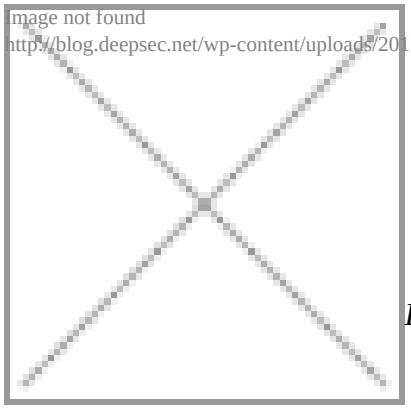
DeepSec 2017 Talk: BITSInject – Control Your BITS, Get SYSTEM – Dor Azouri

Posted on **October 08,2017** by **sanna**

Microsoft has introduced the Background Intelligent Transfer Service (BITS) into Windows 2000 and later versions of the operating system. Windows 7 and Windows Server 2008 R2 feature the version 4.0 of the protocol. BITS is designed to use idle bandwidth in order to transfer data to and from servers. BITS is an obedient servant, and it may be abused into doing transfers on behalf of others. Dor Azouri will present his findings regarding BITS at DeepSec 2007.

> 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?
>
> Current Windows software comes packaged with a mix of old and new features and components. New, shiny features and capabilities are added, with none of the old components needing to give up their place. That's why the Windows software landscape resembles a modern state-of-the-art office, with one or two pieces of refurbished furniture. One of these refurbished pieces of furniture is the BITS service. BITS has been with us since Windows XP and has since evolved through 5 major versions; the most recent release was in 2012. BITS facilitates transferring files over HTTP asynchronously in the background. Its most widespread use is to download Windows updates from Microsoft servers. Many other programs use it as well for downloading updates. In his talk, Dor identifies a new method and tool, called BITSInject, that allows a local administrator to completely control BITS jobs queue using an undocumented interface, and eventually run arbitrary programs as the LocalSystem account, within session 0.

Microsoft Windows administrators, take a look at Dor's talk! Unprivileged users should also attend to elevate their status.



Dor's a security professional, having 6+ years of unique experience with network security, malware research and infosec data analysis. Currently he's doing security research @SafeBreach.

Posted in:Conference,Internet,Security | Tagged:DeepSec,Hacking,MITM,Network,Talk | With 0 comments