⊟ Mounting Hidden Shares
MITRE ATT&CK™ Mapping
Query
Detonation
Contributors
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
Plist Modification
Potential Gatekeeper Bypass
Process Discovery via Built-In Applications
Process Discovery via Windows Tools
Processes Running with Unusual Extensions
Processes with Trailing Spaces
Proxied Execution via Signed Scripts
Reading the Clipboard with pbpaste
Registration of a Password Filter DLL
Registration of Winlogon Helper DLL
Registry Persistence via Run Keys
Registry Persistence via Shell Folders
Registry Preparation of Event Viewer UAC Bypass
RegSvr32 Scriptlet Execution
Remote Desktop Protocol Hijack
Remote Execution via WMIC
Remote System Discovery Commands
Remote Terminal Sessions
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

Mounting Hidden Shares

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

id:	9b3dd402-891c-4c4d-a662-28947168ce61
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Lateral Movement
techniques:	T1077 Windows Admin Shares

Query

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

  // since this command is looking for discovery only, we want to ignore mounting shares
  command_line == "* \\\\*"
| unique parent_process_path, command_line, user_name
```

Detonation

Atomic Red Team: T1077

Contributors

- Endgame

Previous

Next

latest