Resumed Application on Reboot

Root Certificate Install

SAM Dumping via Reg.exe

Scheduled Task Creation via Microsoft Office Application

Searching for Passwords in Files

Searching for Passwords in Files

Service Path Modification with sc.exe

Service Stop or Disable with sc.exe

Startup Folder Execution via VBScript

Startup Folder Persistence with Shortcut/VBScript Files

Stopping Services with net.exe

Suspicious ADS File Creation

Suspicious Bitsadmin Job via bitsadmin.exe

Suspicious Bitsadmin Job via PowerShell

Suspicious File Creation via Browser Extensions

Suspicious MS Office Registry Modifications

Suspicious Process Loading Credential Vault DLL

Suspicious Script Object Execution

System Information Discovery

System Network Connections Discovery

System Owner and User Discovery

Trap Signals Usage

Unload Sysmon Filter Driver with fltmc.exe

Unusual Child Process

User Account Creation

Volume Shadow Copy Deletion via VssAdmin

Volume Shadow Copy Deletion via WMIC

Windows File Permissions Modification

□ Windows Network Enumeration

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

WMI Execution via Microsoft Office Application

WMI Execution with Command Line Redirection

Atomic Blue Detections

Enterprise ATT&CK Matrix

Schemas

Resources

License

Docs » Analytics » Windows Network Enumeration

C Edit on GitHub

Windows Network Enumeration

Identifies attempts to enumerate hosts in a network using the built-in Windows net.exe tool.

id: b8a94d2f-dc75-4630-9d73-1edc6bd26fff

categories: detect

os: windows

created: 11/30/2018

updated: 11/30/2018

MITRE ATT&CK™ Mapping

tactics: Discovery

techniques: T1018 Remote System Discovery

Query

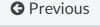
```
process where subtype.create and
process_name == "net.exe" and command_line == "* view*" and command_line != "*\\\*"
```

Detonation

Atomic Red Team: T1018

Contributors

• Endgame



Next 🖸

© Copyright 2019, Endgame Revision 30243396.

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

