Ù^ÛŒÚ˜Ú¯ÛŒâ€ŒÙ‡Ø§ÛŒ Ø§Ù…Ù†ÛŒØªÛŒ Ø¬Ø¯ÛŒØ¯ Ù^ÛŒØ³ØªØ§

Ø¨Ø§ Ù‡Ù…Ú©Ø§Ø±ÛŒ Roger A.Grimes
06 Ø®Ø±Ø¯Ø§Ø¯ 1387 Ø³Ø§Ø¹Øª 18:01

Ø§Ø-ØªÙ…Ø§Ù„Ø§ UAC ÛŒØ§ User Account Control Ø¬Ø¯ÛŒØ¯ØªØ±ÛŒÙ† Ù^ÛŒÚ˜Ú¯ÛŒ Ø§Ù…Ù†ÛŒØªÛŒ Ø§ÛŒÙ†
Ø´Ù^Ù†Ø¯. Ù…ØªØ§Ø³Ù•Ø§Ù†Ù‡ Ø¯Ù„Ø§ÛŒÙ„ÛŒ Ù^Ø¬Ù^Ø¯ Ø¯Ø§Ø±Ø¯ Ú©Ù‡ Ø¨Ø³ÛŒØ§Ø±Ø§ Ú©Ø§Ø±Ø¨Ø±Ø

UAC Ù…Ø§Ù†Ø¹ Ø¨Ø±Ù^Ø² Ø§ÛŒÙ† Ù…Ø´Ú©Ù„ Ù…ÛŒâ€ŒØ´Ù^Ø¯. Ø§ÛŒÙ† Ø¬Ø±Ù†Ø§Ù‡ Ø§Øºù„Ø¨ Ø¬Ø±Ù†Ø§Ù.
Ú©Ø§Ø±Ø¨Ø± ÛŒÚ© Administrator Ø§Ø³Øª.

Ø¬Ù‡ Ø¹Ù†Ù^Ø§Ù† Ù…Ø«Ø§Ù„ØŒ Ø§Ú¯Ø± Ø´Ù…Ø§ Ø¹Ù†Ù^Ø§Ù† Administrator Ù…Øªµù„ Ø´Ø¯Ù‡â€ŒØ§ÛŒØ¯Ø
Ø§Ø¬Ø±Ø§Ø§ÛŒÛŒ Ø´Ù…Ø§ Ù…ÛŒâ€Œâ€•Ø¬Ø§ÛŒØ³Øª Ú©Ù‡ Ø±Ù…Ø² Ù^Ø±Ù^Ø¯ Ø®Ù^Ø¯ Ø±Ø§ Ù…Ø¬Ø¯Ø§ Ù^Ø§

Ø¯Ø± ÛŒÚ© Ù†Ù^Øª Ù…Ø±ØªØ¨Ø·ØŒ Ø§Ù…ØªÛŒØ§Ø² Ø¬Ø¯ÛŒØ§Ø² Ø¬Ø¯Ø± Ø-Ø§Ù„ Ø§Ø¶Ø§Ù•Ù‡ Ø´Ø¯Ù† Ù…ÛŒâ€
Ø®Ù^Ø´Ø§ÛŒÙ†Ø¯ Ù…ÛŒâ€ŒØ¨Ø§Ø´Ø¯.

