* **Detecting ATT&CK Technique**[**T1105**](https://attack.mitre.org/techniques/T1105/) **(Remote File Copy) and**[**T1140**](https://attack.mitre.org/techniques/T1140/) **(De-obfuscate /Decode Files or Information)**

We shall be hunting for BITSAdmin and Certutil commands as mentioned in the above techniques which are utilized by threat actor [APT19](https://attack.mitre.org/groups/G0073/)

*ATP Query*

﻿SecurityEvent | where EventID == "4688" | where (Image endswith "\\bitsadmin.exe" and CommandLine == "/transfer")

﻿SecurityEvent | where EventID == "4688" | where CommandLine contains " -decode " or CommandLine contains " /decode " or CommandLine contains " -decodehex " or CommandLine contains " /decodehex " or CommandLine contains " -urlcache " or CommandLine contains " /urlcache " or CommandLine contains " -verifyctl " or CommandLine contains " /verifyctl " or CommandLine contains " -encode " or CommandLine contains " /encode " or CommandLine matches regex ".\*certutil.\* -URL.\*" or CommandLine matches regex ".\*certutil.\* /URL.\*" or CommandLine matches regex ".\*certutil.\* -ping.\*" or CommandLine matches regex ".\*certutil.\* /ping.\*"

﻿SecurityEvent | where EventID == "4688" | where CommandLine startswith "certutil -f -encode " or CommandLine startswith "certutil.exe -f -encode " or CommandLine startswith "certutil -encode -f " or CommandLine startswith "certutil.exe -encode -f "

* **Detecting** **ATT&CK Technique**[**T1208**](https://attack.mitre.org/techniques/T1208/) **(Kerberoasting)**

We shall be hunting for machines querying Domain Controller for SPN records which are used to uniquely identify each instance of a Windows service.

*ATP Query*

SecurityEvent | where EventID == "4688" | where ((Image endswith "\\setspn.exe" or Description matches regex ".\*Query or reset the computer.\* SPN attribute.\*") and CommandLine contains "-q")

SecurityEvent | where EventID == "4688" | where CommandLine contains " asreproast " or CommandLine contains " dump /service:krbtgt " or CommandLine contains " kerberoast " or CommandLine contains " createnetonly /program:" or CommandLine contains " ptt /ticket:" or CommandLine contains " /impersonateuser:" or CommandLine contains " renew /ticket:" or CommandLine contains " asktgt /user:" or CommandLine contains " harvest /interval:"

* **Detecting ATT&CK Technique** [**T1170**](https://attack.mitre.org/techniques/T1170/) **(execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility)**

We shall be hunting for threats leveraging mshta.exe during initial compromise and for execution of code (nothing by mshta.exe spawning cmd.exe)

*ATP Query*

﻿SecurityEvent | where EventID == "4688" | where ((ParentImage endswith "\mshta.exe"and Image endswith "\\cmd.exe" or Image endswith "\\powershell.exe" or Image endswith "\\wscript.exe" or Image endswith "\\cscript.exe" or Image endswith "\\sh.exe" or Image endswith "\\bash.exe" or Image endswith "\\reg.exe" or Image endswith "\\regsvr32.exe" or Image contains "\\BITSADMIN") and not (CommandLine contains "/HP/HP" or CommandLine contains "\\HP\\HP"))

* **Detecting Windows shell spawns suspicious program**

*ATP Query*

﻿SecurityEvent | where EventID == "4688" | where ((ParentImage endswith "\\mshta.exe" or ParentImage endswith "\\powershell.exe" or ParentImage endswith "\\cmd.exe" or ParentImage endswith "\\rundll32.exe" or ParentImage endswith "\\cscript.exe" or ParentImage endswith "\\wscript.exe" or ParentImage endswith "\\wmiprvse.exe" and Image endswith "\\schtasks.exe" or Image endswith "\\nslookup.exe" or Image endswith "\\certutil.exe" or Image endswith "\\bitsadmin.exe" or Image endswith "\\mshta.exe") and not (CurrentDirectory contains "\\ccmcache\\"))