Edit on GitHub

Bypass UAC via WSReset.exe

Identifies use of WSReset.exe to bypass User Account Control. Adversaries use this technique to execute privileged processes.

id:	532b5ed4-7930-11e9-8f5c-d46d6d62a49e
categories:	detect
confidence:	high
os:	windows
created:	05/17/2019
updated:	05/17/2019

MITRE ATT&CK™ Mapping

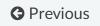|	
tactics:	Privilege Escalation
techniques:	T1088 Bypass User Account Control

Query

```
process where subtype.create and
  parent_process_name == "wsreset.exe" and process_name != "conhost.exe"
```

Detonation

Atomic Red Team: T1088

Contributors

- Tony Lambert

[◀ Previous]   [Next ▶]

Built with Sphinx using a theme provided by Read the Docs.

latest