RTM, Group G0048 | MITRE ATT&CK®

Archived: 2026-04-02 12:02:20 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	RTM has used Registry run keys to establish persistence for the RTM Trojan and other tools, such as a modified version of TeamViewer remote desktop software.[1][2]
Enterprise	T1189		Drive-by Compromise	RTM has distributed its malware via the RIG and SUNDOWN exploit kits, as well as online advertising network `Yandex.Direct`.[1][3]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	RTM has used search order hijacking to force TeamViewer to load a malicious DLL.[2]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	RTM has used spearphishing attachments to distribute its malware.[2]
Enterprise	T1219	.002	Remote Access Tools: Remote Desktop Software	RTM has used a modified version of TeamViewer and Remote Utilities for remote access.[2]
Enterprise	T1204	.002	User Execution: Malicious File	RTM has attempted to lure victims into opening e-mail attachments to execute malicious code.[2]
Enterprise	T1102	.001	Web Service: Dead Drop Resolver	RTM has used an RSS feed on Livejournal to update a list of encrypted C2 server names.[1]

Source: https://attack.mitre.org/groups/G0048/