

Discovery of a Remote System's Time

- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors

Discovery of a Remote System's Time

Identifies use of various commands to query a remote system's time. This technique may be used before executing a scheduled task or to discover the time zone of a target system

id:	fcdb99c2-ac3c-4bde-b664-4b336329bed2
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Discovery
techniques:	T1124 System Time Discovery

Query

```
process where subtype.create and process_name == "net.exe" and
  command_line == "* time *" and command_line == "*\\\\\\*"
| unique parent_process_path, command_line
```

Detonation

Atomic Red Team: T1124

Contributors

- Endgame

Previous	Next
----------	------

© Copyright 2019, Endgame Revision 30243396.

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

Discovery of Domain Groups

Discovery of Network Environment via Built-in Tools

Discovery of Network Environment via Built-in Tools

DLL Search Order Hijacking with known programs

Domain Trust Discovery

Domain Trust Discovery via Nltest.exe

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