#### □ Command-Line Creation of a RAR file

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

**Control Panel Items** 

Creation of an Archive with Common Archivers

Creation of Kernel Module

Creation of Scheduled Task with schtasks.exe

Creation or Modification of Systemd Service

Credential Enumeration via Credential Vault CLI

Delete Volume USN Journal with fsutil

Disconnecting from Network Shares with net.exe

Discovery and Enumeration of System Information via Rundll32

Discovery of a Remote System's Time

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 NItest.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

Docs » Analytics » Command-Line Creation of a RAR file

C Edit on GitHub

# Command-Line Creation of a RAR file

Detect compression of data into a RAR file using the | rar.exe | utility.

id: 1ec33c93-3d0b-4a28-8014-dbdaae5c60ae

categories: detect

confidence: medium

os: windows

created: 11/30/2018 updated: 11/30/2018

# MITRE ATT&CK™ Mapping

tactics: Exfiltration

techniques: T1002 Data Compressed

## Query

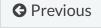
```
process where subtype.create and process_name == "rar.exe" and
command_line == "* a *"
```

#### **Detonation**

Atomic Red Team: T1002

### **Contributors**

Endgame



Next **3** 

© Copyright 2019, Endgame Revision 30243396.

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

