REPTILE, Software S1219 | MITRE ATT&CK®

Archived: 2026-04-05 16:32:09 UTC

Domain	ID		Name	Use
Enterprise	T1547	.006	Boot or Logon Autostart Execution: Kernel Modules and Extensions	The REPTILE rootkit is implemented as a loadable kernel module (LKM).[1]
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	REPTILE can deploy components automatically with shell scripts.[1]
Enterprise	T1543	.004	Create or Modify System Process: Launch Daemon	The REPTILE launcher can daemonize a process.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	The REPTILE launcher component can decrypt kernel module code from a file and load it into memory.[1]
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	REPTILE can use TLS over raw TCP for secure C2.[1][2]
Enterprise	T1546	.017	Event Triggered Execution: Udev Rules	REPTILE has used udev for persistence.[1]
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	REPTILE has the ability to communicate with the kernel-mode component to hide files.[1]
Enterprise	T1095		Non-Application Layer Protocol	REPTILE can communicate using TLS over raw TCP.[1][2]
Enterprise	T1014		Rootkit	REPTILE has the ability to hook kernel functions and modify functions data to

Domain	ID		Name	Use
				achieve rootkit functionality such as hiding processes and network connections.[1]
Enterprise	T1205		Traffic Signaling	The REPTILE reverse shell component can listen for a specialized packet in TCP, UDP, or ICMP for activation.[1][2]
		.001	Port Knocking	REPTILE has the ability to control compromised endpoints via port knocking. [1]

Source: https://attack.mitre.org/software/S1219