Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:33:15 UTC

Tool: MobileOrder

Names	MobileOrder
Category	Malware
Type	Backdoor, Info stealer, Exfiltration, Downloader
Description	(Palo Alto) The malware uses the AMAP SDK to get accurate location of infected devices by GPS, mobile network (such as base stations), WiFi and other information. MobileOrder acts on instructions provided by its C2 server, which it communicates with over TCP port 3728. All C2 communications are encrypted with the AES algorithm using a key generated by computing five MD5 hashes starting with the key “1qazxcvbnm”, and adding a salt value of “.)1/” in each iteration. The C2 server will respond to requests from MobileOrder with commands that the Trojan refers to as “orders”. MobileOrder contains a command handler with functionality that provides a fairly robust set of commands, as seen in Table 6. The first byte of data provided by the C2 server is order number, which is followed by the encrypted data that needed to carry out the specific order.
Information	<https://unit42.paloaltonetworks.com/scarlet-mimic-years-long-espionage-targets-minority-activists/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0079/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.mobile_order>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:MobileOrder>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool MobileOrder

Changed	Name	Country	Observed

APT groups

	Scarlet Mimic		2015-Aug 2022	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e1aa1dd5-eaa8-4bb6-91be-ba0d350827bc