은 (rw--w--w-)의 권한을 가져야 한다.

SCORE_HISTORY="/var/spool/mail/macro-scanner-scores"

o SECURITY_QUARANTINE

sanitizer의 규칙에 따라 감염된(poisoned) 또는 감염된 것으로 판단된 메시지를 보관해두는 장소를 설정한다. 이러한 메시지는 수신자에게 가지 않고 설정된 파일에 쌓이게 된다. 해당 파일은 (rw--w--w-)의 권한을 갖도록 설정하여야 하며, 파일 내용은 표준 메일박스 형태로 쌓이게 된다. 만약 SECURITY_QUARANTINE 값이 설정되지 않으면 감여된 메일은 수신자에게 가게 된다.

SECURITY_QUARANTINE="/var/spool/mail/quarantine"

o SECURITY_NOTIFY

감염된 파일이 탐지되었을 때, 해당 사실을 누구에게 공지할 것인가는 설정한다. 공지는 필터링된 메시지의 헤더를 포함한다. 또한 QUARANTINE이 실패할 경우도 이 사실을 SECURITY_NOTIFY에 설정된 사용자에게 공지하게 된다.

SECURITY_NOTIFY="postmaster, dilbert@example.com"

o SECURITY_NOTIFY_VERBOSE

SECURITY_NOTIFY와 같으나, 필터링된 메시지의 원문이 포함된다. 이는 quarantine 파일 대신에 사용될 수도 있다.

SECURITY_NOTIFY_VERBOSE="wally@example.com, hb@example.com"

o SECURITY_NOTIFY_SENDER

감염된 메시지를 보낸 사람에게 해당 사실을 통지할 것인가를 설정한다. 이를 위해서는 SECURITY_NOTIFY 값이 반듯이 설정되어 있어야 한다. 만약 경고 메시지에 각 기관의 보안정책을 포함하는 등의 것으로 수정하고 싶을 경우에는 파일로 만들어 설정해 주면 된다. 디폴트 메시지를 사용할 경우에는 존재하지 않는 파일이름으로 설정한다.

SECURITY_NOTIFY_SENDER=YES 또는

SECURITY_NOTIFY_SENDER="/etc/procmail/policy-note.txt"

o SECURITY_NOTIFY_RECIPIENT

감염된 메일의 수신자에게 해당 사실을 공지할 것인가를 설정한다. 하지만 메일 릴레이에서는 제대로 작동하지 않으므로 설정하지 않는 것이 좋다.

SECURITY_NOTIFY_RECIPIENT="/etc/procmail/quarantined.txt"

o SECURITY_STRIP_MSTNEF

Microsoft Outlook 과 Microsoft Exchange는 "Outlook Rich Text"라는 포맷을 지원하는데, 이는 모든 종류의 파일 첨부를 Microsoft 포맷 첨부로 묵어주는 역할을 한다. 일반적으로 "WINMAIL.DAT"라는 이름으로 사용되며, "MS-TNEF" 포맷으로 불리운다. 그리고 다른 메일 클라이언트에서는 호환되지 않는다. MS-TNEF는 일반적으로 필터링되지 않으며, 파일내에 송신자의 설정정보를 포함하기 때문에 정보를 유출시킬 수도 있다. MS에서도 MS-TNEF 포맷의 첨부는 조직 내에서만 사용할 것을 권장하고 있다.

SECURITY_STRIP_MSTNEF을 임의의 값으로 설정하게 되면 메시지에서 이러한 첨부를 잘라내게 되며, 해당 사실을 공지하는 내용과 함께 수신자에게 보내지게 된다. 파일 첨부는 복구될 수 없다.

SECURITY_STRIP_MSTNEF=YES

Top

※ 참고자료

See http://support.microsoft.com/support/kb/articles/Q241/5/38.ASP,

http://support.microsoft.com/support/kb/articles/Q138/0/53.ASP

http://www.microsoft.com/TechNet/exchange/2505ch10.asp

o DEFANG_WEBBUGS

"Web bugs" 는 아주 조그마한 이미지로 email 메시지를 추적하는데 사용된다. 이미지를 표시하는 URL을 포함시켜, HTML 기능이 있는 메일 프로그램이 해당 이미지를 표시하기 위해 지정된 URL에 접속할 때, 이를 기록하여 메일 메시지의 위치를 확인하는 방법이다. 이러한 방법은 특히, 스팸 메일이 실제 사용자에게 도달하였는지를 확인하는데 사용되기도 하며, 또는 메시지의 전달을 추적하는데 사용된다. 그리고 이는 음성파일을 이용해 구현될 수도 있다.

