Malware Report

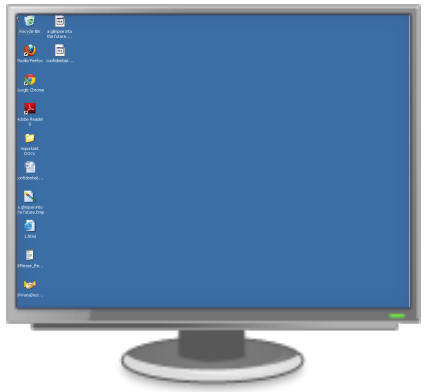
Emulated On: Microsoft Windows XP 32 bit, SP3, Office 2003, Office 2007, Adobe Acrobat Reader 9.0, Adobe Flash Player 9, Java SE 1.6.0

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c...

Malicious Activity Detected

Type	exe
Size	3.4 MB
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467

Download malicious file



Emulation Screenshot

4 Suspicious Activities

Behaves like a known malware (Generic.MALWARE.1b25)
Malware activity observed (Trojan-Ransom.Win32.Wanna.b)
Malware detected (Gen:Variant.Graftor.369176)
Malware signature matched (Trojan-ransom.Win32.Wcry.U.lzpjh)

4 Affected Processes

4 Processes Created | 2 Processes Terminated | 0 Processes Crashed

C:\WINDOWS\system32\attrib.exe
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\cscript.exe
C:\te files\taskdl.exe

13 Affected Registry Keys

13 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Multimedia\Audio
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\MSACM
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\Priority v4.00

more

33 Affected Files

22 Files Created | 25 Files Modified | 4 Files Deleted

C:\$LogFile
C:\Documents and Settings\admin\Desktop\@Please Read Me@.txt
C:\Documents and Settings\admin\Desktop\@WanaDecryptor@.exe
C:\Documents and Settings\admin\Desktop\a glimpse into the future.bm.

more

Emulation Screen Shots

2

Emulation Screen Shots

3

Table of Contents

Malware Residues (1 out of 5) 5

Suspicious Activities
Behaves like a known malware (Generic.MALWARE.1b25)
Malware activity observed (Trojan-Ransom.Win32.Wanna.b)
Malware detected (Gen:Variant.Graftor.369176)
Malware signature matched (Trojan-ransom.Win32.Wcry.U.lzpjh)

Processes Spawned or Interacted with
C:\WINDOWS\system32\attrib.exe (Terminated ,Started)
C:\WINDOWS\system32\cmd.exe (Started)
C:\WINDOWS\system32\cscript.exe (Started)
C:\te_files\taskdl.exe (Terminated ,Started)

Files Changed
C:\$LogFile (Modified)
C:\Documents and Settings\admin\Desktop\@Please_Read_Me@.txt (Created ,Modified)
C:\Documents and Settings\admin\Desktop\@WanaDecryptor@.exe (Created ,Modified)
C:\Documents and Settings\admin\Desktop\a glimpse into the future.bmp (Modified)
C:\Documents and Settings\admin\Desktop\a glimpse into the future.bmp.WNCRYT (Created ,Modified)

Malware Residues (2 out of 5)

6

Files Changed
C:\Documents and Settings\admin\Desktop\confidential.docx (Modified)
C:\Documents and Settings\admin\Desktop\confidential.docx.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\@Please_Read_Me@.txt (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed.zip (Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed.zip.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\@Please_Read_Me@.txt (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\a glimpse.bmp (Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\a glimpse.bmp.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\confidential.docx (Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\confidential.docx.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\roadmap_2021.pptx (Modified)

Malware Residues (3 out of 5)

7

Files Changed
C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\~SD3.tmp (Created ,Deleted)
C:\Documents and Settings\admin\Desktop\important DOCs\a glimpse into the future.bmp (Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\a glimpse into the future.bmp.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\confidential.docx (Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\confidential.docx.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\roadmap_2021.pptx (Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\roadmap_2021.pptx.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\Desktop\important DOCs\~SD2.tmp (Created ,Deleted)
C:\Documents and Settings\admin\Desktop\~SD1.tmp (Created ,Deleted)

