Data from Local System, Technique T1533 - Mobile

Archived: 2026-04-05 17:35:06 UTC

S1061 AbstractEmu

AbstractEmu can collect files from or inspect the device's filesystem.[1]

S1095 AhRat

AhRat can find and exfiltrate files with certain extensions, such as .jpg, .mp4, .html, .docx, and .pdf.[2]

S0422 Anubis

Anubis can exfiltrate files encrypted with the ransomware module from the device and can modify external storage.[3][4]

S1215 Binary Validator

Binary Validator has searched for and has deleted the malicious iMessage attachment used in the initial access phase in various databases.[5]

S1079 BOULDSPY

BOULDSPY can access browser history and bookmarks, and can list all files and folders on the device.[6]

S1094 BRATA

BRATA has collected account information from compromised devices.[7]

S0655 BusyGasper

BusyGasper can collect images stored on the device and browser history.[8]

S1083 Chameleon

Chameleon has gathered cookies and device logs.[9][10]

S0555 CHEMISTGAMES

CHEMISTGAMES can collect files from the filesystem and account information from Google Chrome.[11]

S0426 Concipit1248

Concipit1248 can collect device photos.[12]

S0425 Corona Updates

Corona Updates can collect voice notes, device accounts, and gallery images.[12]

S1243 DCHSpy

DCHSpy has collected files of interest on the device, including WhatsApp files.[13]

S0301 Dendroid

Dendroid can collect the device's photos, browser history, bookmarks, and accounts stored on the device.[14]

S0505 Desert Scorpion

Desert Scorpion can collect attacker-specified files, including files located on external storage.[15]

S0550 DoubleAgent

DoubleAgent has collected files from the infected device.[16]

S1054 Drinik

Drinik can request the `READ_EXTERNAL_STORAGE` and `WRITE_EXTERNAL_STORAGE` Android permissions.[17]

S1092 Escobar

Escobar can collect sensitive information, such as Google Authenticator codes.[18]

S0507 eSurv

eSurv can exfiltrate device pictures.[19]

S0405 Exodus

Exodus Two can extract information on pictures from the Gallery, Chrome and SBrowser bookmarks, and the connected WiFi network's password.[20]

S1080 Fakecalls

Fakecalls can access and exfiltrate files, such as photos or video.[21]

S0408 FlexiSpy

FlexiSpy can monitor device photos and can also access browser history and bookmarks.[22]

S0577 FrozenCell

FrozenCell has retrieved device images for exfiltration.[23]

S0423 Ginp

Ginp can download device logs.[24]

S0535 Golden Cup

Golden Cup can collect images, videos, and attacker-specified files.[25]

S0551 GoldenEagle

GoldenEagle has retrieved .doc, .txt, .gif, .apk, .jpg, .png, .mp3, and .db files from external storage.[16]

S0421 GolfSpy

GolfSpy can collect local accounts on the device, pictures, bookmarks/histories of the default browser, and files stored on the SD card. GolfSpy can list image, audio, video, and other files stored on the device. GolfSpy can copy arbitrary files from the device.[26]

S0290 Gooligan

Gooligan steals authentication tokens that can be used to access data from multiple Google applications.[27]

S0536 GPlayed

GPlayed can collect the user's browser cookies.[28]

S0406 Gustuff

Gustuff can capture files and photos from the compromised device.[29]

S0544 HenBox

HenBox can steal data from various sources, including chat, communication, and social media apps.[30]

S1077 Hornbill

Hornbill can access images stored on external storage.[31]

S0463 INSOMNIA

INSOMNIA can collect application database files, including Gmail, Hangouts, device photos, and container directories of third-party apps.[32]

S1185 LightSpy

LightSpy has collected and exfiltrated files from messaging applications, such as Telegram, QQ, WeChat, and Whatsapp, and browser history from Chrome and Safari.[33][34][35][36][37]

S0407 Monokle

Monokle can retrieve the salt used when storing the user's password, aiding an adversary in computing the user's plaintext password/PIN from the stored password hash. Monokle can also capture the user's dictionary, user-defined shortcuts, and browser history, enabling profiling of the user and their activities.[38]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors used Android backdoors capable of exfiltrating specific files directly from the infected devices.[39]

C0054 Operation Triangulation

During Operation Triangulation, the threat actors stole data from SQLite databases.[5]

S1126 Phenakite

Phenakite can collect and exfiltrate WhatsApp media, photos and files with specific extensions, such as .pdf and .doc.[40]

S1241 RatMilad

RatMilad has listed files and pictures on the device starting from `/mnt/sdcard/`.[41]

S0295 RCSAndroid

RCSAndroid can collect passwords for Wi-Fi networks and online accounts, including Skype, Facebook, Twitter, Google, WhatsApp, Mail, and LinkedIn.[42]

S0549 SilkBean

SilkBean can retrieve files from external storage and can collect browser data.[16]

S1195 SpyC23

SpyC23 can collect and exfiltrate files with specific extensions, such as .pdf, doc.[43]

S0305 SpyNote RAT

SpyNote RAT can copy files from the device to the C2 server.[44]

S0328 Stealth Mango

Stealth Mango collected and exfiltrated data from the device, including sensitive letters/documents, stored photos, and stored audio files.[45]

S1082 Sunbird

Sunbird can access images stored on external storage.[31]

S0329 Tangelo

Tangelo accesses browser history, pictures, and videos.[45]

S1069 TangleBot

TangleBot can request permission to view files and media.[46]

S0558 Tiktok Pro

Tiktok Pro can collect device photos and credentials from other applications.[47]

S1216 TriangleDB

TriangleDB has collected and exfiltrated files.[48]

S0427 TrickMo

TrickMo can steal pictures from the device.[49]

S0418 ViceLeaker

ViceLeaker can copy arbitrary files from the device to the C2 server, can exfiltrate browsing history, can exfiltrate the SD card structure, and can exfiltrate pictures as the user takes them.[50][51]

S0506 ViperRAT

ViperRAT can collect device photos, PDF documents, Office documents, browser history, and browser bookmarks.[52]

G0112 Windshift

Windshift has exfiltrated local account data and calendar information as part of Operation ROCK.[53]

S0489 WolfRAT

WolfRAT can collect user account, photos, browser history, and arbitrary files.[54]
