Phishing: Spearphishing Link, Sub-technique T1566.002 - Enterprise

Archived: 2026-04-05 18:23:36 UTC

S0677 AADInternals

AADInternals can send "consent phishing" emails containing malicious links designed to steal users' access tokens.[8]

S0584 AppleJeus

AppleJeus has been distributed via spearphishing link.[9]

G0006 APT1

APT1 has sent spearphishing emails containing hyperlinks to malicious files.[10]

G0016 APT29

APT29 has used spearphishing with a link to trick victims into clicking on a link to a zip file containing malicious files.[11][12][13]

G0022 APT3

APT3 has sent spearphishing emails containing malicious links.[14]

G0050 APT32

APT32 has sent spearphishing emails containing malicious links.[15][16][17][18][19]

G0064 APT33

APT33 has sent spearphishing emails containing links to .hta files.[20][21]

G0087 APT39

APT39 leveraged spearphishing emails with malicious links to initially compromise victims.[22][23]

G1044 APT42

APT42 has sent spearphishing emails containing malicious links.[24][25][26]

S0534 Bazar

Bazar has been spread via emails with embedded malicious links.[27][28][29]

G0098 BlackTech

BlackTech has used spearphishing e-mails with links to cloud services to deliver malware.[30]

S1039 Bumblebee

Bumblebee has been spread through e-mail campaigns with malicious links.[31][32]

C0011 C0011

During C0011, Transparent Tribe sent emails containing a malicious link to student targets in India.[33]

C0021 C0021

During C0021, the threat actors sent phishing emails with unique malicious links, likely for tracking victim clicks. [34][35]

G0080 Cobalt Group

Cobalt Group has sent emails with URLs pointing to malicious documents.[36][37]

G0142 Confucius

Confucius has sent malicious links to victims through email campaigns.[38]

S1111 DarkGate

DarkGate is distributed in phishing emails containing links to distribute malicious VBS or MSI files.[39] DarkGate uses applications such as Microsoft Teams for distributing links to payloads.[39]

G1006 Earth Lusca

Earth Lusca has sent spearphishing emails to potential targets that contained a malicious link.[40]

G0066 Elderwood

Elderwood has delivered zero-day exploits and malware to victims via targeted emails containing a link to malicious content hosted on an uncommon Web server.[41][42]

S0367 Emotet

Emotet has been delivered by phishing emails containing links. [43][44][45][46][47][48][49][49][50]

G0120 Evilnum

Evilnum has sent spearphishing emails containing a link to a zip file hosted on Google Drive.[51]

G1011 EXOTIC LILY

EXOTIC LILY has relied on victims to open malicious links in e-mails for execution.[52]

G0085 FIN4

FIN4 has used spearphishing emails (often sent from compromised accounts) containing malicious links.[53][54]

G0046 FIN7

FIN7 has conducted broad phishing campaigns using malicious links.[55] Additionally, FIN7 has sent spearphishing emails containing a typosquatted link to "ip-sccanner[.]com."[56]

G0061 FIN8

FIN8 has distributed targeted emails containing links to malicious documents with embedded macros.[57]

S0531 Grandoreiro

Grandoreiro has been spread via malicious links embedded in e-mails.[58][59]

S0561 GuLoader

GuLoader has been spread in phishing campaigns using malicious web links.[60]

S0499 Hancitor

Hancitor has been delivered via phishing emails which contained malicious links.[61]

S1229 Havoc

Havoc has been distributed through ClickFix phishing campaigns.[62]

S0528 Javali

Javali has been delivered via malicious links embedded in e-mails.[63]

S0585 Kerrdown

Kerrdown has been distributed via e-mails containing a malicious link.[19]

G0094 Kimsuky

Kimsuky has sent spearphishing emails containing a link to a document that contained malicious macros or took the victim to an actor-controlled domain.[64][65][66]

S0669 KOCTOPUS

KOCTOPUS has been distributed as a malicious link within an email.[67]

S1160 Latrodectus

Latrodectus has been distributed to victims through emails containing malicious links.[68][69]

G0032 Lazarus Group

Lazarus Group has sent malicious links to victims via email.[70]

G0140 LazyScripter

LazyScripter has used spam emails that contain a link that redirects the victim to download a malicious document.[67]

G0065 Leviathan

Leviathan has sent spearphishing emails with links, often using a fraudulent lookalike domain and stolen branding.[71][72]

G1014 LuminousMoth

LuminousMoth has sent spearphishing emails containing a malicious Dropbox download link.[73]

S1213 Lumma Stealer

Lumma Stealer has been delivered through phishing emails containing malicious links.[74]

G0095 Machete

Machete has sent phishing emails that contain a link to an external server with ZIP and RAR archives.[75][76]