만약 이러한 것이 각 기관의 보안정책 또는 개인정보보호정책에 위반되는 것이라면 DEFANG_WEBBUGS 환경변수를 이용하여 이를 막을 수 있다. DEFANG_WEBBUGS 값을 임의의 값으로 설정하면 sanitizer는 <IMAGE> 와 <BGSOUND> 태그를 수정하여(defang) 이러한 정보수집 행위를 막게된다.

DEFANG_WEBBUGS=YES

o SECURITY_TRUST_STYLE_TAGS

<STYLE> 태그는 공격자가 스크립팅 명령을 사용하도록 하여 다양한 공격을 할 수 있는 기회를 제공한다. Sanitizer는 디폴트로 <STYLE> 태그를 변경시킨다. 하지만 만약 내부 도메인에서 만들어진 <STYLE> 태그에 대하여 변경시키지 않기를 원할 경우에는 다음과 같이 설정할 수 있다. 외부사용자(인터넷)으로부터의 <STYLE> 태그는 제한하는 것이 바람직 하다.

```
:0
* ^From:.*@mydomain.com>
* ^To:.*@mydomain.com>
{
SECURITY_TRUST_STYLE_TAGS=YES
}
```

o LOGFILE

sanitizer의 로그 파일을 지정한다. 디폴트로는 메일 수신자의 홈디렉토리인 "$HOME/procmail.log"로 지정되어 있으나, 하나의 집중된 파일로 만드는 것이 바람직 하다. 파일 권한은 (rw--w--w-)로 설정해야 한다. 사용자 홈디렉토리에 만들 경우에는 이전에 DROPPRIVS=YES를 설정하여야 한다.

```
DROPPRIVS=YES
LOGFILE="$HOME/procmail.log"
```

기타 다른 많은 환경변수 설정이 있는데, 이는 Procmail 맨페이지를 참조하기 바란다.

```
man procmail
man procmailrc
man procmailex
```

Top

3.3 다양한 보안정책 구현을 위한 설정

앞서 설명한 procmailrc 파일은 모든 메시지에 대하여 동일한 보안 정책을 적용시킨다. 하지만 경우에 따라서 특정 도메인 별로 서로 다른 보안정책을 구현할 수도 있을 것이다. 이는 처리되는 메일에 따라 서로 다른 환경변수 값을 설정함으로서 구현 가능하다. 예를 들어 자신의 도메인 내에서는(아래 예의 경우 "mydomain.com") 워드 문서 첨부를 허용할 경우에는 다음과 같은 설정을 추가하면 된다. 단 "INCLUDERC=html-trap.procmail" 라인 이전에서 설정해야 한다.

```
:0

* ^From:.*<[a-z0-9]+@mydomain.com>

* ^To:.*<[a-z0-9]+@mydomain.com>

{

MANGLE_EXTENSIONS='html?|exe|com|cmd|bat|pif|sc[rt]|lnk|dll|ocx|dot|xl[wt]|p[po]
t|rtf|vb[se]
?|hta|p[lm]|sh[bs]|hlp|chm|eml|ws[cfh]|ad[ep]|jse?|md[abew]|ms[ip]
|reg|asd|cil|pps|asx|wm[szd]'

}
```

3.4 자가 보안 필터 구현

Sanitizer가 제공하는 quarantine(격리)과 notification(공지) 기능은 각 기관의 특정 보안정책에 따라 유연하게 사용할 수 있다. Sanitizer는 메시지에 포함된 "X-Content-Security"라는 헤더를 통해 notification과 quarantine 기능을 구현할 수도 있다. 즉, 사용자는 procmail 규칙을 통하여 특정 메시

지에 대하여 Sanitizer가 quarantine(격리)이나 notification(공지) 할 수 있도록 할 수 있다.

예를 들면, Hybris 웜은 임의의 이름을 가진 첨부파일을 제목없이 보냄으로서 유포시키는데, 모든 .exe 첨부를 필터링하지 않고 이를 탐지하여 필터링하기 위한 방법은 다음과 같다.

