# TTP Detail – T1566.001

## TTP Information

Name: Spearphishing Attachment

Description: Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](https://attack.mitre.org/techniques/T1204) to gain execution.(Citation: Unit 42 DarkHydrus July 2018) Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: initial-access

## Malware

* Agent Tesla
* AppleSeed
* Astaroth
* BADFLICK
* BLINDINGCAN
* Bandook
* Bisonal
* Bumblebee
* Chaes
* Clambling
* DanBot
* DarkGate
* DarkTortilla
* DarkWatchman
* Emotet
* EnvyScout
* Flagpro
* Hancitor
* IcedID
* JSS Loader
* Javali
* KOCTOPUS
* KONNI
* KOPILUWAK
* Kerrdown
* Latrodectus
* Lokibot
* Lumma Stealer
* Metamorfo
* NETWIRE
* OceanSalt
* Octopus
* OutSteel
* PoetRAT
* Pony
* QakBot
* REvil
* ROKRAT
* RTM
* Ramsay
* Rifdoor
* SVCReady
* Saint Bot
* Snip3
* Squirrelwaffle
* StrelaStealer
* Taidoor
* ThreatNeedle
* TrickBot
* Valak
* WarzoneRAT
* Woody RAT
* XLoader
* ZxxZ

## APTs (Intrusion Sets)

* APT-C-36
* APT1
* APT12
* APT19
* APT28
* APT29
* APT30
* APT32
* APT33
* APT37
* APT38
* APT39
* APT41
* Ajax Security Team
* Andariel
* BITTER
* BRONZE BUTLER
* BlackTech
* CURIUM
* Cobalt Group
* Confucius
* DarkHydrus
* Darkhotel
* Dragonfly
* EXOTIC LILY
* Elderwood
* FIN4
* FIN6
* FIN7
* FIN8
* Ferocious Kitten
* Gallmaker
* Gamaredon Group
* Gorgon Group
* Higaisa
* Inception
* IndigoZebra
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* Machete
* Malteiro
* Mofang
* Molerats
* Moonstone Sleet
* MuddyWater
* Mustang Panda
* Naikon
* Nomadic Octopus
* OilRig
* PLATINUM
* Patchwork
* RTM
* Rancor
* RedCurl
* Saint Bear
* Sandworm Team
* SideCopy
* Sidewinder
* Silence
* Star Blizzard
* TA2541
* TA459
* TA505
* TA551
* The White Company
* Threat Group-3390
* Tonto Team
* Transparent Tribe
* Tropic Trooper
* WIRTE
* Windshift
* Winter Vivern
* Wizard Spider
* admin@338
* menuPass