

New year, new sector: Transparent Tribe targets India's startup ecosystem

 acronis.com/en/tru/posts/new-year-new-sector-transparent-tribe-targets-indias-startup-ecosystem

Authors: Jozsef Gegeny, Vadim Bunimovich, Subhajeet Singha

Summary

Acronis Threat Research Unit (TRU) has been tracking Transparent Tribe, also known as APT36, and has uncovered a campaign that stands out for its use of startup-oriented, themed lure material delivered via an ISO container-based file.

The group has moved beyond government targets, such as defense organizations and educational institutions, to India's startup ecosystem, delivering Crimson RAT via ISO files and malicious LNK shortcuts using sensitive, startup-themed lures.

Active since 2013 and widely assessed by multiple vendors as a Pakistan-based threat group, Transparent Tribe has historically targeted military personnel, government entities and the education sector.

Recent findings from TRU indicate that Transparent Tribe has **expanded its targeting to include individuals within India's startup ecosystem** using decoy material built around a real startup founder and legitimate OSINT- and cybersecurity-focused content, while delivering the Crimson RAT malware.

Despite this expansion, the campaign remains closely aligned with Transparent Tribe's historical focus on **Indian government and defense-adjacent intelligence collection**, with overlap suggesting that startup-linked individuals may be targeted for their proximity to government, law enforcement or security operations.

APT36 has used other known malware families across multiple campaigns, including remote access trojans such as **AresRAT, AllaKore, GetaRAT, Poseidon** and **DeskRAT**, which make up its malware arsenal.

Introduction

The Acronis Threat Research Unit (TRU) has been actively monitoring APT36, also known as Transparent Tribe and its threat activity targeting the Indian government using lures themed around defense-related events, internal government communications, education and other topics. Recently, TRU identified a notable deviation in the group's targeting, with a shift and addition of its targeting toward Indian startups, particularly those operating in the cybersecurity domain.

These observations indicate that the group is targeting a new victim profile. Analysis of the malware components and the supporting infrastructure used to run this campaign highlights core behavioral TTPs that are consistent with the group's past activity. This report documents the delivery mechanism, execution flow and command-and-control behavior associated with Crimson RAT, while examining the key drivers behind this targeting shift and identifying commonalities between this campaign and previous TRU findings. The analysis also places this activity within the context of broader espionage-oriented trends.

Throughout the research, we've outlined the analytical basis for attributing this activity to Transparent Tribe, with high confidence. This assessment is primarily based on observed victimology, malware used and deployed, infrastructure overlaps and its consistency with that of previous campaigns tracked by TRU. This report details the indicators and behaviors that support this assessment, providing defenders with context on how such overlaps support attribution and how threat groups may occasionally adjust their targeting while maintaining established tradecraft.

Background and context

Transparent Tribe, also known as APT36, is a long-running espionage group commonly attributed by researchers to state aligned interests. It primarily targets countries across South Asia, including India and Afghanistan, using geopolitical and [government-themed](#), [education](#) and military exercise-themed lures to gain access. The group mainly focuses on collecting intelligence from government, defense, diplomatic and research organizations, relying on social engineering and simple, but effective delivery methods such as malicious documents, LNK files, ISO-based container-files, HTA payloads and much more.

Operationally, Transparent Tribe traverses through multiple simple, yet interesting, sets of initial access payloads such as, LNK, HTA, ISO, MSC, ZIP, VHDX and similar file types, sometimes aggressively leaning towards the container file type, which drops interesting decoy-themes with repeatable remote-access-trojan malware such as Crimson RAT and sometimes, depending on modifying and using open-source [credential harvesting projects](#) to perform final execution, on the targets' machine. This group has demonstrated repeated reuse of tooling and infrastructure, enabling analysts to cluster activity. This campaign reflects established behavior while introducing a new target sector, providing context for the analysis that follows.

Attack chain

The initial access vector is a spear-phishing email carrying an ISO image named **MeetBisht.iso**, seemingly tailored to reference the startup's owner. Once executed, the ISO contains a malicious shortcut file named *Meet Bisht.xlsx.lnk* and a folder holding three files: a decoy document, a batch script that acts as the execution runner and persistence mechanism, and the final Crimson RAT payload, disguised as an executable named **excel**.