Ù†Ø±Ù…â€ŒØ§Ù•Ø²Ø§Ø± Antispyware Ø´Ø±Ú©Øª Ù…Ø§ÛŒÚ©Ø±Ù^Ø³Ø§Ù•Øª Ø¯Ø± Ù^ÛŒÙ†Ø¯Ù^Ø² Ù^ÛŒØ³ØªØ§Ø§ Ø§Ø
Ù…Ø-Ø§Ù•Ø¸Øª Ø¯Ø± Ù…Ù‚Ø§Ù„Ù‡ Ø§Ù•Ù‡ maleware Ø§ÛŒØ¬Ø§Ø¯ Ù…ÛŒâ€ŒÚ©Ù†Ø¯. Ø¨Ø±Ù†Ø§Ù…Ù‡â€ŒÙ
Ø§Ù†Ù^Ø§Ø¹ Ø±Ø¬ÛŒØ³Øªâ€Ø±Ù^Ø§Ù•Ø¬Ø§Ù• Ù‡Ø¯Ø§Ø§ÛŒØª Ù…Ø¬Ø¯Ø¯Ù‡ Ù…ÛŒâ€ŒØ´Ù
Ø¨Ù^Øª Ú©Ø±Ø¯Ù† Ø±Ù…Ø²Ú¯Ø°Ø§Ø±Ù‡ Ù†Ù…Ù^Ø¯ Ù^ Ú©Ù„ÛŒØ¯ Ø±Ù…Ø² Ú¯Ø°Ø§Ø±Ù‡ Ø¨Ø§Ø§Ù…Ù†ÛŒØª Øªâ
Ø¯ÛŒØ³Ú©â€ŒÙ‡Ø§ÛŒØ¨Ù^Øª NTFS-aware Ø§Ø³Øªâ•Ø§Ø¯Ù‡ Ù…ÛŒâ€ŒÚ©Ù†Ù†Ø¯ Ø¯ÛŒÚ¯Ø± Ø¬Ø§ÛŒÛŒ Ø¨Ø±Ø

Ø±Ù^Ø´â€ŒÙ‡Ø§ÛŒ Ù¾ÛŒØ´Ø±Ø•Øªâ€ŒØ§ÛŒ Ø¨Ø±Ø§ÛŒ Ù^ÛŒØ±Ø§Ø³Øªâ€ŒØ¬Ø¯Ø¯ Ù^Ø¬Ù^Ø¯ Ø¯Ø§Ø§
Ù‡Ù^ÛŒØª Øºâ€ŒØ± Ø±Ù…Ø² Ù^Ø±Ù^Ø¯ Ù†ÛŒØ² Ø®Ù^Ø§Ù‡Ù†Ø¯ Ø¯Ø§Ø´Ø¯. Ø§Ø² Ø¬Ù…Ù„Ù‡ Ø§Ù†Ù†Ù‡ Ù…ÛŒâ€ŒÚ©Ù†Ù†Ø¯ Ú©Ù†Ù
System Ø±Ø§Ù…Ù‡â€ŒØªÙ^Ø§Ù† Ø¯Ø± Ø§Ù†Ù^Ø§Ø¹ Ú©Ø§Ø±Øªâ€ŒÙ‡Ø§ÛŒ Ù‡Ù^Ø´Ù…Ø¯ Ø°Ø®Ù^Ø±Ù‡ Ú©Ø±

Ø§ÛŒÙ†Ø¨Ø§Ø± Ø®Ø¯Ù…Ø§Ù^Ø¯Ø¹ØŒ Ú©Ù‡ Ø§Øºù„Ø¨ ÛŒÚ© Ù†Ù,Ø·Ù‡ Ù^Ø±Ù^Ø¯ Ø¨Ø±Ø§ÛŒ Ø§Ù†Ù^Ø
Ø¯Ø± Local Service Ù^Ù…Øªù^Ù† Network Service (Ø¨Ù‡ Ø¬Ø§Ø§ÛŒ Local System) Ø§Ø¬Ø±Ø§Ø§ Ù…ÛŒâ€ŒØ´Ù^Ù†Ø¯ØŒ Ø¨
SID Ø®Ù^Ø¯ Ø±Ø§ Ú¯Ø±Ø•Øªù‡â€ŒØ§Ù†Ø¯ØŒ Ú©Ù‡ Ø§Ù†Ù^Ø§Ø¹ Ù…Ø¬Ù^Ø²Ø§Ø§ Ù^ Ø²Ù…ÛŒ

