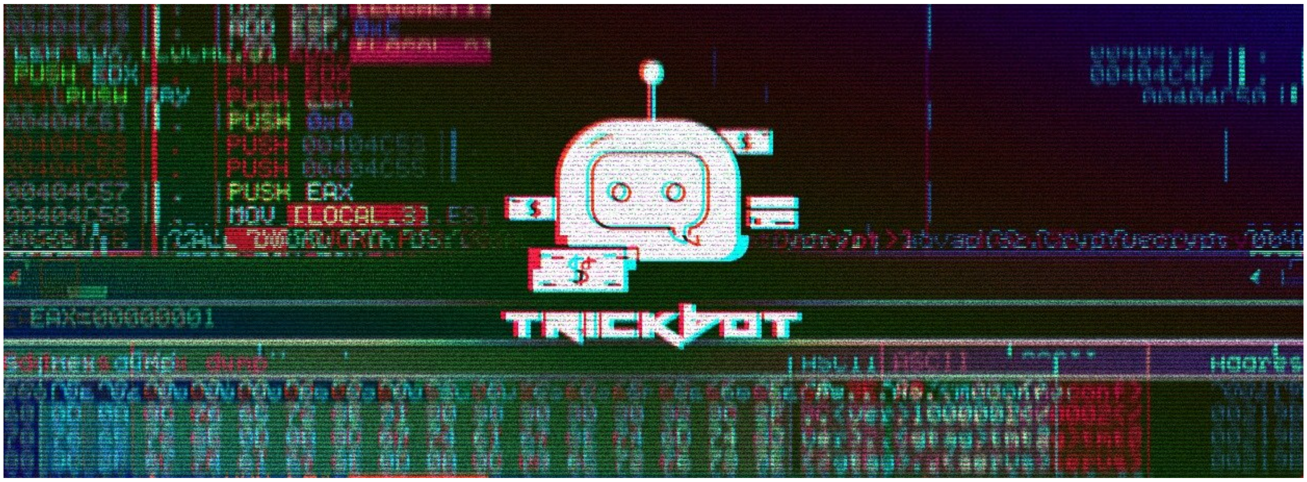
TrickBot Now Uses a Windows 10 UAC Bypass to Evade Detection

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

Lawrence Abrams

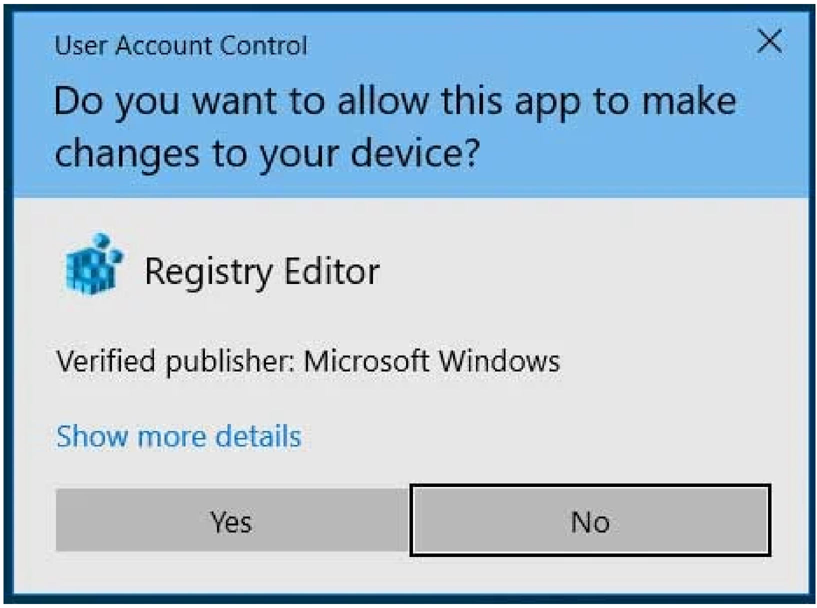
By
Lawrence Abrams

- January 16, 2020
- 04:00 PM
- 7



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.



User Account Control

Do you want to allow this app to make changes to your device?

Registry Editor

Verified publisher: Microsoft Windows

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.

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.