Figure 1: Attack chain demonstration of the payload execution

Technical details

Initial analysis and delivery mechanism Our investigation began after identifying a campaign that deviates from APT36's typical targeting. The activity involved a spear-phishing email delivering a container-based ISO file named **MeetBisht.iso**, uploaded from India to VirusTotal, which contained an XLSX decoy, a runner batch script and the Crimson RAT payload.

Figure 2: Contents inside the malicious container-based payload

The activity in terms of the naming convention stood out due to the personal-name themed ISO file name and the execution chain, which is a standard chain aligned with the pattern observed by us, related to Transparent Tribe, since October 2025. These observations prompted us to perform deeper analysis of the campaign, its decoy, the payload, its execution flow and the other running operations targeting government and critical sectors, followed by the attributional artifacts.

Deviation and decoy — Why?

Figure 3: Decoy-extracted shows data about the Director of Voldebug

Transparent Tribe has historically targeted Indian government related sectors. Analysis of the decoy material used in this campaign shows references to a startup that had pitched an OSINT based monitoring system known as **SIS (Smart Investigation System): A Comprehensive Dashboard for Digital Data Monitoring and Investigation with Advanced GUI and OSINT Features**. The decoy includes publicly accessible and limited personal information associated with the startup [Voldebug](#), suggesting the material was used to increase the credibility of the lure rather than to imply direct targeting intent.

Figure 4: Website mentioning Voldebug's support to LEA

Based on this, our investigation indicates that the targeted startup is actively engaged in providing open-source intelligence services and related products, collaborating with government bodies and law enforcement agencies (LEAs) to enhance security capabilities. This suggests a potential shift in Transparent Tribe's targeting strategy toward companies operating in the OSINT and digital surveillance domain. We've assessed that this activity may reflect an interest in collecting intelligence on such organizations using malware families like **Crimson RAT**.

Malicious LNK and batch script

Once the victim executes the malicious LNK file, which is disguised as an Excel document, it runs the command `%COMSPEC% /c start /MIN ~\mycsd.bat`. This launches cmd.exe to execute the batch file and immediately exit, with the command window minimized to reduce user visibility.

Figure 5: Properties of the LNK file

The malicious batch script displays a decoy Excel file to distract the user while silently copying a malicious directory to C:\ProgramData\. It removes the Mark of the Web (MotW) using PowerShell to bypass SmartScreen warnings, creates a disguised, hard-linked executable in %APPDATA% named *vrjnactsmiagrws.exe*, and finally launches the payload from a user writable location to achieve stealthy execution. The executed payload is Crimson RAT.

Crimson RAT

Crimson RAT is a .NET-based, remote-access trojan distributed as an executable file. The sample analyzed exhibits a significantly inflated file size of 34MB, which is artificially enlarged through the inclusion of substantial amounts of garbage data strategically embedded within the application's resources section.

Figure 6: Large random data

This technique of padding executables with random or junk data serves multiple evasion purposes:

- Many signature-based detection systems struggle with oversized files, as scanning large binaries can impact system performance.

- The random data alters the file's entropy calculations, potentially bypassing entropy-based detection algorithms.

- Some automated analysis environments have file size limitations.

Despite the inflated file size, the actual malicious code footprint is considerably smaller, estimated between 80–150KB.

The malware employs extensive obfuscation techniques to hinder static analysis, including:

- Both client and server components use obfuscated command strings for communication. The server transmits obfuscated commands which the client is programmed to interpret and understand, creating a custom protocol that complicates network analysis and signature detection.

- All function names have been replaced with randomly generated identifiers, making static analysis and code comprehension significantly more difficult.

- Variable names throughout the codebase are randomized, removing any semantic meaning that could assist reverse engineers in understanding the code's purpose and functionality.

This obfuscation strategy effectively removes human-readable elements from the code while maintaining functionality, forcing analysts to rely on dynamic analysis and behavioral observation rather than static code review to understand the malware's capabilities.

Crimson RAT utilizes a custom TCP protocol for command and control (C&C) communications, avoiding standard HTTP / HTTPS protocols that are more easily monitored and filtered. The C&C server addresses are hardcoded directly into the binary.

Figure 7: Hardcoded C&C servers

Crimson RAT uses a predefined set of port numbers for communication. These port numbers are stored in an array, as shown in the picture below:

Figure 8: Port numbers used by the RAT

The following screenshot shows the network traffic generated by the RAT. Two main commands can be observed: first, an information request, and second, a simple ping from the server. As demonstrated, the commands appear obfuscated in the network traffic as well, not only in the .NET binary executable. This clearly indicates that obfuscation has been implemented globally across both server and client components.

