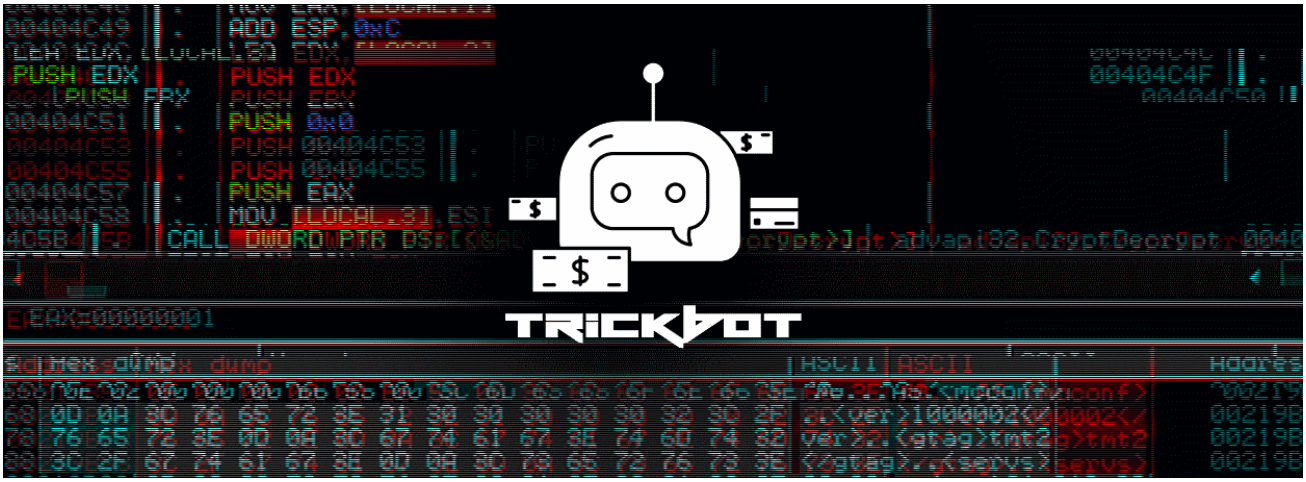
TrickBot Uses a New Windows 10 UAC Bypass to Launch Quietly

bleepingcomputer.com/news/security/trickbot-uses-a-new-windows-10-uac-bypass-to-launch-quietly/

Lawrence Abrams

By
Lawrence Abrams

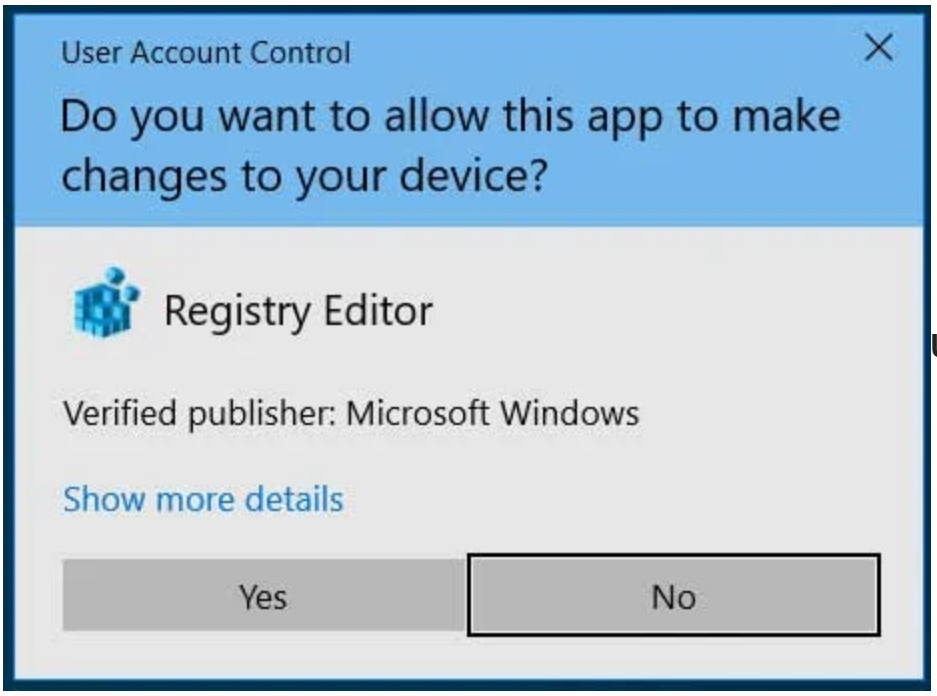
- January 30, 2020
- 03:54 PM
- 1



The TrickBot Trojan has switched to a new Windows 10 UAC bypass to execute itself with elevated privileges without showing a User Account Control prompt.

