Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

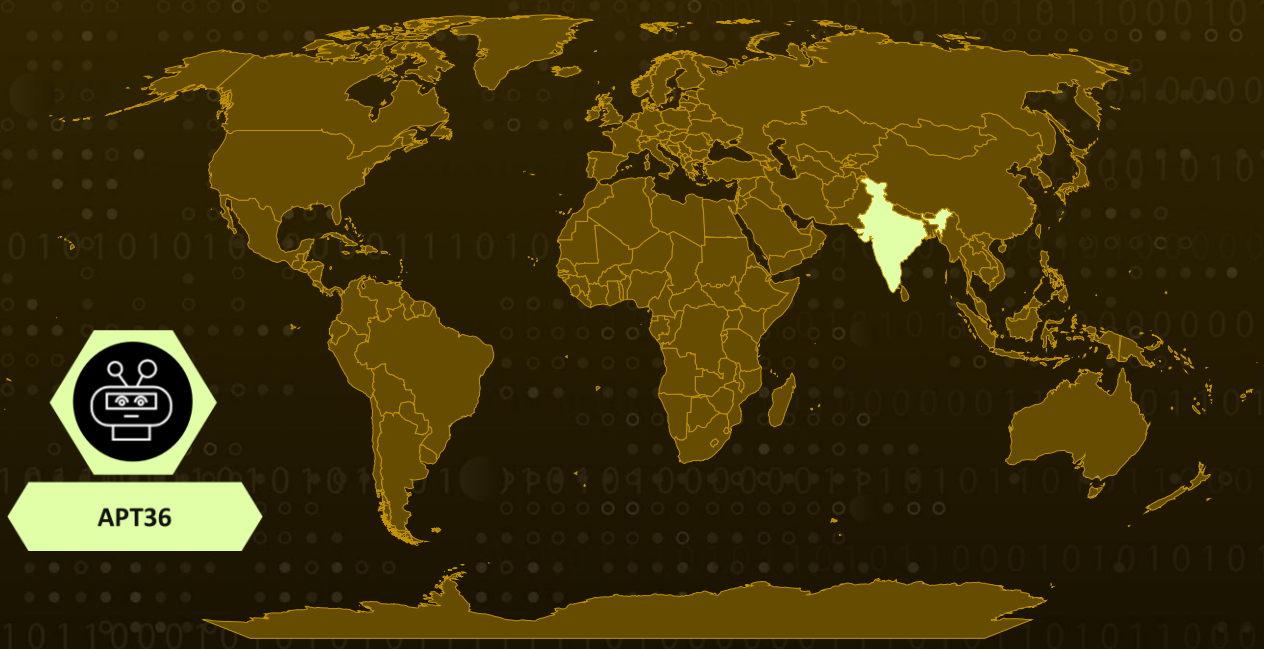
Silent Clicks, Lasting Access: APT36's Fileless Espionage Playbook

Date of Publication	Admiralty Code	TA Number
January 5, 2026	A1	TA2026002

Summary

First Seen: December 15, 2025
Targeted Region: India
Targeted Industries: Government, Academic
Actor: APT36 (aka Transparent Tribe, ProjectM, Mythic Leopard, TEMP.Lapis, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH, Green Havildar, APT-C-56, Storm-0156, Opaque Draco, G0134)
Affected Platform: Windows
Attack: APT36's latest campaign reveals how a single, convincing click can quietly open the door to long-term espionage. Disguised as a harmless PDF inside a familiar ZIP file, a weaponized Windows shortcut triggers a fileless, multi-stage infection that abuses trusted system tools like mshta.exe to stay invisible. While victims see a legitimate document on screen, a sophisticated Remote Access Trojan is deployed in memory, profiling security software, adapting its behavior to evade detection, and establishing encrypted channels for surveillance and data theft. The operation reflects a mature and patient adversary, one that blends social engineering with technical precision to blend into normal user activity, maintain persistence, and silently extract intelligence from high-value Indian targets.

