# TTP Detail – T1204.002

## TTP Information

Name: Malicious File

Description: An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, .cpl, and .reg.

Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs)

While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Agent Tesla
* AppleJeus
* AppleSeed
* Astaroth
* BADFLICK
* BLINDINGCAN
* Bad Rabbit
* Bandook
* Bisonal
* Black Basta
* BoomBox
* Bumblebee
* Bundlore
* Cardinal RAT
* Chaes
* Clambling
* DanBot
* DarkGate
* DarkTortilla
* Disco
* DnsSystem
* Dridex
* Emotet
* EnvyScout
* Flagpro
* Grandoreiro
* GuLoader
* Hancitor
* Heyoka Backdoor
* IcedID
* InvisiMole
* JCry
* JSS Loader
* Javali
* KGH\_SPY
* KOCTOPUS
* KONNI
* KOPILUWAK
* Kerrdown
* Latrodectus
* Lokibot
* Lumma Stealer
* LunarMail
* Mango
* Metamorfo
* Mispadu
* Mongall
* NETWIRE
* NativeZone
* Ninja
* OSX/Shlayer
* Octopus
* OutSteel
* PLEAD
* PoetRAT
* Pony
* QakBot
* REvil
* ROKRAT
* RTM
* Ramsay
* Rifdoor
* SQLRat
* STARWHALE
* SUGARDUMP
* SVCReady
* SYSCON
* Saint Bot
* Snip3
* Squirrelwaffle
* StrelaStealer
* StrongPity
* TYPEFRAME
* Taidoor
* ThreatNeedle
* TrickBot
* Valak
* WarzoneRAT
* Woody RAT
* ZxxZ

## Tools

* Brute Ratel C4
* CARROTBALL
* CSPY Downloader

## APTs (Intrusion Sets)

* APT-C-36
* APT12
* APT19
* APT28
* APT29
* APT30
* APT32
* APT33
* APT37
* APT38
* APT39
* Ajax Security Team
* Andariel
* Aoqin Dragon
* BITTER
* BRONZE BUTLER
* BlackTech
* CURIUM
* Cobalt Group
* Confucius
* Dark Caracal
* DarkHydrus
* Darkhotel
* Dragonfly
* EXOTIC LILY
* Earth Lusca
* Elderwood
* FIN4
* FIN6
* FIN7
* FIN8
* Ferocious Kitten
* Gallmaker
* Gamaredon Group
* Gorgon Group
* HEXANE
* Higaisa
* Inception
* IndigoZebra
* Indrik Spider
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* Machete
* Magic Hound
* Malteiro
* Mofang
* Molerats
* Moonstone Sleet
* MuddyWater
* Mustang Panda
* Naikon
* Nomadic Octopus
* OilRig
* PLATINUM
* PROMETHIUM
* Patchwork
* RTM
* Rancor
* RedCurl
* Saint Bear
* Sandworm Team
* SideCopy
* Sidewinder
* Silence
* Star Blizzard
* Storm-1811
* TA2541
* TA459
* TA505
* TA551
* The White Company
* Threat Group-3390
* Tonto Team
* Transparent Tribe
* Tropic Trooper
* WIRTE
* Whitefly
* Windshift
* Wizard Spider
* admin@338
* menuPass