Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

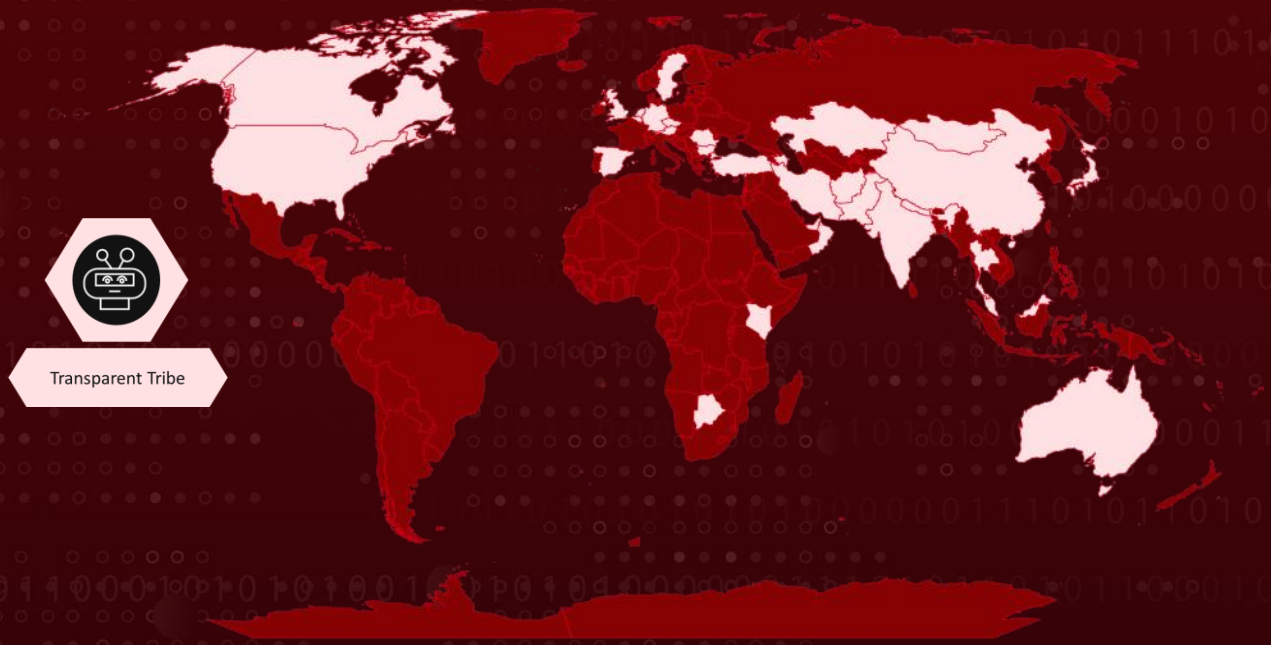
Transparent Tribe's latest campaign targets the education sector

Date of Publication	Admiralty code	TA Number
July 15, 2022	A2	TA2022149

Summary

Transparent Tribe, an Advanced Persistent Threat group also known as APT36 or Mythic Leopard, was discovered actively launching phishing campaigns against educational institutions and students across India. A classic deviation from targeting the military and other government entities.

Actor Map



Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**T1583.001** Acquire Infrastructure: Domains	**TA0002** Execution	**T1059.005** Command and Scripting Interpreter: Visual Basic
T1584.001 Compromise Infrastructure: Domains	**TA0001** Initial Access	**T1189** Drive-by Compromise	**TA0011** Command and Control
T1568 Dynamic Resolution	**T1203** Exploitation for Client Execution	**TA0005** Defense Evasion	**T1564.001** Hide Artifacts: Hidden Files and Directories
T1036.005 Masquerading: Match Legitimate Name or Location	**T1027** Obfuscated Files or Information	**T1566.001** Phishing: Spearphishing Attachment	**T1566.002** Phishing: Spearphishing Link
T1608.004 Stage Capabilities: Drive-by Target	**T1204.001** User Execution: Malicious Link	**T1204.002** User Execution: Malicious File	

Technical Details

#1

Transparent Tribe is expanding their victim list by targeting civilian users with Remote Access Trojans such as CrimsonRAT and custom malware created by this APT group.

