Kinsing, Software S0599 | MITRE ATT&CK®

Archived: 2026-04-05 16:43:59 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Kinsing has communicated with C2 over HTTP.[1]
Enterprise	T1110		Brute Force	Kinsing has attempted to brute force hosts over SSH.[1]
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	Kinsing has used Unix shell scripts to execute commands in the victim environment.[1]
Enterprise	T1609		Container Administration Command	Kinsing was executed with an Ubuntu container entry point that runs shell scripts.[1]
Enterprise	T1610		Deploy Container	Kinsing was run through a deployed Ubuntu container.[1]
Enterprise	T1133		External Remote Services	Kinsing was executed in an Ubuntu container deployed via an open Docker daemon API.[1]
Enterprise	T1083		File and Directory Discovery	Kinsing has used the find command to search for specific files.[1]
Enterprise	T1222	.002	File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification	Kinsing has used chmod to modify permissions on key files for use.[1]

Domain	ID		Name	Use
Enterprise	T1105		Ingress Tool Transfer	Kinsing has downloaded additional lateral movement scripts from C2.[1]
Enterprise	T1057		Process Discovery	Kinsing has used ps to list processes.[1]
Enterprise	T1021	.004	Remote Services: SSH	Kinsing has used SSH for lateral movement.[1]
Enterprise	T1018		Remote System Discovery	Kinsing has used a script to parse files like `/etc/hosts` and SSH `known_hosts` to discover remote systems.[1]
Enterprise	T1496	.001	Resource Hijacking: Compute Hijacking	Kinsing has created and run a Bitcoin cryptocurrency miner.[1][2]
Enterprise	T1053	.003	Scheduled Task/Job: Cron	Kinsing has used crontab to download and run shell scripts every minute to ensure persistence.[1]
Enterprise	T1552	.003	Unsecured Credentials: Shell History	Kinsing has searched `bash_history` for credentials.[1]
		.004	Unsecured Credentials: Private Keys	Kinsing has searched for private keys.[1]
Enterprise	T1078		Valid Accounts	Kinsing has used valid SSH credentials to access remote hosts.[1]