Imminent Monitor, Software S0434 | MITRE ATT&CK®

Archived: 2026-04-05 14:00:07 UTC

Domain	ID		Name	Use
Enterprise	T1123		Audio Capture	Imminent Monitor has a remote microphone monitoring capability.[1][2]
Enterprise	T1059		Command and Scripting Interpreter	Imminent Monitor has a CommandPromptPacket and ScriptPacket module(s) for creating a remote shell and executing scripts.[2]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Imminent Monitor has a PasswordRecoveryPacket module for recovering browser passwords.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Imminent Monitor has decoded malware components that are then dropped to the system.[2]
Enterprise	T1041		Exfiltration Over C2 Channel	Imminent Monitor has uploaded a file containing debugger logs, network information and system information to the C2. [2]
Enterprise	T1083		File and Directory Discovery	Imminent Monitor has a dynamic debugging feature to check whether it is located in the %TEMP% directory, otherwise it copies itself there.[2]
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	Imminent Monitor has a dynamic debugging feature to set the file attribute to hidden.[2]

Domain	ID		Name	Use
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	Imminent Monitor has a feature to disable Windows Task Manager.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Imminent Monitor has deleted files related to its dynamic debugger feature.[2]
Enterprise	T1056	.001	Input Capture: Keylogging	Imminent Monitor has a keylogging module. [1]
Enterprise	T1106		Native API	Imminent Monitor has leveraged CreateProcessW() call to execute the debugger.[2]
Enterprise	T1027		Obfuscated Files or Information	Imminent Monitor has encrypted the spearphish attachments to avoid detection from email gateways; the debugger also encrypts information before sending to the C2. [2]
Enterprise	T1057		Process Discovery	Imminent Monitor has a "Process Watcher" feature to monitor processes in case the client ever crashes or gets closed.[1]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	Imminent Monitor has a module for performing remote desktop access.[2]
Enterprise	T1496	.001	Resource Hijacking: Compute Hijacking	Imminent Monitor has the capability to run a cryptocurrency miner on the victim machine. [1]

Domain	ID	Name	Use
Enterprise	T1125	Video Capture	Imminent Monitor has a remote webcam monitoring capability.[1][2]

Source: https://attack.mitre.org/software/S0434