

[-] Bypass UAC via Fodhelper.exe

- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors

[-] Bypass UAC via Fodhelper.exe

- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors

- Bypass UAC via WSReset.exe
- Change Default File Association
- Clearing Windows Event Logs with wevtutil
- COM Hijack via Script Object
- Command-Line Creation of a RAR file
- Control Panel Items
- Creation of an Archive with Common Archivers
- Creation of Kernel Module
- Creation of Scheduled Task with schtasks.exe
- Creation or Modification of Systemd Service
- Credential Enumeration via Credential Vault CLI
- Delete Volume USN Journal with fsutil
- Disconnecting from Network Shares with net.exe
- Discovery and Enumeration of System Information via Rundll32
- Discovery of a Remote System's

[Docs](#) » [Analytics](#) » Bypass UAC via Fodhelper.exe

[Edit on GitHub](#)

Bypass UAC via Fodhelper.exe

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

id:	e491ce22-792f-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 == "fodhelper.exe"
```

Detonation

 latest

Atomic Red Team: T1088

☐ Bypass UAC via Fodhelper.exe

- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors

☐ Bypass UAC via Fodhelper.exe

- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors

- Bypass UAC via WSReset.exe
- Change Default File Association
- Clearing Windows Event Logs with wevtutil
- COM Hijack via Script Object
- Command-Line Creation of a RAR file
- Control Panel Items
- Creation of an Archive with Common Archivers
- Creation of Kernel Module
- Creation of Scheduled Task with schtasks.exe
- Creation or Modification of Systemd Service
- Credential Enumeration via Credential Vault CLI
- Delete Volume USN Journal with fsutil
- Disconnecting from Network Shares with net.exe
- Discovery and Enumeration of System Information via Rundll32
- Discovery of a Remote System's

Contributors

- [Tony Lambert](#)

⬅ Previous

Next ➡

© Copyright 2019, Endgame Revision 30243396.

Built with [Sphinx](#) using a [theme](#) provided by [Read the Docs](#).

