Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:37:58 UTC

Tool: Helauto

Names	Helauto
Category	Malware
Type	Backdoor, Exfiltration
Description	This family of malware is designed to operate as a service and provides remote command execution and file transfer capabilities to a fixed IP address or domain name. All communication with the C2 server happens over port 443 using SSL. This family can be installed as a service DLL. Some variants allow for uninstallation.
Information	<http://contagiodump.blogspot.lu/2013/03/mandiant-apt1-samples-categorized-by.html> <http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.helauto>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Helauto

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

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