Exaramel for Linux, Software S0401

Archived: 2026-04-05 14:17:48 UTC

Domain	ID		Name	Use
Enterprise	T1548	.001	Abuse Elevation Control Mechanism: Setuid and Setgid	Exaramel for Linux can execute commands with high privileges via a specific binary with setuid functionality.[2]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Exaramel for Linux uses HTTPS for C2 communications.[1][2]
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	Exaramel for Linux has a command to execute a shell command on the system.[1][2]
Enterprise	T1543		Create or Modify System Process	Exaramel for Linux has a hardcoded location that it uses to achieve persistence if the startup system is Upstart or System V and it is running as root.[2]
		.002	Systemd Service	Exaramel for Linux has a hardcoded location under systemd that it uses to achieve persistence if it is running as root.[1][2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Exaramel for Linux can decrypt its configuration file.[2]
Enterprise	T1008		Fallback Channels	Exaramel for Linux can attempt to find a new C2 server if it receives an error.[2]

Domain	ID		Name	Use
Enterprise	T1070	.004	Indicator Removal: File Deletion	Exaramel for Linux can uninstall its persistence mechanism and delete its configuration file.[2]
Enterprise	T1105		Ingress Tool Transfer	Exaramel for Linux has a command to download a file from and to a remote C2 server.[1][2]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	Exaramel for Linux uses RC4 for encrypting the configuration.[1][2]
Enterprise	T1053	.003	Scheduled Task/Job: Cron	Exaramel for Linux uses crontab for persistence if it does not have root privileges. [1][2]
Enterprise	T1033		System Owner/User Discovery	Exaramel for Linux can run `whoami` to identify the system owner.[2]

Source: https://attack.mitre.org/software/S0401