⊟ Interactive AT Job
- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors
- References

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
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

Interactive AT Job

Detect an interactive AT job, which may be used as a form of privilege escalation.

id:	d8db43cf-ed52-4f5c-9fb3-c9a4b95a0b56
categories:	detect
confidence:	medium
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Privilege Escalation
techniques:	T1053 Scheduled Task

Note

As of Windows 8, the `at.exe` command was deprecated and prints the error message

> The AT command has been deprecated. Please use schtasks.exe instead.

Query

```
process where subtype.create and
  process_name == "at.exe" and command_line == "* interactive *"
```

Detonation

Atomic Red Team: T1053

Contributors

- Endgame

References

- https://blogs.technet.microsoft.com/supportingwindows/2013/07/05/whats-new-in-task-scheduler-for-windows-8-server-2012/

Previous   Next

latest