⊟ Domain Trust Discovery via Nltest.exe
- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors

Encoding or Decoding Files via CertUtil
Enumeration of Local Shares
Enumeration of Mounted Shares
Enumeration of Remote Shares
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

Docs » Analytics » Domain Trust Discovery via Nltest.exe   Edit on GitHub

Domain Trust Discovery via Nltest.exe

Identifies execution of nltest.exe for domain trust discovery. This technique is used by attackers to enumerate Active Directory trusts.

id:	03e231a6-74bc-467a-acb1-e5676b0fb55e
categories:	hunt
confidence:	low
os:	windows
created:	05/17/2019
updated:	05/17/2019

MITRE ATT&CK™ Mapping

tactics:	Discovery
techniques:	T1482 Domain Trust Discovery

Query

```
process where subtype.create and
  process_name == "nltest.exe" and command_line == "*domain_trusts*"
```

Detonation

Atomic Red Team: T1482

Contributors

- Tony Lambert

Previous   Next

latest