Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:40:17 UTC

Tool: bangat

Names	bangat
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	The BANGAT malware family shares a large amount of functionality with the Auriga backdoor. The malware family contains functionality for keylogging, creating and killing processes, performing filesystem and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. In addition, the malware also implements a custom VNC like protocol which sends screenshots of the desktop to the C2 server and accepts keyboard and mouse input. The malware communicates to its C2 servers using SSL, with self signed SSL certificates. The malware family will create a copy of cmd.exe to perform its C2 activity, and replace the 'Microsoft corp' strings in the cmd.exe binary with different values. The malware family typically maintains persistence through installing itself as a service.
Information	<https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> <http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.bangat>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool bangat

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

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