Download New Code at Runtime, Technique T1407 - Mobile

Archived: 2026-04-05 13:29:50 UTC

S1061 AbstractEmu

AbstractEmu can download and install additional malware after initial infection.[2]

S0422 Anubis

Anubis can download attacker-specified APK files.[3]

S1079 BOULDSPY

BOULDSPY can download and run code obtained from the C2.[4]

S0293 BrainTest

Original samples of BrainTest download their exploit packs for rooting from a remote server after installation.[5]

S1094 BRATA

BRATA has used an initial dropper to download an additional malicious application, and downloads its configuration file from the C2 server.[6][7]

S0432 Bread

Bread has utilized JavaScript within WebViews that loaded a URL hosted on a Bread-controlled server which provided functions to run. Bread downloads billing fraud execution steps at runtime.[8]

S0655 BusyGasper

BusyGasper can download a payload or updates from either its C2 server or email attachments in the adversary's inbox.[9]

S0529 CarbonSteal

CarbonSteal can dynamically load additional functionality.[10]

S0480 Cerberus

Cerberus can update the malicious payload module on command.[11]

S1083 Chameleon

Chameleon has the ability to download new code at runtime.[12]

S0555 CHEMISTGAMES

CHEMISTGAMES can download new modules while running.[13]

S0505 Desert Scorpion

Desert Scorpion has been distributed in multiple stages.[14]

S0550 DoubleAgent

DoubleAgent has downloaded additional code to root devices, such as TowelRoot.[10]

S0420 Dvmap

Dvmap can download code and binaries from the C2 server to execute on the device as root.[15]

S0507 eSurv

eSurv's Android version is distributed in three stages: the dropper, the second stage payload, and the third stage payload which is Exodus.[16]

S0478 EventBot

EventBot can download new libraries when instructed to.[17]

S0405 Exodus

Exodus One, after checking in, sends a POST request and then downloads Exodus Two, the second stage binaries.[18]

S0577 FrozenCell

FrozenCell has downloaded and installed additional applications.[19]

S0535 Golden Cup

Golden Cup has been distributed in two stages.[20]

S0551 GoldenEagle

GoldenEagle can download new code to update itself.[10]

S0536 GPlayed

GPlayed has the capability to remotely load plugins and download and compile new .NET code.[21]

S0544 HenBox

HenBox can load additional Dalvik code while running.[22]

S0325 Judy

Judy bypasses Google Play's protections by downloading a malicious payload at runtime after installation.[23]

S0485 Mandrake

Mandrake can download its second (Loader) and third (Core) stages after the dropper is installed.[24]

S1241 RatMilad

RatMilad has used a fake application to request permissions and to download itself.[25]

S0295 RCSAndroid

RCSAndroid has the ability to dynamically download and execute new code at runtime.[26]

S0539 Red Alert 2.0

Red Alert 2.0 can download additional overlay templates.[27]

S1055 SharkBot

SharkBot can use the Android "Direct Reply" feature to spread the malware to other devices. It can also download the full version of the malware after initial device compromise.[28]

S0549 SilkBean

SilkBean can install new applications which are obtained from the C2 server.[10]

S0327 Skygofree

Skygofree can download executable code from the C2 server after the implant starts or after a specific command.[29]

S0324 SpyDealer

SpyDealer downloads and executes root exploits from a remote server.[30]

S0545 TERRACOTTA

TERRACOTTA can download additional modules at runtime via JavaScript `eval` statements.[31]

S0424 Triada

Triada utilizes a backdoor in a Play Store app to install additional trojanized apps from the Command and Control server.[32]

S0506 ViperRAT

ViperRAT has been installed in two stages and can secretly install new applications.[33]

G0112 Windshift

Windshift has included malware functionality capable of downloading new DEX files at runtime during Operation BULL.[34]

S0489 WolfRAT

WolfRAT can update the running malware.[35]

S0311 YiSpecter

YiSpecter has used private APIs to download and install other pieces of itself, as well as other malicious apps. [36]

S0494 Zen

Zen can dynamically load executable code from remote sources.[37]

S0287 ZergHelper

ZergHelper attempts to extend its capabilities via dynamic updating of its code.[38]