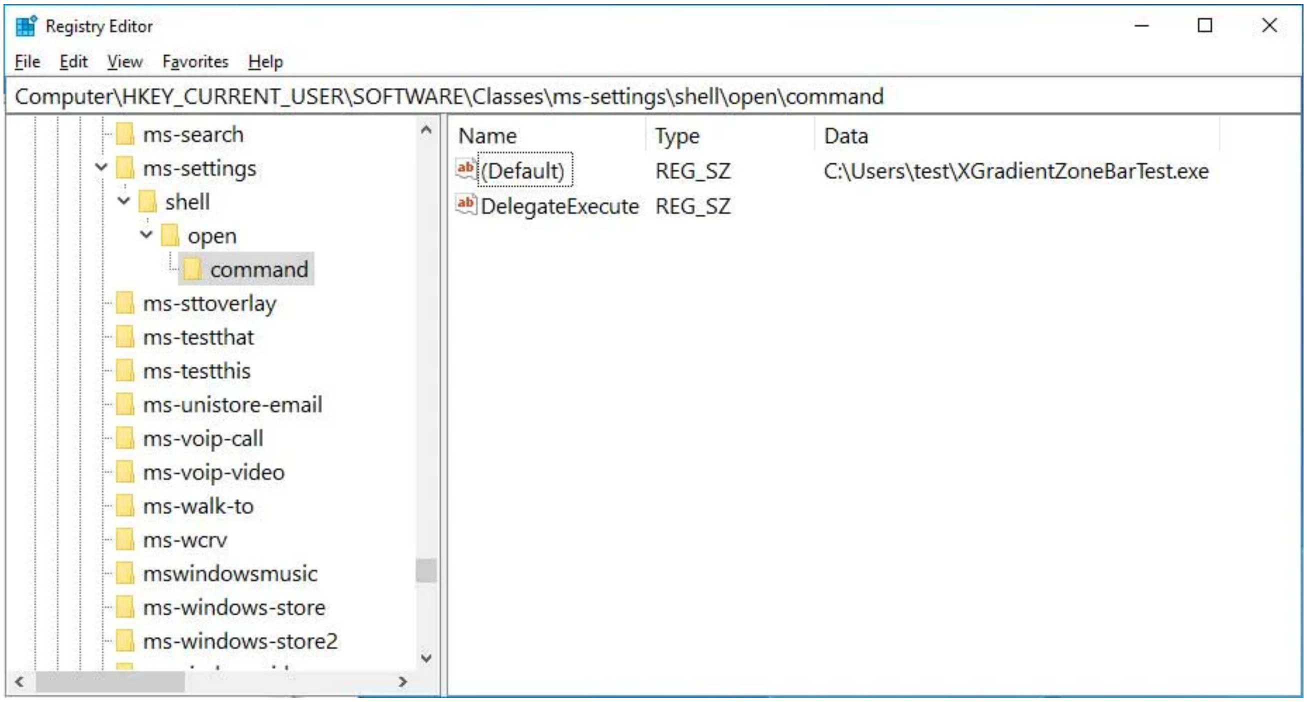
The Fodhelper bypass was discovered in 2017 and uses the legitimate Microsoft C:\Windows\system32\fodhelper.exe executable to execute other programs with administrative privileges.

"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.



Computer\HKEY_CURRENT_USER\SOFTWARE\Classes\ms-settings\shell\open\command

Name	Type	Data
(Default)	REG_SZ	C:\Users\test\XGradientZoneBarTest.exe
DelegateExecute	REG_SZ	

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.

Related Articles:

Emergency Windows 10 updates fix Microsoft Store app issues

Microsoft emergency updates fix Windows AD authentication issues

Windows admins frustrated by Quick Assist moving to Microsoft Store

Microsoft: Windows 10 20H2 has reached end of service

New stealthy Nerbian RAT malware spotted in ongoing attacks

- Fodhelper
- TrickBot
- Trojan
- UAC Bypass
- Windows 10

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

-
  berite100 - 2 years ago
  -
  -

  any remediation?

-
  Lawrence Abrams - 2 years ago
  -
  -

  No, unfortunately not. Microsoft does not give UAC bypasses much priority.

-
  DavidChipman - 2 years ago
  -
  -

  Here's hoping they might now? Or is that expecting too much?

-
  RocketPak - 2 years ago
  -
  -

  Best thing you can do is crank UAC to up to the max setting. Then it will still pop up a UAC prompt even when windows trusted executable need admin privileges.

-
  gabry89 - 2 years ago
  -
  -

  You can set UAC to "Always Notify" and you should be safe from this bypass attack. EDIT: i'm too late :)

- ken_smon - 2 years ago

  The world: Windows in insecure
  Microsoft: OK, here's UAC
  Malware writer: Lets use fodhelper.exe to bypass it
  Microsoft: ...

- Quadroodlesublimated - 2 years ago

  How do you set UAC to "Always Notify" ? Explain, step by step!

  also: MSFT itself does not reliably sign every piece of software it publishes. Why? If they can't even follow their own rules, then what's the point of UAC ? Am I getting this right? Is there something I should know?

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: