

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

Host Artifact Deletion

Image Debuggers for Accessibility Features

Incoming Remote PowerShell Sessions

Indirect Command Execution

Installation of Port Monitor

Installation of Security Support Provider

Installation of Time Providers

Installing Custom Shim Databases

InstallUtil Execution

Interactive AT Job

Launch Daemon Persistence

Loading Kernel Modules with kextload

Local Job Scheduling Paths

Local Job Scheduling Process

Logon Scripts with UserInitMprLogonScript

LSA Authentication Package

LSASS Memory Dumping

LSASS Memory Dumping via ProcDump.exe

Modification of Boot Configuration

Modification of ld.so.preload

Modification of Logon Scripts from Registry

Identifies usage of hh.exe executing recently modified .chm files.

b25aa548-7937-11e9-8f5c-d46d6d62a49e

detect

medium

windows

08/08/2019

09/26/2019

[Defense Evasion, Execution](#)

[T1223](#) Compiled HTML File

```
sequence with maxspan=1d
  [file where file_name == "*.chm"]
  [process where subtype.create and process_name == "hh.
```

[Atomic Red Team: T1223](#)



MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

Host Artifact Deletion

Image Debuggers for Accessibility
Features

Incoming Remote PowerShell
Sessions

Indirect Command Execution

Installation of Port Monitor

Installation of Security Support
Provider

Installation of Time Providers

Installing Custom Shim Databases

InstallUtil Execution

Interactive AT Job

Launch Daemon Persistence

Loading Kernel Modules with
kextload

Local Job Scheduling Paths

Local Job Scheduling Process

Logon Scripts with
UserInitMprLogonScript

LSA Authentication Package

LSASS Memory Dumping

LSASS Memory Dumping via
ProcDump.exe

Modification of Boot Configuration

Modification of Id.so.preload

Modification of Logon Scripts from
Registry

• [Dan Beavin](#)

[← Previous](#)

[Next →](#)

© Copyright 2019, Endgame Revision 30243396.

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