Masquerading: Match Legitimate Name or Location, Sub-technique T1655.001 - Mobile

Archived: 2026-04-02 10:56:22 UTC

S0440 Agent Smith

Agent Smith can impersonate any popular application on an infected device, and the core malware disguises itself as a legitimate Google application. Agent Smith's dropper is a weaponized legitimate Feng Shui Bundle.[1]

S0525 Android/AdDisplay.Ashas

Android/AdDisplay.Ashas has mimicked Facebook and Google icons on the "Recent apps" screen to avoid discovery and uses the `com.google.xxx` package name to avoid detection.[2]

S1214 Android/SpyAgent

Android/SpyAgent has used the official icon of the Korean police application and the package name "kpo," which contain references related to the Korean police.[3]

S0524 AndroidOS/MalLocker.B

AndroidOS/MalLocker.B has masqueraded as popular apps, cracked games, and video players. [4]

S0292 AndroRAT

AndroRAT masquerades as legitimate applications.[5][6]

S0422 Anubis

Anubis has requested accessibility service privileges while masquerading as "Google Play Protect" and has disguised additional malicious application installs as legitimate system updates.[7][8]

G1028 APT-C-23

APT-C-23 has masqueraded malware as legitimate applications.[9][10][11]

S0540 Asacub

Asacub has masqueraded as a client of popular free ads services.[12]

S1079 BOULDSPY

BOULDSPY has been installed using the package name `com.android.callservice`, pretending to be an Android system service.[13]

G0097 Bouncing Golf

Bouncing Golf distributed malware as repackaged legitimate applications, with the malicious code in the `com.golf` package.[14]

S1094 BRATA

BRATA has masqueraded as legitimate WhatsApp updates and app security scanners.[15][16]

C0033 C0033

During C0033, PROMETHIUM used StrongPity on a compromised website to distribute a malicious version of a legitimate application.[17]

S0529 CarbonSteal

CarbonSteal has impersonated several apps, including official Google apps, chat apps, VPN apps, and popular games.[18]

S0480 Cerberus

Cerberus has pretended to be an Adobe Flash Player installer.[19]

S1083 Chameleon

Chameleon has disguised itself as legitimate applications, such as a cryptocurrency application called ‘CoinSpot,’ the IKO banking application in Poland, and an application used by the Australian Taxation Office (ATO). It has also used familiar icons, such as the Chrome and Bitcoin logos.[20][21]

S0555 CHEMISTGAMES

CHEMISTGAMES has masqueraded as popular South Korean applications.[22]

S1243 DCHSpy

DCHSpy has masqueraded as legitimate applications, such as VPN and banking applications.[23]

S0301 Dendroid

Dendroid can be bound to legitimate applications prior to installation on devices.[24]

S0550 DoubleAgent

DoubleAgent has been embedded into trojanized versions of applications such as Voxer, TalkBox, and Amaq News.[18]

S0320 DroidJack

DroidJack included code from the legitimate Pokemon GO app in order to appear identical to the user, but it also included additional malicious code.[25]

S0478 EventBot

EventBot has used icons from popular applications.[26]

S0522 Exobot

Exobot has used names like WhatsApp and Netflix.[27]

S1080 Fakecalls

Fakecalls has masqueraded as popular Korean banking apps.[28]

S0509 FakeSpy

FakeSpy masquerades as local postal service applications.[29]

S0577 FrozenCell

FrozenCell has masqueraded as fake updates to chat applications such as Facebook, WhatsApp, Messenger, LINE, and LoveChat, as well as apps targeting Middle Eastern demographics.[30]

S0423 Ginp

Ginp has masqueraded as "Adobe Flash Player" and "Google Play Verificator".[31]

S1231 GodFather

GodFather has imitated Google Play Protect, a security application pre-installed on all Android devices, and its functionalities, such as scanning the device and requesting for the accessibility service.[32]

S0551 GoldenEagle

GoldenEagle has inserted trojan functionality into legitimate apps, including popular apps within the Uyghur community, VPNs, instant messaging apps, social networking, games, adult media, and Google searching.[18]

S0536 GPlayed

GPlayed has used the Play Store icon as well as the name "Google Play Marketplace".[33]

S0544 HenBox

HenBox has masqueraded as VPN and Android system apps.[34]

S1077 Hornbill

Hornbill has impersonated chat applications such as Fruit Chat, Cucu Chat, and Kako Chat.[35]

S0485 Mandrake

Mandrake can mimic an app called "Storage Settings" if it cannot hide its icon.[36]

G1019 MoustachedBouncer

MoustachedBouncer has used legitimate looking filenames for malicious executables including MicrosoftUpdate845255.exe.[37]

S1126 Phenakite

Phenakite can masquerade as the chat application "Magic Smile."[38]

S0539 Red Alert 2.0

Red Alert 2.0 has masqueraded as legitimate media player, social media, and VPN applications.[39]

S0549 SilkBean

SilkBean has been incorporated into trojanized applications, including Uyghur/Arabic focused keyboards, alphabets, and plugins, as well as official-looking Google applications.[18]

S0419 SimBad

SimBad was embedded into legitimate applications.[40]

S1195 SpyC23

SpyC23 has masqueraded as legitimate messaging applications.[9][10][11][41][42][43]

S0558 Tiktok Pro

Tiktok Pro has masqueraded as TikTok.[44]

S0418 ViceLeaker

ViceLeaker was embedded into legitimate applications using Smali injection.[45]

S0506 ViperRAT

ViperRAT's second stage has masqueraded as "System Updates", "Viber Update", and "WhatsApp Update".[46]

S0489 WolfRAT

WolfRAT has masqueraded as "Google service", "GooglePlay", and "Flash update".[47]

S0314 X-Agent for Android

X-Agent for Android was placed in a repackaged version of an application used by Ukrainian artillery forces.[48]

S0318 XLoader for Android

XLoader for Android has masqueraded as an Android security application.[49]
