⊟ Enumeration of Remote Shares
MITRE ATT&CK™ Mapping
Query
Detonation
Contributors
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
Execution via cmstp.exe
HH.exe execution
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

Enumeration of Remote Shares

Identifies enumeration of remote shares with the built-in Windows tool `net.exe`.

id:	e61f557c-a9d0-4c25-ab5b-bbc46bb24deb
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Discovery
techniques:	T1135 Network Share Discovery

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.exe" and parent_process_name != "net
  command_line == "* view*" and command_line == "*\\\\*"
```

Detonation

Atomic Red Team: T1135

Contributors

- Endgame

Previous   Next

© Copyright 2019, Endgame Revision 30243396.

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

latest