GREW.A 웜 정보

□ 개 요

대량의 메일 및 윈도우의 취약한 암호설정을 악용하여 전파되는 Grew 웜의 감염피해가 발생하고 있어 주의 필요. 감염 시, 감염시스템 내에 저장되어 있는 메일주소를 검색하여,검색된 메일주소로 웜 전파를 위한 악성메일 발송. 웜은 매월 3일 ppt,zip,doc,pdf 등 특정 확장명을 가지는 파일을 파괴하므로 각별한 주의 필요. 또한 마우스 및 키보드 사용 시 장애가 발생하며, 일부 보안 프로그램을 종료 및 삭제함.

□ 감염 대상 시스템

Windows 9X, ME, 2000, NT, XP, 2003

□ 웜 확산 방법

웜 복사본을 첨부한 대량의 메일을 발송하거나, OS의 취약한 암호설정을 악용하여 전파

□ 웜이 발송하는 메일유형

웜은 다음 유형으로 메일을 전송하므로, 아래와 같은 메일을 수신할 경우 첨부를 실행시키지 않도록 주의 필요.

* 제목: 아래 형태 중 하나

- "A Great Video"
- "Arab sex DSC-00465.jpg"
- "eBook.pdf"
- "Fw:"
- "Fw: DSC-00465.jpg"
- "Fw: Funny :)"
- "Fw: Picturs"
- "Fw: Real show"
- "Fw: SeX.mpg"
- "Fw: Sexy"
- "Fwd: Crazy illegal Sex!"
- "Fwd: image.jpg"
- "Fwd: Photo"
- "give me a kiss"
- "04.pif"
- "Miss Lebanon 2006"
- "My photos"
- "Part 1 of 6 Video clipe"
- "Photos"
- "Re:"
- "School girl fantasies gone bad"

* 메일 본문: 아래 형태 중 하나

- ">> forwarded message"
- "forwarded message attached."
- "Fuckin Kama Sutra pics"
- "hello,"
- "Helloi attached the details."
- "Hot XXX Yahoo Groups"
- "how are you?"
- "i just any one see my photos."
- "i send the details."
- "i send the file."
- "It's Free :)"

- "Note: forwarded message attached. You Must View This Videoclip!"
- "Please see the file."
- "Re: Sex Video "
- "ready to be FUCKED ;)"
- "Thank you"
- "The Best Videoclip Ever"
- "the file i send the details"
- "VIDEOS! FREE! (US$ 0,00)"
- "What?"

* 첨부 형태:

- 04.pif
- 007.pif
- 392315089702606E-02,.scR
- 677.pif
- Adults_9,zip.sCR
- ATT01.zip.sCR
- Attachments[001],B64.sCr
- Clipe,zip.sCr
- document.pif
- DSC-00465.Pif
- DSC-00465.pIf
- eBook.pdf
- eBook.PIF
- image04.pif
- New Video,zip
- New_Document_file.pif
- photo.pif
- Photos,zip.sCR
- School.pif
- SeX,zip.scR
- Sex.mim
- Video_part.mim
- WinZip,zip.scR
- WinZip.BHX
- WinZip.zip.sCR

- Word XP.zip.sCR
- Word.zip.sCR

□ 감염 시 증상

- 매월 3일이 되면, 아래 확장자를 가지는 모든 파일 내용을 32byte길이의 " DATA Error [47 0F 94 93 F4 F5] " 내용으로 덮어쓴다. 기존 데이터는 삭제됨.

*.ppt
*.doc
*.pdf
*.xls
*.zip
*.rar
*.mdb
*.mde
*.pps
*.psd
*.dmp

- 파일 생성

"시스템 폴더" \ scanregw.exe
"윈도우폴더" \ Rundll16.exe

"시스템 폴더" \ SAMPLE.ZIP
"시스템 폴더" \ New WinZip File.exe
"시스템 폴더" \ sample.zip
"시스템 폴더" \ Update.exe
"시스템 폴더" \ Winzip.exe
"시스템 폴더" \ WINZIP_TMP.EXE

※ "윈도우 폴더":

C: \ Windows 또는 C: \ Winnt

"시스템 폴더":

Windows 95/98/Me	C: \ Windows \ System
Windows NT/2000	C: \ Winnt \ System32
Windows XP	C: \ Windows \ System32

- 레지스트리 생성

HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \
Windows \ CurrentVersion \ Run
ScanRegistry = "scanregw.exe /scan"

- 마우스 및 키보드 사용 장애 발생

- 일부 보안 프로그램 종료 및 삭제

kaspersky, McAfee, TREND MICRO, Symantec 등의 보안 프로그램을 종료하고 삭제시킨다

- 특정 사이트에 접속

http://webstats.web.rcn.net/cgi-bin/Count.cgi?df=765247

□ 감염 예방 방법

- 확인되지 않은 메일의 첨부 파일을 실행하지 않음.

- 윈도우 OS 암호를 추측하기 어렵게 설정.

불필요한 네트워크 공유를 해제하고 필요할 경우는 반드시 암호설정

- 백신을 최신으로 업데이트 및 주기적인 점검

□ 감염 시 치료 방법

1. 윈도우를 안전모드로 부팅. 부팅 시 F8을 누른 후 안전 모드 선택

2. 웜이 생성한 악성 코드 삭제

   탐색기 -> 도구 -> 폴더 옵션 -> 보기 에서

   "보호된 운영 시스템 파일 숨기기" 를 해제 및
   "숨김 파일 및 폴더 표시" 에 체크한 후 확인을 누른다
   (악성코드 삭제 후에는 원복함).

   아래의 웜이 생성한 아래의 파일을 삭제한다.

   "시스템 폴더" \ scanregw.exe
   "윈도우 폴더" \ Rundll16.exe
   "시스템 폴더" \ Update.exe

   또한, 시스템 폴더에 아래 이름의 파일이 존재할 경우 삭제한다.

   "시스템 폴더" \ SAMPLE.ZIP
   "시스템 폴더" \ New WinZip File.exe
   "시스템 폴더" \ sample.zip
   "시스템 폴더" \ Update.exe
   "시스템 폴더" \ Winzip.exe
   "시스템 폴더" \ WINZIP_TMP.EXE

3. 웜이 생성한 레지스트리 삭제

   HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \
   Windows \ CurrentVersion \ Run
   ScanRegistry = "scanregw.exe /scan"

4. 재 부팅