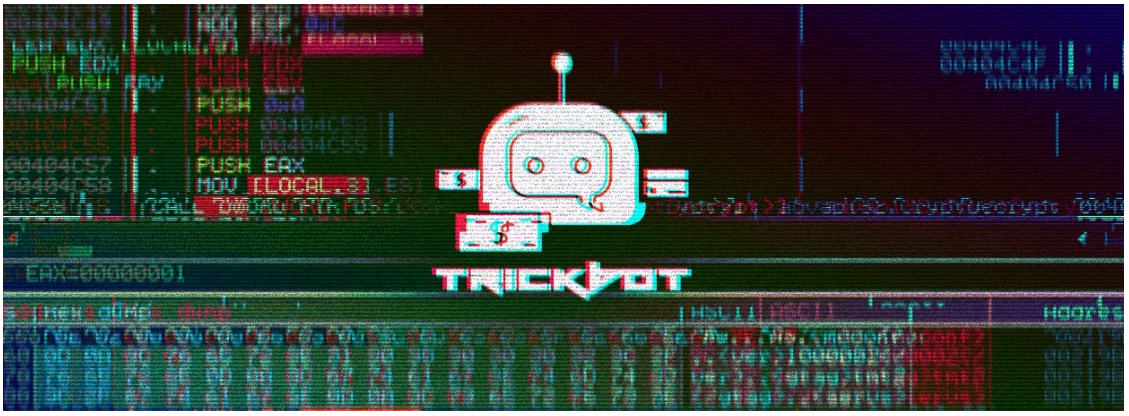
TrickBot Now Uses a Windows 10 UAC Bypass to Evade Detection

