# TTP Detail – T1548.002

## TTP Information

Name: Bypass User Account Control

Description: Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.(Citation: TechNet How UAC Works)

If the UAC protection level of a computer is set to anything but the highest level, certain Windows programs can elevate privileges or execute some elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) objects without prompting the user through the UAC notification box.(Citation: TechNet Inside UAC)(Citation: MSDN COM Elevation) An example of this is use of [Rundll32](https://attack.mitre.org/techniques/T1218/011) to load a specifically crafted DLL which loads an auto-elevated [Component Object Model](https://attack.mitre.org/techniques/T1559/001) object and performs a file operation in a protected directory which would typically require elevated access. Malicious software may also be injected into a trusted process to gain elevated privileges without prompting a user.(Citation: Davidson Windows)

Many methods have been discovered to bypass UAC. The Github readme page for UACME contains an extensive list of methods(Citation: Github UACMe) that have been discovered and implemented, but may not be a comprehensive list of bypasses. Additional bypass methods are regularly discovered and some used in the wild, such as:

\* <code>eventvwr.exe</code> can auto-elevate and execute a specified binary or script.(Citation: enigma0x3 Fileless UAC Bypass)(Citation: Fortinet Fareit)

Another bypass is possible through some lateral movement techniques if credentials for an account with administrator privileges are known, since UAC is a single system security mechanism, and the privilege or integrity of a process running on one system will be unknown on remote systems and default to high integrity.(Citation: SANS UAC Bypass)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: privilege-escalation

**•** mitre-attack: defense-evasion

## Malware

* AppleJeus
* AutoIt backdoor
* Avaddon
* BADHATCH
* Bad Rabbit
* BitPaymer
* BlackCat
* BlackEnergy
* Bumblebee
* CHIMNEYSWEEP
* Clambling
* Cobalt Strike
* DarkGate
* Downdelph
* FinFisher
* Gelsemium
* Grandoreiro
* H1N1
* InvisiMole
* KOCTOPUS
* KONNI
* LockBit 2.0
* LockBit 3.0
* Lokibot
* PLAINTEE
* PipeMon
* RCSession
* RTM
* Ramsay
* Raspberry Robin
* Saint Bot
* Sakula
* Shamoon
* ShimRat
* WarzoneRAT
* WastedLocker
* Winnti for Windows
* ZeroT

## Tools

* CSPY Downloader
* Empire
* Koadic
* PoshC2
* Pupy
* QuasarRAT
* Remcos
* SILENTTRINITY
* Sliver
* UACMe

## APTs (Intrusion Sets)

* APT29
* APT37
* APT38
* BRONZE BUTLER
* Cobalt Group
* Earth Lusca
* Evilnum
* MuddyWater
* Patchwork
* Threat Group-3390