Melcoz, Software S0530 | MITRE ATT&CK®

Archived: 2026-04-02 10:38:04 UTC

Domain	ID		Name	Use
Enterprise	T1185		Browser Session Hijacking	Melcoz can monitor the victim's browser for online banking sessions and display an overlay window to manipulate the session in the background.[1]
Enterprise	T1115		Clipboard Data	Melcoz can monitor content saved to the clipboard.[1]
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	Melcoz can use VBS scripts to execute malicious DLLs.[1]
		.010	Command and Scripting Interpreter: AutoHotKey & AutoIT	Melcoz has been distributed through an AutoIt loader script.[1]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Melcoz has the ability to steal credentials from web browsers.[1]
Enterprise	T1565	.002	Data Manipulation: Transmitted Data Manipulation	Melcoz can monitor the clipboard for cryptocurrency addresses and change the intended address to one controlled by the adversary.[1]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Melcoz can use DLL hijacking to bypass security controls.[1]
Enterprise	T1105		Ingress Tool Transfer	Melcoz has the ability to download additional files to a compromised host.[1]

Domain	ID		Name	Use
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	Melcoz has been packed with VMProtect and Themida.[1]
Enterprise	T1566	.002	Phishing: Spearphishing Link	Melcoz has been spread through malicious links embedded in e-mails.[1]
Enterprise	T1218	.007	System Binary Proxy Execution: Msiexec	Melcoz can use MSI files with embedded VBScript for execution.[1]
Enterprise	T1204	.001	User Execution: Malicious Link	Melcoz has gained execution through victims opening malicious links.[1]