Attack Regions



Attack Details

#1 APT36, also known as Transparent Tribe, continues to demonstrate its focus on cyber-espionage operations targeting Indian governmental and strategic entities. This latest campaign reflects a deliberate and methodical approach, prioritizing stealth, persistence, and long-term intelligence collection over immediate disruption. By blending social engineering with technical sophistication, the threat actor leverages trusted Windows components and familiar document formats to infiltrate environments while minimizing suspicion and forensic visibility.

#2 The attack chain begins with a carefully crafted spear-phishing email delivering a ZIP archive disguised as legitimate examination material. Inside, victims encounter a deceptively named shortcut file masquerading as a PDF, exploiting Windows' tendency to hide file extensions. Unlike typical shortcuts, this oversized LNK embeds a full PDF structure, reinforcing its legitimacy. When executed, it silently launches mshta.exe, a trusted Windows utility, to retrieve and execute attacker-controlled HTA content directly in memory, effectively bypassing traditional file-based security controls.

#3 Once the HTA loader is active, the infection unfolds in multiple stages designed to prepare the system for deeper compromise. The initial "ReadOnly" stage reconstructs a serialized .NET object in memory and weakens built-in deserialization safeguards, deliberately opening the door for unsafe operations. This paves the way for the "WriteOnly" stage, which loads a larger malicious DLL entirely in memory. Throughout this process, the malware displays a legitimate PDF to the victim, reinforcing the illusion of normal activity while malicious components quietly initialize in the background.

#4 At the core of the operation is a fully featured Remote Access Trojan that grants attackers covert, long-term control over infected systems. The malware profiles the host environment; queries installed antivirus solutions via WMI and dynamically adapts its persistence mechanisms to evade detection. Depending on the security software present, it deploys tailored execution paths using startup shortcuts, batch files, registry modifications, or obfuscated HTA loaders. Communication with the command-and-control server is encrypted, enabling remote command execution, file access, screen capture, clipboard manipulation, and extensive data theft without raising immediate alarms.

#5 Overall, this campaign highlights APT36's continued evolution toward more resilient, security-aware intrusion frameworks. By abusing trusted Windows utilities, embedding malicious logic within seemingly benign files, and maintaining a modular, multi-stage execution model, the group effectively blends into normal user activity while sustaining persistent access. The operation underscores the growing risk posed by state-aligned espionage actors, particularly in environments reliant on legacy Windows features and user trust, and reinforces the need for behavior-based detection, continuous monitoring, and heightened awareness across high-value sectors.

Recommendations

- **Treat Shortcuts like Executables:** Windows shortcut (.LNK) files can run hidden commands. Users should avoid opening unexpected shortcuts, even if they appear to be PDFs or documents.
- **Block Misuse of Trusted Windows Tools:** Monitor and restrict the use of mshta.exe, wscript.exe, and similar utilities, as attackers frequently abuse them to run malware invisibly.
- **Network Segmentation:** Isolate sensitive government systems from general user networks. Implement strict egress filtering to detect and block unauthorized C2 communication.
- **User Access Controls:** Enforce least-privilege principles across all endpoints. Implement multi-factor authentication for administrative access.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0010 Exfiltration	**TA0011** Command and Control	**TA0040** Impact	**T1566** Phishing
T1566.001 Spearphishing Attachment	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.005** Visual Basic
T1218 System Binary Proxy Execution	**T1218.005** Mshta	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder

