

## C0011, Campaign C0011 | MITRE ATT&CK®

Archived: 2026-04-05 16:18:56 UTC

Domain	ID	Name	Use
Enterprise	<a href="#">T1583</a> <a href="#">.001</a>	<a href="#">Acquire Infrastructure: Domains</a>	For <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> registered domains likely designed to appear relevant to student targets in India. <sup>[1]</sup>
Enterprise	<a href="#">T1059</a> <a href="#">.005</a>	<a href="#">Command and Scripting Interpreter: Visual Basic</a>	For <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> used malicious VBA macros within a lure document as part of the <a href="#">Crimson</a> malware installation process onto a compromised host. <sup>[1]</sup>
Enterprise	<a href="#">T1587</a> <a href="#">.003</a>	<a href="#">Develop Capabilities: Digital Certificates</a>	For <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> established SSL certificates on the typo-squatted domains the group registered. <sup>[1]</sup>
Enterprise	<a href="#">T1566</a> <a href="#">.001</a>	<a href="#">Phishing: Spearphishing Attachment</a>	During <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> sent malicious attachments via email to student targets in India. <sup>[1]</sup>
	<a href="#">.002</a>	<a href="#">Phishing: Spearphishing Link</a>	During <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> sent emails containing a malicious link to student targets in India. <sup>[1]</sup>
Enterprise	<a href="#">T1608</a> <a href="#">.001</a>	<a href="#">Stage Capabilities: Upload Malware</a>	For <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> hosted malicious documents on domains registered by the group. <sup>[1]</sup>
Enterprise	<a href="#">T1204</a> <a href="#">.001</a>	<a href="#">User Execution: Malicious Link</a>	During <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> relied on student targets to click on a malicious link sent via email. <sup>[1]</sup>

Domain	ID	Name	Use
		<a href="#">.002</a> <a href="#">User Execution:</a> <a href="#">Malicious File</a>	During <a href="#">C0011</a> , <a href="#">Transparent Tribe</a> relied on a student target to open a malicious document delivered via email. <sup>[1]</sup>

---

Source: <https://attack.mitre.org/campaigns/C0011>