Ù…Ø§ÛŒÚ©Ø±Ù^Ø³Ø§Ù•Øª ÛŒÚ© Ù^ÛŒÚ˜Ú¯ÛŒ Ù…Ø¬Ù^Ø²ÛŒ Ø¬Ø¯Ù^Ø²ÛŒ access control entry) NTFS ACE) Ø±Ø§Ø¨Ù
ØµØ§Ø-Ø¨Ø§Ù† Ø¢Ù†Ù‡Ø§ Ø§Ø² Ù¾ÛŒØ´ ØªØ¹ÛŒÛŒÙ† Ú©Ù†Ø¯. Ø§Ø®ÛŒØ±Ø§Ù…Ø¬Ù^Ø²Ù‡Ø§Ø§ÛŒ NTFS Ø±Ø§Ø Ù…
Owner ÛŒÚ© Ø§ØµÙ„ Ø§Ù…Ù†Ù†Ø¯ÛŒÚ¯Ø± Ø¯Ø±Ø§Ø§Ù•Øª Ù†Ù…Ø§Ù†Ø¯.

Ú¯Ø±Ù^Ù‡ Power User Ú©Ù… Ø§Ø²Ø´Ø¯ Ù…ÛŒâ€ŒØ´Ù^Ø¯ Ù^ ÛŒØ§ Ø¨Ù‡ Ú©Ù„ Ø-Ø°Ù• Ù…ÛŒâ€ŒØ´Ù^Ø¯. Ù•Ø§ÛŒØ
Ø¨Ú¯ÛŒØ±Ø¯ Ù^ ÛŒØ§ Ù…ÛŒÚ©Ù^Ø´Ø¯ Ø®Ø¯Ù…Ø§Ø³Ø¬ Ø´Ù†ÛŒØ§Ø§ÛŒ Ø¨Ù‡ Ø±Ø§Ù‡ Ø¨ÛŒØ§Ù†Ø¯Ø§Ø² Ø§

Ø¨Ø§ Ù†Øµø¨ OS Ø¬Ø¯ÛŒØ¯ Ù•Ø§ÛŒØ±Ù^Ø§Ù„ Ù^ÛŒÙ†Ø¯Ù^Ø² Ù•Ø¹Ø§Ù„ Ù…ÛŒâ€ŒØ´Ù^Ø¯ Ø¨Ù^Ù† Ù‡Ù‡
Ø§Ù†Ù^Ø§Ø¹ malware Ø³Ø±Ú¯Ø±Ø¯Ø§Ù† Ø¨Ù‡ Ù^ÛŒÙ†Ø¯Ù^Ø² Ø±Ø§Ù‡ Ù¾ÛŒØ¯Ø§ Ú©Ù†Ù†Ø¯.

Ø¨Ø±Ø§ÛŒ Ù¾ÛŒÚ©Ø±Ø¨Ù†Ø¯Ù‡ Ø¬Ø§Ù^ Ø§Ø¯Ø¹Ø§Ù… Ø¯Ù,ÛŒÙ,â€ŒØªØ± IPSec Ù^ Ù•Ø§ÛŒØ±Ù^Ø§Ù„Ù„ Ú©Ù
Ø§Ø² Ø§ÛŒÙ† Ú©Ù†Ø³Ù^Ù„ Ø¢Ø³Ø§Ù†Øªâ€Ø± Ø§Ø³Øª Ù^ Øªâ€Ø§Ø§ÛŒ Ú©Ù…Øªâ€ŒØ± Ø¬Ù‡Ø§ Ù¾ÛŒÚ©Ø±Ø¨Ù†Ø¯Ù‡ Ø±Ø±

Ù^ÛŒØ³Øªâ€Ø§Ø§ Ø¨Ø± MDÛµÙ^ SHA-Û±hashing Ø§Øªâ€Ø§Ø¯. Ø§Ø² Ø¢Ù†Ø¬Ø§Ø§ Ú©Ù‡ Ø§Ù„Ù^Ø±Ù^Ø±Ø§Ù…Ù‡â€
Û²ÛµÛ¶Ø§Ø³Øªâ€Ø§Ù•Ø§Ø¯Ù‡ Ù…ÛŒâ€ŒÚ©Ù†Ù†Ø¯.

