The Wayback Machine - https://web.archive.org/web/20101010084653/http://www.threatexpert.com:80/report.aspx?md5=87a2583de6f...

ThreatExpert

Visit ThreatExpert web site | Close Report

Submission Summary:

- Submission details:
  - Submission received: 13 May 2009, 10:50:56
  - Processing time: 6 min 48 sec
  - Submitted sample:
    - File MD5: 0x87A2583DE6F6FBB5104E0433E89B1BCF
    - File SHA-1: 0x6048D36DB2207A1CEA877742C9403A816D711C6D
    - Filesize: 24,064 bytes
    - Alias:
      - Mal/UnkPack-Fam [Sophos]
      - TrojanDropper:Win32/Opachki.A [Microsoft]
      - Trojan-Dropper.Win32.Opachki [Ikarus]
- Summary of the findings:

What's been found	Severity Level
Creates a startup registry entry.	🟨🟨

Technical Details:

File System Modifications

- The following files were created in the system:

#	Filename(s)	File Size	File Hash	Alias
1	%Temp%\nsrbgxod.bak	0 bytes	MD5: 0xD41D8CD98F00B204E9800998ECF8427E SHA-1: 0xDA39A3EE5E6B4B0D3255BFEF95601890AFD80709	(not available)
2	%UserProfile%\protect.dll %Programs%\Startup\ChkDisk.dll %System%\autochk.dll [file and pathname of the sample #1]	24,064 bytes	MD5: 0x87A2583DE6F6FBB5104E0433E89B1BCF SHA-1: 0x6048D36DB2207A1CEA877742C9403A816D711C6D	Mal/UnkPack-Fam [Sophos] TrojanDropper:Win32/Opachki.A [Microsoft] Trojan-Dropper.Win32.Opachki [Ikarus]
3	%Programs%\Startup\ChkDisk.lnk	655 bytes	MD5: 0x6F61156F14AEED438770D31391E67EC9 SHA-1: 0x277B806CEC1AEDE9F9B934B7DD655D0BBB542597	(not available)

- Notes:
  - %Temp% is a variable that refers to the temporary folder in the short path form. By default, this is C:\Documents and Settings\[UserName]\Local Settings\Temp\ (Windows NT/2000/XP).
  - %UserProfile% is a variable that specifies the current user's profile folder. By default, this is C:\Documents and Settings\[UserName] (Windows NT/2000/XP).
  - %Programs% is a variable that refers to the file system directory that contains the user's program groups. A typical path is C:\Documents and Settings\[UserName]\Start Menu\Programs.
  - %System% is a variable that refers to the System folder. By default, this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

Memory Modifications

- There was a new process created in the system:

Process Name	Process Filename	Main Module Size

[generic host process]	[generic host process filename]	20,480 bytes

- Notes:
  - [generic host process filename] is a full path filename of [generic host process].
- The following modules were loaded into the address space of other process(es):

Module Name	Module Filename	Address Space Details
[filename of the sample #1]	[file and pathname of the sample #1]	Process name: explorer.exe Process filename: %Windir%\explorer.exe Address space: 0x18D0000 - 0x18D9000
[filename of the sample #1]	[file and pathname of the sample #1]	Process name: dllhost.exe Process filename: %System%\dllhost.exe Address space: 0x2530000 - 0x2539000
[filename of the sample #1]	[file and pathname of the sample #1]	Process name: sdnsmain.exe Process filename: %Windir%\dns\sdnsmain.exe Address space: 0x1620000 - 0x1629000
[filename of the sample #1]	[file and pathname of the sample #1]	Process name: [generic host process] Process filename: [generic host process filename] Address space: 0x390000 - 0x399000
[filename of the sample #1]	[file and pathname of the sample #1]	Process name: IEXPLORE.EXE Process filename: %ProgramFiles%\internet explorer\iexplore.exe Address space: 0x3D0000 - 0x3D9000
[filename of the sample #1]	[file and pathname of the sample #1]	Process name: VMwareUser.exe Process filename: %ProgramFiles%\vmware\vmware tools\vmwareuser.exe Address space: 0x9A0000 - 0x9A9000

- Notes:
  - %Windir% is a variable that refers to the Windows installation folder. By default, this is C:\Windows or C:\Winnt.
  - %ProgramFiles% is a variable that refers to the Program Files folder. A typical path is C:\Program Files.

Registry Modifications

- The newly created Registry Values are:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
    - autochk = "rundll32.exe %System%\autochk.dll,_IWMPEvents@16"

    so that autochk.dll runs every time Windows starts
  - [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
    - autochk = "rundll32.exe %UserProfile%\protect.dll,_IWMPEvents@16"

    so that protect.dll runs every time Windows starts

Other details

- Analysis of the file resources indicate the following possible country of origin:

🇷🇺	Russian Federation

- There was application-defined hook procedure installed into the hook chain (e.g. to monitor keystrokes). The installed hook is handled by the following module:
  - [file and pathname of the sample #1]

The Information is provided on an "as is" basis. ThreatExpert disclaims all warranties, whether express or implied, to the maximum extent permitted by law, including the implied warranties that the Information is merchantable, of satisfactory quality, accurate, fit for a particular purpose or need, or non-infringing, unless such implied warranties are legally incapable of exclusion. Further, ThreatExpert does not warrant or make any representations regarding the use or the results of the use of the Information in terms of their correctness, accuracy, reliability, or otherwise.