

ProductsPricingSearchAboutDocs

Request a Demo →

⚙️👤

 Search for windows process filenames or hashes

Search

mshta.exe

Author: Microsoft

Source: Wild

Summary

Mshta.exe is used to execute an HTML Application (HTA). An HTA is a Microsoft Windows program whose source code consists of HTML, Dynamic HTML, and one or more scripting languages supported by Internet Explorer, such as VBScript or JScript.

EchoTrail Prevalence Score (EPS)

31.97

?

Rank Analysis

Host Prevalence

5.3%

?

Execution Rank

2,659th

?

Behavioral Analysis

Top Hashes

355beb0ff255e495bba836298f79ff

28.57 %

More features and access with an account

Top Paths

C:\Windows\SysWOW64

80.14 %

More features and access with an account

Top Network Ports

443

66.13 %

More features and access with an account

Ancestry Analysis

Top GrandParents

explorer.exe

39.42 %

More features and access with an account

Top Parents

HP DeskJet 3630 series.exe

22.70 %

More features and access with an account

Top Children

HPPAHelper.exe

28.87 %

More features and access with an account

Security Analysis

Intel

Mshta.exe isn't normally launched by shells. When this does happen, it's possible an attacker is attempting to abuse mshta's ability to run arbitrary scripts and make network connections.

Sigma Detection Rule:

https://github.com/SigmaHQ/sigma/blob/eb382c4a59b6d87e186ee269805fe2db2acf250e/rules/windows/process_creation/win_shell_spawn_mshta.yml

[About](#)[Blog](#)[Terms](#)[Privacy Policy](#)[Contact Us](#)



© 2024 EchoTrail, Ltd. All rights reserved.
This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.