Regin, Software S0019 | MITRE ATT&CK®

Archived: 2026-04-05 17:43:45 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	The Regin malware platform supports many standard protocols, including HTTP and HTTPS. [1]
		.002	Application Layer Protocol: File Transfer Protocols	The Regin malware platform supports many standard protocols, including SMB. [1]
Enterprise	T1564	.004	Hide Artifacts: NTFS File Attributes	The Regin malware platform uses Extended Attributes to store encrypted executables. [1]
		.005	Hide Artifacts: Hidden File System	Regin has used a hidden file system to store some of its components. [1]
Enterprise	T1056	.001	Input Capture: Keylogging	Regin contains a keylogger. [1]
Enterprise	T1036	.001	Masquerading: Invalid Code Signature	Regin stage 1 modules for 64-bit systems have been found to be signed with fake certificates masquerading as originating from Microsoft Corporation and Broadcom Corporation. [1]
Enterprise	T1112		Modify Registry	Regin appears to have functionality to modify remote Registry information. [1]
Enterprise	T1040		Network Sniffing	Regin appears to have functionality to sniff for credentials passed over HTTP, SMTP, and SMB. [1]

Domain	ID		Name	Use
Enterprise	T1095		Non-Application Layer Protocol	The Regin malware platform can use ICMP to communicate between infected computers.[1]
Enterprise	T1090	.002	Proxy: External Proxy	Regin leveraged several compromised universities as proxies to obscure its origin.[1]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	The Regin malware platform can use Windows admin shares to move laterally.[1]

Source: https://attack.mitre.org/software/S0019/