Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:57:45 UTC

Tool: Auriga

Names	Auriga Riodrv
Category	Malware
Type	Backdoor, Keylogger
Description	The AURIGA malware family shares a large amount of functionality with the bangat backdoor. The malware family contains functionality for keystroke logging, creating and killing processes, performing file system and registry modifications, spawning interactive command shells, performing process injection, logging off the current user or shutting down the local machine. The AURIGA malware contains a driver component which is used to inject the malware DLL into other processes. This driver can also perform process and IP connection hiding. 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.auriga>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Auriga

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

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