

DoubleAgent, Software S0550 | MITRE ATT&CK®

Archived: 2026-04-02 11:05:23 UTC

Mobile [T1437 Application Layer Protocol](#)

[DoubleAgent](#) has used both FTP and TCP sockets for data exfiltration. ^[1]

Mobile [T1429 Audio Capture](#)

[DoubleAgent](#) has captured audio and can record phone calls. ^[1]

Mobile [T1623 .001 Command and Scripting Interpreter: Unix Shell](#)

[DoubleAgent](#) can run arbitrary shell commands. ^[1]

Mobile [T1645 Compromise Client Software Binary](#)

[DoubleAgent](#) has used exploits to root devices and install additional malware on the system partition. ^[1]

Mobile [T1533 Data from Local System](#)

[DoubleAgent](#) has collected files from the infected device. ^[1]

Mobile [T1407 Download New Code at Runtime](#)

[DoubleAgent](#) has downloaded additional code to root devices, such as TowelRoot. ^[1]

Mobile [T1404 Exploitation for Privilege Escalation](#)

[DoubleAgent](#) has used exploit tools to gain root, such as TowelRoot. ^[1]

Mobile [T1420 File and Directory Discovery](#)

[DoubleAgent](#) has searched for specific existing data directories, including the Gmail app, Dropbox app, Pictures, and thumbnails. ^[1]

Mobile [T1628 .001 Hide Artifacts: Suppress Application Icon](#)

[DoubleAgent](#) has hidden its app icon. ^[1]

Mobile [T1630 .002 Indicator Removal on Host: File Deletion](#)

[DoubleAgent](#) has deleted or renamed specific files. ^[1]

Mobile [T1655 .001 Masquerading: Match Legitimate Name or Location](#)

[DoubleAgent](#) has been embedded into trojanized versions of applications such as Voxer, TalkBox, and Amaq News.^[1]

Mobile [T1406 Obfuscated Files or Information](#)

[DoubleAgent](#) has used an AES encrypted file in the assets folder with an unsuspecting name (e.g. 'GoogleMusic.png') for holding configuration and C2 information.^[1]

Mobile [T1636 .002 Protected User Data: Call Log](#)

[DoubleAgent](#) has accessed the call logs.^[1]

[.003 Protected User Data: Contact List](#)

[DoubleAgent](#) has accessed the contact list.^[1]

[.004 Protected User Data: SMS Messages](#)

[DoubleAgent](#) has captured SMS and MMS messages.^[1]

Mobile [T1418 Software Discovery](#)

[DoubleAgent](#) has accessed the list of installed apps.^[1]

Mobile [T1409 Stored Application Data](#)

[DoubleAgent](#) has accessed browser history, as well as the files for 15 other apps.^[1]

Mobile [T1426 System Information Discovery](#)

[DoubleAgent](#) has accessed common system information.^[1]

Source: <https://attack.mitre.org/software/S0550/>