Threat Group Cards: A Threat Actor Encyclopedia

Tool: TabMsgSQL

Names	TabMsgSQL LETSGO
Category	Malware
Type	Backdoor, Exfiltration
Description	This malware family is a full-featured backdoor capable of file uploading and downloading, arbitrary execution of programs, and providing a remote interactive command shell. All communications with the C2 server are sent over HTTP to a static URL, appending various URL parameters to the request. Some variants use a slightly different URL.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.tabmsgsql>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool TabMsgSQL

Changed	Name	Country	Observed	
APT groups				
	Comment Crew, APT 1		2006-May 2018	

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