1. /etc/procmail/local-rules.procmail (owner root, group root, mode 644) 파일 작성

```
# Messages with .EXE attachments must have a subject line
#
:0
* !^Subject:
* ^Content-Type:.*multipart/mixed;
{
:0 B hfi
* ^Content-Disposition:.*₩.EXE
* ^Content-Type:.*₩.EXE
| formail -A "X-Content-Security: NOTIFY" ₩
-A "X-Content-Security: QUARANTINE" ₩
-A "X-Content-Security: REPORT: Trapped anonymous .EXE"
}
```

2. /etc/procmailrc 파일 수정

INCLUDERC=/etc/procmail/html-trap.procmail 라인을 다음과 같이 수정
INCLUDERC=/etc/procmail/local-rules.procmail
INCLUDERC=/etc/procmail/html-trap.procmail

위 설정은 procmail 룰셋을 통하여 anonymous 웜을 탐지하고, X-Content-Security 헤더를 삽입하게 된다. 그리고나서 sanitizer를 호출하여 이를 처리하는 것이다. sanitizer는 해당 메시지를 필터링하여 격리시키게 된다.

Top

4. Inflex 보안도구를 통한 E-mail 보안

Inplex는 메일서버에서 로컬이나 외부로 나가는 E-Mail을 검사하여 E-mail에 대한In-Outbound 정책을 새울수 있게 해주는 도구이다. 이러한 In-Outbound 정책기능을 통하여 관리자는 최근의 바이러스나 인터넷 웜이 첨부된 메일을 필터링할 수 있도록 해준다. 또한 임의 파일 이름과 파일 유형에 대하여 검색하고 필터링하는 기능을 제공하여 Anti-virus 패키지에 의해 탐지되지 않는 바이러스로부터의 공격에 대응할 수 있도록 해준다. Procmail을 이용한 필터링보다는 설치 및 운영이 쉬운반면, Inflex는 첨부파일만을 필터링할 수 있다.

Inflex는 sendmail이 sendmail.cf 대신에 inflex.cf 파일을 설정파일로 사용하도록 함으로서 원하는 기능을 구현한다. inflex.cf 설정에 따라 inflex 프로그램이 메일에 대하여 검사를 하게 된다. inflex의 룰셋으로 차단된 메일은 송·수신자와 서버관리자에게 경고 메시지를 보내게 되고, 룰셋에서 통과된 메일은 다시 sendmail.cf 가 적용되도록 하여 정상적인 메일 처리를 하게 된다.

4.1 Inflex 설치 및 실행

a. 다음 사이트에서 최신버전의 Inflex(Inflex-0.1.5c.tar.gz)를 다운로드 받는다.

http://www.inflex.co.za/mainpage.html

b. Inflex 도구를 gzip, tar를 통하여 압축을 푼다.

```
# gzip -d Inflex-0.1.5c.tar.gz
# tar -xvf Inflex-0.1.5c.tar
```

```
# cd Inflex-0.1.5.c
```

c. inflex가 사용할 메일큐 디렉토리 생성

```
# mkdir /var/spool/inflexmq
```

d. inflex 실행 파일을 /usr/sbin에 복사

```
# cp inflex /usr/sbin
```

e. inflex 설정파일인 inflex.cf 파일을 /etc 디렉토리에 복사

```
# cp inflex.cf /etc
```

f. 실행되고 있는 모든 sendmail 데몬을 종료시킨다.

```
# killall sendmail
```

g. sendmail이 /etc/inflex.cf 파일을 참조하여 실행되도록 한다.

```
# /usr/sbin/sendmail -bd -C/etc/inflex.cf
```

Top

4.2 Inflex 룰셋 설정

Inflex 프로그램이 메일을 검사하는 과정은 다음과 같다.

. inflex에서 사용될 변수를 초기화 한다
. email 분석을 위한 디렉토리를 설정한다.
. email을 읽어들인다.
. email에 대한 자세한 내용을 로그한다.
. email을 디코드한다.
. 파일 타입에 따라 email을 스캔한다.
. 파일이름에 따라 email을 스캔한다.
. 바이러스에 대하여 email을 스캔한다.
. 필요한 경우 관리자, 송신자, 수신자에게 메시지를 보낸다.

