BOLDMOVE, Software S1184 | MITRE ATT&CK®

Archived: 2026-04-05 12:54:31 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	BOLDMOVE uses web services for command and control communication.[1]
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	BOLDMOVE is capable of spawning a remote command shell.[1]
Enterprise	T1554		Compromise Host Software Binary	BOLDMOVE contains a watchdog-like feature that monitors a particular file for modification. If modification is detected, the legitimate file is backed up and replaced with a trojanized file to allow for persistence through likely system upgrades.[1]
Enterprise	T1543		Create or Modify System Process	BOLDMOVE can free all resources and terminate itself on victim machines.[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	BOLDMOVE uses the WolfSSL library to implement SSL encryption for command and control communication.[1]
Enterprise	T1480		Execution Guardrails	BOLDMOVE verifies it is executing from a specific path during execution.[1]
Enterprise	T1190		Exploit Public-Facing Application	BOLDMOVE is associated with exploitation of CVE-2022-49475 in FortiOS.[1]
Enterprise	T1083		File and Directory Discovery	BOLDMOVE can list information of all files in the system recursively from the root directory or from a

Domain	ID		Name	Use
				specified directory.[1]
Enterprise	T1564	.011	Hide Artifacts: Ignore Process Interrupts	BOLDMOVE calls the signal function to ignore the signals SIGCHLD, SIGHIP, and SIGPIPE prior to starting primary logic.[1]
Enterprise	T1562		Impair Defenses	BOLDMOVE can modify proprietary Fortinet logs on victim machines.[1]
		.006	Indicator Blocking	BOLDMOVE can disable the Fortinet daemons `moglogd` and `syslogd` to evade detection and logging.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	BOLDMOVE can remove files on victim systems.[1]
Enterprise	T1090	.003	Proxy: Multi-hop Proxy	BOLDMOVE is capable of relaying traffic from command and control servers to follow-on systems.[1]
Enterprise	T1082		System Information Discovery	BOLDMOVE performs system survey actions following initial execution.[1]
Enterprise	T1016		System Network Configuration Discovery	BOLDMOVE enumerates network interfaces on the infected host.[1]

Source: https://attack.mitre.org/software/S1184