Bypass UAC via CMSTP

Detect child processes of automatically elevated instances of Microsoft Connection Manager Profile Installer (`cmstp.exe`).

id:	e584f1a1-c303-4885-8a66-21360c90995b
categories:	detect
confidence:	medium
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Defense Evasion, Execution
techniques:	T1191 CMSTP, T1088 Bypass User Account Control

Query

```
sequence
  [ process where subtype.create and
      process_name == "cmstp.exe" and command_line =="*/s*" and command_line =="*/au*"] by
  [ process where subtype.create ] by unique_ppid
```

Detonation

Atomic Red Team: T1191

Contributors

- Endgame

Previous Next