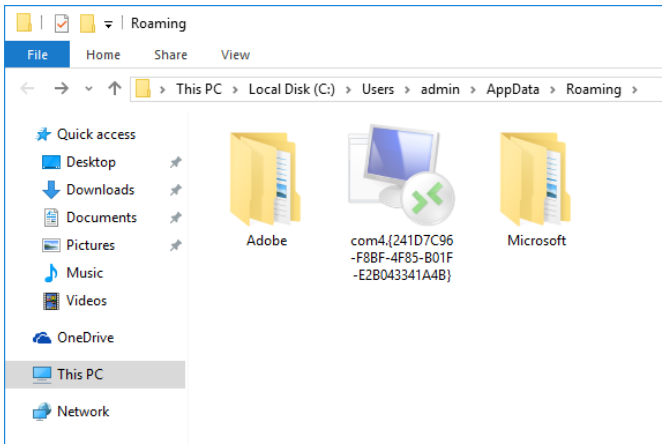
Dynamer malware sign of evolving threat landscape

5 May 2016, by Nancy Owano



Credit: mcafee

Security watchers are talking about a McAfee Labs blog from its research architect Craig Schmugar. He recently reported on a type of malware which takes advantage of Windows 'GodMode.'

Larry Loeb in *Security Intelligence* addressed the malware Dynamer and how it uses Windows GodMode, present since the days of Vista.

"This undocumented God Mode allows a user to create a special kind of folder that will act as a shortcut to Windows settings. The shortcut can also link to other special folders such as Control Panel, My Computer or Printers. These do not open like normal folders, but rather redirect the user to a fresh program."

Briefly, GodMode refers to a short-cut to access various control settings in Windows Vista and later operating systems.

"GodMode doesn't add functionality," *PCWorld* had written back in 2011,"but it helps administrators work more efficiently by collecting all these tweaks and controls in one place."

Schmugar's blog posting said, "Microsoft Windows has hidden an Easter Egg since Windows Vista." Admins could find this convenient but Dynamer, as the variant is called, fell into mischievous hands with more than handy functionality in mind.

With Dynamer, "the malware is installed into one of these folders inside of %AppData%. A registry run key value is created to persist across reboots. (The executable name is dynamic.)

HKEY_CURRENT_USERSOFTWAREMicrosoftWindowsCurrentVersionRun
lsm = C:UsersadminAppDataRoamingcom4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}lsm.exe

This key allows the malware to execute normally, but when the folder "com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}" is opened, it redirects to the RemoteApp and Desktop Connections control panel item."

Good luck if you try to delete with console commands or Explorer. Nonetheless, McAfee's Schmugar said there is a way to win.

"First, the malware must be terminated (via Task Manager or other standard tools). Next, run this specially crafted command from the command prompt (cmd.exe):
rd "\.%appdata%com4.{241D7C96-F8BF-4F85-B01F-E2B043341A4B}" /S /Q

McAfee antimalware products are not fooled by these tricks; no special action is required to deal with this threat."

In the bigger picture, Loeb commented that "Dynamer shows how malware will take advantage of any quirks in an OS to gain a foothold."

Ryan Whitwam in *ExtremeTech* remarked that "it will be interesting to see if Microsoft makes changes to prevent these sort of super-directories

from being created so easily."

SecurityWeek said "Dynamer proves that as the threat landscape evolves, new malware variants are attempting to leverage various operating system functions to perform malicious operations. Recently, attackers were observed abusing PowerShell and Google Docs to deliver the Laziok Trojan, while the PowerWare ransomware was seen earlier this year abusing PowerShell and Office macros to infect computers."

More information:
blogs.mcafee.com/mcafee-labs/m … of-windows-god-mode/

APA citation: Dynamer malware sign of evolving threat landscape (2016, May 5) retrieved 28 May 2022 from https://techxplore.com/news/2016-05-dynamer-malware-evolving-threat-landscape.html