Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

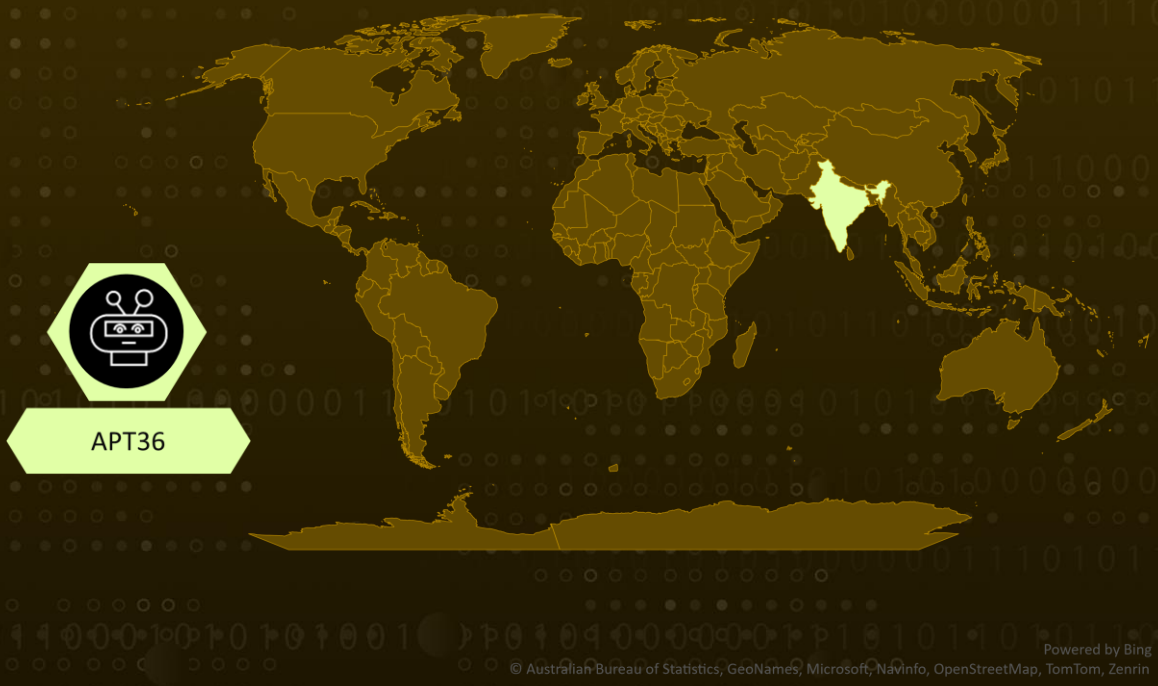
APT36 targets Indian educational institutions with Crimson RAT

Date of Publication	Admiralty Code	TA Number
April 18, 2023	A1	TA2023190

Summary

Attack Began: February 2023
Threat Actor: APT 36(Transparent Tribe, ProjectM, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH)
Attack Country: India
Attack Indutry: Education
Malware: Crimson RAT
Attack: APT36, a suspected Pakistani threat group, is targeting educational institutions and students in the Indian subcontinent by distributing malicious documents disguised as education-themed content to stage the Crimson RAT malware using tactics like OLE embedding.

Attack Regions



Attack Details

#1

APT36, a suspected Pakistani threat group, which is also known as Transparent Tribe is known for its persistence and continuous adaptation of operational strategies. The latest report reveals that the group is targeting educational institutions and students in the Indian subcontinent, in addition to its previous targeting of Indian military and government personnel. The group has been distributing malicious documents with education-themed content and names such as "assignment" or "Assignment-no-10." The group distributes these documents as attachments to phishing emails or on file hosting services and attacker-created domains.

#2

The documents are designed to stage Crimson RAT, a consistent staple in Transparent Tribe's malware arsenal. The malware can exfiltrate system information, capture screenshots, and start or stop processes. In addition to its usual tactics, the group has recently introduced OLE embedding to stage the malware. The technique requires users to double-click an image within the document, which activates an OLE package that stores and executes Crimson RAT disguised as an update process.