Malware Residues (4 out of 5)

Files Changed
C:\Documents and Settings\admin\My Documents\roadmap_2021.pptx.WNCRYT (Created ,Modified)
C:\Documents and Settings\admin\My Documents\~SD4.tmp (Created ,Deleted)
C:\te_files\219161325495940.bat (Created)
C:\te_files\@WanaDecryptor@.exe (Created)
C:\te_files\taskdl.exe (Created)
C:\te_files\taskse.exe (Created)

Registry Keys Modified
HKCU\Software\Microsoft\Multimedia\Audio (Modified)
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager (Modified)
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\MSACM (Modified)
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\Priority v4.00 (Modified)
HKCU\Software\Microsoft\Windows Script Host\Settings (Modified)
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders (Modified)
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal (Modified)
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders (Modified)
HKCU\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing (Modified)
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed (Modified)

Malware Residues (5 out of 5)

9

Registry Keys Modified
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings (Modified)
HKLM\SOFTWARE\WanaCrypt0r (Modified)
HKLM\SOFTWARE\WanaCrypt0r\wd (Modified)

Unexpected Activities By Time (1 out of 7)

10

Elapsed Time	Type	Action
00:00:04	Registry Create	C:\te_files\emulatedFile58511_1.exe **Created** HKLM\SOFTWARE\WanaCrypt0r
00:00:04	Registry Set	C:\te_files\emulatedFile58511_1.exe **Set** HKLM\SOFTWARE\WanaCrypt0r\wd
00:00:05	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\te_files\taskdl.exe
00:00:05	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\te_files\taskse.exe
00:00:05	Process Creation	C:\te_files\emulatedFile58511_1.exe **Created** C:\WINDOWS\system32\attrib.exe
00:00:09	Registry Set	C:\WINDOWS\system32\attrib.exe **Set** HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
00:00:09	Registry Create	C:\WINDOWS\system32\attrib.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio
00:00:13	Registry Create	C:\WINDOWS\system32\attrib.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio Compression Manager
00:00:13	Registry Create	C:\WINDOWS\system32\attrib.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\MSACM
00:00:13	Registry Create	C:\WINDOWS\system32\attrib.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\Priority v4.00
00:00:17	Process Termination	C:\te_files\emulatedFile58511_1.exe **Terminated** C:\WINDOWS\system32\attrib.exe
00:00:17	Registry Set	C:\te_files\emulatedFile58511_1.exe **Set** HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
00:00:19	Process Creation	C:\te_files\emulatedFile58511_1.exe **Created** C:\te_files\taskdl.exe
00:00:20	Process Termination	C:\te_files\emulatedFile58511_1.exe **Terminated** C:\te_files\taskdl.exe
00:00:21	Process Creation	C:\te_files\emulatedFile58511_1.exe **Created** C:\WINDOWS\system32\cmd.exe
00:00:21	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\te_files\@WanaDecryptor@.exe
00:00:21	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\te_files\219161325495940.bat

Unexpected Activities By Time (2 out of 7)

11

Elapsed Time	Type	Action
00:00:22	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\~SD1.tmp
00:00:22	File Delete	C:\te_files\emulatedFile58511_1.exe **Deleted** C:\Documents and Settings\admin\Desktop\~SD1.tmp
00:00:22	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\confidential.docx.WNCRYT
00:00:22	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\confidential.docx.WNCRYT
00:00:23	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\confidential.docx
00:00:23	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\$LogFile
00:00:23	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\@Please_Read_Me@.txt
00:00:23	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\@Please_Read_Me@.txt
00:00:23	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\@WanaDecryptor@.exe
00:00:23	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\@WanaDecryptor@.exe
00:00:23	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\~SD2.tmp
00:00:23	File Delete	C:\te_files\emulatedFile58511_1.exe **Deleted** C:\Documents and Settings\admin\Desktop\important DOCs\~SD2.tmp

