

Flame, Software S0143 | MITRE ATT&CK®

Archived: 2026-04-05 14:17:44 UTC

Domain	ID	Name	Use
Enterprise	T1123	Audio Capture	Flame can record audio using any existing hardware recording devices. ^{[1][4]}
Enterprise	T1547	.002 Boot or Logon Autostart Execution: Authentication Package	Flame can use Windows Authentication Packages for persistence. ^[3]
Enterprise	T1136	.001 Create Account: Local Account	Flame can create backdoor accounts with login "HelpAssistant" on domain connected systems if appropriate rights are available. ^{[1][4]}
Enterprise	T1011	.001 Exfiltration Over Other Network Medium: Exfiltration Over Bluetooth	Flame has a module named BeetleJuice that contains Bluetooth functionality that may be used in different ways, including transmitting encoded information from the infected system over the Bluetooth protocol, acting as a Bluetooth beacon, and identifying other Bluetooth devices in the vicinity. ^[2]
Enterprise	T1210	Exploitation of Remote Services	Flame can use MS10-061 to exploit a print spooler vulnerability in a remote system with a shared printer in order to move laterally. ^{[1][4]}
Enterprise	T1036	.010 Masquerading: Masquerade Account Name	Flame can create backdoor accounts with login <code>HelpAssistant</code> on domain connected systems if appropriate rights are available. ^{[1][4]}
Enterprise	T1091	Replication Through Removable Media	Flame contains modules to infect USB sticks and spread laterally to other Windows systems the stick

Domain	ID	Name	Use
			is plugged into using Autorun functionality. ^[1]
Enterprise	T1113	Screen Capture	Flame can take regular screenshots when certain applications are open that are sent to the command and control server. ^[1]
Enterprise	T1518	.001 Software Discovery: Security Software Discovery	Flame identifies security software such as antivirus through the Security module. ^{[1][4]}
Enterprise	T1218	.011 System Binary Proxy Execution: Rundll32	Rundll32.exe is used as a way of executing Flame at the command-line. ^[3]
ICS	T0893	Data from Local System	Flame has built-in modules to gather information from compromised computers. ^[5]
ICS	T0882	Theft of Operational Information	Flame can collect AutoCAD design data and visio diagrams as well as other documents that may contain operational information. ^[5]

Source: https://attack.mitre.org/software/S0143