# TTP Detail – T1566.002

## TTP Information

Name: Spearphishing Link

Description: Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place.

Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023)

Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Adversaries may also utilize spearphishing links to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s that grant immediate access to the victim environment. For example, a user may be lured through “consent phishing” into granting adversaries permissions/access via a malicious OAuth 2.0 request URL .(Citation: Trend Micro Pawn Storm OAuth 2017)(Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Similarly, malicious links may also target device-based authorization, such as OAuth 2.0 device authorization grant flow which is typically used to authenticate devices without UIs/browsers. Known as “device code phishing,” an adversary may send a link that directs the victim to a malicious authorization page where the user is tricked into entering a code/credentials that produces a device token.(Citation: SecureWorks Device Code Phishing 2021)(Citation: Netskope Device Code Phishing 2021)(Citation: Optiv Device Code Phishing 2021)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: initial-access

## Malware

* AppleJeus
* Bazar
* Bumblebee
* DarkGate
* Emotet
* Grandoreiro
* GuLoader
* Hancitor
* Javali
* KOCTOPUS
* Kerrdown
* Latrodectus
* Lumma Stealer
* Melcoz
* Mispadu
* NETWIRE
* OutSteel
* Pony
* QakBot
* Saint Bot
* Snip3
* SocGholish
* SpicyOmelette
* Squirrelwaffle
* TrickBot
* Valak

## Tools

* AADInternals

## APTs (Intrusion Sets)

* APT1
* APT29
* APT3
* APT32
* APT33
* APT39
* APT42
* BlackTech
* Cobalt Group
* Confucius
* EXOTIC LILY
* Earth Lusca
* Elderwood
* Evilnum
* FIN4
* FIN7
* FIN8
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* LuminousMoth
* Machete
* Magic Hound
* Mofang
* Molerats
* MuddyWater
* Mustang Panda
* Mustard Tempest
* OilRig
* Patchwork
* RedCurl
* Sandworm Team
* Sidewinder
* Storm-1811
* TA2541
* TA505
* TA577
* Transparent Tribe
* Turla
* Windshift
* Wizard Spider
* ZIRCONIUM