# Abuse Elevation Control Mechanism: Bypass User Account Control, Sub-technique T1548.002 - Enterprise

Archived: 2026-04-05 17:37:00 UTC

S0584 AppleJeus

AppleJeus has presented the user with a UAC prompt to elevate privileges while installing.[9]

G0016 APT29

APT29 has bypassed UAC.[10]

G0067 APT37

APT37 has a function in the initial dropper to bypass Windows UAC in order to execute the next payload with higher privileges.[11]

G0082 APT38

APT38 has used the legitimate application `ieinstal.exe` to bypass UAC.[12]

S0129 AutoIt backdoor

AutoIt backdoor attempts to escalate privileges by bypassing User Access Control.[13]

S0640 Avaddon

Avaddon bypasses UAC using the CMSTPLUA COM interface.[14]

S0606 Bad Rabbit

Bad Rabbit has attempted to bypass UAC and gain elevated administrative privileges.[15]

S1081 BADHATCH

BADHATCH can utilize the CMSTPLUA COM interface and the SilentCleanup task to bypass UAC.[16]

S0570 BitPaymer

BitPaymer can suppress UAC prompts by setting the `HKCU\Software\Classes\ms-settings\shell\open\command` registry key on Windows 10 or `HKCU\Software\Classes\mscfile\shell\open\command` on Windows 7 and launching the `eventvwr.msc` process, which launches BitPaymer with elevated privileges.[17]

S1068 BlackCat

BlackCat can bypass UAC to escalate privileges.[18]

S0089 BlackEnergy

BlackEnergy attempts to bypass default User Access Control (UAC) settings by exploiting a backward-compatibility setting found in Windows 7 and later.[19]

G0060 BRONZE BUTLER

BRONZE BUTLER has used a Windows 10 specific tool and xxmm to bypass UAC for privilege escalation.[20][21]

S1039 Bumblebee

Bumblebee has the ability to bypass UAC to deploy post exploitation tools with elevated privileges.[22]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP can make use of the Windows `SilentCleanup` scheduled task to execute its payload with elevated privileges.[23]

S0660 Clambling

Clambling has the ability to bypass UAC using a `passuac.dll` file.[24][25]

G0080 Cobalt Group

Cobalt Group has bypassed UAC.[26]

S0154 Cobalt Strike

Cobalt Strike can use a number of known techniques to bypass Windows UAC.[27][28]

S0527 CSPY Downloader

CSPY Downloader can bypass UAC using the SilentCleanup task to execute the binary with elevated privileges.[29]

S1111 DarkGate

DarkGate uses two distinct User Account Control (UAC) bypass techniques to escalate privileges.[30]

S0134 Downdelph

Downdelph bypasses UAC to escalate privileges by using a custom "RedirectEXE" shim database.[31]

G1006 Earth Lusca

Earth Lusca has used the Fodhelper UAC bypass technique to gain elevated privileges.[32]

S0363 Empire

Empire includes various modules to attempt to bypass UAC for escalation of privileges.[33]

G0120 Evilnum

Evilnum has used PowerShell to bypass UAC.[34]

S0182 FinFisher

FinFisher performs UAC bypass.[35][36]

S0666 Gelsemium

Gelsemium can bypass UAC to elevate process privileges on a compromised host.[37]

S0531 Grandoreiro

Grandoreiro can bypass UAC by registering as the default handler for .MSC files.[38]

S0132 H1N1

H1N1 bypasses user access control by using a DLL hijacking vulnerability in the Windows Update Standalone Installer (wusa.exe).[39]

S0260 InvisiMole

InvisiMole can use fileless UAC bypass and create an elevated COM object to escalate privileges.[40][41]

S0250 Koadic

Koadic has 2 methods for elevating integrity. It can bypass UAC through `eventvwr.exe` and `sdclt.exe`.[42]

S0669 KOCTOPUS

KOCTOPUS will perform UAC bypass either through fodhelper.exe or eventvwr.exe.[43]