가. 파일타입에 따라 필터링하는 방법

Inflex에서 디포트로 필터링하는 파일타입은 다음과 같으나, inflex 스크립트 실행파일을 수정하여 더 추가하거나 제거할 수 있다.

o 디폴트로 필터링되는 파일 Types

- MS-DOS Executables
- PC Bitmap Data [BMP files]
- AVI movies
- MPEG movies
- WAVE type audio files

파일타입에 따른 필터링 규칙을 수정하기 위해서는 /usr/sbin/inflex 파일의 124번 라인 근처에서 다음과 같은 내용을 찾아 수정한다.

```
grep "MS-DOS executable" ${tmpdir}/fileresults >> ${badfileslog}
grep "PC bitmap data" ${tmpdir}/fileresults >> ${badfileslog}
grep "AVI" ${tmpdir}/fileresults >> ${badfileslog}
grep "MPEG" ${tmpdir}/fileresults >> ${badfileslog}
```

```
grep "WAVE" ${tmpdir}/fileresults >> ${badfileslog}
```

만약 새로운 파일 타입을 추가할 경우, 예를 들어 ARB를 추가한다고 하면 다음과 같은 라인을 추가하면 된다.

```
grep "ARB" ${tmpdir}/fileresuls >> ${badfileslog}
```

주 : 여기서 파일타입은 /etc/magic 파일에 존재하여야 한다. 만약 존재하지 않으면 다음에서 설명하는 파일이름으로 필터링하는 방법을 사용하면 된다.

나. 파일이름으로 필터링하는 방법

파일이름이나 확장자에 따라 메일을 필터링할 수 있는데, 이는 /usr/sbin/inflex 파일의 136번 라인 근처에서 다음과 같은 내용을 찾아 수정하면 된다.

```
find ${tmpdir} -iname 'links.vbs' >> ${badfileslog}
find ${tmpdir} -iname '*.mp3' >> ${badfileslog}
find ${tmpdir} -iname '*.ppt' >> ${badfileslog}
```

만약 새로운 파일 이름을 추가할 경우, 예를 들어 ".CTP"를 추가한다고 하면 다음과 같은 라인을 추가하면 된다.

```
find ${tmpdir} -iname '*.CTP' >> ${badfileslog}
```

여기서 필터링해야될 파일이름 및 확장자는 1장에서 설명한 확장자 및 파일이름에 대하여 모두 필터링 하면된다.

```
*.asd, *.chm, *.dll, *.ocx, *.hlp, ... *.vbs, story.doc, suppl.doc, surprise!.exe ...
```

또 다른 예로 파일명중에서 특정 문자열을 필터링하기 원할 경우, 예를 들어 VBS Love Letter 웜바이러스를 예를 들면 다음과 같은 라인을 추가하면 된다.

```
${find} ${tmpdir} -iname 'LOVE-LETTER-FOR-YOU*' >> ${badfileslog}
```

주 : iname 옵션은 대소문자를 구분하지 않도록 하며, 와일드카드 문자를 사용할 수 있어 유연한 규칙을 사용할 수 있다.

다. 경고 메시지 설정 방법

필터링된 메일 메시지에 대하여 경고 메시지를 보내도록 설정할 수 있는데 이는 /usr/sbin/inflex 파일의 232번 라인 근처에서 찾을 수 있으며, 경보 메시지를 보내고자 하는 사람만을 지정해 주면 된다.

4.3 Virus Scanner(백신)과의 연동

다음 사이트를 방문하여 평가판을 다운로드하여 설치하면 된다.

sophos 백신 : http://www.sophos.com/downloads/eval/savunix.html

uvscan 백신 : http://www.nai.com/asp_set/buy_try/try/products_evals.asp

[참고 자료]

[1] 악성 프로그램(virus/worm/trojan) 예방지침, http://www.certcc.or.kr/paper/tr2000/2000-08/tr2000-08.htm

[2] 프락메일에 관하여, http://trade.chonbuk.ac.kr/~leesl/procmail/index.html

[3] Procmail, http://www.procmail.org/

[4] Enhancing E-Mail Security With Procmail the E-mail - Sanitizer
ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-security.html

[5] Inflex, http://www.inflex.co.za/mainpage.html

[6] Anomy Sanitizer, http://mailtools.anomy.net/

[7] Mimedefang, http://www.roaringpenguin.com/mimedefang/

Top