Figure 9: Network traffic demonstration

Capabilities of Crimson RAT:

The RAT implements comprehensive surveillance capabilities:

- o Desktop screen recording
- o Capturing and streaming webcam
- o Recording of audio via the microphone

Robust disk manipulation features enable data exfiltration and system reconnaissance:

- o Listing of available drives
- o Advanced search functionality to locate specific file types
- o Bidirectional file transfer: Upload and download
- o Targeted deletion capabilities

System intelligence gathering:

- o Current username and privilege level enumeration
- o OS version
- o Identification of installed antivirus products, firewalls and security tools
- o Interface details, IP addressing, routing tables and network connectivity status

Process manipulation capabilities provide:

- o Real-time listing of running processes
- o Selective killing of processes
- o Arbitrary command execution
- o Download and execution of additional malicious components or tools

Figure 10: User information gathering

Figure 11: Code snippet about screen capturing functionality

Infrastructural artifacts

The samples we analyzed were observed communicating with a command-and-control server hosted at 93[.]127[.]133[.]9, has historically been resolving multiple other domains. The infrastructure is in Kansas City in the United States, and is part of **ASN 401479** belonging to **DBM-ASN-KC**.

According to our analysis, this specific infrastructure has connections to previous campaigns of the same group, specifically using the domain **certstorein[.]shop**, targeting government sector, using the lure of document submission followed by deploying malicious macro, leading to another distinctive implant known as [GymRAT](#), discovered by other security researchers.

Pivotal findings

We pivoted based on filenames and certain artifacts related to this campaign. Initially, looking at the filenames and its alternate filenames, we found that the malicious LNK, which was uploaded under the name **Meet Bishkt.xlsx.lnk**, had also been uploaded as **Evidence.pdf.lnk**. By examining the naming scheme and the repeated misspelling of “Evidence,” **where the letter “e” was replaced with “a,”** we pivoted on this pattern to identify similar activity across other campaigns.

In this campaign, we observed the use of a similar version of the Crimson RAT payload, along with links to [other campaigns targeting government sectors](#). Analysis of the decoy document revealed a message stating, “There was an error opening this document. Access denied.”

Finally, we discovered two further decoys, with a similar naming convention, having the files **Evidence1_.pdf** and **Evidence for RR Number.jpeg**.

While analyzing the remaining decoys, we identified a set of notable images, including a purchase receipt and photographs taken from an individual computer in what appears to be a personal or office environment, with an “Award of Excellence” visible. Geolocation and contextual indicators suggest that both originate from India.

Although these files were identified on VirusTotal through pivoting and are not directly tied to a specific campaign or other known artifacts, their filenames follow the same naming scheme and share similar characteristics; namely, image-based content embedded within PDFs. Based on these overlaps, we’ve assessed with medium confidence that these files were part of the threat actor’s resource development activities, likely intended to support the creation of realistic operational or social engineering material.

Conclusion

This campaign highlights Transparent Tribe’s (APT36) shift from traditional government targets toward India’s startup ecosystem — particularly, firms operating in OSINT and cybersecurity. The use of Crimson RAT to deliver via startup-themed lures and container-based files reflects a continued reliance on proven tooling adapted for new victim profiles. Reuse of malware, infrastructure and tradecraft across earlier campaigns strongly reinforces attribution and demonstrates that emerging technology sectors are now core intelligence targets, along with the previous sectors.

Detection by Acronis

This threat has been detected and blocked by Acronis EDR / XDR:

Figure 12: Acronis detects and stops Crimson RAT

IoCs

Samples

Filename

MD5

Description

MeetBisht.iso

5c4488b4eda72d245dac5382f3587f09

ISO attachment

Meet Bisht.xlsx.lnk

4976ef0054b0283c0d013be2f442e17b

Malicious shortcut

Excel

5b4a48815446cd40d8e141cbf8582296

Crimson RAT

mycsd.bat

22218f19425b78dfd6a4f42e43f5486f

Runner batch script

Meet_Bisht.xlsx

47a55959c1eee2ea3a8885f8e08eb3ab

Decoy excel file

Servers

Host

Description

93.127.133.9

Crimson RAT's C&C server

sharmaxme11.org

Crimson RAT's C&C server

© 2003–2026 Acronis International GmbH.