

Kasidet, Software S0088 | MITRE ATT&CK®

Archived: 2026-04-05 14:02:00 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Kasidet creates a Registry Run key to establish persistence. [1][2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Kasidet can execute commands using cmd.exe. [1]
Enterprise	T1083		File and Directory Discovery	Kasidet has the ability to search for a given filename on a victim. [1]
Enterprise	T1562	.004	Impair Defenses: Disable or Modify System Firewall	Kasidet has the ability to change firewall settings to allow a plug-in to be downloaded. [1]
Enterprise	T1105		Ingress Tool Transfer	Kasidet has the ability to download and execute additional files. [1]
Enterprise	T1056	.001	Input Capture: Keylogging	Kasidet has the ability to initiate keylogging. [1]
Enterprise	T1057		Process Discovery	Kasidet has the ability to search for a given process name in processes currently running in the system. [1]
Enterprise	T1113		Screen Capture	Kasidet has the ability to initiate keylogging and screen captures. [1]

Domain	ID	Name	Use	
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Kasidet has the ability to identify any anti-virus installed on the infected system. [1]
Enterprise	T1082	System Information Discovery	Kasidet has the ability to obtain a victim's system name and operating system version. [1]	

Source: <https://attack.mitre.org/software/S0088>