Ø¯Ø± Ø²Ù…ÛŒÙ†Ù‡ patchØŒ Ù^ÛŒØ³Øªâ€Ø§Ø§ Ø§Ø² Ù^ÛŒÚ˜Ú¯ÛŒâ€ŒÙ‡Ø§ÛŒ patch-in-place Ù¾Ø´Øªâ€ŒØ¬Ø§Ù†Ù‡ Ù…
Ø¨Ø±Ù†Ø§Ù…Ù‡ Ù•Ø¹Ù„Ø§Ù‡ Ø±Ø§Ø§ Ø¯Ø± reboot Ø-Ù•Ø¸ Ù…ÛŒâ€ŒÚ©Ù†Ø¯. Ø§Ù„Ø¢Ø§Ù‡Ø§Ø§ Ø¨Ù‡Øªâ€Ø± Ø¬Ù‡Ø§Ø± Ø¬Ù^Ø¯ Ø§Ú¯Ø±

Ø¨Ø§ ÛŒÚ© Ø¬Ø±Ù†Ø§Ù‡ Ø¬Ø¯Ù^Ø§Ù‡ Network Center Ø§Ù…Ú©Ø§Ù† Ø¯Ø¯Ù†Ø¯Ù† Ù¾ÛŒÚ©Ø±Ø¨Ù†Ø¯Ù‡ Ù^ Ù
Protection Ø¯Ø± Ù^Ø§Ù„Ø¹Ø¹ ÛŒÚ©Ú©Ù„Ø§ÛŒÙ†Ø¹Ø§ Ú©Ù†Ø¹Ø±Ù„ Ø¯Ø³Ø±Ø±Ø³Ø¹ÛŒ Ø´Ø¬Ú©Ù‡ Ø§Ø§Ø³Øª. Ø²Ù…Ø§Ù†Ù‡ Ú©
Ø§Ø®ÛŒØ± NAP Ø´Ø±Ú©Øª Ù…Ø§ÛŒÚ©Ø±Ù^Ø³Ø§Ù•Øª Ú†Ù†Ø¯Ø§Ù† Ø¯Ù^Ø³Øªâ€Ø¯Ø§Ø§ Ú©Ø§Ø±Ø¨Ø±Ù^Ù‡ Ø

Ù^ÛŒØ³Øªâ€Ø§Ø§ Ù‡Ù…Ú†Ù†Ø¯ Ø´Ø§Ù„Ù„ Ø§Ú©Ø³Ù¾Ù„Ù^Ø±Ø±Ù· Ø¨Ø³Ø±Ù^Ø¯Ø¹ Ø§Ù•Ø¬Ø§Ù• Ø¬Ø¯Ø´Ø¯Ù‡ Ù•Ø¹Ø§Ù•Ù‡
group policy object Ù^Ø¬Ù^Ø¯ Ø¯Ø§Ø±Ø¯ Ú©Ù‡ Ø§Ø² Ù„Ø-Ø§Ø¸ Ø§Ù†Ù†Ø¯Øªâ€Ø¯ Ø¨Ù‡ Ú©Ø§Ø± Ù…Ø¬Ø¯Ø¯Ø¢Ø¬Ù†Ø
Ú©Ù†Ù….

Ù…Ø³Ø±Ø¬Ù…: Ø²Ù‡Ø±Ù‡ Ú†Ú©Ù†ÛŒ

Ø¬Ù†Ù‘Ø¨ÛŒâ€ŒÙ‡Ø§