Samurai, Software S1099 | MITRE ATT&CK®

Archived: 2026-04-05 15:35:04 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Samurai can use a .NET HTTPListener class to receive and handle HTTP POST requests.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Samurai can use a remote command module for execution via the Windows command line.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Samurai can create a service at `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost` to trigger execution and maintain persistence.[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Samurai can base64 encode data sent in C2 communications prior to its encryption.[1]
Enterprise	T1005		Data from Local System	Samurai can leverage an exfiltration module to download arbitrary files from compromised machines.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Samurai can encrypt C2 communications with AES.[1]
Enterprise	T1083		File and Directory Discovery	Samurai can use a specific module for file enumeration.[1]

Domain	ID		Name	Use
Enterprise	T1105		Ingress Tool Transfer	Samurai has been used to deploy other malware including Ninja.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Samurai has created the directory `%COMMONPROGRAMFILES%\Microsoft Shared\wmi\` to contain DLLs for loading successive stages.[1]
Enterprise	T1112		Modify Registry	The Samurai loader component can create multiple Registry keys to force the svchost.exe process to load the final backdoor.[1]
Enterprise	T1106		Native API	Samurai has the ability to call Windows APIs.[1]
Enterprise	T1095		Non-Application Layer Protocol	Samurai can use a proxy module to forward TCP packets to external hosts.[1]
Enterprise	T1027		Obfuscated Files or Information	Samurai can encrypt the names of requested APIs.[1]
		.004	Compile After Delivery	Samurai can compile and execute downloaded modules at runtime.[1]
		.007	Dynamic API Resolution	Samurai can encrypt API name strings with an XOR-based algorithm.[1]
		.015	Compression	Samurai can deliver its final payload as a compressed, encrypted and base64-encoded blob.[1]
Enterprise	T1090		Proxy	Samurai has the ability to proxy connections to specified remote IPs and ports through a a proxy module.[1]

Domain	ID	Name	Use
Enterprise	T1012	Query Registry	Samurai can query `SOFTWARE\Microsoft\.NETFramework\policy\v2.0` for discovery.[1]
Enterprise	T1518	Software Discovery	Samurai can check for the presence and version of the .NET framework.[1]

Source: https://attack.mitre.org/software/S1099