#2

The victim is approached through a spear-phishing email with malicious documents attached that, when unzipped, install the CrimsonRAT malware on the victim's system. The CrimsonRAT used in the recent campaign is capable of listing files, folders, and process IDs in the path specified by Command and Control, as well as exfiltrating system details and taking screenshots of the current screen and keylogger logs and sending them to the C2.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONs	TARGET INDUSTRIES
Transparent Tribe (APT36, Mythic Leopard)	Pakistan	Information theft and espionage	Afghanistan, Australia, Austria, Azerbaijan, Belgium, Botswana, Bulgaria, Canada, China, Czech, Germany, India, Iran, Japan, Kazakhstan, Kenya, Malaysia, Mongolia, Nepal, Netherlands, Oman, Pakistan, Romania, Saudi Arabia, Spain, Sweden, Thailand, Turkey, UAE, UK, USA.	Defense, Education, Government, Embassies and Research Organizations

Indicator of Compromise (IOC)

TYPE	VALUE
Maldocs	bdeb9d019a02eb49c21f7c04169406ac586d630 032a059f63c497951303b8d00 388f212dfca2bfb5db0a8b9958a43da6860298cd d4fcd53ed2c75e3b059ee622 0d61d5fe8dbf69c6e61771451212fc8e587d9324 6bd866adf1031147d6d4f8c2 14ee2e3a9263bab359bc19050567d0dbd6371c 8c0a7c6aeba71adbf5df2fc35b
IP	192.3.99.68 198.37.123.126
Domains	studentsportal.live geo-news.tv cloud-drive.store user-onedrive.live drive-phone.online studentsportal.co studentsportal.website nsdrive-phone.online statefinancebank.com in[.]statefinancebank.com centralink.online cloud-drive.geo-news.tv drive-phone.geo-news.tv studentsportal.geo-news.tv user-onedrive.geo-news.tv studentsportal.live.geo-news.tv phone-drive.online.geo-news.tv sunnyleone.hopto.org swissaccount.ddns.net

TYPE	VALUE
Archives	8c1a5052bf3c1b33aff9e249ae860ea1435ce716d5b5be2ec3407520507c6d3779aee357ea68d8f66b929ba2e57465eaee4d965b0da5001fe589afe1588874e3
URLs	hxxps://studentsportal.live/download.php?file=Mental_Health_Survey.docm hxxps://studentsportal.website/download.php?file=5-mar.zip
CrimsonRAT	8b786784c172c6f8b241b1286a2054294e8dc2c167d9b4daae0e310a1d923ba0 b4819738a277090405f0b5bbcb31d5dd3115f7026401e5231df727da0443332a e2cf71c78d198fdc0017b7bfd6ce8115301174302b3eaaf50cfc384db96bc573 8c9b0fd259e7f016f53be8edc53fe5f908b48ae691e21f0f820da11429e595d8 f3a1ac021941b481ac7e2335b74ebf1e44728e8917381728f1f5b390c6f34706 fc34f9087ab199d0bac22aa97de48e5592dbf0784342b9ecd01b4a429272ab5b b3f8e026f39056ec5e66700e03eeaf57454ee9c0bc1c719d74e10f57029573059159d4e354218870461c96bedcc7b5b026f872d30235bb4536cc4a5ce4154725 b614436bf9461b80384bae937d699f8c3886bcc65b907e0c8126b4df59ea8cdb 28390e3ea8a547f05ca08551f484292d46398a2b38fd4aae001ac7d056c5abc0

References

https://blog.talosintelligence.com/2022/07/transparent-tribe-targets-education.html?m=1

https://attack.mitre.org/groups/G0134/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 15, 2022 • 4:19 AM

More at www.hivepro.com