# TTP Detail – T1059.005

## TTP Information

Name: Visual Basic

Description: Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and the [Native API](https://attack.mitre.org/techniques/T1106) through the Windows API. Although tagged as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.(Citation: VB .NET Mar 2020)(Citation: VB Microsoft)  
  
Derivative languages based on VB have also been created, such as Visual Basic for Applications (VBA) and VBScript. VBA is an event-driven programming language built into Microsoft Office, as well as several third-party applications.(Citation: Microsoft VBA)(Citation: Wikipedia VBA) VBA enables documents to contain macros used to automate the execution of tasks and other functionality on the host. VBScript is a default scripting language on Windows hosts and can also be used in place of [JavaScript](https://attack.mitre.org/techniques/T1059/007) on HTML Application (HTA) webpages served to Internet Explorer (though most modern browsers do not come with VBScript support).(Citation: Microsoft VBScript)  
  
Adversaries may use VB payloads to execute malicious commands. Common malicious usage includes automating execution of behaviors with VBScript or embedding VBA content into [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) payloads (which may also involve [Mark-of-the-Web Bypass](https://attack.mitre.org/techniques/T1553/005) to enable execution).(Citation: Default VBS macros Blocking )

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Astaroth
* BabyShark
* BackConfig
* Bandook
* Bisonal
* Bumblebee
* CHIMNEYSWEEP
* Chaes
* Cobalt Strike
* Comnie
* DanBot
* DarkGate
* Emotet
* Exaramel for Windows
* Ferocious
* Flagpro
* Goopy
* Grandoreiro
* Helminth
* IPsec Helper
* IcedID
* JCry
* JSS Loader
* Javali
* KOCTOPUS
* Kerrdown
* KeyBoy
* Lokibot
* LookBack
* LunarMail
* Melcoz
* Metamorfo
* Mispadu
* NETWIRE
* NanHaiShu
* NanoCore
* OSX\_OCEANLOTUS.D
* OopsIE
* POWERSTATS
* PoetRAT
* PowerShower
* Pteranodon
* QUADAGENT
* QakBot
* REvil
* ROKRAT
* Ramsay
* Remexi
* STARWHALE
* SUNBURST
* SVCReady
* Saint Bot
* ShrinkLocker
* Sibot
* Smoke Loader
* Snip3
* Squirrelwaffle
* StoneDrill
* TAMECAT
* TYPEFRAME
* Ursnif
* VBShower
* WhisperGate
* Xbash
* jRAT

## Tools

* Donut
* Koadic

## APTs (Intrusion Sets)

* APT-C-36
* APT32
* APT33
* APT37
* APT38
* APT39
* APT42
* BRONZE BUTLER
* Cobalt Group
* Confucius
* Earth Lusca
* FIN13
* FIN4
* FIN7
* Gamaredon Group
* Gorgon Group
* HEXANE
* Higaisa
* Inception
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* Machete
* Magic Hound
* Malteiro
* Molerats
* MuddyWater
* Mustang Panda
* OilRig
* Patchwork
* Rancor
* RedCurl
* Sandworm Team
* SideCopy
* Sidewinder
* Silence
* TA2541
* TA459
* TA505
* Transparent Tribe
* Turla
* WIRTE
* Windshift