Mango, Software S1169 | MITRE ATT&CK®

Archived: 2026-04-05 16:29:15 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Mango can retrieve C2 commands sent in HTTP responses.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Mango can receive Base64-encoded commands from C2.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Mango can receive XOR-encrypted commands from C2.[1]
		.002	Encrypted Channel: Asymmetric Cryptography	Mango can use TLS to encrypt C2 communications.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Mango can use its HTTP C2 channel for exfiltration.[1]
Enterprise	T1083		File and Directory Discovery	Mango can enumerate the contents of current working or other specified direct [1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Mango contains an unused capability to block endpoint security solutions from loading user-mode code hooks via a DLL in a specified process by using the `UpdateProcThreadAttribute API` to set the `PROC_THREAD_ATTRIBUTE_MITIGATION_POLICY` to `PROCESS_CREATION_MITIGATION_POLICY_BLOCK_NON_MICROSOFT_BINARIES_ALWAY` for an identified process. [1]
Enterprise	T1106		Native API	Mango has the ability to use Native APIs.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Mango contains a series of base64 encoded substrings.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Mango can create a scheduled task to run every 32 seconds to communicate wi C2 and execute received commands.[1]

Domain	ID		Name	Use
Enterprise	T1082		System Information Discovery	Mango can collect the machine name of a compromised system which is later u as part of a unique victim identifier.[1]
Enterprise	T1033		System Owner/User Discovery	Mango can collect the user name from a compromised system which is used to create a unique victim identifier.[1]
Enterprise	T1204	.002	User Execution: Malicious File	Mango has been executed through a Microsoft Word document with a maliciou macro.[1]

Source: https://attack.mitre.org/software/S1169