Fire Chili - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:50:31 UTC

Tool: Fire Chili

Names	Fire Chili
Category	Malware
Type	Rootkit
Description	(BleepingComputer) In a recent Deep Panda campaign discovered by Fortinet, the hacking group is deploying the new 'Fire Chili' rootkit to evade detection on compromised systems. A rootkit is malware typically installed as a driver that hooks various Windows APIs to hide the presence of other files and configuration settings in the operating system. For example, by hooking Windows programming functions, a rootkit can filter data to not display malicious file names, processes, and Registry keys APIs to Windows programs requesting the data. In the attacks, the rootkit is signed by valid digital certificates allowing it to bypass detection by security software and load into Windows without any warnings.
Information	<https://www.bleepingcomputer.com/news/security/chinese-hacking-group-uses-new-fire-chili-windows-rootkit/> <https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.firechili>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool Fire Chili

Changed	Name	Country	Observed	
APT groups				
	APT 19, Deep Panda, C0d0so0		2013-Mar 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b2a4a72c-91cf-4a8e-be0e-ae24de1e080c