Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:33:09 UTC

Tool: GREENCAT

Names	GREENCAT
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	Members of this family are full featured backdoors that communicates with a Web-based Command & Control (C2) server over SSL. Features include interactive shell, gathering system info, uploading and downloading files, and creating and killing processes, Malware in this family usually communicates with a hard-coded domain using SSL on port 443. Some members of this family rely on launchers to establish persistence mechanism for them. Others contains functionality that allows it to install itself, replacing an existing Windows service, and uninstall itself. Several variants use %SystemRoot%\Tasks or %WinDir%\Tasks as working directories, additional malware artifacts may be found there.
Information	<http://contagiodump.blogspot.com/2013/03/mandiant-apt1-samples-categorized-by.html>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool GREENCAT

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

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