Windows uses a security mechanism called User Account Control (UAC) that will display a prompt every time a program is run with administrative privileges.

When these prompts are shown, they will ask logged in user if they wish to allow the program to makes changes, and if the program is suspicious or unrecognized, allows the user to prevent the program from running.



UAC Prompt

These UAC bypasses are found in legitimate Microsoft Windows programs that are used by the operating system to launch other programs. As they are not considered a high priority to Microsoft, it could be a while before discovered bypasses are fixed, if at all.

To avoid being detected, malware developers sometimes use a UAC bypass so that the malware runs with administrative privileges, but without displaying a UAC prompt and alerting the user.

Trickbot switches to the Wsreset.exe UAC bypass

Just recently we reported that TrickBot had begun using a Windows 10 UAC bypass that utilizes the legitimate Microsoft fodhelper.exe program.

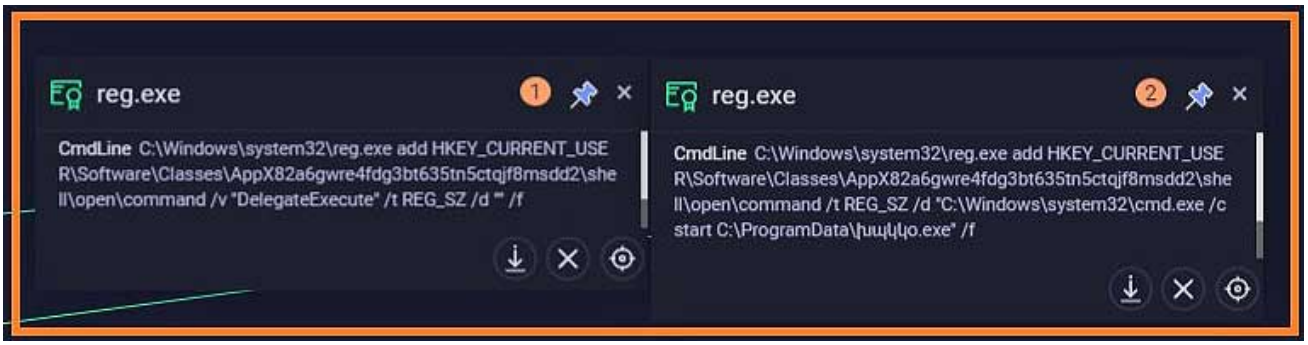
This week, ReaQta discovered that TrickBot has now switched to a different UAC bypass that utilizes the Wsreset.exe program.

Wsreset.exe is a legitimate Windows program used to reset the Windows Store cache.

When executed, Wsreset.exe will read a command from the default value of the HKCU\Software\Classes\AppX82a6gwre4fdg3bt635tn5ctqjf8msdd2\Shell\open\command key and execute it.

When executing the command it will not display a UAC prompt and users will have no idea that a program has been executed.

TrickBot is now exploiting this UAC bypass to launch itself with elevated privileges, but without the logged in Windows user being notified by a UAC prompt.



Registry commands added by TrickBot

Source: ReaQta

This allows the trojan to run silently in the background while it harvests saved login credentials, SSH keys, browser history, cookies, and more.

TrickBot is particularly dangerous as it can propagate throughout the network and if it gains admin access to a domain controller, it can steal the Active Directory database to gain further credentials on the network.

Eventually, TrickBot is known to open a reverse shell back to the Ryuk Ransomware actors so that they can encrypt the entire compromised network.

Update 1/30/20: MorphiSec published analysis of TrickBot using the Wsreset.exe UAC bypass and it's great read for those who want a more technical nosedive.

H/T @gN3mes1s

Related Articles:

Ukraine warns of “chemical attack” phishing pushing stealer malware

Pixiv, DeviantArt artists hit by NFT job offers pushing malware

Google exposes tactics of a Conti ransomware access broker

New powerful Prynt Stealer malware sells for just $100 per month

New ZingoStealer infostealer drops more malware, cryptominers

- Malware
- Password Stealing Trojan
- TrickBot
- 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

RocketPak - 2 years ago

-
-

Set UAC to always notify even when changing windows settings and you'll still get a UAC pop up if this happens.

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: