MESSAGETAP, Software S0443 | MITRE ATT&CK®

Archived: 2026-04-05 18:14:35 UTC

Domain	ID		Name	Use
Enterprise	T1560	.003	Archive Collected Data: Archive via Custom Method	MESSAGETAP has XOR-encrypted and stored contents of SMS messages that matched its target list. [1]
Enterprise	T1119		Automated Collection	MESSAGETAP checks two files, keyword_parm.txt and parm.txt, for instructions on how to target and save data parsed and extracted from SMS message data from the network traffic. If an SMS message contained either a phone number, IMSI number, or keyword that matched the predefined list, it is saved to a CSV file for later theft by the threat actor.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	MESSAGETAP stored targeted SMS messages that matched its target list in CSV files on the compromised system.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	After checking for the existence of two files, keyword_parm.txt and parm.txt, MESSAGETAP XOR decodes and read the contents of the files. [1]
Enterprise	T1083		File and Directory Discovery	MESSAGETAP checks for the existence of two configuration files (keyword_parm.txt and parm.txt) and attempts to read the files every 30 seconds.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Once loaded into memory, MESSAGETAP deletes the keyword_parm.txt and parm.txt configuration files from disk. [1]

Domain	ID	Name	Use
Enterprise	T1040	Network Sniffing	MESSAGETAP uses the libpcap library to listen to all traffic and parses network protocols starting with Ethernet and IP layers. It continues parsing protocol layers including SCTP, SCCP, and TCAP and finally extracts SMS message data and routing metadata. [1]
Enterprise	T1049	System Network Connections Discovery	After loading the keyword and phone data files, MESSAGETAP begins monitoring all network connections to and from the victim server. [1]

Source: https://attack.mitre.org/software/S0443