# TTP Detail – T1204.001

## TTP Information

Name: Malicious Link

Description: An adversary may rely upon a user clicking a malicious link in order to gain execution. Users may be subjected to social engineering to get them to click on a link that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Clicking on a link may also lead to other execution techniques such as exploitation of a browser or application vulnerability via [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). Links may also lead users to download files that require execution via [Malicious File](https://attack.mitre.org/techniques/T1204/002).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* AppleJeus
* BackConfig
* Bazar
* Bumblebee
* Emotet
* Gootloader
* Grandoreiro
* GuLoader
* Hancitor
* Javali
* KOCTOPUS
* Kerrdown
* Latrodectus
* Melcoz
* NETWIRE
* ObliqueRAT
* OutSteel
* PLEAD
* Pony
* QakBot
* SMOKEDHAM
* Saint Bot
* Snip3
* SocGholish
* SpicyOmelette
* Squirrelwaffle
* TSCookie

## APTs (Intrusion Sets)

* APT28
* APT29
* APT3
* APT32
* APT33
* APT38
* APT39
* BlackTech
* Cobalt Group
* Confucius
* Daggerfly
* EXOTIC LILY
* Earth Lusca
* Elderwood
* Evilnum
* FIN4
* FIN7
* FIN8
* Gamaredon Group
* Kimsuky
* LazyScripter
* Leviathan
* LuminousMoth
* Machete
* Magic Hound
* Mofang
* Molerats
* MuddyWater
* Mustang Panda
* Mustard Tempest
* OilRig
* Patchwork
* RedCurl
* Saint Bear
* Sandworm Team
* Sidewinder
* TA2541
* TA505
* TA577
* TA578
* Transparent Tribe
* Turla
* Windshift
* Winter Vivern
* Wizard Spider
* ZIRCONIUM