

# .. /Bitsadmin.exe

Alternate data streams

Download

Copy

Execute

Used for managing background intelligent transfer

## Paths:

C:\Windows\System32\bitsadmin.exe

C:\Windows\SysWOW64\bitsadmin.exe

## Resources:

- <https://www.slideshare.net/chrisgates/windows-attacks-at-is-the-new-black-26672679>
- [https://www.youtube.com/watch?v=\\_8xJaaQlpBo](https://www.youtube.com/watch?v=_8xJaaQlpBo)
- <https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f>

## Acknowledgements:

- Rob Fuller ([@mubix](#))
- Chris Gates ([@carnal0wnage](#))
- Oddvar Moe ([@oddvarmoe](#))

## Detections:

- Sigma:  
[https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process\\_creation/proc\\_creation\\_win\\_bitsadmin\\_download.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_bitsadmin_download.yml)
- Sigma:  
[https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/web/proxy\\_generic/proxy\\_ua\\_bitsadmin\\_susp\\_tld.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/web/proxy_generic/proxy_ua_bitsadmin_susp_tld.yml)
- Sigma:  
[https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process\\_creation/proc\\_creation\\_win\\_bitsadmin\\_potential\\_persistence.yml](https://github.com/SigmaHQ/sigma/blob/62d4fd26b05f4d81973e7c8e80d7c1a0c6a29d0e/rules/windows/process_creation/proc_creation_win_bitsadmin_potential_persistence.yml)
- Splunk:  
[https://github.com/splunk/security\\_content/blob/3f77e24974239fcb7a339080a1a483e6bad84a82/detections/endpoint/bitsadmin\\_download\\_file.yml](https://github.com/splunk/security_content/blob/3f77e24974239fcb7a339080a1a483e6bad84a82/detections/endpoint/bitsadmin_download_file.yml)
- IOC: Child process from bitsadmin.exe
- IOC: bitsadmin creates new files
- IOC: bitsadmin adds data to alternate data stream

## Alternate data streams

Create a bitsadmin job named 1, add cmd.exe to the job, configure the job to run the target command from an Alternate data stream, then resume and complete the job.

```
bitsadmin /create 1 bitsadmin /addfile 1 c:\windows\system32\cmd.exe c:\data\playfolder\cmd.exe bitsadmin /SetNotifyCmdLine 1 c:\data\playfolder\1.txt:cmd.exe NULL bitsadmin /RESUME 1 bitsadmin /complete 1
```

<b>Use case:</b>	Performs execution of specified file in the alternate data stream, can be used as a defensive evasion or persistence technique.
<b>Privileges required:</b>	User
<b>Operating systems:</b>	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
<b>ATT&amp;CK® technique:</b>	T1564.004

## Download

Create a bitsadmin job named 1, add cmd.exe to the job, configure the job to run the target command, then resume and complete the job.

```
bitsadmin /create 1 bitsadmin /addfile 1 https://live.sysinternals.com/autoruns.exe
c:\data\playfolder\autoruns.exe bitsadmin /RESUME 1 bitsadmin /complete 1
```

<b>Use case:</b>	Download file from Internet
<b>Privileges required:</b>	User
<b>Operating systems:</b>	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
<b>ATT&amp;CK® technique:</b>	T1105

## Copy

Command for copying cmd.exe to another folder

```
bitsadmin /create 1 & bitsadmin /addfile 1 c:\windows\system32\cmd.exe c:\data\playfolder\cmd.exe & bitsadmin
/RESUME 1 & bitsadmin /Complete 1 & bitsadmin /reset
```

<b>Use case:</b>	Copy file
<b>Privileges required:</b>	User
<b>Operating systems:</b>	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10
<b>ATT&amp;CK® technique:</b>	T1105

## Execute

One-liner that creates a bitsadmin job named 1, add cmd.exe to the job, configure the job to run the target command, then resume and complete the job.

```
bitsadmin /create 1 & bitsadmin /addfile 1 c:\windows\system32\cmd.exe c:\data\playfolder\cmd.exe & bitsadmin
/SetNotifyCmdLine 1 c:\data\playfolder\cmd.exe NULL & bitsadmin /RESUME 1 & bitsadmin /Reset
```

<b>Use case:</b>	Execute binary file specified. Can be used as a defensive evasion.
------------------	--------------------------------------------------------------------

**Privileges required:** User  
**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10  
**ATT&CK® technique:** T1218