Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:48:42 UTC

Tool: Sepulcher

Names	Sepulcher
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration
Description	(Proofpoint) Sepulcher malware has seven work modes that include conducting reconnaissance on an infected host, spawning a reverse command shell, reading from file, and writing to file. More granularly, additional commands exist within the intelligence gathering/reconnaissance work modes (1002, 1003, 1004) which carry out reconnaissance functionality within the infected host. These commands include obtaining information about the drives, file information, directory statistics, directory paths, directory content, running processes, and services. Additionally, it is capable of more active functionalities like deleting directories and files, creating directories, moving file source to destination, spawning a shell to execute commands, terminating a process, restarting a service, changing a service start type, and deleting a service.
Information	<https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic> <https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sepulcher>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:sepulcher>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Sepulcher

Changed	Name	Country	Observed

APT groups

	TA413		2019-2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0c4b65ac-4631-443d-8091-e5197e57575f