Unexpected Activities By Time (3 out of 7) 12

Elapsed Time	Type	Action
00:00:24	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\confidential.docx.WNCRYT
00:00:24	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\confidential.docx.WNCRYT
00:00:25	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\confidential.docx
00:00:25	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\roadmap_2021.pptx.WNCRYT
00:00:25	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\roadmap_2021.pptx.WNCRYT
00:00:25	Process Creation	C:\WINDOWS\system32\cmd.exe **Created** C:\WINDOWS\system32\cscript.exe
00:00:25	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\roadmap_2021.pptx
00:00:25	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\@Please_Read_Me@.txt
00:00:25	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\@Please_Read_Me@.txt
00:00:25	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\~SD3.tmp

Unexpected Activities By Time (4 out of 7)

13

Elapsed Time	Type	Action
00:00:25	File Delete	C:\te_files\emulatedFile58511_1.exe **Deleted** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\~SD3.tmp
00:00:25	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\confidential.docx.WNCRYT
00:00:25	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\confidential.docx.WNCRYT
00:00:25	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\confidential.docx
00:00:25	Registry Set	C:\WINDOWS\system32\cscript.exe **Set** HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
00:00:26	Registry Create	C:\WINDOWS\system32\cscript.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio
00:00:28	Registry Create	C:\WINDOWS\system32\cscript.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio Compression Manager
00:00:29	Registry Create	C:\WINDOWS\system32\cscript.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\MSACM
00:00:29	Registry Create	C:\WINDOWS\system32\cscript.exe **Created** HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\Priority v4.00
00:00:29	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\roadmap_2021.pptx.WNCRYT
00:00:29	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\roadmap_2021.pptx.WNCRYT

Unexpected Activities By Time (5 out of 7)

14

Elapsed Time	Type	Action
00:00:31	Registry Create	C:\WINDOWS\system32\cscript.exe **Created** HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings
00:00:31	Registry Create	C:\WINDOWS\system32\cscript.exe **Created** HKCU\Software\Microsoft\Windows Script Host\Settings
00:00:31	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\roadmap_2021.pptx
00:00:32	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\@Please_Read_Me@.txt
00:00:32	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\@Please_Read_Me@.txt
00:00:33	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed.zip.WNCRYT
00:00:33	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed.zip.WNCRYT
00:00:34	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed.zip
00:00:34	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\a glimpse into the future.bmp.WNCRYT
00:00:34	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\a glimpse into the future.bmp.WNCRYT

Unexpected Activities By Time (6 out of 7)

Elapsed Time	Type	Action
00:00:36	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\a glimpse into the future.bmp
00:00:36	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\a glimpse into the future.bmp.WNCRYT
00:00:36	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\a glimpse into the future.bmp.WNCRYT
00:00:36	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\a glimpse into the future.bmp
00:00:36	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\a glimpse.bmp.WNCRYT
00:00:36	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\a glimpse.bmp.WNCRYT
00:00:36	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\Desktop\important DOCs\Classifed\a glimpse.bmp
00:00:36	Registry Create	C:\te_files\emulatedFile58511_1.exe **Created** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:36	Registry Create	C:\te_files\emulatedFile58511_1.exe **Created** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00:00:37	Registry Set	C:\te_files\emulatedFile58511_1.exe **Set** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal
00:00:37	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\My Documents\~SD4.tmp
00:00:37	File Delete	C:\te_files\emulatedFile58511_1.exe **Deleted** C:\Documents and Settings\admin\My Documents\~SD4.tmp
00:00:37	File Create	C:\te_files\emulatedFile58511_1.exe **Created** C:\Documents and Settings\admin\My Documents\roadmap_2021.pptx.WNCRYT
00:00:37	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\My Documents\roadmap_2021.pptx.WNCRYT

Unexpected Activities By Time (7 out of 7)

16

Elapsed Time	Type	Action
00:00:37	Registry Create	C:\WINDOWS\system32\cscript.exe **Created** HKCU\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
00:00:39	File Write	C:\te_files\emulatedFile58511_1.exe **Wrote To** C:\Documents and Settings\admin\My Documents\roadmap_2021.pptx