Mori, Software S1047 | MITRE ATT&CK®

Archived: 2026-04-05 16:36:55 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Mori can communicate using HTTP over IPv4 or IPv6 depending on a flag set.[1]
		.004	Application Layer Protocol: DNS	Mori can use DNS tunneling to communicate with C2.[1][2]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Mori can use Base64 encoded JSON libraries used in C2.[1]
Enterprise	T1001	.001	Data Obfuscation: Junk Data	Mori has obfuscated the FML.dll with 200MB of junk data.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Mori can resolve networking APIs from strings that are ADD-encrypted.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Mori can delete its DLL file and related files by Registry value.[1]
Enterprise	T1112		Modify Registry	Mori can write data to `HKLM\Software\NFC\IPA` and `HKLM\Software\NFC\` and delete Registry values.[1][2]
Enterprise	T1012		Query Registry	Mori can read data from the Registry including from `HKLM\Software\NFC\IPA` and `HKLM\Software\NFC\`.[1]

Domain	ID		Name	Use
Enterprise	T1218	.010	System Binary Proxy Execution: Regsvr32	Mori can use `regsvr32.exe` for DLL execution.[1]

Source: https://attack.mitre.org/software/S1047