Catchamas, Software S0261 | MITRE ATT&CK®

Archived: 2026-04-05 14:32:37 UTC

Domain	ID		Name	Use
Enterprise	T1010		Application Window Discovery	Catchamas obtains application windows titles and then determines which windows to perform Screen Capture on.[1]
Enterprise	T1115		Clipboard Data	Catchamas steals data stored in the clipboard.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Catchamas adds a new service named NetAdapter to establish persistence.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Catchamas stores the gathered data from the machine in .db files and .bmp files under four separate locations.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	Catchamas collects keystrokes from the victim's machine.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	Catchamas adds a new service named NetAdapter in an apparent attempt to masquerade as a legitimate service.[1]
Enterprise	T1112		Modify Registry	Catchamas creates three Registry keys to establish persistence by adding a Windows Service.[1]
Enterprise	T1113		Screen Capture	Catchamas captures screenshots based on specific keywords in the window's title.[1]

Domain	ID	Name	Use
Enterprise	T1016	System Network Configuration Discovery	Catchamas gathers the Mac address, IP address, and the network adapter information from the victim's machine.[1]

Source: https://attack.mitre.org/software/S0261