Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:11:12 UTC

Tool: Remsec

Names	Remsec Backdoor.Remsec ProjectSauron
Category	Malware
Type	Backdoor, Info stealer, Exfiltration, Tunneling
Description	(Kaspersky) Remsec is particularly interested in gaining access to encrypted communications, hunting them down using an advanced modular cyber-espionage platform that incorporates a set of unique tools and techniques. The most noteworthy feature of Remsec's tactics is the deliberate avoidance of patterns: Remsec customizes its implants and infrastructure for each individual target, and never reuses them. This approach, coupled with multiple routes for the exfiltration of stolen data, such as legitimate email channels and DNS, enables Remsec to conduct secretive, long-term spying campaigns in target networks. Remsec gives the impression of being an experienced and traditional actor that has put considerable effort into learning from other extremely advanced actors, including Duqu, Flame, Equation and Regin; adopting some of their most innovative techniques and improving on their tactics in order to remain undiscovered.
Information	<https://www.kaspersky.com/about/press-releases/2016_remsec-top-level-espionage-platform-covertly-extracts-encrypted-government-comms>
MITRE ATT&CK	<https://attack.mitre.org/software/S0125/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.remsec_strider>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:remsec>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Remsec

Changed	Name	Country	Observed	
APT groups				
	Strider, ProjectSauron		2011	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=3f13e218-95a3-47bd-935f-0e195bdb1779