Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:28:06 UTC

Tool: Ramsay

Names	Ramsay
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration, Worm
Description	(ESET) ESET researchers have discovered a previously unreported cyber-espionage framework that we named Ramsay and that is tailored for collection and exfiltration of sensitive documents and is capable of operating within air-apped networks. Ramsay’s architecture provides a series of capabilities monitored via a logging mechanism intended to assist operators by supplying a feed of actionable intelligence to conduct exfiltration, control, and lateral movement actions, as well as providing overall behavioral and system statistics of each compromised system. The realization of these actions is possible due to the following capabilities: • File collection and covert storage • Command execution • Spreading
Information	<https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/> <https://www.antiy.cn/research/notice&report/research_report/20200522.html> <https://blog.bushidotoken.net/2020/06/deep-dive-darkhotel-apt.html> <https://www.sentinelone.com/blog/why-on-device-detection-matters-new-ramsay-trojan-targets-air-gapped-networks/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0458/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ramsay>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Ramsay

Changed	Name	Country	Observed	
APT groups				
	DarkHotel		2007-2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=31f37051-bd42-48ce-bfaf-3dcef73fc18f