# Exfiltration Over C2 Channel, Technique T1646 - Mobile

Archived: 2026-04-05 16:49:02 UTC

S1061 AbstractEmu

AbstractEmu can send large amounts of device data over its C2 channel, including the device's manufacturer, model, version and serial number, telephone number, and IP address.[1]

S1095 AhRat

AhRat can exfiltrate collected data to the C2, such as audio recordings and files.[2]

S1215 Binary Validator

Binary Validator has exfiltrated collected data to the C2 server.[3]

S1079 BOULDSPY

BOULDSPY has exfiltrated cached data from infected devices.[4]

S1094 BRATA

BRATA has exfiltrated data to the C2 server using HTTP requests.[5]

C0033 C0033

During C0033, PROMETHIUM used StrongPity to exfiltrate to the C2 server using HTTPS.[6][7]

S1083 Chameleon

Chameleon has sent stolen data over HTTP.[8]

S1225 CherryBlos

CherryBlos has exfiltrated credentials collected from pictures that have been analyzed using optical character recognition (OCR).[9]

S1054 Drinik

Drinik can send stolen data back to the C2 server.[10]

S0507 eSurv

eSurv has exfiltrated data using HTTP PUT requests.[11]

S1080 Fakecalls

Fakecalls can send exfiltrated data back to the C2 server.[12]

S1067 FluBot

FluBot can send contact lists to its C2 server.[13]

S1093 FlyTrap

FlyTrap can use HTTP to exfiltrate data to the C2 server.[14]

S1231 GodFather

GodFather has exfiltrated sensitive information over C2.[15][16]

S0551 GoldenEagle

GoldenEagle has exfiltrated data via both SMTP and HTTP.[17]

S0421 GolfSpy

GolfSpy exfiltrates data using HTTP POST requests.[18]

S1077 Hornbill

Hornbill can exfiltrate data back to the C2 server using HTTP.[19]

S1185 LightSpy

LightSpy has exfiltrated collected data to the C2.[20]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors used Android backdoors that would send information and data from a victim's mobile device to the C2 servers.[21]

S0399 Pallas

Pallas exfiltrates data using HTTP.[22]

S1241 RatMilad

RatMilad has exfiltrated collected data to the C2.[23]

S0326 RedDrop

RedDrop uses standard HTTP for exfiltration.[24]

S1055 SharkBot

SharkBot can exfiltrate captured user credentials and event logs back to the C2 server. [25]

S1082 Sunbird

Sunbird can exfiltrate compressed ZIP files containing gathered info to C2 infrastructure.[19]

S0424 Triada

Triada utilized HTTP to exfiltrate data through POST requests to the command and control server.[26]

S0418 ViceLeaker

ViceLeaker uses HTTP data exfiltration.[27][28]

S0490 XLoader for iOS

XLoader for iOS has exfiltrated data using HTTP requests.[29]

---