T1112 Modify Registry	**T1055** Process Injection	**T1036** Masquerading	**T1027** Obfuscated Files or Information
T1070 Indicator Removal	**T1202** Indirect Command Execution	**T1497** Virtualization/Sandbox Evasion	**T1564** Hide Artifacts
T1564.001 Hidden Files and Directories	**T1555** Credentials from Password Stores	**T1539** Steal Web Session Cookie	**T1082** System Information Discovery
T1057 Process Discovery	**T1083** File and Directory Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery
T1113 Screen Capture	**T1115** Clipboard Data	**T1005** Data from Local System	**T1560** Archive Collected Data
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1095** Non-Application Layer Protocol	**T1573** Encrypted Channel
T1105 Ingress Tool Transfer	**T1041** Exfiltration Over C2 Channel	**T1565** Data Manipulation	**T1565.001** Stored Data Manipulation
T1047 Windows Management Instrumentation			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	06fb22c743fcc949998e280bd5deaf8f80d616b371576b5e11fd5b1d3b23a5f2, c1f3dea00caec58c9e0f990366ff40ae59e93f666f92e1c218c03478bf3abe17, fc43f4c618bce57461df5752a8d3bedf243eacfdd3e648ea8b1310083764fd92
Domains	innlive[.]in, drjagrutichavan[.]com
IPv4	2[.]56[.]10[.]86

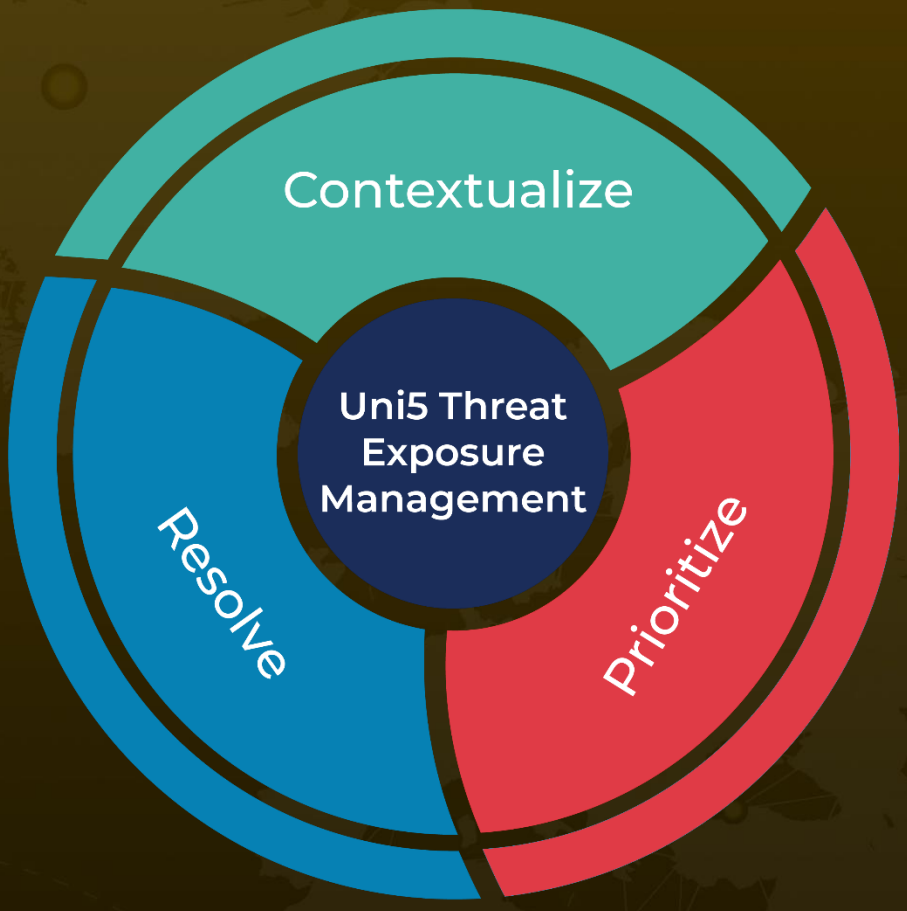
References

https://www.cyfirma.com/research/apt36-multi-stage-lnk-malware-campaign-targeting-indian-government-entities/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 5, 2026 • 7:10 AM

More at www.hivepro.com