

Open in app ↗

Sign up

Sign in

Medium

Search

Write



FalconFriday — Detecting UAC Bypasses — 0xFF16



Gijs Hollestelle · [Follow](#)



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 \$/month

detection rules for several of these UAC bypasses that will allow detection of techniques that are not detected by default using MDE.

TL;DR for red teams: While many functional UAC bypass techniques are available, many of them allow for relatively easy detection. It might be beneficial to research your own techniques instead of relying on widely known techniques that can be easily detected.



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

The techniques in UACME are simply numbered 1 to 69 and can be invoked by running the “akagi” tool available in the Github repository and providing the technique number as the first command line argument. An additional argument providing the binary to launch can be provided but in our tests we omitted it, causing the default (which is “cmd.exe”) to be launched.

```
C:\Windows\System32\cmd.exe
C:\Temp\UACME\Source\Akagi\output\x64\Debug>whoami /groups | find "Label"
Mandatory Label\Medium Mandatory Level      Label      S-1-16-8192

C:\Temp\UACME\Source\Akagi\output\x64\Debug>.\akagi.exe 68
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

We also investigated whether or not the techniques are detected by Microsoft Defender for Endpoint (MDE) out of the box. This yields 6 techniques that are detected using the ‘UAC bypass was detected’ alert (techniques 33, 34, 56, 59, 62, and 67), and one technique that is detected using the ‘Behavior:Win32/UACBypassExp.F!sdclt’ alert (technique 53).

The other 5 functional techniques are not detected by MDE out of the box and require custom detection rules to be detected. Below we go through these techniques, investigate how they work and how they can be detected.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- 43 — {D2E7041B-2927-42fb-8E9F-7CE93B6DC937} — colorui.dll
- 65 — {E9495B87-D950-4AB5-87A5-FF6D70BF3E90} — wscui.cpl

With an excellent tool called OleViewDotNet (released by James Forshaw of Google Project Zero), we can view the properties of COM objects. If we use this tool to view one of the entries above we can see that these COM objects indeed provide elevation using “Auto Approval”.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "dllhost.exe"
| where ProcessIntegrityLevel == "High"
| where InitiatingProcessCommandLine has_any ("E9495B87-D950-4AB5-87A5-FF6D70BF3E90", "3E5FC7F9-9A51-4367-9063-A120244FBEC7", "D2E7041B-2927-42fb-8E9F-7CE93B6DC937")
```

Another approach would be to create a list of the CLSIDs of COM objects that are known to spawn child processes with high integrity under normal circumstances and look for process creation from other CLSIDs. This would also allow identifying newly discovered Elevated COM interfaces in the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

```
DeviceProcessEvents  
| where InitiatingProcessFileName =~ "wsreset.exe"  
| where ProcessIntegrityLevel == "High"
```

. . .

Technique 61 — ChangePK / SLUI Registry tampering

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

obviously a lot of ground to cover implementing a good detection capability. Keep an eye out for our next FalconFriday articles where we will dive into other areas.

- Falconfriday
- Uac
- Defender For Endpoint



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app