G0059 Magic Hound

Magic Hound has sent malicious URL links through email to victims. In some cases the URLs were shortened or linked to Word documents with malicious macros that executed PowerShells scripts to download Pupy.[77][78][79][80]

S0530 Melcoz

Melcoz has been spread through malicious links embedded in e-mails.[63]

S1122 Mispadu

Mispadu has been spread via malicious links embedded in emails.[81]

G0103 Mofang

Mofang delivered spearphishing emails with malicious links included.[82]

G0021 Molerats

Molerats has sent phishing emails with malicious links included.[83]

G0069 MuddyWater

MuddyWater has sent targeted spearphishing e-mails with malicious links.[84][85][86]

G0129 Mustang Panda

Mustang Panda has delivered malicious links to their intended targets.[87][88][89] Mustang Panda has distributed spear-phishing emails with embedded links that direct the victim to a malicious archive hosted on Google or Dropbox.[90]

G1020 Mustard Tempest

Mustard Tempest has sent victims emails containing links to compromised websites.[91]

S0198 NETWIRE

NETWIRE has been spread via e-mail campaigns utilizing malicious links.[60]

C0002 Night Dragon

During Night Dragon, threat actors sent spearphishing emails containing links to compromised websites where malware was downloaded.[92]

G0049 OilRig

OilRig has sent spearphising emails with malicious links to potential victims.[93][94]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group sent malicious OneDrive links with fictitious job offer advertisements via email.[95][96]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors sent spearphishing emails containing a malicious link.[97]

C0005 Operation Spalax

During Operation Spalax, the threat actors sent phishing emails to victims that contained a malicious link.[98]

S1017 OutSteel

OutSteel has been distributed through malicious links contained within spearphishing emails.[99]

G0040 Patchwork

Patchwork has used spearphishing with links to deliver files with exploits to initial victims.[100][101][102]

C0036 Pikabot Distribution February 2024

Pikabot Distribution February 2024 utilized emails with hyperlinks leading to malicious ZIP archive files containing scripts to download and install Pikabot.[103]

S0453 Pony

Pony has been delivered via spearphishing emails which contained malicious links.[104]

S0650 QakBot

QakBot has spread through emails with malicious links.[105][106][107][108][109][110][111]

S1242 Qilin

Qilin has been delivered via malicious links in spearphishing emails.[112][113]

G1039 RedCurl

RedCurl has used phishing emails with malicious links to gain initial access.[114][115]

C0047 RedDelta Modified PlugX Infection Chain Operations

Mustang Panda distributed malicious links in phishing emails leading to HTML files that would direct the victim to malicious MSC files if running Windows based on User Agent fingerprinting during RedDelta Modified PlugX Infection Chain Operations.[116]

S1018 Saint Bot

Saint Bot has been distributed through malicious links contained within spearphishing emails.[99]

G0034 Sandworm Team

Sandworm Team has crafted phishing emails containing malicious hyperlinks.[117]

G0121 Sidewinder

Sidewinder has sent e-mails with malicious links often crafted for specific targets.[118][119]

S1086 Snip3

Snip3 has been delivered to victims through e-mail links to malicious files.[120]

S1124 SocGholish

SocGholish has been spread via emails containing malicious links.[91]

S0646 SpicyOmelette

SpicyOmelette has been distributed via emails containing a malicious link that appears to be a PDF document.[37]

S1030 Squirrelwaffle

Squirrelwaffle has been distributed through phishing emails containing a malicious URL.[121]

G1046 Storm-1811

Storm-1811 has distributed malicious links to victims that redirect to EvilProxy-based phishing sites to harvest credentials.[122]

G1018 TA2541

TA2541 has used spearphishing e-mails with malicious links to deliver malware. [123][120]

G0092 TA505

TA505 has sent spearphishing emails containing malicious links.[124][125][126][127]

G1037 TA577

TA577 has sent emails containing links to malicious JavaScript files.[68]

G0134 Transparent Tribe

Transparent Tribe has embedded links to malicious downloads in e-mails.[128][129]

S0266 TrickBot

TrickBot has been delivered via malicious links in phishing e-mails.[130]

G0010 Turla

Turla attempted to trick targets into clicking on a link featuring a seemingly legitimate domain from Adobe.com to download their malware and gain initial access.[131]

S0476 Valak

Valak has been delivered via malicious links in e-mail.[132]

G0112 Windshift

Windshift has sent spearphishing emails with links to harvest credentials and deliver malware.[133]

G0102 Wizard Spider

Wizard Spider has sent phishing emails containing a link to an actor-controlled Google Drive document or other free online file hosting services.[134][135]

G0128 ZIRCONIUM

ZIRCONIUM has used malicious links in e-mails to deliver malware.[136][137][138]