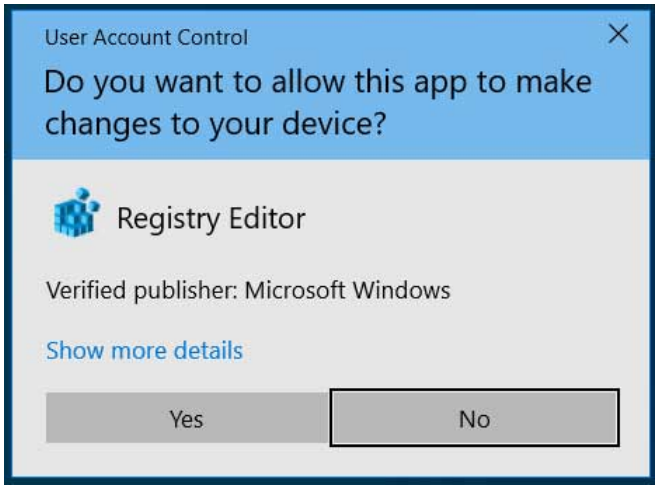
By Lawrence Abrams

Published: 2020-01-16 · Archived: 2026-04-05 19:00:02 UTC



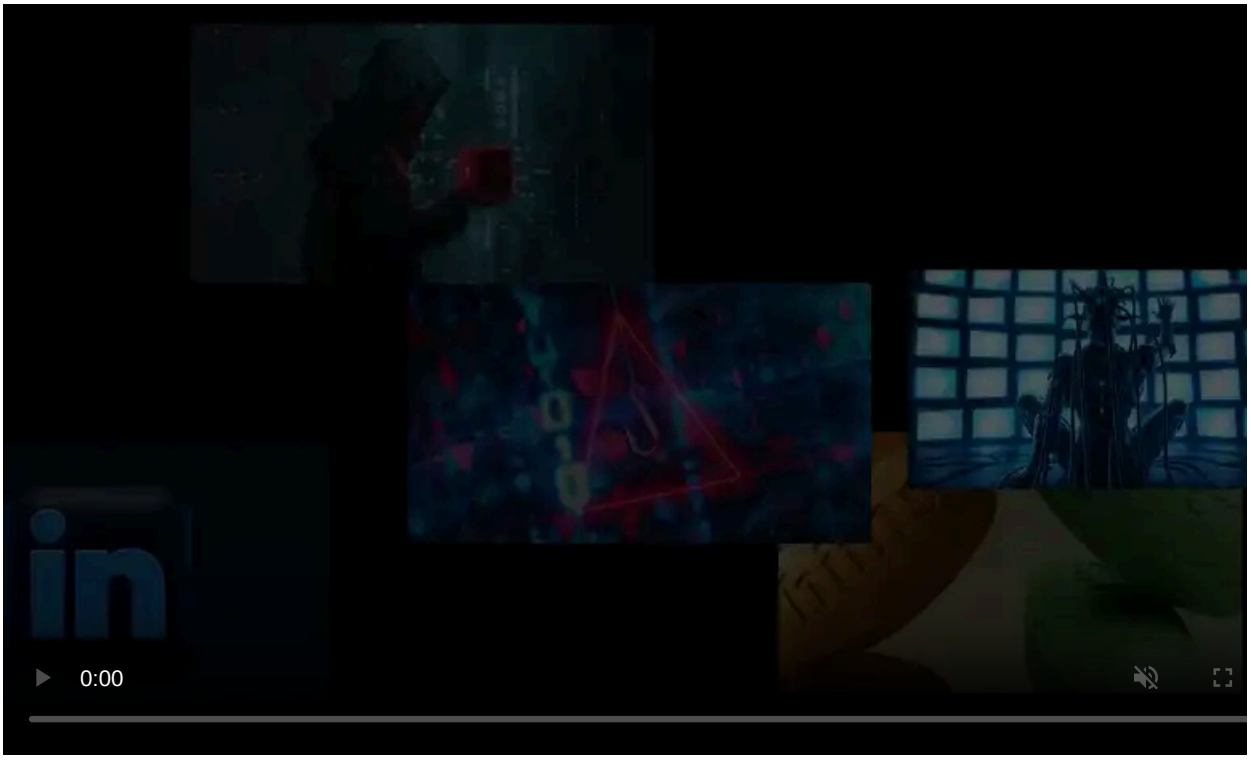
The TrickBot Trojan has received an update that adds a UAC bypass targeting the Windows 10 operating system so that it infects users without displaying any visible prompts.

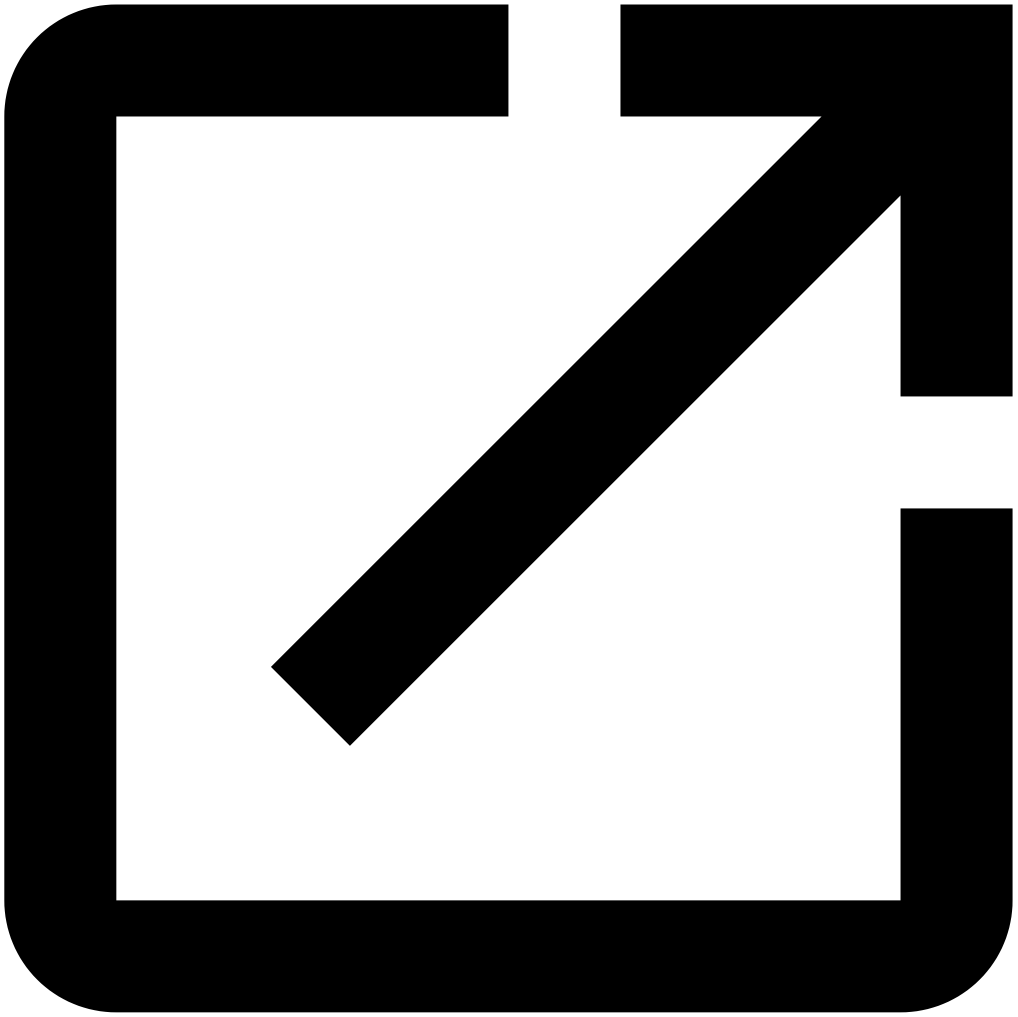
A UAC bypass allows programs to be launched without displaying a User Account Control prompt that asks users to allow a program to run with administrative privileges.



