Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:52:47 UTC

Tool: Remexi

Names	Remexi CACHEMONEY
Category	Malware
Type	Backdoor, Keylogger, Info stealer
Description	(Kaspersky) Remexi boasts features that allow it to gather keystrokes, take screenshots of windows of interest (as defined in its configuration), steal credentials, logons and the browser history, and execute remote commands. Encryption consists of XOR with a hardcoded key for its configuration and RC4 with a predefined password for encrypting the victim's data. Remexi includes different modules that it deploys in its working directory, including configuration decryption and parsing, launching victim activity logging in a separate module, and seven threads for various espionage and auxiliary functions. The Remexi developers seem to rely on legitimate Microsoft utilities.
Information	<https://securelist.com/chafer-used-remexi-malware/89538/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0375/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.remexi>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool Remexi

Changed	Name	Country	Observed
APT groups			

	Chafer, APT 39		2014-Sep 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=26363b6b-e756-4ba3-93ab-2513e5352143