□ Bypass UAC via CMSTP

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

Bypass UAC via CompMgmtLauncher

Bypass UAC via Fodhelper.exe

Bypass UAC via Fodhelper.exe

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

Disconnecting from Network Shares with net.exe

Discovery and Enumeration of System Information via Rundll32

Discovery of a Remote System's Time

Discovery of Domain Groups

Discovery of Network Environment via Built-in Tools

Discovery of Network Environment via Built-in Tools

DLL Search Order Hijacking with known programs

Domain Trust Discovery

Domain Trust Discovery via NItest.exe

Encoding or Decoding Files via CertUtil

Enumeration of Local Shares

Enumeration of Mounted Shares

Enumeration of Remote Shares

Enumeration of System Information

Enumeration of System Information

Executable Written and Executed by Microsoft Office Applications

Execution of a Command via a SYSTEM Service

Execution of Existing Service via Command

Docs » Analytics » Bypass UAC via CMSTP

C Edit on GitHub

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

created: 11/30/2018

updated: 11/30/2018

MITRE ATT&CK™ Mapping

windows

tactics: Defense Evasion, Execution

techniques: T1191 CMSTP, T1088 Bypass User Account Control

Query

os:

```
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



Next **②**

© Copyright 2019, Endgame Revision 30243396.

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

