Remexi, Software S0375 | MITRE ATT&CK®

Archived: 2026-04-05 14:28:05 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Remexi uses BITSAdmin to communicate with the C2 server over HTTP.[1]
Enterprise	T1010		Application Window Discovery	Remexi has a command to capture active windows on the machine and retrieve window titles.[1]
Enterprise	T1560		Archive Collected Data	Remexi encrypts and adds all gathered browser data into files for upload to C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Remexi utilizes Run Registry keys in the HKLM hive as a persistence mechanism.[1]
		.004	Boot or Logon Autostart Execution: Winlogon Helper DLL	Remexi achieves persistence using Userinit by adding the Registry key `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit`.[1]
Enterprise	T1115		Clipboard Data	Remexi collects text from the clipboard.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Remexi silently executes received commands with cmd.exe.[1]
		.005	Command and Scripting Interpreter: Visual Basic	Remexi uses AutoIt and VBS scripts throughout its execution process.[1]

Domain	ID		Name	Use
Enterprise	T1140		Deobfuscate/Decode Files or Information	Remexi decrypts the configuration data using XOR with 25-character keys.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Remexi performs exfiltration over BITSAdmin, which is also used for the C2 channel.[1]
Enterprise	T1083		File and Directory Discovery	Remexi searches for files on the system. [1]
Enterprise	T1056	.001	Input Capture: Keylogging	Remexi gathers and exfiltrates keystrokes from the machine.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Remexi obfuscates its configuration data with XOR.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Remexi utilizes scheduled tasks as a persistence mechanism.[1]
Enterprise	T1113		Screen Capture	Remexi takes screenshots of windows of interest. [1]
Enterprise	T1047		Windows Management Instrumentation	Remexi executes received commands with wmic.exe (for WMI commands). [1]

Source: https://attack.mitre.org/software/S0375