YiSpecter, Software S0311 | MITRE ATT&CK®

Archived: 2026-04-05 14:28:16 UTC

Domain	ID		Name	Use
Mobile	T1437	.001	Application Layer Protocol: Web Protocols	YiSpecter has connected to the C2 server via HTTP. [1]
Mobile	T1577		Compromise Application Executable	YiSpecter has replaced device apps with ones it has downloaded.[1]
Mobile	T1407		Download New Code at Runtime	YiSpecter has used private APIs to download and install other pieces of itself, as well as other malicious apps. [1]
Mobile	T1456		Drive-By Compromise	YiSpecter is believed to have initially infected devices using internet traffic hijacking to generate abnormal popups.[1]
Mobile	T1628	.001	Hide Artifacts: Suppress Application Icon	YiSpecter has hidden the app icon from iOS springboard.[1]
Mobile	T1625		Hijack Execution Flow	YiSpecter has hijacked normal application's launch routines to display ads.[1]
Mobile	T1424		Process Discovery	YiSpecter has collected information about running processes.[1]
Mobile	T1418		Software Discovery	YiSpecter has collected information about installed applications.[1]

Domain	ID		Name	Use
Mobile	T1409		Stored Application Data	YiSpecter has modified Safari’s default search engine, bookmarked websites, opened pages, and accessed contacts and authorization tokens of the IM program "QQ" on infected devices.[1]
Mobile	T1632	.001	Subvert Trust Controls: Code Signing Policy Modification	YiSpecter has used fake Verisign and Symantec certificates to bypass malware detection systems. YiSpecter has also signed malicious apps with iOS enterprise certificates to work on non-jailbroken iOS devices.[1]
Mobile	T1426		System Information Discovery	YiSpecter has collected the device UUID.[1]
Mobile	T1422		System Network Configuration Discovery	YiSpecter has collected compromised device MAC addresses.[1]

Source: https://attack.mitre.org/software/S0311