⊟ HH.exe execution
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
Modification of rc.common Script
Modifications of .bash_profile and .bashrc
Mounting Hidden Shares
Mounting Windows Hidden Shares with net.exe
MS Office Template Injection
Mshta Descendant of Microsoft Office
Mshta Network Connections
Network Service Scanning via Port
Non-browser processes making DNS requests to Dynamic DNS Providers
Office Application Startup via Template File Modification
Office Application Startup via Template Registry Modification
Password Policy Enumeration
Persistence via AppInit DLL
Persistence via NetSh Key
Persistence via Screensaver
Persistent process via Launch Agent

HH.exe execution

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

id:	b25aa548-7937-11e9-8f5c-d46d6d62a49e
categories:	detect
confidence:	medium
os:	windows
created:	08/08/2019
updated:	09/26/2019

MITRE ATT&CK™ Mapping

tactics:	Defense Evasion, Execution
techniques:	T1223 Compiled HTML File

Query

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

Detonation

Atomic Red Team: T1223

Contributors

- Dan Beavin

Previous   Next

© Copyright 2019, Endgame Revision 30243396.

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

latest