⊟ Mshta Network Connections
- MITRE ATT&CK™ Mapping
- Query
- Detonation
- Contributors

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

Docs » Analytics » Mshta Network Connections

Edit on GitHub

Mshta Network Connections

Identifies suspicious `mshta.exe` commands that make outbound network connections.

id:	6bc283c4-21f2-4aed-a05c-a9a3ffa95dd4
categories:	detect
confidence:	medium
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Execution, Defense Evasion, Command and Control
techniques:	T1170 Mshta

Query

```
sequence by unique_pid
  [process where subtype.create and process_name == "msht
  [network where process_name == "mshta.exe"]
```

Detonation

Atomic Red Team: T1170

⊟ Mshta Network Connections

MITRE ATT&CK™ Mapping

Query

Detonation

Contributors

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

Contributors

- Endgame

➜ Previous

Next ➜

© Copyright 2019, Endgame Revision 30243396.

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