Recommendations

- Security teams should monitor for **OLE embedding** techniques and other new tactics being used by **APT36/Transparent Tribe** and take appropriate measures to block or mitigate attacks.
- **Educational institutions** and **students** in the **Indian** subcontinent should be made aware of the threat posed by **APT36/Transparent Tribe** and should also educated on how to identify and avoid phishing emails with suspicious file attachments.
- Organizations should ensure that their cybersecurity defenses are up to date and that their employees are trained on how to identify and report suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0009** Collection	**TA0011** Command and Control	**TA0040** Impact
T1566 Phishing	**T1559** Inter-Process Communication	**T1547** Boot or Logon Autostart Execution	**T1113** Screen Capture
T1102 Web Service	**T1127** Trusted Developer Utilities Proxy Execution	**T1531** Account Access Removal	**T1140** Deobfuscate/Decode Files or Information
T1027 Obfuscated Files or Information			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	richa-sharma.ddns[.]net cloud-drive[.]store drive-phone[.]online s1.fileditch[.]ch
SHA1	738d31ceca78ffd053403d3b2bc15847682899a0 9ed39c6a3faab057e6c962f0b2aaab07728c5555 af6608755e2708335dc80961a9e634f870aecf3c e000596ad65b2427d7af3313e5748c2e7f37fba7 fd46411b315beb36926877e4b021721fcd111d7a 516db7998e3bf46858352697c1f103ef456f2e8e 842f55579db786e46b20f7a7053861170e1c0c5e 87e0ea08713a746d53bef7fb04632bfcd6717fa9 911226d78918b303df5110704a8c8bb599bcd403 973cb3afc7eb47801ff5d2487d2734ada6b4056f

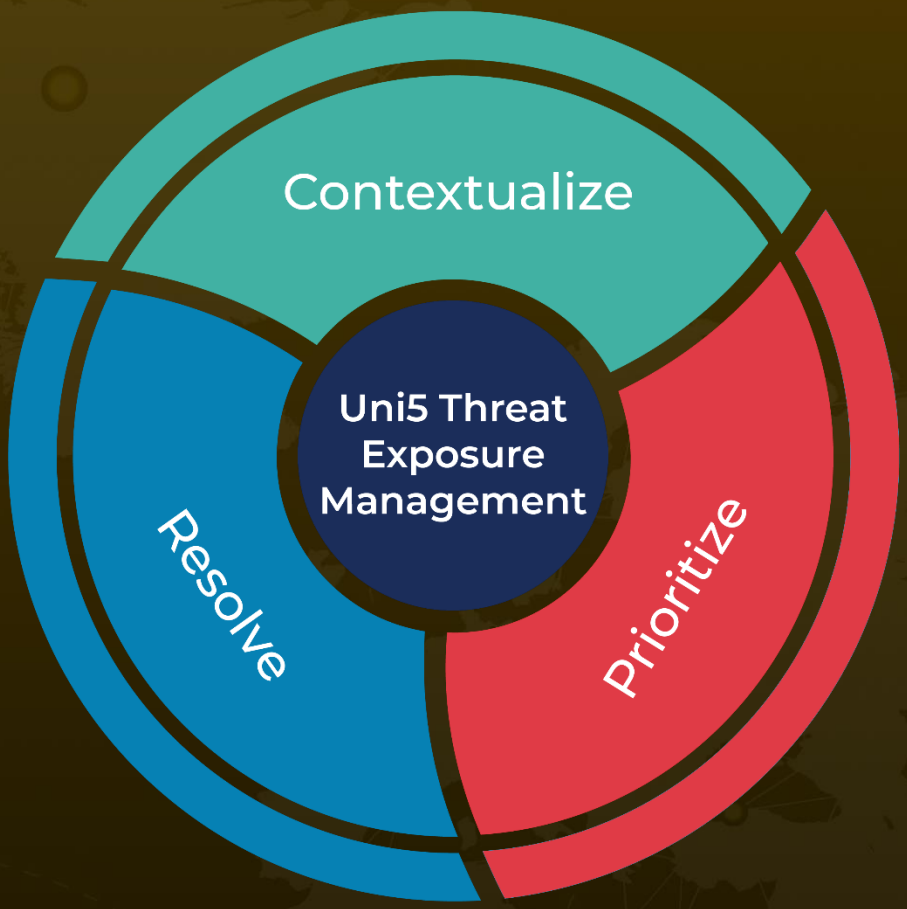
References

https://www.sentinelone.com/labs/transparent-tribe-apt36-pakistan-aligned-threat-actor-expands-interest-in-indian-education-sector/

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

April 18, 2023 • 1:45 AM

More at www.hivepro.com