Example of UAC prompt

In a new TrickBot sample, Head of SentinelLabs Vitali Kremez discovered that the trojan is now using the Windows 10 Fodhelper bypass.


0:00



Using Windows 10 UAC bypass

When executed, TrickBot will check if the operating system is Windows 7 or Windows 10.

If it is Windows 7, TrickBot will utilize the CMSTPLUA UAC bypass and if Windows 10, will now use the Fodhelper UAC Bypass.

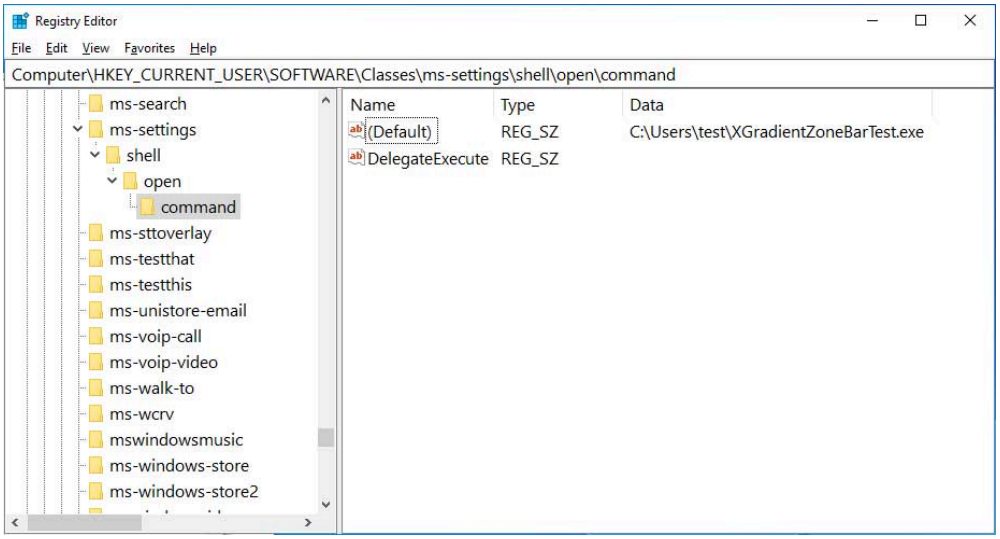
The Fodhelper bypass was discovered in 2017 and uses the legitimate Microsoft C:\Windows\system32\fodhelper.exe executable to execute other programs with administrative privileges.

"Fodhelper.exe is a trusted binary on Windows 10 that TrickBot uses to execute the malware stage bypassing UAC via the registry method," Kremez told BleepingComputer in a conversation.

When properly configured, when executed Fodhelper will also launch any command stored in the default value of the HKCU\Software\Classes\ms-settings\shell\open\command key.

As Fodhelper is a trusted Windows executable, it allows auto-elevation without displaying a UAC prompt. Any programs that it executes will be executed without showing a UAC prompt as well.

TrickBot utilizes this bypass to launch itself without a warning to the user and thus evading detection by the user.



Command executed by the Fodhelper UAC bypass

As more users move to Windows 10 and as Windows Defender matures, more malware has begun to target the operating system and its security features.

In September 2019 we reported how the GootKit banking Trojan also added the Fodhelper bypass in 2019 to execute a command that whitelists the malware executable's path in Windows Defender.

In July 2019, TrickBot also targeted Windows Defender by trying to disable various scan options. With the inclusion of Fodhelper, we continue to see the malware developers attempt to reduce the security features found in Windows 10.

Source: https://www.bleepingcomputer.com/news/security/trickbot-now-uses-a-windows-10-uac-bypass-to-evade-detection/