Many Vietnamese networks are attacked by Tro_small

According to Misoft Company, in the past 1 week, many networks in Vietnam have been attacked by the worm TROJ_SMALL.DK. This worm after infecting immediately locks access to the option folder, registry, taskmanger, hiding all folders on the system and generating c & a

According to Misoft Company, in the past 1 week, many networks in Vietnam have been attacked by the worm TROJ_SMALL.DK. This worm after infecting immediately blocks access to the option folder, registry, taskmanger, hiding all folders on the system and generating malicious files with the same name and icon as hidden folders . This has helped this worm to spread very strongly because it has succeeded in deceiving users. It is especially dangerous for data sharing servers, ftp.

To remove this worm, we need to do 3 steps :

1. Remove malicious files: To remove malicious files, users can use Trend Micro's antivirus products such as OfficeScan, Pccillin 2007 with the latest updated templates from Trend Lab, Then proceed to scan the entire machine to remove files containing malicious code.

2. Restore current status of directories: Use the attrib -s -h [path] / s / d command to run in the command line to

remove the hidden properties of the directories.

3. Restore registry: To restore the status of TaskManager, user FolderOption can use the following code, save as **file.reg** and then execute this file to restore the registry state.

****

Windows Registry

[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerAdvancedFolderHidden]
"Text" = "@ shell32.dll, -30499"
"Type" = "group"
"Bitmap" = hex (2): 25,00,53,00,79.00,73,00,74.00,65,00,6d, 00,52,00,6f, 00,6f, 00,74 ,
00,25,00,5c, 00,73,00,79.00,73.00,74.00,65,00,6d, 00,33.00,32,00,5c, 00,53.00,
48.00,45,00,4c, 00,4c, 00,33.00,32,00,2e, 00,64.00,6c, 00,6c, 00,2c, 00,34,00,00,
00
"HelpID" = "shell.hlp # 51131"

[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerAdvancedFolderHiddenNOHIDI
"RegPath" = "SoftwareMicrosoftWindowsCurrentVersionExplorerAdvanced"
"Text" = "@ shell32.dll, -30501"
"Type" = "radio"
"CheckedValue" = dword: 00000002
"ValueName" = "Hidden"
"DefaultValue" = dword: 00000002
"HKeyRoot" = dword: 80000001
"HelpID" = "shell.hlp # 51104"

[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionExplorerAdvancedFolderHiddenSHOWA
"RegPath" = "SoftwareMicrosoftWindowsCurrentVersionExplorerAdvanced"
"Text" = "@ shell32.dll, -30500"
"Type" = "radio"
"CheckedValue" = dword: 00000001
"ValueName" = "Hidden"
"DefaultValue" = dword: 00000002
"HKeyRoot" = dword: 80000001
"HelpID" = "shell.hlp # 51105"

****

You finished reading the article "**Many Vietnamese networks are attacked by Tro_small**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com