S0356 KONNI

KONNI has bypassed UAC by performing token impersonation as well as an RPC-based method, this included bypassing UAC set to "AlwaysNotify".[44][45]

S1199 LockBit 2.0

LockBit 2.0 can bypass UAC through creating the Registry key `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\ICM\Calibration`.[46][47]

S1202 LockBit 3.0

LockBit 3.0 can bypass UAC to execute code with elevated privileges through an elevated Component Object Model (COM) interface.[48]

S0447 Lokibot

Lokibot has utilized multiple techniques to bypass UAC.[49]

G1051 Medusa Group

Medusa Group has attempted to bypass UAC using Component Object Model (COM) interface.[50]

G0069 MuddyWater

MuddyWater uses various techniques to bypass UAC.[51]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors used the malicious NTWDBLIB.DLL and `cliconfig.exe` to bypass UAC protections.[52]

G0040 Patchwork

Patchwork bypassed User Access Control (UAC).[53]

S0501 PipeMon

PipeMon installer can use UAC bypass techniques to install the payload.[54]

S0254 PLAINTEE

An older variant of PLAINTEE performs UAC bypass.[55]

S0378 PoshC2

PoshC2 can utilize multiple methods to bypass UAC.[56]

S0192 Pupy

Pupy can bypass Windows UAC through either DLL hijacking, eventvwr, or appPaths.[57]

S1242 Qilin

Qilin can bypass standard user access controls by using stolen tokens to launch processes at an elevated security context.[58]

S0262 QuasarRAT

QuasarRAT can generate a UAC pop-up Window to prompt the target user to run a command as the administrator.[59]

S0458 Ramsay

Ramsay can use UACMe for privilege escalation.[60][61]

S1130 Raspberry Robin

Raspberry Robin will use the legitimate Windows utility fodhelper.exe to run processes at elevated privileges without requiring a User Account Control prompt.[62]

S0662 RCSession

RCSession can bypass UAC to escalate privileges.[24]

S0332 Remcos

Remcos has a command for UAC bypassing.[63]

S0148 RTM

RTM can attempt to run the program as admin, then show a fake error message and a legitimate UAC bypass prompt to the user in an attempt to socially engineer the user into escalating privileges.[64]

S1018 Saint Bot

Saint Bot has attempted to bypass UAC using `fodhelper.exe` to escalate privileges.[65]

S0074 Sakula

Sakula contains UAC bypass code for both 32- and 64-bit systems.[66]

S0140 Shamoon

Shamoon attempts to disable UAC remote restrictions by modifying the Registry.[67]

S0444 ShimRat

ShimRat has hijacked the cryptbase.dll within migwiz.exe to escalate privileges. This prevented the User Access Control window from appearing.[68]

S0692 SILENTTRINITY

SILENTTRINITY contains a number of modules that can bypass UAC, including through Window's Device Manager, Manage Optional Features, and an image hijack on the `.msc` file extension.[69]

S0633 Sliver

Sliver can leverage multiple techniques to bypass User Account Control (UAC) on Windows systems.[70]

G0027 Threat Group-3390

A Threat Group-3390 tool can use a public UAC bypass method to elevate privileges.[71]

S0116 UACMe

UACMe contains many methods for bypassing Windows User Account Control on multiple versions of the operating system.[5]

S0670 WarzoneRAT

WarzoneRAT can use `sdclt.exe` to bypass UAC in Windows 10 to escalate privileges; for older Windows versions WarzoneRAT can use the IFileOperation exploit to bypass the UAC module.[72][73]

S0612 WastedLocker

WastedLocker can perform a UAC bypass if it is not executed with administrator rights or if the infected host runs Windows Vista or later.[74]

S0141 Winnti for Windows

Winnti for Windows can use a variant of the sysprep UAC bypass.[75]

S0230 ZeroT

Many ZeroT samples can perform UAC bypass by using eventvwr.exe to execute a malicious file.[76]

---

Source: https://attack.mitre.org/techniques/T1548/002