Hancitor, Software S0499 | MITRE ATT&CK®

Archived: 2026-04-05 15:29:17 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Hancitor has added Registry Run keys to establish persistence.[2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Hancitor has used PowerShell to execute commands.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Hancitor has decoded Base64 encoded URLs to insert a recipient's name into the filename of the Word document. Hancitor has also extracted executables from ZIP files.[1][2]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Hancitor has deleted files using the VBA `kill` function.[2]
Enterprise	T1105		Ingress Tool Transfer	Hancitor has the ability to download additional files from C2.[1]
Enterprise	T1106		Native API	Hancitor has used `CallWindowProc` and `EnumResourceTypesA` to interpret and execute shellcode.[2]
Enterprise	T1027		Obfuscated Files or Information	Hancitor has used Base64 to encode malicious links.[1]
		.015	Compression	Hancitor has delivered compressed payloads in ZIP files to victims.[2]

Domain	ID		Name	Use
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Hancitor has been delivered via phishing emails with malicious attachments.[2]
		.002	Phishing: Spearphishing Link	Hancitor has been delivered via phishing emails which contained malicious links.[1]
Enterprise	T1218	.012	System Binary Proxy Execution: Verclsid	Hancitor has used verclsid.exe to download and execute a malicious script.[3]
Enterprise	T1204	.001	User Execution: Malicious Link	Hancitor has relied upon users clicking on a malicious link delivered through phishing.[1]
		.002	User Execution: Malicious File	Hancitor has used malicious Microsoft Word documents, sent via email, which prompted the victim to enable macros.[2]
Enterprise	T1497		Virtualization/Sandbox Evasion	Hancitor has used a macro to check that an ActiveDocument shape object in the lure message is present. If this object is not found, the macro will exit without downloading additional payloads.[2]

Source: https://attack.mitre.org/software/S0499