Transparent Tribe, COPPER FIELDSTONE, APT36, Mythic Leopard, ProjectM, Group G0134

Archived: 2026-04-05 12:59:40 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

Transparent Tribe has registered domains to mimic file sharing, government, defense, and research websites for use in targeted campaigns.[1][3]

For C0011, Transparent Tribe registered domains likely designed to appear relevant to student targets in India.[7]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

Transparent Tribe has crafted VBS-based malicious documents.[1][2]

For C0011, Transparent Tribe used malicious VBA macros within a lure document as part of the Crimson malware installation process onto a compromised host.[7]

Enterprise T1584 .001 Compromise Infrastructure: Domains

Transparent Tribe has compromised domains for use in targeted malicious campaigns.[1]

Enterprise T1587 .003 Develop Capabilities: Digital Certificates

For C0011, Transparent Tribe established SSL certificates on the typo-squatted domains the group registered.[7]

Enterprise T1189 Drive-by Compromise

Transparent Tribe has used websites with malicious hyperlinks and iframes to infect targeted victims with Crimson, njRAT, and other malicious tools.[1][6][3]

Enterprise T1568 Dynamic Resolution

Transparent Tribe has used dynamic DNS services to set up C2.[1]

Enterprise T1203 Exploitation for Client Execution

Transparent Tribe has crafted malicious files to exploit CVE-2012-0158 and CVE-2010-3333 for execution.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Transparent Tribe can hide legitimate directories and replace them with malicious copies of the same name.[2]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Transparent Tribe can mimic legitimate Windows directories by using the same icons and names.[2]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Transparent Tribe has dropped encoded executables on compromised hosts.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Transparent Tribe has sent spearphishing e-mails with attachments to deliver malicious payloads.[1][2][8][3][6]

During C0011, Transparent Tribe sent malicious attachments via email to student targets in India.[7]

.002 Phishing: Spearphishing Link

Transparent Tribe has embedded links to malicious downloads in e-mails.[8][3]

During C0011, Transparent Tribe sent emails containing a malicious link to student targets in India.[7]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

For C0011, Transparent Tribe hosted malicious documents on domains registered by the group.[7]

.004 Stage Capabilities: Drive-by Target

Transparent Tribe has set up websites with malicious hyperlinks and iframes to infect targeted victims with Crimson, njRAT, and other malicious tools.[1][6][3]

Enterprise T1204 .001 User Execution: Malicious Link

Transparent Tribe has directed users to open URLs hosting malicious content.[8][3]

During C0011, Transparent Tribe relied on student targets to click on a malicious link sent via email.[7]

.002 User Execution: Malicious File

Transparent Tribe has used weaponized documents in e-mail to compromise targeted systems.[1][2][8][3][6]

During C0011, Transparent Tribe relied on a student target to open a malicious document delivered via email.[7]
