1030 - BITSInject

Sunday at 10:30 in Track 3
20 minutes | Demo, Tool
Dor Azouri*Security researcher, @SafeBreach*

Windows' BITS service is a middleman for your download jobs. You start a BITS job, and from that point on, BITS is responsible for the download. But what if we tell you that BITS is a careless middleman? We have uncovered the way BITS maintains its jobs queue using a state file on disk, and found a way for a local administrator to control jobs using special modifications to that file

Comprehending this file's binary structure allowed us to change a job's properties (such as RemoteURL, Destination Path...) in runtime and even inject our own custom job, using none of BITS' public interfaces. This method, combined with the generous notification feature of BITS, allowed us to run a program of our will as the LocalSystem account, within session 0. So if you wish to execute your code as NT AUTHORITY/SYSTEM and the first options that come to mind are psexec/creating a service, we now add a new option: BITSInject.

Here, we will not only introduce the practical method we formed, but also: Reveal the binary structure of the state file for you to play with, and some knowledge we gathered while researching the service flow

We will also provide free giveaways: A one-click python tool that performs the described method; SimpleBITSServer - a pythonic BITS server; A struct definition file, to use for parsing your BITS state file
Dor Azouri
Dor Azouri is a security professional, having 6+ years of unique experience with network security, malware research and infosec data analysis. Currently doing security research @SafeBreach.

#defcon25/by_track/track3/sunday #defcon25/By_Day/_Sunday